GESELLSCHAFT
FÜR INFORMATIK

Heiko Roßnagel, Christian H. Schunck,
Sebastian Mödersheim, Detlef Hühnlein (Eds.)

Open Identity Summit 2020

26. - 27.05.2020
Copenhagen, Denmark

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-305

ISBN 978-3-88579-699-2
ISSN 1617-5468

Volume Editors
Heiko Roßnagel | Christian Schunck
Fraunhofer Institute for Industrial Engineering IAO
Nobelstr. 12, D-70569 Stuttgart, Germany
heiko.rossnagel|christian.schunck@iao.fraunhofer.de
Sebastian Mödersheim
Sebastian Mödersheim
Technical University of Denmark Compute
Richard Petersens Plads, Building 324, Room 180
DK-2800 Kgs. Lyngby, Denmark
samo@dtu.dk
Detlef Hühnlein
ecsec GmbH
Sudetenstr. 16, D-96247 Michelau, Germany
detlef.huehnlein@ecsec.de

printed by Köllen Druck+Verlag GmbH, Bonn

Preface

Welcome to the “Open Identity Summit 2019”, which has been jointly organized by the Special Interest Groups BIOSIG within the German Computer Science Society (Gesellschaft für Informatik) and the Technical University of Denmark.

The international program committee performed a strong review process according to the LNI guidelines with at least three reviews per paper and accepted 50 % of the 24 submitted papers as full scientific papers.

Furthermore, the program committee has created a program including selected contributions of strong interest (further conference contributions) for the outlined scope of this conference.

We would like to thank all authors for their contributions and the numerous reviewers for their work in the program committee.

Copenhagen, 22nd of April, 2020

Heiko Roßnagel
Fraunhofer IAO

Christian H. Schunck
Fraunhofer IAO

Sebastian Mödersheim
DTU Compute

Detlef Hühnlein
ecsec GmbH

Conference Chairs

Heiko Roßnagel, Fraunhofer Institute for Industrial Engineering IAO
Christian H. Schunck, Fraunhofer Institute for Industrial Engineering IAO
Sebastian Mödersheim, Technical University of Denmark Compute
Detlef Hühnlein, ecsec GmbH

Programme Committee

Franco Arcieri, Italy
Moez Ben MBarka, France
Arslan Broemme, Germany
Christoph Busch, Germany
Victor-Philipp Busch, Germany
Andrea Caccia, Italy
Jörg Caumanns, Germany
Juan Carlos Cruellas, Spain
Roger Dean, United Kingdom
Jos Dumortier, Belgium
Lothar Fritsch, Sweden
Walter Fumy, Germany
Igor Furgel, Germany
Robert Garskamp, The Netherlands
Ulrich Greveler, Germany
Marit Hansen, Germany
Olaf Herden, Germany
Gerrit Hornung, Germany
Detlef Houdeau, Germany
Detlef Hühnlein, Germany
Tina Hühnlein, Germany
Jan Jürjens, Germany
Ulrike Korte, Germany
Michael Kubach, Germany
Andreas Kuckartz, Germany
Andreas Kühne, Germany
Sebastian Kurowski, Germany
Herbert Leitold, Austria
Peter Lipp, Austria
Luigi Lo Iacono, Germany
Milan Markovic, Serbia
Tarvi Martens, Estonia
Gisela Meister, Germany
Daniela Merella, Italy
Alexander Nouak, Germany
Sebastian Pape, Germany
René Peinl, Germany
Henrich Pöhls, Germany
Kai Rannenberg, Germany
Alexander Roßnagel, Germany
Heiko Roßnagel, Germany
Carlos Sanchez, United Kingdom
Aleksandr Sazonov, Russia
Christian H. Schunck, Germany
Jörg Schwenk, Germany
Jon Shamah, United Kingdom
Maurizio Talamo, Italy
Don Thibeau, United States
Tobias Wich, Germany
Thomas Wieland, Germany
Alex Wiesmaier, Germany
Jan Zibuschka, Germany
Jan Ziesing, Germany
Frank Zimmermann, Switzerland

Hosts and Partners

BIOSIG – Biometrics and Electronic Signatures (www.biosig.org)
The special interest group “Biometrics and Electronic Signatures” (BIOSIG) within GI e.V. is dedicated to the fundamentals, methods, techniques, processes and implementations used to guarantee the authenticity and integrity of entities.

Table of Contents

Open Identity Summit 2020 – Regular Research Papers

Open Identity Summit 2020 – Further Conference Contributions

Open Identity Summit 2020

Regular Research Papers

Identification collapse - contingency in Identity Management

Lothar Fritsch[1]

Abstract: Identity management (IdM) facilitates identification, authentication and authorization in most digital processes that involve humans. Digital services as well as work processes, customer relationship management, telecommunications and payment systems rely on forms of IdM. IdM is a business-critical infrastructure. Organizations rely on one specific IdM technology chosen to fit a certain context. Registration, credential issuance and deployment of digital identities are then bound to the chosen technology. What happens if that technology is disrupted? This article discusses consequences and mitigation strategies for identification collapse based on case studies and literature search. The result is a surprising shortage of available documented mitigation and recovery strategies for identification collapse.

Keywords: Identity management; business continuity; cybersecurity; contingency management

> No death, no doom, no anguish can arouse the surpassing despair
> which flows from a loss of identity. – H.P. Lovecraft

1 Introduction

Identity management (IdM) is a critical function in many contexts. Its sudden unavailability will disrupt various processes that rely on IdM, and may cause major information security compromize or financial damage to the affected organizations or persons. I call this disruption *identification collapse*. It should be planned ahead for, and there should be resources for mitigation at hand.

This article reviews literature, standards and reports that are concerned with identification contingency. It then discusses identification collapse against case examples, both from reality as well as hypothetical ones. Specific threats and particular mitigation strategies follow the cases.

[1] Karlstad University, Dept. of Mathematics and Computer Science, Universitetsgatan 2, Karlstad, Sweden
lothar.fritsch@kau.se

1.1 Identification collapse

Definition: *Identification collapse is the unexpected disruption or loss of identity management which has negative impact on business processes and may compromize relying parties' and credential holders.*

Identification is the foundation of system access, customer relationships, supplier inclusion, payments, and increasingly the basis for the management of devices on the Internet of Things. Identification collapse will disrupt those processes, and therefore needs attention.

1.2 Background: Literature overview

In this section, a background search for identification failure, contingency and mitigation strategies is presented. There is a surprisingly low number of publications that investigate preventative, corrective or compensatory strategies for identification failure available in scientific literature. Security standards demand unspecific safeguards to be taken. A literature search on e-ID contingency has been performed on Google Scholar using the search keywords below:

digital identity contingency, digital identity management contingency, digital identity management business continuity, digital identity management disaster recovery, identity provider compromised business continuity, identity provider compromise disaster recovery, identity correlation, digital identity substitution, digital identity replacement, Identity Relationship Management

The search resulted in zero scientific publications from the computer science, technology or information systems domain that were clearly focused on the collapse of IdM and of its contingency management. In the patents category, a number of patents that deal with recovery passwords and additional authentication factors for credit cards appeared. The search was then repeated on the regular Google.com search engine with the same list of keywords. This resulted in a large number of reports from consulting firms that offer business continuity services for various core IT services. IdM systems were briefly and in very unspecific ways mentioned as critical assets in the context of the IT managment standard ITIL for business continuity management. The most advanced perspective on identification contingency was found in documents from the financial sector, namely in reports from the EU project *Parsifal* (2008-2010, by now expired from the Internet), and in later proposals for governments that offer the financial sector's IdM services to governments and to global actors [Mc16]. Searching for particular actions that support recovery from a total breakdown of IdM that will require re-issuance of credentials, notable only the United Nation's UNHCR disaster relief agency has a clearly formulated strategy for the mass issuance of new digital identity under adverse conditions [UN18]. An estimate of the efforts of re-issuance can be gained from section 2, 'Registration and Issuance Requirements' in the Federal Identitiy Management Handbook [FICCB05]. The Australian Identity Proofing

Requirements require identity providers to document their recovery and disaster procedures in an operations handbook [Au18]. The operations manuals are not published, though. They recommend:

Establish and maintain an Identity Service Provider Operations Manual, which at a minimum includes the following information: (...) Processes, procedures and workflows used to support the IdP's identity management functions (i.e. access control, storage, backup, archive and retrieval, disaster recovery, business continuity and records management) (...)

The International Civil Aviation Organization defines guidelines for thorough identification of flight passengers [IC18], which provide further insight into re-registration efforts. No dedicated mention of strategies or technologies for redundant IdM infrastructures, suppliers or fallback mechanisms with proportional security levels were found in the search. Summarizing the search I conclude that there is very little explicit guidance on disaster preparedness, recovery, mitigation and business continuity published that specifically targets identity management as a critical infrastructure.

2 Case examples of Identification collapse

This section will illustrate the concept of identification collapse. For this purpose, three case studies about collapses relevant to the end user are used to describe identification collapse. The following autoethographic case studies [Ma10] show identification collapse and discuss its consequences specific to the use case. Autoethonography is, according to [Ma10], *a form or method of research that involves self-observation and reflexive investigation in the context of ethnographic field work or writing*. It refers, among others, to *reflexive accounting of the narrator's subjective experience and subjectivity. (...) Systematic, self-conscious introspection enables the disciplined analysis of personal resonance and the effects of the researchers' connections wit the research situation on their actions and interpretations, in dialogue with the representations of others*.

2.1 Case 1: Swedish Railway - customer profile passwords insecure

A Swedish railway company servicing international connections offers customer web pages with individual ticketing services, payment options and loyalty program functions. Customers can pay loyalty points to obtain tickets, review their travel history or order and download tickets. Authentication is based on e-mail/password, while payments are authorized via credit cards' mechanisms. Customers provide a citizen number and address when registering for the loyalty program. In 2019, the railway carrier detected password hacking activities with the goal to issue tickets with loyalty points from hacked customer web accounts. As a reaction, spending loyalty points was restricted to the mobile phone app, and required a Swedish BankID installed and activated on the phone. The BankID is only

available to persons who are living in Sweden, have a Swedish citizen number issued, and who use a Swedish mobile phone subscription. Other customers are referred to the telephone hotline for assisted ticketing. By moving from a cheap one-factor password solution to a national identity silo that has strong dependencies (citizen number, bank account, local phone card), the railway company alienated most of its international customers. In addition, they increased costly traffic on their phone hotline, where callers identify by speaking their loyalty number and a PIN code, which both are visible in the customer profiles once an attacker has logged in. The situation persists as of January 2020. So far, no alternative authentication methods or other efforts have been communicated that may ease the situation. The company has no alternative identification strategy.

Summary: Train company has no digital back-up identification channel. All international customers, such as cross-border commuters, are excluded from on-line booking and app booking services based on the loyalty program. Cost occurs for phone service. Alternative identification via phone is equally insecure as web passwords. Duration of problem: very long. Tab. 1 shows an assessment of the compromized IdM services.

Cause (internal, external)	Scope		Affected IdM phase				
	Small scope	Global scope	Registration	Issuance	Provision	Termination	Archive
I: Weak authentication compromized, fallback to telephone service		X	Attributes may be changed by attacker	Credential available to others	Identification compromized	-	Archive accessible to other parties, archive content potentially compromized.
Consequences	Large-scale identification collapse for foreign customers. Business process endangered, identity compromized in four out of 5 phases, alternative oral password authentication via phone, foreign and 'dumb phone' customers alienated.						

Tab. 1: Classification of Swedish railway identification failure.

2.2 Case 2: Norwegian BankID - token battery low

The Norwegian BankID uses a code generator as a second, personalized and hardware-based authentication factor. It is issued based on a bank account, which in turn is based on citizen numbers or passport identification. BankID offers authentications to other sectors, including government. It is the most commonly used electronic identity for signing up to new services in Norway. However once the token battery is low, the renewal of the token is performed in a disruptive way: The existing token is deactivated immediately when ordering a new

token - which then is sent by physical mail with expected three days delivery time, including the usual risks of lost mail, postal strike, weather-caused and seasonal delivery delays. For the delivery period, the BankID owner technically is unidentifiable for banks, private sector or government services. The bank offered a back-up identification channel: it advised its customer to use a Mobile BankID in the meantime, an alternative credential that is issued based on BankID to Norwegian phone subscribers with smart phones. However, the customer was not advised to install and activate Mobile BankId before the BankID token was blocked. Neither had the bank a suggestion for users who may use other phones or foreign phone cards.

Summary: Bank has an equally secure back-up credential based on BankID, which however has dependencies towards phone subscriptions and phone hardware which impose customer cost. The risk of being unidentifiable is limited to a few working days while the postal distribution works as expected. Tab. 2 shows an assessment of the compromized IdM services.

Cause (internal, external)	Scope		Affected IdM phase				
	Small scope	Global scope	Registration	Issuance	Provision	Termination	Archive
I: Token renewal procedure causes delay or imposes cost	X		-	Issuance has delay OR demands expensive alternative channel	Identification prevented	-	-
Consequences	Short period of service denial for users without national smartphone solution.						

Tab. 2: Classification of bank token replacement identification failure.

2.3 Case 3: Norwegian BankID registration issue - re-newal of registration

One immigrant customer of a Norwegian bank had opened additional bank services within his bank with his BankID token. After Norway changed regulations for identity verification, banks had to re-assess customer identity. This process led to the discovery of the fact that the aforementioned customer's citizen number was incorrect in the BankId certificates due to issuance of a new citizen number. However the bank's procedures did not allow for change of citizen numbers bound to accounts and financial assets. Different departments were handling the update of the identity attribute 'citizen number' in different ways. Regular accounts were deleted and set up anew (with significant delays until old correspondence had been manually retrieved from back-up). Investment assets were preserved, while the

investment department had procedures for re-registration that demanded physical presence and passport-showing for the re-issuance of the authorization to access the financial assets.

Summary: Bank had no procedures for change of core identity attributes (or, in a wider perspective, for a registration failure with credential issuer). Various procedures for recovery applied which involved several days of inconsistent access to services and documents as sell as required a physical visit to the bank to verify passports. Tab. 3 shows an assessment of the compromized IdM services.

Cause (internal, external)	Scope		Affected IdM phase				
	Small scope	Global scope	Registration	Issuance	Provision	Termination	Archive
I: Identity attribute expired	X		Registration compromized	Identification revoked	Provisioning denied	-	-
Consequences	Several day of identification collapse leading to major manual procedures for content recovery, identity mapping and re-resgistration of customer.						

Tab. 3: Classification of banking attribute renewal identification failure.

There has been, in addition, a major collapse with an issuer of commercial web certificates, *DigiNotar*, which was hacked and then used to issue large numbers of fake certificates. Only after several months this was discovered, and business terminated by the Dutch government . Here, registration and issuance were compromized, then provision stopped. Certificates were not person certificates, though.

3 Causes and Consequences of identification collapse

Consequences of identification collapse have a wide bandwidth of impact on business continuity. As seen from the cases above, impact ranges from shorter waiting times for renewal to multi-month identification failure.

3.1 Types and magnitude of identification collapse

Generalizing the root causes, identification collapse can be caused by the following causes of failure:

Technological failure: Breakdown of core technologies involved in IdM, including compromized cryptography;

See full descripition: https://www.enisa.europa.eu/media/news-items/operation-black-tulip, accessed 03-Apr-2020

Procurement failure: Externally procured IdM is unavailable or compromized. IdM is procured along a supply chain from external providers, either as the whole service, as a cloud service or in part through technological platforms or processes controlled by suppliers;

Administrative failure: Wrongly executed procedures under registration, revocation or attribute handling compromize digital identities and relying services.

Force majeure: Operations of IdM are discontinued due to higher forces such as natural disasters, war, bankruptcy or global crisis.

The magnitude of the collapse can appear in a wide range. As illustrated in the case examples above, only parts of the user base may become excluded. Technological issues or registration problems may appear locally only. On the other hand, compromized cryptography, lack of back-up authentication methods, comprimized registration data of the whole user population or technological disasters may shut complete services down, which creates a negative event of high magnitude. Magnitude is best expressed in the number of digital identities affected as well as in how much of an identity ecosystem will be affected for how long:

$magnitude =$
(number of users affected $\bigotimes$ number of services affected $\bigotimes$ duration of collapse)

Risk managers should therefore model the magnitude of identity collapse not only from a perspective of data compromize, privacy breach or access control failure, but in addition in the perspective of loss of service and exclusion of customers in face of the planned recovery channels for identification. Commonly appearing consequences of major identification collapse will be: Access control systems compromized; External relationships break (customer relations); Critical services stop (payment, public services, private services, signing); Historic authorization and non-repudiation endangered (prior signatures or transactions or certificate validity back in time not verifiable) (see 7.3.5 in [Wi07]).

4 Mitigation and business continuity

Due to the very small body of literature found in the literature search (see Sec. 1.2, this section will present reasoning and options for handling identification failure for the sake of business continuity. While there are many operational requirements such as ensuring equivalence in information security parameters such as trustworthiness, security, usability and privacy, in addition aspects of integration, cost, time-to-deployment, of international availability and regulatory issues will come into play. The analysis in this section focuses on the phases of identity management in a perspective of technical and administrative controls to prevent, mitigate or compensate identity collapse. When looking for mitigation of identification collapse, certain requirements occur naturally:

- equivalence of security, privacy, usability and integration/application cost;
- short time-to-availability in case of replacement;
- availability to user base, e.g. hardware tokens, cross-border availability for customers or users from other countries.

In addition, a crisis communication strategy [WP17] that targets the user base and the relying parties has to get planned. Depending on the root causes, other communications such as data breach notifications must be included [Fu16, KJP17].

4.1 Technologies for mitigation

Technological solutions or identity contingency are available. Below a variety of building blocks will be summarized. They include identity federations [Su05], identity brokerage, biometric anchoring, identity correlation and blockchain-based approaches.

Identity brokerage: The FutureID research project has developed an identity brokerage infrastructure that uses a centralized Identity Broker that has the ability to extract identity attributes from various identity providers [BR16]. Thereby it is able to extract attributes from the same person's various digital identities, connecting them into a new synthetic identity. The Identity broker could be used such that upon technical compromize of an IdM system it would request identifications from other identity silos based on the just compromized identity. This method requires a pre-established brokerage federation, though. It does not overcome issues with archive compromize, and does not help in situations where identity registation is compromized. It is however an effective way to establish a short-term emergency identification mechanism.

Biometric authentication factors: Using biometric authentication as an additional authentication factor for re-registration will help re-establishing credentials. While biometrics are not without issues (reliability, survellance and privacy issues), they could be used as a recovery channel for more efficient registration or issuance.

Verifiable cryptographic identity correlation: Identity correlation connects identities across silos, and thereby supports swift contingency management . Keybase is a service that allows its users to cryptographically verifiably prove ownership and correlation of digital identities such as social media accounts. Credential owners can create links between their existing identities. However, replying parties must prepare to accept Keybase proofs, and then be ready to connect to the alternative identity silos. Identity correlation is therefore weaker as brokerage as it only shows correlation, but does not provide federation services.

Identity correlation, `https://en.wikipedia.org/wiki/Identity_correlation`, 20200131
See `https://github.com/keybase/client`, 20200131

Block chain securiztation of IdM: Archival of relevant status information can be facilitated with block chain technology [EHEK19, NJ19]. Several approaches are under scientific investigation:

- Cross-referencing identities as equivalent through a public block chain by credential issuers (thereby creating the foundation for federations);
- Recording of identity history in a block chain for rollback;
- Self-sovereign identity management (SSI) enables credential holders to register and publish their credentials on block chains for reference for others [NJ19].

Mapping digital identities into each other and at the same time keep track of relevant trust information in block chains may solve a number of issues when recovering from registration or archive compromize. As discussed in [Fr13], growing complexity of the identity ecosystem will degrade the quality and value of identity management. SSI may enable credential holders to reference an alternative IdM silo and would in consequence enable the acceptance of an alternative credential by the relying party.

Standards for identity federation and brokerage: Standardized formats, protocols and algorithms for IdM will help prevent identification collapse. Compatible infrastructures as suggested in OPAL [HP18] will enable swift recovery from infrastructure or technology failure.

4.2 Administrative measures

In addition to technological preparedness, administrative measures that lower risk of identity collapse as well as procedures for mitigation and recovery must be in place. For each phase of the IdM lifecycle, thorough analysis of the administrative issues with identity collapse should get performed, in particular:

- Planning for ID continuity with back-up channels and back-up registration methods with high throughput and appropriate geographical spread;
- Deployment of identity brokers that help include the best possible alternative across multiple industrial digital identities (e.g. inclusion of banks, mobile operators, government IdM);
- Consideration of eIDAS as a recovery channel for persons who own multiple, independent government credentials (however eIDAS is mostly designed to project national sovereign IdM into other countries);
- Train staff for migration activities, such as re-registration of users based on identity documents or a variety of electronic identities.

Further considerations that are important are alternative authentication channels used for either using back-up channels, to federate or broker identities, or to re-register efficiently.

Availability of alternative identification channels: Review of existing back-up channels (alternative or multiple IDs) for customers will support the establishment of recovery channels (e-mail, multiple e-mail, phone numbers for SMS, security phrases, "recognize your friends"). What will be the 'anchor' identity (e.g. passports, bank IDs, social security numbers)?

Emergency registration procedures: The UNHCR has very explicit procedures for the set-up and registration of large populations of refugees in cases of disaster. Biometrics are used to anchor registration into IdM systems [Lo16] as part of the United Nation's UNHCR Guidance on Registration and Identity Management [UN18]. In its Future of Financial Services Series, the World Economic Forum (WEF) has analyzed the potential and the roles of the global and national financial institutions in identity management [Mc16]. In its report, the WEF concludes that the most resilient, reliable and user-friendly structure of IdM should either be organized as a silo or as a network of collaborating providers using standardized technologies (pp. 62, centralized or distributed identity).

4.2.1 Problems caused by mitigation

Mitigation strategies may have side effects. They open up identity silos, and may therefore cause issues concerning information privacy, secrecy or even sovereignity over IdM ecosystems. Landau and More [LM12] identify several issues that impair economic success of federated IdM: Issues of trust and liability across federations occur as well as reliability and the distribution of duties/benefits between participants. Data privacy when sharing attributes in federations is a major issue.

- Identity silo collapse: Federation or correlation of separate identities for contingency may lead to identity leakage, pseudonym compromize or privacy breaches (see [Ja15] for example on how swift biometrics deployment in a no-alternative-choice disaster relief registration campaign takes decision power from individuals).
- Degradation of security level through contingency solution;
- Exclusion and discrimination of parts of the user base through chosen alternative channels, e.g. through geographic limitations, nationality or individual disability [FFS10].

In addition, fraud protection will face major challenges in case of mitigation through alternative identification channels. The only viable solution in this context will be the pre-establishment of trust in IdM quality through common standards and procedures, e.g. in

industry sector organizations such as the financial industry, in the government sector and in critical infrastructure protection.

5 Conclusion

Identification collapse is a serious threat to business continuity. It can be caused by technical and non-technical issues. This article shows that there is little scientific work on preventive and contingency strategies and options to prevent or to mitigate identification collapse,in spite of available technologies and tactics. Cases have shown that relying parties show a wide spread in their preparedness for alternative identification channels or for business continuity. A general impression persists that either weak and cheap identification methods are used (social media single-sign-on, passwords or phone numbers), more secure two-factor authentication being restricted to national silos in spite of European Union efforts, and finally the back-up channel being off-loaded to smartphones paid for by the credential holder. In various industry standards, general precautions and measures are suggested, however not specified. Most concrete are guidelines for identity verification documents upon registration from a variety of organizations, including air travel and international disaster relief. In summary, there is a lack of knowledge in various important aspects of Identification collapse that should be further investigated. Strategies, technology and processes for emergency re-registration or federation of identities will be important, as well as strategies, technologies and solutions for redundant identification, such as digital identity correlation, federation and brokerage between identity silos, industry sectors and governments. Trust status aggregation and risk information about the identity ecosystem supply chain nodes will complement contingency measures.

Identity Management continuity should be regarded as a priority in national cybersecurity policy, and in particular where involved in the operations of critical infrastructures, as identification failure with long recovery times will have catastrophic consequences for most digital infrastructures.

References

[Au18] Australia: Identity Proofing Requirements - Trusted Digital Identity Framework v1.07. Technical report, Digital transformation agency, 2018.

[BR16] Bruegger, Bud P.; Rossnagel, Heiko: Towards a decentralized identity management ecosystem for Europe and beyond. Gesellschaft für Informatik e.V., Bonn, pp. 55–66, 2016.

[EHEK19] El Haddouti, Samia; El Kettani, M Dafir Ech-Cherif: Analysis of Identity Management Systems Using Blockchain Technology. In: 2019 International Conference on Advanced Communication Technologies and Networking (CommNet). IEEE, pp. 1–7, 2019.

[FFS10] Fritsch, Lothar; Fuglerud, Kristin Skeide; Solheim, Ivar: Towards inclusive identity management. Identity in the Information Society, 3(3):515–538, 2010.

[FICCB05] Federal Identity Credentialing Committee, Office of Management; Budget, U.S. Government: Federal Identity Management Handbook (public draft). Technical report, Federal Identity Credentialing Committee, Office of Management and Budget, U.S. Government, 2005.

[Fr13] Fritsch, Lothar: The clean Privacy Ecosystem of the future internet. Future Internet, 5(1):34–45, 2013.

[Fu16] Fuller, Ryan P: The big breach: An experiential learning exercise in mindful crisis communication. Communication Teacher, 30(1):27–32, 2016.

[HP18] Hardjono, Thomas; Pentland, Alex: Open algorithms for identity federation. In: Future of Information and Communication Conference. Springer, pp. 24–42, 2018.

[IC18] ICAO: ICAO TRIP Guide on EVIDENCE OF IDENTITY v5.3. Technical report, ICAO Security and Facilitation, 2018.

[Ja15] Jacobsen, Katja Lindskov: Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees. Security Dialogue, 46(2):144–164, 2015.

[KJP17] Kim, Bokyung; Johnson, Kristine; Park, Sun-Young: Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. Cogent Business & Management, 4(1):1354525, 2017.

[LM12] Landau, Susan; Moore, Tyler: Economic tussles in federated identity management. First Monday, 17(10), 2012.

[Lo16] Lodinová, Anna: Application of biometrics as a means of refugee registration: focusing on UNHCR's strategy. Development, Environment and Foresight, 2(2):91–100, 2016.

[Ma10] Marechal, G: , Autoethnography. Albert J. Mills, Gabrielle Durepos and Elden Wiebe (Eds.), Encyclopedia of case study research (Vol. 2, pp. 43-45), 2010.

[Mc16] McWaters, Jesse: A Blueprint for Digital Identity - The Role of Financial Institutions in Building Digital Identity. Technical report, World Economic Forum, 2016.

[NJ19] Nauta, Jelle C; Joosten, Rieks: Self-Sovereign Identity: A Comparison of IRMA and Sovrin. Technical Report TNO2019R11011, 2019.

[Su05] Sullivan, Roger K: The case for federated identity. Network Security, 2005(9):15–19, 2005.

[UN18] UNHCR, United Nations: UNHCR Guidance on Registration and Identity Management. Technical report, United Nations UNHCR, 2018.

[Wi07] Wisse, Pieter: Semiotics of identity management. In: The History of Information Security, pp. 167–196. Elsevier, 2007.

[WP17] Wang, Ping; Park, Sun-A: Communication in Cybersecurity: A public communication model for business data breach incident handling. Issues in Information Systems, 18(2), 2017.

Digital and mobile identities

Holger Funke[1]

Abstract: In this paper current developments in mobile identities are described. A scalable architecture, standard future-proven technologies such as ISO/IEC 23220 and a Cryptographic Service Provider build the framework for secure, failsafe and large deployments. The building blocks specified in ISO/IEC 23220 deliver a framework that can be easily used for identities stored on secure devices such as smartphones. This paper lists a selection of outstanding projects using mobile and digital identities in the field of mobile ID. The focus is on Digital Travel Credentials (DTC) which are currently specified by the International Civil Aviation Organization (ICAO).

Keywords: Mobile ID, Digital ID, Digital Travel Credentials, Smartphone, Cryptographic Service Provider, eIDAS, identification

1 Introduction

As in many areas of life, a paradigm shift from 'one size fits all' to 'bring your own device' can be observed for the use of official documents. People have become accustomed to completing their daily tasks with their smartphone and now want to do the same with their eID card or eMRTD (electronic machine readable travel document). After all, they almost always carry their smartphone with them and are used to using it or even expect to use it for a wide range of applications. Examples include airport boarding passes or entrance tickets, which many people prefer to access digitally via their smartphones instead of in paper form. Rail transport passengers are also increasingly using their smartphones to store tickets and specific railway cards digitally.

Which technological options already exist for a digital or mobile identity and what international efforts are being made to uncouple official identities from their previous form factor and digitise them? One idea is the 'ID Wallet', through which the owner can manage and release a range of identities online and offline, from user ID cards and driving licences to passports. The smartphone is fast becoming the focus of such efforts and is playing an increasingly important role for users – particularly for identification and authentication. A survey conducted by the International Air Transport Association (IATA) in 2017 showed that air passengers want to use their smartphones more and more at the airport. Design and technical aspects of identification and authentication are playing an increasingly important role not only online, but also in the real world. Given the ubiquity of smartphones, it makes sense to use them to store identity data. Of course,

[1] secunet Security Networks AG, Division Homeland Security, Paderborn, holger.funke@secunet.com

the security of the data stored is of great importance, as it constitutes key information about each individual.

The guidelines of the German Federal Office for Information Security (BSI) [Fe19] and the EU's eIDAS Regulation [Eu14] therefore specify rules for the implementation of authentication procedures in order to achieve specific security levels. However, the smartphone should only be seen as a representative of an entire class of devices. In principle, other mobile devices can also be used for this purpose, for instance smart watches or wearables. Regarding the design and architecture, a few fundamental questions arise:

- Does an original identity already exist and how is it initially transferred to the smartphone derivation?
- Where is the identity data stored? On the smartphone? In the cloud? In a hybrid solution?
- Which interfaces are used to access the data and how is it secured?

The answer to the first question is relatively obvious in the context of official documents: the physical passport or ID card can be used as a secure trust anchor. In the case of emergency documents however, this original identity must be transferred to the smartphone in other ways, as temporary replacement of the document has taken place due to the loss of the original document.

What's even more interesting is the question about the location of the data. Two very different options present themselves here: the smartphone and the cloud. If the data is stored locally, precautions must naturally be taken to ensure that the data can only be read for legitimate purposes. Secure storage systems such as secure elements or smart cards (SIM cards), which are usually installed in smartphones, could be used for this purpose. Similarly, storing the identity in the cloud also requires cryptographic protection, typically using an asymmetric encryption key that requires special protection. In addition, you can combine the two methods and store parts of the data in the smartphone's secure memory and parts in the cloud. The choice of storage location then raises new questions, e. g. how an identity can be restored if the mobile device is lost or destroyed. One solution is My Identity App (MIA): a smartphone-based mobile ID implemented by Österreichische Staatsdruckerei [Tr16].

Just as interesting is the question of which interfaces should be used to read the data. In the context of official documents, the NFC interface offers a possible solution. This is similar to the ISO / IEC 14443 interface used for smart cards so that parts of it can continuously be used. However, there are also other interfaces under discussion, such as Bluetooth or QR codes. Deutsche Bahn uses a QR code for its tickets as a relatively robust interface between the traveller's smartphone and the ticket inspector's reader, for instance. The topic of mobile identities first became popular in the field of electronic driving licences. The standardisation groups that operate in this environment – such as ISO SC17 WG10 – have been working on the question of how to store physical driver's

licence data securely on a smartphone for several years. Since these mechanisms are not limited to driving licences, the technical requirements and proposed solutions are currently being discussed generically in working groups such as ISO SC17 WG3 or the New Technology Working Group (NTWG).

2 Related work

2.1 Cryptographic Service Provider

A fundamental basis for identification and authentication on a substantial level of assurance according to [EP14] is a Secure Element (SE). The SE is capable of hosting various third party applets, e.g. for identification, authentication, public transport, payment, etc. The installation itself of such an applet by a Trusted Service Manager (TSM) is independent from the concrete applet. The administration of applets (loading, installation, deletion and personalisation) can be implemented based on Trusted Service Management Systems (TSMS). Generally the security mechanisms of the applet hosted by the SE can also be proven by security certification. Usually Common Criteria demands a composite certification of the applet in conjunction with the underlying Protection Profile of the underlying SE. To allow installation of CC-certified applets without the need of a Composite Certification of the applet on top of each type of SE, the cryptographic functionalities are encapsulated in a Cryptographic Service Provider (CSP), providing secure cryptographic services to the applet. Since the CSP's security services are logically separated and provided through well-defined external interfaces, the operational environment cannot affect the security and correctness of the CSP. Consequently, the security functionalities of the applet can be certified independently. All functionalities can be implemented on the SE itself or alternatively the SE can provide a key store/management back end for a CSP implemented outside of the SE. In both cases, the Secure Element itself must be certified on at least Assurance Level EAL4+AVA_VAN.4. [Kü20]

2.2 ISO/IEC 23220

This standard series provides building blocks for mobile eID System infrastructures and normalizes protocols, interfaces and services for mobile eID Apps and mobile verification applications. This is done by specifying generic system architectures of mobile eID Systems, generic transaction flows of mobile eID Systems and generic lifecycle phases of mobile eID Systems. One important part of this standard is the secure area of a secure device which can be implemented by several types of secure elements, e.g. embedded universal integrated circuit card (eUICC), embedded secure elements (eSE) or Trusted Execution Environments (TEE) [ISO20].

3 Current projects around the world

3.1 Mobile Driving Licence

The mobile Driving Licence (mDL) was the first popular initiative transferring an ID onto a smartphone. Based on existing chip-based electronic driving licences standardized in ISO/IEC 18013 [ISO18] a mobile driving licence is specified in this series now. The purpose of this standard is to standardize interface specifications for the implementation of a driving licence in association with a mobile device. It standardizes the interface between the mDL and mDL Reader, and the interface between the mDL Reader and the issuing authority infrastructure. Key functionality is the access to the security anchor of the smartphone. To authenticate the origin of the mDL data and to verify the integrity of the mDL data, it is necessary to get access to the secure element that is used in the smartphone. Therefore, the mDL uses protocols that are standardized in ISO/IEC 23220.

3.2 Digital Travel Credentials

In 2016 the ICAO New Technologies Working Group (NTWG) established a specialised subgroup in cooperation with the International Organization for Standardization (ISO) to standardise digital travel credentials (DTC). Such credentials can be issued or applied in a digital format, e.g. on smart devices or on servers. A DTC could temporarily or permanently substitute a conventional passport by a digital representation of the traveller's identity. To assure security and convenience a DTC has to provide similar functionality and security features that are comparable to those of a current eMRTD. The role of ICAO is to define policies and use cases in this context; the role of ISO is to specify technical guidelines.

One important advantage of an eMRTD is the digitisation of the traveller's biographic and biometric data stored in a chip embedded in the document. The chip data already offers many benefits, including the verification of the passport holder's identity through facial recognition and providing authorities with the tools to verify and to authenticate the ePassport. Therefore, the eMRTD is the template and the reference for the idea of digital travel credentials. The ICAO has defined several core principles for DTC in [IA18]:

- The DTC must be at least as secure as an eMRTD.
- The information contained in the DTC must be derived from the Travel Document Issuing Authority's data, and may come directly from the eMRTD.
- The lifecycle management of the DTC must not necessarily be dependent on the lifecycle management of the eMRTD.
- Incompatible changes must not be required in the current eMRTD standards or in the current process of issuing eMRTDs.

- The revocation of a DTC may result in a revocation of the eMRTD associated with this DTC at the discretion of the issuing State.
- The revocation of the eMRTD must automatically revoke all underlying DTCs.
- The DTC must be issued by a Travel Document Issuing Authority.

3.2.1 Form factor of DTC

A number of different form factors for storing a DTC have been evaluated by ICAO, and at the end the preferred one is a hybrid model that would consist of a virtual component (DTC-VC) and a physical component (DTC-PC). The virtual component acts like a credential that is linked to at least one physical component (authenticators). The technical specifications are developed by ISO SC17 WG3 and contain protocols, data structures and PKI [IA19].

The benefit of a hybrid travel credential is the combination of a virtual and a physical travel credential in a way that the advantages of both approaches are merged while the disadvantages are minimised.

To achieve this, a virtual travel credential is linked to one or more physical devices that perform additional active authentication or chip authentication of the credential when required for increased security. A hybrid travel credential may be used as virtual travel credential alone where cloning protection may be arranged differently. In use cases where a stronger binding is required, it may additionally be verified that a linked physical token (the eMRTD) is in possession of the traveller, e.g. through biometrics.

Today an eMRTD can already be considered as a hybrid travel credential using the logical data structure (LDS) as virtual travel credential and active authentication or chip authentication implemented on the chip as the physical token. The virtual credential may also consist of the data stored in a remote system, e.g. a database or a web service, with the physical authenticator being a smart device (e.g. a smartphone) that can be used to retrieve the data from the remote system by authenticating the holder of the physical credential to the remote system.

This is preferred as the credential is already linked to the issuer by passive authentication. The physical token allows the verifier to select the correct virtual credential, with the added benefit of this being potentially provided in advance. It also provides the verifying authority with the flexibility to decide whether the virtual credential is sufficient or the physical authenticator is additionally required for authentication.

The following matrix explains the mapping between the three options defined in the mentioned policy paper and the specifications contained in the technical report:

	DTC-VC data identical to existing eMRTD	DTC-VC data not tied to any existing eMRTD
No separate DTC-PC	Self-Derived	(Not defined)
DTC-PC tied to DTC-VC	Authority Derived	Authority Issued

Tab. 1: Mapping of eMRTD and DTC

3.2.2 Interesting use case

A digital representation of an emergency travel document could be a first use case for the DTC. This solution allows a flexible process to support travellers who lost their ePassport and who are now in need of urgent travel documents yet in a location where delivery of a standard ePassport is either impossible or unfeasible.

In an emergency case a traveller could apply for an urgent renewal enabling the issuing authority to issue a hybrid DTC: essentially a virtual credential with a linked verified physical authenticator provided remotely to the smartphone of the traveller. The citizen could then travel back home or to a location where the ePassport could be collected. This way requires that the DTC is acceptable for travelling (exit and entry for all crossed borders) without the physical passport in the traveller's possession.

The following first projects have started where DTC are used:

- Known Traveller Digital Identity (KTDI) funded by World Economic Forum [KT20]
- New Zealand and Australia are using biometric and logical data structures in a frequent traveller program
- IATA One ID: Document-free process at airport based on identity management and biometric recognition [OI20]

3.3 OPTIMOS 2

OPTIMOS 2 aims at creating an open, usable and secure identity ecosystem for mobile services. Goal of the project is to supply a platform for eID-providers and enable them to offer mobile eID services at eIDAS level "substantial". Another goal is to offer service providers - relying on a certain security level - a secure, privacy friendly platform for mobile services. To assure this security level, access to a secure element of the smart device is essential. The derived holder data (in this case derived from the German ID card) is securely stored in the secure element of the smartphone. A Trusted Service Manager (TSM) grants access to the secure element and allows secure and authentic storing of holders data.

4 Outlook

This list of outstanding projects in the context of mobile ID shows the importance of this topic. Today it is already possible to store eID data on a smartphones with eIDAS level "substantial". As soon as the standards are finalized and officially released they will be the base for several projects and new use cases for mobile identities. The use case "emergency travel document" might be the first milestone in the area of travelling with derived credentials stored on smartphones.

Bibliography

[Fe19] Federal Office for Information Security (BSI): Technical Guideline TR-03159 Mobile Identities, August 2019

[Eu14] European Parliament, Council of the European Union: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[Kü20] Kügler, Dennis (BSI): Identities Go Mobile - The Future of Electronic Identification. In: Omnisecure Proceedings 2020, Berlin

[IA18] ICAO: Policy paper – Digital Travel Credentials, 24.10.2018

[IA19] ICAO: Technical Report – Digital Travel Credentials, Version 0.7, 13.08.2019

[ISO18] ISO: Information technology - Personal identification - ISO-compliant driving licence, 2018

[ISO20] ISO: Card and security devices for personal identification - Building blocks for identity management on mobile devices, 2020

[KT20] Website: Known traveller digital identity: https://ktdi.org/ (last accessed 06.04.2020)

[OI20] Website: IATA One ID: https://www.iata.org/en/programs/passenger/one-id/ (last accessed 06.04.2020)

[Tr16] Terbu, Oliver. et.al.: One mobile ID to secure physical and digital Identity. In (D. Hühnlein, H. Roßnagel, C. Schunck, M. Talamo, ed.): Open Identity Summit 2016, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016

Self-sovereign and Decentralized identity as the future of identity management?

Michael Kubach[1], Christian H. Schunck[1], Rachelle Sellung[1], and Heiko Roßnagel[1]

Abstract: Blockchain-based Self-sovereign and Decentralized identity approaches are seen by many as the future of identity management. These solutions are supposed to finally bring universally usable, trustworthy, secure, and privacy friendly digital identities for everyone and all use cases. This paper first presents the promises of this technological approach. It then discusses some apparent challenges for this new approach and their potential impact.

Keywords: Self-sovereign identity, Decentralized identity, identity management, IT-security, privacy, blockchain, distributed ledger.

1 Introduction

Market researchers still foresee a massive growth potential in the digital identity market [Di20a], [Wh19]. Efforts to provide high assurance electronic identities to European citizens date back by more than 20 years. However, from today's perspective one can argue that significant efforts into developing identity solutions with high levels of assurance have only led to very limited adoption: daily (or even monthly) use by citizens and uptake in the private sector is scarce in the vast majority of European member states (with a few exceptions [Ku20]). The private sector is dominated by the single-sign-on solutions that are in the hands of big international platform corporations and that only provide low levels of assurance.

Therefore, it is no surprise that new approaches based on high-impact technologies, such as distributed ledgers and blockchain, have attracted major attention in the last 3-4 years, both in industry and politics. These often called "Decentralized" and "Self-sovereign Identity" (SSI) solutions, claim to bring identity management to the next level.

However, these novel concepts have their own challenges. Many technologies in the identity management sector that were previously hyped as "revolutionary", such as CardSpace, Uprove, and Attribute Based Credentials, have failed miserably on the market [Up20],[Ro16]. So, the question we would like to address in this paper is the following: will Decentralized identities be able to survive the "hype" and truly live up to the high expectations?

This paper will thus explore the current promises and intentions that are associated with SSI based solutions. We conduct an overview analysis by summarizing the challenges for

[1] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, firstname.lastname@iao.fraunhofer.de

identity ecosystems (chapter 2) and by critically reviewing Decentralized and Self-sovereign identity solutions (chapter 3). We identify critical issues and constructively evaluate what is required for SSI to overcome the identified challenges (chapter 4).

2 Basic challenges for identity ecosystems

Although the world has become increasingly digital in every aspect of life for the last decades, a major problem remains the transfer of personal identity into the digital world. In this context, many issues have been addressed: privacy, security, data protection, interoperability, and user experience. However, what is substantially lacking is a digital ecosystem with sustainable business models and appropriate incentives for all participating entities that can ultimately drive uptake.

The development of secure and federated digital identities in Europe over the past 20 years was driven forward by initiatives such as the "Large Scale Pilots" Stork [Ta15] and Stork 2.0 funded by the European Commission. The results of these pilots formed an important basis for the eIDAS regulation. In Germany, the development of secure digital identities was primarily promoted by the government through the introduction of the electronic identity card (nPA). Despite eIDAS and the nPA, the everyday and private sector use of digital identities by citizens continues to be dominated by username/password applications and the use of single-sign-on systems controlled by big international platform operators, who offer only lower levels of assurance.

Research efforts regarding government issued eIDs have been ongoing and keep addressing missing building blocks for a potential market uptake. For example, there have been publicly funded projects (e.g. FutureID, SkIDenity [Sh15], [Si20]) that have developed an identity broker, which mediates between different identity and service providers, and thus provides a solution for a federated identity management across sovereign and private service providers. Nevertheless, despite of work that has already been invested by the research community and public sector, there are still major challenges being faced by the digital identity ecosystem and a broad use of eIDs has not materialized (except for niche markets, e.g. Estonia).

The identity market still faces problems associated with a complicated multi-sided market that leads to a “chicken or egg” problem [Zi12]. Creating sustainable and balanced trust relationships between identity providers, relying parties and users has also remained a challenge [Zi12]. From an identity provider perspective, there is still a key problem of generating sustainable business models as pointed out in reference [Ku13].

A relying party’s interest focuses on gaining more users or customers that are using a service provided [Zi12]. It favors identity solutions that provide easy onboarding of new customers, and a reasonable security at low cost. As for the relationships between relying parties and users, the challenge remains that these are influenced by indirect network effects and thus difficult to establish top-down.

The main determinant for uptake on identity schemes is still the number of applications and services where they are accepted.

In regards to the user, there have been many claims and assumptions to what features users would like to have in regards to privacy and security. However, these claims often neglect that privacy and security are just two among many other requirements user balance when making decisions and detailed user studies on those claims are often lacking. A study in relation to users' willingness to pay and their preferences regarding identity management systems [Ro14], finds that the users' willingness to pay is generally low and preferences of convenience often overtake privacy and security concerns. Overall, digital identity ecosystems continue to face the issue of generating sustainable business models for identity providers, and of addressing indirect network effects between key players of the identity ecosystem. These issues continue to hamper the uptake and reusability of digital identities.

3 Decentralized identity management and Self-sovereign identity

After describing some key challenges for any digital identity ecosystems, we are now focusing on what is being marketed as the future of digital identity management [Si18],[Ar17]. It promises the key to empower users to reclaim control over their data [Je19],[Al16], and to break the dominance of the platform giants in web identity management, e.g. through making identities easily portable [Va19],[Wa20]. In the following, we will first clarify necessary fundamental terms of Decentralized identity management and Self-sovereign identity concept before turning to the potential that is associated with the concept. Finally, we will take a brief look at current approaches implementing the concept.

3.1 Fundamental terms

A number of particular terms are frequently used in the context of Decentralized and blockchain-based identity management. To avoid misconceptions, we will briefly define the key terms without going into further detail – acknowledging that this is an evolving field and definitions are not universally established yet.

In traditional identity management, every service provider (or relying party) stores credentials of each user and enables them to authenticate directly to the business. However, this also means that the user needs to separately register and authenticate with each individual service they wants to use. Federated identity management simplifies this process for the user. Here, an identity provider or credential service provider as intermediary manages user credentials and enables the user to register and sign on to various service providers. Most blockchain-based identity management approaches, however, follow a user-centric model of identity management. This is supposed to address interoperability, security, and privacy concerns, given the privileged position of the

identity provider. In this model, the user controls their identity data and interacts directly with the service providers – without relying on a trusted intermediary. Verifiable information – credentials that the user received from credential issuers – are being shared by the user on a need-to-know basis. The blockchain as such is mainly used an integrity-protected "bulletin board" for a public key infrastructure (PKI) that supports the mapping of keys to identifiers [Le20]. Following the characterization of a blockchain as a Distributed Ledger Technology (DLT), this concept to manage public keys has been described as Decentralized Public Key Infrastructure [Mü18], [Al15].

Self-sovereign Identity (SSI) is a frequently used term for blockchain-based identity management approaches. The term is not always used consistently, but according to [Mü18], a few key properties of the concept have emerged. Those can be summarized as that a Self-sovereign identity management system allows users to fully own and manage their identity without having to rely on a third party. This can be traced back to the so called *Ten Principles of Self-sovereign Identity* proposed by [Al16] that apply a strong user focus to identity management. Parts of these principles had already been included in the *Seven Laws of Identity* proposed by [Ca05]. [Le20] characterize Self-sovereign identity as a bottom-up approach, where no single entity acts as central authority that has control over identifier origination and/or credential issuance. Identifiers and credentials are solely managed by the users, without requiring any permissions. This is contrasted by the top-down approach that is on the other side of a spectrum of possible organizational structures. In this approach, a central authority controls identifier origination and/or issuance while power may be delegated hierarchically through roles. Here, an owner of the system with control of its governance exists. However, as [Ku19] shows in a survey of blockchain-based IdM systems, the term SSI is used by solutions that do not completely follow a bottom-up approach as well.

Two technical concepts that are an essential part of most blockchain-based identity approaches are Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). Both are currently being developed by the World Wide Web Consortia (W3C), which also illustrates the ongoing standardization efforts around Decentralized identity management.

Recently, a working draft v1.0 for Decentralized Identifiers (DIDs), has been presented [De19]. DIDs are identifiers that can be used for credential exchange and authentication. Ownership of a DID is proven by demonstrating the possession of the private key associated with the public key bound to the DID [Le20]. According to the W3C, the term DID refers' only to the *Uniform Resource Identifier (*URI) with the format *"did:"<did-method-name>":" <method-specific-id>*, for example: *did:example:123ABCdef*. Other elements of the specification are the DID scheme, which is the formal syntax of a DID and the DID method that defines how to implement a specific scheme. This includes information on how to create, update, and deactivate DIDs. A DID resolver returns the DID document for a given DID that contains associated data describing the DID subject, such as public keys, other attributes and metadata [De19]. A universal resolver is currently in development by the Decentralized Identity Foundation (DIF). It is envisioned to enable interoperability between different Decentralized identity management solutions [De20].

The W3C recommendation for Verifiable Credentials (VCs) v1.0 [Ve19] defines a format for credentials that are key element in many blockchain-based identity architectures (but could be used in other architectures as well). A VC is a tamper-proof statement about the subject that is cryptographically signed by its issuer. Besides the statement, it contains metadata linking to the issuer, validity period, cryptographic schemes etc. The VC concept also needs to include a revocation mechanism, which needs to balance privacy aspects with effective revocation. This challenge can be approached in various ways and is one significant difference between the W3C's proposal for VCs and alternative implementations. While in an on-chain claims registry, such as proposed for Ethereum-based IdM systems, issuers can directly add and revoke claims [To17b], the W3C approach does not utilize such a registry. Here, the blockchain is only used to map identifier and authentication method. The W3C approach is more privacy-focused, but makes revocation more difficult and brings challenges regarding collusions between the issuer of claims with the claim holder as described in [Mü18]. Due to the problems associated with the storage of personally identifying information contained in claims on an immutable blockchain that result from regulations such as the GDPR, Ethereum-based IdM proposals are recently moving away from on-chain to off-chain claims as well [Br19]. Therefore, while the concrete implementation of VCs may differ, the fundamental concept of VCs is that of a cryptographically signed credential that is usually under the control of the user and can be passed on to a service provider/relying party. Using different cryptographic techniques, the service provider can check who issued the credential, whether it has not been revoked and to whom it has been issued. This is achieved without the issuer of the credential being directly involved in the process.

Private keys and credentials are usually managed by the user in a so-called wallet application. This is also the application to interact with other entities, e.g. to sign in for new services, and receive credentials. This application is often implemented on a smartphone, but can reside on other edge devices, such as a desktop computer, too [Le20], [So19]. Wallets can also be located on cloud computing infrastructure as cloud wallets or be provided by third parties as so-called custodial wallets. Then they establish a stable, always available endpoint for other services [Le20], [So18], [Ha19] and might also be used to recover credentials if a wallet on an edge device is no longer available. Finally, hardware wallets (USB sticks or smart cards) and paper wallets (private key and/or seed phrases and/or QR-Codes that are printed out on paper) serve as alternative options to back up and recover private keys [Le20], [So19], [Bl18].

3.2 Associated Potential

As mentioned earlier, the Decentralized approach is seen by many as the future of identity management [Si18],[Ar17]. Decentralization is often used as a "synonym for a better architecture: less monopoly/oligopoly, more control for the end user, more room for the market forces, etc." [Ku19]. However, to critically analyze the real potential it seems advisable to break this argument down.

The most prominently mentioned potential of Decentralized identity management is certainly to give users the ultimate control over their data. Ideally, portability lets users take their data out of the siloes of service providers and dependence on (trusted) third parties as intermediaries for the use of identity data is eliminated. This goes with a high level of privacy, which is particularly emphasized by the proposed solutions and plays a major role in the case for Decentralized identity management [Si18], [Ai18], [Je19], [Wa20], [Le20], [To17a]. The Decentralized, user-centric approach is also seen as a way to reduce the risk associated with large aggregated sets of identity data – both regarding hacks/leaks (e.g. Equifax) as well as misuse/manipulation (e.g. Facebook/Cambridge Analytica) [Go19a], [Va19], [So18]. Moreover, the solutions often integrate cryptographic schemes such as zero-knowledge proofs. Those enable the use of verifiable credentials with selective disclosure so that users can disclose identity data directly to service providers on a need-to-know basis, thus protecting the user's privacy even further [Le20], [So18], [Ab17].

Privacy, however, might not be a sufficient feature for the broad adoption of Decentralized identity management. Therefore, following the user-centric approach further, usability aspects are frequently stressed as well. Several Decentralized or Self-sovereign identity solutions promise to eliminate the username/password problem. They promise to achieve this via single-sign on (SSO) and/or logins via their smartphone wallet as well as biometrics [Ku19], [So18]. As all identity data is managed at the user side, it should be easy for them to keep data updated with all the services that they uses. Moreover, signing up for new services becomes easier if no forms have to be filled out as already existing identity data can be simply shared. On the other hand, this should also be attractive to service providers as it reduces friction from customer onboarding. If verified identity data is easily accessible, this could be used to reduce fraud and fulfil compliance requirements too e.g. from Know Your Customer/Anti-Money Laundering (KYC/AML) regulations. As the identity data could be shared directly from the user with the service provider, the service provider would not be dependent on a third-party identity provider that might profit from this relationship and/or constitute a point of failure [Go19b]. At the same time, businesses would not have to manage the user information themselves. Hence, they could be relieved from the associated costs and risks (e.g. for infrastructure, security) [Le20].

Finally, Decentralized identity management systems might have a potential to provide the ID-infrastructure for currently over one billion people lacking valid identity information that are thus excluded from even basic societal and business services. This can be refugees, stateless persons or people in areas lacking proper infrastructure [Je19], [Wa20]. Several initiatives are promoting digital identities to address this issue, for example the ID2020 Alliance [Di20b] and the World Bank's Identification for Development (ID4D) Initiative [Id20]. A number of proof of concept projects are/have been practically evaluating the use of blockchain based identity management for this use case [Wa20], e.g. the World Food Programme (WFP) in refugee camps and reported promising results [Bu20].

3.3 Approaches to Decentralized identity management

Blockchain-based, Decentralized identity management can be implemented in various ways. Three recently published papers analyze the different approaches, so that we refer to them at this point. Without analyzing actual projects, [Le20] discuss different approaches on a generic level according to the organizational structure (top-down vs. a bottom-up), different models for identifier and credential management, presentation disclosure, general system architecture design and the use of public registries. [Mü18] survey essential components of a Self-sovereign identity, highlighting differences in specifications and in actual projects/designs. In his extensive survey of market offerings for blockchain-based identity management, [Ku19] analyses 43 approaches with different levels of maturity and availability. The three papers show that despite these promises, the technology is still in a quite early stage with a number of questions unanswered. While standards are slowly forming, there is a significant number of competing approaches that are not necessarily interoperable.

4 Critical analysis of centralized identity management

As discussed in the previous section Decentralized identity management has created high expectations. Here we identify a number of critical challenges this approach is facing and that will need to be addressed in the future. An important driving force behind the development of SSIs was to enhance privacy and control for users by taking advantage of a distributed architecture and thus avoiding single points of failure as well as single points of control that exist in the conventional identity schemes based on PKIs and/or large-scale, international, platform based identity providers and brokers. However, privacy is merely one requirement among others and for broad user adoption ease-of-use, cost, reliability, and convenience are important criteria, which cannot be implemented without trade-offs. Even addressing the privacy protection goals by themselves requires trade-offs for example between transparency and unlinkability [Zi19].

During our work over the last two years, we have repeatedly identified the following challenges, without making a claim for completeness:

1. Building solutions while SSI technologies and standards are still under development and evolving rapidly
2. Self-administration of digital identities and private keys for non-technical users
3. Reliable and transparent revocation of SSI based credentials and claims
4. Absence of a natural trust anchor for DLT-based digital identities

4.1 Building solutions while SSI technologies and standards are still under development and evolving rapidly

There is currently a strong desire to demonstrate that SSI technologies are useful and can

live-up to their promise. A high number of demonstrators and prototypes have been presented, but existing solutions are still on a low to medium TRL (technology readiness level) with the highest being around a TRL6 (technology demonstrated in relevant environment) [Ho17].This considers that wallet applications found in App stores are still missing important functions, so that the solutions are not applied in productive environments. Therefore, developers are encouraged to rapidly customize and deploy SSI based solutions using the existing frameworks, such as Hyperledger Indy, Aries and Ursa. However, due to still ongoing rapid developments, the existing releases are not yet very stable and undergo frequent changes. For example, it might be challenging to reliably assess and certify the "level of assurances" (LoAs) of these solutions. While we believe that these issues will be resolved eventually, the development of production level applications is currently risky and could require expensive re-developments as technologies and standards are adjusted.

4.2 Self-administration of digital identities and key management for non-technical users

Self-sovereign management of digital identities implies that users manage their digital identities without the need to rely on third parties. To achieve the highest degree of privacy, users must thus take care of key management entirely by themselves. In this case, also key-recovery becomes the sole responsibility of the user with all associated risks and inconveniences in case of permanent loss. For most users, an appropriate balance between privacy and convenience needs to be achieved and thus third parties will need to get involved in key management and recovery.

For this reason, mechanisms like Decentralized Key Management Systems (DKMS), a global interoperable standard for portable digital wallets, which hold the user's private keys are being developed. DKMS shall enable users to rely on a third-party application to manage their digital wallets, and in particular aid with key recovery.

A completely Self-sovereign approach resembles users keeping their cash (credentials) in a safe at home, while using a third-party digital wallet application is similar to opening a bank account. DKMS then standardizes key recovery procedures (both offline and social) and ensures that users can easily move their accounts to another bank (portability) if they wish to do so.

However, standardization will not be sufficient. As banks underlie regulatory oversight, there will emerge a need for governance bodies that oversee the certification of portable wallet providers to ensure that these adhere to the DKMS standard.

Further, development, maintenance and certification of portable digital wallets will incur costs. Currently, it is unclear if users' willingness to pay will be sufficiently high to cover these costs, or whether new sustainable business models can emerge, that do not attempt to monetize user data.

Finally, advocates of SSI based solutions stress that "portability" is a truly unique concept that does not exist in traditional identity solutions. However, portability could easily be ensured via regulation in all traditional solutions as well. In both approaches, governance bodies are required to ensure adherence to standards and regulation.

4.3 Reliable and transparent revocation of SSI based credentials and claims

Most SSI schemes spend significant effort to achieve "unlinkability" (one of the six privacy protection goals [Ha15]: no one, neither the credential issuer nor verifiers, should be able to monitor credential use by the owner. The revocation of SSI based credentials and claims is thus not trivial since the "phone home" problem must be avoided: a credential verifier should not need to contact the credential issuer ("phone home") to verify that the credential has not been revoked. Mechanisms to circumvent this "phone home" problem have been developed in several SSI schemes [Ve19], [To18] and are currently being implemented.

However, there is another important privacy protection goal that is often in conflict and thus needs to be balanced with unlinkability: transparency. This gives rise to an important, so far unsolved problem: as all SSI schemes focus on unlinkability it has become impossible to monitor and audit credential use – even for the credential owner. This becomes problematic if a wallet is compromised: an intruder can just copy the associated private keys and then use the respective credentials. The credential owner might never become aware of the compromise since the key is not "missing". The complete absence of an audit log and thus of transparency regarding credential use prevents any systematic approach for credential owners to detect improper use by another party.

4.4 Absence of a natural trust anchor for DLT-based digital identities.

An important problem that SSI-based credentials must address is: How can one trust that the credential issuing entity is in fact the entity that it claims to be? If, for example, anyone could issue credentials in the name of "Harvard University" one clearly runs into a trust problem if someone presents a "Harvard University" Self-sovereign degree certificate.

Thus – if certificates should retain their value – SSI must deal with the very same problems that were addressed with centralized PKIs and Decentralized Webs of Trust years ago: to ensure that a public key is really issued by the entity that claims to have issued it. One might argue that one can eventually implement DLT based consensus schemes that implement mechanisms via which a community agrees on what is trustworthy. However, it is unclear if their speed and the associated costs to prevent attempts to introduce bias can compete with the ease at which fake accounts can be created at close to zero cost.

Therefore, most SSI schemes introduce centralized governance layers and trust frameworks with trust anchors and/or trust intermediaries to address this problem. However, those approaches destroy one of the main arguments for SSI, moving from an

open ecosystem to one with a dominant stakeholder (or cartel) acting as gatekeeper. Moreover, the developers (programmers) of the SSI components (crypto libraries, wallets etc.) still possess significant power, which requires users to trust them for being honest and competent (this aspect is mitigated by an open source strategy that is pursued by many solutions). As of the time of this writing, we are not aware of solutions that take a unique advantage of DLT architecture to develop a game changing new answer to this fundamental problem for identity management frameworks.

5 Conclusion

How game-changing will SSI be for digital identity management? SSI does not have an inherent answer to the problem of creating and managing trust anchors. The lack of audit trails for credential use and thus transparency can create severe problems for detecting compromised user accounts even for the legitimate account owners. Finally, efficient and convenient key management requires users to rely (to a varying degree) on cloud service providers. Approaches to build SSI Ecosystems for example according to the REAL framework [Bo19] show that Decentralized ledger technologies just dominate layer one out of four layers: the Self-sovereign aspects get increasingly diluted as the ecosystems are constructed. This is by itself not necessarily a negative outcome, but the question is whether such systems could not been built as well using conventional technologies without a DLT layer.

Apart from architectural/technological issues relating to the functional performance of the technology and at least as important is the question of adoption and economic sustainability of the innovation. So far it has not been demonstrated how the chicken and egg problem of attracting enough service providers/relying parties can be solved. Moreover, sustainable business models for such a Decentralized identity ecosystem that emphasizes privacy and data minimization still seem to be missing.

In addition, the focus on providing privacy in the form of unlinkability might actually not be the most pressing need for users of such systems. According to [Ro14], users do not value unlinkability (in form of privacy preserving credentials) as much as researchers often assume. In fact, the majority of the sample showed less willingness to pay compared to centralized solutions [Ro14].

Great attention should be paid to the new trust frameworks that are suggested. Rather than building completely new frameworks like SOVRIN, that slowly need to attract recognition and could suffer from a lack transparency, more conventional approaches, including the incorporation of Web of Trust technologies, should be considered. An interesting approach has been explored by the EU-funded project LIGHTest: LIGHTest has built a Global Trust Infrastructure based on the DNS system, which not only allows to easily check which public key belongs to which entity, but also to certify this entity according to which "trust scheme" (e.g. eIDAS) [Ro17]. With a non-binding and extremely lightweight integration of LIGHTest with DLT-based identities, an unwanted introduction of a PKI through the

back door can be avoided. The advantage of such approaches is that one can already rely on a trust root that is globally well established.

So, what is the ultimate advantage of DIDs and SSI? Without doubt, SSI brought a lot of new movement into the digital identity sphere. Businesses, governments and supranational bodies are paying attention and share the hope associated with this a novel approach. New possibilities emerge to overcome the challenges that hampered the successful and sustainable development of conventional digital identity ecosystems. This brings entrenched stakeholders with sometimes conflicting interests back together to the table, which could lead to solutions previously impossible. One important aspect that could drive success is that the DLT layer is not controlled by a single entity. This can encourage businesses to take advantage of market opportunities without being afraid to ultimately just support the growth of a platform operator. In this context, it remains to be seen whether sustainable business models for credential issuers, wallet operators, certification, and governance bodies will emerge.

6 References

[Ab17] Abraham, A.: Self-sovereign Identity: Whitepaper about the Concept of Self-sovereign Identity including its Potential. E-Government Innovationszentrum, Graz, 2017.

[Ai18] Forbes, https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/, accessed: 05.02.2020.

[Al15] Github, https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/draft-documents/Decentralized-Public-Key-Infrastructure-CURRENT.md, 2015.

[Al16] GitHub, https://github.com/ChristopherA/Self-sovereign-identity, accessed: 05.02.2020.

[Ar17] Security intelligence, https://securityintelligence.com/reimagining-the-future-of-identity-management-with-blockchain/, accessed: 05.02.2020.

[Bl18] Blockchain Bundesverband, https://bundesblock.de/de/new-position-paper-self-sovereign-identity-defined/, accessed: 11.02.2020.

[Bo19] Medium, https://medium.com/@trbouma/Self-sovereign-identity-making-the-ecosystem-real-v2-536345a10738, accessed: 24.02.2020.

[Br19] GitHub, https://github.com/ethereum/EIPs, accessed: 06.02.2020.

[Bu20] World Food Programme, https://innovation.wfp.org/project/building-blocks, accessed: 13.02.2020.

[Ca05] Microsoft, https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf., 2005.

[De19] W3C, https://www.w3.org/TR/did-core/, accessed: 06.02.2020.

[De20] Identity, https://identity.foundation/, 2020.

[Di20a] MarketsandMarkets, https://www.marketsandmarkets.com/Market-Reports/digital-identity-solutions-market-247527694.html, accessed: 21.02.2020.

[Di20b] ID2020, http://id2020.org/, accessed: 13.02.2020.

[Go19a] Goodell, G.; Aste, T.: A Decentralized Digital Identity Architecture. Frontiers In Blockchain, Volume 2, 2019

[Go19b] Evernym, https://www.evernym.com/blog/5-ways-Decentralized-identity-will-cut-costs-and-grow-revenues/, accessed: 13.02.2020.

[Ha15] Hansen, M.; Jensen, M.; Rost, M.: Protection Goals for Privacy Engineering. In: 2015 IEEE Security and Privacy Workshops, San Jose, CA, p. 159-166, 2015.

[Ha19] GitHub, https://github.com/hyperledger/aries-rfcs, accessed: 11.02.2020.

[Ho17] European Commission, http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2016-2017/annexes/h2020-wp1617-annex-ga_en.pdf., accessed: 13.02.2020.

[Id20] World Bank, https://id4d.worldbank.org/, accessed: 13.02.2020.

[Je19] Accenture-insights, https://www.accenture-insights.nl/en-us/articles/identity-management-on-blockchain, accessed: 05.02.2020.

[Ku15] Kubach, M.; Leitold, H.; Roßnagel, H.; Schunck, C.; Talamo, M.: SSEDIC.2020 on Mobile eID. In: Lecture Notes in Informatics, Open Identity Summit 2015, Berlin, Germany, Bonn: Köllen, p. 29–41, 2015.

[Ku13] Kubach, M.; Rossnagel, H.; Sellung, R: Service providers' requirements for eID solutions: Empirical evidence from the leisure sector, In: Lecture Notes in Informatics, Open Identity Summit, Stuttgart, Germany, Bonn: Köllen, p. 69-81, 2013.

[Ku19] Kuperberg, M.: Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective. IEEE Transactions on Engineering Management, p. 1–20, 2019.

[Le20] Lesavre, L.; Varin, P.; Mell, P.; Davidson, M.; Shook, G.: A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. National Institute of Standards and Technology, 2020.

[Mü18] Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C.: A survey on essential components of a Self-sovereign identity. Comput. Sci. Rev, Volume 30, p. 80–86, 2018.

[Ro14] Roßnagel, H.; Zibuschka, J.; Hinz, O.; Muntermann, J: Users' willingness to pay for web identity management systems, European Journal of Information Systems, Volume 23, p. 36–50, 2014.

[Ro16] Roßnagel, H.; Zibuschka, J.; Hinz, O.; Muntermann, J.: Zahlungsbereitschaft für Föderiertes Identitätsmanagement. In (Hornung, G.; Engemann, C. eds.): Der digitale Bürger und seine Identität, Baden-Baden: Nomos Verlagsgesellschaft, p. 225-245, 2016.

[Ro17] Roßnagel, H.: A Mechanism for Discovery and Verification of Trust Scheme Memberships: The Lightest Reference Architecture. In: Lecture Notes in Informatics,

Open Identity Summit 2017, Karlstadt, Sweden, Bonn: Köllen, p. 81-92, 2017.

[Sh15] Cordis.europa, https://cordis.europa.eu/project/id/318424, accessed: 21.02.2020.

[Si18] Microsoft, https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/Decen tralized-digital-identities-and-blockchain-the-future-as-we-see-it/, accessed: 05.02.2020.

[Si20] SkIDentity, https://www.skidentity.de/, accessed: 21.02.2020.

[So18] Sovrin Foundation, https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf., accessed: 06.02.2020.

[So19] Soltani, R.; Nguyen, T.; An, A.: Practical Key Recovery Model for Self-sovereign Identity Based Digital Wallets. In: 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress, Japan, p. 320–325, 2019.

[Ta15] European Commision, https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu, accessed: 21.02.2020.

[To17a] Sovrin Foundation, https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-sovereign-Identity.pdf., accessed: 11.02.2020.

[To17b] GitHub, https://github.com/ethereum/EIPs/issues/780, accessed: 06.02.2020.

[To18] Tobin, A.: Sovrin: What goes on the Ledger? Sovrin, Evernym, 2018.

[Up20] Microsoft, https://www.microsoft.com/en-us/research/project/u-prove/?from=https%3A %2F%2 Fresearch.microsoft.com%2Fen-us%2Fprojects%2Fu-prove, accessed: 25.03.2020.

[Va19] Van Bokkem, D.; Hageman, R.; Koning, G.; Nguyen, L.; Zarin, N.: Self-sovereign Identity Solutions: The Necessity of Blockchain Technology, Delft, 2019.

[Ve19] W3C, https://www.w3.org/TR/vc-data-model/, accessed: 06.02.2020.

[Wa20] Wang, F.; De Filippi, P.: Self-sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain, Volume 2, p. 1–22, 2020.

[Wh19] McKinsey Global Institute, https://www.mckinsey.com/~/media/McKinsey/Business %20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%2 0key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx, accessed: 21.02.2020.

[Zi12] Zibuschka, J.; Rossnagel, H: Stakeholder Economics of Identity Management Infrastructures for the Web. In: Proc. 17th Nord Work Secure IT, Karlskrona, 2012.

[Zi19] Zibuschka, J.; Kurowski, S.; Roßnagel, H.; Schmuck, C.; Zimmermann, C.: Anonymization Is Dead–Long Live Privacy. In: Lecture Notes in Informatics, Open Identity Summit 2019, Garmisch-Partenkirchen, Germany, Bonn: Köllen, p. 71-82, 2019.

Criteria for trustworthy digital transactions – Blockchain/ DLT between eIDAS, GDPR, Data and Evidence Preservation

Tomasz Kusber[1], Steffen Schwalm[2], Kalinda Shamburger[3] and Ulrike Korte[4]

Abstract: With the help of eIDAS [Re14], legislators have created a resilient framework in EU and EFTA to place trustworthy digital transactions more and more in the centre of business relationships. The regulated use of the trust services (e.g. qualified electronic signature or seal etc.) as well as that of the secure electronic identities provides a solid foundation for the advancement of digitization. The adequate evidence of electronic records as long as they are needed is a critical success-factor for trustworthy digital transactions. The trustworthiness of the transactions must be based on compliance with the basic values of authenticity, integrity, reliability, availability, confidentiality and transferability. After a first hype there are increasingly more considerations also in regulated industries to use DLT for digital processes which have to be accountable. In order to make them evident and to fulfil documentation requirements it is necessary that DLT fulfils the legal framework and prior art based on defined criteria for trustworthy digital transactions. This paper focuses on the challenges and requirements for utilisation of DLT for trustworthy digital processes including long-term preservation.

Keywords: DLT, Blockchain, eIDAS, Trust Service, evidence preservation, trustworthiness

1 Introduction

Since some years, Blockchain and Distributed ledger technology (DLT) generate a real hype in particular with the most famous use case Bitcoin [OE17]. A great potential is seen for the technology e.g. in finance industry, utilities, logistics or public sector. [We17]. Distributed ledger technology (DLT) is basically a peer-to-peer network of nodes sharing decentralized, distributed, digital data. It allows the transfer of data or value from one party to another without having intermediates involved. Each node has a copy of the ledger, to which all network transactions are written and which is only updated throughout all nodes after consensus between the nodes has been reached [IS20b]. Once written to the ledger the transactions are immutable. Any transaction can reliably be tracked on the chain. The well-known Blockchain is a special category of DLT, which organizes data/transactions in blocks that are sequentially linked to each other by incorporating a hash of the previous block [IS20b]. The hash protection also exists in DLT while the transactions are not organized in blocks. DLT does not necessarily require the elimination of an operator/consortium providing the peer-to-peer

[1] Fraunhofer Institute for Open Communication Systems, Kaiserin-Augusta-Allee 31, 10789 Berlin, Germany
[2] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany
[3] msg group, Robert-Bürkle-Str. 1, 85737 Ismaning, Germany
[4] Federal Office for Information Security. Heinemannstr. 11,-13, 53175 Bonn, Germany

network, this depends on the type of DLT. In terms of access and participation DLT can be public, making it possible for anyone to participate, or private, granting access only to specific parties. There is a differentiation regarding permissions as well. DLT that offer full transparency and allow every party to take part in issuance and validation of transactions are called permissionless (unpermissioned). Whereas permissioned platforms do not allow their participants to be freely engaged in the platform, restricting reading access, transaction validation and issuance. Because of that, this later type of DLT is widely used in regulated environments such as aerospace, healthcare, life sciences and pharma, logistics or public sector. Some main platforms are e.g. Hyperledger Fabric and Corda in comparison to the much more famous Ethereum [Fe19], [OE17], [UK16], [Ya18].

2 Fundamental requirements on trustworthy digital transactions

2.1 Trustworthiness of digital transactions and records

Trustworthiness of digital transactions and records means that the process and the records are really what they seem to be and that this is provable by independent 3rd parties. Trustworthy digital transactions ensure the unique and lossless evidence of authenticity, integrity, reliability of the electronic records which are created, received, stored and managed during the life-cycle of transaction against independent 3rd parties as long as they are needed. This means typically until the end of the defined retention periods based on and compliant to existing laws (between 2 & 110 years or permanent). Some main pre-condition are their availability as well as the protection of the confidentiality of records worthy of protection. The records contain content, metadata and transaction (process) data. The basic preconditions for this is the transferability [UN17] of the records. The evidence will be proven based on the records themselves so the named requirements and in consequence the evidence value of a record are significant properties of the electronic record itself ([WE18], [KHS14], [Ro07]). The utilization of cryptographic measures, e.g. qualified e-signatures, seals and time stamps acc. to eIDAS [Re14], enables users to preserve the evidence of their electronic records without losing the transferability of the records. The evidence value of a qualified electronic signature (e-signature) is the same as a handwritten signature, the seal makes the authenticity and integrity of the sealed record evident. These cryptographic measures are inherent and significant properties of the records. They require measures concerning long-term preservation focusing on the record itself not the storage, the software environment etc. to keep the trustworthiness of the records in the sense of preservation of the information of the data record and its evidence ([Sc17] [Fi06] [KHS14], [ET19b], [ET20]). Main precondition is the establishment of a valid records management according to [IS16]. This includes established policies, roles & responsibilities, processes as well as appropriate functionalities in business-IT to managing records properly during their whole life-cycle from the creation or receiving over utilisation and storage until archiving and disposition ([We18], [IS16]).
These basic burdens of proofs and requirements on trustworthy digital records and transactions are independent from used IT-system, organization or process. Currently there is no regulation defining technology or institution as trustworthy by themselves.

Trustworthiness always requires the evidence of the significant properties based on the records themselves as long as they are needed and without any losses. This requires especially the transferability of the records and so the utilisation of (qualified) electronic signatures, seals and timestamp acc. to eIDAS [Re14], [KHS14]. An evidence value of a record is an inherent property of the record itself. That is why records should only be archived in self-contained AIP which contain any necessary information (metadata, content, evidence relevant and technical evidence data) in a standardized container acc. to [IS12a]. The proof is typically done by trustworthy 3rd parties such as courts, regulative authorities, auditors etc. depending on the legal requirements [We18]. This means trustworthiness can be achieved only by proof not by self-declaration. Essentially it is necessary to make compliance to legal requirements and prior art – so technical standards given and audited by trustworthy 3rd parties – evident [KKS18], [We18], [He18].

2.2 Legal and organizational requirements

Since September 2014, the eIDAS regulation was defined, which came fully into force in July 2016 as a European wide mandatory legal framework for trustworthy digital transactions between citizens, business and government. The eIDAS-regulation contains two parts which both affect trustworthy digital transactions in any business IT-systems: secure digital identities (identification systems) and trust services, in the context of this paper especially, of creation and validation of (qualified) electronic signatures, seals and timestamps as well as preservation services. Any notified electronic identification scheme has to be recognized and accepted by any public administration. Any minimum advanced electronic signature, seal or timestamp from any qualified trust service provider has to be accepted and validated by any public administration. Regarding retention periods between 2 and 110 years or more the long-term preservation of electronic signatures, seals, timestamps and the corresponding data is a mandatory need to ensure the traceability of digital transactions by their records as long as they are needed ([Sc15], [We18]). This was recognized by legislators, e.g. in Europe by the Articles 34 and 40 in eIDAS [Re14] and in Germany with the obligation for long-term evidence preservation (§ 15 VDG [Ve17]). In combination of secure digital identification and trust services the eIDAS [Re14] enables public administration and private companies to establish trustworthy digital transactions and to make them evident against regulative authorities, auditors, courts etc. as well as to preserve the evidence value as long as necessary. eIDAS [Re14] is technically underpinned by corresponding European Standards of ETSI and CEN with Mandate 460. The standards are tied to special state-of-the-art-technologies, which achieve the technical and security requirements.

Furthermore the General Data Protection Regulation GDPR [Re16] has to be recognized to ensure the confidentiality of personal data in digital transactions. The technical and organizational measures to ensure confidentiality of personal data acc. to GDPR [Re16] can also be used to keep trade and business secrets to achieve a holistic management of protective records. In Art. 6 GDPR [Re16]), the obligation for information (Art. 13+14 GDPR [Re16]) as well as the rights of the affected person are in focus so right of access, right of rectification, right to erasure and right of data portability. These obligations and

rights require not only organizational and technical measures included in a well-defined data protection management system but also the technical ability of the applied IT-system to change, export or delete personal data as well as a defined access management or functionalities to decrease amount of the processing of personal data. Taking into account retention periods for decades as well as existing documentation obligations and burden of proof the GDPR [Re16] reflects the ensuring, preservation and evidence of the significant properties of electronic records: authenticity, integrity and reliability (e.g. evidence for consent, obligation of information, access, data portability), availability (e.g. rectification, erasure, portability). This means if DLT is used in processes where personal data are collected, managed and stored, the requirements of GDPR [Re16] have to be fulfilled [We18].

The eIDAS [Re14] and the GDPR [Re16] are underpinned by sector specific regulations concerning the documentation and traceability of digital transactions and records e.g. EASA [EA20], FDA [CF19], EGovG [EG13].

2.3 Relevant Standards

The picture below shows the main organizational and technical standards for the traceability and long-term preservation of digital transactions as preservation objects or preservation object containers based on [IS16] and [Fe18]. One main basis is a valid records management according to [IS16]. The preservation of information requires a trustworthy digital archive compliant to [IS12a], [IS12b] with well-defined processes and information packages to achieve independence from a special soft- or hardware environment. Measures and protocols concerning long-term data preservation are specified in [Fe18] and [ET20], especially on basis of the preservation evidence formats Evidence Records according to RFC4998 [GBP07], RFC 6382 [JSG11] and {C/X/P}AdES Archive Timestamps.

3 DLT in trustworthy digital transactions

3.1 Assessment of DLT against requirements on trustworthy digital transactions

If DLT should be used for trustworthy digital transactions, it is mandatory to long-term preserve their data and evidences, also against 3rd parties, until the end of the retention periods in force and to keep them provable – as it is required for any business IT-system. This means a valid records management incl. evidence preservation is mandatory. The table below shows an overview how DLT achieves or does not achieve the named requirements currently without additional measures [FE19], [KKS18], [Ko18], [Ko19], [DI20A], [Le16], [We18].

Property	Degree of fulfilment	Justification
Authenticity	Very Limited	Commonly, there are no standardized measures for unique linking of transactions or records on DLT to

Property	Degree of fulfilment	Justification
		corresponding legal or natural entities (persons). Further investigation of currently existing mechanisms, e.g. e-signature or -seals acc. to eIDAS [Re14] in order to be used in pair with DLT is necessary. Standardization of such approaches should be aimed for in parallel. At the present, only private, permissioned DLT instances could fulfil this requirement, especially while implementing a proprietary solution.
Integrity	Limited	Immutability is built on the hash protection of blocks/transactions but no resilient[5] Proof of Existence (PoE)[6]. Furthermore, no rehashing & resigning measures acc. to prior art exist. Especially the use of hash algorithms, which became weak, leads to loss of the integrity (c.f. Fig. 1).
Confidentiality	Limited	Only private, permissioned DLT seems to fulfil this requirement. Fulfilment of GDPR [Re16] is only possible with off-chain storage of affected data. (Keeping crucial data on-chain prevents the fulfilment of deletion of those data without having the chain integrity unaffected. Anonymization and pseudonymization can become critical concerning transparency of transactions also in private, permissioned DLT.
Transferability	Very Limited	No standardized migration or ex-/import measures exist. At this stage, there is no common standard or mechanism, which could be used in order to retrieve the data (transaction or a set of them) from one DLT-based application and put it on the other one. This includes also the use case of providing the evidence data based on DLT to the authorities (e.g. to fulfil legal requirements).

Tab. 1: Assessment of DLT against core requirements of records management

In the conclusion of the DLT assessment against significant requirements on records management to achieve trustworthiness it can be ascertained that DLT needs further, additional measures to be enabled for the execution of trustworthy digital transactions. Furthermore it can be determined that only permissioned DLT with limited reading and writing rights for the participants (e.g. consortium or private DLT) and an off-chain storage of the records are currently recommended. Only data about the transaction, not the content itself should be stored on-chain [Ko18], [DI20a], [Le16], [Fe19]. This need is recognized by national and international standardization to define a valid

[5] There used to be applied a system time stamp, but not a trustworthy timestamp issued by corresponding authority, e.g. a qualified trust service provider for qualified time stamp acc. to [eIDAS].
[6] Evidence that proves that an object existed at a specific date/time (c.f. [ETSI119102-1])

organizational and technical framework for trustworthy utilization of DLT.

3.2 Relevant Standardization of DLT and interim conclusion

Currently the standardization in subject of this paper focuses on complementing DLT with the needed tools for long-term traceability and preservation of its transactions and their records, e.g. using secure digital identities and trust services regarding eIDAS [Re14]. So especially the [DI20a] defines determined and provable criteria to use DLT for trustworthy digital transactions by fulfilling records management and long-term data preservation with focus on eIDAS [Re14] and GDPR [Re16].The DIN-specification normatively references corresponding national and international standards regarding DLT e.g. [DI20b] concerning privacy or [W320] for self-sovereign-identity as well as [IS16] regarding records and [ET19b], [ET20], [Fe18] reg. long-term data and evidence preservation. [DI20a] is a main input for [IS20a] which will act as the worldwide pendant.

4 Criteria for trustworthy digital transactions with DLT

The criteria in [DI20a] for trustworthy digital transactions with DLT are discussed under two headings – functional and technical criteria. While the functional criteria describe mainly measures especially regarding general issues, governance, privacy or digital identities that shall be considered, the technical criteria describe in detail, how DLT needs to be set up in order to be used for trustworthy digital transactions.

4.1 Functional criteria

First of all it is necessary to meet requirements described in chap. 3.1 and 3.2 by integrating DLT in a valid records management. This requires the compliance with regulatory requirements is achieved as well as the definition and implementation of well-described roles, responsibilities and policies for records management integrating DLT with the corresponding business-IT. It also requires the records themselves to be stored off-chain for the whole life-cycle of records and their transaction/process information on-chain.

Secure digital Identities & Trust Services

In order to utilize DLT for records management and trustworthy digital transactions, the identities of the participants have to be known unambiguously. This is necessary to make transactions and their records evident against 3rd parties, to fulfil burden of proof and documentation needs compliant to prior art for records management and trustworthy digital transactions [We18], [BB15]. To attain this, DLT inherent functions have to be enhanced with addition of eIDAS [Re14] compliant identification in appropriate level of assurance. This can be achieved with self-sovereign-identity acc. to [W320]. In this case only the anonymized or pseudonymized data are stored on-chain. The identity data itself is stored off-chain in order to ensure compliance to GDPR [Re16]. Decentralized identifiers (DIDs based on W3C standard [W320]) are suitable to be integrated for this

purpose and maintain compliance to privacy regulations as no identifying data is stored on chain. In fact the holder of the DID has complete control over the DID and there is no central authority needed to implement it. The inclusion of identities provides the basis for assignment of permissions to these identities further improving security of the system. It should be carefully considered which participant should be allowed to execute what type of actions within the system. A trusted authority in role of gatekeeper assigns permissions to nodes operated by trusted identities thus defining the actions these are allowed to execute. This approach is currently executed e.g. by ESSIF [ES20] and EBSI [EB20] in EU but also several other initiatives around Europe.

Furthermore DLT inherent functions have to be enhanced with addition of eIDAS [Re14] compliant identification in appropriate level of assurance and by trust services. Especially the trust services for creation of qualified electronic signatures, seals (X.509 based or token based using content of X.509 envelope) and timestamps are needed to provide genuine verifiability of digital processes using DLT authenticity, reliability and integrity of transactional data by keeping provability by independent 3rd parties. This means in fact that a trusted "gatekeeper" could enable the DLT with secure digital identities and trust services acc. to eIDAS [Re14] to be used for trustworthy digital transactions.

Privacy

Setting up and running a system for records management and preservation of evidences should always be done with consideration of data protection regulations. If personal data is involved the system needs to be GDPR [Re16] compliant. This requires that affected data are strictly stored off-chain and can be deleted on demand. There are some solutions in the field of applied research for GDPR [Re16] compliance of DLT, e.g. [Bu18], but currently neither standardized nor matured. Any access to data on-chain needs valid access rights management. DLT have to be integrated in data protection management including appropriate technical and organizational measures [Ko18], [Zi17], [Fe19].

4.2 Technical criteria

One main challenge concerning the long-term stability of DLT is the possibility to migrate data stored on-chain. Currently only migration between different DLT-platforms is possible via a bridge but standardized migration from DLT to another business – necessary e.g. to fulfil the right of data portability GDPR [Re16] – is still in research stage. That is why personal data should be stored off-chain only.

Information Security

Although DLT contains properties to ensure integrity of the transactions there are also different security vulnerabilities against possible attacks. Before DLT is used, a security concept is necessary which covers a well-grounded risk management and detailed security measures including further information concerning consensus mechanism and its fault tolerance [Fe19]. The cryptographic mechanisms shall be based on state-of-the-art algorithms as recommended e.g. in [SO16] or [ET19a].

Long-Term Preservation and Proof of Existence

A main vulnerability concerning long-term burden of proof of digital transactions in DLT is the lack of standardized rehashing and resigning measures as well as Proof of Existence. In DLT the blocks or ledger are hashed in the father-son-principle but without a standardized procedure for the rehashing of the whole chain in case that the cryptographic algorithms or their parameters lose their suitability as security measures over the course of time. This lack can lead to recalculation of old hash algorithms and manipulation of the chain by an attacker without notice

The reason for this is that with obsolete hash-algorithms the secured data can be changed by recalculation and afterwards replacement of the hash protection**,** which still seem to protect the original data but were manipulated.[FE19] [SM17] [DI20a]. This vulnerability is well-known since hash and also signature integrity protection is used and not exclusive to DLT. Furthermore, there is also no Proof of Existence acc. [ET18] and [ET19b] with a trustworthy time for transactions in DLT. Existing time-stamps in DLT only make evident a period of time, but not a point of time where a transaction was executed or transaction/data were still unaltered from a trustworthy source e.g. (qualified) trust service provider acc. to Art. 41 eIDAS [Re14].

The hash-based integrity protection in DLT uses Merkle-Trees [Me80]. This makes it possible to use well-established measures e.g. acc. to TR-03125 [Fe18] and RFC4998 [GBP07], also included in the standards for (qualified) preservation services eIDAS [Re14] and [ET19b], [ET20] to solve the rehashing and Proof of Existence challenge in DLT. In this case the system for long-term preservation regarding the [Fe18] in connection with a (qualified) preservation service on basis of [ET19b], [ET20] is connected and complements it with the missing functionalities. The picture below illustrates a possible solution [Ko18], [SM17].

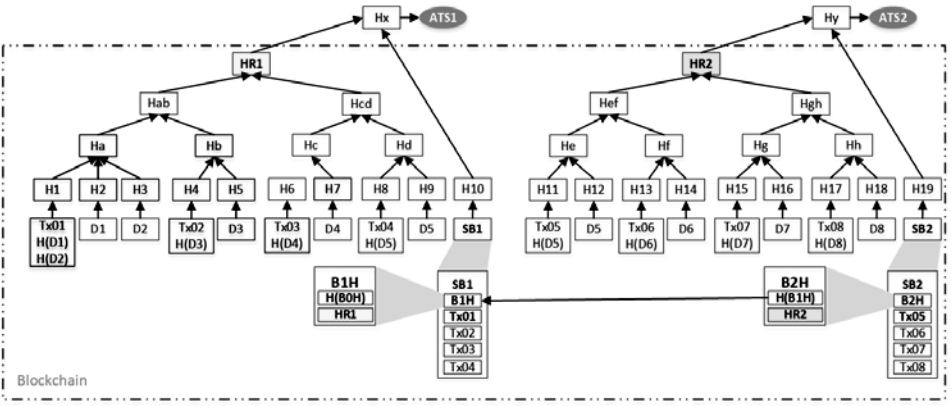


Fig. 1: Evidence Preservation in DLT

The transactions form a data object group acc. to [GBP07] together with the referenced records (content) e.g. Tx01 with D1 and D2 or Tx04 with D5. A Merkle- Hashtree [Me80] is created over all transactions and the referenced records which will be closed with the root-hash-value e.g. HR1. The calculated root-hash-value will be stored in the belonging blockheader e.g. B1H inside the block-description, e.g. SB1, and protected with the same hash-tree. As a result the hash-tree of the block gets a new root-element,

e.g. Hx, which will input for hash-tree acc. [GBP07] e.g. in a [Fe18] compliant system for evidence preservation or preservation service acc. to eIDAS [Re14] and [ET20] and closed by a qualified archive timestamp [Ad01] e.g. ATS1. Some procedure can be done with the next block (B2) so that the needed concatenation of the blocks will be achieved. The same system or preservation service can be used for the off-chain stored records too. In the result the evidence preservation as well as rehashing and Proof of Existence of on-chain transaction information and the referenced records can be done in this way.

5 Perspective and Need for further Standardization

In summary it can be determined that a valid records management together with appropriate security measures, evidence preservation as well as the identification systems and trust services acc. to eIDAS [Re14] enable DLT to be used for trustworthy digital transactions. Secure digital identities and trust services can be easily added to DLT networks to achieve non-repudiation and thus long-term preservation of evidences on authenticity and integrity of on-chain stored transaction data. Although further standardization is ongoing in CEN concerning interoperability of digital identities, especially self-sovereign-identity in DLT according to ESSIF-initiative as well as to identify and realize further development of eIDAS [Re14] and corresponding European standards for user-friendly and compliant utilisation of digital identities in DLT.

The well-described connection between DLT and corresponding business-IT, where the records and especially personal data are stored off-chain, achieves compliance to GDPR [Re16]. The combination makes it possible to use the advantages of both worlds DLT and eIDAS [Re14], GDPR [Re16] and establishes the basis for innovative network based business models G2B2C in trustworthy digital ecosystem. In order to make the business models easier as well as to ensure long-term stability, further standardization concerning GDPR [Re16] but also migration facilities of DLT is recommended. Another subject for further standardization is appropriate security measures, especially the long-term stability of hash algorithms and Proof of Existence in DLT as well as their preservation of evidence to fulfil legally binding burden of proof or documentation needs.

Bibliography

[Ad01] Adams, C. et al.: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). IETF RFC 3161. 2001.

[BB15] Buchmann, N.; Baier, H.: Elektronische Identifizierung und vertrauenswürdige Dienste. In D-A-CH Security 2015. Bestandsaufnahme - Konzepte - Anwendungen - Perspektiven. 08. - 09. September 2015, St. Augustin, 2015.

[Bu18] Bundesdruckerei GmbH: From the Almighty Administrator to the Self-determined User. An Innovative Approach from Bundesdruckerei's Research Lab: Identity and Rights Management with FIDES, 2018.

[CF19] CFR: Title 21 - Part 11 Electronic Records; Electronic Signatures. 21CFR11. 2019

[DI20a] DIN SPEC 31648: Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/Blockchain. 2020.

[DI20b] DIN SPEC 4997: Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology. 2020.

[EA20] EASA: Part 21 - Airworthiness and Environmental Certification. https://www.easa.europa.eu/acceptable-means-compliance-and-guidance-material-group/part-21-airworthiness-and-environmental, accessed: 30/03/2020.

[EB20] EBSI, European Blockchain Services Infrastructure, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI, accessed: 30/03/2020.

[EG13] E-Government Act. EgovG. 2013.

[ES20] ESSIF, European Self-Sovereign Identity Framework, https://www.eesc.europa.eu/en/news-media/presentations/european-self-sovereign-identity-framework, accessed: 30/03/2020.

[ET18] ETSI: TS 119102-1 – V1.2.1 - Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, 2018.

[ET19a] ETSI: TS 119 312 - V1.3.1 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. 2019.

[ET19b] ETSI: TS 119 511 - V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques. 2019.

[ET20] ETSI: TS 119 512 - V1.1.1 - Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services. 2020.

[Fe18] Federal Office for Information Security (BSI): BSI Technical Guideline 03125, TR-ESOR – Preservation of Evidence of Cryptographically Signed Documents.v.1.2.2, https://www.bsi.bund.de/EN/tr-esor, 2018

[Fe19] Federal Office for Information Security (BSI): Towards Secure Blockchains. Concepts, Requirements, Assessments. 2019.

[Fi06] Fischer-Dieskau, S.: Das elektronisch signierte Dokument als Mittel zur

Beweissicherung. Anforderungen an seine langfristige Aufbewahrung. Kassel, 2006.

[GBP07] Gondrom, T.; Brandner, R.; Pordesch, U.: Evidence Record Syntax (ERS), IETF RFC 4998. 2007

[He18] Henne, T.: Juristische Anforderungen an die Beweiswerterhaltung bei digitaler Archivierung. Marburg, 2018.

[IE17] IEEE: ICCCN 2017. 26th International Conference on Computer Communications and Networks (ICCCN) July 31-August 3, 2017, Vancouver, Canada. IEEE, Piscataway, NJ, 2017.

[IS12a] ISO 14721:2012 Space data and information transfer systems - Open archival information system (OAIS) - Reference model, 2012.

[IS12b] ISO 16363:2012 Space data and information transfer systems - Audit and certification of trustworthy digital repositories, 2012.

[IS16] ISO 15489-1:2016 Information and documentation - Records management - Part 1: Concepts and principles, 2016.

[IS20a] ISO/AWI TR 24332 Information and documentation - Blockchain and DLT and records management: Issues and considerations, 2020.

[IS20b] ISO/DIS 22739: Blockchain and distributed ledger technologies - Terminology, 2020.

[JSG11] Jerman, A.; Saljic, S.; Gondrom, T.: Extensible Markup Language Evidence Record Syntax (XMLERS). IETF RFC 6283. 2011.

[KHS14] Korte, U.; Hühnlein, D.; Schwalm, S.: Standards for the preservation of evidence and trust. Proceedings Archiving 2014, Springfield 2014, S. 9-14.

[KKS18] Korte, U.; Kusber, T.; Schwalm, S.: Vertrauenswürdiges E-Government - Anforderungen und Lösungen zur beweiswerterhaltenden Langzeitspeicherung, 2018.

[Ko18] Korte, U. et al.: Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain, DACH-Security 2018. S. 177-191 Frechen 2018.

[Ko19] Korte, U. et al.: Vertrauenswürdige digitale Transaktionen - Records Management und Beweiswerterhaltung mit Blockchain, 2019.

[Le16] Lemieux, V. L.: Trusting records: is Blockchain technology the answer? In Records Management Journal, 2016, 26; S. 110–139.

[Me80] Merkle, R. C.: Protocols for Public Key Cryptosystems. In: 1980 IEEE Symposium on Security and Privacy. IEEE, Oakland, CA, 1980. S. 122-134.

[OE17] OECD: OECD Digital Economy Outlook 2017. Organisation for Economic Co-operation and Development OECD, Paris, 2017.

[Re14] Regulation (EU) No 910/2014 of the European Parliament and of the Council - of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. eIDAS, 2014.

[Re16] Regulation (EU) 2016/ 679 of the European Parliament and of the Council - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation). GDPR, 2016.

[Ro07] Roßnagel, A. et al.: Langfristige Aufbewahrung elektronischer Dokumente. Anforderungen und Trends. Baden-Baden, 2007.

[Sc15] Schwalm, S. et al.: Die Bedeutung der eIDAS-Verordnung für Unternehmen und Behörden - Neue Chancen und Herausforderungen für vertrauenswürdige elektronische Geschäftsprozesse in Europa. Berlin, 2015.

[Sc17] Schwalm, S.: A service for the preservation of evidence and data – a key for a trustworthy & sustainable electronic business. Open Identity Summit 2017. Lecture Notes in Informatics (LNI). Proceedings. Bonn 2017 S. 131-144

[Sc18] Schwalm, S. et al.: Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain, 2018.

[SM17] Sato, M.; Matsuo, S.'i.: Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography. In ICCCN: 26th International Conference on Computer Communications and Networks (ICCCN) July 31-August 3, 2017, Vancouver, Canada. IEEE, Piscataway, NJ; 2017, S. 1–8.

[SO16] SOG-IS Crypto-Evaluation Scheme - Agreed Cryptographic Mechanisms-1.0. 2016.

[UK16] UK Government Chief Scientific Adviser: Distributed Ledger Technology: beyond block chain, 2016.

[UN17] UN United Nations Commission on International Trade: UNCITRAL model law on electronic transferable records. United Nations, New York, 2017.

[Ve17] Vertrauensdienstegesetz. VDG, 2017.

[W320] W3C: Decentralized Identifiers (DIDs) v1.0. 2020.

[We17] Welzel, C. et al.: Mythos Blockchain: Herausforderung für den öffentlichen Sektor. Kompetenzzentrum Öffentliche IT, Berlin, 2017.

[We18] Weber, M. et al.: Records Management nach ISO 15489. Einführung und Anleitung. Beuth Verlag, Berlin, 2018.

[Ya18] Yaga, D. et al.: Blockchain technology overview. National Institute of Standards and Technology, Gaithersburg, MD, 2018.

[Zi17] Zimprich, S.: Blockchain. Der Hype und das Recht, Hamburg, 2017.

H. Rossnagel, C.H. Schunk, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 61

Identity Management as a target in cyberwar

Lothar Fritsch[1]

Abstract: This article will discuss Identity Management (IdM) and digital identities in the context of cyberwar. Cyberattacks that target or exploit digital identities in this context gain leverage through the central position of IdM digital infrastructures. Such attacks will compromize service operations, reduce the security of citizens and will expose personal data - those of military personell included. The article defines the issue, summarizes its background and then discusses the implications of cyberwar for vendors and applicants digital identity management infrastructures where IdM is positioned as a critical infrastructure in society.

Keywords: Identity management; Cyberwar; Cyber conflict; Digital identities; Information Privacy; Critical Infrastructure Protection; Security; Cyberconflict; Cybersecurity

```
"The events which can not be prevented, must be directed."
- Klemens von Metternich
```

1 Introduction

Identity management is a technological platform that enables the identification and verification of persons or computers as well as the processing of persons, of ownership over physical or virtual objects and over all other imaginable resources. Mobile phone subscriptions and bank accounts as well as payment systems are well-known domains where IdM plays a critical role. Less visible domains are public utilities, government administration or health services, where in progressing digitization of services IdM is introduced to both control access and roles of employees as well as to identify persons who are being administered, billed or privileged through IdM.

IdM is therefore a critical infrastructure that underlies many other of society's critical infrastructures and functions, while making citizens involuntarily accessible to external actors [HG08]. This article will discuss Identity Management as a critical asset in the context of cyberwar. It will discuss the relevance in face of power and military action, then illustrate the issue with examples. Digital identity will be positioned as an attack vector for

[1] Karlstad University, Dept. of Mathematics and Computer Science, Universitetsgatan 2, Karlstad, Sweden lothar.fritsch@kau.se emailaddress@author2

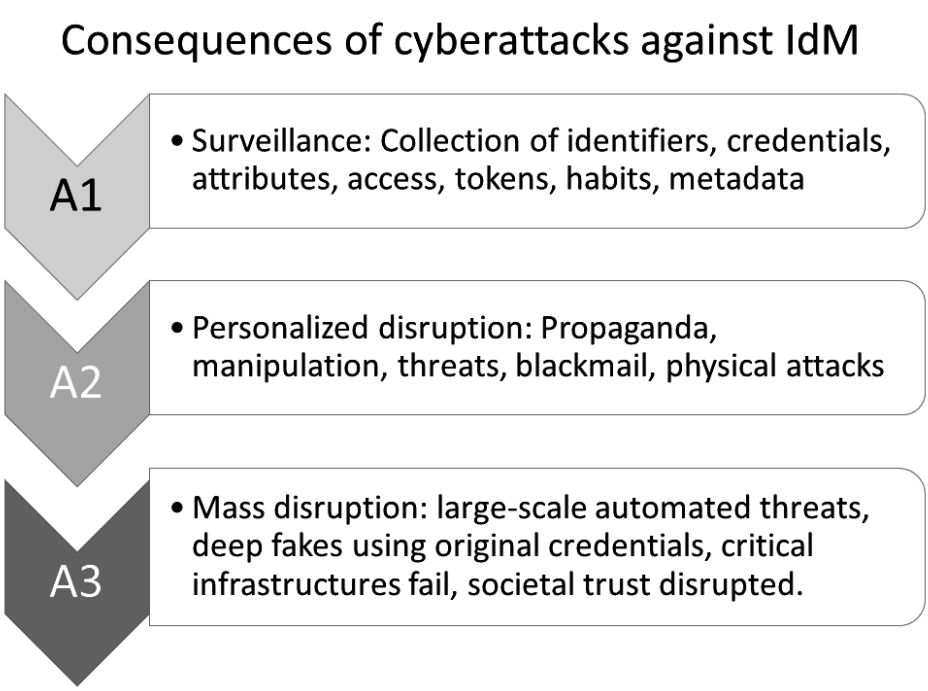


Fig. 1: Consequences of three escalating categories A1,A2 and A3 of cyberattacks on identity management.

cyberattacks. Next, possible regulatory restrictions will be introduced, before I conclude and summarize.

The main argument of this article is:
IdM ist the key to most digital environments, the key to all citizens (military and civil), and has therefore major relevance in national security and sovereignty in the context of cyberwar.

2 Background

IdM is of major relevance in the national security context. First, it enables the governance of digital services of all kinds, and is therefore a part of most digital civil, administrative and critical infrastructures, including communications. Next, digital identities are directly associated with individuals, which turns them into tools to track, profile, find and access those people. Third, digital identities are used directly in military contexts where they are the key to personnel, equipment or actions. The role of RFID auto-identification of goods and products in industrial espionage and sabotage has been illustrated by Fritsch in

[Fr09]. The remainder of this section will discuss examples of how IdM is closely related to cybersecurity, and how compromize of digital identities endangers societal security and sovereignty.

Digital identities can get exploited for various adverse actions in escalating levels of impact on societal security (labeled as categories A1-A3 below):

A1: Surveillance and intelligence gathering: Key persons or large segments of populations can be targeted through digital identities for observation.

A2: Personalized manipulation and disruption: Through individual digital identities, people can be targeted for influence campaigns or can become the individual target of adverse action.

A3: Mass exploitation or disruption of services: Compromize of IdM at a large scale will enable the disruption of critical societal functions, either through their simple destruction that will render identification as well as archives useless, or through targeted exploitation of stolen identities for disruptive actions that target society's critical processes and services.

The consequences of these actions are llustrated in Fig. 1. It is noteworthy that digital identities bridge from the digital into the physical domain. Cyberattacks may combine into cyberphysical attacks where digital surveillance from A1 may lead to physical action against persons in A2 and A3. Fig. 2 illustrates how digital identifiers connect digital and physical spaces in ways that are exploitable by attackers even in the physical domain.

Simple observation of digital identities can leak critical secrets. In 2018, a fitness app for self-metering of jogging performance published trail maps of joggers that were found to reveal secret military facilities used by U.S. troops [2].Such data extraction relates to category A1. Further investigation of fitness apps' data extraction confirmed how unverified apps can easily access critical identities and personal data [MHF19].

Kallberg [Ka16] discusses pillars of societal stability that will be at risk through cyber attacks (pp. 121). Cyberwar strategy aims at the destabilization of the target contry's functioning institutional arrangements. He explicitly discusses governmental registers and archives with institutional knowledge such as property registers as potential targets. The pivotal role of IdM in governance puts IdM in the core of such attack strategies. Such actions fall into category A3.

Dunlap [Du14] discusses the consequences of a future hyperpersonalization of war through digital identities. Dunlap reasons about digital technologies as enablers of acts of war that target specific individuals. He describes two relevant cases which are in category A2:

[2] The Guardian: Fitness tracking app Strava gives away location of secret US army bases, 2018-01-28, https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases , accessed 2020-02-21

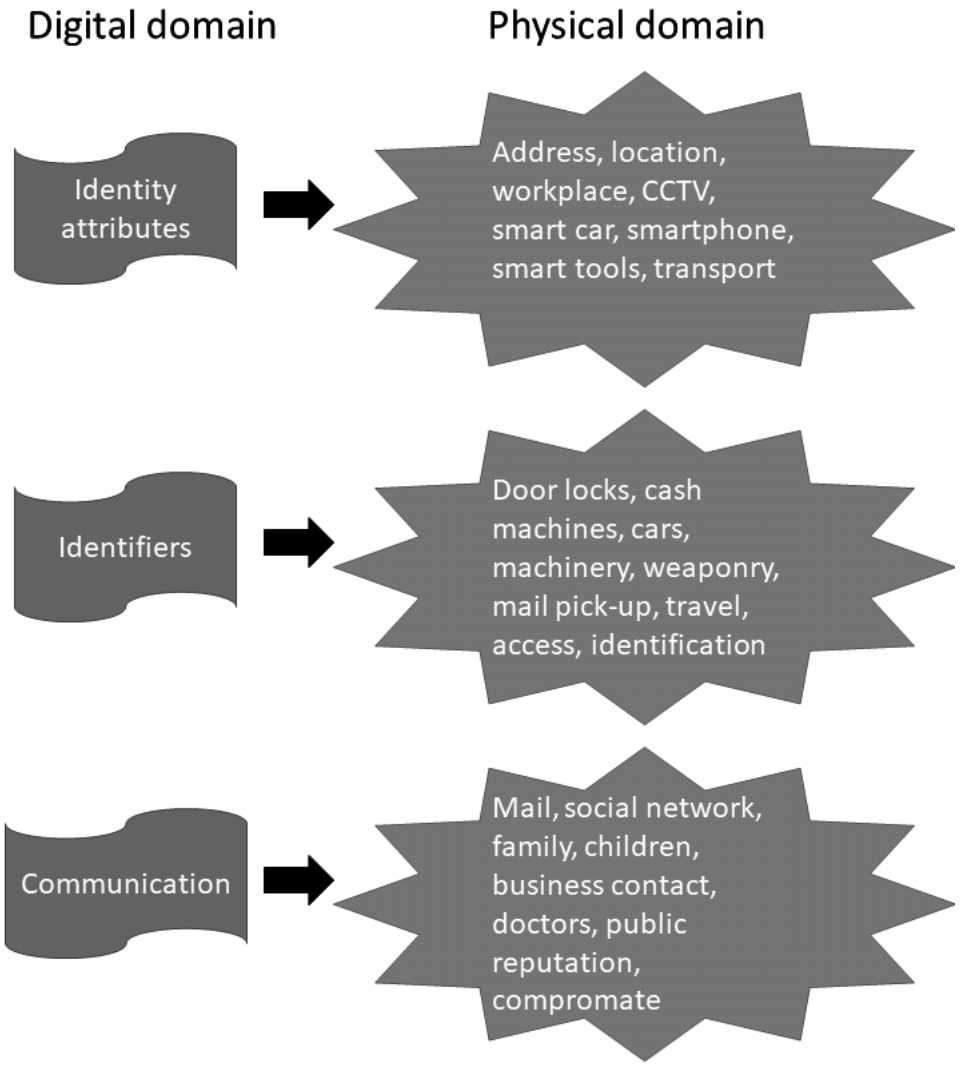


Fig. 2: Identity management causes cyberphysical security and privacy problems when exploited in cyberwar.

1. The targeting of individual soldiers with biometrics-enabled or otherwise personalized weapons.This vision is illustrated by the short film *Slaughterbots* [3]. Similar tactics have already historically been observed being used against U.S. soldiers in the Pacific who found their private browser history published on the Internet [4]. Similar threats have been addressed to U.S. soldier's smart phones in 2019 [5]. Worries about digital targeting have been voiced by Swedish defense researchers Sigholm and Andersson [SA11] who reason about future battlefield technology's exposing of soldier's personal data. Case examples from the Iraq war have been collected by Conti et al. [Co10] who documented the naive use of identifiers in battlefield. Personal data gets weaponized in conflicts. This problem has been noticed by privacy technology researchers at Karlstad University who suggest the use of privacy enhancing technology (PET) in battle contexts [FFH18].
2. The targeting of civillians with misinformation for the purpose of destabilization (A2). The impact of such tactics when applied against massses (A3) has been seen in the manipulation election services deployed by Cambridge Analytica in 2016 [Be18]. Military personnel and their families recently have been exposed to such tactics, for example during NATO exercises in the Baltics where wifes of Dutch military pilots reveived threatening phone calls [6].

Individuals may come under surveillance and may suffer from intelligence actions that steal their identities. Eakin [Ea17] describes in his essay 'The Swedish Kings of Cyberwar' a joint intelligence effort called WINTERLIGHT where intelligence targeted the whole spectrum of identities from access control credentials up to fabrication of 'real' LinkedIn pages in the name of targets. The aforemention propaganda against soldiers' families are part of these tactics. A. Pfitzmann warned against naive application of RFID identification of humans in 2007 through the example of person-specific bombs that explode when certain person's RFID passport walks by [7] (category A2).

A suspected intelligence cyberattack agaainst a Dutch issuer of commercial web certificates, *DigiNotar*, The provider was hacked and then used to issue large numbers of fake domain certificates [vdM13, WB18]. The issued certificates were found to be used by intelligence services to intercept SSL-encrypted web traffic. Only after several months this was discovered, and business terminated by the Dutch government[8]. Meulen [vdM13] concludes:

[3] See video 'Slaughterbots' at https://autonomousweapons.org/slaughterbots/ , accessed 2020-02-21

[4] Bruce Schneier about Future Cyberwar, https://www.schneier.com/blog/archives/2018/08/future_cyberwar.html, accessed 2020-02-21

[5] Interview with Keir Giles on Military,com, https://www.military.com/daily-news/2019/09/03/russian-harassment-nato-personnel-families-next-chapter-information-warfare.html , accessed 2020-02-21.

[6] De Telegraf, Telefoonterreur treft thuisfront: 'Russen' intimideren vrouwen Nederlandse F-16-vliegers, 2019-09-19, https://www.telegraaf.nl/nieuws/838014510/russen-intimideren-vrouwen-nederlandse-f-16-vliegers ,accessed 2020-02-21

[7] Neues Deutschland: Personspezifische Bomben mit RFID-Pass, 25.04.2007, https://www.neues-deutschland.de/artikel/108709.regierung-baut-personenspezifische-bomben.html , accessed 2020-02-21

[8] See full description: https://www.enisa.europa.eu/media/news-items/operation-black-tulip, accessed 03-Apr-2020

The DigiNotar disaster was a painful wake-up call for the world, not just for the Dutch government. They provided the stage on which this disaster could unfold. The breach maintained considerable repercussions for various parties around the globe, especially the affected Gmail users in Iran. (...)it is clear DigiNotar is unfortunately not an isolated incident. In the same year, the media also reported on other attacks against RSA and an affiliate of Comodo, another CA. (...) Other examples include multiple breaches against Verisign, another CA, in 2010, which did not come into the public eye until 2012.

Large-scale IdM infrastructures that process vulnerable populations may lead to genocidal abuse (A3). In spite of historic precedence of the perils of mass identification in the Thrid Reich [Al04, Bl01], modern technology facilitates the mass sorting of populations by applying easily isusable technology such as the mass application of facial biometrics in public areas [Bo17]. Other vulnerable scenarios include digital identities for refugees in UNHCR camps who get registered with biometrics, which may expose them to new classes of risks [Ja15] where conflict moves from the physical into the cyber domain.

3 Attack vectors

The attack vectors through identity management need further attention. IdMs are complex systems combining many parties into the execution of multi-party protocols. End users of all levels of knowledge and relying parties without domain expertise are connected to and trust in certificate authorities, access control systems and document archives. Such systems have vast attack surfaces for intelligence, takeover or disruption. Attack vectors, in general, are:

- Traceable and linkable identifiers;
- Recognizable (unencrypted and identifiable) identity attributes;
- Registration attacks against certificate authorities;
- Directory attacks against directory services;
- Denial of service attacks against parts or all of IdM;
- Identifier, token and credential theft and misuse in replay, imposture or social engineering;

Attacks can get launched directed against IdM technology as well as against procedures and administrative staff. A wide overview over attack vectors against IdM is described by Haber and Rolls in [HR20b]. Tradscending digital risks they illustrate - as observed by Conti et al. [Co10] - the threats to IdM that come through physical information on paper or plastic [HR20a].

The observation of use patterns of IdM tokens has been noted by Paintsil [PF10], in particular accommodating tracking risks. Fritsch and Momen show how tracking of ID attributes

over time enables the collection of identity attributes [FM17, MF20], which constitutes an additional intelligence risk of specific types of IdM with observable tokens or personal information.

3.1 Impact

IdM as an attack vector in cyberwar and cyberphysical war will have serious impact. From the examples discussed above we can expect that IdM will be used in cyber attacks to seek the following purposes:

- Personalized surveillance of individuals of interest;
- Personalized and individual attacks (today drone killings, tomorrow run over by a smart car)
- Attacks on infrastructure (IdM compromized - infrastructure compromized);
- Attacks on documents, archives, authorizations, bank accounts et cetera (trolling and bot networks exploiting real accounts for adversary purposes);
- Identification opens channels for personalized propaganda and manipulation (Cambridge analytica, threats, blackmail and distortion).
- Identity is key to personal data that can get weaponized (compromates, blackmail, disruption, interference).

Facing the vast potential consequences of cybebrattacks, IdM should be both hardened and regulated to mitigate the perils of cyberwar.

3.2 Rules and regulation

IdM in cyber conflict relates to many rules and regulations that vendors of IdM might normally not have in mind when they develop or deploy their technology. Starting from the top level, one's ability to use digital identities and related services in undisrupted ways is anchored in the Universal human rights [As48]. Robinson et al. [Ro18] directly relate cyber conflicts that involve personal digital identity or personal data to three articles of the Universal human rights (pp.7). Article 3 guarantees the right to a safe life, article 12 protects the privacy of the individual, and article 19 guarantees freedom of expression and freedom of information against interference.

Further regulation of cyberwar action can be drawn from the rules of war laid forth in the Geneva convention. Specific requirements are the distinction of civilians from military under attack [Ro17] and the minimization of collateral damage to civilians. However, the concept

of cyber collateral damage [RG16] is ill-defined at this time while the IdM infrastructures are configured and deployed in ways that are close to guaranteeing cyber collateral damage on the civil society.

A closer look at privacy and data protection requirements for secure identity management has been taken by privacy regulators and technology experts in the scope of the FutureID project in [Ha13]. The report formulates strong requirements concerning the secrecy, unlinkability, integrity and control over identifiers. Privacy regulation such as the EU General data protection regulation (GDPR) [9] imposes similar strict data protection and privacy requirements on identity providers.

It may surprise that the EU NIS directive [10] does not focus explicitly on IdM as a critical service in society, given its role and its impact in the functioning of society.

4 Conclusion

Identity management (IdM) is an attractive target for cyber attacks. It enables adversarial surveillance, intelligence gathering, and identity theft. IdM can open channels for direct attacks on individuals as well as on large segments of the population, easily scaling up to the level of a genocide. The attack and disruption of IdM will affect, compromize or destroy critical societal services and critical infrastructures.

IdM should therefore be treated as a critical infrastructure of high relevance for societal security. In consequence, IdM needs to consider its weaknesses, implications and impact when attacked for the aforementioned purposes in cyberwar. Vendors and relying parties need to make sure that citizens will not be endangered through easily traceable or abusable digital identifiers. Identity attributes must be protected with high security assurance. Access to critical services and the integrity of digital archives must be preserved with special attention, which will demand protection measures as well as redundancy.

Effort will have to be spent to ensure that identity and access management providers prevent their directory services from becoming 'kill lists' for adversaries. One particular important question will be: How can we protect digital identities against nonconsensual use by other parties for the purpose of cyberwar? Biometric technology and plain-text identity attributes are two specific high-risk areas of IdM.

International laws and treaties may regulate future cyberwar consequences for IdM, however as of now they do not exist. Therefore should IdM be assessed for cyberwar risks and consequences in multiple perspectives: strategic, national security, national sovereignty, and last but not least focusing on the impact on citizens, in analogy to data protection or privacy impact assessments performed for personal data processing.

[9] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016, https://gdpr-info.eu/ , accessed 2020-02-21
[10] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016

We have to accept that IdM is both a critical infrastructure and an attractive target for cyberwar. Vendors and users of the technology need to be aware of the risks and consequences.

References

[Al04] Aly, Götz; Roth, Karl Heinz; Black, Edwin; Oksiloff, Assenka: The Nazi census: Identification and control in the Third Reich, volume 61. Temple University Press, 2004.

[As48] Assembly, UN General: Universal declaration of human rights. UN General Assembly, 302(2), 1948.

[Be18] Berghel, Hal: Malice domestic: The Cambridge analytica dystopia. Computer, (5):84–89, 2018.

[Bl01] Black, Edwin: IBM and the Holocaust: The strategic alliance between Nazi Germany and America's most powerful corporation. Random House Inc., 2001.

[Bo17] Botsman, Rachel: Big data meets Big Brother as China moves to rate its citizens. Wired UK, 21, 2017.

[Co10] Conti, Gregory; Larkin, Dominic Larkin; Raymond, David; Sobiesk, Edward: The Military's Cultural Disregard for Personal Information. Small Wars Journal, pp. 108–118, 2010.

[Du14] Dunlap, Charles J: The hyper-personalization of war: cyber, big data, and the changing face of conflict. Georgetown Journal of International Affairs, pp. 108–118, 2014.

[Ea17] Eakin, Hugh: The Swedish Kings of Cyberwar. The New York Review of Books, 2017.

[FFH18] Fritsch, Lothar; Fischer-Hübner, Simone: Implications of Privacy & Security Research for the Upcoming Battlefield of Things. Journal of Information Warfare, 17(4):72–87, 2018.

[FM17] Fritsch, Lothar; Momen, Nurul: Derived partial identities generated from app permissions. Proceedings of Open Identity Summit 2017, Lecture Notes in Informatics 277, 2017.

[Fr09] Fritsch, Lothar: Business risks from naive use of RFID in tracking, tracing and logistics. In: 5th European Workshop on RFID Systems and Technologies, RFIDSysTech. VDE, pp. 1–7, 2009.

[Ha13] Hansen, Marit; Jensen, Meiko; Marnau, Ninja; Zwingelberg, Harald; Fritsch, Lothar; Rodriguez, Charles Bastos; Aranda, Nuria Ituarte: FutureID Deliverable D22.3 - Privacy Requirements. Technical report, 2013.

[HG08] Hildebrandt, Mireille; Gutwirth, Serge: Profiling the European citizen. Springer, 2008.

[HR20a] Haber, Morey J.; Rolls, Darran: Identity Attack Vectors. In: Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. Apress, Berkeley, CA, pp. 107–116, 2020.

[HR20b] Haber, Morey J.; Rolls, Darran: Identity Management Controls in the Cyber Kill Chain. In: Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution. Apress, Berkeley, CA, pp. 117–124, 2020.

[Ja15] Jacobsen, Katja Lindskov: Experimentation in humanitarian locations: UNHCR and biometric registration of Afghan refugees. Security Dialogue, 46(2):144–164, 2015.

[Ka16] Kallberg, Jan: Strategic Cyberwar Theory-A Foundation for Designing Decisive Strategic Cyber Operations. The Cyber Defense Review, 1(1):113–128, 2016.

[MF20] Momen, Nurul; Fritsch, Lothar: App-generated digital identities extracted through Android permission-based data access-a survey of app privacy. SICHERHEIT 2020, 2020.

[MHF19] Momen, Nurul; Hatamian, Majid; Fritsch, Lothar: Did App Privacy Improve After the GDPR? IEEE Security & Privacy, 17(6):10–20, 2019.

[PF10] Paintsil, Ebenezer; Fritsch, Lothar: A taxonomy of privacy and security risks contributing factors. In: IFIP PrimeLife International Summer School on Privacy and Identity Management for Life. Springer, pp. 52–63, 2010.

[RG16] Romanosky, Sasha; Goldman, Zachary: Cyber collateral damage. Procedia Computer Science, 95(2):10–17, 2016.

[Ro17] Rowe, Neil C: Challenges of civilian distinction in cyberwarfare. In: Ethics and Policies for Cyber Operations, pp. 33–48. Springer, 2017.

[Ro18] Robinson, Michael; Jones, Kevin; Janicke, Helge; Maglaras, Leandros: An introduction to cyber peacekeeping. Journal of Network and Computer Applications, 114:70–87, 2018.

[SA11] Sigholm, Johan; Andersson, Dennis: Privacy on the battlefield?: Ethical issues of emerging military ICTs. In: 9th International Conference of Computer Ethics: Philosophical Enquiry (CEPE 2011), May 31st-June 3rd, 2011, Milwaukee, USA. INSEIT, pp. 256–268, 2011.

[vdM13] van der Meulen, Nicole: DigiNotar: Dissecting the First Dutch Digital Disaster. Journal of Strategic Security, 6(2):46–58, 2013.

[WB18] Wolff, J.; Braman, S.: 5 Certificates Gone Rogue: The DigiNotar Compromise and the Internet's Fragile Trust Infrastructure. In: You'll see this message when it is too late: The Legal and Economic Aftermath of Cybersecurity Breaches. pp. 81–100, 2018.

H. Roßnagel, C.H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 71

Accountable Trust Decisions: A Semantic Approach

Anders Schlichtkrull[1], Sebastian Mödersheim[2]

Abstract: This paper is concerned with the question of how to obtain the highest possible assurance on trust policy decisions: when accepting an electronic transaction of substantial value or significant implications, we want to be sure that this did not happen because of a bug in a policy checker. Potential bugs include bugs in parsing documents, in signature checking, in checking trust lists, and in the logical evaluation of the policy. This paper focuses on the latter kind of problems and our idea is to validate the logical steps of the trust decision by another, complementary method. We have implemented this for the Trust Policy Language of the LIGHTest project and we use the completely independently developed FOL theorem prover RP_X as a complementary method.

Keywords: Trust policies, Accountability, Security, Logic, Theorem Prover, Isabelle, eIDAS

1 Introduction

When an organization engages in an electronic transaction of substantial value or with significant implications for the organization, it should have *policies* in place to protect themselves or mitigate risks. For instance, before starting a costly production the business wants to be sure that the apparent customer that ordered the production is really the entity who initiated the order and that the electronic signature on the order is indeed legally binding (so it is reasonable to assume that it can be enforced by the legal system in the applicable jurisdiction). This may also include limits on the total value of the order so that even if a legal dispute fails or takes time, the company can stay operational.

The project LIGHTest [BL16] offers an infrastructure for formulating trust policies for this kind of purpose, e. g., a company may define the following policy: we accept every order up to a specified amount, if it was signed with an eIDAS qualified signature. They may additionally allow for trust schemes outside the European Union, but rely on trust translation recommendations: suppose the European Commission defines a translation from a foreign scheme to eIDAS, say level 3 in the foreign scheme is regarded as equivalent to level advanced in eIDAS, then the company may accept those signatures as well, but may choose to set a lower cap on the value of accepted orders. The reason for such a lower cap is that a legal dispute outside the European Union may be much more difficult for this company. On the other hand, they may have other business policies, e. g. if the customer

[1] Technical university of Denmark, DTU Compute, Richard Petersens Plads, Bygning 324, 2800 Kongens Lyngby, Denmark andschl@dtu.dk
[2] Technical university of Denmark, DTU Compute, Richard Petersens Plads, Bygning 324, 2800 Kongens Lyngby, Denmark samo@dtu.dk

is well-known or has a good reputation from other partners. Finally, We may also have delegation, i. e., if the customer is itself a company, it may be an employee signing on behalf of the company. For all these purposes, LIGHTest offers a Trust Policy Language (TPL) and has an automated trust verifier (ATV) to evaluate a given transaction against a given policy, possibly looking up trust list entries as needed [Mö19].

This paper is concerned with the question: how can we trust the trust decision made by the ATV, or more generally, how can we be sure about the result of an automated policy evaluation? The problem would be if we accidentally accept a transaction that actually does not meet the requirements of the policy – due to a bug in policy evaluation tool. We see at least the following aspects relevant to this question:

Cryptography Are for instance the electronic signature algorithms sufficiently secure (until the time we rely on them) and implemented correctly?

Parsing When extracting information from a document, is this parsing done correctly? Potential problems include ambiguous document formats, parts erroneously not included in the signature, vulnerabilities to injection/overflow attacks.

History Can we later prove to a third party what was the state of a trust list at the time of the policy decision? There can be modifications of the trust list by the hosting organization, as well as the problem of revocation.

Semantics Assume the previous points are all correct: does the transaction then indeed logically satisfy the policy? Potential problems include that the ATV has some logical bugs such as instantiating variables inconsistently.

Real world Does the policy actually make sense to the business such as limiting damages and providing sufficient legal assurances?

The main contribution of this paper is to propose a solution for the point "Semantics" by an "independent set of eyes". The idea comes from the area of proof assistants like Isabelle/HOL [NPW02] which provide a way to formalize mathematical claims and proofs for them in a language similar to programming languages, and that the proof assistant can check. This gives an overwhelming assurance that proofs are indeed correct, because it rules out the problem of holes, false conclusions, or imprecisions in proofs that often occur in standard proofs that are written in a mixture of mathematical terms and natural language. While Isabelle/HOL offers some automation to find proofs, the human prover still has to provide at least the main idea of a proof. The prover RP_X [SBT19], in contrast, is an automatic prover for First-Order Logic (FOL) that was proven correct in Isabelle. It is based on a handbook chapter by Bachmair and Ganzinger [BG01] and thus proves that their approach is correct. The formalization, however, revealed several non-trivial mistakes in the chapter, all of which were then rectified. With RP_X we thus have a theorem prover where we have the same overwhelming assurance as in Isabelle when RP_X accepts a FOL-statement

as logically valid. Since LIGHTest's TPL is inspired by Prolog, we can cast policy decisions as FOL theorem proving problems and thus use RP_X for double checking them.

One may wonder why not to use RP_X as the policy decision tool in the first place. The reason is that the ATV of LIGHTest evaluates policies in a different way than a theorem prover: it processes a transaction (parsing, signature checking, comparing fields) and interacts with different servers maintaining trust lists; also it has to process policy rules and their elements in a given order. In contrast, a theorem prover deals only with logical formulae and needs the freedom to "process" them in an arbitrary order in order to be most effective. We thus propose the combination of ATV and RP_X – or more generally: the combination of a policy decision tool with a verifier – as they benefit from complementary strengths.

The main contribution of this paper is the integration of the ATV and RP_X. This includes defining a good interface for the first three aspects **Cryptography**, **Parsing** and **History** that are beyond what RP_X can check. The implementation of our approach is part of the LIGHTest distribution and first experiments have indeed revealed a few mistakes in a preliminary implementation of the ATV that are now all corrected; thus our verification has, if anything, already practically contributed to improving the ATV.

2 Preliminaries

Our work is based on the LIGHTest Trust Policy Language TPL [Mö19] which we first briefly introduce by way of an example TPL policy (adapted from [Mö19]). This example is that an auction house receives bids for auction lots over the Internet in a custom format (defined by the auction house themselves) and it accept all bids up to 1500 Euro as long as the bidding form is signed by an eIDAS qualified signature. In TPL this looks as follows:

```
 1. accept(Transaction) :-
 2.   extract(Transaction, format, theAuctionHouse2020format),
 3.   extract(Transaction, bid, Bid),
 4.   Bid <= 1500,
 5.   extract(Transaction, certificate, Certificate),
 6.   extract(Certificate, format, x509),
 7.   extract(Certificate, pubKey, PK),
 8.   verify_signature(Transaction, PK),
 9.   check_eIDAS_qualified(Certificate).
10.
11. check_eIDAS_qualified(Certificate) :-
12.   extract(Certificate, format, eIDAS_qualified_certificate),
13.   extract(Certificate, issuer, IssuerCertificate),
14.   extract(IssuerCertificate, trustScheme, TrustSchemeClaim),
15.   trustscheme(TrustSchemeClaim, eIDAS_qualified),
```

```
16.   trustlist(TrustSchemeClaim, IssuerCertificate, TrustListEntry),
17.   extract(TrustListEntry, format, trustlist_entry),
18.   extract(TrustListEntry, pubKey, PkIss),
19.   verify_signature(Certificate, PkIss).
```

Lines 1 to 9 define a *predicate* `accept`. Such a definition is called a *clause*. The predicate `accept` specifies when a transaction is accepted. The transaction is here represented as a parameter variable `Transaction` to the predicate (on line 1). As a convention, variables always start with a capital letter, while identifiers that start with a lower-case letter are constants or predicate symbols. The following lines give constraints on the transaction that need to be all true in order to satisfy `accept(Transaction)`.

TPL supports the use of arbitrary data formats as long as a parser for that format exists. Consider the constraint on line 2 that uses the `extract` predicate. The `extract` predicate connects TPL with the parsers of the various data formats where the first two parameters are the input and the third parameter is the output. In the concrete example we ask what the `format` of `Transaction` is and we expect a particular result defined by the constant `theAuctionHouse2020format`. In the example, this is a custom format defined by the auction house themselves, containing a number of fields that they require to be filled in in order to make a bid at their current auction; assume these fields include at least the fields `bid` and `certificate` that we formulate constraints on below. The policy decision would be negative if at this point the parser for this format does not successfully parse the given transaction.

In line 3 the `extract` predicate is given as parameters `Transaction`, `bid` and `Bid`. As said before, the `theAuctionHouse2020format` contains a field called `bid`, and the constraint here is to simply bind the concrete value in the transaction to the variable `Bid` (in fact this constraint cannot fail). Line 4 specifies the constraint that whatever is now the value of `Bid` should be at most 1500. Again, if the concrete bid in the transaction is above 1500, then at this point the policy decision stops with a negative result.

In lines 5-7 we first extract a certificate from the transaction, now represented as variable `Certificate`, then we put the constraint that it should be of the x509 format, and lastly we extract a public key from it, binding it to a new variable `PK`. Here we assume a similar interface to the x509 format as for the auction house format. In line 8 we use the `verify_signature` predicate to require that the signature on the transaction `Transaction` can be verified with the `PK` public key. In fact, this requires that `theAuctionHouse2020format` is a format with a notion of a signature.

Each constraint of the clause so far (lines 2-8) uses *built-in* predicates of TPL (`extract`, `<=`, and `verify_signature`). The predicate in line 9, however, is not built-in: it is defined by the clause in lines 11-19. Lines 11-14 constrain what format the certificate must have and also extracting from it an issuer certificate and from that a trust scheme claim. A trust scheme claim is a URL to a trust list that the issuer certificate claims to be represented on. In line 15 we use the built-in `trustscheme` predicate with second parameter `eIDAS_qualified` which

checks if the URL points to the eIDAS trust list. In line 16 we use the built-in predicate `trustlist` actually perform the trustlist lookup, to check if it indeed contains the required `IssuerCertificate`. As a result of a successful lookup, we obtain a `TrustListEntry` that we check in lines 17 to 19: we check the entry format, extract the public key stored in the entry, now `PkIss`, and verify `Certificate`'s signature with respect to `PkIss`.

In this example we have defined both the predicates `accept` and `check_eIDAS_qualified` by one clause each. In general, we can define any number of clauses, and they represent alternative ways to satisfy a predicate. For instance, in the example a bid above 1500 Euro would not fulfill the above clause, but if another `accept` clause is specified (e. g. on known customers) then the ATV tries that next.

3 Transcripts

The goal of this paper is to verify the logical aspect of the trust decisions of the ATV – and we leave out the aspects that are "outside" the logical realm, namely the verification of signatures, parsing, and server lookups. We thus need an appropriate interface between the logical and the extra-logical side. To this end we introduce the notion of a *transcript* as a triple (P, Q, E) where P is the TPL policy, Q is a *query* and E is an *event log*. The query will be simply of the form `accept(transaction)` where `transaction` is a constant representing the transaction document in question. In fact, for all elements that we talk about in the transcript, we use such symbolic constants. The event log contains a recording of all built-in predicates that were successfully evaluated by the ATV during the policy decision.

Since we need to work later with symbolic constants, but the ATV works on quite different data-structures, we need to take an intermediate step to arrive at a transcript. As a policy is being checked, the ATV will build what is basically a tree representation of the various objects that it stores. Running the above policy on with a concrete transaction could result in the following tree representation:

```
(root)
+--transaction
|  +-- format = "the_auction_house_2020"
|  +-- bid = "600"
|  +-- certificate
|      +-- pubKey
|      +-- issuer
|          +-- trustScheme = "trust.eidas.eu"
+--trustlistentry1
   +-- pubKey
```

This tree represents a state of the ATV where it contains a transaction and a trust list entry which each are represented as subtrees, namely the subtrees rooted in "(root).transaction"

and "(root).trustlistentry1" respectively. We shall from now on ignore the root node in paths and thus the mentioned paths of the example start with "transaction" or "trustlistentry1". The tree has internal nodes like "transaction.certificate". The tree also has leaves such as "transaction.bid". This leaf contains the value "600". Additionally, the ATV keeps track of the concrete data that some parts of the tree represent, for instance "transaction.certificate" and "trustlistentry1.pubKey" represent a certificate and a public key, respectively, and the ATV needs to keep track of the certificates signature.

We have thus augmented the ATV so that it can generate the event log as a side effect during its normal work. We use again the example policy from section 2 and as a transaction the concrete objects shown in the above tree (fulfilling the policy):

```
extract(transaction, format, theAuctionHouse2020format).
extract(transaction, bid, 600).
600 <= 1500.
extract(transaction, certificate, transaction_certificate).
extract(transaction_certificate, format, x509).
extract(transaction_certificate, pubKey, transaction_certificate_pubKey).
verify_signature(transaction, transaction_certificate_pubKey).
extract(transaction_certificate, format, eIDAS_qualified_certificate).
extract(transaction_certificate, issuer, transaction_certificate_issuer).
extract(transaction_certificate_issuer, trustScheme,
            transaction_certificate_issuer_trustScheme).
trustscheme(transaction_certificate_issuer_trustScheme, eIDAS_qualified).
trustlist(transaction_certificate_issuer_trustScheme,
            transaction_certificate_issuer, trustlistentry1).
extract(trustlistentry1, format, trustlist_entry).
extract(trustlistentry1, pubKey, trustlistentry1_pubKey).
verify_signature(transaction_certificate, trustlistentry1_pubKey).
```

This log contains an encoding of the concrete instance of all built-in predicates that occurred during evaluation. The representation includes constants representing the paths into the tree that were used during the execution; for example, `transaction_certificate` represents the path "transaction.certificate". We take care that when such constants are introduced they do not clash with the constants already present in the policy.

4 Translating Transcripts to Logical Formulae

We now translate a transcript to logical formulae. Our running example policy will be translated to the following logical formula:

$(\forall \mathit{Transaction}, \mathit{Bid}, \mathit{Certificate}, \mathit{PK}.$
$\quad \mathit{accept}(\mathit{Transaction}) \leftarrow ($

$$
\begin{aligned}
&\quad extract(Transaction, format, theAuctionHouse2020format) \wedge \\
&\quad extract(Transaction, bid, Bid) \wedge \\
&\quad less\_or\_eq(Bid, i1500) \wedge \\
&\quad extract(Transaction, certificate, Certificate) \wedge \\
&\quad extract(Certificate, format, x509) \wedge \\
&\quad extract(Certificate, pubKey, PK) \wedge \\
&\quad verify\_signature(Transaction, PK) \wedge \\
&\quad check\_eIDAS\_qualified(Certificate) \\
&\quad) \\
&) \\
&\wedge \\
&(\forall Certificate, IssuerCertificate, PkIss, TrustListEntry, TrustSchemeClaim. \\
&\quad check\_eIDAS\_qualified(Certificate) \leftarrow (\\
&\quad extract(Certificate, format, eIDAS\_qualified\_certificate) \wedge \\
&\quad extract(Certificate, issuer, IssuerCertificate), \wedge \\
&\quad extract(IssuerCertificate, trustScheme, TrustSchemeClaim) \wedge \\
&\quad trustscheme(TrustSchemeClaim, eIDAS\_qualified) \wedge \\
&\quad trustlist(TrustSchemeClaim, IssuerCertificate, TrustListEntry) \wedge \\
&\quad extract(TrustListEntry, format, trustlist\_entry) \wedge \\
&\quad extract(TrustListEntry, pubKey, PkIss) \wedge \\
&\quad verify\_signature(Certificate, PkIss) \\
&\quad) \\
&)
\end{aligned}
$$

The translation for each clause replaces the commas (`,`) with conjunction symbols ($\wedge$), and the colon dash (`:-`) is replaced with an implication symbol ($\leftarrow$). Lastly all variables in the clause are universally quantified (using the $\forall$ symbol). The translation of the policy is then simply the conjunction (using $\wedge$) of the translated clauses. Note that numbers such as 1500 are translated to symbolic constants *i1500* and the <= operator becomes the predicate *less_or_eq*. Our implementation makes sure that these names do not clash with names of other logical constants or predicates as to avoid an ambiguity in their meaning. Let us call the above example formula P^{ex}.

The event log is translated as a conjunction as well, in our example E^{ex} is the formula:

$$
\begin{aligned}
&extract(transaction, format, theAuctionHouse2020format) \wedge \\
&extract(transaction, bid, i600) \wedge \\
&less\_or\_eq(i600, i1500) \wedge \\
&\ldots \\
&verify\_signature(transaction\_certificate, trustlistentry1\_pubKey)
\end{aligned}
$$

With the query $Q^{ex} = accept(transaction)$ we have the translated transcript (P^{ex}, Q^{ex}, E^{ex}).

5 Semantics: From Logic Programming to FOL

Check the Transcripts Essentially the idea is now that after a successful run of the ATV we have three formulae (P, Q, E): the policy P, the query Q and the event log E. We essentially want to double check with RP_X whether $P \wedge E$ logically implies Q. If so, then the positive decision of the ATV is *verified*. However, as always, the devil is in the details and we describe now how to make the connection to RP_X semantically precise.

RP_X [SBT19] is an automatic theorem prover for First-Order Logic (FOL). Given a FOL formula in TPTP format [Su17], RP_X attempts to prove that the negation of the formula is unsatisfiable. While RP_X can run into non-termination (since validity is undecidable for FOL), we have a strong guarantee when it does terminate. The reason is that the inference engine of RP_X has been proved to be *sound* and *complete* using the proof assistant Isabelle/HOL [SBT19]. *Soundness* gives us strong mathematical guarantees that if RP_X claims that the formula is unsatisfiable then indeed it is unsatisfiable. *Completeness* gives us strong mathematical guarantees that if the formula is unsatisfiable then RP_X will be able to prove that, when given enough time.

Since TPL is inspired by Prolog, unsurprisingly its semantics is based on logic programming as well, and in fact this work exploits how close TPL is to the semantics of FOL for which RP_X implements an automated theorem prover. There are some differences however, and we now highlight these details carefully and discuss how we can handle them.

Free Algebra Logic programming generally works on so-called *free models*, for an overview see for instance [EFT94, Chapter 11] and since there is sometimes confusion about the semantics, Hinrichs and Genesereth suggested the formal definition of *Herbrand Logic* [HG06] to contrast it more precisely with FOL. One of the key differences is that in Herbrand logic and logic programming in general, function symbols behave like in a free term algebra. For instance, if we have a binary function symbol f, then $f(t_1, t_2) = f(s_1, s_2)$ holds iff both $t_1 = s_1$ and $t_2 = s_2$. In other words: two terms are equal iff they are syntactically equal. This means in particular that for any two distinct constants c and d, it holds that $c \neq d$, because constants are just functions of arity 0. In contrast, standard FOL allows to model function symbols with algebraic properties such as commutativity.

Universes The model-theoretic definition of a logic is based on the concept of a *universe*, i. e. a non-empty set U of objects. For standard FOL, every function f of arity n is interpreted as a function from U^n to U, and every relation symbol of arity n is interpreted as a subset of U^n. For instance, the universe may be $U = \{0, 1\}$ and + is interpreted as disjunction, and $\cdot$ is interpreted as conjunction, and the binary relation $<$ is interpreted to be true only for the pair $(0, 1)$. The difference for Herbrand logic is that the universe is determined by the set of function symbols we employ: we take as universe the set of terms that can be built from the terms. For instance if we have just two function symbols 0 of arity 0 and s of arity 1,

then $U = \{0, s(0), s(s(0)), \ldots\}$ which can be regarded as the set of natural numbers. The "interpretation" of function symbols is then as expected.

Arithmetics In fact, this makes Herbrand logic even more expressive than standard FOL: we cannot formalize arithmetics in first-order logic because we lack the expressive power to formalize that the universe U is the natural numbers (we would have to formalize well-foundedness or the induction principle which are higher-order concepts), while Herbrand logic fixes the universe and we can thus get the natural numbers "for free". This even allows formalizing arithmetics (addition, multiplication, and comparison on natural numbers) as Hinrichs and Genesereth show [HG06]: even though we cannot for instance define addition as a binary function directly, we can use a ternary relation like $add(x, y, z)$ to represent that the addition of x and y gives z, and based on this axiomatize arithmetics completely. While this allows a semantically unambiguous integration of arithmetic into our policy language, what TPL (or logic programming approaches for that matter) can actually support is the direct evaluation of ground arithmetic statements like $5 + 3 < 100$, but they cannot solve equations. Therefore, in TPL we have to require that when the ATV reaches a condition like $X < 100$ that X is instantiated with a concrete integer through some other condition. In fact, note that while validity of formulae in FOL is semi-decidable, for Herbrand logic neither validity nor its complement is semi-decidable.

Least Models A last important difference to FOL is that most logic programming approaches do also fix the interpretation of the relationship symbols to be the *least* interpretation that satisfies all clauses. For instance, consider the policy that consists only of the single clause $p() : -q()$, and no more information is given. Then in normal FOL, there are three interpretations satisfying this clause: $q()$ can be false and $p()$ can be either true or false, or both $q()$ and $p()$ are true. The least interpretation, i. e. the interpretation chosen by Prolog-style semantics, is that both $p()$ and $q()$ are false. This is sometimes also called *negation by failure*: since we fail to prove $q()$, it counts as false and thus we also fail to prove $p()$ which is therefore also false.

While this behavior can cause confusion in logic programming (e. g. when using *not* and *cuts* as in Prolog), for policies it can make specifications actually quite intuitive: a policy is described always in a positive way, i. e. by sufficient conditions to satisfy the policy (or a particular concept of the policy), and everything else is outside the policy, i. e. a default-deny behavior which also means that forgetting to describe a case leads to erring on the safe side.

Mind the Gap Now that we have highlighted all the differences, let us consider how they need to be taken into account so that the verification we perform in the FOL-prover RP_X indeed agrees precisely with the semantics of TPL. Recall that we already

have predicates like `extract` that are interfaces between the logical side and the real-world documents and servers. We handle them axiomatically in the logic, i. e. whatever checks and lookups the ATV does are recorded and supplied as facts, e. g. that $extract(transaction, format, theAuctionHouse2020format)$ holds.

The first idea is now that, since we cannot formalize arithmetic in FOL, we handle all arithmetic checks axiomatically as well, e. g., if the ATV encountered the check $500 < 1000$, then this is also added as an axiom to the library. Indeed, it is easy to check such statements outside the FOL, so there was no sense in trying to integrate them in RP_X (which would only be possible in some approximation, anyway).

For the other issues – free algebra, universes and least models – we make use that all policy decisions have a particular form, namely evaluating a goal predicate with respect to a policy. More in detail, let H be a conjunction of the policy rules and all other information we have (statements about extractions, signature verifications, server lookups, and arithmetic checks), and let q be a query q (a ground predication). The *least model* of H is the least interpretation that satisfies all conditions we described above: the universe is the set of ground terms that can be built using the function symbols, every function symbol is freely interpreted in that universe, and all relationship symbols are interpreted as the least relation that satisfies all clauses in H. The policy decision, written $H \models_{TPL} q$, is now the question whether q holds in the least model of H.

The corresponding question that we ask RP_X is whether the formula $H \wedge \neg q$ is *satisfiable* in FOL. Satisfiable means that there is at least one satisfying FOL interpretation for this formula. If RP_X answers "no", then there is no way to interpret the universe and the function and relation symbols such that both H and $\neg q$ are satisfied – and this includes the least TPL model of H and thus $H \models_{TPL} q$. Thus if RP_X finds $H \wedge \neg q$ unsatisfiable, we know that q was correctly accepted as satisfied by the Automated Trust Verifier and we have successfully verified the trust decision.

In fact, the converse statement also holds: if RP_X answers "yes" to the question whether $H \wedge \neg q$ is satisfiable, then actually $H \not\models_{TPL} q$. In other words, a correct positive trust decision from the ATV is never refuted by RP_X, only when the ATV erroneously marks a query q as fulfilled, will RP_X complain. The proof of this is trickier though and we only give a brief sketch. Suppose we have some satisfying FOL interpretation $\mathcal{I}$ for $H \wedge \neg q$ and compare it to the least TPL model of H, then the TPL model will be "at least as fine": equality on terms is the finest possible relation in the least TPL model, and thus the least TPL model of the predicates contains at most as much as $\mathcal{I}$. Thus since q is not true in $\mathcal{I}$, it is also not true in the least TPL model of H, thus $H \not\models_{TPL} q$.

6 Experiments and Conclusion

The approach described in this paper is completely implemented and part of the LIGHTest distribution. In fact, we have already started testing it when the implementation of the ATV

was still in a preliminary state. We found a couple of examples where the ATV and RP_X did not agree on policy decisions. For example a predicate like $p(X, X)$ is actually true for an arbitrary value as the first parameter – only the second parameter must be identical. This *unification* between parameters was not correctly implemented in the first version of the ATV. The error was of type *wrong reject*, i. e. the decision was negative when it should be positive, which is erring on the safe side, but undesirable nonetheless. All mistakes have been corrected and extensively tested using our RP_X connection.

To our knowledge, the only other work that double checks policy decision through a connection to an independent verifier is by Jim [Ji01]. There, the accountability argument hinges on the proof checker being a relatively simple program; in contrast, we use with RP_X a verifier that itself is verified in Isabelle. We believe that such works are in principle feasible and worthwhile for other policy languages where a formal semantics is defined that can be verified by means other the main policy decision tools. This exploits the fact that the design of such a semantics is often simpler than the procedure to obtain decisions that also integrates the extra-logical aspects like server lookups.

This work has focused exclusively on verifying the logical aspects of the decision. Let us at least briefly discuss the other aspects. For the parsing of documents, we have proposed a notion akin to the formats of TPL that in a heterogenous eco-system of formats prevent confusion about the meaning of messages [MK14]. For the cryptography and transmission channels there are first works on verifying implementations [Bh16]. This is crucial for server lookups, but not sufficient. The problem that trust lists may change over time implies the problem to later prove to a third party that the policy was satisfied at the time of checking. In fact, it is a reasonable requirement that trust lists maintain historical records, but especially in a volatile environment like servers for delegation that also try to protect the contents of the delegation lists against monitoring, this may be non-trivial.

This is actually related to the more "high-level" problem, namely whether a policy makes even sense for a business in the first place: that all conditions we check and all information we have gathered in a policy decision are sufficient to prove to a third party – e. g. in a legal dispute – what has happened. While many legal aspects are outside a technical view, we plan as future work to verify accountability properties [KTV10] of logging mechanisms and their relation to the policies we put in place.

Acknowledgments We thank Andreas Viktor Hess, Georg Wagner, Stefan More and Lukas Alber for helpful discussions and support in the adaption of the ATV. This work was supported by the Sapere-Aude project "Composec: Secure Composition of Distributed Systems", grant 4184-00334B of the Danish Council for Independent Research, by the EU H2020 project no. 700321 "LIGHTest: Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Trust schemes" (lightest.eu) and by the "CyberSec4Europe" European Union's Horizon 2020 research and innovation programme under grant agreement No 830929.

References

[BG01] Bachmair, L.; Ganzinger, H.: Resolution Theorem Proving. In (Robinson, A.; Voronkov, A., eds.): Handbook of Automated Reasoning. Vol. I, Elsevier and MIT Press, pp. 19–99, 2001.

[Bh16] Bhargavan, K.; Delignat-Lavaud, A.; Fournet, C.; Kohlweiss, M.; Pan, J.; Protzenko, J.; Rastogi, A.; Swamy, N.; Béguelin, S. Z.; Zinzindohoue, J. K.: Implementing and Proving the TLS 1.3 Record Layer. IACR Cryptology ePrint Archive 2016/, p. 1178, 2016.

[BL16] Bruegger, B. P.; Lipp, P.: LIGHT^{est} - A Lightweight Infrastructure for Global Heterogeneous Trust Management. In (Hühnlein, D.; Roßnagel, H.; Schunck, C. H.; Talamo, M., eds.): Open Identity Summit 2016, 13.-14. October 2016, Rome, Italy. Vol. P-264. LNI, GI, pp. 15–26, 2016.

[EFT94] Ebbinghaus, H.; Flum, J.; Thomas, W.: Mathematical logic (2. ed.) Springer, 1994, ISBN: 978-3-540-94258-0.

[HG06] Hinrichs, T.; Genesereth, M.: Herbrand Logic, tech. rep. LG-2006-02, http://logic.stanford.edu/reports/LG-2006-02.pdf, CA, USA: Stanford University, 2006.

[Ji01] Jim, T.: SD3: A Trust Management System with Certified Evaluation. In: 2001 IEEE Symposium on Security and Privacy, Oakland, California, USA May 14-16, 2001. IEEE Computer Society, pp. 106–115, 2001.

[KTV10] Küsters, R.; Truderung, T.; Vogt, A.: Accountability: definition and relationship to verifiability. In (Al-Shaer, E.; Keromytis, A. D.; Shmatikov, V., eds.): CCS 2010. ACM, pp. 526–535, 2010.

[MK14] Mödersheim, S.; Katsoris, G.: A Sound Abstraction of the Parsing Problem. In: CSF 2014. IEEE Computer Society, pp. 259–273, 2014.

[Mö19] Mödersheim, S.; Schlichtkrull, A.; Wagner, G.; More, S.; Alber, L.: TPL: A Trust Policy Language. In (Meng, W.; Cofta, P.; Jensen, C. D.; Grandison, T., eds.): IFIPTM 2019. Vol. 563. IFIP Advances in Information and Communication Technology, Springer, pp. 209–223, 2019.

[NPW02] Nipkow, T.; Paulson, L. C.; Wenzel, M.: Isabelle/HOL — A Proof Assistant for Higher-Order Logic. Springer, 2002.

[SBT19] Schlichtkrull, A.; Blanchette, J. C.; Traytel, D.: A verified prover based on ordered resolution. In (Mahboubi, A.; Myreen, M. O., eds.): CPP 2019. ACM, pp. 152–165, 2019.

[Su17] Sutcliffe, G.: The TPTP Problem Library and Associated Infrastructure. From CNF to TH0, TPTP v6.4.0. Journal of Automated Reasoning 59/4, pp. 483–502, 2017.

On the diffusion of security behaviours

An informed argument using diffusion of innovations theory on the uptake of four different security behaviours

Sebastian Kurowski, Heiko Roßnagel[1]

Abstract: Security behaviour has been researched from a variety of theoretical lenses, however a clear picture on the factors that foster secure behaviour is still missing. This contribution uses the diffusion of innovations theory and applies it to four exemplary security behaviours to identify how it can explain the uptake of each behaviour. In contrast to many other approaches, it focuses on the behaviour itself, not the behaving individual. We are able to show differences in the uptake of idealized security behaviours. A perceived relative advantage positively impacts the uptake of a behaviour, however this advantage seems rarely to be motivated by a perceived risk. Risk only seems to play a minor role for the diffusion of security behaviours. Additionally, the relative advantage does not seem to be a necessity for the diffusion of a behaviour. If the other properties namely compatibility, triability, observability, and low complexity of a behaviour are adequately fulfilled a successful diffusion is still possible.

Keywords: Security behaviour; Policy Compliance; Diffusion of Innovation; Security Culture

1 Introduction

Secure behaviour is an important asset in an information security architecture. And while there has been a multitude of studies on secure behaviour, policy compliance, and policy adherence, there is to date no settled theoretical foundation [So15a], and thus no reliable guidance on how to foster secure behaviour in organizations. Additionally, recent findings suggest that the effect of training and awareness on the organizations security may be limited [Kw19]. Still human behaviour remains an important antecedent for security attacks [Jo16]. Some security behaviours seem to be picked up more easily than others' by individuals. Which leads to an interesting question: Why? Behavioural research in security tackles this question mostly by considering the behaving individual, with limited success so far [So14][So15a][Ku19]. However, there is little research on the impact of the security behaviour itself on its adoption rate. In order to shed light on this, we employ the theory on diffusion of innovations [Ro03] to security behaviours in order to discuss potential adoption successes or failures of secure behaviours. By doing so, we reduce the individual and its characteristics from the consideration, which makes sense if secure behaviour is considered an ideal behaviour, idealized by security experts.

[1] Fraunhofer-Institute for Industrial Engineering IAO, Team Identity Management, Stuttgart, 70599, firstname.lastname@iao.fraunhofer.de

This contribution includes a brief summary on the existing research on secure behaviour along with a brief discussion of its methodological constraints (Section 2.1), an introduction of the application of diffusion of innovations theory in security research (Section 2.2), followed by an overview on diffusion of innovations theory itself (Section 2.3). In order to approach the research question, we analyse four different security behaviours in the context of diffusion theory: employing privacy screens, covering the device camera, using e-mail encryption, and using single sign-on systems. We then use a Google Trends analysis on these behaviours in order to see which behaviours show an increasing interest, and which behaviours do not. We conclude with a summary of the diffusion properties of these behaviours (see Section 3). Of course, this contribution uses limited methodology, and informed arguments in order to draw its conclusion. Therefore, this research has mentionable limitations (see Section 4). However, our discussion will argue the practical relevance, and the epistemological appropriateness of our approach (Section 5).

2 Related Work

2.1 Security Behaviour

Secure behaviour has been approached from a variety of theoretical lenses, including value-focused (e.g. Theory of Planned Behaviour, TPB), rationality-focused (e.g. Rational Choice Theory, RCT), deterrence-focused (e.g. Protection Motivation Theory, PMT, and General Deterrence Theory, GDT), and environment-focused (e.g. Social Cognitive Theory, SCT) theories. For instance, the theory of planned behaviour (TPB) highlights that before we can expect actual secure behaviour, we need to induce the intention to act. That in turn relies heavily on the personal goal system, the external environment as well as the perceived personal ability to take control over the situation. TPB is founded in socio-psychology and combines individual and environmental aspects for explaining secure behaviour. It is used in various quantitative studies on secure behaviour [Sa15][Si14][So15b]. Rational choice theory is usually seen as evaluating the cost-benefit situation of non-secure behaviour, waging of sanction or consequence severity, and detection probability [If16][VS12] or waging of benefits of non-secure behaviour versus the costs of secure behaviour [Bu10][Ka13]. Quite contrary to the TPB, the subject actively wages off benefits versus costs of the situation and decides upon the maximum utility for itself. This view on rationality aligns well with the use of sanctions versus the benefits of a non-secure behaviour and is used accordingly [If16][Ka13][VS12]. PMT offers a foundation of secure behaviour that can be quite intuitive. After all, why should there be any other reason for individuals to exhibit secure behaviour, rather than averting a threat? PMT is therefore quite extensively used in quantitative studies on both secure and non-secure behaviours [Bo15][Jo16][Po15][PH14][Si14][So15a]. Social Cognitive Theory employing research stems from a theoretical foundation, where successful adaption of secure behaviour benefits from a social system that promotes and rewards and

where one gains experiences both by observing role models as well as engaging in activities raising their self-efficacy [GY12][Rh09]. Finally, general deterrence theory is a possible useful model for explaining why people adhere to rules and policies. Its focus aligns very well with possible considerations around secure behaviour. Similar to PMT the intuitive cause of secure behaviour should be the aversion of a threat, in this case the deterrence of a threat or punishment. Therefore GDT, such as PMT is widely used in quantitative studies on secure information security behaviour and the lack thereof [If16][Jo16][Li14]. All these approaches have in common that they try to explain secure behaviour in individuals. However, meta-analyses find no clear winner among these theoretical foundations [So15a]. Additionally, some of those quantitative studies show response biases [Ku19]. In addition, if one considers that research on secure behaviour mixes ideals with observable realities, namely something that security experts consider an ideal behaviour with actual behaviours by people mostly outside of the security domain, then the whole approach of researching the individual along with an idealized behaviour is questionable. Secure behaviour means that an individual is ought to behave in an idealized way, a „secure way". This however may collide with the individuals reality, which may be very different from the reality of a security researcher. If secure behaviour is considered an ideal, whereas behaviour itself is considered an empirically observable reality, then the observation of ideal versus behaviour can only be employed with epistemologies that do not reduce the social relationship between researcher and observation, such as interpretivism [Wa93]. One conclusion of this thought could be that secure behaviour should be approached with methodologies that are able to reflect the researcher in the observation. Another conclusion could be to focus on the idealized behaviour itself, rather than the individual and an idealized behaviour in conjunction. This contribution takes the latter path, by considering the diffusion of behaviours and thus how likely a behaviour is being picked up, and not how likely an individual may pick up a certain behaviour.

2.2 Diffusion of Information Security

The adoption and diffusion of information technology has been well researched in the economics and information systems domains. This has led to the development of widely accepted and used theories such as the diffusion of innovations theory [Ro03] and the technology acceptance model [Da89]. In information security research, however, these theories have only been used very rarely. [RZ12] proposed a structured approach to assess market success of information security technologies based on the Diffusion of Innovations process. They also applied this approach to several technologies such as electronic signatures [Ro06], privacy enhancing technologies [Ro10] and federated identity management [Hü10]. However, to the best of our knowledge it has not yet been applied to security behaviour, which is surprising, as security behaviour can be considered as an innovation just as likely as technology.

2.3 Diffusion of Innovations

This research examines a variety of factors, which have been shown to be determinants of IT adoption and usage, and further has been applied to explain the adoption and diffusion of a great variety of innovations ranging from new methods of agriculture to modern communication technology. In his seminal work Rogers defines five attributes of innovations, as perceived by the members of the social system that determine the rate of adoption of an innovation [Ro03]: Relative Advantage, Compatibility, Complexity, Triability and Observability.

Relative advantage is the degree to which an innovation is perceived as better than the idea it supersedes. It is not so important if the innovation has an objective advantage, but rather if the individual perceives the innovation as advantageous. Advantages can be measured in economic terms, but social prestige, convenience, and satisfaction also can play an important role. **Compatibility** is the degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters. An Innovation that is consistent with the existing values will diffuse more rapidly than one that is incompatible with the norms and values of the social system. **Complexity** is the degree to which an innovation is perceived as difficult to understand and use. Innovations that are easier to understand will be adopted more rapidly than those which require the adopter to develop new skills and understandings. **Triability** is the degree to which an innovation may be experimented with on a limited basis. New ideas that can be tried before the potential adopter has to make a significant investment in the innovation are adopted more quickly. **Observability** is the degree to which the results of an innovation are visible to others. The easier it is for individual to observe the results of an innovation, the more likely they are to adopt [Ro03]. In addition to the main attributes, Rogers also describes the diffusion process: ”The innovation-decision process is the process through which an individual passes from gaining initial knowledge of an innovation, to forming an attitude toward the innovation, to making a decision to adopt or reject, to implementation of the new idea, and to confirmation of this decision” [Ro03]. The start and speed of the innovation-decision process varies between the different members of the social system. Therefore, the various decisions to adopt or reject the innovation are also spread over time. The dynamic of this process is a result of the changes in the information the individual acquires and possesses about the innovation [Li00].

3 Diffusion properties of security behaviour

In the following we are going to apply the diffusion of innovations theory to several exemplary security behaviours. We will discuss how it can explain the successful adoption of each behaviour.

3.1 Privacy Screen Protector

Shoulder surfing is a low cost attack that can be utilized easily, especially with mobile users [Lo11]. An effective deterrent against these kinds of attacks are privacy screen protectors, which reduce the possible angle of view on the device screen. This way, only individuals that are at the right angle with regard to the device are able to see the screen contents. **The risk:** The risk of shoulder surfing is quite tangible. Unlike other information security threats, materialization of this risk does not require some virtual, invisible attacker. In fact the risk of shoulder surfing can become tangible, in principle, as soon as one spots someone else, who is looking at one's device screen. However, apart from social engineering enthusiasts and security experts, the risk of shoulder surfing is seemingly not perceived as an existing one [Ha14][Tr16].**The impediments:** Privacy screens darken the device screen, and inhibit individuals to one's left or right to look at the screen. This means that there could be a major work impediment for individuals who rely on physically sharing their screen. However, especially in times of mobile work, physically sharing the screen becomes less and less likely as remote work increases. Furthermore, the screen can easily be removed if needed. **The countermeasure:** A screen protector is tangible and easy to understand. Its effects are visible as soon as it is applied. Finally, it is removable and can therefore be tried out. **Assessing the diffusion:** Summing up, the privacy screen protector could provide a *relative advantage* by providing felt security. However, in light of the lack of risk perception it is questionable as to how a relative advantage can be perceived through this. On the other hand a perceived relative advantage could be reduced if physical sharing of a device screen is required, but especially with the rise of mobile work, it is disputable as to what extent this influences the relative advantage of screen protectors. The solutions *compatibility* again depends largely on the requirement to physically share a device screen, which we expect to be relatively seldom. The solution is easy to understand (low *complexity*), its application can be observed (*Observability*), and it can be tried out easily (*Triability*). Due to the lack of relative advantage of applying screen protectors, we would expect this behaviour to not be widely adopted. However, as Figure 1 shows, the opposite is the case. Applying screen protectors shows slowly, but increasing interest according to Google Trends.

Relative Advantage	Compatibility	Low Complexity	Observability	Triability	Expected Adoption Speed
✕	■	■	■	■	Moderate

Table 1 Diffusion properties of applying screen protectors. (■ = Given, ○ = Conditionally given, ✕ = Not given)

3.2 Encryption of E-Mails

E-Mail encryption is the only effective countermeasure against passive and active Man-in-the-middle (MitM) attacks. Since E-Mails are inherently insecure, unauthenticated and not confidential, everyone who is involved in sending a mail can read and change the contents. By encryption of the mail, breaches of the mails contents confidentiality can be avoided, and the authenticity and integrity of contents can be ensured. **The risk:** Perceived risks of emails seem to influence user attitudes towards emails only minimal [Ch11]. This is unsurprising given findings whereas a man-in-the-middle, or the risk of confidential information being disclosed to untrusted networks are among the lowest perceived security risks [Tr16]. **The impediment:** The work impediment of encrypting e-mails can be substantial. After all, additional software, configuration, certificate management and credentials are required. This process provides numerous pitfalls for users, which themselves have led to security vulnerabilities in the past [Sh06]. **The countermeasure:** Commercial and non-commercial encryption solutions are not developed with the user experience in mind. Although they can be obtained easily, users must still achieve a certain level of security literacy. For instance in order to use PGP, one must understand the difference between a public and a private key certificate, and how to use the certificate server and its trust evaluations. **Assessing the diffusion:** The *relative advantage* of email encryption largely depends on the perceived risk of a Man-in-the-Middle. However, it seems that this risk is usually not perceived to be a major concern. Therefore, the relative advantage of email encryption seems to be very low. *Compatibility* of the solutions should be low, as processes require additional steps, and additional literacy is required to even use the solutions. Likewise, the *complexity* of encrypting emails is high. The encryption itself however is visible (*Observability*), however, the effects of encrypting emails can never be observed, since the threat is a virtual and non-tangible one. Finally, email encryption requires obtaining additional literacy, installation and configuration of additional tools. These perceivable hurdles stand against the *triability* of encrypting emails.

Relative Advantage	Compatibility	Low Complexity	Observability	Triability	Expected Adoption Speed
×	×	×	×	×	Slow, if at all

Table 2 Diffusion properties of encrypting emails. (■ = Given, ○ = Conditionally given, × = Not given)

3.3 Covering of the device camera

Threats that use the device camera, for instance privacy breaches by Facebook [Go20], or government institutions have been publicly visible through various media reports and the Snowden leaks. Besides of physically deactivating the camera, a possible avoidance tactic for this could be the taping of the devices camera. Hereby a tape is applied, which cannot

be seen through. It renders the camera virtually useless. **The risk:** As to our knowledge there is no study available that measures the perceived risk of being spied on through the device camera. However, there are studies that involve cameras in smart homes which show that users tend to be more aware of their own behaviour, and some even more cautious because they were feeling observed by the cameras in their smart home devices [Ta19]. Therefore, it seems reasonable to assume that the risk of being spied on through the device camera is perceived as a likely and tangible one by individuals. **The impediment:** The camera in devices can be useful for selfies and video conferences. In that case, simply covering the camera would be an impediment, as the cover always has to be removed prior to the selfie, or prior to the conference. On the other hand, there are camera covers available, which can be opened and closed, drastically reducing the possible impediment. **The countermeasure:** Covering the camera is a tangible action, whose consequences can be seen immediately. When the camera is covered, individuals will notice that they only see a dark image when using the camera. Additionally, camera covers are relatively easy to obtain and can be applied without additional security literacy. **Assessing the diffusion:** The relative advantage seems to build on a tangible and perceived risk. However, if the camera is heavily used the impediment of the camera covers can reduce or even eliminate the perceived relative advantage of the solution. Compatibility of the solution is high, since it can be applied without additional steps and to virtually any device camera. The behaviour is easy to understand (low *complexity*), can be observed with others (*Observability*). Finally, because the camera cover is easy to obtain, easy to apply, easy to remove, and its consequences easy to understand, it can be tried out well (*Triability*).

Relative Advantage	Compatibility	Low Complexity	Observability	Triability	Expected Adoption Speed
○	■	■	■	■	Moderate

Table 3 Diffusion properties of covering the device camera. (■ = Given, ○ = Conditionally given, ✕ = Not given)

3.4 Use Single-Sign-On systems

Single sign-on (SSO) system provide the possibility to reduce complexity and ease the use of credentials for users. They are an option to eliminate password reuse [Iv04], and weak passwords [Ne94]. Additionally, they offer the reduction of implementation complexity by standardizing application authentication interfaces, and the automation of access rights and authentication data provisioning and deprovisioning. **The risk:** Single sign-on addresses risks regarding passwords. However, we suspect that these risks are mostly perceived by individuals with a given security literacy. Apart from these, there are no further risks that are addressed by SSO. **The impediment:** The impediment is little, once SSO is available. Using SSO resembles the use of known credentials such as username and passwords. **The countermeasure:** While the technical implementation of SSO is

demanding, users are not necessarily required to obtain further security literacy in order to use SSO. Additionally, every application can, in principle, be integrated with SSO. Even in consumer areas, SSO services provided by Google and Facebook via protocols such as oAuth are available. **Assessing the diffusion:** SSO provides automation capabilities and solves a security risk. However, probably the biggest advantage of SSO lies in the standardization of interfaces and drastical reduction of required authentication procedures. Therefore, we assume that SSO will yield a high perceived *relative advantage*. While the *complexity* of the implementation can be challenging, the complexity of use is not. SSO can leverage already known authentication mechanisms such as username and password. The observability of SSO in terms of reduced authentication steps is observable (*Observability*). And since SSO is available in the consumer branch through Facebook and Google, it can be tried out (*Triability*).

Relative Advantage	Compatibility	Complexity	Observability	Triability	Expected Adoption Speed
■	■	■	■	■	Fast

Table 4 Diffusion properties of using SSO (■ = Given, ○ = Conditionally given, ✕ = Not given)

3.5 Security Behaviours and their diffusion properties

The analysis in the previous Subsections is summarized in the following Table 5. Hereby each behaviour is ranked, based on the Google Trends analysis shown in Figure 1 and Figure 2. The Google Trends analysis clearly shows that SSO has largely increased in interest over the last years, followed by a slower but steady increase in interest in privacy screen protectors (see Figure 1). The interest in camera covers has also steadily increased, although at a much slower pace as in the case of privacy screen protectors. Therefore, it is only visible in Figure 2. Hereby, the interest in camera covers has bypassed the interest in e-mail encryption since 2017, with a notable exception in May 2018 (the year where the European General Data Protection Regulation went into action). Against this, E-Mail encryption has steadily lost interest, since 2004. Notably the interest peaks only shortly in 2013, 2014, and 2018, whereas 2013 and 2014 mark the years of the Snowden revelations. In our opinion it is therefore safe to say, that the interest in E-Mail encryption, despite for short lapses of attention, is constantly decreasing, while the interest in camera covers increases. Additionally, one must take into account that all Trends Analyses are for topics, which comprise multiple search terms on a certain topic. Camera cover is the only search term that is included in the Google Trends Analysis. However, due to the higher specifity of the search term, interest should be lower than that measured for the respective topics. This however is not the case. Table 5 summarizes the diffusion properties of the different security behaviours. The assigned rank reflects the interest in the behaviour, according to Google Trends.

Behaviour	Rel. Adv-	Compatibility	Complexity	Observability	Triability	Rank
Use SSO	■	■	■	■	■	1
Screen protector	✕	■	■	■	■	2
Camera Cover	○	■	■	■	■	3
E-Mail Encryption	✕	✕	✕	✕	✕	4

Table 5 Overview on the diffusion properties of security behaviors (Rel. Adv. = Relative Advantage, ■ = Given, ○ = Conditionally given, ✕ = Not given). The rank orders the behaviours according to the interest in Google Trends with 1 being the highest interest, and 4 being the lowest.

As expected, the perceived relative advantage seems to contribute to the uptake of a behaviour, but not as dominant as for other innovations. The reason is the dependence of perceived relative advantage on perceived risks addressed by the security behaviour.

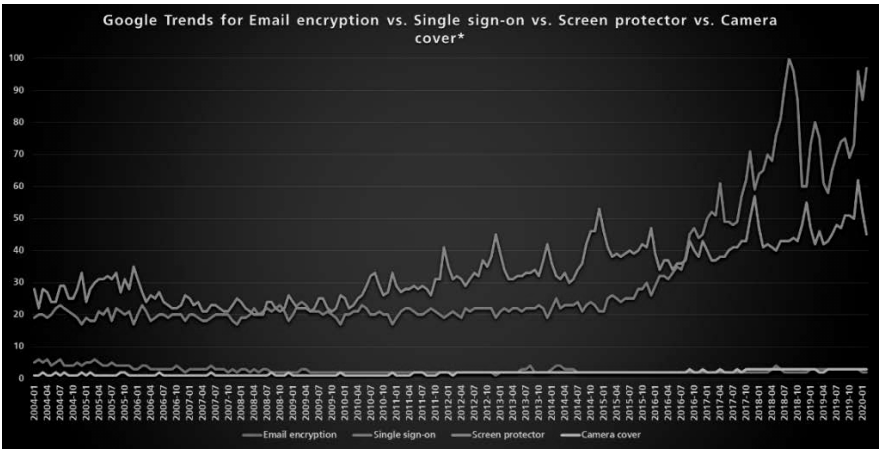


Figure 1 Google Trends for Email encryption, SSO, screen protector and camera cover. Camera cover is the only search term in the comparison, the others are topics

As those risks are often not recognized by users the relative advantage is very low. For privacy screen protectors, we cannot conclude a perceived relative advantage, in light of the relatively low perceived risk of shoulder surfing [Ha14][Tr16]. On the other hand, a relative advantage can only be expected for camera covers, if the camera is not heavily used. As a result, Compatibility, Complexity, Triability, and Observability seem to play a leading role with security behaviours. If a perceived relative advantage is not given individuals may still adopt a security behaviour. However, if it is hard to try out, if its

functions and consequences are not observable, and if it is not compatible with what one knows and does, it will likely fail in the long run, as the case of email encryption.

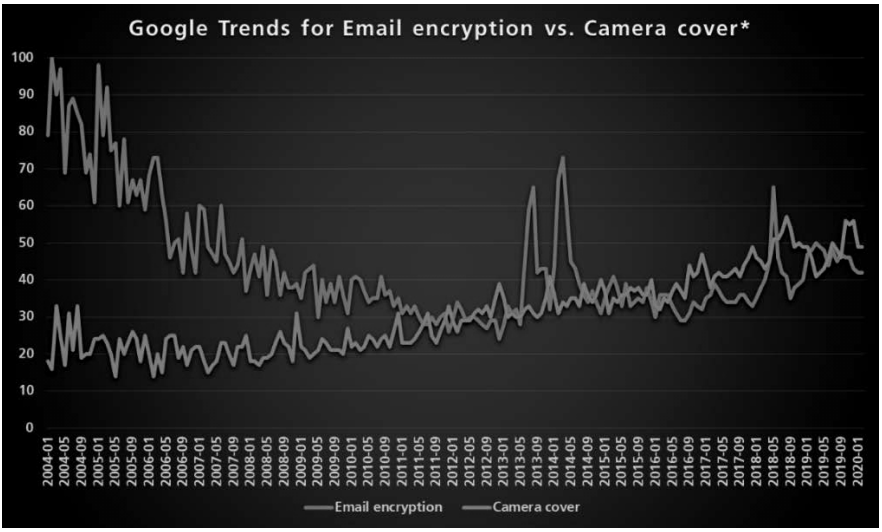


Figure 2 Google Trends for Email encryption and Camera cover. Email encryption is a Google Topic, whereas camera cover is only a search term

Risk on the other hand, does not really seem to play a role in the uptake of security behaviours. Even if a relative advantage could not be attributed to a risk that was actually perceived as a large one by individuals, the behaviour seems to still be interesting, if triability and observability are given, and the complexity of the behaviour is low. In light of the findings of [Kw19] however, this is hardly surprising as they find that awareness and security training only impacts an organizations security marginally.

4 Discussion and Impact

The results clearly show that diffusion theory can provide an explanatory framework for the likelihood of widespread adoption of certain security behaviours, and the absence thereof. It does not provide any insight into how to foster a certain secure behaviour with individuals. But it enables security experts to talk about behaviours which may make sense to include in an organizational policy or campaign, and which are likely to fail. Therefore, these results can provide a lasting impact on how security behaviour is approached in organizations. The findings align well with the observations on the diffusion of preventive innovations [Ro02], where the perceived relative advantage also tends to be generally lower. Rogers therefore proposes marketing the relative advantage of the innovation. However, while this may work well with health interventions, such as [LE00], one has to

be careful when applying this principle to information security. When perceived security risks constitute for an individuals perceived relative advantage, then the constitution is built on a constructed, anticipated event [Lu90] rather than a naturally occurring event such as a health disease. This shows that the epistemological discussion is in principle important for this research topic. In the end of Section 2.1, a discussion of secure behaviour research as research on actual behaviour in light of idealized behaviour was conducted. It led to the point that this kind of research should either focus on the idealized behaviour itself (which is what we did in this contribution), or employ epistemological focuses that do not separate between the idealist, the idea, and the observation (e.g. interpretivism [Wa93]). An important take away from interpretivism however is that quantitative methodologies that rely on the testing of fact rather than on interaction may not be useful after all. With other epistemological focuses that do not reduce the relationship of researcher and research, like phenomenology [Hu09], or constructivism [Lu84], generalizable methodologies and the transfer of knowledge between cases of research subjects itself even are questionable. In this field, the qualitative approach that is provided by diffusion theory is suiting, but not settled. Criticism on diffusion theory [LD01] can basically be reduced to a phenomenological approach or to the employment of radical constructivism. Therefore, this research seems to be on a good path and at least in the short term able to provide insights with value for security professionals on secure behaviour.

5 Limitations

There are several limitations to this contribution. It does not involve any empirical work besides Google Trends analyses. While the absence of quantitative empirical work makes sense due to the reasons laid out in Section 4, the absence of qualitative empirical work does not. We tried to scrutinize the different security behaviours as comprehensible as possible but the analysis drawn only represents our personal view. Google Trends is of course itself a biased research mechanism. It only measures queries by Google and not actual behaviours. Therefore, it can only provide an indication of the diffusion of a security behaviour under the assumption that individuals will inform themselves via Google about the behaviour. And especially with encrypting emails, the behaviour may be common knowledge. But then privacy screen protectors have been around nearly as long as email encryption. And for instance PGP, which has been around for around 30 years, still is "only" a niche product. Additionally, Google is the leading search engine around. Therefore, we believe the indications from Google Trends to be useful data in the context of this research.

6 Conclusion

By separating the idealized security behaviour, from the behaving individual we were able to provide an insight into why certain security behaviours are successful, while others are not. This research shows that the diffusion of innovations theory provides a framework

that enables a discussion and anticipation of the success of different security behaviours. As relative advantage is often rather small, it alone does not provide a safe bet, but seems to enhance the adoption of a behaviour. Necessary factors for a security behaviour to be successful however are the compatibility, triability and observability of the security behaviour. Risk does not seem to play major role in the uptake of security behaviours, which aligns well with the findings of [Kw19]. Of course, this research is limited regarding its use of informed arguments, and its reduction of the idealized security behaviours towards the adoption factors of diffusion theory. The use of Google Trends, while providing a good indication can also not be regarded as satisfyingly settling information on the adoption of security behaviours. Future research will employ qualitative methods in order to research best and worst cases of security behaviours in organizations to test the diffusion of theory framework. More scrutiny can be put into the cases of security behaviour, taking into account the environment and stakeholders that a security behaviour may involve, by employing perception-critical epistemological focuses such as interpretivism or radical constructivism.

Bibliography

[Bo15] Boss, S. et al.: What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. (2015).

[Bu10] Bulgurcu, B. et al.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. Management Information Systems Quarterly. 34, 3, 523–548 (2010).

[Ch11] Chen, R. et al.: An investigation of email processing from a risky decision making perspective. Decision Support Systems. 52, 1, 73–81 (2011).

[Da89] Davis, F.D.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. Management Information Systems Quarterly (MISQ). 13, 3, 319–340 (1989).

[Go20] Goud, N.: Facebook to spy through your Webcam or Phone, https://www.cybersecurity-insiders.com/facebook-to-spy-through-your-webcam-or-phone/, (2020).

[GY12] Guo, K.H., Yuan, Y.: The effects of multilevel sanctions on information security violations: A mediating model. Information & Management. 49, 6, 320–326 (2012).

[Ha14] Harbach, M. et al.: It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In: 10th Symposium On Usable Privacy and Security (${$SOUPS$}$ 2014). pp. 213–230 (2014).

[Hü10] Hühnlein, D. et al.: Diffusion of Federated Identity Management. In: Freiling, F.C. (ed.) Sicherheit 2010. pp. 25–36 Köllen Druck + Verlag GmbH, Bonn (2010).

[Hu09] Husserl, E.: Philosophie als strenge Wissenschaft. Felix Meiner Verlag (2009).

[If16] Ifinedo, P.: Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines? Information Systems Management. 33, 1, 30–41 (2016). https://doi.org/10.1080/10580530.2015.1117868.

[Iv04] Ives, B. et al.: The Domino Effect of Password Reuse. Communications of the ACM. 47, 4, 75–78 (2004).

[Jo16] Johnston, A.C. a et al.: Dispositional and situational factors: Influences on information security policy violations. European Journal of Information Systems. 25, 3, 231–251 (2016). https://doi.org/10.1057/ejis.2015.15.

[Ka13] Kajtazi, M. a et al.: Assessing self-justification as an antecedent of noncompliance with information security policies. In: Proceedings of the 24th Australasian Conference on Information Systems. (2013).

[Ku19] Kurowski, S.: Response Biases in Policy Compliance Research. Information & Computer Security, Vol. ahead-of-print No. ahead-of-print. (2019). https://doi.org/10.1108/ICS-02-2019-0025

[Kw19] Kweon, E. et al.: The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. Inf Syst Front. (2019). https://doi.org/10.1007/s10796-019-09977-z.

[Li14] Li, H. a et al.: Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. Information Systems Journal. 24, 6, 479–502. https://doi.org/10.1111/isj.12037 (2014).

[LE00] Lock, C. A., Kaner, FS. E.: Use of marketing to disseminate brief alcohol intervention to general practitioners: promoting health care interventions to health promoters. Journal of evaluation in clinical practice. 6, 4, 354-357 (2000).

[Li00] Litfin, T.: Adoptionsfaktoren: Empirische Analyse am Beispiel eines innovativen Telekommunikationsdienstes. DUV, Wiesbaden (2000).

[Lo11] Long, J.: No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress (2011).

[Lu84] Luhmann, N.: Soziale systeme. Suhrkamp Frankfurt am Main (1984).

[Lu90] Luhmann, N.: Technology, environment and social risk: a systems perspective. Organization & Environment. 4, 3, 223-231 (1990).

[LD01] Lyytinen, K., Damsgaard, J.: What's wrong with the diffusion of innovation theory? In: Working conference on diffusing software product and process innovations. pp. 173–190 Springer (2001).

[Ne94] Neumann, P.G.: Risks of Passwords. Communications of the ACM. 37, 4, 126 (1994).

[Po15] Posey, C. a et al.: The impact of organizational commitment on insiders motivation to protect organizational information assets. Journal of Management Information Systems. 32, 4, 179–214 (2015). https://doi.org/10.1080/07421222.2015.1138374.

[PH14] Putri, F., Hovav, A.: Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. In: ECIS 2014 Proceedings - 22nd European Conference on Information Systems. (2014).

[Rh09] Rhee, H.-S. et al.: Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security. 28, 8, 816–826 (2009).

[Ro03] Rogers, E.M.: Diffusion of Innovations. Free Press, New York (2003).

[Ro02] Rogers, E.M.: Diffusion of preventive innovations. Addictive behaviors 27, 6, 989-993 (2002).

[Ro06] Roßnagel, H.: On Diffusion and Confusion: Why Electronic Signatures Have Failed. Trust and Privacy in Digital Business. 71–80 (2006).

[Ro10] Roßnagel, H.: The Market Failure of Anonymity Services. In: IFIP. pp. 340–354 (2010).

[RZ12] Roßnagel, H., Zibuschka, J.: eID in Leisure Time Activities: Results from the SSEDIC Stakeholder Consultations in the Leisure Sector, (2012).

[Sa15] Safa, N.S. a et al.: Information security conscious care behaviour formation in organizations. Computers and Security. 53, 65–78 (2015). https://doi.org/10.1016/j.cose.2015.05.012.

[Sh06] Sheng, S. et al.: Why johnny still can't encrypt: evaluating the usability of email encryption software. In: Symposium On Usable Privacy and Security. (2006).

[Si14] Siponen, M. a et al.: Employees' adherence to information security policies: An exploratory field study. Information and Management. 51, 2, 217–224 (2014). https://doi.org/10.1016/j.im.2013.08.006.

[So15a] Sommestad, T. et al.: A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. International Journal of Information Security and Privacy (IJISP). 9, 1, 26–46 (2015).

[So15b] Sommestad, T. et al.: The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information and Computer Security. 23, 2, 200–217 (2015). https://doi.org/10.1108/ICS-04-2014-0025.

[So14] Sommestad, T. et al.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Information Management & Computer Security. 22, 1, 42–75 (2014).

[Ta19] Tabassum, M. et al.: " I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In: Fifteenth Symposium on Usable Privacy and Security (${$SOUPS$}$ 2019). (2019).

[Tr16] Trewin, S. et al.: Perceptions of risk in mobile transaction. In: 2016 IEEE Security and Privacy Workshops (SPW). pp. 214–223 IEEE (2016).

[VS12] Vance, A. a, Siponen, M. b: IS security policy violations: A rational choice perspective. Journal of Organizational and End User Computing. 24, 1, 21–41 (2012). https://doi.org/10.4018/joeuc.2012010102.

[Wa93] Walsham, G.: Interpreting information systems in organizations. John Wiley & Sons, Inc. (1993).

Privacy and availability needs regarding user preferences for Smart Availability Assistant – towards a digitally enabled work life balance

Zofia Saternus [1]

Abstract: The use of communication technologies (CTs) enables blurring the traditional boundaries between work and private life. Many employers are worried about this situation and addressed those issues with different technological and organizational approaches. The goal of our research is to introduce improved enterprise availability management by developing an employee-friendly technological solution that actually reflects the variety of employees' availability needs. Due to the overall aim of broadening and bridging research on an availability management, results of a quantitative study (N=821) insights into the management of individuals' availability and key requirements regarding the development of a Smart Availability Assistant. In general, it became apparent that to appropriately design this kind of smart assistant we must not only recognize the heterogeneity of peoples' availability preferences but also identify and meet employees' privacy expectations by use of a Smart Availability Assistant.

Keywords: availability management, smart assistant, information privacy, privacy concerns

1 Introduction

Over the last twenty years, the presence and usage of information and communication technologies (ICTs) changed from selective to ubiquitous, transforming both private and professional environments. It became imperative for most individuals to permanently engage with these technologies to accomplish work tasks efficiently [AGP11]. A constant connection to work enabled by modern communication technologies allows employees to stay connected with their job anywhere and anytime (Diaz et al. 2012). In fact, the results of surveys among employees are disturbing: 64% of knowledge workers in Germany indicated to be available for their boss, collogues or clients even during holidays [Bi18]. Moreover, 40% of European employees commonly get work-related requests outside their regular working hours [AN13].

The emerging and pervasive proliferation of ICTs in the workplace has led to extensive research, especially in the fields of information systems (IS) and organizational behavior (OB). Scholars indicate both positive and damaging outcomes of ICT-enabled availability [BO07], [Sc17]. On one hand, ICT usage elicits flexibility and autonomy due to increased control and possibilities to work beyond the traditional boundaries of the workplace and workday [Di12]. Previously prevalent confines of the traditional office space or work time in fact disappear. Therefore, employees' ability to appropriately manage work-life demands [To06] as well as work satisfaction and productivity are positively affected [MC06]. On the other hand, researchers regularly underline also

[1] Goethe University Frankfurt, Chair of Information Systems and Information Management, Theodor-W.-Adorno-Platz 4, 60629 Frankfurt am Main, saternus@wiwi.uni-frankfurt.de

harmful effects of ICT usage, mostly regarding emotional and mental capacities of employees [BMG11], [SPK19]. Extensive organizational ICT interaction is found to be a driver for increased stress levels, in IS literature referred to as technostress [AGP11], [TTR17], and partially for decreased work productivity due to technology overload [KL10], which can cause even health issues like burnout [Ba11], [Ra08], [DB12]. Moreover, enhanced flexibility and autonomy of the individual are accompanied by increased expectations from managers and colleagues to be almost constantly available for work due to an "always on" culture, which has evolved in many organizations over the last years [Sc17]. Keeping up with these expectations may result in greater workloads and encroachment on family and private time [To06].

Employee problems become company problems. Over the last few years, labor and union representatives as well as politicians started to address the ICT-enabled constant availability and its potential detrimental outcomes for workers. Several businesses are taking the initiative in this regard by integrating either resolute technological approaches or tightened availability policies. For instance, automobile manufacturers pioneer limited availability, e.g. automatically blocking incoming e-mails and messages after the employee's regular working hours (from 6.15 pm until 7.00 am) by switching off the e-mail servers [Ha11] or by deleting all incoming e-mails while employees are on holiday [Da14]. Similarly, political awareness about employees' availability problem is increasing. Under pressure from trade unions, France has introduced a labor law, that is supposed to guarantee employees the "right to disconnect" from work-related e-mails and calls [TG16].

Basically, all these solutions can restrict the usage of smartphones and computers by blocking calls, messages, and e-mail notifications only for a specified period of time. However, the effectiveness of these solutions to improve work-life balance varies across segments of employees, because they do not map the complexity of the individuals' availability preferences [Sc17]. It becomes clear, that a more sophisticated availability management is needed. In this context, we aim at the development of a Smart Availability Assistant (SAA), that will reflect the complexity and variety of peoples' availability needs. Despite potential benefits, smart assistants in form of a mobile app raise several security and privacy challenges for consumers. Mobile apps often transmit a large amount of personal data in real time, rendering strong potential for privacy intrusion [FT09]. In the case of a data breach an adversary could access users' detailed SAA usage history and potentially additional information about the employees' lifestyle, availability behavioral patterns, location, personal identity, and daily behavior [CL18], [Do18]. Recent headlines have highlighted this potential risk by reporting cases, where vendors and app developers are indeed collecting personal data through users' smartphones and transmitting them to other entities [Xu12]. These practices of data access and transmission employed by operating systems have aggravated privacy concerns among users. Accordingly, Bélanger and Crossler [BC11] stated that "one area of future research that seems likely to gain importance is the balancing of information privacy concerns with the advantages of location-based services". For this reason, in this paper we present the results of a quantitative study of users' preferences for a Smart

Availability Assistant through the lens of privacy challenges and employees' privacy concerns. Through a user study with 821 participants we point out important desires, demands and influencing factors for acceptance and use of this technological solution tool.

2 Research and Theoretical Background

2.1 Research Background

Considering the paradoxical character of ICT [JL05], we assure that, while mobile communication technologies can cause, that the work-private boundary regularly becomes blurred and unclear, they should also be used as a tool for managing the work-non-work boundary [KHS09], [GG07]. In fact, a number of papers emphasize the agency of ICTs' use in managing work-family boundaries. For example, Golden and Geisler's [GG07] research on ICTs' usage among knowledge workers in the USA provides few detailed insights into how these employees could use them in different ways to support the particular styles of work-private boundary they preferred. Moreover, a field study among 31 professional workers from Germany, which use a special application Availability-Monitor, indicates, that assistance systems may contribute to an improvement of users' work-life balance and a reduced exhaustion and stress level [Sc17]. The goal of our research is to introduce an enterprise availability assistant that actually reflects the complexity and variety of the individuals' availability preferences. According to the underlying concept (see Fig. 1), the assistant analyses incoming communication requests in order to delay or block undesired e-mails, phone calls, and text messages for a specified time period in a smart way. The decision whether to block, delay or let trough the delivery of calls and messages will be based on the analysis of its content and further information about the individuals' availability preferences, like the users' current life domain, location data and time as well as from the type of contact and its defined priority [LR17].

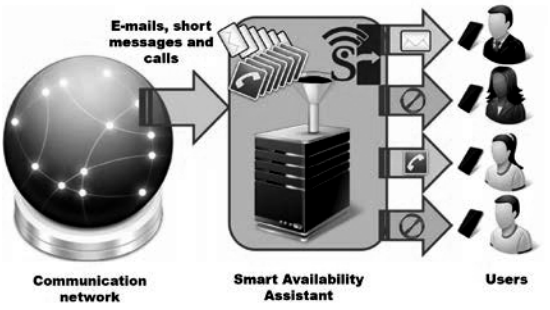


Fig. 1: General overview of system functionality [LR17]

Indeed, previous studies have provided valuable initial insights about the use of ICT for cross-border communication and availability management. They have not, to the authors' best knowledge, investigated the cross-border communication, availability needs and employees' privacy concerns regarding the use of an availability app. To address this research gap, we asked the following research question: How do employees from different fields manage their cross-border communication, what are their availability needs, how can digital assistants support them in order to fully harmonize their actual availability and what are their privacy preferences regarding the SAA?

2.2 Theoretical Background

We define the objectives of the solution by analyzing the data gained from a qualitative study [SR18] and drawing on the boundary theory [Ni96], [AKF00], [KL12] as our main theoretical framework. The boundary theory defines how humans create boundaries considering their diverse life domains. In this regard, research suggests that employees can be grouped into five dominant work-life boundary management styles (separators, family firsters, cyclers, work firsters and integrators) and that the life contexts and values of each individual lead to different desired levels of availability and thus to different boundary management styles [Ko16]. Separators tend to mainly keep work and private lives separated in defined blocks of time and to strongly focus on each performed role with few interruptions from the other. In contrary, integrators constantly blend or merge work and private lives due to a high degree of cross-role interruptions, e.g. voluntarily checking work-related e-mails at home while also responding to personal calls or text messages throughout the workday. Cyclers are neither of the previous pure styles. In fact, cyclers practice a more fluctuating style in which they switch back and forth between cycles of high work-life integration and periods of complete separation. These situations are often caused by habitual peak work times such as deadlines for construction works for builders or emergencies for medical staff. However, in times of higher work-life integration, cyclers focus more on private contacts they did not have sufficient time for during peak work periods. Lastly, work firsters and private life firsters have dominant role identities, that are prioritized. They respond to interruptions asymmetrically, i.e. in one direction but not the other. Whether work or private life is prioritized depends on the person's preferences [Cl00], [Ko16].

In this study we adopt the Technology Acceptance Model (TAM) and its extensions inform the current study's exploration of the factors that affect SAA adoption. According to the original model [Da89], users' attitudes toward technology use determine their behavioral intentions, which directly influence the individuals' final use or rejection of the technology. In TAM, attitudes toward technology use are influenced by two personal beliefs: perceived ease of use and perceived usefulness. However, TAM falls short in recognizing how external contextual factors inform technology acceptance [Ba07]. In response, the Unified Theory of Acceptance and Use of Technology (UTAUT) [Ve03] suggests that three key constructs drive behavioral intentions to use the technology: performance expectancy (the perceived usefulness of the system), effort

expectancy (the perceived ease of use), and social influence (to what degree an individual perceives, that important others believe he or she should use the system) [Li19]. Consequently, this research provides an opportunity to apply and extend technology acceptance frameworks by investigating privacy as determinant of availability management's acceptance and use.

3 Research Method

The data for this study was collected using a cross-sectional survey design with a sample of knowledge workers. Knowledge workers are employees whose main capital is knowledge [Re11]. As mobile technology use represents a central part of their work [WBB08], we consider knowledge workers as a particularly relevant sample. The completion of the survey took 25 minutes on average.

3.1 Participants

The questionnaire was opened for almost 1,600 times and yielded a response rate of 54%. In total, a great number of 864 surveys were completed. However, data cleansing excluded some answers of participants, who unrealistically completed the survey e.g. in less than 10 minutes, which leads to the final sample of N=821. The invitations for participation were sent using traditional digital communication like e-mail and some messaging applications: WhatsApp, Messenger, Skype. Also public posts on social media platforms spread the questionnaire as widely as possible. The sample consisted of participants, who are employed in 30 different countries, but mainly in Germany (85%), Poland (4%), Romania (2%), the USA (2%) and Italy (1%). The average age of the respondents was 34,6 years (SD = 12 years) with a quite equal division of participants on gender – 49.6% women (N=408) and 50.4% men (N=413). Participants work for employers of different sizes and diverse industry sectors (e.g., information technology, consulting and finance), which creates a broad perspective regarding stakeholders' preferences towards the SAA. In their current position, 31% of participants exhibit leadership responsibility. The weekly work time according to employment contract was between 31 and 40 hours (61%). Because we wish to include only persons with a certain degree of current work experience, the pool of participants is limited to employed knowledge workers with at least 20 working hours per week [SSH 19].

3.2 Questionnaire Design

The survey contains of 87 questions divided into 4 thematic blocks. The first part collects demographic data, the second part deals with the participant's current employment, the third part covers the research questions about availability behaviors and preferences and the fourth part comprises the user's preferences towards the use, design and development of a SAA.

4 Results Findings

Due to the privacy focus of this paper, we will only shortly describe the general findings of the study, whereas concentrate in detail on the privacy challenges.

According to the employment contract, most participants (61%) work from 31 to 40 hours per week. In comparison, the actual work time appears to be longer, more than 50% of participants work in average more than according to their employment contract.

In addition, the participants were asked about their attitudes towards and experiences with work-related matters in their spare time; opinions are divided. On the one hand, 30.8% of the participants advocate the constant availability for work even though three-fourths of them feel stressed about it. On the other hand, 39.6% of the participants generally do not want to be available for work-related matters in their spare time.

The attitudes towards the separation and integration of work and private life vary among individuals. Most of the participant desire either a complete separation (37.3%) or an interactive integration (35.7%) of work and private life. However, the desired states of availability often differ from the actual states. For instance, every fifth participant (19.7%) currently has work-related interruptions in their private life, whereas only 3.8% of participants really desire it. Overall, the mismatch between actual and desired availability (calculated by comparing the participant's indicated actual availability with his or her desired availability) is substantial: Every second participant (50.3%) does not achieve his or her desired level of availability in actual practice. Moreover, half of the participants (50.2%) actually do not have any clear arrangement, that clarifies one's availability. In terms of work-related e-mails and text messages, behaviors are somewhat heterogeneous. Half of the participants (46.7%) check and read incoming e-mails in their spare time where even four-fifths of those participants (79.4%) usually reply. In the end, of those participants, that also reply to work-related messages, the vast majority of the participants (87.3%) is doing so, because otherwise they would not be able to successfully manage their workload.

The results above demonstrate a need for availability management. Analyzing the participants' preferences towards potential functions of a SAA, the introduction of certain default modes was mainly supported. In detail, most participants considered the following settings to be useful: The user can only be contacted in an emergency (76.9%), the user can only be contacted by a specific group of people or topic of issue (73.9%), the user can only be contacted by text message (71.2%), the user is not available at all (62.3%) or the user can only be contacted via phone call (49.1%).

Moreover, most participants (73.4%) consider it useful to be able to rate the decisions of the assistant so that it can learn from these evaluations and deduce enhanced future decisions. In contrast, only a narrow majority of the participants (54.1%) want the SAA to interpret the content of a message automatically in order to assess its urgency.

Regarding reliability of the SAA, we asked three questions to recognize how the SAA

should decides regarding the availability management: “Based on my settings, the availability assistant should be able...”. Most participants (60.8%) consider it useful or very useful “to make suggestions for a change of the availability setting” (M=4.91; SD=1.82). Considerably fewer participants (44.2%) rated it as useful “…to change the availability setting independently and to be informed by message” (M=4.09; SD=2.11). The less desired option (21.5%) was “…to change the availability setting independently without my information”, (M=2.77; SD=2.04). The respondents are selected from a seven-point Linkert scale from 1 (not useful at all) to 7 (very useful).

In case a message gets delayed or a phone call gets blocked, participants predominantly consider it useful that the assistant gives a feedback to the sender. To understand which information users want to reveal, we asked three questions: “The availability assistant should be able to inform the sender of a delayed message or a rejected call about...”. Most participants (87.1%) would like to inform the sender about “...when I can be reached again” (M=6.08; SD=1.39). The option “…how I can be reached alternatively” (M=4.08; SD=2.04) were less desired (61.3%), same as “…why I cannot be reached at the moment” (M=4.70; SD=2.12) (59.8%). Our respondents chose along a seven-point Linkert scale from 1 (not useful at all) to 7 (very useful). Interestingly, in this context, most participants do not differentiate between the specific groups of senders: The notification about the user’s unavailability is considered useful similarly for the employer or supervisor (76%), colleagues (67.4%), and customers (70.7%).

Regarding the person, which defines the settings for a SAA, our participants showed high desire for self-determination. We asked “In your opinion, who should define the default settings for the availability assistant - for example, when and for whom you are available as a user? (Multiple answers are selectable)”. Clearly, the most of our participants chose “I as a user myself” (78.8%), the second most desirable option was “I and the team I work with” (43.0%), 18.51% respondents responded “My employer/superior” and only 8.89% would like the SAA settings to be defined by “The employee council”.

We observed the same trend in regard to the question “Who do you think should be able to review the settings that your personal availability assistant contains? (Multiple answers are selectable)”. 91.35% chose the answer “I as a user myself“, 25.58% responded “The system administrator”, 25.46% replied “The (team) colleagues”, 25.09% selected “The employer / supervisor”, 14.06% answered “The head of department”, and only 8.89% would like, that “The workers council” reviews the SAA’s settings.

Moreover, the responders clearly desire an availability arrangement within the usage of a SAA. To the question “In your opinion, how should the use of an availability assistant be regulated with your employer”, the majority (70.77%) answered “Through a works agreement”. The option “Through a company practice” was less desired (23.63%).

The tendency for a self-determination and participant’s wish for independent control and privacy of the personal availability settings were also showed through answers to the question “Where should the settings, your personal availability assistant contains, be

saved?". 72.59% of the participants chose the option "On the device".

To sum up, the usage of a software to regulate availability is considered useful or very useful by most participants (55.9%), while, in contrast, few participants (21.1%) consider it not useful. When asked how likely it is for the participant to personally use such a software, the tendencies are somewhat evenly distributed. A great number of participants indicated a high likelihood (36%) or a moderate likelihood (27.5%), while 36.5% of our participants show a low likelihood to use the SAA. For the 300 respondents, who said, that they would not use SAA, we asked them to select factors that may have played a role in their decision. The factors most often cited by these respondents reflected concerns about utility and privacy. They included: "In my professional context there is no need for availability management" (61.0%), "I believe that better availability management cannot be achieved by using a software" (31.0%), "I have privacy/security concerns about these features" (17.67%). In addition, participants provided open-ended responses to the question, "What is the main reason you don't use a SAA?" The vast majority of responses reflected classical constructs in TAM and UTAUT with many revealing low performance expectancy (i.e. low perceived usefulness) associated with SAA usage. For example, "I can regulate my availability well without software", "In my spare time I have a choice not to log into my e-mails or turn off the phone". A second cluster of responses suggested a high effort expectancy (i.e. "Availability software still has too many open questions for me", "One app more, no thanks". Finally, social influence played a role for participants' decision not to use a SAA with one respondent noting "It is all about the culture and behaviors".

5 Discussion and Conclusion

The future of work has become one of the trendiest buzzwords in today's business world. Politicians, employers and workers alike need to find answers to the coming challenges of combining automation with human work, enhancing the physical world with capabilities offered by digital technologies, and finding the most effective balance between work and private life as well as individual availability management. In this context, the present study adds to the current academic knowledge and provides valuable insights into the successful management of individuals' availability as well as preferences regarding availability applications through the lens of privacy challenges and employees' privacy concerns.

The quantitative study we conducted shows very clear, that the potential users have high desire for self-determination regarding the arrangement of SAA' settings. Nearly unanimously our participants opted that only the user self should determine the settings of the SAA and only the user self should have an access into the personal settings. Moreover, in the extension of boundary theory [Ko16] our study results provide valuable insights into how employees abstract their individual boundary style and translate it into tangible availability preferences. The results clearly show, that there is no fixed model

regarding the attitudes towards the separation and integration of work and private life. Moreover, the preferences are changing within the life domain and time. Consequently, lack of flexibility and self-determination seem to be a principal reason why existing approaches, like blocking or deleting automatically incoming e-mails and messages after the employee's regular working hours [Ha11], [Da14] do not meet facets of employees' availability needs. Moreover, the findings of the study reveal, that the potential users would like to have a right to inspect the SAA's decision regarding the availability management. Although, the majority of the participants declare, that SAA should be able to learn from user's availability behaviors, only around 21% would allow the SAA to change the availability setting independently. Interestingly, there is also a clear tendency which information should be reveals in the feedback to a sender in case a message gets delayed. Participants predominantly consider it useful that the assistant informs the sender when the user can be reached again (87.1%). The information "how instead" and "why" the user is not available are much less desired.

On the one hand, the quantitative study we conducted shows an alarming reality that every second knowledge worker does not achieve the individually desired availability, precisely 50.3% of the participants do not achieve the desired level of availability in the actual workplace. Moreover, in the extension of boundary theory [Ko16], [KHS09] our study results provide valuable insights into how employees abstract their individual boundary style and translate it into availability preferences. The results clearly show, that there is no fixed model regarding the attitudes towards the separation and integration of work and private life. Most of the participant desire either a complete separation 37.3% or an interactive integration 35.7% of work and private life. Individuals vary in their availability preferences regarding their life domain, context and contact, meaning that the work and private life boundary is shaped through an individual's day-to-day decisions, needs and obligations.

On the other hand, the results indicate, that the technological solution, which allows differentiated adaptive management has the potential to contribute to individuals' well-being. Practice indicates, that actual employers do not respond adequately to the diverse needs of their employees, since present solutions concentrate only on regulating the extent of availability. In this context, there is a need for a technological solution, that will reflect the diversity and complexity of peoples' availability preferences. Under those circumstances, the SAA shows great potential in successfully managing and regulating individual availability, as it supports users' flexibility and autonomy. Specifically, the majority of study participants 55.9% validate the underlying concept of the SAA by perceiving it as useful and declaring to eventually use it. Furthermore, our analysis demonstrates that this kind of assistant will support particularly employees with a mismatch between their actual and preferred boundary style, leadership responsibilities, from large companies and/or those who receive work-related calls during their spare time. Differently, the results indicate, that older employees are less likely to adopt this technological solution. It shows the need for more information and awareness regarding smart availability management, as well as training concepts for employees.

Potential limitations of this study relate to the study participants as well as the form of our questionnaire. First and foremost, the sample profile might not result in entirely universal conclusions, i.e. the study only considered knowledge workers in an organizational context. However, availability issues affect individuals from all backgrounds as well as the scope of a SAA could go far beyond such specific context. By the same token, most participants of the study live and work in Germany 85% (697) thus complicating international comparisons. Moreover, as is the case with most work–life and organizational behavior research, our study relies on cross-sectional, self-report data and is thus subject to common method variance [PM03]. In designing this study, we followed recommendations described by Conway and Lance [CL10] to reduce the likelihood of common method variance biasing results. Finally, the depth of the study's research questions resulted in an extensive and exhausting questionnaire: On average, it took the participant 20 to 30 minutes to complete it. Therefore, it is conceivable, that with increasing processing time particularly the final questions have received less attention, so that in the end, the results might be slightly distorted.

Given these points, forthcoming research is also invited to extend our study. So far, the usage and preferences regarding SAA have been discussed only on a theoretical level. However, it would be useful to understand and closely measure what effects can actually be observed in practice using SAA, i.e. how much of the potential benefit can be realized and to what extent the technical solution can help to solve availability issues. Moreover, future researchers should take a more inductive approach to identify consumers' privacy expectations. Understanding the factors that drive mutually beneficial and sustainable privacy norms is also important for service providers to best meet the privacy expectations of users and maintain the social contract proven essential for continued adoption of such devices. For this purpose, we suggest a long-term study that could evaluate an availability assistant, that effectively supports employees in managing their availability in line with their individual availability and privacy preferences.

Bibliography

[AGP11] Ayyagari, R., V. Grover and R. Purvis (2011). "Technostress: TechnologicalAntecedents and Implications," *MIS Quarterly* 35 (4), 831-858.

[AKF00] Ashforth, B. E., G. E. Kreiner and M. Fugate (2000). "All in a Day's Work: Boundaries and Micro Role Transitions." *Academy of Management Re*view 25 (3), 472-491.

[AN13] Arlinghaus, A. and F. Nachreiner (2013). „When work calls-associations between being contacted outside of regular working hours for work-related matters and health." *Chronobiology International* 30 (9), 1197-1202.

[Ba07] Bagozzi, R.P.: The legacy of the technology acceptance model and a proposal for a paradigm shift. J. Assoc. Inf. Syst. 8, 4, 3 (2007).

[BC11] Bélanger, F., and Crossler, R.E. 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," MIS Quarterly (35:4), pp 1017-1041.

[Bi18] Bitkom (2018). *Web-Meeting am Strand: Zwei von drei Berufstätigen sind im Urlaub erreichbar*. URL: https://www.bitkom.org/Presse/Presseinformation/Web-Meeting-am-Strand-Zwei-von-drei-

Berufstaetigen-sind-im-Urlaub-erreichbar.html (visited on 17/11/2018).

[BMG11] Barley, S. R., D. E. Meyerson and S. Grodal (2011). "E-mail as a Source and Symbol of Stress." *Organization Science* 22 (4), 887-906.

[BO07] Boswell, W. R. and J. B. Olson-Buchanan (2007). "The Use of Communication Technologies After Hours: The Role of Work Attitudes and Work-Life Conflict." *Journal of Management* 33 (4), 592-610.

[Cl00] Clark, S. C. (2002). "Communicating across the work/home border." *Community, Work & Family* 5, 23-48.

[CL10] Conway J, Lance C (2010) What reviewers should expect from authors regarding common method bias in organizational research. Journal of Business and Psychology 25(3):325-334.

[CL18] Chung, H., Lee, S.: Intelligent virtual assistant knows your life. CoRRabs/1803.00466 (2018).

[Da14] Daimler AG (2014). *Daimler Mitarbeiter können im Urlaub eingehende E-mails löschen lassen*. URL: http://media.daimler.com/marsMediaSite/de/instance/ko/ Daimler-Mitarbeiter-koennen-im-Urlaub-eingehende-E-mails-loeschen-lassen.xhtml?oid=9919305 (visited on 17/11/2019).

[Da89] Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 319–340 (1989).

[DB12] Derks D, Bakker AB (2012) Smartphone use, work-home interference and burnout: a diary study on the role of recovery.Applied Psychology: An International Review 63, 411-440

[Di12] Diaz, I., D. S. Chiaburu, R. D. Zimmerman and W. R. Boswell (2012). "Communication Technology: Pros and Cons of Constant Connection to Work." *Journal of Vocational Behavior* 80 (2), 500-508.

[Do18] Dorai, G. et al.: I know what you did last summer: Your smart home Internet of Things and your iPhone forensically ratting you out. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. pp. 49:1–49:10 ACM, New York, NY, USA (2018).

[FT09] FTC. 2009. "Beyond Voice: Mapping the Mobile Marketplace." from www.ftc.gov/opa/2009/04/mobilerpt.shtm (visited on 17/11/2019).

[GG07] Golden, A. G. and C. Geisler (2007). "Work–life boundary management and the personal digital assistant." *Human Relations* 60 (3), 519-551.

[Ha11] Handelsblatt.com (2011). *Keine E-mails mehr nach Feierabend*. URL: http://www.handelsblatt.com/unternehmen/industrie/volkswagen-keine-e-mails-mehr-nach-feierabend/5992370.html (visited on 17/11/2019).

[JL05] Jarvenpaa, S. and Lang, K. (2005). "Managing the paradoxes of mobile technology." *Ubiquitous Computing*, 7−23.

[KHS09] Kreiner, G. E., E. C. Hollensbe and M. L. Sheep (2009). "Balancing borders and bridges: Negotiating the work-home interface via boundary work tactics." *Academy of Management Journal* 52, 704.

[KL12] Kossek, E. E. and B. A. Lautsch, (2012). "Work-Family Boundary Management Styles in Organizations: Cross-Level Model." *Organizational Psychology Review* 2 (2), 152-171.

[Ko16] Kossek, E. E. (2016). "Managing work-life boundaries." *Organisational Dynamics* 45, 258-270.

[Li19] Liao, Yuting et al. "Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption." iConference (2019).

[LR17] Laufs, U., and H. Roßnagel (2017). "Towards a smart assistant for enterprise availability management:" In: Frisch, Lothar (Ed.) et al.: *Open Identity Summit 2017*: Karlstad, (GI-Edition 277), 175-180.

[MC06] Middleton, C. A. and W. Cukier (2006). "Is Mobile Email Functional or Dysfunctional? Two Perspectives on Mobile Email Usage." *European Journal of Information Systems* 15 (3), 252-260.

[Ni96] Nippert-Eng, C. (1996). "The Classification of 'Home' and 'Work'." *Sociological Forum* 11 (3), 563-582.

[PM03] Podsakoff, P. M., S. B. MacKenzie, J. Y. Lee and N. P. Podsakoff (2003). “Common method biases in behavioral research: A critical review of the literature and recommended remedies.” *Journal of Applied Psychology* 88 (5), 879-903.

[Ra08] Ragu-Nathan, T. S., M. Tarafdar, B. S. Ragu-Nathan and Q. Tu (2008). “The consequences of technostress for end users in organizations: Conceptual development and empirical validation.” *Information Systems Research* 19 (4), 417-433.

[Re11] Reinhardt, W., B. Schmidt, P. Sloep and H. Drachsler (2011). “Knowledge Worker Roles and Actions – Results of Two Empirical Studies.” *Knowledge and Process Management* 18 (3), 150–174.

[Sc17] Schneider, K., K. Reinke, G. Gerlach, C. Anderson, S. Wojtek, S. Neitzel, R. Dwarakanath, D. Boehnstedt and R. Stock (2017). “Aligning ICT-enabled Availability and Individual Availability Preferences: Design and Evaluation of Availability Management Applications.” In: *Proceedings of the International Conference on Information Systems 2017*, Seoul, South Korea.

[SPK19] Salo M, Pirkkalainen H, Koskelainen T (2019) Technostress and Social Networking Services: Explaining Users’ Concentration, Sleep, Identity, and Social Relation Problems. Information Systems Journal (29):408–435

[SR18] Saternus, Z. and K. Rost (2018). “Towards a smart availability assistant for desired work life balance.” In: *Proceedings of the International Conference on Information Systems (ICIS), San Francisco 2018*, USA.

[SSH19] Saternus, Z. K., Staab, and O. Hinz (2019). “Challenges for a Smart Availability Assistant – Availability Preferences”, In: *Proceedings of the American Conference on Information Systems 2019,* Mexico.

[TG16] The Guardian (2016). *French workers win legal right to avoid checking work email out-of-hours*. URL: https://www.theguardian.com/money/2016/dec/31/french-workers-win-legal-right-to-avoid-checking-work-email-out-of-hours (visited on 17/11/2019).

[To06] Towers, I., Duxbury, L., Higgins, C., Thomas, J. 2006. “Time thieves and space invaders: technology, work and the organization,” in: Journal of Organizational Change Management, (19:5), pp. 593-618.

[TTR17] Tarafdar M, Tu Q, Ragu-Nathan TS, (2011) Impact of Technostress on End-User Satisfaction and Performance. Journal of Management Information Systems 27(3):303-334

[Ve03] Venkatesh, V. et al.: User acceptance of information technology: Toward a unified view. MISQ. 425–478 (2003).

[WBB08] Wajcman, J., M. Bittman and J. Brown (2008). “Families without borders: Mobile phones, connectedness and work–home divisions.” *Sociology* 42, 635−652.

[Xu12] Xu, Heng; Gupta, Sumeet; Rosson, Mary Beth; Carroll, John M. Measuring Mobile Users' Concerns for Information Privacy 2012 In: *Proceedings of the International Conference on Information Systems 2017*, Orlando, USA, 2012.

H. Roßnagel, C.H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 109

Agent-based Models as a Method to Analyse Privacy-friendly Business Models in an Assistant Ecosystem

Michael Kubach[1] Nicolas Fähnrich[2] Cristina Mihale-Wilson[3]

Abstract: Various projects and initiatives strive towards designing privacy friendly open platforms and ecosystems for digital products and services. However, besides mastering technical challenges, achieving economic viability and broad market success has so far proven to be difficult for these initiatives. Based on a publicly funded research project, this study focuses on the business model design for an open digital ecosystem for privacy friendly and trustworthy intelligent assistants. We present how the agent-based modelling technique can be employed to evaluate how business models perform in various constellations of an open digital ecosystem. Thus, our work relates to the strategic choice of suitable business models as an important success factor for privacy and security-relevant technologies.

Keywords: agent-based modelling; business models; smart assistants; ecosystem; diffusion

1 Introduction

Warnings of the dominance of big centralized platform players exploiting the data of their customers, primarily for advertising purposes, have been frequent [Th17] [Bu17] [ABR19] [SFP16]. While the creation of open, interoperable and privacy friendly platforms or ecosystems is part of numerous initiatives and research projects (a few European and German examples are RERUM [RE16], Big-IoT [Bi20], SmartOrchestra [Sm20], OpenIoT [Op20] and of course the new GAIA X initiative [Fe19]), the success of such initiatives is still questionable. At the end of 2019, the following 6 companies were among the 7 most valuable companies by market capitalization: Apple, Microsoft, Alphabet, Amazon, Facebook and Alibaba (the list is led by oil-giant Saudi Aramco) [Wi19]. That significant parts of these companies' business models rests on proprietary platforms indicates how powerful these platforms have become in the world economy.

Akin to the initiatives mentioned above, the research project ENTOURAGE, whose work forms the basis for this paper, aimed at building an open digital ecosystem for trustworthy and privacy friendly smart assistants [EN19]. To deliver on to their promises and support their user with context-sensitive and personalised assistance, smart assistants need to continuously gather as well as process significant amounts of contextual and personal information. If the

[1] Fraunhofer IAO, Hardenbergstraße 20, 10623 Berlin, michael.kubach@iao.fraunhofer.de
[2] Fraunhofer IAO, Nobelstraße 12, 70569 Stuttgart, nicolas.faehnrich@iao.fraunhofer.de
[3] Goethe University Frankfurt, Information Systems, Theodor-W-Adorno-Platz 4, 60629 Frankfurt am Main, mihale-wilson@wiwi.uni-frankfurt.de

data-collection and processing is performed on one single platform, or within a proprietary ecosystem controlled by one company, it can become an easy target for attackers [KGH16]. To address the various data privacy [MZH17] as well as security concerns arising when data is stored and handled on one platform, ENTOURAGE envisioned an open digital ecosystem without dominant participants and high privacy as well as security standards. Within this open digital ecosystem users can then combine smart assistants and data sources from vendors of their choice to achieve a trustworthy (secure and privacy friendly) assistance experience. How the project defines and implements privacy is detailed in its privacy and security reference architecture [ZHK19].

Most of the current open platform and ecosystem initiatives focus on technical aspects, developing open standards, powerful architectures and flexible interfaces [MK19]. In this respect, current open platform and ecosystem initiatives are similar to many initiatives in the areas of IT security, privacy enhancing technologies (PETs) and privacy friendly identity management. However, while it is certainly necessary to ensure the technical functioning of security and privacy friendly solutions, this is not sufficient for their broad adoption. Only with simultaneous consideration of non-technical aspects, a broad adoption can be achieved. This is what would be necessary to raise the actual level of privacy of the solutions in use [ZR12]. When setting up the project, the development of viable business models for the operation of the various ecosystem components was identified as a crucial non-technical determinant for the ecosystems' success [KGH16]. Since viable business models secure the required resources to develop the ecosystem further, attract the necessary amount of participants to create value, and are a fundamental ingredient to the success of innovations [Li11], [Ka15], the project dedicated significant efforts to the design of business models which find acceptance by potential ecosystem participants and users alike [MK19], [MZH19], [MZK19]. This was driven by various research and practice related challenges: As [Le12] point out, research on viable business models for open digital ecosystems is very scarce. Accordingly, with no or very little guidance from academia, practitioners would have to follow very costly and time-consuming trial and error approaches to identify the business models that would work in the context of open digital ecosystems. Besides, since digital ecosystems are very complex entities with many stakeholders whose goals are sometimes conflicting rather than aligned, practitioners must not only choose the business models suitable for their own business, but also be able to predict their value within various ecosystem constellations.

Unfortunately, testing the performance of various business models within an open digital ecosystem with several actors in the real world would exceed the resources of any research project. Hence, ENTOURAGE chose to explore how business models would perform within a digital ecosystem based on an agent-based simulation approach. In the following, this paper will focus on the simulation method that was used to analyse the general viability of the business model of the open assistant ecosystem. We do this, because the agent-based modelling approach employed in this study is very likely to be valuable for other privacy and security-relevant technologies facing similar challenges. Privacy-friendly identity

management ecosystems, for instance, are one noteworthy example for which our simulation approach might be valuable.

Within the ENTOURAGE project, the simulations were complemented by workshops and surveys with end-users, experts, as well as practitioners. These workshops helped to study important business model related aspects like user preferences, willingness to pay for secure and privacy friendly assistants [MZH17], and general preferences towards different business models [MZK19].

The paper is structured as follows: A brief overview of the related literature in chapter two substantiates the choice of our method. Then, in chapter three, the paper focuses on the agent-based modelling approach for ENTOURAGE and presents first experiences with the method. Ultimately, chapter four concludes the main insights generated by the agent-based simulation.

2 Related Work and Suitability of the method

The selection of the agent-based modelling approach used in this paper is substantiated by comparing and weighing the basic advantages of simulations against their disadvantages. Furthermore, our choice to perform an agent-based modelling approach is supported by research in comparable fields that shows how agent-based models can be applied. Following [Bö10], applying simulations as a method gives researchers the opportunity to investigate complex system structures that are not subject to the limitations of analytical methods. Moreover, processes as well as resources can be modelled with system-relevant restrictions and problem-relevant key parameters can be represented as well as observed at simulation runtime. As the simulation can be run several times, flexible sensitivity analysis of solutions are possible. Further, simulations also make it possible to observe complex system behaviour step by step in their temporal development and through clear, graphic representation. Besides, as [DF16] point out, simulations are also possible with less empirical data compared to a classical quantitative observational analysis of a specific market. Against this background, simulations allow researchers to create assessments of potential future developments as well.

Despite the numerous advantages mentioned above, agent-based simulations have also limits that need to be discussed. In terms of disadvantages, [Bö10] mentions that simulations typically have no standard benchmarking criteria, do not recognize an optimum and do not have clear abort criteria. Additionally, [SK16] point out that the data and the model and parameter assumptions of such simulations are decisive for the results, so that the calibration of simulation models is often challenging. Researchers can mitigate the methodological deficits of simulations through a variety of strategies: For one, researchers can make the simulation assumptions transparent. Then, researchers can engage experienced simulation experts to assess and improve their model. Further, researchers can also combine and complement their chosen simulation method with other suitable research methods.

In our study, we chose agent-based modelling as the particular simulation method. Simplified, the agent-based modelling method is a special form of discrete simulation that can act as a kind of virtual lab for experimental (socio-)economic research [DK10], [EA96]. The goal of an agent-based simulation is the reproduction of a real multi-agent system in a virtual environmental simulation. The simulation consists of different components and captures the co-interaction of these components. Further, the agent-based modelling method can provide insights into distributed, interactive connections and developments between many independent decision makers (agents). As such, the agent-based modelling approach allows researchers to perform analyses albeit limited empirical data availability [TCS14]. Typically, agent-based models consist of three elements: (1) the agents, with particular attributes and behaviours; (2) the agent relationships and methods of interaction; and (3) the agents' environment, which describes where the agents "live" and with which of the other agents they interact [MN14]. Recently, agent-based modelling has been applied in information systems research as well, for example to analyse digital business models for individual businesses [ZGJ14], service platforms [TBT19], platform diffusion [SB19], and incentive structures in blockchain-based applications [HT19]. In the context of privacy, the agent-based approach has been applied to model privacy concerns and behaviour depending on privacy-settings in social media [TCS14], [Ba11]. This list reveals the popularity and versatility of the agent-based modelling approach, which can be employed in different contexts. Nonetheless, while the agent-based modelling (ABM) approach has been applied to investigate a variety of IS related topics, we could not identify any work that employed it particularly to evaluate business models for privacy-friendly ecosystems.

3 Proposing ABM as a Method

From an economic perspective, an ecosystem is a network of market participants that are in interdependent service relationships. Thus, the ecosystem contains a multitude of networked actors with different competencies, therewith serving different stages of the value chain. The relationships amongst ecosystem participants are generally based on the cooperation principle. Yet, whenever several companies occupy similar value creation stages or companies have similar competences and offer them in the ecosystem, the cooperative relationships between ecosystem participants can take a competitive character.

An open ecosystem consists of diverse stakeholders with different economic interests. Whether it can sustain on the market depends on many factors such as the business models it supports, the distribution of costs and benefits amongst stakeholders, the number of end users and the share of actively participating companies. Since real-world market-testing of the full ecosystem exceeds the resources of any project, a simulation-approach was chosen for the evaluation of suitable business models. Building upon the related work discussed in the previous chapter, our agent-based model included a simplified set of ecosystem participants (i.e., agents): These were "end users" , "smart assistants" , "smart device manufacturers" and the digital ecosystem "ENTOURAGE" itself.

Market activities are driven by the movement process of the end-user agents that can be triggered by direct contact with other agents or environmental influences. The ENTOURAGE agent serves as a kind of control center for the realization of the overall ecosystem, through which smart device manufacturers and smart assistant providers are connected with the end users and provide their products and services. Smart assistant agents and smart device manufacturers offer various services and products to end users that are compatible with the ENTOURAGE ecosystem. The services and products are offered via a subscription plan or purchase within the respective area of influence. The agent-based model was implemented using the software-package NetLogo[4]. The model's user interface is shown in Figure 1.

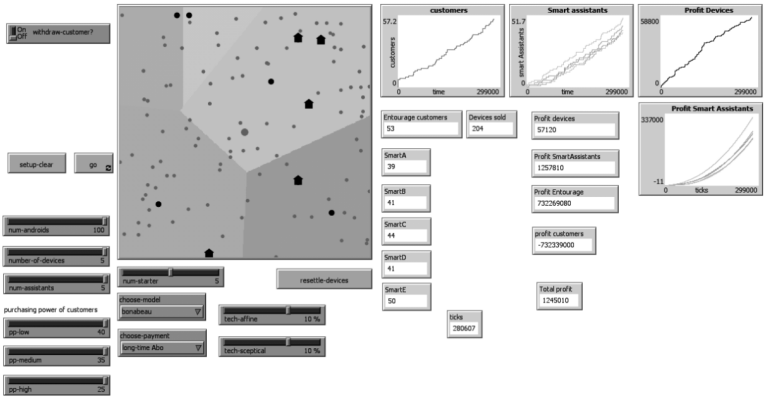


Fig. 1: User interface

The visualization in the center of the user interface (see Figure 2) shows a visualization with end users as small dots, smart assistants as large black dots, and manufacturers of smart devices as black houses. ENTOURAGE is represented as a large red dot in the center of the area. The colored Voronoi partitions[5] represent the sphere of market influence of the smart assistants.

The flowchart shown in Figure 3 describes the ongoing processes of the model. After the model initialization, the movement process starts randomly moving the end users in the area. End users that have an ENTOURAGE subscription are shown as red dots and end users without an ENTOURAGE subscription are shown as grey dots.

The distribution of ENTOURAGE happens via word-of-mouth marketing when a non-subscriber meets an ENTOURAGE customer or the central ENTOURAGE instance. This principle corresponds to the spread of a virus infection. We implemented the following diffusion models that can be chosen via the user interface:

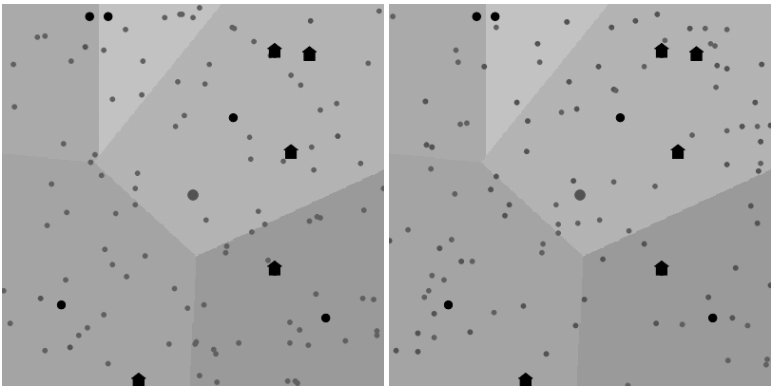
- Bass diffusion model [Ba69]

[4] https://ccl.northwestern.edu/netlogo

[5] Voronoi partition: A polygon with one generating point from which every point in the polygon is closer to than to any other generating point of other polygons.

- Bonabeau diffusion model [Bo02]
- Sigmoid function

We chose the Bass diffusion model because it is a commonly used and well-established model in the literature to estimate technology diffusion. Furthermore, we implemented the newer, ABM-related Bonabeau diffusion model and a simple sigmoid function.



(a) Initial situation (0 ticks) (b) Advanced simulation progress (280.607 ticks)

Fig. 2: Visualization of the model

If the non-subscriber becomes an ENTOURAGE customer, the grey dot turns red and the new subscriber distributes ENTOURAGE itself, which accelerates the growth of the customer base (see Figure 2). The distribution of smart assistants is based on the corresponding Voronoi partitions wherein the end users become customers with a defined probability at every step of the movement process. The size of the Voronoi partitions thereby represents the market power of the corresponding smart assistant. The distribution of smart devices works in a similar way, but in contrary to smart assistants, a distribution requires direct contact of the end user with the smart device manufacturers.

All described forms of interactions with the end users are summarized under "business contact" (see Figure 3). At every step of the movement process, any subscription of the corresponding end users is cancelled by a given probability.

We implemented the cash flow between stakeholders and their profit in the model. The calculated profits have to be interpreted in relation to the other stakeholders and thus serve as an indicator of how well a business model performs. The cash flow was implemented dimensionless, since the framework conditions of the model do not allow any explicit conclusions regarding revenues and profits.

The influencing factors for the profit of the respective stakeholders is illustrated in Figure 4.

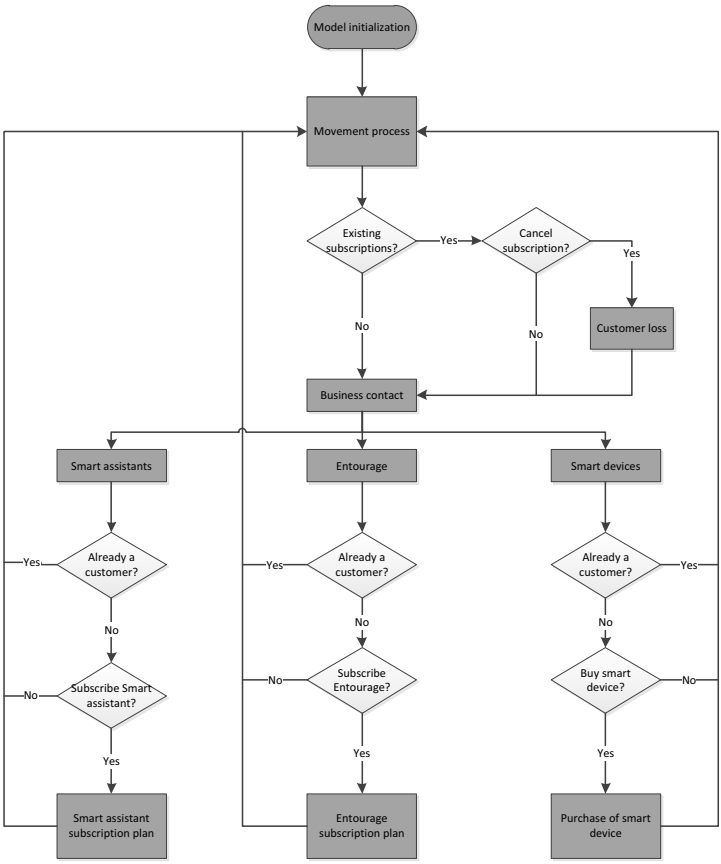


Fig. 3: Flowchart of the model

So far, three business models for ENTOURAGE have been implemented: An ad-financed business model without subscription fees for end users (potentially less privacy-friendly), a subscription model with a short contract commitment and higher subscription fees in comparison for end users and a subscription model with long contract commitment and lower subscription fees in comparison. In this first prototype of the model we did not include the possibility of different business models inside a group of stakeholders (i.e. different smart device manufacturers following different business models).

In all business models the cash flow between the other stakeholders is the same: Smart assistant providers and smart devices manufacturers pay a license/usage fee for the ENTOURAGE implementation. Furthermore, operational costs are incurred as fixed and variable costs depending on the number of users.

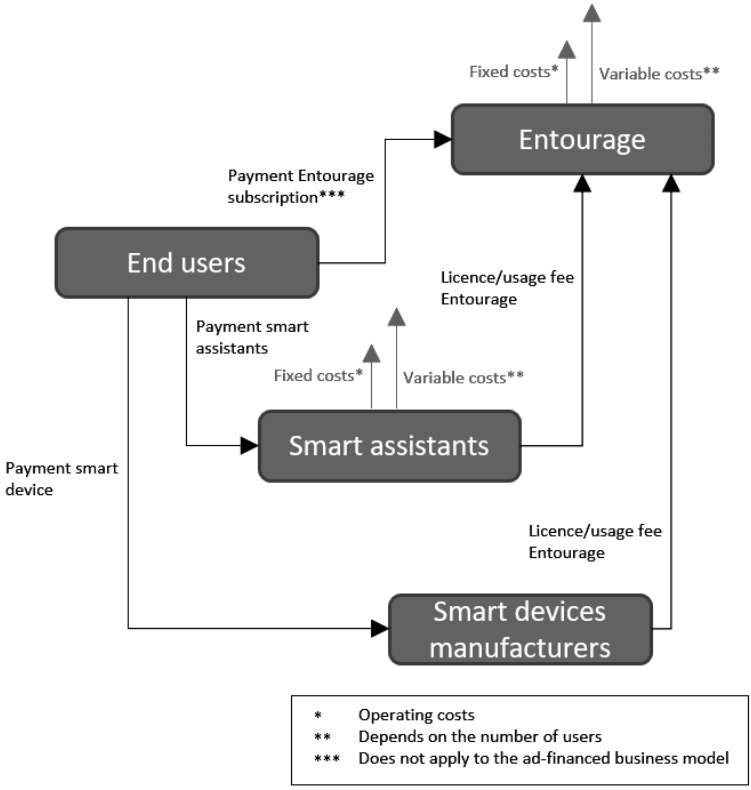


Fig. 4: Visualized cash flows

In order to be able to control the interdependencies of stakeholders, all parameters of the model can be easily modified via the user interface shown in Figure 1 or via the source code. The behaviour of the end-user agents can be fine-tuned in this way: The end users are divided into three groups, of which the ratio can be modified, with low, medium and high purchasing power affecting the likelihood of purchases. Furthermore, the model differentiates between regular, interested and skeptical users regarding ENTOURAGE as well. Regular users are moving purely random, whereas interested users are more likely to follow, and skeptical users are more likely to move away from ENTOURAGE customers in their immediate vicinity. Further parameters that strongly impact the simulation process are the number of end users, the initial number of ENTOURAGE customers, the number of smart device manufacturers and the number of smart assistant providers.

At first, simulations indicated strong differences regarding profits and customer base of individual stakeholders. Thus, the simulations indicated the challenge of a well-balanced business model, since a market situation in which a gap in profit between stakeholders is

too large inevitably leads to the failure of the business model in the long term. However, first simulation results showed that a decentralized, open ecosystem as envisioned in ENTOURAGE can basically be simulated and underlying business models are viable when well-adjusted. Our results indicate that a privacy-friendly open ecosystem as described in section 1 can be viable on the market. However, aspects of privacy and security need to be integrated into the model for further investigation. This includes both, the added value for end users and the privacy preferences of other stakeholders regarding the use and utilization of user data.

4 Conclusion

As consumers as well as the general public grow increasingly aware of privacy and security issues related to digital products and services they connect to, various initiatives and research projects strive towards designing and implementing trustworthy and privacy friendly digital offerings, platforms and ecosystems. However, designing privacy friendly digital offers poses various novel challenges that need to be addressed. Based on a real project sponsored by the Germany Ministry of Economy and Energy, this study focused on the challenge of designing an open digital ecosystem for privacy friendly and trustworthy intelligent assistants while still ensuring the attractiveness and economic viability of the construct. In this regard, this study presents how the agent-based modelling technique can be employed to evaluate how business models perform in various constellations of an open digital ecosystem. Thus, this study relates to the strategic choice of suitable business models as an important success factor for all technologies, including privacy and security-relevant technologies.

Typically, a company's or a business network's chances to survive and thrive in the market depends on various individual but also interdependent factors. Business models, distribution of costs and benefits amongst stakeholders, the number of end users and the share of actively participating companies are only a few of such success-critical factors that influence each other. Beyond the complicated interactions between various determinants for success, companies who want to successfully join an open digital ecosystem also need to fine-tune their strategic decisions in accordance with the constraints and dynamics of the ecosystem and its participants.

Against the background that a real-world market-testing of the full ecosystem exceeds the resources of any company or project, this paper shows how an agent-based simulation-approach can be used to evaluate the suitability of business models in the context of privacy friendly digital ecosystems. Our first modelling approach as presented in this paper is focused on the business models as such and their economic viability – not on the privacy aspects of these business models and their influence. Although the model is still a rudimentary early prototype (this is why we did not present quantitative results at this stage), it is extendable to investigate a variety of success relevant factors other than business models. Further, the model is also modifiable with regard to the agents, their goals and relationships of these entities. This way, this paper presents a viable model which supports both researchers and

practitioners to foresee how success-relevant factors interact with each other and behave in various ecosystem conditions. In future evolutions further factors can be added and for example enable sensitivity analysis can be performed.

As privacy-friendly digital services, platforms and ecosystems gradually gain traction, researchers' and practitioners' demand for suitable simulation and probably more sophisticated ABM models is also very likely to increase. Hence, we invite fellow researchers to build upon our model to develop a more extended and refined version of it.

References

[ABR19] Alleman, J. H.; Baranes, E.; Rappoport, P.: Multisided Markets and Platform Dominance. In: 30th European Conference of the International Telecommunications Society (ITS): "Towards a Connected and Automated Society", Helsinki, Finland, 16th-19th June 2019. Inteernational Telecommunications Society (ITS), Helsinki, 2019.

[Ba11] Baracaldo, N.; López, C.; Anwar, M.; Lewis, M.: Simulating the effect of privacy concerns in online social networks. In: 2011 IEEE International Conference on Information Reuse Integration. Pp. 519–524, Aug. 2011.

[Ba69] Bass, F. M.: A new product growth for model consumer durables. Management science 15/5, pp. 215–227, 1969.

[Bi20] Big IoT Project, http://big-iot.eu/, 2020.

[Bo02] Bonabeau, Eric: Agent-based modeling: Methods and techniques for simulating human systems./99, pp. 7280–7287, 2002.

[Bö10] Böhnlein, C.: Simulationsunterstützte Spezifikation und Analyse von Geschäftsmodellen und Geschäftsprozessen. ASIM Fachtagung/, pp. 83–104, 2010.

[Bu17] Bundesministerium für Wirtschaft und Energie: Weißbuch Digitiale Plattformen: Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe, tech. rep., Berlin, 2017.

[DF16] Desmarchelier, B.; Fang, E. S.: National culture and innovation diffusion. Exploratory insights from agent-based modeling. en, Technological Forecasting and Social Change 105/, pp. 121–128, Apr. 2016, visited on: 01/29/2020.

[DK10] Deckert, A.; Klein, R.: Agentenbasierte Simulation zur Analyse und Lösung betriebswirtschaftlicher Entscheidungsprobleme. de, Journal für Betriebswirtschaft 60/2, pp. 89–125, June 2010, visited on: 01/28/2020.

[EA96] Epstein, J. M.; Axtell, R.: Growing artificial societies: social science from the bottom up. Brookings Institution Press, 1996, ISBN: 0-262-05053-6.

[EN19] ENTOURAGE Project, http://entourage-projekt.de/, 2019.

[Fe19] Federal Ministry for Economic Affairs and Energy (BMWi): Project GAIA-X – A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem. Federal Ministry for Economic Affairs and Energy, Berlin, 2019.

[HT19] Hülsemann, P.; Tumasjan, A.: Walk this Way! Incentive Structures of Different Token Designs for Blockchain-Based Applications. In: ICIS 2019 Proceedings. Munich, Nov. 2019.

[Ka15] Kaufmann, T.: Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge: der Weg vom Anspruch in die Wirklichkeit. Springer-Verlag, Wiesbaden, 2015.

[KGH16] Kubach, M.; Görwitz, C.; Hornung, G.: Non-technical Challenges of Building Ecosystems for Trustable Smart Assistants in the Internet of Things: A Socioeconomic and Legal Perspective. In (Hühnlein, D.; Roßnagel, H.; Schunck, C.; Talamo, M., eds.): Open Identity Summit 2016, Lecture Notes in Informatics – Proceedings. Köllen, Bonn, pp. 105–116, 2016.

[Le12] Leminen, S.; Westerlund, M.; Rajahonka, M.; Siuruainen, R.: Towards IOT Ecosystems and Business Models. In (Andreev, S.; Balandin, S.; Koucheryavy, Y., eds.): Internet of Things, Smart Spaces, and Next Generation Networking. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, pp. 15–26, 2012, ISBN: 978-3-642-32686-8.

[Li11] van Limburg, M.; van Gemert-Pijnen, J. E. W. C.; Nijland, N.; Ossebaard, H. C.; Hendrix, R. M. G.; Seydel, E. R.: Why business modeling is crucial in the development of eHealth technologies. Journal of Medical Internet Research 13/4, e124, Jan. 2011.

[MK19] Mihale-Wilson, C.; Kubach, M.: Business Models for Open Digital Ecosystems of Trustable Assistants. In: Open Identity Summit 2019 (OID2019), GI, Lecture Notes of Informatics. Köllen Druck + Verlag GmbH, Bonn, pp. 59–70, 2019.

[MN14] Macal, C.; North, M.: Introductory tutorial: Agent-based modeling and simulation. In: Proceedings of the Winter Simulation Conference 2014. Pp. 6–20, Dec. 2014.

[MZH17] Mihale-Wilson, C.; Zibuschka, J.; Hinz, O.: About user preferences and willingness to pay for a secure and privacy protective ubiquitous personal assistant. In: Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017. 2017, ISBN: 978-989-20-7655-3.

[MZH19] Mihale-Wilson, C.; Zibuschka, J.; Hinz, O.: Nutzerpräferenzen und Zahlungsbereitschaften für einen sicheren und datenschutzfreundlichen digitalen Assistenten. In: Workshop PRINT im Rahmen der Jahrestagung der Gesellschaft für Informatik 2019. LNI, 2019.

[MZK19] Mihale-Wilson, C.; Zibuschka, J.; Kubach, M.: Consumer-based Ranking for Strategic Selection of IoT Business Models. In: Fortieth International Conference on Information Systems. Munich, 2019.

[Op20] OpenIoT Project, http://www.openiot.eu/, 2020.

[RE16] RERUM: REliable, Resilient and secUre IoT for sMart city applications, https://ict-rerum.eu/, 2016, visited on: 01/24/2020.

[SB19] Schalowski, J.; Barrot, C.: The Long-term Diffusion of Digital Platforms — An Agent-based Model. In: ICIS 2019 Proceedings. Munich, Nov. 2019.

[SFP16] Schweitzer, H.; Fetzer, T.; Peitz, M.: Digitale Plattformen : Bausteine für einen künftigen Ordnungsrahmen. ZEW Discussion Paper/16, pp. 70–70, 2016.

[SK16] Silvia, C.; Krause, R. M.: Assessing the impact of policy interventions on the adoption of plug-in electric vehicles: An agent-based model. en, Energy Policy 96/, pp. 105–118, Sept. 2016, visited on: 01/29/2020.

[Sm20] SmartOrchestra Project, http://smartorchestra.de/, 2020.

[TBT19] Torres Pena, M.; Breidbach, C.; Turpin, A.: Crafting Agent-based Models to Analyze Service Platforms. In: ICIS 2019 Proceedings. Munich, Nov. 2019.

[TCS14] Tubaro, P.; Casilli, A. A.; Sarabi, Y.: Against the hypothesis of the end of privacy: an agent-based modelling approach to social media. Springer, Cham, 2014, ISBN: 3-319-02456-6.

[Th17] The Economist: The world's most valuable resource is no longer oil, but data, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, May 2017.

[Wi19] Wikipedia: List of public corporations by market capitalization, https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization, 2019, visited on: 01/24/2020.

[ZGJ14] Zutshi, A.; Grilo, A.; Jardim-Gonçalves, R.: A Dynamic Agent-Based Modeling Framework for Digital Business Models: Applications to Facebook and a Popular Portuguese Online Classifieds Website. In (Benghozi, P.-J.; Krob, D.; Lonjon, A.; Panetto, H., eds.): Digital Enterprise Design & Management. Advances in Intelligent Systems and Computing, Springer International Publishing, Cham, pp. 105–117, 2014, ISBN: 978-3-319-04313-5.

[ZHK19] Zibuschka, J.; Horsch, M.; Kubach, M.: The ENTOURAGE Privacy and Security Reference Architecture for Internet of Things Ecosystems. In (Roßnagel, H.; Wagner, S.; Hühnlein, D., eds.): Open Identity Summit 2019. Proceedings: GI-Edition - Lecture Notes in Informatics (LNI). Köllen Druck + Verlag GmbH, Bonn, pp. 119–130, 2019.

[ZR12] Zibuschka, J.; Roßnagel, H.: A Structured Approach to the Design of Viable Security Systems. In: ISSE 2011 - Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2011 Conference. Vieweg+Teubner, Wiesbaden, pp. 246–255, 2012.

H. Roßnagel, C. H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 121

Automation Potentials in Privacy Engineering

Christian Zimmermann[1]

Abstract: The GDPR enshrines the privacy by design paradigm in law, making sound privacy engineering methods more important than ever. Integrating automation and extensive tool support into the privacy engineering process has the potential to support organizations in streamlining the implementation of privacy and data protection by design and reducing its cost. Based on a privacy engineering reference process, this paper systematically investigates automation potential in privacy engineering. In particular, it discusses potentials and implications of automation in privacy engineering and illustrates directions for future research.

Keywords: Privacy Engineering; Data Protection; Automation

1 Privacy by Design

The GDPR enshrines the "privacy by design"paradigm in law by stipulating "data protection by design and default" in its Article 25. In order to fulfill the data protection by design and default (DPbDD) obligations pursuant Art. 25 GDPR, data controllers need to consider privacy and data protection risks early on in the design of systems for processing personal data. Moreover, privacy and data protection need to be considered in the complete development life-cycle [Eu19]. The implementation of a privacy engineering process can support companies in doing so. Privacy engineering is "the discipline of understanding how to include privacy as non-functional requirement in system engineering" [CSC14] and, hence, a method to integrate the privacy by design paradigm [CSC14] into product development. From a governance perspective, privacy engineering can also be defined as "engineering data governance for personal information into the design and implementation of routines, systems, and products that process personal information" [DFF14].

Developers of systems, devices and software for processing personal data are often no privacy or legal experts and not able to fully consider data protection intricacies and requirements [Ha18]. Consequently, privacy experts need to be involved in systems and privacy engineering to support architects and developers. However, privacy experts are sparse and costly, especially those with a background in both law and computer science. Automating privacy engineering or specific steps of the privacy engineering process seems to be a promising way to mitigate the sparsity of privacy experts and to reduce development cost. Moreover, automation might also help companies establish a consistent minimum

[1] Bosch Research, 71272 Renningen, christian.zimmermann3@de.bosch.com

level of quality with respect to analyses and measures for compliance with data protection legislation.

This paper investigates automation potentials in privacy engineering. In order to discuss privacy engineering in a systematic manner, I first present and discuss a privacy engineering reference process in Section 2. Subsequently, in Section 3, I identify potential for automation, semi-automation or tool support in the individual steps of the reference process and illustrate research streams to be addressed to foster automation of privacy engineering. Section 4 discusses advantages, disadvantages and limits of (semi-)automation in privacy engineering. Section 5 concludes the paper.

2 Privacy Engineering Reference Process

The goal of privacy engineering is to ensure the implementation of appropriate measures and safeguards for specific processing means and purposes. Figure 1 depicts the privacy engineering reference process upon which the discussion in this paper is based. The presented reference process is grounded in and extends the work by Hoepman [Ho14] and his mapping of privacy design strategies and patterns to the software development cycle. I also draw from Gürses et al. [GTD15] and Spiekermann & Cranor [SC09] and take into account the GDPR, the EDPB's Guidelines on Article 25 [Eu19] and the "Standard-Datenschutzmodell" (SDM) [Ko16], the latter of which has been drafted by German DPAs. As can be seen, the privacy engineering reference process can roughly be mapped to the "classic" software development process (see also [Ho14]). The following will briefly introduce the individual process steps and discuss associated challenges.

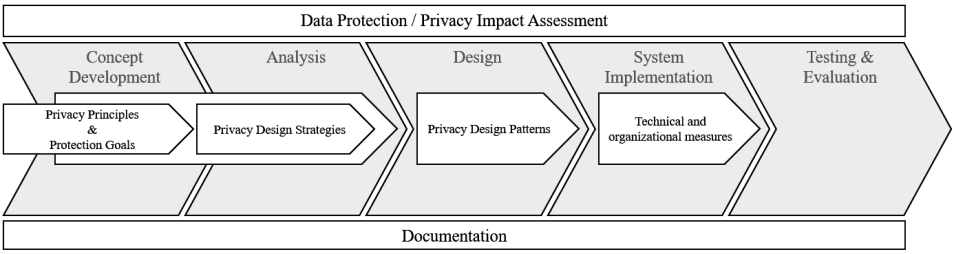


Fig. 1: Generic privacy engineering process

Note that the figure is not intended to imply a necessarily linear, one-time process but a process that might (at least partly) need to be applied iteratively, e.g., within agile development methods. Obviously, privacy engineering is also not an end in itself but a sub-activity of system engineering and product development and a means to design systems and products compliant with data protection legislation and catering to users' needs and demands. Hence, the depicted process is also not to be understood as a stand-alone process but as embedded into a broader system engineering and (product) development process and needs to include interfaces to security engineering (cf. Art. 32 GDPR).

Companies face a variety of challenges when trying to implement privacy by design and privacy engineering processes. Overarching challenges refer to the sparsity of privacy and data protection experts and to the communication-related and cultural challenges that arise in the collaboration between technologists and legal staff. Besides these more general challenges, specific challenges arise in the different process steps. In the following the individual steps of the reference process and associated challenges are briefly illustrated in order to inform the discussion on automation potentials.

2.1 Privacy Principles and Protection Goals

For controllers or processors to comply with the data protection by design and default requirement, systems for processing personal data obviously need to be implemented under consideration of the relevant obligations laid down in the applicable data protection regulations. Consequently, the first step in the depicted privacy engineering process refers to the elicitation of relevant protection goals and privacy-related requirements that the system needs to achieve or fulfill, respectively. Obviously, these encompass primarily the data protection principles laid down in the legislation, e.g., the GDPR. Guidelines by various DPAs and other institutions (e.g. [OE13] or [IS11]) aim to support the translation of these principles and abstract legal requirements into actionable technical and organizational requirements. Notably, the SDM [Ko16] provides a mapping of GDPR articles to the data protection goals proposed by Hansen et al. [HJR15]. It is also advisable to take into account user expectations and demands regarding privacy and to elicit those using, e.g., user studies. Not only might considering user expectations increase user satisfaction and acceptance. Those expectations are also highly relevant in most jurisdictions, e.g. under the GDPR where reasonable expectations of data subjects play a prominent role in assessing lawfulness of data processing based on legitimate interest (cf. Recital 47 GDPR).

The protection goals for privacy engineering [HJR15] are general enough in order to provide guidance for designing systems regardless of their intended domain of deployment. However, translating legal texts and the obligations specified therein into technical requirements is often a daunting task. On the one hand, non-legal staff such as software developers often lack the expertise to interpret legal texts and the knowledge of current legal interpretations of the law. On the other hand, legal staff often lacks the technological expertise to translate legal obligations into technical requirements.

Further problems can arise from the novelty of certain systems, e.g., autonomous systems or IoT systems. In the absence of broad adoption of such systems and the resulting lack of well-defined social norms and expectations regarding their usage, it is hard to formulate reasonable expectations of privacy. Consequently, deploying such systems entails the risk of violating newly forming social norms and expectations of privacy. While this does not necessarily have to amount to a compliance problem, it has the potential to deter potential users from using the systems.

2.2 DPIA and Documentation

The potential risk to privacy and data subjects' rights and freedoms posed by the system to be developed needs to be assessed early on in the development process [Eu19]. In many cases, performing a data protection impact analysis (DPIA) will also be legally required, e.g., in case a planned processing of personal information is likely to pose a high risk to the rights and freedoms of the affected data subjects (Art. 35 GDPR). However, as depicted in Figure 1, it is not sufficient to conduct DPIAs only at the beginning of the engineering process, especially in case agile development practices are used [ZZ20]. Rather, impact assessments need to be conducted repeatedly in order to be able to assess whether changes in the system (either in functionality or in applied measures for data protection) or changes in the state of the art change the identified risk [Eu19]. The (updated) DPIA results need to be reflected in all other process steps.

Several aspects make DPIAs challenging. On the one hand, the need to repeatedly update DPIAs imposes high efforts. This is particularly challenging in case agile development methods are used and changes to the system occur very often [ZZ20] or service-oriented architectures are utilized [GG18]. DPIAs require expert knowledge and assessment, which further increases cost and can delay development when experts are sparse.

DPIA results and information on implemented measures and the actual processing need to be documented (Art. 35 & 5(2) GDPR). Ideally, documentation of DPIA results, design decisions, planned processing steps and implemented measures is conducted in parallel to development. While this will decrease the efforts to be spent after development and during the operation of the system, it imposes a high effort in the development process.

2.3 Privacy Design Strategies & Patterns

The first process steps focus on initial risk and impact assessment and the elicitation of requirements. Subsequently, approaches to satisfying those requirements and mitigating the risks need to be chosen. Privacy Design Strategies "refer to distinct approaches that can be used to achieve privacy protection" [GTD15], e.g., aggregation of information or hiding of information. They describe fundamental approaches that can be implemented using privacy design patterns. A privacy design pattern is "a commonly recurring structure of communicating components that solves a general design problem within a particular context" [GTD15]. Privacy design patterns can also be defined as "design solutions to common privacy problems - a way to translate 'privacy-by-design' into practical advice for software engineering" . For example, encryption can be considered one design pattern for the "information hiding" strategy [Ho14]. Privacy design patterns are similar to software design patterns and more detailed or closer to implementation level than privacy design strategies.

https://privacypatterns.org/

Privacy design strategies can be derived from the data protection principles and protection goals defined in the relevant regulations and best practice guidelines to be adhered to in the development process (cf. [Ho14]). Based on the identified requirements, user and business needs, privacy design strategies should be chosen or developed in the early phases of product concept development. Some (mandatory) strategies can be directly found in regulation, e.g., data minimization as laid down in Art. 5 GDPR. Further, the eight privacy design strategies derived by Hoepman [Ho14] from the OECD privacy guidelines [OE13], Directive 95/46/EC and the ISO 29100 privacy framework [IS11] can be taken into account. Finally, user expectations and desires should be considered in the selection or definition of privacy design strategies.

Challenges related to privacy design strategies refer to the selection of strategies fitting the planned context and scope of the processing, i.e., strategies that provide an optimal balance between effectiveness in reducing the impact on data subjects' rights and freedoms, cost and utility of the system.

Privacy design patterns can be used to implement a chosen privacy design strategy. A broad variety of privacy design patterns have been proposed in the literature. Many of those are collected on the privacypatterns.org website curated by, among others, Jaap-Henk Hoepman, co-author of [Ho14]. The website not only lists privacy design patterns proposed in the literature but also assigns them to privacy design strategies as defined in [Ho14]. However, while privacy patterns are available, it is hard for developers to select and implement fitting patterns as "privacy patterns are scattered, unrelated, inconsistent, and immature" [Co18]. Further, it still needs to be evaluated whether and under which conditions and assumptions "classic" patterns are still viable in new domains such as autonomous systems or the IoT.

2.4 Technical and Organizational Measures

In the final step of the presented process, actual measures for implementing the selected strategies and patterns need to be selected and implemented. The privacy engineering process provided in Figure 1 culminates in the process steps "Technical and organizational measures", whereas the approach presented in [Ho14] puts "privacy-enhancing technologies". In the reference process presented here, a broader perspective is chosen in order to emphasize that technology in general and PETs in particular can not be implemented detachedly from accompanying organizational measures. Moreover, the broader term is used to clearly indicate the inclusion of not only PETs but also transparency-enhancing technologies (TETs) [JWV13; Zi15] as measures for data protection and privacy preservation.

Challenges associated with this step are very similar to those faced in security engineering. Choosing appropriate technology, methods and artifacts is one side of the challenge. The other is the correct implementation of the selected solutions, e.g., selecting appropriate parameters for encryption. Further challenges arise from the application of machine learning and artificial intelligence to personal data [Pa18].

3 Potential for Automation

In the following, automation potentials in privacy engineering are illustrated. The investigation is structured along the steps of the reference process. In particular, I will analyze which aspects of the individual process steps lend themselves to (semi-)automation and discuss avenues for future research. The feasibility and desirability of automation are discussed further in Section 4.

3.1 Privacy Principles and Protection Goals

In this process step, three coarse sub-steps can be delineated. (a) First, relevant legal requirements and protection goals need to be identified. This entails identification of relevant legislation, DPA guidelines, the state of the art and user expectations. (b) Subsequently, relevant parts of these sources need to be identified based on the scope and context of the planned processing. For example, which of the obligations stipulated in the GDPR will apply depends on, i.a., whether data will be transferred to third countries, which types and extent of personal data will be processed or whether the controller will act alone or as a joint controller with others. (c) Finally, the identified (legal) requirements need to be translated into technical or organizational requirements specific to the planned processing. Albeit possibly hard to harness, there is potential for automation or semi-automation in all of these process sub-step.

Sub-step (a) requires knowledge of the context of the planned processing, e.g., applicable jurisdiction and applicable laws. Further, knowledge of relevant case law, legal decisions and DPA opinions and guidelines might be necessary. In the context of international service contracts, Waldburger et al. [Wa10] address the former and propose and implement a modeling method and information model for automated determination of jurisdiction and applicable law. While their approach is not directly transferable to the data protection domain, it illustrates avenues for future research into automated identification of relevant laws. At least semi-automation is conceivable in this sub-step, e.g., based on automated selection of relevant documents based on some input such as a questionnaire.

Once the relevant sources have been identified, the relevant parts, i.e., those including applicable obligations or requirements, need to be identified in sub-step (b). First examples of semi-automation or decision-support tools for this sub-step have already been presented. For example, Colesky et al. [Co19] present a tool to provide information on which recitals and articles of the GDPR are to be considered based on a questionnaire. Work like this can constitute the basis for further automation.

Automated elicitation of technical requirements from identified legal text might be based on work towards formal models of relevant requirement sources, e.g., [Ma08; Me05]. Models of the system as well as the scope and context of the planned processing would also support automation of sub-step (c). Obviously, a chicken-and-egg problem arises here.

Notwithstanding, initial models of the planned system or at least the scope and context of the processing could be used. Several approaches for modeling security-relevant or privacy-relevant system behavior and requirements have been presented [Ah17a; Ah17b; MG07]. Kalloniatis et al. "provide a set of concepts for modeling privacy requirements in the organisation domain and a systematic way-of-working for translating these requirements into system models" [KKG08]. They formally define process patterns for "(1) analysing the impact of privacy requirement(s) on organisational goals, subgoals and processes and (2) suggesting of appropriate system implementation technique(s) for realising these requirements" [KKG08]. Approaches like these might build the basis for automated requirements analysis or translation and merit further research.

3.2 DPIA and Documentation

Performing a DPIA requires an understanding of the system and the scope and context of the planned processing. It further requires analysis and assessment of the impact of the processing on data subjects' rights and freedoms. Consequently, DPIAs are time-consuming and require expert input and, hence, seem desirable candidates for automation. Given their conceptual relation to threat and risk analysis from the field of cyber security and the progress in automation in that area (cf. Threat Dragon , MS Threat Modeling Tool), there is at least reason to hope, that DPIAs can at least be (semi-)automated, potentially based on the methods described above. For example, the STRIDE-based LINDDUN [De11] framework might be extendable into a foundation for semi-automated analysis. In fact, some work in the direction of DPIA automation have already been conducted. For example, as already described in [Zi19], the French DPA CNIL provides a tool for performing data protection impact analysis and generating standardized documentation of the analysis results, which comes in the form of an interactive questionnaire with knowledge base . Hence, the tool supports and formalizes DPIAs, but does not provide full automation.

As already described above, potentials for further automation can be found in the formalization of privacy goals (e.g. [MV19]), system behavior and processing context and model-based engineering (see e.g. [Ah17a; Ah17b; KKG08]). In case a DPIA has to be updated during the development process and software code is available, code analysis as applied in the area of cyber security [CM04] but focusing on the flow of personal data might be another research avenue worth following (e.g. [ML00]).

A more detailed analysis of automation potential in privacy impact assessment processes is presented in [Zi19], to which I refer the interested reader. A similar investigation in the area of automation of security engineering is presented in [MF11].

https://owasp.org/www-project-threat-dragon/migrated_content
https://docs.microsoft.com/de-de/azure/security/develop/threat-modeling-tool
https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

3.3 Privacy Design Strategies and Patterns

As already mentioned in Section 2.3, architects and developers often face difficulties selecting suitable privacy strategies and patterns. Clearly, this is an area where automation or decision support tools might be beneficial. (Semi-)Formally described pattern systems can support automated selection of patterns given a set of requirements. Work towards pattern systems has been presented, e.g., [Co18]. In addition to supporting pattern selection with automation, in some instances, it might also be feasible to (semi-)automate the actual implementation of selected patterns [Bu03].

3.4 Technical and Organizational Measures

Technical and organizational measures need to be implemented in order to protect the rights and freedoms of data subjects. While this does not seem as a typical candidate for automation, there are several aspects that exhibit high potential for automation.

Changes to the system will often require the implementation of new measures. Nowadays, many development and release processes take place in a CI/CD fashion. (Frequent) updates to a system might lead to changes that impact users' privacy, be it by design or as a side effect. Consequently, measures might also have to be updated on system updates. Further, some updates might need the implementation of new measures.

Automation potential lies in the automated detection of system changes that require adaption of existing of implementation of new measures. Obviously, this is related to automated continuous DPIA (see above). Further potential lies in the automated selection of measures to be updated or newly applied, based on updated DPIA results. Examples exist in the cyber security area where, e.g., automated code analysis is well established and a variety of tools exist to automatically recommend measures to be taken to make code more secure.

Still, more research into data flow analysis (see, e.g., [ML00]) and automated pattern selection (see 3.4) is necessary in order to investigate methods for supporting automated selection and implementation of technical measures. However, the implementation of organizational measures will usually not be open to automation.

4 Discussion & Limitations

The previous section briefly outlined automation potentials in privacy engineering and suggested avenues for future research. However, only an overview has been presented and many questions deserving further investigation have only been touched upon. For example, the analysis presented in this paper focused primarily on the design phase and not on the operation of systems processing personal information. In the operation phase, an interesting

area for automation is related to data subjects' rights, e.g., to access data or to erasure of data. As there is only a rather short window of time for reacting to data subject requests (DSRs), automation seems highly beneficial. Further, CI/CD and DevOps were discussed only briefly. For privacy engineering to be truly integrated with modern software development approaches, it needs to be integrated into CI/CD and DevOps methods and tools, especially when controllers implement the systems for processing personal data themselves. Future research into Privacy DevOps might be able to draw from the work in the area of SecDevOps [MO16].

Controllers that develop own systems for processing personal data will most likely benefit most directly from automation of privacy engineering, at least from an economic perspective. Automating time consuming tasks requiring expert input can reduce cost and might be able to supports consistency in the engineering process. Still, the actual economic impact of automation in privacy engineering deserves a closer look, as well as the potential of automation to actually support more consistent, compliant or, generally, privacy-preserving results in privacy engineering.

Some of the process steps illustrated above are of less technical nature than others. In particular, privacy and data protection impact assessment often require interpretation and case-specific balancing of technical, economic and legal aspects. Clearly, such a task is a less suited candidate for full automation than more mechanical tasks not requiring balancing decisions. However, besides feasibility, the desirability of automation in privacy engineering also needs to be discussed. In particular, automation in privacy engineering needs to be considered in the light of it's impact on the human rights aspects underlying data protection regulation and the regulator's intentions in stipulating DPIAs, balancing tests and the implementation of measures for ensuring the rights and freedoms of data subjects. As already hinted at in [Zi19], automated DPIAs (in contrast to manual privacy impact assessments) might lead to negligence of relevant privacy aspects and a too narrow focus on compliance [Wr12]. Automation of DPIAs using AI also entails the risk of bias introduced by biased AI [YW18] and, more generally, the codification into technology of "one-size-fits-all" approaches in an area where case-specific deliberation is required [PD16]. Still, automation also has the potential to provide for more secure software products, e.g., through automated security testing as described above. This in turn can prevent privacy violations based on data leaks due to insecure systems. Further, automated DPIAs might also be able to capture a broader spectrum of risks and threats due to a larger knowledge base compared to individual privacy engineering teams.

5 Conclusion

This paper discussed the potential for automation in privacy engineering. To allow for a more systematic investigation, it presented a privacy engineering reference process and discussed the automation potential of the process's steps individually. Based on the discussion, avenues for future research were illustrated .

References

[Ah17a] Ahmadian, A. S.; Peldszus, S.; Ramadan, Q.; Jürjens, J.: Model-based privacy and security analysis with CARiSMA. In: Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering. ACM Press, pp. 989–993, 2017.

[Ah17b] Ahmadian, A. S.; Strüber, D.; Riediger, V.; Jürjens, J.: Model-Based Privacy Analysis in Industrial Ecosystems. In (Anjorin, A.; Espinoza, H., eds.): Modelling Foundations and Applications. Vol. 10376. LNCS, Springer International Publishing, Cham, pp. 215–231, 2017.

[Bu03] Bulka, A.: Design Pattern Automation. In: Proceedings of the 2002 Conference on Pattern languages of Programs - Volume 13. CRPIT '02, Australian Computer Society, Inc., Melbourne, Australia, pp. 1–10, 2003.

[CM04] Chess, B.; McGraw, G.: Static analysis for security. IEEE Security & Privacy 2/6, pp. 76–79, 2004.

[Co18] Colesky, M.; Caiza, J. C.; Del Álamo, J. M.; Hoepman, J.-H.; Martin, Y.-S.: A System of Privacy Patterns for User Control. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. SAC '18, Association for Computing Machinery, New York, NY, USA, pp. 1150–1156, 2018.

[Co19] Colesky, M.; Demetzou, K.; Fritsch, L.; Herold, S.: Helping Software Architects Familiarize with the General Data Protection Regulation. In: 2019 IEEE International Conference on Software Architecture Companion (ICSA-C). IEEE, pp. 226–229, 2019.

[CSC14] Cavoukian, A.; Shapiro, S.; Cronk, R. J.: Privacy Engineering: Proactively Embedding Privacy, by Design, 2014, URL: https://iapp.org/resources/article/privacy-engineering-proactively-embedding-privacy-by-design/, visited on: 01/27/2020.

[De11] Deng, M.; Wuyts, K.; Scandariato, R.; Preneel, B.; Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering 16/1, pp. 3–32, 2011.

[DFF14] Dennedy, M. F.; Fox, J.; Finneran, T.: The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value. Apress, 2014.

[Eu19] European Data Protection Board: Guidelines 4/2019 on Article 25 - Data Protection by Design and by Default (Adopted - version for public consultation), Guidelines 04/2019, European Data Protection Board, 2019.

[GG18] Galvez, R.; Gurses, S.: The Odyssey: Modeling Privacy Threats in a Brave New World. In: 2018 IEEE European Symposium on Security and Privacy Workshops. Pp. 87–94, 2018.

[GTD15] Gürses, S.; Troncoso, C.; Diaz, C.: Engineering privacy by design reloaded. In: Amsterdam Privacy Conference. 2015.

[Ha18] Hadar, I.; Hasson, T.; Ayalon, O.; Toch, E.; Birnhack, M.; Sherman, S.; Balissa, A.: Privacy by designers: software developers' privacy mindset. Empirical Software Engineering 23/1, pp. 259–289, 2018.

[HJR15] Hansen, M.; Jensen, M.; Rost, M.: Protection goals for privacy engineering. In: 2015 IEEE Security and Privacy Workshops, SPW 2015. Pp. 159–166, 2015.

[Ho14] Hoepman, J.-H.: Privacy Design Strategies. In: ICT Systems Security and Privacy Protection. Springer, Berlin, Heidelberg, pp. 446–459, 2014.

[IS11] ISO/IEC Joint Technical Committee 1 SC 27: ISO/IEC 29100 Information technology - Security techniques - Privacy framework, 2011.

[JWV13] Janic, M.; Wijbenga, J.; Veugen, T.: Transparency Enhancing Tools (TETs): An Overview. In: 2013 Third Workshop on Socio-Technical Aspects in Security and Trust (STAST). Pp. 18–25, 2013.

[KKG08] Kalloniatis, C.; Kavakli, E.; Gritzalis, S.: Addressing privacy requirements in system design: the PriS method. Requirements Engineering 13/3, pp. 241–255, 2008.

[Ko16] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder: Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (V.1.0), 2016.

[Ma08] May, M. J.: Privacy APIs: formal models for analyzing legal and privacy requirements, Dissertation, University of Pennsylvania, 2008.

[Me05] Mercatali, P.; Romano, F.; Boschi, L.; Spinicci, E.: Automatic Translation from Textual Representations of Laws to Formal Models through UML. In: 18. International Conference on Legal Knowledge and Information Systems (JURIX). Vol. 134, pp. 71–80, 2005.

[MF11] Montesino, R.; Fenz, S.: Information Security Automation: How Far Can We Go? In: 2011 Sixth International Conference on Availability, Reliability and Security. Pp. 280–285, 2011.

[MG07] Mouratidis, H.; Giorgini, P.: Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering 17/02, pp. 285–309, 2007.

[ML00] Myers, A. C.; Liskov, B.: Protecting privacy using the decentralized label model. ACM Transactions on Software Engineering and Methodology (TOSEM) 9/4, pp. 410–442, 2000.

[MO16] Mohan, V.; Othmane, L. B.: SecDevOps: Is It a Marketing Buzzword? - Mapping Research on Security in DevOps. In: 2016 11th International Conference on Availability, Reliability and Security (ARES). IEEE, pp. 542–547, 2016.

[MV19] Mödersheim, S.; Viganò, L.: Alpha-Beta Privacy. ACM Transactions on Privacy and Security 22/1, pp. 1–35, 2019.

[OE13] OECD: The OECD Privacy Framework, 2013, URL: https://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf, visited on: 01/24/2020.

[Pa18] Papernot, N.: A Marauder's Map of Security and Privacy in Machine Learning: An overview of current and future research directions for making machine learning secure and private. In: AISec '18: Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security. ACM Press, 2018.

[PD16] Pagallo, U.; Durante, M.: The Pros and Cons of Legal Automation and its Governance. European Journal of Risk Regulation 7/2, pp. 323–334, 2016.

[SC09] Spiekermann, S.; Cranor, L. F.: Engineering Privacy. IEEE Transactions on Software Engineering 35/1, pp. 67–82, 2009.

[Wa10] Waldburger, M.; Charalambides, M.; Schaaf, T.; Stiller, B.: Automated determination of jurisdiction and applicable law for international service contracts: Modeling method, information model, and implementation. In: 18th Biennial and Silver Anniversary International Telecommunications Society Conference (ITS 2010). Pp. 1–31, 2010.

[Wr12] Wright, D.: The state of the art in privacy impact assessment. Computer Law & Security Review 28/1, pp. 54–61, 2012.

[YW18] Yapo, A.; Weiss, J.: Ethical Implications of Bias in Machine Learning. In: Proceedings of the 51st Hawaii International Conference on System Sciences. Pp. 5365–5372, 2018.

[Zi15] Zimmermann, C.: A Categorization of Transparency-Enhancing Technologies. In: Amsterdam Privacy Conference. Amsterdam, NL, 2015.

[Zi19] Zibuschka, J.: Analysis of Automation Potentials in Privacy Impact Assessment Processes. In: 1st Workshop on Security, Privacy, Organizations, and Systems Engineering. Luxembourg, 2019.

[ZZ20] Zibuschka, J.; Zimmermann, C.: Lean Privacy by Design. In (Reinhardt, D.; Langweg, H.; Witt, B. C.; Fischer, M., eds.): SICHERHEIT 2020. Gesellschaft für Informatik e.V., Bonn, pp. 125–128, 2020.

H. Roßnagel, C. H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 133

A Human Digital Twin as Building Block of Open Identity Management for the Internet of Things

Jan Zibuschka[1], Christopher Ruff[2], Andrea Horch[2], Heiko Roßnagel[2]

Abstract: In networked industry, digital twins aggregate product data along the entire life cycle, from design and production to deployment. This enables interoperability between different data sources and analysis functions and creates an integrated data environment. Human digital twins have the potential to create a similarly interoperable and integrated data environment for more user-centric use cases in the field of the Internet of Things. In this case, personal data is processed and transmitted; therefore, the underlying infrastructure is then not product data management but identity management. In this paper, we discuss general aspects of the human digital twin, its role in open identity management systems, and illustrate its application in the field of home, building and office automation. We identify advantages and limitations and suggest future research opportunities.

Keywords: digital twin; internet of things; interoperability; data protection; identity management

1 Introduction

Devices that we use every day are increasingly networked in the so-called Internet of Things (IoT). The communication between these devices poses both interoperability challenges, i.e. whether different devices are capable of exchanging data, and privacy challenges, such as how to control such data exchange [He16; ZHK19]. An identity management infrastructure, a key architectural component in many IoT ecosystem architectures [Ba19; ZHK19], can create an overarching, networked data space that allows both comprehensive analysis of the data and fine-grained control of their exchange.

There are corresponding developments in industrial IoT scenarios. Here, so-called digital twins [AE17], integrated artifacts that aggregate master data pertaining to a device type, observations of sensors at individual device instances, data processing functions, and derived data resulting from processing along the entire life cycle of a product or production machine. There are different approaches for specific implementation, but in general digital twins are intelligent, virtual images of physical devices [AE17]. They have the potential to enable new business models for companies in various verticals and serve as standardized units for cross-organizational data exchange, both in the interaction along the value chain and with regard to the resulting products [KHB18]. These changes affect the entire product life cycle [Ta18]. Besides industrial applications, digital twins

[1] Robert Bosch GmbH, Renningen, 70465 Stuttgart, Jan.Zibuschka@de.bosch.com
[2] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, firstname.lastname@iao.fraunhofer.de

have also found their way into building control systems, where they enable large-scale orchestration of devices [Kh19].

Like the digital twin of a device, the human digital twin has its origin in production technology [Ha20]. In addition to research in this field, where the focus is on capturing the behavior of workers in production environments, there are also applications in medical technology, where the patient's condition is monitored, and and treatment, such as dosage of medications, is controlled using a human digital twin [Ch19]. However, an application of the concept to end users is not covered by existing work.

In the following, we first characterize general characteristics of the human digital twin in a reference architecture, and then describe its application the consumer IoT fields of smart home and building, and how it enables identity management and privacy functions. We then discuss our findings.

2 Human Digital Twins

To characterize a human digital twin, we build on the more general C2PS[3] reference architecture for digital twins [AE17], removing components which are not applicable to humans. We identify the following subsystems, illustrated in Figure 1:

Virtual sensors represent sensors that collect information about the user for storage in the digital twin [AE17]. Unlike the digital twin of a device, sensors do not necessarily have a direct, physical connection to the human. Instead, any sensors that capture information concerning a subject can contribute data to the human digital twin [Ha20].

Observations of these sensors are stored in the digital twin [AE17]. The observations are usually available in a variety of formats and accuracies, and express various contextual data related to the user [Ja17].

Functional units process the information available in the digital twin [AE17]. In contrast to devices, where model-based approaches and physical simulation are central [Ta18] the human digital twin focuses on the empirical, statistical investigation of behavior [Ha20]. Simulations may be possible in cases such as medical applications, based on biological rather than physical processes [Ch19].

Derived knowledge results from this processing, is also stored in the digital twin and can in turn serve as input for subsequent processing steps. In particular, a derivation of user objectives and preferences from observations is possible [Ha20]. Derived events, as specified in C2PS [AE17], form a subset of the broader knowledge about users that a human digital twin can derive, which also includes

[3] Short for "cloud-based cyber-physical systems" [AE17], referring to a digital twin architecture reference model for such systems [AE17]

e.g. location types [KBB18] and user preferences [Ro14].

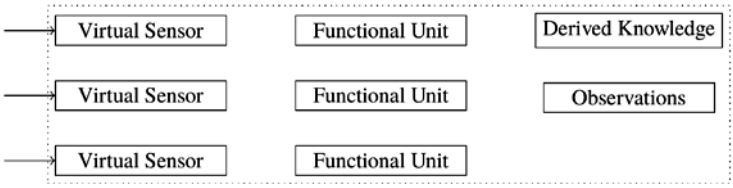


Fig. 1: Human digital twin reference architecture (adapted from [AE17])

In contrast to the device centric C2PS [AE17], a human digital twin does not contain virtual actuators or virtual power supply. The reasons for this are evident: The information system can observe but not control the human being, and the human being does not need to be powered by the electrical system.

Similarly, also in contrast to devices, direct communication between people on the physical level is outside the boundaries of the technical system. Therefore, we assume that the implementation of human digital twins leverages the transmission of observations of user attributes and derived knowledge via virtual connections in the sense of C2PS, which corresponds to federated identity management [Ro14].

3 Fields of Application

3.1 Smart Home

In Smart Home applications, a human digital twin helps to observe and simulate the actions and behavior of residents, guests and other visitors like craftsmen, living or working in the Smart Home environment for a finite timeframe. For this purpose, various sensors, like cameras, motion or pressure sensors may capture relevant data of the people in the home. Further sensors like thermostats, humidity or sound sensors, can measure additional environmental data of the Smart Home. Sensors and electrical switches on lights and the other Smart Home devices record the current state of the devices as well as modifications made by the residents or visitors. The data of the people in the Smart Home environment and the data of the environment itself is necessary in order to gain knowledge about the preferences and behavior of the people in the environment as well as to be able to derive further knowledge about the context of specific situations. Additionally, residents can provide additional context information like data from a personnel calendar or personal preferences like color preferences of the lighting conditions.

Using the captured data in the digital twin, the Smart Home can derive context information, i.e. whether a specific person entering the home is identified and subsequently classified as a resident, guest or an unauthorized person. Additionally, it can use the data to provide general and personalized services or to adjust parameters like

room lighting, temperature of a room or the sound volume of devices within the environment to the preferences of one person or even several people in a specific room. Electrically adjustable furniture or appliances can also be adjusted to the required settings or physical needs of an individual or a group of people.

The Smart Home system can use the data about the environment or individuals to learn detecting special contexts or even (medical) emergencies in order to provide special services or to call for assistance. Furthermore, the Smart Home could implement preventive measures, e.g. recommending and supporting a diet for individual residents when detecting weight problems and support individuals in forming healthier (sleeping) habits by adjusting the living environment accordingly

To provide these services and adjust the environment to the needs and preferences of the residents and visitors or to detect the context, the Smart Home system needs to collect a variety of general and personal data from the people within the environment and the environment itself. The collected data has a high risk of abuse if access is not carefully managed and secured. Identification of individuals at the location or data related to medical condition are prominent examples of this risk. Evidently, the personal data, but also the environmental data is very sensitive and should be carefully managed and safeguarded.

The Smart Home system also needs to implement a concept to manage the data transfer between residents and visitors. Disclosure of private data has to be avoided. This also includes actions allowing individuals in the environment to derive personal information about other individuals in the environment, e.g. showing the weight in the smart mirror in the bathroom to a visitor or displaying private appointments to other residents.

3.2 Smart Building

Similar to the application in a Smart Home environment, the concept of a digital twin can be expanded on and subsequently applied to operate smart buildings. However, the focus and central point of the data collection is the individual residing in the building. A smart building constantly produces valuable data, which in combination with the data captured in the human digital twin, can act as decision support for human or machine-operated systems using rule engines or artificial intelligence. The derived knowledge can then be used to adjust various parts of the building's infrastructure automatically. Several useful applications and benefits of the combination of human digital twins in smart buildings are listed below:

Energy Efficiency

By locating and identifying residents inside the building and thereby identifying rooms that are currently occupied and other facilities in use, the controlling system could dynamically adjust the heating, ventilation or lightning conditions, so that energy resources are efficiently used and managed according to the current requirements.

Individual preferences as well as environmental context data could also be taken into account, to adjust the building conditions to an optimal level.

Automation

The digital twin can enable highly individual but at the same time and transparent forms of building automation by using real time and historic information about occupants as well as the infrastructure and resources. Repetitive or context sensitive tasks like i.e. turning on sprinklers or moving shades according to certain rules or lightning conditions could be easily monitored and configured.

Access Control

Using and combining the captured and derived knowledge about building infrastructure, occupants' location information as well as their respective security clearance levels stored in the digital twin, a control system could automatically grant or deny access to certain resources, facilities, appliances or parts of the buildings in a secure, transparent and convenient manner.

Predictive Maintenance

Similarly, to smart production environments, the context information about building infrastructure and various appliances or machinery in combination with a human digital twin can be used to quickly detect and subsequently repair malfunctions by informing responsible personnel. Furthermore, by using historical data and machine learning, the data can be used to predict were failures or malfunctions are most likely to happen in the future.

3.3 Smart Office

Smart Office systems implement applications from Smart Buildings for energy efficiency as well as security and cost improvements. Additionally, Smart Office solutions contain similar applications like Smart Homes in order to create a pleasant, healthy and motivating working environment. Using a human digital twin in this context can benefit a Smart Office concept by providing additional historic and real time context information to be used to create smart and adaptive office environments.

A Smart Building system, which integrates the Smart Office environment, enables applications like the regulation of heating, lights or air conditioning depending on the number of people in a room. Airing or heating of (meeting) rooms can be prepared in advance, based on contextual data like calendar entries for a room in the booking system of the Smart Office.

Waiting times for elevators can be optimized by analyzing the data of different sensors and predicting the demands on the different floors of the building.

Smart Office environments, which are usually integrated into Smart Buildings, also provide access control systems to control and monitor the access to the building itself or to single departments. Additionally, Smart Offices provide services like the optimization of the utilization of technical infrastructure like servers and other (network) components.

Similar to Smart Home environments, Smart Offices provide applications and services to improve the motivation, work satisfaction and overall well-being of employees and preventing certain illnesses. Examples for such services are the personalization of room settings, e.g. light color, music or room scent, based on the personal preferences of the persons in a room. Functionalities like the automated adjustment of height settings of furniture like tables or chairs depending on the height of the person, who is using it, create an ergonomic office environment in order to avoid postural defects and accompanying diseases.

In summary, the application and utilization of digital twins in smart environments such as smart homes, smart buildings or smart offices offers various benefits and advantages over previous systems. The usage of personal and context related data of individuals, stored and processed in the digital twin can lead to better, more personalized, safer and more efficient applications and use cases of smart environments powered by IoT devices.

4 Identity Management and Data Protection Functions

As described in section 2, human digital twins clearly leverage virtual connections in the sense of C2PS's reference architecture. Thus, we assume identity information, such as observations from sensors and other inputs as well as derived knowledge is transmitted between the digital twins, and not between humans or devices on the physical layer. Standard federated identity management protocols, such as OpenID Connect or SAML are suitable for this [Ro14]. The information can be linked to an identifier of the specific human digital twin to enable traceability. The human digital twin can also enable pseudonymization, acting as a privacy-protecting identity intermediary [Ra07] in such a case. This also enables mapping between distributed clusters of human digital twins with different identifier regimes. Information can also be de-aggregated or even anonymized by functional units within the human digital twin [Ra07].

In general, it is notable that human digital twins are especially suitable for enabling key data protection goals via their functional components, leveraging the holistic perspective on users' personal information immanent in the paradigm. To illustrate this, consider the implementation of the privacy dashboard pattern for information in a human digital twin depicted in Figures 2 and 3.

Privacy dashboard are widely used for offering transparency, intervenability, and accountability for users' personal information in corporations' systems [ZAM14], and thus support the majority of privacy goals [HJR15]. As the digital twin gives access to

both all observations and derived knowledge about a user, and functions to modify this information, all that is needed is an interface connecting the dashboard frontend to the human digital twin's functional units and data stores. The functions in such a privacy interface would include retrieving observations and/or derived information about a user from a digital twin's data stores. The interface also connects to the digital twin's functional modules for updating the information – or at least correcting it, if it is wrong, and deleting personal information on request of the user – or at least blocking it in case deletion is not feasible [ZHK19].

In scenarios where personal information is not linked to identifiers, human digital twins can be equipped with functionality to identify users from observations about them, in essence making the instance of human digital twin an observation is assigned to and associated identifier derived knowledge in the sense of the reference architecture. For example, a system can use biometrics based on camera information to identify a user, and then direct observations from other sensors also capturing information about the user to the appropriate human digital twin. This can enable more precise analytics, but can also improve users' privacy as it enables targeted transparency, enabling e.g. a dashboard implementation that does not give all users access to all information [ZAM14], which is a privacy issue in itself.

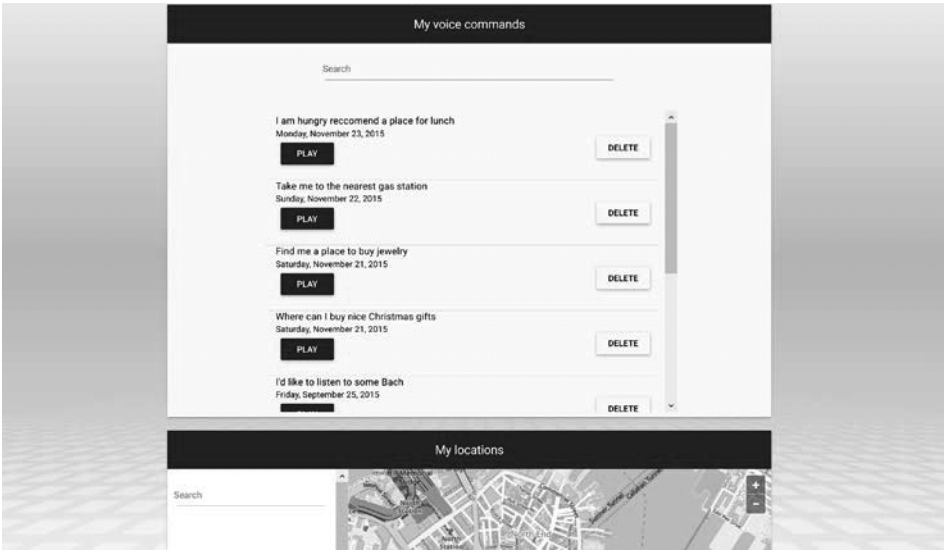


Fig. 2: Privacy dashboard for observations stored in a human digital twin

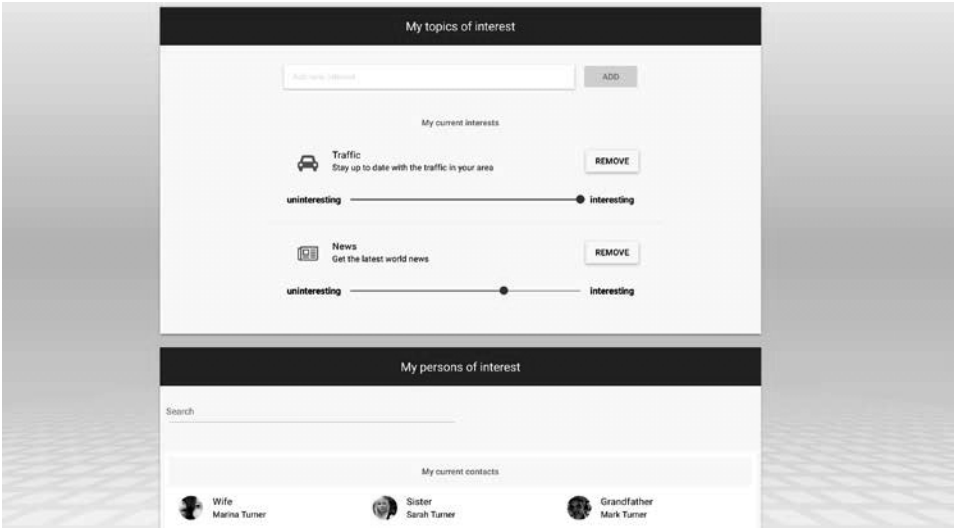


Fig. 3: Privacy dashboard for derived knowledge stored in a human digital twin

Beyond that, digital twins have also been successfully used for anomaly detection [GV17]. Human digital twins could likewise be used to spot unauthorized access to information or physical assets, or to detect anomalous human behaviour indicative of health issues, a common use case in ambient assisted living [Ja17].

5 Discussion

While a human digital twin for end users is a promising concept, some complexities are foreseeable in practice, leaving room for further research. In consumer scenarios such as home automation, a fragmentation of the digital twin by silos of different manufacturers [Ja17] is to be expected. Unlike in industrial and building scenarios, there is no obvious integrator role. This could coincide with the building management; it could be the end user, a device manufacturer, or a dedicated integrator. This also causes challenges in interoperability. The use cases implemented by intelligent home automation vary greatly for different manufacturers [Ja17], which makes it difficult to define certain functional components and data using the reference presented here, and calls into question whether we can reach semantic interoperability before the features offered by such systems have converged.

In many instances, a human digital twin in the field of intelligent household appliances poses significant data protection challenges, as an integrated representation can involve aggregating raw data from the most intimate spaces. As we described, they also enable a high degree of data sovereignty. Collected information is bound to be critical personal information, thus, data minimization and unlinkability, the protection goals not

addressed by privacy dashboards, should be a target of system design. Depending on the characteristics of the integrator and the implemented use cases, different approaches are conceivable here. Therefore, solutions addressing the issue are out of the scope of this reference architecture.

Summing up, digital twins are a proven concept in networked production systems, which as we illustrated also holds a lot of promise for the field of intelligent home automation. Human digital twins are a logical extension of the concept, and address core challenges in the Internet of Things, enabling various use cases, interoperability, and key privacy functions.

Bibliography

[AE17] Alam, K.M.; El Saddik, A.: C2PS: A Digital Twin Architecture Reference Model for the Cloud-Based Cyber-Physical Systems. IEEE Access 5, pp. 2050– 2062, 2017.

[Ba19] Bauer, J.; Hoffmann, H.; Feld, T.; Runge, M.; Hinz, O.; Mayr, A.; Förster, K.; Teske, F.; Schäfer, F.; Konrad, C.; Franke, J.: ForeSight - Platform Approach for Enabling AI-based Services for Smart Living. In: How AI Impacts Urban Living and Public Health. Bd. 11862, Springer International Publishing, Cham, pp. 204–211, 2019.

[Ch19] Chakshu, N.K.; Carson, J.; Sazonov, I.; Nithiarasu, P.: A semi-active human digital twin model for detecting severity of carotid stenoses from head vibration—A coupled computational mechanics and computer vision method. International Journal for Numerical Methods in Biomedical Engineering 35/5, 2019.

[GV17] Grieves, M.; Vickers, J.: Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. In: Transdisciplinary Perspectives on Complex Systems. Springer International Publishing, Cham, pp. 85–113, 2017.

[Ha20] Hafez, W.: Human Digital Twin: Enabling Human-Multi Smart Machines Collaboration. In: Intelligent Systems and Applications. Bd. 1038, Springer International Publishing, Cham, pp. 981–993, 2020.

[He16] Hernández-Serrano, J.; Muñoz, J.L.; Bröring, A.; Esparza, O.; Mikkelsen, L.; Schwarzott, W.; León, O.; Zibuschka, J.: On the Road to Secure and Privacy-preserving IoT Ecosystems. In: Interoperability and Open-Source Solutions for the Internet of Things. Springer, Cham, pp. 107–122, 2016.

[HJR15] Hansen, M.; Jensen, M.; Rost, M.: Protection Goals for Privacy Engineering. In: 2015 IEEE Security and Privacy Workshops, San Jose, CA, pp. 159-166, 2015.

[Ja17] Jakobi, T.; Ogonowski, C.; Castelli, N.; Stevens, G.; Wulf, V.: The Catch(es) with Smart Home: Experiences of a Living Lab Field Study. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. ACM Press, pp. 1620–1633, 2017.

[Kh19] Khajavi, S.H.; Motlagh, N.H.; Jaribion, A.; Werner, L.C.; Holmstrom, J.: Digital Twin: Vision, Benefits, Boundaries, and Creation for Buildings. IEEE Access 7, pp. 147406–147419, 2019.

[KBB18] Karatzoglou, A.; Koehler, D.; Beigl, M.: Purpose-of-Visit-Driven Semantic Similarity Analysis on Semantic Trajectories for Enhancing The Future Location Prediction. In: 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Athens, pp. 100-106, 2018.

[KHB18] Klostermeier, R.; Haag, S.; Benlian, A.: Digitale Zwillinge – Eine explorative Fallstudie zur Untersuchung von Geschäftsmodellen. HMD Praxis der Wirtschaftsinformatik 55/2, pp. 297–311, 2018.

[Ra07] Radmacher, M.; Zibuschka, J.; Scherner, T.; Fritsch, L.; Rannenberg, K.: Privatsphärenfreundliche topozentrische Dienste unter Berücksichtigung rechtlicher, technischer und wirtschaftlicher Restriktionen. In: Wirtschaftsinformatik (1), pp. 237-254, 2007.

[Ro14] Roßnagel, H.; Zibuschka, J.; Hinz, O.; Muntermann, J.: Users' willingness to pay for web identity management systems. European Journal of Information Systems 23/1, pp. 36–50, Jan. 2014.

[Ta18] Tao, F.; Cheng, J.; Qi, Q.; Zhang, M.; Zhang, H.; Sui, F.: Digital twin-driven product design, manufacturing and service with big data. The International Journal of Advanced Manufacturing Technology 94/9-12, pp. 3563–3576, Feb. 2018.

[ZHK19] Zibuschka, J.; Horsch, M.; Kubach, M.: The ENTOURAGE Privacy and Security Reference Architecture for Internet of Things Ecosystems. In: Open Identity Summit 2019. Gesellschaft für Informatik, Bonn, pp. 119–130, 2019.

[ZAM14] Zimmermann, C.; Accorsi R.; Müller, G.: Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy. In: 2014 Ninth International Conference on Availability, Reliability and Security, Fribourg, pp. 152-157, 2014.

H. Roßnagel, C.H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 143

IoT Device Profiling: From MUD Files to S×C Contracts

Guðni Matthíasson [1], Alberto Giaretta [2], Nicola Dragoni [3]

Abstract: Security is a serious, and often neglected, issue in the Internet of Things (IoT). In order to improve IoT security, researchers proposed to use Security-by-Contract (S×C), a paradigm originally designed for mobile application platforms. However, S×C assumes that manufacturers equip their devices with security contracts, which makes hard to integrate legacy devices with S×C. In this paper, we explore a method to extract S×C contracts from legacy devices' Manufacturer Usage Descriptions (MUDs). We tested our solution on 28 different MUD files, and we show that it is possible to create basic S×C contracts, paving the way to complete extraction tools.

Keywords: Internet of Things; S×C; Security-by-Contract; MUD; Manufacturer Usage Description; Device profiling

1 Introduction

The Internet of Things (IoT) is becoming more and more pervasive in our society. With the increasing number of connected devices come additional security risks. IoT devices are usually simple and resource constrained, which also means that they tend to have a limited capacity for security routines. Moreover, in order to gain market shares, manufacturers tend to prioritise easily perceivable features over security [DGM18]. As a result, hackers have been targeting IoT devices for various purposes: distributed denial-of-service (DDoS) attacks [Go], cryptocurrency mining [An], espionage, and many others [Hi]. These types of attacks are expected to become more common as the IoT expands.

Security-by-Contract (S×C) is a promising paradigm for mitigating some IoT security issues. Originally proposed for mobile applications [Dr07], S×C envisions devices that carry security contracts, easy to validate and verify against network security policies [GDM19b]. The S×C framework utilises the fog computing paradigm, which extends the concept of cloud computing by adding a middle layer between the end devices and the cloud. Practically, this middle layer consists of fog nodes, machines dedicated to data aggregation and data processing. Fog nodes are distributed and localised, allowing lower latency for time-sensitive tasks with respect to the cloud. They also provide a more local and controlled storage

[1] Technical University of Denmark (DTU), Department of Applied Mathematics and Computer Science, Anker Engelunds Vej 1, 2800 Kgs. Lyngby, Denmark s190064@student.dtu.dk
[2] Örebro University, AASS Research Centre, Fakultetsgatan 1, 702 81 Örebro, Sweden alberto.giaretta@oru.se
[3] Technical University of Denmark (DTU), Department of Applied Mathematics and Computer Science, Anker Engelunds Vej 1, 2800 Kgs. Lyngby, Denmark and Örebro University, AASS Research Centre, Fakultetsgatan 1, 702 81 Örebro, Sweden ndra@dtu.dk

location for sensitive data. In the fog computing paradigm, the cloud can still be used for less time-sensitive and security-sensitive operations. These features make fog computing especially useful for IoT networks where latency and data security are important. They also make fog nodes ideal for security-critical roles within a network.

When a new device first connects, it provides a fog node with a contract formally describing its intended behaviour on the network, denoted as a list of security rules. An example of such a rule for a Philips Hue White smart lighting system can be seen in Tab. 1. This rule allows other Philips devices to access its *On*, *Bri* and *Hue* services, and requires access to the HueMotion *Presence* service over the local area network (LAN).

	Rule R_{B1}
D	PHILIPS.HUEWHITE
DOM	LAN
SHARES	PHILIPS.*
PROVIDES	ON, BRI, HUE
REQUIRES	PHILIPS.HUEMOTION.PRESENCE

Tab. 1: A security rule for the Philips Hue White smart lighting system [GDM19a]

Similarly, a security policy is a set of rules which describes the behaviours allowed within the network. In S×C, fog nodes act as security gateways on the local network. They are responsible for verifying and validating contracts, as well as for maintaining and enforcing the security policy. Upon receiving a device contract, the fog node validates it against the existing security policy. The validation phase checks the contract for inconsistencies and tests if the rules violate the existing security policy; if the contract is valid, the fog node adds the rules to the policy. This helps to ensure an up-to-date, specific, and internally consistent security policy, providing a good basis for identifying abnormal behaviour on the network.

Contribution of the Paper In an ideal world, manufacturers would produce contracts and store them in their devices, and this is not a realistic short-term goal. We have to face thousands of devices on the market which cannot naturally comply with S×C. But a growing number of these devices are compliant with the Manufacturer Usage Description (MUD) specification [LDR19], an Internet Engineering Task Force (IETF) standard which allows devices to signal to the network their requirements in order to work properly. As shown in Fig. 1, we propose a method for integrating MUD-compliant devices with an S×C framework. Our approach is based on extracting S×C contracts from MUD definitions, by means of access control list (ACL) analysis, Dynamic Host Configuration Protocol (DHCP) fingerprints and queries to the Fingerbank application programming interface (API).

For S×C to achieve widespread use, we need a way for analysing a device behaviour, before we can generate a suitable contract and grant network access. The S×C framework shows great promise in terms of sustainable security on a local network, but in its current state it

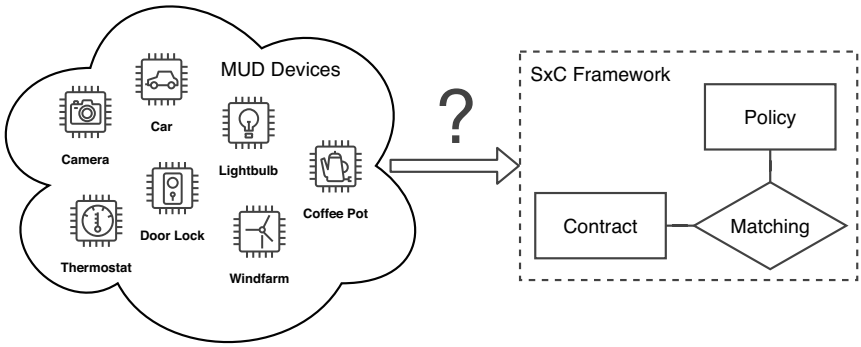


Fig. 1: MUD-compliant devices are growing in number. How can we integrate such devices with an S×C framework? We need a method for extracting S×C contracts from MUD definitions.

requires drastic additions to the development and manufacturing processes of IoT devices. Through an experiment performed on 28 different MUD files, we show that it is possible to extract basic S×C contracts from MUD ACL specifications. Even though the resulting contracts are partial, our work paves a promising way for profiling MUD devices and extracting complete S×C contracts.

Paper Outline The paper is organised as follows. In Sect. 2 we give an overview of related work. In Sect. 3 we present our proposal for extracting S×C contracts from MUD files, and in Sect. 4 we evaluate our results. Limitations and next steps to achieve complete S×C contracts are discussed in Sect. 5. Last, in Sect. 6 we draw our conclusions.

2 Related Work

MUD is a standard meant to allow devices to describe their requirements in order to function properly. A MUD file describes the types of communication a device establishes under normal operating conditions. Namely, it provides access control lists for both inbound and outbound communication, grouped by protocols. According to the standard, a MUD file is hosted on servers run by the device manufacturer, and the device stores a link to its MUD file as a DHCP option [LDR19].

MUD strives to achieve similar goals as S×C, but it does not go as far in describing device-based communication patterns. It also differs from S×C in that the MUD file is not provided directly by the device, but rather by an online server. Thus, an internet connection is required for MUD to function. The research community anticipated issues similar to those described in Sect. 1 and Hamza et al. [Ha18] came up with a way of generating MUD

files for devices from behavioural analysis. In their work, they collected packets for 28 IoT devices over 6 months and produced the related proof-of-concept MUD files [Ha].

DHCP is a protocol for dynamically assigning IP addresses to network devices. The protocol specifies several parameters for the initial *DHCP DISCOVER* packet including option 55, the Parameter Request List, which allows a device to request configuration information from the DHCP server [Al].The specific information fields requested, and the order in which they are listed, are usually manufacturer- and often device-specific. To the degree that it is commonly referred to as a *DHCP fingerprint*. Fingerbank is an online database that collects DHCP fingerprints and pairs them with device profiles which contain useful information, such as the device name and manufacturer. It offers an API that allows a user to query the database with DHCP DISCOVER packet data and replies with the relevant device information [Fi].

Thomsen [Th19] proposed a method of determining the device type (lamp, speaker, etc.) using a Random Forest Machine-Learning algorithm. His research included extracting information from MUD files for the purpose of this classification. Thomsen's approach to MUD-based device type classification revolved around the MUD file *systeminfo* field. This identifier was used as a query string for an online search. The results of the search were scraped for text, which was then fed to the classification algorithm. The *systeminfo* field is the only information from the MUD files utilised in the classification process. This paper investigates what other relevant information can be extracted from the MUD files and to what degree contracts can be generated based on that information.

Several papers have been published on the topic of profiling IoT device behaviour on a network outside the context of S×C. Notable examples include IoT SENTINEL by Miettinen et al. [Mi17], IoTSense by Bezawada et al. [Be18] and AuDI (Autonomous IoT Device-Type-Identification) by Marchal et al. [Sa19]. All of these solutions include allowing a new device to connect and passively observing its behaviour after the fact. This approach may be required to assemble a complete profile for an unknown device but it does represent a compromise in the pursuit of preemptive profiling. The insights provided by the aforementioned research are not discussed in individual detail in this paper, but instead recommended as potentially useful methods for further progress along this line of research.

3 From MUD Files to S×C Contracts

As aforementioned, in this paper we decided to focus on MUD files. The choice was driven by three main reasons:

1. MUD is designed for different environments, from home networks to larger ones. It is reasonable to assume that MUD will become widely adopted in the future.
2. Hamza et al.[Ha18] showed a reliable method for generating MUD profiles for non-MUD devices.

3. Even though MUD does not provide enough information to build a full security contract, it gives helpful information about the devices' expected communications.

For the purposes of this research, the main point of interest in MUD files are their ACL specifications. ACLs provide information on communication patterns, including domain names (in the case of Internet communication), as well as ports and protocols involved. The first question is: are MUD ACLs enough to create an S×C contract? The information required for building complete S×C contracts is:

1. Device name and manufacturer
2. Domain of communication (LAN/internet)
3. List of devices which the device can communicate with
4. List of services provided and required
5. ACL in terms of identified devices and services

Manufacturer and device names are not stored in the MUD file but they can be retrieved by feeding DHCP fingerprints to the Fingerbank API. Also, MUD ACLs provide a list of source and destination ports used for LAN and internet communications. However, with MUD devices we miss the services required and provided, as well as a list of other devices which the device can communicate with. MUD is not sufficient to construct complete security contracts for S×C, but it provides useful information. The goal of our work is to see how much useful data we can extract from the 28 MUD ACLs provided by Hamza et al. [Ha18].

3.1 Implementation

The first step was to create a fork of Thomsen's codebase [Th19]. Additional code was then written to break up and extract information from the MUD ACLs [Ma].We determined that the following information could be reliably extracted: ports used for communication, grouped by LAN/internet and local/remote, and domains communicating with the device over the internet, grouped by inbound/outbound.

The profiling solution, depicted in Fig. 2, consists of the following steps:

1. **Receive DHCP DISCOVER request containing MUD URL**
2. **Extract DHCP fingerprint, user-agent string, media access control (MAC) address and MUD URL** This info is included in the DHCP DISCOVER packet.
3. **Query the Fingerbank API for manufacturer and device names using the extracted client information** The API accepts a DHCP fingerprint, user-agent string and MAC address.

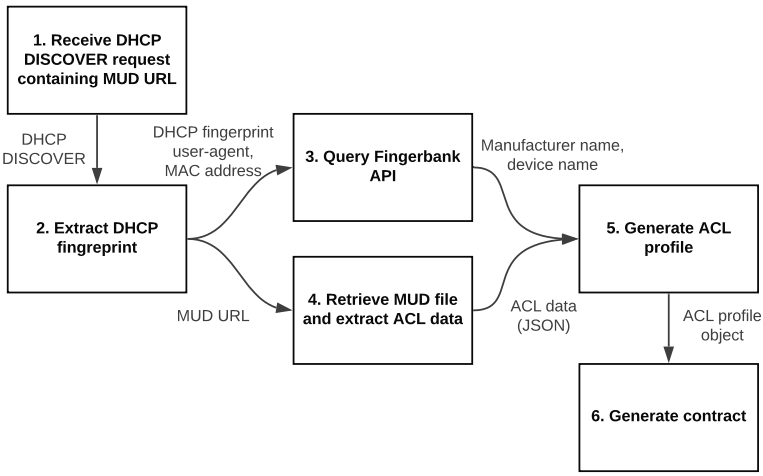


Fig. 2: This workflow shows our proposed approach for extracting S×C contracts from MUD ACLs.

4. **Retrieve MUD file from extracted URL and extract the ACLs** We made some base assumptions about the ACL data: 1) each local port represents a provided service and 2) each remote port represents a required service.
5. **Generate an ACL profile object using manufacturer name, device name, and ACLs** We defined a data model class, the ACL profile, to encapsulate relevant ACL information, along with functionality to instantiate such objects from raw ACL data. The protocols used are also available for extraction, but it is unclear how they would help in constructing contracts for S×C, so they were not included in this model.
6. **Generate a contract object using the ACL profile object** We defined a second data model class, the contract, to represent a security contract, complete with functionality to instantiate contracts from ACL profile objects.

4 Evaluation

For the purpose of testing this functionality, we decided to use unique identifiers, acquired by manually looking up each device, for Fingerbank API lookups. This was necessary due to the lack of physical devices to test and scarcity of raw DHCP fingerprint examples readily available online. Because of this, we were unable to determine the reliability of identifying device and manufacturer names with DHCP fingerprint lookups. We wrote a script to run the modified MUD profiling solution on each of the 28 MUD files provided.

```
Device type:            Camera
Classification score:   0.17817759870529015
Name:                   Belkin.NetCam
Mud file ACLs:
Security contract Belkin.NetCam:
        Rule Belkin.NetCam.all:
                Device:     Belkin.NetCam
                Domain:     *
                Shares:     *
                Provides:   {'5104'}
                Requires:   {'5104'}
        Rule Belkin.NetCam.lan:
                Device:     Belkin.NetCam
                Domain:     LAN
                Shares:     *
                Provides:   {'67', '3478', '53'}
                Requires:   {'67', '3478', '1900', '53'}
        Rule Belkin.NetCam.net:
                Device:     Belkin.NetCam
                Domain:     Internet
                Shares:     *
                Provides:   ['443', '8443', '8899', '123', '3475']
                Requires:   ['443', '8443', '8899', '123', '3475']

Contact domains:
        nat.xbcs.net
        api.xbcs.net
        [..]
```

Fig. 3: Test output for a Belkin Camera device

Fig. 3 shows a test output example for a Belkin camera device. The generated partial contract represents the following communication profile:

- The camera communicates on port 5104 over both LAN and the internet.
- The camera communicates on ports 53, 67 and 3478, and transmits to remote port 1900 over LAN.
- The camera communicates on ports 8899, 123, 3475, 8443 and 443 over the internet.

The raw test output can be found on the GitHub repository [Ma].As stated in Sect. 3, the basic ACL data also contains information on the domains contacted over the internet, as well as the protocols used. We excluded the protocols from the basic contract model for simplicity. Sect. A presents the results in a condensed format where the domain names identified are omitted. Instead, the number of domain names extracted from the MUD ACLs is specified along with the list of identified ports used by each device for inbound and outbound communication, on the local network and the internet.

This data may be used to define enforceable security policies on a network, by putting restrictions on which external domains can contact a device, using which ports and protocols, and which ports can be used for local network communication. However, this is not enough for describing devices' behaviour to the degree required by S×C contracts.

5 Future Work

The contracts we produced with our method can be used to achieve a basic behavioural whitelist. But they do not encompass the entire behavioural profile of a device. There is a question left: how can we improve our output S×C contracts? Based on our results, we suggest two potential approaches:

1. Define a general contract for each device type, select for every new device the appropriate contract based on the type classification, and use MUD ACL data to narrow it down.
2. Add an intermediate, *tentative* state to the S×C process. A new device is granted access to the network, limited by the MUD ACL, while additional profiling takes place and a valid contract is generated.

The first option would define which external domains the device could communicate under standard conditions. This could provide the S×C fog node with a baseline for identifying abnormal communications, but it would not be perfect. For example, this approach might produce contracts too general, granting unnecessary permissions. The second option would produce better contracts, as the data described in Sect. 4 would be enhanced with observed network data, allowing device-specific and service-specific permissions. But it would also require the S×C fog node to actively monitor new devices communications while they are in this *tentative* access state, increasing the computational burden.

Both options could also be combined, whereby a temporary contract could be created by augmenting an existing general type-specific contract for the analysis period. During this period, a more specific contract could be generated based on a more thorough and sophisticated behaviour analysis. Methods for such analysis are rapidly emerging, as mentioned with some notable examples in Sect. 2.

6 Conclusion

The market demand for IoT devices has considerably outpaced the development of secure IoT solutions. Security-by-Contract (S×C) attempts to improve the IoT shortcomings, with respect to security configurability and lacking behavioural descriptions. At the time of writing, one issue S×C has to face is its compatibility with existing technology. In this paper,

we presented Manufacturer Usage Description (MUD), an IETF standard which describes basic requirements for compliant IoT devices. Within MUD files, we identified information for extracting S×C contracts, and integrating MUD-compliant devices in S×C frameworks.

Then, we proposed a method to extract such information and, in order to verify our hypothesis, we applied this method to 28 different MUD files. Our experiment shows that it is possible, indeed, to extract some useful information for basic S×C contracts. However, we show that our method outputs only partial S×C contracts. We have also identified two potential methods for extracting valid and useful S×C contracts for previously unknown devices. Both include the approximation of a valid contract from ACLs, device type, and further behaviour analysis.

With the increase in resource-constrained IoT devices on the market, we are facing an increase in attack surface. This presents a huge challenge for cybersecurity, but the growing research on IoT security is promising for the future of the Internet.

Appendix A Test results

MUD File	S×C Device	LAN		Internet		# Dom.
amazonEcho	Amazon.Echo	5353	O	33434	I/O	20
		1900	O	443	I/O	
		67	I/O	123	I/O	
		53	I/O	89	I/O	
augustdoorbellcam	August.DoorBellCamera	67	I/O	443	I/O	19
		53	I/O			
		547	I/O			
awairAirQuality	Awair.R2	67	I/O	8883	I/O	3
		53	I/O	443	I/O	
belkincamera	Belkin.NetCam	5104	I/O	8899	I/O	8
		3478	I/O	8443	I/O	
		1900	O	5104	I/O	
		67	I/O	3475	I/O	
		53	I/O	443	I/O	
				123	I/O	
blipcareBPmeter	BLIP.Systems	67	I/O	8777	I/O	1
		53	I/O			
canaryCamera	Canary.All-in-One	67	I/O	443	I/O	8
		53	I/O	80	I/O	
chromecastUltra	Google.ChromecastUltra	5353	O	5228	I/O	37
		1900	O	443	I/O	
		67	I/O	123	I/O	
		53	I/O	80	I/O	
dropcam	Nest.Camera	67	I/O	443	I/O	4
		53	I/O	123	I/O	
hellobarbie	Nabi.BarbieTablet	67	I/O	443	I/O	3
		53	I/O			

MUD File	S×C Device	LAN		Internet		# Dom.
hpprinter	HP.Printer	5355	O	5223	I/O	3
		5353	O	5222	I/O	
		547	I/O	443	I/O	
		137	O	80	I/O	
		67	I/O			
		53	I/O			
HueBulb	Philips.PhilipsHueSmartlighting	5353	O	443	I/O	12
		1900	O	123	I/O	
		67	I/O	80	I/O	
		53	I/O			
ihomepowerplug	iHome.SmartPlug	5353	O	443	I/O	2
		67	I/O	80	I/O	
		53	I/O			
lifxbulb	LIFX.lighting	56700	O	56700	I/O	2
		67	I/O	123	I/O	
		53	I/O			
nestsmokesensor	Nest.Smoke+COAlarm	67	I/O	11095	I/O	46
		53	I/O			
NetatmoCamera	Netatmo.Camera	67	I/O	4500	I/O	12
		53	I/O	500	I/O	
				443	I/O	
				123	I/O	
				80	I/O	
NetatmoWeatherStation	Netatmo.PersonalWeatherStations	67	I/O	25050	I/O	1
		53	I/O			
pixstarphotoframe	Pix-Star.WiFiFrame	138	O	443	I/O	2
		137	O	80	I/O	
		67	I/O			
		53	I/O			
ringdoorbell	Ring.Doorbell	67	I/O	9998	I/O	4
		53	I/O	443	I/O	
				123	I/O	
				80	I/O	
samsungsmartcam	Samsung.IPCamera	5353	O	5222	I/O	5
		1900	O	443	I/O	
		67	I/O	123	I/O	
		53	I/O			
SmartThings	Samsung.SmartThings	1900	O	443	I/O	3
		67	I/O	123	I/O	
		53	I/O			
tplinkcamera	TP-Link.IPCamera	5353	O	3478	I/O	6
		67	I/O	443	I/O	
		53	I/O	123	I/O	
				80	I/O	
tplinkplug	TP-Link.HS100	67	I/O	50443	I/O	11
		53	I/O	123	I/O	

MUD File	S×C Device	LAN		Internet		# Dom.
tribyspeaker	Invoxia.SmartPortableSpeaker	5353	O	10003	O	14
		67	I/O	10002	I/O	
		53	I/O	8090	I/O	
				5228	I/O	
				443	I/O	
				123	I/O	
				80	I/O	
wemomotion	Belkin.WeMo	1900	O	8899	I/O	3
		123	I/O	8443	I/O	
		67	I/O	3478	I/O	
		53	I/O			
wemoswitch	Belkin.SmartHome	1900	O	8443	I/O	2
		3478	I/O	3475	I/O	
		123	I/O			
		67	I/O			
		53	I/O			
withingsbabymonitor	Withings.SBM	5353	O	1935	I/O	7
		67	I/O	80	I/O	
		53	I/O			
withingscardio	Nokia.-WithingsIoT	67	I/O	443	I/O	1
		53	I/O			
withingssleepsensor	Withings.AURA	5353	O	443	I/O	1
		67	I/O	80	I/O	
		53	I/O			

References

[Al] Alexander, S.: RFC 2132, `https://tools.ietf.org/html/rfc2132`, Accessed: 2020-04-09.

[An] Anonymous: Linux Worm targets Internet-enabled Home appliances to Mine Cryptocurrencies, `https://thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html`, Accessed: 2020-04-09.

[Be18] Bezawada, B. et al.: Behavioral Fingerprinting of IoT Devices. In: Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security. ASHES '18, Association for Computing Machinery, Toronto, Canada, pp. 41–50, 2018, ISBN: 9781450359962, URL: `https://doi.org/10.1145/3266444.3266452`.

[DGM18] Dragoni, N.; Giaretta, A.; Mazzara, M.: The Internet of Hackable Things. In: Proceedings of 5th International Conference in Software Engineering for Defence Applications. Springer International Publishing, Rome, Italy, pp. 129–140, 2018, ISBN: 978-3-319-70578-1.

[Dr07] Dragoni, N. et al.: A Security-by-Contract Architecture for Pervasive Services. In: Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007). IEEE, pp. 49–54, 2007.

[Fi] Fingerbank: Device Fingerprints, https://fingerbank.org/, Accessed: 2020-04-09.

[GDM19a] Giaretta, A.; Dragoni, N.; Massacci, F.: IoT Security Configurability with Security-by-Contract. eng, Sensors (Basel, Switzerland) 19/19, Sept. 2019.

[GDM19b] Giaretta, A.; Dragoni, N.; Massacci, F.: Protecting the Internet of Things with Security-by-Contract and Fog Computing. In: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, Limerick, Ireland, pp. 1–6, Apr. 2019, ISBN: 978-1-5386-4980-0, URL: https://ieeexplore.ieee.org/document/8767243/, visited on: 10/08/2019.

[Go] Goodin, D.: Record-breaking DDoS reportedly delivered by >145k hacked cameras, https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/, Accessed: 2020-04-09.

[Ha] Hamza, A.: MUD Profiles, https://iotanalytics.unsw.edu.au/mudprofiles, Accessed: 2020-04-09.

[Ha18] Hamza, A. et al.: Clear as MUD: Generating, Validating and Applying IoT Behavioral Profiles. In: Proceedings of the 2018 Workshop on IoT Security and Privacy. IoT S&P '18, Association for Computing Machinery, Budapest, Hungary, pp. 8–14, 2018, ISBN: 9781450359054, URL: https://doi.org/10.1145/3229565.3229566.

[Hi] Hill, K.: Baby Monitor Hacker Still Terrorizing Babies And Their Parents, https://www.forbes.com/sites/kashmirhill/2014/04/29/baby-monitor-hacker-still-terrorizing-babies-and-their-parents/, Accessed: 2020-04-09.

[LDR19] Lear, E.; Droms, R.; Romascanu, D.: Manufacturer Usage Description Specification. Published: RFC 8520, RFC Editor, 2019.

[Ma] Matthíasson, G.: DBAC Device Detection, https://github.com/gdnoz/DBAC-Device-Detection, Accessed: 2020-04-09.

[Mi17] Miettinen, M. et al.: IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). Pp. 2177–2184, June 2017.

[Sa19] Samuel Marchal et al.: AuDI: Toward Autonomous IoT Device-Type Identification Using Periodic Communication - IEEE Journals & Magazine. IEEE Journal on Selected Areas in Communications 37/6, pp. 1402–1412, June 2019, URL: https://ieeexplore.ieee.org/abstract/document/8664655, visited on: 10/27/2019.

[Th19] Thomsen, M. D.: Device-Based Access Control, Accessed: 2020-04-09, MA thesis, Denmark: Danmarks Tekniske Universitet, 2019.

Open Identity Summit 2020

Further Conference Contributions

Consumer Privacy Concerns and Preferences for Certification and Accreditation of Intelligent Assistants in the Internet of Things.

K. Valerie Carl[1] and A. Cristina Mihale-Wilson[2]

Abstract: Interoperable Intelligent Assistant Systems (IAS) could help realize the advantages of the Internet of Things (IoT). Yet, due to their insufficient skill set and persistent privacy concerns on the consumers' side, such IAS experience only limited popularity. While enabling IAS to communicate and exchange data with each other could help such systems improve performance, certifications and accreditations can help build user's trust by addressing some of the consumers' privacy concerns. To better understand the incentives necessary to instigate the mass adoption of interoperable IAS, this paper presents a study exploring consumer privacy concerns and preferences for privacy certifications. The ultimate purpose of this paper is to provide certification recommendations for intelligent IoT networks in general and IAS in particular.

Keywords: Internet of Things, Intelligent Assistant Systems, certification and accreditation, privacy concerns

1 Introduction

The Internet of Things (IoT) paradigm envisions that objects, devices, machines, buildings, and several other items are equipped with microprocessors, sensors, tags, actuators, and software. Although invisible to individuals, the computational capabilities of things, along with their connectivity to the Internet, enable each of them to continually gather and send vast amounts of information [LL15]. Although this is useful for the optimized operation of some devices, the real value of IoT can be reached only if all devices and data are connected into an Internet of Everything (IoE) [LL15] that is then orchestrated by Intelligent Assistants Systems (IAS). However, currently, the realization of the IoE still hinges on technical and non-technical challenges [WF15] of seamless interoperability. Privacy-related aspects and potential users' privacy concerns are amongst such challenges. And although privacy consists of both technical and non-technical aspects, the focus of this study lies on privacy in the non-technical context.

Due to the central role of privacy concerns in the consumer adoption of IoT enabled products, this study explores consumers' attitudes and preferences for certifications and accreditations that might help gain user's trust by addressing some of the consumers'

[1] TU Darmstadt, Fachbereich Rechts- und Wirtschaftswissenschaften, Hochschulstraße 1, Darmstadt, 64289, valerie.carl@web.de
[2] Goethe University Frankfurt, Professur für Wirtschaftsinformatik und Informationsmanagement, Theodor-W.-Adorno-Platz 4, Frankfurt am Main, 60323, mihale-wilson@wiwi.uni-frankfurt.de

privacy concerns. In doing so, we wish to gain insights and provide certification recommendations for intelligent IoT networks in general, and interoperable IAS in particular.

2 Theoretical Background and Related Work

Studying consumers' attitudes and behavior has a long history in academia [Oi13], [Ve03], such that, to date, there are numerous theories dedicated to understanding the essential antecedents of consumers' technology adoption behavior. Despite the different settings and technologies prior research has considered, consumers' privacy concerns and trust have repeatedly loomed to be at the center of the debate concerning technologies adoption [APA18], [CCT13], [GKS03]. Similarly, prior research has shown that consumers' privacy concerns are closely related to consumers' trust and thus to their propensity to adopt or reject Internet or e-commerce technology [Lu02]. In general, consumers' privacy concerns refer, amongst others, to improper access, improper collection, inadequate monitoring, improper analysis, improper transfer. For more dimensions of privacy concerns, see also Hong and Thong [HT13].

The previously mentioned infringements are not exhaustive but rather exemplary for the violations users can face when using technology and especially IAS. More specifically, since IAS' support performance (skill set, support quality) hinges on the amount of (personal) data it can gather and process, we argue that users' privacy concerns might be especially salient when using such intelligent assistants. On the one hand, to orchestrate and combine the amenities of a variety of IoT devices, services, and other intelligent agents to personalized and meaningful support for their users, IAS must gather and combine a variety of personal data and context-relevant information. Yet, on the other hand, the collection, processing, and storage of such data by a central entity such as an IAS raise several severe data privacy and security related concerns.

Given consumers' well-documented concerns towards the unauthorized and or opaque collection and processing of their data [Lu02], [MZH17], scholars proposed various mechanisms to support the trust-building process and thus enhance the chances of adoption. In this context, scholars reported that technology and service providers could foster consumers' trust with institution-based mechanisms (e.g., digital certifications, accreditations [Lu02]), process-based mechanisms (e.g., repeated purchases [Lu02] and return policy [CCT13]), or characteristic-based mechanisms (e.g., consumer age, sex, socio-demographic background [CCT13]).

Notably, not all trust-building mechanisms address consumers' privacy concerns equally effectively. In this regard, institution-based mechanisms are the most effective way to address consumers' privacy concerns [Lu02]. With its formal and marketable structure, institution-based trust mechanisms address privacy concerns through third-party guarantors pledging integrity and fairness [Lu02]. Since users can usually not see, understand or evaluate whether IAS or other services they use are handling their data

appropriately and as agreed, trust can theoretically be established by acquiring membership in an association, professional credentials, third-party certifications or through intermediary mechanisms, such as insurance, escrows, legal regulations [CCT13].

In theory, third-party certifications are expected to address some of the consumers' privacy concerns and thus instill their trust by testifying compliance with a variety of best practices or rules. In practice, however, both providers and consumers are facing a plethora of certification and accreditation programs and seals issued by industrial, national, international, private, or governmental institutions. These accreditations suggest compliance with underlying data protection principles. As such third-party certifications and seals vary significantly in terms of duration, quality requirements, and certification subject, consumers are increasingly unable to evaluate the value of such institution-based trust mechanisms. Therefore, understanding consumers' view on certifications as a trust-building mechanism becomes increasingly essential.

3 Study Design and Participants

To investigate consumers' privacy concerns and preferences for certifications of IAS in IoT, we designed a survey based on an exemplary case study that visualizes the amenities of IAS in a networked IoT environment spawning the areas of smart public transportation, smart home, and connected car. All IoT areas were orchestrated by an IAS, which was in constant data exchange with IoT devices and other services to assist their user in a personalized way.

After introducing all participants to the IAS and IoT concept via the use case mentioned above, the participants were asked to answer a set of questions that documented their general attitude towards the IAS, their privacy concerns and preferences for trust-building mechanisms such as third-party certification, reputation, and return policy [CCT13], [MCK02]. Further, participants were shown a set of randomly selected EU and German seals (see Tab. 1) and were asked to indicate which of the presented seals they knew, whether they knew what the seals were certifying in detail, and whether they tend to trust or distrust such certifications. Ultimately, the participants were also asked to answer a set of questions that documented their demographic and socioeconomic status.

The online survey was implemented with Dynamic Intelligent Survey Engine (DISE) [SS12]. A marketing research entity that was hired to provide a sample representative of the population of Germany administered the survey to 400 individuals, from which 229 answered the questionnaire thoroughly. The final participant sample (N=229) closely mimics the German population.

Seal	Brief description
	Private company certifying online shops, performing cybersecurity assessments, and many other data security and privacy assessments.
	Private company certifying conformity assessments in the field of data protection and information security. The focus lies on IT systems, products, procedures, and processes.
	Registered association. Companies can use the seal if the affiliation is established by acquiring membership in the association.
	Registered association focused on small and medium-sized IT providers in Germany. Again, affiliation necessary in order to use the seal.
	Registered association. Companies can use the seal if they are members of the association, and the data of their products and services are hosted in Germany, and the hosting contract is governed exclusively by German law.
	Public organization. Certification based on the ISO standard 27001, which focuses on information security management systems.
	Private company. Attests a product's compliance with a list of ePrivacyseal criteria that are supposed to reflect the requirements imposed by the EU General Data Protection Regulation (GDPR). However, the seal is not an accredited procedure within the meaning of article 42, 43 GDPR.

Tab. 1: Overview third-party certifications shown in the study

4 Users' Preferences for Certification and Accreditation

The results underscore existing theories postulating that privacy concerns are crucial for consumers' decision to adopt or reject new products and services. Further, it corroborates almost half (i.e., 51.5%) of the participants are still unsure if they would like to adopt such an IAS and IoT networked environment. 63% of the participants feel uncomfortable if the IAS would know their personal preferences. 79% of the participants are afraid that their personal information could be misused. Lastly, 42% of participants are fearful that IAS and IoT networks, could bring them into uncontrollable and dangerous situations. These findings reflect consumers' current state of distrust in IAS, IoT networks, and perhaps, by extension, in their providers.

Furthermore, the analysis results show that from the prompted certifications, the majority of participants know the established third-party seals issued by the TUEV (76%), 32% know the ISO certification seal, 22% are familiar with the BSI certification logo, and 17% know the "software made in Germany" logo. The remaining certifications are widely unknown, with less than 10% of the participants knowing one of them. Additionally, when asked about their detailed knowledge of the certifications with which they are familiar, participants admit that they do not know exactly which certifications

testify what, en detail. Even so, despite participants' lack of detailed knowledge on the individual certifications, 35% of the individuals in our survey would tend to trust certificates and hence certified products and providers. Thereby, it does not seem to matter whether certificates are issued by a non-profit association, a federal organization, or a private profit-driven third-party. What matters more is the sheer existence of a certification or accreditation of products, while the certification entity and the accreditation process itself only seems secondary, if at all important.

Group comparisons between participants who reported to be willing to adopt an IAS like the one presented in the study, with the groups of participants who were undecided, or would not adopt the IAS show that adopters and non-adopters differ from each other mainly in their willingness to trust certifications they do not know. In this regard, our analyses show that adopters are, on average, more willing to trust unknown certifications than non-adopters are eager to. What is also surprising is that the origin of the IAS and IoT technology provider, or the location where the data of the IAS is hosted does not seem to matter. On the contrary, our data shows that participants would value the price-performance ratio of technological products more than product origin.

5 Discussion

The primary purpose of this paper was to provide certification recommendations for smart IoT networks in general and IAS in particular. Based on our participant sample, our study corroborates that technology adopters and non-adopters distinguish themselves significantly in terms of privacy concerns. In this regard, our study showed that adopters display lower levels of privacy concerns, while non-adopters are much more skeptical against IAS and networked IoT environments. Additionally, our results also suggest that trust-building mechanisms might be a powerful tool to address consumers' privacy concerns and thus foster technology adoption. More particularly, our data set shows that consumers have a high propensity and willingness to trust certifications, regardless of the issuer, the type of certifying entity, or the certification process. What seems to matter more is the sheer existence of a certification or accreditation. Against this background, it is advisable that companies developing and launching new intelligent systems and IoT environments try to leverage trust-building mechanisms, and in particular institution-based mechanisms in the form of third-party certifications to their advantage. Besides, with consumers having a high tendency to trust seals they do not know, companies and business networks might even want to think about founding their own certification association and issue their own certification seals.

Despite our efforts to ensure the validity and robustness of the presented results, the study has been conducted only with German participants. This might be an issue given the Germans' increased awareness regarding data security, data safety, and informational empowerment. Furthermore, the study presents only a snapshot in time and only for the given, fictional use case. Additionally, since the participants' attitudes and beliefs

captured in this study might depend on the use case shown, and thus might vary in another smart assistance scenario, future work should focus on other suitable use cases than the one presented in this study. Ultimately, because the IAS and IoT paradigm is yet to be materialized in the future while consumers' attitudes are changing over time, the research question addressed in this study should be repeated at a later stage in the development of such artifacts.

Acknowledgment

This work has been funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) as Part of the ENTOURAGE Project (01MD16009F).

Bibliography

[APA18] Adjerid, I., Peer, E.; Acquisti, A.: Beyond the privacy paradox: Objective versus relative risk in privacy decision making. MIS Quarterly 42/2, pp. 465–488, 2018.

[CCT13] Chang, M. K., Cheung, W.; Tang, M.: Building trust online: Interactions among trust building mechanisms. Information & Management 50/7, pp. 439–445, 2013.

[GKS03] Gefen, D., Karahanna, E.; Straub, D. W.: Trust and TAM in online shopping: an integrated model. MIS Quarterly 27/1, pp. 51–90, 2003.

[HT13] Hong, W.; Thong, J. Y.: Internet privacy concerns: An integrated conceptualization and four empirical studies. MIS Quarterly 37/1, pp. 275–298, 2013.

[LL15] Lee, I.; Lee, K.: The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons 58/4, pp. 431–440, 2015.

[Lu02] Luo, X.: Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. Industrial Marketing Management 31/2, pp. 111–118, 2002.

[MCK02] McKnight, D. H., Choudhury, V.; Kacmar, C.: Developing and validating trust measures for e-commerce: An integrative typology. Information systems research 13/3, pp. 334–359, 2002.

[MZH17] Mihale-Wilson, C., Zibuschka, J.; Hinz, O.: About user preferences and willingness to pay for a secure and privacy protective ubiquitous personal assistant. In: Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017, pp. 32–47, 2017.

[Oi13] Oinas-Kukkonen, H.: A foundation for the study of behavior change support systems. Personal and ubiquitous computing 17/6, pp. 1223–1235, 2013.

[SS12] Schlereth, C.; Skiera, B.: DISE: dynamic intelligent survey engine. In: Quantitative marketing and marketing management. Gabler Verlag, Wiesbaden, pp. 225–243, 2012.

[Ve03] Venkatesh, V., Morris, M. G., Davis, G. B.; Davis, F. D.: User acceptance of information technology: Toward a unified view. MIS Quarterly 27/3, pp. 425–478, 2003.

[WF15] Wortmann, F.; Flüchter, K.: Internet of things. Business & Information Systems Engineering 57/3, pp. 221–224, 2015.

Privacy by Design Architecture Composed of Identity Agents Decentralizing Control over Digital Identity

Kalman C. Toth[1] and Ann Cavoukian[2] and Alan Anderson-Priddy[3]

Abstract: Proposed is an identity architecture that satisfies the principles of privacy by design, decentralizes control over digital identity from providers to users, mitigates breach and impersonation risks, and reduces dependency on remote access passwords. The architecture is composed of interoperating identity agents that work on behalf of their owners and deploy digital identities that are virtualized to look and behave like identities found in one's wallet and contacts list. Encapsulating authentication data, identity agents strongly bind owners to their digital identities and private keys enabling them to prove who they are, protect their private data, secure transactions, conduct identity proofing, and reliably delegate consent. Identity agents also off-load application services from identity-related and privacy-related tasks. A gestalt privacy by design process has been used to discover the architecture's privacy requirements and design elements and systematically reason about how the design elements satisfy the privacy requirements. Identity-related functionality has been intentionally compartmentalized within identity agents to focus development on creating trustworthy software. A reference model for development derived from the described identity architecture is proposed.

Keywords: privacy, privacy by design, digital identity, authentication, verification, security.

1 Introduction

The identity architecture proposed herein has been motivated by the alarming growth in identity theft, impersonation, fraud and lost privacy due to private data collection by service providers, remote access password vulnerabilities, and the web's patchwork of identity schemes. Large-scale breaches (e.g. Facebook, Google, Capital One, Marriott, Sony, Target, JP Morgan, Home Depot, Equifax) have disclosed social security numbers, personal information, medical records, credit reports, credit card records, bank accounts, voter data, and other such sensitive information. Authorities are deeply concerned about threats to our critical infrastructure including power, transportation and voting systems.

The identity architecture satisfies the principles of privacy by design, decentralizing digital identities to owners enabling them to prove who they are, protect their private

[1] NexGenID, Portland, Oregon 97205, USA, kalmanctoth@gmail.com
[2] Global Privacy & Security by Design Centre, Toronto, M4S 2X6, Canada, ann.cavoukian@gpsbydesign.com
[3] Portland State University, OIT, Portland, Oregon 97207, USA, andersonpriddy@gmail.com

data, secure transactions, elevate identity assurances, and reliably delegate consent.

2 Privacy by Design Dependent on Capable Digital Identity System

Explained by Ann Cavoukian in [Ca17], the principles of privacy by design include minimizing private data disclosure and collection; safeguarding private data, securing transactions end-to-end; delegating consent to access private resources; and establishing privacy as the system default setting to ensure acceptable levels of privacy protection.

Consider that privacy can be lost when underlying identity schemes are broken. Users can be tricked by rogue data collection sites to disclose passwords, second factor access codes, and social security numbers; weak passwords can be broken and used by imposters to access private data in the cloud; transactions can be intercepted; and delegated consent can be defeated when stolen identities are used by imposters. In other words, enhanced privacy is highly dependent on the efficacy of the identity system used.

3 **Decentralizing I**dentity Reduces Risks for Providers and Users

Many web services have become honeypots for identity theft partly because of the enormous volume of private and identifying data they collect. To address this problem, writers including [Al16], [So18] and [WW19b] have proposed deploying *self-sovereign identities* and *decentralized identifiers* (DIDs) to shift control over identity to users.

The architecture described in this paper decentralizes digital identity by providing users trustworthy agents that help them make safe identity and privacy-related decisions. Installed on the user's personal device, an identity agent protects and tightly binds the owner to her digital identities. Her identity agent helps her decide which digital identities to create and use, what private data to protect, which consent permissions to reliably delegate, how to elevate identity assurances, and what private data to disclose. Minimizing disclosure limits how much data service providers need to collect which reduces breach risk while dispersing the attack surface.

4 System Concept: Decentralized and Privacy Enhanced Identity

Depicted in Fig. 1, the system concept for the proposed identity architecture [TA18], [TA19a], [TA19b], [TCA20][4] is composed of *identity agents* and *digital identities* installed on the devices of users and providers (e.g. smart phones, servers, laptops).

[4] "Electronic Identity and Credentialing System", US Patent 9,646,150 B2, May 9, 2017.

Identity agents decentralize control over identity from service providers to users while satisfying the principles of privacy by design for their joint benefit - safely managing disclosure, data collection, privacy protection, transaction security and delegated consent.

Identity agents empower users and administrators by virtualizing digital identities such that they look and behave like physical credentials in their digital wallets and contact lists. They tightly bind owners to their digital identities, consent tokens, PINs, keys, and other artifacts by encapsulating the authentication data of the owner. Identity agents also off-load application services from identity and privacy management tasks and interoperate with other identity agents, digital identity exchange services, and proof-of-existence identity registries. Digital identities specify an identifier plus selected attributes/images characterizing the owner, or little or no identifying information for pseudonymous and anonymous uses. Depending on perceived identity correlation risks, an identifier can be unique within a given context, globally unique, or pair-wise unique [WW19b].

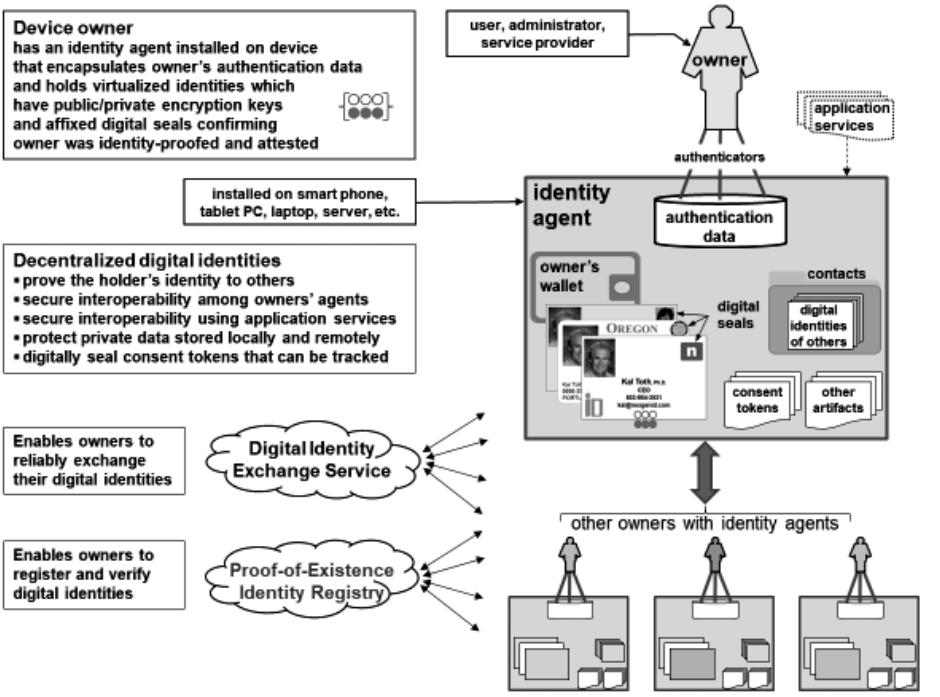


Fig. 1: System concept diagram

Each digital identity created by an owner is allocated multiple public/private encryption key-pairs, each pair used for designated purposes when selected to prove identity, secure

transactions, and delegate consent to access private data. The private embossing key of a digital identity can be used to digitally seal attestations to digital artifacts [TCA20][5]. Such attestations cannot be repudiated because the owner controls her device, identity agent, selected digital identity, and embossing key used to bind her identity and attestation to the digital artifact (e.g. to a digital identity, a consent token, or a legal document).

For example, a requesting owner can present his digital identity and identifying data to an issuing owner who proofs his identity. If successfully proofed, the issuer can use one of her digital identities to issue a digital seal affixing her attestation plus her identity to the requester's digital identity which the issuer cannot repudiate and can be verified.

5 Privacy by Design Process and Validation

Early in development, system engineers routinely use a gestalt process to define requirements and evaluate designs, iterating until they converge on an acceptable design satisfying the requirements. Fig. 2 depicts the privacy by design process used to discover and validate the architecture's privacy requirements (R) and design elements (D). Upon thoroughly iterating over all the privacy requirements and design elements, the listed requirements and elements were validated. Each iteration contributed to the goal of showing that the principles of privacy by design were satisfied.

[5] "Methods for Using Digital Seals for Non-Repudiation of Attestations", US Patent 9,990,309B2, 2-20-2018.

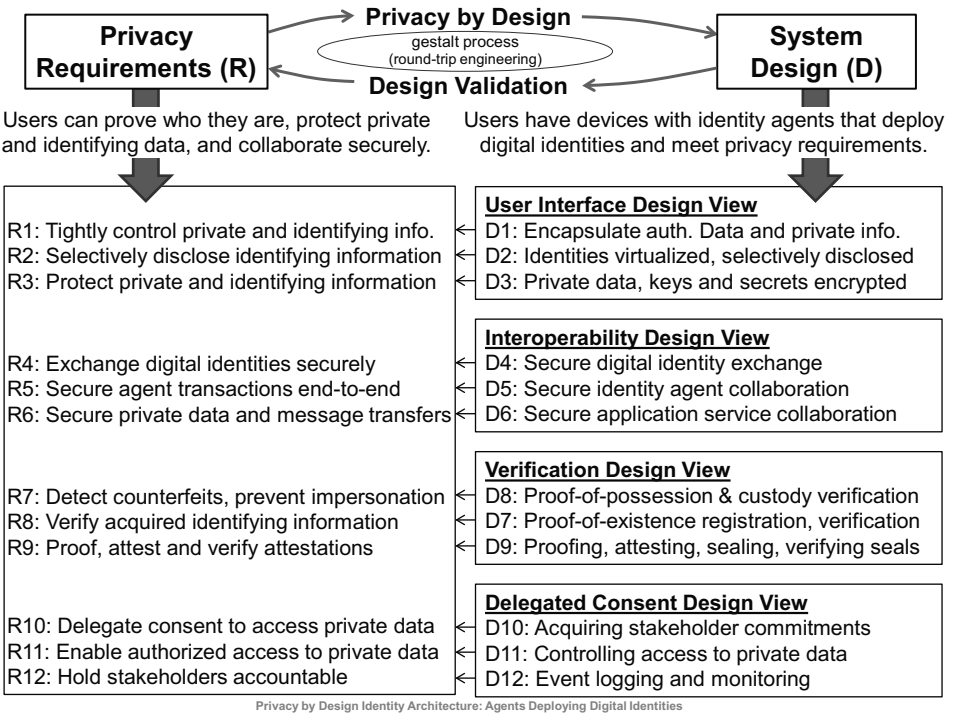


Fig. 2: Privacy by design process

The privacy by design validation process detailed in [TCA20] reasons about how the proposed identity architecture enables the following functions and features:

- Prevents compromise by encapsulating authentication data (e.g. biometric minutia, PIN hashes) used by device authenticators to verify owner presence and custody.
- Virtualizes the look and feel of physical identities rendering them as simple to use as passwords but with enhanced utility, usability and intuitive ease of use.
- Leverages an identity data model (e.g. [WW19a]) to specify civil digital identities for owners as well as so-called pseudonymous and anonymous identities.
- Allocates public/private encryption key-pairs to digital identities used to secure private data, transactions, messages, and consent tokens for the owner.
- Elevates identity assurances associated with digital identities by proofing [NI17] and affixing attestations to them with digital seals that cannot be repudiated.
- Registers digital identities that are hashed and digitally sealed in a proof-of-existence registry [Ro16], [TCA20][6] that other parties can verify.

[6] "Systems and Methods for Registering and Acquiring E-Credentials using Proof-of-Existence and Digital Seals", US Pat 10,127,378 B2, issued Nov. 13, 2018.

- Mitigates attack risks by leveraging an adaptation of the Diffie-Hellman key agreement method to exchange digital identities [Re99], [TCA20][7].
- Launches challenges to verify private key possession [ANL03] of presented digital identities and custody of owner devices to detect counterfeits and impersonation.
- Uses digital seals to affix requests, approvals and access permissions to consent tokens that can be tracked for accountability and cannot be repudiated.
- Establishes privacy by design default settings according to context and risks including using pseudonymous and anonymous identities; applying the adapted Diffie-Hellman exchange method; securing all transactions using digital identities; executing proof-of-possession and proof-of-custody challenges; and registering digital identities and consent tokens in a proof-of-existence registry.

6 Discussion: Privacy by Design Reference Model for Identity

A reference model derived from the identity architecture is proposed to communicate essential methods, interfaces and protocols[8] to developers. A key objective will be to ensure that deployed identity agents are trustworthy, namely, that they reliably and correctly integrate authentication data, user interfaces, cryptographic mechanisms, identity proofing and attestation, programming interfaces, and collaboration protocols. These essential building blocks have been intentionally compartmentalized within identity agents to facilitate the development of software that is reliable and trusted.

Options for implementing such trustworthy software include open source and proprietary development, and possibly a combination of both. Software licensing, support, and maintenance arrangements can vary widely. Pundits argue that open source software is more, less, or just as secure as proprietary software. The debate revolves mainly around developers having or lacking visibility into the code. Arguments about the merits and shortcomings of these options address issues related to hacking vulnerability, security by obscurity, responsiveness to problems, development methods, skills and tools used, time-to-deliver, business failure, liability, and warranty.

Whichever option is adopted, effective software inspections, comprehensive testing, quality assurance, and configuration management are essential. Formal software engineering methods can be applied to identity agents to enhance trustworthiness.

[7] "Architecture and Methods for Self-Sovereign Digital Identity", US Patent (pending), provisional filed Oct. 8, 2018, utility application filed Nov. 12, 2018.

[8] Founding team intends to issue a license to developers similar to RedHat's patent promise to discourage patent aggression https://www.redhat.com/en/about/patent-promise.

7 Closing Remarks

The privacy by design process has progressively baked privacy into the identity architecture [TCA20]. Decentralizing identity from service providers to users decreases what providers need to collect while dispersing the attack surface. Identity agent owners can control and use their digital identities to reliably prove who they are, verify the identities of others, protect their private and identifying information, and reliably delegate consent. Because digital identities are intuitive, and owners can control what they disclose, they are less dependent on remote access passwords. Digital identities that have been proofed, attested and digitally sealed elevate identity assurances for all stakeholders.

Bibliography

[Al16] Christopher Allen: The Path to Self-Sovereign Identity, April 27, 2016, http://coindesk.com.

[ANL03] N. Asokan, Baltteri Niemi, Pekka Laitinen: On the Usefulness of Proof of Possession, 2nd Annual PKI Workshop, Apr. 28-29, 2003, pp.136-141.

[Ca17] Ann Cavoukian: Privacy by Design, The 7 Foundational Principles, https://ipc.on.ca/wpcontent/uploads/Resources/7foundationalprinciples.pdf, 2017.

[NI17] NIST Special Publication 800-63A: "Digital Identity Guidelines, Enrollment and Identity Proofing", Jan. 2017, https://doi.org/10.6028/NIST.SP.800-63a.

[Re99] E. Rescorla: Diffie-Hellman Key Agreement Method, RTFM Inc., June 1999.

[Ro16] Kiara Robles: Tool for Creating Verifiable IDs on the Blockchain, BlockchainMe, Dec. 2, 2016, https://github.com/kiarafrobles/blockchainMe.

[So18] Sovrin Foundation: Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust, Version 1, January 2018, https://sovrin.org.

[TA18] Kalman C. Toth and Alan Anderson-Priddy: Architecture for Self-Sovereign Digital Identity, Computer Applications for Industry and Engineering (CAINE), New Orleans, LA, Oct. 8-10, 2018.

[TA19a] Kalman C. Toth and Alan Anderson-Priddy: Self-Sovereign Digital Identity: A Paradigm Shift for Identity, IEEE Security and Privacy, Vol. 17, No. 3, May/June 2019.

[TA19b] Kalman C. Toth and Alan Anderson-Priddy: Privacy by Design using Agents and Sovereign Identities, Information Security and Privacy Protection Conference (IFIP-SEC), Work in Process and Emerging Research, Lisbon, Portugal, June 25-27, 2019.

[TCA20] Kalman C. Toth, Ann Cavoukian and Alan Anderson-Priddy: Privacy by Design Identity Architecture Using Agents and Digital Identities, Annual Privacy Forum, Lisbon, Portugal, accepted for presentation and publication, June 4-5, 2020

(postponed).

[WW19a] World Wide Web Consortium (W3C): Verifiable credentials data model 1.0: Expressing verifiable information on the web, proposed recommendation, 9-5-2019.

[WW19b] World Wide Web Consortium (W3C): Decentralized Identifiers (DIDs) v1.0: Core Data Model and Syntaxes, WC3 Working Draft 09 December 2019.

H. Roßnagel, C.H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 171

IdToken: the new decentralized approach to digital identity

Edoardo Talamo[1] Alma Pennacchi[1]

Abstract: The ability to store and share digital data offers benefits that the digitization of information has become a growing trend but has raised questions about the security of personal data. There have been countless high-profile hacks and personal information leaks. Furthermore users don't (and shouldn't) always trust an external server of a third party to store their personal data. Blockchain tries to offer a compelling solution to the problem of combining accessibility with privacy and security. Records can be held securely, using end-to-end encryption, and yet openly authenticated so that data can still be trusted as reliable. This project goes deeper in this solution thanks to an innovative idea and development of a new kind of blockchain non fungible token specifically created to store and manage digital identities and sensible data. It has the potential to resolve issues blockchain alone was starting to approach and improves security, privacy and accessibility.

Keywords: Blockchain non fungible token; blockchain; digital identity; idtoken; security; privacy; idchain; hyperledger indy

1 Introduction

A blockchain is a growing list of blocks across several computers that are linked in a peer-to-peer network using cryptography. Each block contains a cryptographic hash of the previous one, a timestamp and transaction data. A token in the blockchain ecosystem is any asset that is digitally transferable between two people. They are accessible only by the person who has the private key for that address and can only be signed using this private key. So tokens represent programmable assets or access rights, managed by a smart contract[Cr] and an underlying distributed ledger. Blockchain is a particular type or a subset of distributed ledger technology. DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers (nodes) that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently. In the digital identity management, blockchain solutions have the potential to make operations more efficient and improve the delivery of services in the public and private sectors[Wo]. Identity management built on blockchain technology would enable an identity model, which reduces issues for certain use cases. Blockchain identity management provides a software ecosystem for

[1] Fondazione universitaria INUIT Tor Vergata, Via dell'Archiginnasio snc – Casale 4 00133 Rome (Italy), edoardo.talamo@gmail.com,alma.pennacchi@gmail.com

private, secure, powerful identity. Nowadays even though thanks to blockchain technology digital identity management could have a significative improvement, there are still open issues: usability, handling of (lost) private keys, achieving a critical mass of users and furthermore the majority of blockchains for digital identities store some data in a third party system (like a wallet that saves informations in the memory of a computer or a server) because still there isn't a technology totally blockchain native[Ku][Mu]. In this article we will introduce a new tool for digital identities management to take full advantage of blockchain to minimize the amount of data saved outside it. We will introduce a new concept of non fungible token[Ho], IdToken, and we show how to use it in defining the process of authentication of a digital identity by a reliable party. The use of the IdToken makes the solution safer, faster and reusable.

2 State of art

Without blockchain technology, Identity federation allows users to maintain login credentials with multiple credential service providers[Da] (CSP) and then choose among them when logging into different online services. Users register once with their selected CSP and establish online credentials to be managed by that CSP for authentication. When a user wants to access a relying party (RP) service, that user is redirected to their preferred CSP for authentication using the credentials the user established with that CSP. The CSP then presents the status of the authentication to the RP so that the user may be granted access to the service or application they wish to use. In this way, users do not need to register or establish login credentials with each service they want to access, and instead they only need to provide their credentials to their selected CSP. Identity federations consist of CSPs and RPs that have agreed to participate in a specific federated identity management arrangement. This identity model comes with certain issues such as there is always trust to a central authority required. Transparency cannot be fully provided, since there is a trusted authority involved. These issues can play an important role in certain use cases, which leads to the conclusion that a new identity model for these use cases has to be developed. In the blockchain ecosystem there aren't organizations that traditionally centralize identity. The immutable blockchain ledger verifies and ensures that the users, transactions, messages are legitimate. Blockchain authentication[Is] is done by smart contracts which are written and deployed to blockchain. The need for a third party to authenticate transactions is eliminated. Costs can be reduced while security and privacy are greatly enhanced. Effort of hijacking the authentication process would be much greater in the distributed environment. The result is a reliable, public source of truth under no single entity's control, robust to system failure, resilient to hacking, and highly immune to subversion by hostile entities. Nowadays probably the best example of identity management blockchain software is: Hyperledger Indy[Hy]. There are numerous solutions to manage data using Hyperledger Indy blockchain such as Sovrin[Li], a decentralized global public utility for self- sovereign identity and MyData[Li] an initiative which joint forces with Sovrin to build self- sovereign identity and authentication mechanism. Indy is a distributed ledger, purpose-built for decentralized

identity. It has complete open source specifications, terminology, and design patterns that allow for the development of decentralized identity solutions. Hyperledger Indy would seem to be a good solution for solving problems on digital identity but some issues still remain unsolved. In the next section we present a more efficient and innovative solution; it is based on the Indy software and manages the exchange of information between two users, in a more faster and secure way, thanks to a new kind of non fungible token based on the model designed in HYperledger Fabric: IdToken. A non-fungible token (NFT) is a special type of cryptographic token which represents something unique; non-fungible tokens are thus not mutually interchangeable by their individual specification. A NFT is generated by a smart contract which is a computer program that directly controls digital assets. This contracts are stored on blockchain technology.

3 IdToken

From now on we will refer to Hyperledger Indy with the new improvement of the IdToken as IdChain. While we will discuss about IdChain we will consider the issues of Hyperledger Indy[2] highlighting the solutions that we obtained with IdChain.

3.1 Description

To better understand the development of IdToken and IdChain let's consider three actors: Alice (normal user), Acme (a corporation), Faber College (the guarantee of identity attributes for Alice: for example in this case the college certifies that a subject has obtained a degree with a certain grade). The registration in IdChain is the same for everyone, so we consider the Alice's example. Alice wants to register in the IdChain, she provides personal data (i.e. name, surname) and biometric data[Ga] (fingerprint or facial recognition). The biometric data is converted in a cryptographic hash and becomes the private key, which is stored in a crypto engine of a personal device, and after the generation of the private key will be generate the public key. When the registration in IdChain is complete, a new block in the ledger is created and the smart contract generator of token will execute and automatically generates, in the new block, her IdToken where Alice can insert all her personal data that are stored and encrypted with her public key. Alice can read and insert new informations in her IdToken using her private key (which is the biometric data hashed - ref. paragraph 3.1 row 7); if she wants to grant access to read-only data in the IdToken to someone she will have to share her public key. A strength of this token is that Alice can insert all the information that she wants inside the IdToken. Furthermore in Hyperledger Indy there were a wallet where a lot of sensible data were stored locally (smartphone, computer) and this could leave to losing fundamental information. Instead if a user loses his personal device, it is easy to access in the IdChain using biometric data[3]. IdChain allows users to exchange

[2]Here[De] there is the description of the procedure

[3]"The biometric data is converted in a cryptographic hash and becomes the private key"paragraph 3.1 row 7

personal data without the control of a central authority. Now let's examine an example using IdChain platform of Alice who wants to obtain a job at Acme using a reliable party (Faber College). If Alice wants to be an employee in Acme, she must exchange her personal data to Acme and she has to perform the following procedure:

1. Both Alice and Acme have an account on IdChain. Alice wants to identify herself to Acme with her attributes certified by Faber College with her IdToken.
2. Subsequently Alice request a connection to Acme giving access to her IdToken providing her public key. After receiving the request Acme accepts because it verified the Verifiable Credentials[Ve] in the IdToken.
3. The identity of Alice and Acme are verified (digital signature).
4. After the verification of identities, Acme sends the request of transcript to Alice asking for the information that the corporation needs to decide whether to hire Alice or not.
5. Alice accepts and sends the IdToken with only the transcript information required by Acme and validated by the reliable party.
6. Acme will be able to read Alice's data, decrypting the IdToken with her public key.
7. In the meantime that all these operations take place, each of these will be associated with a timestamp. In this way both users will be aware of the other's identity and will thus be able to carry out the operations between them in a safe and reliable manner.

The substantial difference between Hyperledger Indy and IdChain is the reusability of IdToken: in fact if Alice wanted to present her CV in other companies, in Hyperledger Indy all these companies should contact Faber College again. In IdChain, thanks to the reusability of the IdToken, there is no need for this step anymore. In the picture below we can find an explanatory workflow of IdChain.

3.2 IdChain properties and technical aspects

- There is no proprietary software or infrastructure, IdChain uses the public permissioned blockchain. This means that Identity Requesters do not have to invest a large amount of money to set up the technology infrastructure to support the IdChain Platform solution.
- Data is revocable, identity data is revocable by the authenticating owner of the data. For example, if a user changes his credit card number, then the former/invalid credit card number data is revoked on the blockchain by the authenticating owner of the data.
- Globally compatible, users store and share their own identity anywhere in the world. Their data is accessible anywhere in the US, Europe, Africa, or Asia.

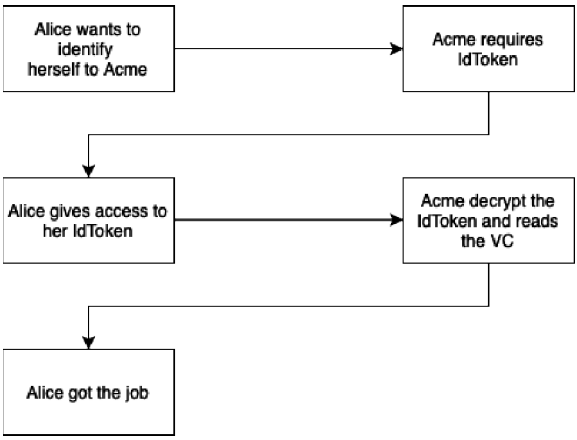


Fig.1:IdToken procedure

- Everything is blockchain native and nothing is stored locally.
- The Verifiable Credentials, and every personal information is stored and encrypted in the IdToken which is unique and not replicable.

Hyperledger Indy Issues	IdToken Solution
The Verifiable Credentials are not stored on the blockchain but they go in the wallet of the VC holder.	The Verifiable Credentials are stored in the IdToken which is blockchain native.
If the user wants to work in a new company, the new company has to request all the infos at the old one and after receiving them the user can finally interact with the new company.	If the user wants to work in a new company, he can directly give access to updated IdToken to the new company
The user has different DIDs for each service so for every interaction with applications that requires username/password a DID is created. Those occupy a lot of memory in the blockchain	The IdToken is unique and the user can access directly with it everywhere.
The lenght of a DID is too short and so there is a security problem because it is susceptible to security breaches	The IdToken is hashed so it's impossible to brute force it
The scalability reduce the security	The scalability is pair with the security

Tab.1:Hyperledger Indy issues and IdToken solution

In the table above we can observe what are the issues of Hyperledger Indy without IdToken and the solution that the token brings to the platform.

4 Conclusions and future developments

This new approach is useful, economical and secure for the digital identity management and certificate distribution thanks to the improvements of privacy, security and efficiency. Furthermore it can easily replace every kind of exchange of paper information and speed up the identification of users and companies, eliminating the open problems presented before in the management of digital identity. An important characteristic of the proposed solution is the impact in the usability of the blockchain. The IdChain open the doors to the use of crypto-engines embedded in portable devices (es. smart cards and others) and then is a first step to separate the peer from a specific device (computer). Biometrical key act as second authentication factor, giving an answer to weaknesses of the Indy authentication system for example the absence of a Certification Authority[Ce]. For future developments, we are working on extensions that allow us to solve problems still related to privacy and the use of biometric data in blockchain which, except for solutions related to fingerprints, is still a subject of study and experimentation. Another important tool that we are going to develop is to partition the amount of data within the IdToken to share only the information necessary in every use case witch is another aspect about usability and blockchain.

Literaturverzeichnis

[Ce] Certification Authority, https://csrc.nist.rip/groups/ST/crypto_apps_infra/documents/B2B-article.pdf, accessed 17/02/20.

[Cr] Creating a safe Smart Contract https://experts.illinois.edu/en/publications/step-by-step-towards-creating-a-safe-smart-contract-lessons-and-i, accessed 14/02/20.

[Da] Damiani, E. et al.: Managing Multiple and Dependable Identities (2003), IEEE Computer Society.

[De] Demonstration of Hyperledger Indy, https://github.com/hyperledger-archives/education/blob/master/LFS171x/indy-material/nodejs/README.md, accessed 17/02/20.

[Ga] Garcia, Paco: Biometrics on the blockchain (2018), Biometric Technology Today, volume 2018, issues 5, pages 5-7.

[Ho] Hong, S. et al.: Design of Extensible Non-Fungible Token Model in Hyperledger Fabric (2019), pages 1-2.

[Hy] Hyperledger Indy, https://www.hyperledger.org/projects/hyperledger-indy, accessed 15/02/20.

[Is] Ismail, Reza: Enhancement of Online Identity Authentication Though Blockchain Technology (2017), https://www.syscode.asia/assets/files/oia-blockchain.pdf.

[Ku] Kuperberg, M.: Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective (2019), IEEE Transactions on Engineering Management.

[Li] Lim, S.Y. et al.: Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey (2018), International Journal on Advanced Science, Engineering and Information Technology, volume 8, pages 1737.

[Mu] Muhle, A. et al.: A survey on essential components of a self-sovereign identity (2018), Computer Science Review, volume 30, pages 80-86.

[Ve] Verifiable Credentials, https://www.w3.org/TR/vc-data-model, accessed 18/02/20.

[Wo] Wolfond, Greg: A Blockchain Ecosystem for Digital Identity: Improving Service Delivery in Canada's Public and Private Sectors (2017), Technology Innovation Management Review, volume 7, pages 35-40.

Token Based Authorization

Giovanni Augusto Baruzzi[1]

Abstract: A secure, scalable, fine grained and flexible access control is extremely important for the digital society. The approaches used until now (RBAC, Groups in an LDAP Directory, XACML) alone may not be able to deliver to this challenge. Building from past experiences in the Industry, we propose an Access Management Framework where the central role is played by a token containing all the information needed to implement fine grained access control. This Authorization Token should be signed by the approver and embedded into a "claim" to the application at session time. The application, after checking the validity of the token will control access to the desired resource. In this way we can achieve fine granular access control, scalability and independence from network topologies.

Keywords: Access Control, Token, Fine-grained Access, Authorization, Claim.

1 Evolution of Access Management

1.1 The Beginning

In the early days (1970), to give access to a computing resource, the list of legitimate users was appended to the resource itself. This was then called the Access Control List (ACL).

This first approach had the problem of the ever-increasing administrative effort: each time a resource was added, the administrator had to list all legitimated users again. Similarly, the addition of a new user forced administrators to add her/him to the access list of each resource he may need.

1.2 Role Based Access Management

Role-Based Access Control (RBAC) [FK92] has been introduced to grant access based on the roles that users own in their organization, recognizing that, if a user has a certain role in the organization, he/she must be granted access to a definite, but variable, list of resources. The roles are often associated to user groups which are a list of members: *Users* are assigned to *groups*, and in turn, *groups* associated to *roles* and then *to resources*.

[1] Syntlogo GmbH, Mercedesstraße 1, 71063 Sindelfingen, Germany, giovanni.baruzzi@syntlogo.de

RBAC was a vast improvement compared to the management of simple lists of users for every resource and offered an improved security; the Role Manager could be a different user to the Resource Manager, introducing the first type of segregation of duties.

1.3 The Experience of large-scale Implementations

The experience gathered in large installations (a large German Telecommunication Provider, a large Insurance Company, a major ERP Software Vendor) revealed a number of issues in the implementation of Access Management using pure RBAC: the complexity of modern enterprises prevented the use of RBAC to the organizational roles and the fast life cycle of application, often independently operated, was an obstacle to the original idea to associate all the entitlements needed to a single organizational role.

The adoption of RBAC at application level was very successful, using not organizational roles, but application roles. But even this approach has issues.

1.4 The fine-granular access right

Consider the case where a complex application must manage the access to many resources: the application architect applying RBAC has the possibility to define a very high number of roles. The alternative is to separate the access information into two (or more) pieces: the role itself, defining the function, and additional parameters specifying the resource.

Let's assume that you must define the role of a "Cost Center Chief" but you have a large number of them. Using the pure RBAC, you may be forced to define a long list of roles like "Chief of Cost Center 001", "Chief of Cost Center 002", "Chief of Cost Center 003" and so on.

A more intelligent alternative is to define the functional role "Cost Center Chief" and assign the parameter identifying the cost center. This is what we call fine-granular access management[2].

1.5 Technological Limits of Group Objects

This issue becomes relevant as the numbers of users comes to the millions: the best practice to associate a role with a user group proves as not scalable enough.

[2] The RBAC approach generates an N*M problem (role chief * number of cost centers). With a role parameter this problem is reduced to a more manageable N+M problem

1.6 Reactions in the Industry

Confronted with these problems, the major ERP Software vendor completely defined it's own Access Management (for sure not RBAC) while the Telecomm vendor and the Large Insurance Company USED THE FINE-GRANULAR APPROACH AND added information to the role name, stored as additional user attribute.

2 The Access Management Framework

Building on the experiences cited before, we designed an Access Management Framework built around the idea of storing all access information inside a token and delivering this token at OIDC or SAML session time to the application. The digital signature added to the token allows us to move it around without losing the trust.

2.1 Basic Ideas

1. The ownership of a role is not represented by a membership in a group, but it is stored as a USER ATTRIBUTE, removing the scalability problems.
2. Additional information is added to the role name allowing more granular definitions
3. The format used is JSON and with the addition of a signature it becomes a JSON Web Token (JWT). Libraries to process them are broadly available.

2.2 Authorization Token

The authorization token is a JWT Token containing all the information necessary to define an access right and is the central concept of the proposed Access Management Framework illustrated in Figure 1, below on page 4.[3]

We are going to analyze briefly the entities and the processes that describe this Framework and we are going to see the processes that define, manage and send Authorization Tokens to implement access control for an application. [4]

2.3 The Model

We describe the Framework from different points of view: the interaction view, de-

[3] A word of caution is needed here: we use the JWT formats and the Token is built like a JWT Token but it is never used as Session Token. As a matter of fact, the Authorization Token BUILDS ON OIDC or SAML and is inserted INSIDE a Session Token to be sent as a "Claim" to the application.

[4] The model refers to an SAML or OIDC Environment, where users present to the application a set of *claims*, but is not limited to it.

scribing the processes and the Entity view, describing the responsibilities

2.4 The Interactions

- The “Contract Life Cycle” is the time span between the signature of a contract for an offer from the “Service Organization” and the termination of the contract itself.
- The “Application Life Cycle” marks the time between the start of availability of an application, with the definition of its security model and corresponding role metadata. During the “Application Life Cycle” Authorization Tokens are built, assigned to users or withdrawn from them.
- The “Session life Cycle”. A session starts as a user authenticates to the system and terminates with the logout. During the time span of a session, the system restricts the access to application resources to the legitimated users.

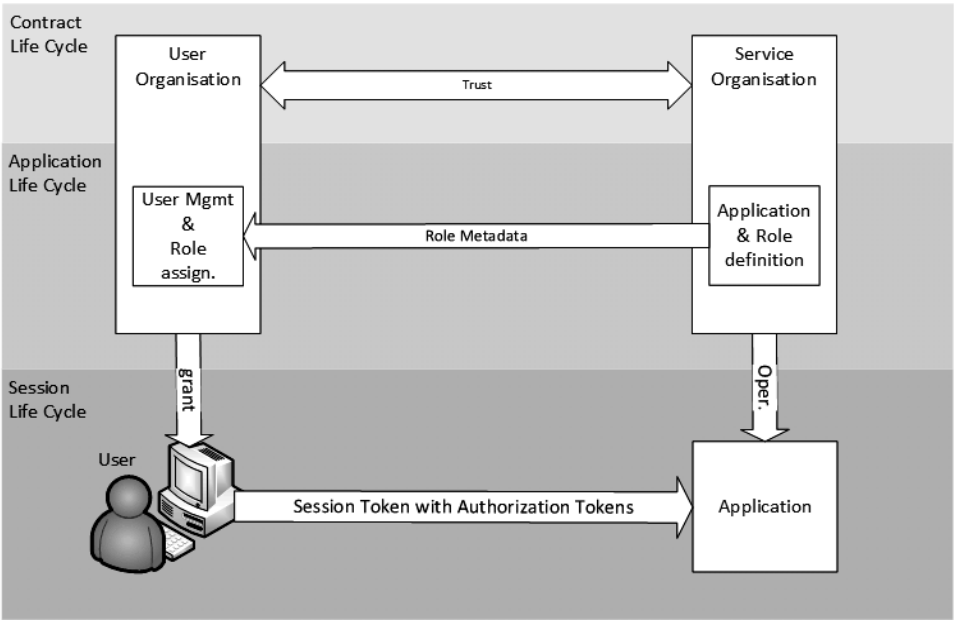


Fig. 1 Authorization Token Framework

3 Life Cycle of an Authorization Token

3.1 Application Architect defines the Roles

The application architect, during the application design process, defines the conditions under which a user can access resources. The resulting set of rules of this process builds the application "Security Model".

3.2 Roles Metadata is being loaded in the IAM (Identity & Access Management System)

After the definition of the application "Security Model", the role metadata must be loaded in the Identity and Access Management. The ID's of Security Domain, Application and Role must be included in the metadata.

3.3 Management of User and assigned Roles

The grant of a role is governed by the typical identity processes and must define beyond the value of the optional parameters a few other information like the granting actor, the assignee and validity dates. As all attributes defined are known, the JWT can be generated and digitally signed by the Customer Organization. This is stored as a user attribute. This signed element is the Authorization Token.

3.4 User accesses an Application

After having authenticated, the user may want to access an application. During this process, he introduces himself to an application presenting a session (access) token containing claims along the SAML [6] or OIDC [7] Standards. One or more of these claims would be Authorization Token.[5]

3.5 Application checks Authorization Tokens and manages access

The Application receives the access token sent in the session, extracts the embedded Authorization Tokens from their "claims", checks their validity, and grants the logged user the corresponding privileges.

[5] As written in note 2: The Authorization Token is never used as Session Token. Instead the Authorization Token is inserted INSIDE a Session Token as a "Claim".

4 Current Deployment

The solution is being used in our IAM System, allowing us to easily implement advanced features like a flexible and easy to understand “Delegated Administration”. Here the role of delegated administrator is coupled with a parameter specifying the set of users for which he is the administrator.

Due to the evolutionary character of this framework and the modest technical effort needed to implement it, the framework has been already successfully used in a financial institution and a government owned agency.

5 Conclusions

The Authorization Token is especially attractive in a Cloud Environment, where the User Organization may be a different one as the Organization providing the application, connected only by the Internet. In such a scenario, it may be very difficult to provide access for the application to the Directories or Databases holding the groups associated with a role or perform provisioning to an Application’s registry. The usage of an Authorization Token solves both problems with a very limited cost.

Bibliography

[FK92] Ferraiolo D.F., Kuhn D.R. : "Role-Based Access Control". 15th National Computer Security Conference: 554–563, 1992.

[CO02] Chadwick D.W., Otenko A., The PERMIS X.509 Role Based Privilege Management Infrastructure ISI, University of Salford, Salford, M5 4WT, 2002.

[WG12] Whitson Gordon: "Understanding OAuth: What Happens When You Log Into a Site with Google, Twitter, or Facebook". https://lifehacker.com/understanding-oauth-what-happens-when-you-log-into-a-s-5918086, 2012

[BS15] Bradley John, Sakimura Nat and Jones Michael: JWT: "JSON Web Token (JWT)". RFC7519, 2015

[EC17] JSON: "The JSON Data Interchange Format", http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf, 2017.

H. Roßnagel, C.H. Schunck, S. Mödersheim, D. Hühnlein (Hrsg.): Open Identity Summit 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2020 185

Data Protection Impact Assessment in Identity Management With a Focus on Biometrics

Tamas Bisztray[1], Nils Gruschka[2], Vasileios Mavroeidis[3], Lothar Fritsch[4]

Abstract:

Privacy issues concerning biometric identification are becoming increasingly relevant due to their proliferation in various fields, including identity and access control management (IAM). The General Data Protection Regulation (GDPR) requires the implementation of a data protection impact assessment for privacy critical systems. In this paper, we analyse the usefulness of two different privacy impact assessment frameworks in the context of biometric data protection. We use experiences from the SWAN project that processes four different biometric characteristics for authentication purposes. The results of this comparison elucidate how useful these frameworks are in identifying sector-specific privacy risks related to IAM and biometric identification.

Keywords: data protection, privacy, impact assessment, GDPR, DPIA, identity management, biometrics

1 Introduction

Managing digital identities involves the storage and processing of *personally identifiable information* (PII), i.e., data that link to individuals and can reveal confidential information such as name, address, date of birth etc. Biometric identifiers are PII and is a general term for describing a measurable physiological or behavioral characteristic of a person. Misuse of biometric data can have severe consequences [Ca13], such as identity theft or customer profiling. The European *General Data Protection Regulation* (GPDR) [Eu16] allows the processing of biometric data only under specific conditions, and it recommends conducting a *Data Privacy Impact Assessment* (DPIA).

The purpose of a DPIA is the evaluation of the activities related to data processing with respect to possible privacy risks (e.g., disclosure). Our research has identified two limiting factors applicable to DPIAs in the context of their usage. First, the GDPR does not provide any recommendations as to which of the available DPIA methods is preferred or any meaningful categorization of them. Second, privacy risks identified by the GDPR or a DPIA

[1] University of Oslo, Department of Informatics, Oslo, Norway tamasbi@ifi.uio.no
[2] University of Oslo, Department of Informatics, Oslo, Norway nilsgrus@ifi.ui.no
[3] University of Oslo, Department of Informatics, Oslo, Norway vasileim@ifi.uio.no
[4] Karlstad University, Dept. of Mathematics and Computer Science, Karlstad, Sweden Lothar.Fritsch@kau.se

are mostly generic and do not necessarily address risks applicable to particular sectors or technological domains. Although for some applications domain or sector-specific DPIA methodologies have been introduced, like RFID technologies [Eu11] and smart grid systems [Sm09], most of the existing widely-used methodologies are context independent. Thus, their use in different technological and sector-specific applications needs to be further studied.

This paper analyzes the usefulness of two different DPIA methodologies for the domain-specific use case of biometric authentication. First, we compile two lists of privacy requirements specific to IAM and biometric authentication. Second, we analyze and compare the adequacy of two widely used DPIA methodologies in assessing the privacy of the identified requirements by performing a DPIA on a biometric system and validating the results.

The paper is organized as follows. Section 2 provides background information on DPIA and the GDPR in the context of biometric authentication. Section 3 presents related work. Section 4 presents privacy requirements. Section 5 maps the identified requirements to two DPIA methodologies with the help of a concrete use case in biometrics. Finally, Section 6 discusses the results of the analysis conducted.

2 Background on Data Protection

The General Data Protection Regulation (GDPR) [Eu16] is the current privacy and data protection regulation in the European Union (including Norway, Liechtenstein, and Iceland). Of particular importance when processing data is Article 35 *Data protection impact assessment* that describes how a data controller should carry out a data protection impact assessment (DPIA) when the processing is likely to result in a high-risk related to the rights and freedoms of natural persons (data subjects). The GDPR does not provide an exhaustive list of high-risk processing operations that require a DPIA, but gives some examples within Article 35, such as *automated processing including profiling* and *personal data relating to criminal convictions and offences*.

Part of the recommendations of *Article 29 Working Party* (WP29) [Ar17] is a list of nine criteria that can be used for identifying processing operations that are likely to result in a high-risk, such as *evaluation or scoring for profiling*, and *automated decision making*. In such cases, a DPIA is recommended. It is worth mentioning that criterion 8 of WP29 is of high relevance to this research as it remarks on the potential high-risk involved when processing data for innovative use or for applying technological solutions, like in cases where multiple biometric modalities are combined for improved physical access control (e.g., fingerprint and face). The use case analyzed in this paper handles four different biometric modalities (face, iris, voice, and fingerprint) for the purpose of providing advanced biometric authentication technology in smartphone applications, such as online banking.

Article 35 specifies that a DPIA is required in cases where a type of processing is done with regards to new technology. In the context of this paper, the aforementioned is directly applicable since our use case develops innovative biometric technologies for identity and access management (IAM). What is considered to be biometric data is defined in Article 4(14). However, defining what is considered or not as new technology could be difficult to determine; thus, the general recommendation of GDPR is that in uncertain cases one should always consult the supervisory authority for recommendations. Since national-level regulations should not establish weaker criteria than the sophisticated GDPR, it is essential to review what GDPR includes about a specific topic. The Norwegian supervisory authority only requires a DPIA when biometric data is processed for identification purposes and when it is in conjunction with at least one additional criterion, whereas, Article 9(1) of GDPR clearly states that processing of biometric data for the purpose of uniquely identifying a natural person shall be prohibited, unless one of the conditions described in the second paragraph of Section 2 are fulfilled. Moreover, Recital 51 mentions that authentication will require the same precautions as identification.

Based on the above, an IDM system that can process biometric data needs to go through a DPIA because of the nature of the processing that identity management systems demand. In this context, biometric data is always used to uniquely identify a natural person, which is the type of processing that Article 9 refers to. Additionally, Article 35(3.b) states that the processing of such data on a large scale requires a DPIA. Recital 91 underlines the necessity of a DPIA if the scope of processing is for making decisions or profiling regarding specific natural persons. Consequently, this involves the processing of biometric data, and generally, it can be viewed as a field of landmines where an IDM system can easily fulfill several criteria that trigger the need for a data protection impact assessment. Finally, since the data subjects have the right to withdraw their consent (for processing or storing their information) at any time it is crucial to keep track of the biometric data throughout the life-cycle of the operations. For that reason a DPIA is very useful not only for being compliant, but also for having the ability to demonstrate compliance.

3 Related work

Meints et al. [Me08] outlined some of the key data protection principles concerning biometrics based on Article 29 Working Party's paper on biometrics [Ar03] and the Directive 95/46/EC. The GDPR repealed the latter, but the principles were kept and can be found throughout the Articles of the GDPR. Additionally, Meints et al. [Me08] pointed out relevant privacy-related risks regarding biometric data: identity theft, extraction and use of additional information in biometric reference data, linking of biometric data with other personal data and profiling, tracking and surveillance using biometric systems, misleading expectations of the reliability of biometric systems and violation of the right to informational self-determination by forcing people to use biometric systems. In [Re05] Rejman-Greene formulated 8 principles based on the Directive 95/46/EC. Some of these points can also

be found in [Me08], but in addition it mentions an important principle: *"Not keeping the data for longer than its necessary for the stated purposes (that is in a form that permits identification of the data subjects)"*.

Wuyts et al. [WJ15] evaluated the LINDDUN methodology using two case studies and concluded that it is easy to learn and useful in practice, but its completeness needs to be improved. In a study conducted by Veseli et al. [Ve19] LINDDUN was used for privacy risk assessment against a cloud-based platform named Identity Wallet Platform. In a previous work [BG19], we compared LINDDUN, ISO/IEC 29134:2017, and the framework from the Commission Nationale de l'Informatique et des Libertés (CNIL) which is an independent French administrative regulatory body. We evaluated their performance based on principles of data protection and privacy impact assessment collected from an extensive literature review. Hansen et al. [HJR15] identified six privacy protection goals for identity, and in another work [Ha13] the authors outlined some of the major privacy risk factors threatening these goals. In this paper, we use the identified risks as benchmarks along with the privacy risks of Meints [Me08] (that focus on biometrics), and other points identified in the literature to see how well are addressed by the frameworks we selected for our case study.

4 Privacy Protection Goals and Risks

The analysis in this paper focuses on privacy risks that occur when personal information is mishandled, and consequently, an individual's privacy is threatened. In our case study, the emphasis is given on finding privacy risks related to IAM [Ha13, Pa12] and raw biometric information or templates created from them. Privacy risks are divided into two tables based on if they are generally related to IAM or specifically to biometrics. The points discussed below are related to IAM and are collected in Table 1. IAM uses tokens to assign roles for access control. These are technical artifacts providing assurance about identities.

Token frequency and duration of use: information transfer between identity providers and service providers can allow profiling when the same token is used repeatedly. An identity management system should be designed in a way that prevents the activities of the end-user to be linked. For example, several services rely on Google and Facebook as an identity provider.

Token use and purpose: if a token is used for multiple purposes or services, it might be abused or processed illegally. It is essential to define who uses the ID infrastructure and determine how probable it is for the service providers to link different identifiers of the same user.

Provisioning: a token must be monitored through its whole life-cycle. Creation of a token should incorporate principles like data minimisation and clear purpose of use. Updating tokens should be possible for ensuring its authenticity and integrity. In addition, other attributes like deletion, transmission, and consent management should be available for the user.

Secrecy: a token needs to be classified according to the necessary secrecy level, such as inferable, public, or obfuscated supports token secrecy against linkability, re-identification, and unauthorised use. Inferable tokens are easily guessed, whereas public tokens are known by multiple people in an organisation or are available on several databases. In contrast, obfuscated tokens need to remain secret like a credit card pin.

Claim Type: attaching a claim to the token can increase its security. There are three types of claims: 1: information like a password, 2: physical characteristics like a fingerprint, 3: physical items like a card, or a USB key. Combining secrets with high entropy raises the cost for an attacker. Security levels can be managed based on single or multiple-factor authentication.

Obligation and Policy: a privacy policy for checking and evaluating data protection operations should be present.

Assignment and Relationship: defining how a token is created, assigned, and knowing who controls the token can contribute to reducing privacy or security risks. A token can be chosen by a person, can be jointly established, or forced upon by an authority.

Mobility: the following four properties characterize the degree of mobility of a token: *copyable*: how easily it can be copied; *remotely usable*: if it can be used for remote identity management; *concurrently usable*: if it can be used in parallel sessions; *immobile*: if it must be physically present to be used.

Value at risk: The significance of token security has to be classified based on the following events: loss, misuse, disclosure, disruption, theft and cost of replacing it.

Biometric systems handle biometric reference patterns that are attached to a person's identity. In risk and impact analysis, each of the above categories contributes to biometric privacy breach consequences. As explained in detail in [Pa12], major risks are introduced from the use of biometric identifiers when used by third parties without a data subject's consent (can lead to involuntary de-anonymization and profiling by others). The loss of biometric tokens (reference patterns) renders a fingerprint or face unusable (in case of primitive biometrics), which damages the data subject's ability to use this biometric feature in the future. Furthermore, the identified privacy risks specifically for biometric use cases [Me08],[Re05] are analysed as well as whether or not different DPIA methods address them. Table 2 presents the aforementioned privacy risks.

5 Case Study

5.1 Introduction to SWAN

The SWAN project (Secured access over Wide Area Network) is funded by the Research Council of Norway with the goal of researching and developing measures and innovative

technologies that lead to a usable, economic, and privacy-preserving access control based on biometric authentication. The project harvested and processed the following biometric characteristics: face, iris, fingers, and voice. Additionally, name, age, gender, and email address were collected from the data subjects. Data were collected for research purposes and specifically for developing a privacy-preserving access control platform based on biometrics. The envisioned application of the project is to authenticate banking transactions and to secure access to services over broadband and mobile networks. The project overcomes the need for centralized storage of biometric data by storing biometric references locally, and authentication is done based on a pre-shared secret. The inner workings of the authentication protocols were published in [HB10] and [SRB18].

5.2 Methodology

The SWAN project was first assessed using the CNIL's framework, followed by the ISO/IEC standard 29134:2017. Only after the impact assessments were conducted, we performed the analysis comparing its results to the specific privacy risks related to IDM and biometrics. This was done for avoiding being influenced during the assessment and not look for specifically these questions (or learn them after the first assessment), but to see if they can be discovered with the help of the frameworks. For each privacy risk, we analysed if performing the steps of a DPIA helps to identify the risk. If the framework addresses it, the point receives a checkmark ✓. The bias introduced by knowing the project is inevitable since it is a prerequisite for performing the DPIA. Note that neither of these is an exhaustive list, but they are meant to test the DPIA frameworks in a structured manner. The first table contains points for general IAM, whereas the second table focuses on questions specifically about biometrics.

Privacy Protection Risks in general IAM	ISO	CNIL
Token frequency and duration of use	-	-
Token use and purpose	✓	✓
Provisioning	✓	✓
Secrecy	-	-
Claim Type	-	✓
Obligation and Policy	✓	✓
Assignment and Relationship	-	-
Mobility	✓	-
Value at Risk	✓	✓

Tab. 1: Privacy Risks in IAM

The frameworks are performing equally in IAM related topics. Five out of nine points are addressed for each, but even jointly, they don't cover every important aspect.

Privacy Protection Risks in Biometrics	ISO	CNIL
Identity theft	-	✓
Extraction and use of additional information in biometric reference data	✓	✓
Tracking using biometric systems	-	-
Avoid misleading expectations of the reliability of biometric systems	✓	✓
Violation of the right to informational self determination by not giving other option but to use biometrics	-	✓
Explicit raw data disposal policy	-	-
De-anonymization by third parties	-	-

Tab. 2: Privacy Risk in Biometrics

CNIL performs better on addressing biometric specific privacy protection goals, but still, several questions are not addressed by either of the frameworks. This shows that general DPIA methodologies have to be complemented with additional sector-specific supporting materials.

6 Summary

In this paper, we have introduced privacy and data protection with a focus on biometric identification. We discussed the regulatory background and the existing principles for risk and impact assessment of biometric identity management with respect to privacy, as well as related privacy protection goals. In a direct comparison of the ISO/IEC 29134:2015 standard with the CNIL methodology, we found the CNIL method to be slightly better prepared for impact analysis of biometric systems. In general, IAM related questions performed equally, whereas in privacy protection risks for biometrics CNIL covered four out of seven points. In contrast, ISO addresses only two. However, none of these methods can be considered being a standalone solution for applications related to biometrics. The danger of de-anonymization by third parties is a critical privacy issue that is not addressed at all. The fact that CNIL performed better in this comparison regardless of the ISO standard better overall process shows that a good workflow provides no guarantee for addressing specific technological or sector-specific questions. For this reason, we emphasize the importance of developing official supporting documents and guidelines elaborating on privacy and data protection principles related to this rapidly growing field.

References

[Ar03] Article 29 Data Protection Working Party: WP 80 – Working Paper on Biometrics. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf, retrieved on 20.02.2020.

[Ar17] Article 29 Data Protection Working Party: Guidelines on Data Protection Impact Assessment (DPIA). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236, retrieved on 08.08.2019.

[BG19] Bisztray, Tamas; Gruschka, Nils: Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality. In: Nordic Conference on Secure IT Systems. Springer, 2019.

[Ca13] Campisi, Patrizio: Security and privacy in biometrics. Springer, 2013.

[Eu11] Privacy and Data Protection Impact Assessment Framework for RFID Applications. https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications, retrieved on 08.08.2019.

[Eu16] European Parliament & Council: Regulation (EU) 2016/679 – Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119(4.5.2016):1–88, April 2016.

[Ha13] Hansen, Marit et al.: FutureID Deliverable D22.3 Privacy Requirements. Technical report, 2013.

[HB10] Hartung, Daniel; Busch, Christoph: Biometric Transaction Authentication Protocol. In: 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies. pp. 207–215, July 2010. ISSN: 2162-2116.

[HJR15] Hansen, M.; Jensen, M.; Rost, M.: Protection Goals for Privacy Engineering. In: 2015 IEEE Security and Privacy Workshops. pp. 159–166, 2015.

[Me08] Meints, Martin et al.: Biometric Systems and Data Protection Legislation in Germany. In: 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing. pp. 1088–1093, 2008.

[Pa12] Paintsil, Ebenezer: Evaluation of privacy and security risks analysis construct for identity management systems. IEEE Systems Journal, 7(2):189–198, 2012.

[Re05] Rejman-Greene, Marek: Privacy Issues in the Application of Biometrics: a European Perspective. In (Wayman, James; Jain, Anil; Maltoni, Davide; Maio, Dario, eds): Biometric Systems: Technology, Design and Performance Evaluation, pp. 335–359. Springer London, London, 2005.

[Sm09] Smart Grids Task Force. https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force, retrieved 20.02.2020.

[SRB18] Stokkenes, Martin; Ramachandra, Raghavendra; Busch, Christoph: Biometric Transaction Authentication using Smartphones. In: 2018 International Conference of the Biometrics Special Interest Group (BIOSIG). pp. 1–5, September 2018.

[Ve19] Veseli, Fatbardh; Olvera, Jetzabel Serna; Pulls, Tobias; Rannenberg, Kai: Engineering privacy by design: lessons from the design and implementation of an identity wallet platform. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing - SAC '19. ACM Press, Limassol, Cyprus, pp. 1475–1483, 2019.

[WJ15] Wuyts, Kim; Joosen, Wouter: LINDDUN privacy threat modeling: a tutorial. CW Reports, 2015.

Towards Universal Login

Detlef Hühnlein[1], Tina Hühnlein[1], Gerrit Hornung[2], Hermann Strack[3]

Abstract: The present paper provides an overview of existing protocols and infrastructures for Identity Management on the Internet and discusses potential paths towards integrating the different approaches in a user centric manner into a "Universal Login" infrastructure, which allows Users to manage their authentication preferences and Service Providers to integrate with Identity Providers in an easy manner.

Keywords: SAML, OpenID Connect, FIDO, eIDAS

1 Introduction

Successful digital transformation relies on secure digital identities. In the light of the obvious need for user-friendly, legally compliant and trustworthy digital identities on the Internet, many different solutions for authentication and identification have emerged in recent years and hence there are many Identity Providers (IdP), which could perform the authentication and identification of Users on behalf a Service Provider (SP).

On the other hand, the large and seemingly still increasing number of IdPs leads to a rather fragmented market for identity services in which SPs and Users are often forced to use multiple IdPs to reach a sufficient service coverage. Furthermore, despite tireless standardisation and harmonisation efforts, the available infrastructures are not yet fully integrated in a seamless fashion, so that SPs either (1) would have to stick with one or a few IdPs, (2) undertake major, often uneconomic, integration efforts and engage in strategically unpleasant dependencies by supporting proprietary interfaces, or (3) completely forego the use of secure digital identities. To address this unfortunate situation, the present paper aims at paving the way for a "Universal Login" procedure in which the SPs are able to connect to arbitrary IdPs via a simple interface and the User (Subject) may select her favourite Credential or IdP for login at a certain SP.

To reach this goal, the rest of the paper is structured as follows: Section 2 recalls basics with resepect to Federated Identity Management. Section 3 introduces a refined reference architecture, which will form the technical basis for the "Universal Login" procedure presented in Section 4. The paper concludes with Section 5 by summarising the main aspects and providing an outlook towards potential future developments.

[1] {detlef.huehnlein, tina.huehnlein}@ecsec.de, ecsec GmbH, Sudetenstraße 16, 96247 Michelau, Germany
[2] gerrit.hornung@uni-kassel.de, Universität Kassel, Henschelstraße 4, 34127 Kassel, Germany
[3] hstrack@hs-harz.de, Hochschule Harz, Friedrichstraße 57-59, 38855 Wernigerode, Germany

2 An abstract model for Identity Management

Within the various approaches and infrastructures for Identity Management[4] one may recognise aspects related to *"Credential Management"*, in which a *"Subject"* (User) is equipped with some sort of digital credential, which allows to authenticate or prove certain claims, and aspects related to *"Federated Identity Management"* which allows that a *"Service Provider"* delegates the main tasks related to the management of credentials to one or more specialised *"Identity Providers"* while compensating this step with suitable *"Trust Management"* means.

2.1 Credential Management

The *Credential Management* comprises suitable procedures and protocols between the Subject and the IdP, whereas the credentials may involve multiple authentication factors[5] and provide a Level of Assurance (LoA)[6] ranging from "low" (e.g. user name and static password) over "substantial" (e.g. multiple factors within a dynamic authentication protocol) to "high" (e.g. highly secure and sophisticated credentials, which involve cryptographic hardware, which reliably prevent misuse of the credential protecting "against duplication and tampering as well as against attackers with high attack potential"[7]).

The Commission Implementing Regulation (EU) 2015/1502 specifies minimum requirements for the credentials to reach a certain LoA and [eID18] provides additional guidance for interpretation of the stipulations. There is a very wide range of possibilities for the implementation of credentials, which covers public-key based mechanisms with[8] or without certificates[9], with privacy-friendly features[10] or based on distributed ledger technology[11] as well as secret-key based mechanisms with a variety of protocols[12].

2.2 Federated Identity Management

The *Federated Identity Management* aspects especially comprise a suitable set of protocols for the secure integration of the three nodes of the system (Subject, SP and IdP), whereas the dominant protocol families in practice are [SAML] and [OpenID], which is

[4] See [KH14, SAML, OpenID, Ro12] for example.
[5] Section 1 (2) of CIR (EU) 2015/1502 distinguishes "possession-based", "knowledge-based" and "inherent authentication factors".
[6] See Art. 8 of Regulation (EU) No. 910/2014 and CIR (EU) 2015/1502.
[7] See CIR (EU) 2015/1502/EU, Annex, Section 2.2.1.
[8] Among the widely used formats are X.509-based (see [RFC 5280]) and card-verifiable certificates (see [BSI15], Part 3, Annex C).
[9] See [Bh15, W3C19a] for example.
[10] See [Ch85, IBM, Micr, CL01, Br95, W3C19b] for example.
[11] See [Ja16, Li18] for example.
[12] See [BM03, RFC 4226, RFC 6283, RFC 6287] for example.

in turn based on OAuth 2.0 [RFC 6749].

Note that this kind of federation is optional in the sense that the duties of the IdP, such as the issuing, management and validation of credentials, could be assumed by the SP itself and hence there is no distributed setup, but the authentication and identification may be performed by the SP itself.

2.3 Trust Management

With suitable *Trust Management* measures the SP seeks to compensate the loss of control due to delegating the security sensitive Credential Management tasks to the Identity Provider. The Trust Management measures may in particular comprise the stipulation and verification of requirements for the Credential Management, as specified in CIR (EU) 2015/1502/EU and outlined in Section 2.1. That the specified requirements are indeed fulfilled could be ensured by appropriate self-assessments, peer-reviews, independent audits or formal certification procedures. The trust information could be aligned to the various requirements defined in CIR (EU) 2015/1502 and encoded and organised and communicated within "vectors of trust" as specified in [RFC 8485].

3 Reference Architecture for Universal Login and more

The "Reference Architecture" presented in Figure 1 below is a refinement and enhancement of the classical model for Federated Identity Management and related architectures developed within previous work conducted in pertinent research projects, such as SkIDentity[13] and FutureID[14]. The most important aspects of this reference architecture are outlined in the following.

3.1 Trust, Discovery & Collaboration Framework

The "Trust, Discovery & Collaboration Framework" realises the "Trust Management" in a Federated Identity Management architecture and is an enhancement of the eIDAS Trust Framework[15] in the sense that it also includes not (yet) notified eID-schemes and IdPs, which are not formally endorsed by some EU Member State. As for those providers, there is no formal peer review in the sense of Chapter III of CIR (EU) 2015/296, and therefore there needs to be an adequate enhancement, which aims at maintaining a high level of trust and transparency. A possible path might be to introduce a two dimensional trust system (see Figure 2), which on the one hand side assesses which LoA is reached for an eID solution and Identity Provider with respect to the different requirements defined in

[13] See [KH14] and https://project.skidentity.de/en/publikationen/.
[14] See [Ro12].
[15] See Chapter 2 of Regulation (EU) No. 910/2014 and related implementing acts, such as CIR (EU) 2015/296, CIR (EU) 2015/1501, CIR (EU) 2015/1502, CIR (EU) 2015/1984 as well as additional guidance documents, such as [eID18] for example.

[2015/1502/EU] and listed in Section 2.1 and which "Level of Confidence" (LoC) was used for this assessment.

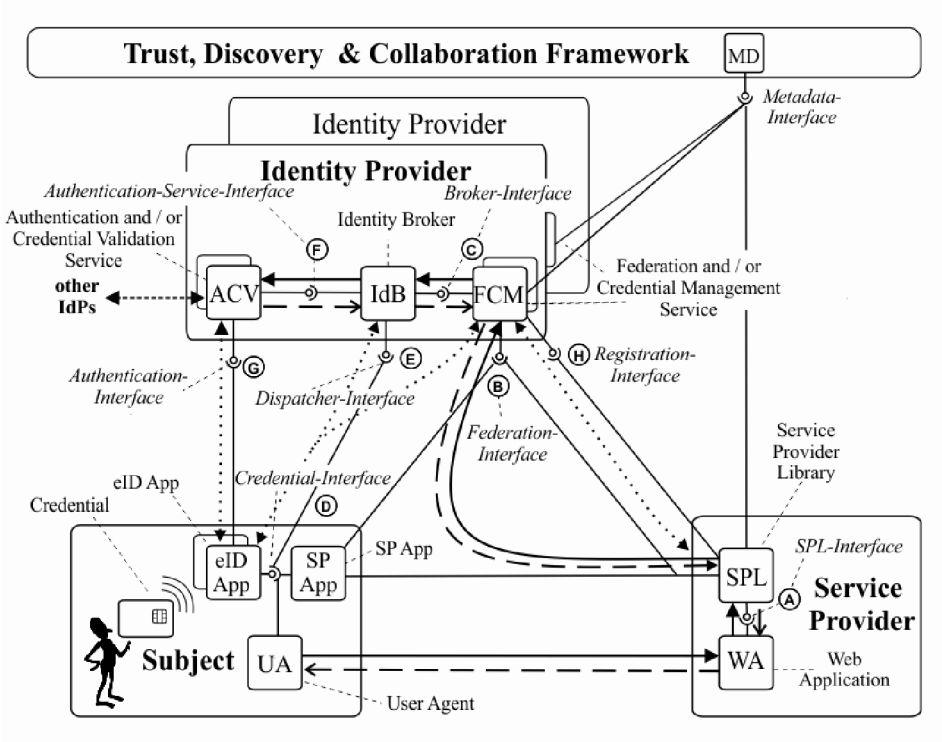


Figure 1: Reference Architecture for "Universal Login" and more

While the current eIDAS Trust Framework[16] only has one LoC-level, which corresponds to the formal notification according to Art. 9 of Regulation (EU) No. 910/2014, the enhanced trust system could have a graded approach with multiple levels, which could range from a simple self-assessment with or without validation (1) over external audits (2) and formal certifications (3) to the formal notification (4) of an eID scheme.

As the overall system is more open than the current eIDAS Trust Framework, it is important that there is some possibility for the trustworthy registration and retrieval of metadata for Identity Providers and SPs in standardised formats including [Ca05, Ca19a, Ca19b, Sa14a, Sa14b, RFC 8414, RFC 7591].

[16] For the legal background of this framework see [Ho16].

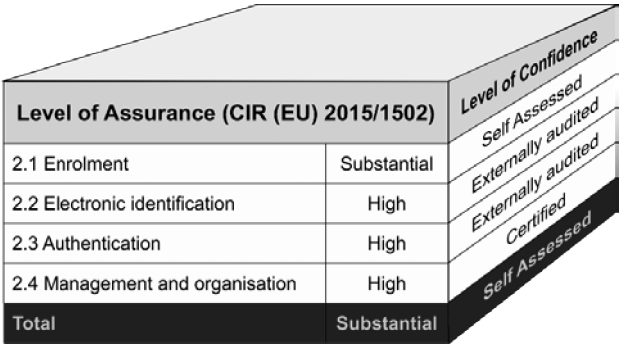


Figure 2: Enhanced Trust System with "Level of Confidence"

To enable a user friendly “Universal Login” procedure in which a User may select and persist its authentication preferences for a SP in its local storage, it is necessary (see also [Op19] and [Seamless] that the envisioned Trust, Discovery & Collaboration Framework allows to serve some “trustworthy JavaScript”[17] from a “neutral and trusted domain”[18], in order to support the management of the user preferences and persistence of the data in the local storage of the browser for the neutral and trusted domain.

3.2 Identity Provider

There may be a large number of Identity Providers, which may be “monolithic” in the sense that they support a single federation protocol and a single credential and authentication protocol, or “modular” in the sense that they may contain multiple Federation Services and Authentication Services, which are integrated via some Identity Broker. The latter approach also gives rise to the issuance and validation of credentials in various formats (see Section 2.1) and the invocation of other IdPs.

3.3 Subject

The Subject may in general be a natural or legal person, a (mobile) device, a computation node or even a service. Depending on the used credentials there may be one or more eID Apps besides the plain browser (User Agent) and a SP specific app (SP App), which complements the server side SP. A pivotal role plays the “Credential Interface” (D), as it may allow to discover that there is a specific eID App and credential or to initiate a protocol for issuing such a credential.

[17] For obvious reasons, the “trustworthy JavaScript” shall be available as open source.

[18] It needs to be ensured, by suitable privacy-specific certifications for example, that the neutral and trusted domain does not create any unwanted User or communication profiles, but only serves the said JavaScript in a reliable manner.

3.4 Service Provider

The SP typically contains a "Service Provider Library" (SPL), which handles the protocol flow based on [SAML] or [OpenID] after the corresponding metadata (see Section 3.1) have been registered at the supported IdPs and/or the central metadata repository. The SPL plays an important role in the practical and user friendly realisation of the envisioned "Universal Login" procedure outlined in Section 4 by letting (1) the SP configure its requirements including the acceptable LoA/LoC, IdPs and credentials and (2) by persisting the necessary history and previously chosen preferences of the User, such as the used credential, IdP and authentication options, for a specific SP.

4 Universal Login

The "Universal Login" procedure outlined in the present paper aims at enabling

- the SPs to easily support the relevant IdPs via standardised interfaces based on [SAML] or [OpenID] and
- the Users to manage their authentication preferences for the accessed SPs and involved IdPs and credentials in a suitable local storage on their device.

The IdPs benefit from the proposed approach by an increased number of participating SPs and Users.

After a suitable registration procedure, the metadata[19] of the participating IdPs is available in the "Trust, Discovery & Collaboration Framework" and can be retrieved from there by the SPs via a suitable interface[20]. Next, the SP is installing a suitable SPL, which supports [SAML] and/or [OpenID] and allows to register itself at the selected IdPs via some protocol along the lines of [Sa14a] and [RFC 7591]. Such SPLs may be built upon existing "Cloud Connector"[21] components, which have been created within the SkIDentity project.

Now the „Universal Login" system is set up and can be used. The process starts at the SP when the User wants to access a resource. If there are no authentication preferences stored or upon explicit request to enter the "configuration mode", the User is prompted to select the preferred authentication means (IdP, credential etc.) she wants to use at the specific SP. This information is stored within the local storage of the User via the trustworthy JavaScript, which is shipped via the neutral and trustworthy domain for example. In subsequent authentication processes the User's preferences can simply looked up, before the regular authentication process based on [SAML] or [OpenID] is performed. Besides this basic use case (User-driven management of authentication preferences), there may also be more advanced use cases which involve trustworthy identity attributes, which have

[19] See [Ca19a, Ca19b, Sa14b, RFC 8414].
[20] This interface can be built upon an enhanced version of [Hü19] and will allow to list the participating IdPs, which satisfy a set of specific criteria.
[21] See https://skidentity.com/cloud-connector and [KH14].

been retrieved from the User's credential or the storage of the IdP. This set of identity attributes may be signed and notarised by a suitable trust service, such as the "YourCredential" notarisation service, which has been developed in the StudIES+ EU CEF project [St19].

5 Conclusion and Outlook

In the present document we outlined a "Universal Login" framework, which allows Users to manage their authentication preferences for the accessed SPs and involved IdPs and SPs to easily integrate with IdPs via standardised interfaces based on [SAML] or [OpenID]. In the next step, the components and procedures sketched here will be specified technically and implemented within the SHIELD project[22], which will be supported by the German Federal Ministry of Economics.

Bibliography

[Bh15] Bharadwaj, V. & al. Web API for accessing FIDO 2.0 credentials, W3C Member Submission. https://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120/, 2015

[BM03] Boyd, C., Mathuria, A.: Protocols for authentication and key establishment, Springer, 2003

[Br05] Brands, S.: Secret-key certificates. Technical Report CS-R9510 CWI, 1995

[BSI15] Bundesamt für Sicherheit in der Informationstechnik (BSI): Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token, BSI TR-03110, 2015-2016

[Ca05] S. Cantor, J. Moreh, R. Philpott, E. Maler. Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf, 2005

[Ca19a] S. Cantor. SAML V2.0 Metadata Interoperability Profile Version 1.0, OASIS Standard. https://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop-os.pdf, 2019

[Ca19b] S. Cantor. SAML V2.0 Metadata Extensions for Login and Discovery User Interface Version 1.0, OASIS Standard. https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ui/v1.0/os/sstc-saml-metadata-ui-v1.0-os.pdf, 2019

[Ch85] Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. Communications of the ACM, 28 (10), pp. 1030-1044, 1985

[CL01] Camenisch, J., Lysyanskaya, A.: Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. EUROCRYPT 2001, LNCS 2045, pp. 93-118. Springer, 2001

[22] See https://shield24.de.

[eID18] eIDAS-Cooperation Network. Guidance for the application of the levels of assurance which support the eIDAS Regulation, 2018

[Ho16] Hornung, G.: Rechtliche Perspektiven des Identitätsmanagements in Europa. In C. E. G. Hornung, Der digitale Bürger und seine Identität (pp. 153-185). Nomos, 2016

[IBM10] IBM: Specification of the Identity Mixer Cryptographic Library. Version 2.3.0. http://domino.research.ibm.com/library/cyberdig.nsf/papers/EEB54FF3B91C1D648525759B004FBBB1/$File/rz3730_revised.pdf, 2010

[Ja16] Jacobovitz, O.: Blockchain for identity management. The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf, 2016

[KH14] Kubach, M., Hühnlein, D.: Vertrauenswürdige Identitäten für die Cloud: Arbeiten und Ergebnisse des SkIDentity-Projekts. Fraunhofer Verlag, 2014

[Li18] Lim, S. & al.: Blockchain technology the identity management and authentication service disruptor: a survey. International Journal on Advanced Science, p. 1735., 2018

[Micr] Microsoft: U-Prove. https://www.microsoft.com/en-us/research/project/u-prove/.

[Hü19] Hühnlein, D. (ed.): Digital Signature Service Metadata Version 1.0, OASIS CSD 02. https://docs.oasis-open.org/dss-x/dss-md/v1.0/dss-md-v1.0.html, 2019

[Op19] OpenID WG: Account Chooser & Open YOLO (You Only Login Once) Working Group Home Page. https://openid.net/wg/ac/, 2019

[OpenID] OpenID Foundation. Specifications. https://openid.net/developers/specs/

[Ro12] Roßnagel, H., Camenisch, J., Fritsch, L., Gross, T., Houdeau, D., Lehmann, A., & Shamah, J. (2012, 36 3). FutureID – Shaping the Future of Electronic Identity. DuD, pp. 189-194.

[Sa14a] N. Sakimura, J. Bradley, M. Jones: OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 1, https://openid.net/specs/openid-connect-registration-1_0.html, 2014

[Sa14b] N. Sakimura, J. Bradley, M. Jones, E. Jay: OpenID Connect Discovery 1.0 incorporating errata set 1, https://openid.net/specs/openid-connect-discovery-1_0.html, 2014

[SAML] OASIS. SAML Wiki. https://wiki.oasis-open.org/security/FrontPage

[Seamless] Welcome to SeamlessAccess.org. We offer seamless access. You get research as it should be. https://seamlessaccess.org/, 2019

[St19] Strack, H., Otto, O., Klinner, S., & Schmidt, A.: eIDAS eID & eSignature based Service Accounts at University environments for cross-border/domain access. Open Identity Summit 2019 (pp. 171-176). Bonn: GI, LNI 293, 2019

[W3C19a] W3C: Web Authentication: An API for accessing Public Key Credentials Level 1. W3C Recommendation. https://www.w3.org/TR/webauthn-1/, 2019

[W3C19b] W3C: Verifiable Credentials Data Model 1.0 - Expressing verifiable information on the Web. W3C Recommendation. https://www.w3.org/TR/vc-data-model/, 2019

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Lan-guage to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni_ (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund (Ergänzungs-band).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Er-fahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures, Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 24. July 2003 in Darmstadt, Germany

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Adhoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): “Heute schon das Morgen sehen“

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems

P-86 Robert Krimmer (Ed.): Electronic Voting 2006

P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik

P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006

P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur

P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006

P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006

P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1

P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2

P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen

P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies

P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006

P-98 Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices

P-99 Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik

P-100 Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik

P-101 Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten

P-102 Otto Spaniol (Eds.): Mobile Services and Personalized Environments

P-103 Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)

P-104 Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.) MMS 2007: Mobilität und mobile Informationssysteme

P-105 Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.) Software Engineering 2007

P-106 Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.) Software Engineering 2007 – Beiträge zu den Workshops

P-107 Heinrich C. Mayr, Dimitris Karagiannis (eds.) Information Systems Technology and its Applications

P-108 Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.) BIOSIG 2007: Biometrics and Electronic Signatures

P-109 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 1

P-110 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 2

P-111 Christian Eibl, Johannes Magenheim, Sigrid Schubert, Martin Wessner (Hrsg.) DeLFI 2007: 5. e-Learning Fachtagung Informatik

P-112 Sigrid Schubert (Hrsg.) Didaktik der Informatik in Theorie und Praxis

P-113 Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.) The Social Semantic Web 2007 Proceedings of the 1st Conference on Social Semantic Web (CSSW)

P-114 Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.) IMF2007 IT-incident management & IT-forensics Proceedings of the 3rd International Conference on IT-Incident Management & IT-Forensics

P-115 Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walther (Eds.) German conference on bioinformatics GCB 2007

P-116 Witold Abramowicz, Leszek Maciszek (Eds.) Business Process and Services Computing 1st International Working Conference on Business Process and Services Computing BPSC 2007

P-117 Ryszard Kowalczyk (Ed.) Grid service engineering and manegement The 4th International Conference on Grid Service Engineering and Management GSEM 2007

P-118 Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.) European Conference on ehealth 2007

P-119 Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.) Enterprise Modelling and Information Systems Architectures Concepts and Applications

P-120 Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa, Leandro Soares Indrusiak (Eds.) Coordination of Collaborative Engineering - State of the Art and Future Challenges

P-121 Korbinian Herrmann, Bernd Bruegge (Hrsg.) Software Engineering 2008 Fachtagung des GI-Fachbereichs Softwaretechnik

P-122 Walid Maalej, Bernd Bruegge (Hrsg.) Software Engineering 2008 - Workshopband Fachtagung des GI-Fachbereichs Softwaretechnik

P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008)

P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)
9th Workshop on Parallel Systems and Algorithms (PASA)
Workshop of the GI/ITG Speciel Interest Groups PARS and PARVA

P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)
Unternehmens-IT:
Führungsinstrument oder Verwaltungsbürde
Referate der 28. GIL Jahrestagung

P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)
10th Workshop Software Reengineering (WSR 2008)

P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)
Modellierung 2008

P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)
Sicherheit 2008
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
2.-4. April 2008
Saarbrücken, Germany

P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)
Sigsand-Europe 2008
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems

P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
1. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung

P-131 Robert Krimmer, Rüdiger Grimm (Eds.)
3rd International Conference on Electronic Voting 2008
Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting. CC

P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)
DeLFI 2008:
Die 6. e-Learning Fachtagung Informatik

P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 1

P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 2

P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)
Didaktik der Informatik –
Aktuelle Forschungsergebnisse

P-136 Andreas Beyer, Michael Schroeder (Eds.)
German Conference on Bioinformatics GCB 2008

P-137 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2008: Biometrics and Electronic Signatures

P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)
Synergien durch Integration und Informationslogistik
Proceedings zur DW2008

P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)
Industrialisierung des Software-Managements
Fachtagung des GI-Fachausschusses Management der Anwendungsentwick-lung und -wartung im Fachbereich Wirtschaftsinformatik

P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)
IMF 2008 - IT Incident Management & IT Forensics

P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)
Modellierung betrieblicher Informations-systeme (MobIS 2008)
Modellierung zwischen SOA und Compliance Management

P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung

P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)
Software Engineering 2009
Fachtagung des GI-Fachbereichs Softwaretechnik

P-144 Johann-Christoph Freytag, Thomas Ruf, Wolfgang Lehner, Gottfried Vossen (Hrsg.)
Datenbanksysteme in Business, Technologie und Web (BTW)

P-145 Knut Hinkelmann, Holger Wache (Eds.)
WM2009: 5th Conference on Professional Knowledge Management

P-146 Markus Bick, Martin Breunig, Hagen Höpfner (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Entwicklung, Implementierung und Anwendung
4. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2009)

P-147 Witold Abramowicz, Leszek Maciaszek, Ryszard Kowalczyk, Andreas Speck (Eds.)
Business Process, Services Computing and Intelligent Service Management
BPSC 2009 · ISM 2009 · YRW-MBP 2009

P-148 Christian Erfurth, Gerald Eichler, Volkmar Schau (Eds.)
9th International Conference on Innovative Internet Community Systems
I^{2}CS 2009

P-149 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
2. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)
Software Engineering
2009 - Workshopband

P-151 Armin Heinzl, Peter Dadam, Stefan Kirn, Peter Lockemann (Eds.)
PRIMIUM
Process Innovation for Enterprise Software

P-152 Jan Mendling, Stefanie Rinderle-Ma, Werner Esswein (Eds.)
Enterprise Modelling and Information Systems Architectures
Proceedings of the 3rd Int'l Workshop EMISA 2009

P-153 Andreas Schwill, Nicolas Apostolopoulos (Hrsg.)
Lernen im Digitalen Zeitalter
DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik

P-154 Stefan Fischer, Erik Maehle Rüdiger Reischuk (Hrsg.)
INFORMATIK 2009
Im Focus das Leben

P-155 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2009:
Biometrics and Electronic Signatures
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-156 Bernhard Koerber (Hrsg.)
Zukunft braucht Herkunft
25 Jahre »INFOS – Informatik und Schule«

P-157 Ivo Grosse, Steffen Neumann, Stefan Posch, Falk Schreiber, Peter Stadler (Eds.)
German Conference on Bioinformatics 2009

P-158 W. Claupein, L. Theuvsen, A. Kämpf, M. Morgenstern (Hrsg.)
Precision Agriculture Reloaded – Informationsgestützte Landwirtschaft

P-159 Gregor Engels, Markus Luckey, Wilhelm Schäfer (Hrsg.)
Software Engineering 2010

P-160 Gregor Engels, Markus Luckey, Alexander Pretschner, Ralf Reussner (Hrsg.)
Software Engineering 2010 – Workshopband
(inkl. Doktorandensymposium)

P-161 Gregor Engels, Dimitris Karagiannis Heinrich C. Mayr (Hrsg.)
Modellierung 2010

P-162 Maria A. Wimmer, Uwe Brinkhoff, Siegfried Kaiser, Dagmar Lück-Schneider, Erich Schweighofer, Andreas Wiebe (Hrsg.)
Vernetzte IT für einen effektiven Staat
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2010

P-163 Markus Bick, Stefan Eulgem, Elgar Fleisch, J. Felix Hampe, Birgitta König-Ries, Franz Lehner, Key Pousttchi, Kai Rannenberg (Hrsg.)
Mobile und Ubiquitäre Informationssysteme
Technologien, Anwendungen und Dienste zur Unterstützung von mobiler Kollaboration

P-164 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2010: Biometrics and Electronic Signatures Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-165 Gerald Eichler, Peter Kropf, Ulrike Lechner, Phayung Meesad, Herwig Unger (Eds.)
10th International Conference on Innovative Internet Community Systems (I^2CS) – Jubilee Edition 2010 –

P-166 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
3. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-167 Robert Krimmer, Rüdiger Grimm (Eds.)
4th International Conference on Electronic Voting 2010
co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-168 Ira Diethelm, Christina Dörge, Claudia Hildebrandt, Carsten Schulte (Hrsg.)
Didaktik der Informatik
Möglichkeiten empirischer Forschungsmethoden und Perspektiven der Fachdidaktik

P-169 Michael Kerres, Nadine Ojstersek Ulrik Schroeder, Ulrich Hoppe (Hrsg.)
DeLFI 2010 - 8. Tagung der Fachgruppe E-Learning der Gesellschaft für Informatik e.V.

P-170 Felix C. Freiling (Hrsg.)
Sicherheit 2010
Sicherheit, Schutz und Zuverlässigkeit

P-171 Werner Esswein, Klaus Turowski, Martin Juhrisch (Hrsg.)
Modellierung betrieblicher Informationssysteme (MobIS 2010)
Modellgestütztes Management

P-172 Stefan Klink, Agnes Koschmider Marco Mevius, Andreas Oberweis (Hrsg.)
EMISA 2010
Einflussfaktoren auf die Entwicklung flexibler, integrierter Informationssysteme
Beiträge des Workshops der GI-Fachgruppe EMISA (Entwicklungsmethoden für Informationssysteme und deren Anwendung)

P-173 Dietmar Schomburg, Andreas Grote (Eds.)
German Conference on Bioinformatics 2010

P-174 Arslan Brömme, Torsten Eymann, Detlef Hühnlein, Heiko Roßnagel, Paul Schmücker (Hrsg.)
perspeGKtive 2010
Workshop „Innovative und sichere Informationstechnologie für das Gesundheitswesen von morgen“

P-175 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 1

P-176 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 2

P-177 Witold Abramowicz, Rainer Alt, Klaus-Peter Fähnrich, Bogdan Franczyk, Leszek A. Maciaszek (Eds.)
INFORMATIK 2010
Business Process and Service Science – Proceedings of ISSS and BPSC

P-178 Wolfram Pietsch, Benedikt Krams (Hrsg.)
Vom Projekt zum Produkt
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschafts-informatik (WI-MAW), Aachen, 2010

P-179 Stefan Gruner, Bernhard Rumpe (Eds.)
FM+AM`2010
Second International Workshop on Formal Methods and Agile Methods

P-180 Theo Härder, Wolfgang Lehner, Bernhard Mitschang, Harald Schöning, Holger Schwarz (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW)
14. Fachtagung des GI-Fachbereichs „Datenbanken und Informationssysteme“ (DBIS)

P-181 Michael Clasen, Otto Schätzel, Brigitte Theuvsen (Hrsg.)
Qualität und Effizienz durch informationsgestützte Landwirtschaft, Fokus: Moderne Weinwirtschaft

P-182 Ronald Maier (Hrsg.)
6th Conference on Professional Knowledge Management
From Knowledge to Action

P-183 Ralf Reussner, Matthias Grund, Andreas Oberweis, Walter Tichy (Hrsg.)
Software Engineering 2011
Fachtagung des GI-Fachbereichs Softwaretechnik

P-184 Ralf Reussner, Alexander Pretschner, Stefan Jähnichen (Hrsg.)
Software Engineering 2011
Workshopband
(inkl. Doktorandensymposium)

P-185 Hagen Höpfner, Günther Specht, Thomas Ritz, Christian Bunse (Hrsg.)
MMS 2011: Mobile und ubiquitäre Informationssysteme Proceedings zur 6. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2011)

P-186 Gerald Eichler, Axel Küpper, Volkmar Schau, Hacène Fouchal, Herwig Unger (Eds.)
11th International Conference on Innovative Internet Community Systems (I^2CS)

P-187 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
4. DFN-Forum Kommunikations-technologien, Beiträge der Fachtagung 20. Juni bis 21. Juni 2011 Bonn

P-188 Holger Rohland, Andrea Kienle, Steffen Friedrich (Hrsg.)
DeLFI 2011 – Die 9. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. 5.–8. September 2011, Dresden

P-189 Thomas, Marco (Hrsg.)
Informatik in Bildung und Beruf
INFOS 2011
14. GI-Fachtagung Informatik und Schule

P-190 Markus Nüttgens, Oliver Thomas, Barbara Weber (Eds.)
Enterprise Modelling and Information Systems Architectures (EMISA 2011)

P-191 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2011
International Conference of the Biometrics Special Interest Group

P-192 Hans-Ulrich Heiß, Peter Pepper, Holger Schlingloff, Jörg Schneider (Hrsg.)
INFORMATIK 2011
Informatik schafft Communities

P-193 Wolfgang Lehner, Gunther Piller (Hrsg.)
IMDM 2011

P-194 M. Clasen, G. Fröhlich, H. Bernhardt, K. Hildebrand, B. Theuvsen (Hrsg.)
Informationstechnologie für eine nachhaltige Landbewirtschaftung
Fokus Forstwirtschaft

P-195 Neeraj Suri, Michael Waidner (Hrsg.)
Sicherheit 2012
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)

P-196 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2012
Proceedings of the 11th International Conference of the Biometrics Special Interest Group

P-197 Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser, Erich Schweighofer, Maria A. Wimmer (Hrsg.)
Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012

P-198 Stefan Jähnichen, Axel Küpper, Sahin Albayrak (Hrsg.)
Software Engineering 2012
Fachtagung des GI-Fachbereichs Softwaretechnik

P-199 Stefan Jähnichen, Bernhard Rumpe, Holger Schlingloff (Hrsg.)
Software Engineering 2012
Workshopband

P-200 Gero Mühl, Jan Richling, Andreas Herkersdorf (Hrsg.)
ARCS 2012 Workshops

P-201 Elmar J. Sinz Andy Schürr (Hrsg.)
Modellierung 2012

P-202 Andrea Back, Markus Bick, Martin Breunig, Key Pousttchi, Frédéric Thiesse (Hrsg.)
MMS 2012:Mobile und Ubiquitäre Informationssysteme

P-203 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
5. DFN-Forum Kommunikations-technologien
Beiträge der Fachtagung

P-204 Gerald Eichler, Leendert W. M. Wienhofen, Anders Kofod-Petersen, Herwig Unger (Eds.)
12th International Conference on Innovative Internet Community Systems (I2CS 2012)

P-205 Manuel J. Kripp, Melanie Volkamer, Rüdiger Grimm (Eds.)
5th International Conference on Electronic Voting 2012 (EVOTE2012)
Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-206 Stefanie Rinderle-Ma, Mathias Weske (Hrsg.)
EMISA 2012
Der Mensch im Zentrum der Modellierung

P-207 Jörg Desel, Jörg M. Haake, Christian Spannagel (Hrsg.)
DeLFI 2012: Die 10. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V.
24.–26. September 2012

P-208 Ursula Goltz, Marcus Magnor, Hans-Jürgen Appelrath, Herbert Matthies, Wolf-Tilo Balke, Lars Wolf (Hrsg.) INFORMATIK 2012

P-209 Hans Brandt-Pook, André Fleer, Thorsten Spitta, Malte Wattenberg (Hrsg.) Nachhaltiges Software Management

P-210 Erhard Plödereder, Peter Dencker, Herbert Klenk, Hubert B. Keller, Silke Spitzer (Hrsg.) Automotive – Safety & Security 2012 Sicherheit und Zuverlässigkeit für automobile Informationstechnik

P-211 M. Clasen, K. C. Kersebaum, A. Meyer-Aurich, B. Theuvsen (Hrsg.) Massendatenmanagement in der Agrar- und Ernährungswirtschaft Erhebung - Verarbeitung - Nutzung Referate der 33. GIL-Jahrestagung 20. – 21. Februar 2013, Potsdam

P-212 Arslan Brömme, Christoph Busch (Eds.) BIOSIG 2013 Proceedings of the 12th International Conference of the Biometrics Special Interest Group 04.–06. September 2013 Darmstadt, Germany

P-213 Stefan Kowalewski, Bernhard Rumpe (Hrsg.) Software Engineering 2013 Fachtagung des GI-Fachbereichs Softwaretechnik

P-214 Volker Markl, Gunter Saake, Kai-Uwe Sattler, Gregor Hackenbroich, Bernhard Mit schang, Theo Härder, Veit Köppen (Hrsg.) Datenbanksysteme für Business, Technologie und Web (BTW) 2013 13. – 15. März 2013, Magdeburg

P-215 Stefan Wagner, Horst Lichter (Hrsg.) Software Engineering 2013 Workshopband (inkl. Doktorandensymposium) 26. Februar – 1. März 2013, Aachen

P-216 Gunter Saake, Andreas Henrich, Wolfgang Lehner, Thomas Neumann, Veit Köppen (Hrsg.) Datenbanksysteme für Business, Technologie und Web (BTW) 2013 – Workshopband 11. – 12. März 2013, Magdeburg

P-217 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.) 6. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung 03.–04. Juni 2013, Erlangen

P-218 Andreas Breiter, Christoph Rensing (Hrsg.) DeLFI 2013: Die 11 e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. (GI) 8. – 11. September 2013, Bremen

P-219 Norbert Breier, Peer Stechert, Thomas Wilke (Hrsg.) Informatik erweitert Horizonte INFOS 2013 15. GI-Fachtagung Informatik und Schule 26. – 28. September 2013

P-220 Matthias Horbach (Hrsg.) INFORMATIK 2013 Informatik angepasst an Mensch, Organisation und Umwelt 16. – 20. September 2013, Koblenz

P-221 Maria A. Wimmer, Marijn Janssen, Ann Macintosh, Hans Jochen Scholl, Efthimios Tambouris (Eds.) Electronic Government and Electronic Participation Joint Proceedings of Ongoing Research of IFIP EGOV and IFIP ePart 2013 16. – 19. September 2013, Koblenz

P-222 Reinhard Jung, Manfred Reichert (Eds.) Enterprise Modelling and Information Systems Architectures (EMISA 2013) St. Gallen, Switzerland September 5. – 6. 2013

P-223 Detlef Hühnlein, Heiko Roßnagel (Hrsg.) Open Identity Summit 2013 10. – 11. September 2013 Kloster Banz, Germany

P-224 Eckhart Hanser, Martin Mikusz, Masud Fazal-Baqaie (Hrsg.) Vorgehensmodelle 2013 Vorgehensmodelle – Anspruch und Wirklichkeit 20. Tagung der Fachgruppe Vorgehensmodelle im Fachgebiet Wirtschaftsinformatik (WI-VM) der Gesellschaft für Informatik e.V. Lörrach, 2013

P-225 Hans-Georg Fill, Dimitris Karagiannis, Ulrich Reimer (Hrsg.) Modellierung 2014 19. – 21. März 2014, Wien

P-226 M. Clasen, M. Hamer, S. Lehnert, B. Petersen, B. Theuvsen (Hrsg.) IT-Standards in der Agrar- und Ernährungswirtschaft Fokus: Risiko- und Krisenmanagement Referate der 34. GIL-Jahrestagung 24. – 25. Februar 2014, Bonn

P-227 Wilhelm Hasselbring,
Nils Christian Ehmke (Hrsg.)
Software Engineering 2014
Fachtagung des GI-Fachbereichs Softwaretechnik
25. – 28. Februar 2014
Kiel, Deutschland

P-228 Stefan Katzenbeisser, Volkmar Lotz, Edgar Weippl (Hrsg.)
Sicherheit 2014
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
19. – 21. März 2014, Wien

P-229 Dagmar Lück-Schneider, Thomas Gordon, Siegfried Kaiser, Jörn von Lucke,Erich Schweighofer, Maria A.Wimmer, Martin G. Löhe (Hrsg.)
Gemeinsam Electronic Government ziel(gruppen)gerecht gestalten und organisieren
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI)
2014, 20.-21. März 2014 in Berlin

P-230 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2014
Proceedings of the 13th International Conference of the Biometrics Special Interest Group
10. – 12. September 2014 in Darmstadt, Germany

P-231 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
7. DFN-Forum Kommunikationstechnologien
16. – 17. Juni 2014
Fulda

P-232 E. Plödereder, L. Grunske, E. Schneider, D. Ull (Hrsg.)
INFORMATIK 2014
Big Data – Komplexität meistern
22. – 26. September 2014
Stuttgart

P-233 Stephan Trahasch, Rolf Plötzner, Gerhard Schneider, Claudia Gayer, Daniel Sassiat, Nicole Wöhrle (Hrsg.)
DeLFI 2014 – Die 12. e-Learning Fachtagung Informatik
der Gesellschaft für Informatik e.V.
15. – 17. September 2014
Freiburg

P-234 Fernand Feltz, Bela Mutschler, Benoît Otjacques (Eds.)
Enterprise Modelling and Information Systems Architectures
(EMISA 2014)
Luxembourg, September 25-26, 2014

P-235 Robert Giegerich, Ralf Hofestädt, Tim W. Nattkemper (Eds.)
German Conference on Bioinformatics 2014
September 28 – October 1
Bielefeld, Germany

P-236 Martin Engstler, Eckhart Hanser, Martin Mikusz, Georg Herzwurm (Hrsg.)
Projektmanagement und Vorgehensmodelle 2014
Soziale Aspekte und Standardisierung
Gemeinsame Tagung der Fachgruppen Projektmanagement (WI-PM) und Vorgehensmodelle (WI-VM) im Fachgebiet Wirtschaftsinformatik der Gesellschaft für Informatik e.V., Stuttgart 2014

P-237 Detlef Hühnlein, Heiko Roßnagel (Hrsg.)
Open Identity Summit 2014
4.–6. November 2014
Stuttgart, Germany

P-238 Arno Ruckelshausen, Hans-Peter Schwarz, Brigitte Theuvsen (Hrsg.)
Informatik in der Land-, Forst- und Ernährungswirtschaft
Referate der 35. GIL-Jahrestagung
23. – 24. Februar 2015, Geisenheim

P-239 Uwe Aßmann, Birgit Demuth, Thorsten Spitta, Georg Püschel, Ronny Kaiser (Hrsg.)
Software Engineering & Management 2015
17.-20. März 2015, Dresden

P-240 Herbert Klenk, Hubert B. Keller, Erhard Plödereder, Peter Dencker (Hrsg.)
Automotive – Safety & Security 2015
Sicherheit und Zuverlässigkeit für automobile Informationstechnik
21.–22. April 2015, Stuttgart

P-241 Thomas Seidl, Norbert Ritter, Harald Schöning, Kai-Uwe Sattler, Theo Härder, Steffen Friedrich, Wolfram Wingerath (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW 2015)
04. – 06. März 2015, Hamburg

P-242 Norbert Ritter, Andreas Henrich, Wolfgang Lehner, Andreas Thor, Steffen Friedrich, Wolfram Wingerath (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW 2015) – Workshopband
02. – 03. März 2015, Hamburg

P-243 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
8. DFN-Forum Kommunikationstechnologien
06.–09. Juni 2015, Lübeck

P-244 Alfred Zimmermann, Alexander Rossmann (Eds.)
Digital Enterprise Computing (DEC 2015)
Böblingen, Germany June 25-26, 2015

P-245 Arslan Brömme, Christoph Busch , Christian Rathgeb, Andreas Uhl (Eds.)
BIOSIG 2015
Proceedings of the 14th International Conference of the Biometrics Special Interest Group
09.–11. September 2015
Darmstadt, Germany

P-246 Douglas W. Cunningham, Petra Hofstedt, Klaus Meer, Ingo Schmitt (Hrsg.)
INFORMATIK 2015
28.9.-2.10. 2015, Cottbus

P-247 Hans Pongratz, Reinhard Keil (Hrsg.)
DeLFI 2015 – Die 13. E-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. (GI)
1.–4. September 2015
München

P-248 Jens Kolb, Henrik Leopold, Jan Mendling (Eds.)
Enterprise Modelling and Information Systems Architectures
Proceedings of the 6th Int. Workshop on Enterprise Modelling and Information Systems Architectures, Innsbruck, Austria
September 3-4, 2015

P-249 Jens Gallenbacher (Hrsg.)
Informatik allgemeinbildend begreifen
INFOS 2015 16. GI-Fachtagung Informatik und Schule
20.–23. September 2015

P-250 Martin Engstler, Masud Fazal-Baqaie, Eckhart Hanser, Martin Mikusz, Alexander Volland (Hrsg.)
Projektmanagement und Vorgehensmodelle 2015
Hybride Projektstrukturen erfolgreich umsetzen
Gemeinsame Tagung der Fachgruppen Projektmanagement (WI-PM) und Vorgehensmodelle (WI-VM) im Fachgebiet Wirtschaftsinformatik der Gesellschaft für Informatik e.V., Elmshorn 2015

P-251 Detlef Hühnlein, Heiko Roßnagel, Raik Kuhlisch, Jan Ziesing (Eds.)
Open Identity Summit 2015
10.–11. November 2015
Berlin, Germany

P-252 Jens Knoop, Uwe Zdun (Hrsg.)
Software Engineering 2016
Fachtagung des GI-Fachbereichs Softwaretechnik
23.–26. Februar 2016, Wien

P-253 A. Ruckelshausen, A. Meyer-Aurich, T. Rath, G. Recke, B. Theuvsen (Hrsg.)
Informatik in der Land-, Forst- und Ernährungswirtschaft
Fokus: Intelligente Systeme – Stand der Technik und neue Möglichkeiten
Referate der 36. GIL-Jahrestagung
22.-23. Februar 2016, Osnabrück

P-254 Andreas Oberweis, Ralf Reussner (Hrsg.)
Modellierung 2016
2.–4. März 2016, Karlsruhe

P-255 Stefanie Betz, Ulrich Reimer (Hrsg.)
Modellierung 2016 Workshopband
2.–4. März 2016, Karlsruhe

P-256 Michael Meier, Delphine Reinhardt, Steffen Wendzel (Hrsg.)
Sicherheit 2016
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 8. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
5.–7. April 2016, Bonn

P-257 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
9. DFN-Forum Kommunikationstechnologien
31. Mai – 01. Juni 2016, Rostock

P-258 Dieter Hertweck, Christian Decker (Eds.)
Digital Enterprise Computing (DEC 2016)
14.–15. Juni 2016, Böblingen

P-259 Heinrich C. Mayr, Martin Pinzger (Hrsg.)
INFORMATIK 2016
26.–30. September 2016, Klagenfurt

P-260 Arslan Brömme, Christoph Busch, Christian Rathgeb, Andreas Uhl (Eds.)
BIOSIG 2016
Proceedings of the 15th International Conference of the Biometrics Special Interest Group
21.–23. September 2016, Darmstadt

P-261 Detlef Rätz, Michael Breidung, Dagmar Lück-Schneider, Siegfried Kaiser, Erich Schweighofer (Hrsg.)
Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltung
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2016
22.–23. September 2016, Dresden

P-262 Ulrike Lucke, Andreas Schwill, Raphael Zender (Hrsg.)
DeLFI 2016 – Die 14. E-Learning Fachtagung Informatik
der Gesellschaft für Informatik e.V. (GI)
11.–14. September 2016, Potsdam

P-263 Martin Engstler, Masud Fazal-Baqaie, Eckhart Hanser, Oliver Linssen, Martin Mikusz, Alexander Volland (Hrsg.)
Projektmanagement und Vorgehensmodelle 2016
Arbeiten in hybriden Projekten: Das Sowohl-als-auch von Stabilität und Dynamik
Gemeinsame Tagung der Fachgruppen Projektmanagement (WI-PM) und Vorgehensmodelle (WI-VM) im Fachgebiet Wirtschaftsinformatik
der Gesellschaft für Informatik e.V., Paderborn 2016

P-264 Detlef Hühnlein, Heiko Roßnagel, Christian H. Schunck, Maurizio Talamo (Eds.)
Open Identity Summit 2016
der Gesellschaft für Informatik e.V. (GI)
13.–14. October 2016, Rome, Italy

P-265 Bernhard Mitschang, Daniela Nicklas,Frank Leymann, Harald Schöning, Melanie Herschel, Jens Teubner, Theo Härder, Oliver Kopp, Matthias Wieland (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW 2017)
6.–10. März 2017, Stuttgart

P-266 Bernhard Mitschang, Norbert Ritter, Holger Schwarz, Meike Klettke, Andreas Thor, Oliver Kopp, Matthias Wieland (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW 2017)
Workshopband
6.–7. März 2017, Stuttgart

P-267 Jan Jürjens, Kurt Schneider (Hrsg.)
Software Engineering 2017
21.–24. Februar 2017, Hannover

P-268 A. Ruckelshausen, A. Meyer-Aurich, W. Lentz, B. Theuvsen (Hrsg.)
Informatik in der Land-, Forst- und Ernährungswirtschaft
Fokus: Digitale Transformation – Wege in eine zukunftsfähige Landwirtschaft
Referate der 37. GIL-Jahrestagung
06.–07. März 2017, Dresden

P-269 Peter Dencker, Herbert Klenk, Hubert Keller, Erhard Plödereder (Hrsg.)
Automotive – Safety & Security 2017
30.–31. Mai 2017, Stuttgart

P-270 Arslan Brömme, Christoph Busch, Antitza Dantcheva, Christian Rathgeb, Andreas Uhl (Eds.)
BIOSIG 2017
20.–22. September 2017, Darmstadt

P-271 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
10. DFN-Forum Kommunikations-technologien
30. – 31. Mai 2017, Berlin

P-272 Alexander Rossmann, Alfred Zimmermann (eds.)
Digital Enterprise Computing (DEC 2017)
11.–12. Juli 2017, Böblingen

P-273 Christoph Igel, Carsten Ullrich, Martin Wessner (Hrsg.)
BILDUNGSRÄUME
DeLFI 2017
Die 15. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. (GI)
5. bis 8. September 2017, Chemnitz

P-274 Ira Diethelm (Hrsg.)
Informatische Bildung zum Verstehen und Gestalten der digitalen Welt
13.–15. September 2017, Oldenburg

P-275 Maximilian Eibl, Martin Gaedke (Hrsg.)
INFORMATIK 2017
25.–29. September 2017, Chemnitz

P276 Alexander Volland, Martin Engstler, Masud Fazal-Baqaie, Eckhart Hanser, Oliver Linssen, Martin Mikusz (Hrsg.)
Projektmanagement und Vorgehensmodelle 2017
Die Spannung zwischen dem Prozess und den Menschen im Projekt
Gemeinsame Tagung der Fachgruppen Projektmanagement und Vorgehensmodelle im Fachgebiet Wirtschaftsinformatik der Gesellschaft für Informatik e.V. in Kooperation mit der Fachgruppe IT-Projektmanagement der GPM e.V., Darmstadt 2017

P-277 Lothar Fritsch, Heiko Roßnagel, Detlef Hühnlein (Hrsg.)
Open Identity Summit 2017
5.–6. October 2017, Karlstad, Sweden

P-278 Arno Ruckelshausen, Andreas Meyer-Aurich, Karsten Borchard, Constanze Hofacker, Jens-Peter Loy, Rolf Schwerdtfeger, Hans-Hennig Sundermeier, Helga Floto, Brigitte Theuvsen (Hrsg.)
Informatik in der Land-, Forst- und Ernährungswirtschaft
Referate der 38. GIL-Jahrestagung
26.–27. Februar 2018, Kiel

P-279 Matthias Tichy, Eric Bodden, Marco Kuhrmann, Stefan Wagner, Jan-Philipp Steghöfer (Hrsg.)
Software Engineering und Software Management 2018
5.–9. März 2018, Ulm

P-280 Ina Schaefer, Dimitris Karagiannis, Andreas Vogelsang, Daniel Méndez, Christoph Seidl (Hrsg.)
Modellierung 2018
21.–23. Februar 2018, Braunschweig

P-281 Hanno Langweg, Michael Meier, Bernhard C. Witt, Delphine Reinhardt (Hrsg.)
Sicherheit 2018
Sicherheit, Schutz und Zuverlässigkeit
25.–27. April 2018, Konstanz

P-282 Arslan Brömme, Christoph Busch, Antitza Dantcheva, Christian Rathgeb, Andreas Uhl (Eds.)
BIOSIG 2018
Proceedings of the 17th International Conference of the Biometrics Special Interest Group
26.–28. September 2018
Darmstadt, Germany

P-283 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
11. DFN-Forum Kommunikations-technologien
27.–28. Juni 2018, Günzburg

P-284 Detlef Krömker, Ulrik Schroeder (Hrsg.)
DeLFI 2018 – Die 16. E-Learning Fachtagung Informatik
10.–12. September 2018, Frankfurt a. M.

P-285 Christian Czarnecki, Carsten Brockmann, Eldar Sultanow, Agnes Koschmider, Annika Selzer (Hrsg.)
Workshops der INFORMATIK 2018 - Architekturen, Prozesse, Sicherheit und Nachhaltigkeit
26.–27. September 2018, Berlin

P-286 Martin Mikusz, Alexander Volland, Martin Engstler, Masud Fazal-Baqaie, Eckhart Hanser, Oliver Linssen (Hrsg.)
Projektmanagement und Vorgehensmodelle 2018
Der Einfluss der Digitalisierung auf Projektmanagementmethoden und Entwicklungsprozesse
Düsseldorf 2018

P-287 A. Meyer-Aurich, M. Gandorfer, N. Barta, A. Gronauer, J. Kantelhardt, H. Floto (Hrsg.)
Informatik in der Land-, Forst- und Ernährungswirtschaft
Fokus: Digitalisierung für landwirtschaftliche Betriebe in kleinstrukturierten Regionen – ein Widerspruch in sich?
Referate der 39. GIL-Jahrestagung
18.–19. Februar 2019, Wien

P-288 Arno Pasternak (Hrsg.)
Informatik für alle
18. GI-Fachtagung
Informatik und Schule
16.-18. September 2019 in Dortmund

P-289 Torsten Grust, Felix Naumann, Alexander Böhm, Wolfgang Lehner, Jens Teubner, Meike Klettke, Theo Härder, Erhard Rahm, Andreas Heuer, Holger Meyer (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW 2019)
4.–8. März 2019 in Rostock

P-290 Holger Meyer, Norbert Ritter, Andreas Thor, Daniela Nicklas, Andreas Heuer, Meike Klettke (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW 2019)
Workshopband
4.–8. März 2019 in Rostock

P-291 Michael Räckers, Sebastian Halsbenning, Detlef Rätz, David Richter, Erich Schweighofer (Hrsg.)
Digitalisierung von Staat und Verwaltung
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2019
6.–7. März 2019 in Münster

P-292 Steffen Becker, Ivan Bogicevic,Georg Herzwurm, Stefan Wagner (Hrsg.)
Software Engineering and Software Management 2019
18.–22. Februar 2019 in Stuttgart

P-293 Heiko Roßnagel, Sven Wagner, Detlef Hühnlein (Hrsg.)
Open Identity Summit 2019
28.–29. März 2019
Garmisch-Partenkirchen

P-294 Klaus David, Kurt Geihs, Martin Lange, Gerd Stumme (Hrsg.)
INFORMATIK 2019
50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft
23.–26. September 2019 in Kassel

P-295 Claude Draude, Martin Lange, Bernhard Sick (Hrsg.)
INFORMATIK 2019
50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft
Workshop-Beiträge
23.–26. September 2019 in Kassel

P-296 Arslan Brömme, Christoph Busch, Antitza Dantcheva, Christian Rathgeb, Andreas Uhl (Eds.)
BIOSIG 2019
Proceedings of the 18th International Conference of the Biometrics Special Interest Group
18.–20. September 2019
Darmstadt, Germany

P-297 Niels Pinkwart, Johannes Konert (Hrsg.)
DELFI 2019 –Die 17. Fachtagung Bildungstechnologien
16.–19. September 2019 in Berlin

P-298 Oliver Linssen, Martin Mikusz, Alexander Volland, Enes Yigitbas, Martin Engstler, Masud Fazal-Baqaie, Marco Kuhrmann (Hrsg.)
Projektmanagement und Vorgehensmodelle 2019 –Neue Vorgehensmodelle in Projekten – Führung, Kulturen und Infrastrukturen im Wandel
1Gemeinsame Tagung der Fachgruppen Projektmanagement (WI-PM), Vorgehensmodelle (WI-VM) und Software Produktmanagement (WI-ProdM) im Fachgebiet Wirtschaftsinformatik der Gesellschaft für Informatik e.V.
in Kooperation mit der Fachgruppe IT-Projektmanagement der GPM e.V.,
Lörrach 2019

P-299 M. Gandorfer, A. Meyer-Aurich, H. Bernhardt, F. X. Maidl, G. Fröhlich, H. Floto (Hrsg.)
Informatik in der Land-, Forst- und Ernährungswirtschaft
Fokus: Digitalisierung für Mensch, Umwelt und Tier
Referate der 40. GIL-Jahrestagung
17.–18. Februar 2020,
Campus Weihenstephan

P-300 Michael Felderer, Wilhelm Hasselbring, Rick Rabiser, Reiner Jung (Hrsg.)
Software Engineering 2020
24.–28. Februar 2020
Innsbruck, Austria

P-301 Delphine Reinhardt, Hanno Langweg, Bernhard C. Witt, Mathias Fischer (Hrsg.)
Sicherheit 2020
Sicherheit, Schutz und Zuverlässigkeit
17.–20. März 2020, Göttingen

P-302 Dominik Bork, Dimitris Karagiannis, Heinrich C. Mayr (Hrsg.)
Modellierung 2020
19.–21. Februar 2020, Wien

P-304 Heinrich C. Mayr, Stefanie Rinderle-Ma, Stefan Strecker (Hrsg.)
40 Years EMISA
Digital Ecosystems of the Future: Methodology, Techniques and Applications
May 15.–17. 2019
Tutzing am Starnberger See

P-305 Heiko Roßnagel, Christian H. Schunck, Sebastian Mödersheim, Detlef Hühnlein (Hrsg.)
Open Identity Summit 2020
26.–27. May 2020, Copenhagen

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de