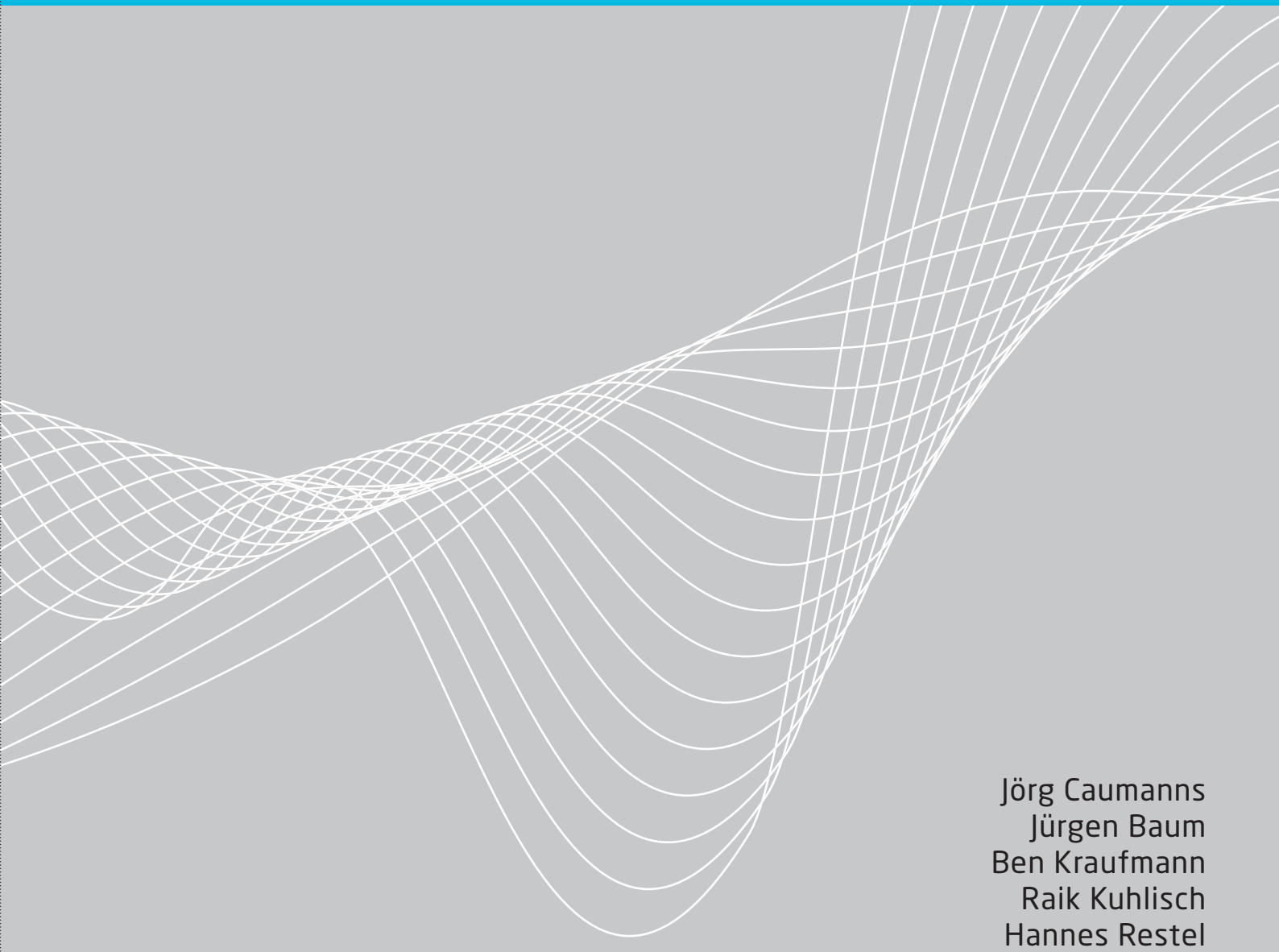
P2 3R
NON-STOP-GOVERNMENT

IT-INVESTITIONS-
PROGRAMM
Wir gestalten Zukunft.

P23R: Sicherheitsarchitektur

Ein Ergebnisdokument des Projekts P23R | Prozess-Daten-Beschleuniger
im Auftrag des Bundesministeriums des Innern



Jörg Caumanns
Jürgen Baum
Ben Kraufmann
Raik Kuhlisch
Hannes Restel

Das P23R-Projekt wurde im Rahmen des IT-Investitionsprogramms der Bundesregierung durchgeführt (Fördernummer D4-06-1).

Generalunternehmer

Fraunhofer

Projektbeteiligte

Atos

Eberhard Karls Universität Tübingen

ESG Consulting

Fraunhofer FOKUS

Fraunhofer IAO

Fraunhofer IESE

Fraunhofer ISST

Fraunhofer SIT

Metropolregion Rhein-Neckar

provet Projektgruppe verfassungsverträgliche Technikgestaltung

tsm total-sourcing-management

GAD IT für Banken

Projekt
P23R | Prozess-Daten-Beschleuniger

P23R: Sicherheitsarchitektur

Ergebnisdokument

Dezember 2012

Autoren
Dr. Jörg Caumanns, Fraunhofer ISST
Jürgen Baum, Fraunhofer SIT
Ben Kraufmann, Fraunhofer ISST
Raik Kuhlisch, Fraunhofer ISST
Hannes Restel, Fraunhofer ISST

Zusammenfassung

Die Kernfunktionalität eines Prozess-Daten-Beschleunigers (P23R) ist die Generierung von Benachrichtigungen. Hierbei werden Unternehmensdaten anhand von zentral bereitgestellten Benachrichtigungsregeln ausgewertet, verdichtet, in eine strukturierte Form gebracht und an eine Verwaltung übermittelt. Die Hoheit über die verarbeiteten und erzeugten Daten sowie über den Kontrollfluss innerhalb des P23R liegt beim Unternehmen. Hierdurch ergibt sich insbesondere für Unternehmen mit einem hohen IT-Durchdringungsgrad die Anforderung nach einer möglichst nahtlosen Integrierbarkeit eines P23R in unternehmensinterne, IT-gestützte Abläufe. Für kleine Unternehmen und Unternehmen mit geringer IT-Durchdringung stellt der von einem P23R umgesetzte Schritt einer weitergehenden Prozesskette eine IT-technisch isolierte Aktion dar, die idealerweise über eine weitgehend in sich abgeschlossene IT-Anwendung abgedeckt werden sollte.

Diese Spannbreite von zu unterstützenden Umsetzungsoptionen erfordert eine hochgradig modulare Architektur, bei der je nach Einsatzumgebung eines P23R einzelne Funktionalitäten entweder im Unternehmen oder in der geschlossenen Umgebung eines P23R angesiedelt sind. Darüber hinaus müssen externe Kommunikationsbeziehungen auf standardisierte Protokolle des eGovernment – insbesondere OSCI Transport 2.0 – abgebildet werden können. Diese Anforderungen gelten nicht nur für die Fachdienste des P23R, sondern gleichermaßen für die Sicherheitsarchitektur des P23R mit ihren Sicherheitsdiensten. Aus diesem Grund wird für den P23R eine Sicherheitsarchitektur spezifiziert, die eine – teilweise sogar dynamische – Verlagerung von Sicherheitsdiensten und Sicherheitsobjekten zwischen der IT-Infrastruktur eines Unternehmens und einem P23R erlaubt:

- Authentifizierungen von P23R-Nutzern können sowohl im Unternehmen als auch am P23R vorgenommen werden. Über OSCI 2.0 vermittelte Authentifizierungsnachweise können im P23R verarbeitet werden.
- Berechtigungsregeln können aus dem Berechtigungsmanagement eines Unternehmens übernommen oder als Konfiguration eines P23R gepflegt werden.
- Für die Auswertung von Berechtigungsregeln erforderliche Attribute (z. B. Rollen- und Gruppenzuordung von Nutzern) können „on demand“ aus Verzeichnisdiensten oder anderen Systemen des Unternehmens abgefragt werden.

Technisch wird diese Flexibilität durch die Nutzung der Standards SAML, XACML und WS-Trust unterstützt, die eine Kapselung von Sicherheitsfunktionalitäten in modularen, weitgehend voneinander entkoppelten Komponenten unterstützen. Dies erlaubt es z. B. auch, Sicherheitsmaßnahmen nicht nur am Perimeter des P23R anzulegen, sondern auch einzelne Funktionalitäten und Ressourcen innerhalb des P23R gezielt und gegen spezifische Bedrohungen zu sichern. Bestehende Arbeitsorganisationen und Verantwortlichkeiten in einem Unternehmen können so auf einen P23R abgebildet werden.

Weitere Anforderungen an die Sicherheitsarchitektur des P23R ergeben sich aus der per se vernetzten Charakteristik eines P23R als Bestandteil einer verwaltungs- und unternehmens-übergreifenden Prozesskette. Hierdurch müssen nicht nur unterschiedliche Kommunikations-beziehungen in Bezug auf die Integrität und Vertraulichkeit der ausgetauschten Daten geschützt werden, sondern es müssen insbesondere auch unbekannte, erst über eine Benachrichtigungregel

identifizierte Dienstschnittstellen sicher lokalisiert und authentifiziert werden können. Um die erforderliche Flexibilität und Dynamik zu erzielen, ohne dabei aufwändige, neue administrative Prozesse in Unternehmen und Verwaltungen zu fordern, publizieren alle Akteure im Umfeld eines P23R ihre Dienstadressen und Zertifikate über eine Trusted Service List (TSL). Derartige Listen können sowohl aus bestehenden Verzeichnissen und Systemkonfigurationen exportiert als auch recht einfach manuell gepflegt werden. Sie sind damit eine leichtgewichtige und dennoch für die meisten Szenarien ausreichende und insbesondere auch in dezentraler Verwaltung der einzelnen Akteure umsetzbare Alternative zur Online-Abfrage von Kommunikationsparametern und Zertifikaten aus zentralen Verzeichnisdiensten.

Executive Summary

The core functionality of a „Prozess-Daten-Beschleuniger (P23R)“ is the generation of notifications. In this connection, data from business establishments is evaluated based on the centrally provided notification rules, concentrated in a structured format and transmitted to an administration. The sovereignty over the processing and generated data as well as flow of control within the P23R lies with the business establishment. This results, in particular for business establishments with high IT penetration the requirement for seamless ease of integration of a P23R in corporate, IT-supported processes. For small business establishments and business establishments with a low IT penetration, the step implemented by a P23R represents a further process chain in an IT isolated environment, that ideally should be covered by a completed IT application.

This breath supporting implementation options requires a high level modular architecture, where depending on the field of implementation of a P23R individual functionalities are either residing in the business establishment or in the closed environment of a P23R. Furthermore external communication relationships must be mapped to standardised protocols of the eGovernment – in particular OSCI Transport 2.0. These requirements apply not only for the business services of the P23R, but equally for the security infrastructure of the P23R with their security services. For this reason, a security architecture for a P23R will be specified, that permits a partial dynamic relocation of security services and security objects between the IT infrastructure of a business establishment and a P23R:

- Authentication of P23R users can be undertaken both in the business establishment as well as at the P23R. Via OSCI 2.0 communicated authentication assertions can be processed in the P23R.
- Acces rules can be assumed from the access management of a business establishment, or be maintained as a configuration of a P23R.
- For the evaluation of attributes required for access rules (e. g. roles and group assignment of users) can be requested from directory services or other systems of the business establishment „on demand“.

This flexibility is technically supported by use of the standards SAML, XACML and WS-Trust, that support the encapsulation of security functionalities in modular components largely decoupled from each other. This permits for example to reside security measures not only at the perimeter of the P23R but also protect from specific threats individual functionalities and resources within the P23R. Existing working groups and responsibilities within a business establishment can be mapped onto a P23R.

Further requirements on the security infrastructure of the P23R ensue from the per se connected characteristic of a P23R as a component of a comprehensive process chain of administration and business establishments. Hereby, not only various communication relationships must be protected in relation to integrity and confidentiality of exchanged data but also in-particular unknown via the notification rule defined service interfaces must first be identified.

In order to attain the required flexibility and dynamism without calling for complex and new administrative processes in business establishments and administration, all actors in the environment of a P23R, make public their official addresses and certificates via a Trusted Service List (TSL). Such lists can be rather easily exported as well as manually maintained from existing directories and system configurations. They thereby are a lightweight however for most scenarios sufficient, realisable alternative to on-line query of communication parameters and certificates from central directory services, and in particular decentralised administration of individual actors.

Inhaltsverzeichnis

Verzeichnis der Abbildungen

Verzeichnis der Tabellen

1 EINLEITUNG

Eine Prozesskette ist eine durch mehrere, kooperierende Stakeholder abgearbeitete Sequenz von Teilprozessen. Während aus fachlicher Sicht immer der gesamte Prozess betrachtet wird, ist auf der technischen Ebene die Integration der in der Hoheit und technisch-organisatorischen Umgebung der einzelnen Stakeholder laufenden Teilprozesse die wesentliche Herausforderung. Neben der Herstellung von interoperablen Übergabeschnittstellen zwischen den Anwendungsdiensten der Teilprozesse müssen insbesondere auch Schutzziele, wie z. B. Vertraulichkeit und Integrität, durchgängig gewährleistet sein.

Der im Rahmen des Projekts zu entwickelnde Prozess-Daten-Beschleuniger (P23R) realisiert innerhalb einer solchen Prozesskette einen Teilprozess, der für die Nachrichtenübermittlung zwischen den Stakeholdern Unternehmen und Verwaltung zuständig ist. Typische Einsatzszenarien eines solchen P23R sind neben den im Projekt prototypisch zu realisierenden gesetzlich vorgeschriebenen Meldungen (Benachrichtigungen) auch Antragstellungen und Registerauskünfte, die jeweils von Unternehmen an Verwaltungen versendet werden. Eine Übersicht zu Aufbau und Einsatzszenarien eines Prozess-Daten-Beschleunigers bietet das Kapitel „Die P23R-Infrastruktur“ in dem Dokument zur P23R-Rahmenarchitektur .

1.1 ZWECK DES DOKUMENTS

In diesem Dokument wird die Sicherheitsarchitektur des P23R mit ihren Sicherheitsdiensten als Ergänzung zur P23R-Rahmenarchitektur [1] spezifiziert.

Eine Sicherheitsarchitektur stellt im Kern einen Bausatz von zu Sicherheitszielen korrespondierenden Sicherheitsdiensten bereit, um standardisierte Sicherheitsmechanismen, wie z. B. digitale Signaturen und Verschlüsselung, auf Daten und Dienste anzuwenden (siehe Abbildung 1, in Anlehnung an [2]). Dieses setzt neben einer Analyse der Schutzbedarfe voraus, dass zunächst auf einer konzeptionellen Ebene festgelegt wird, wo technische Maßnahmen erforderlich sind und wie diese durch organisatorische Maßnahmen flankiert werden müssen. Die in die Kontrollflüsse des P23R integrierten technischen Sicherheitsdienste und deren zugrunde liegenden Mechanismen und Objekte werden in der P23R-Sicherheitsarchitektur spezifiziert. Vorgaben und Empfehlungen zu technischen und organisatorischen Maßnahmen zur Aufrechterhaltung des angestrebten Sicherheitsniveaus im Betrieb des P23R sind hingegen Gegenstand des Sicherheitskonzepts [3].

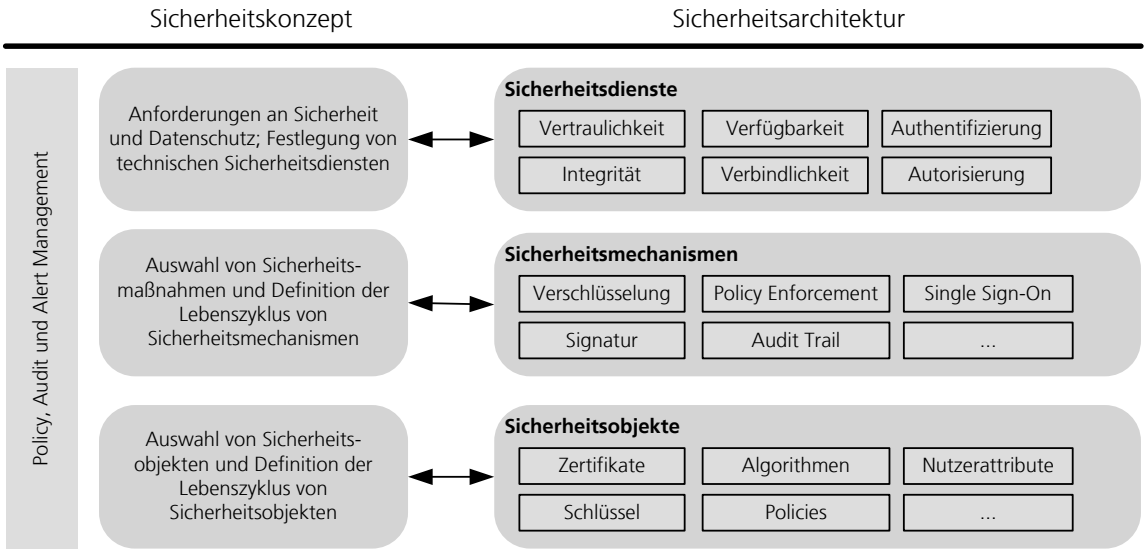


ABBILDUNG 1: SICHERHEITSKONZEPT UND SICHERHEITSARCHITEKTUR

Die Auswahl von Schutzmaßnahmen erfolgt anhand der ermittelten Schutzbedarfe und Bedrohungen. In vielen Fällen kann hierbei auf die bewährten organisatorischen und technischen Maßnahmen der IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) [4] zurückgegriffen werden. Für hohe und sehr hohe Schutzbedarfe, spezialisierte Hard- und Software sowie besondere Einsatzumgebungen verlangt die Grundschutzmethodik des BSI die Auswahl höherwertiger Schutzmaßnahmen, deren Notwendigkeit ggf. in dedizierten Risikoanalysen zu begründen ist. Diese Maßnahmen prägen sehr häufig das Design der Sicherheitsarchitektur und haben oftmals auch Auswirkungen auf das Design und die Verteilung von Diensten der Anwendungsebene (siehe Abschnitt 2.1).

Die in diesem Dokument spezifizierten Sicherheitsdienste zur Herstellung der Vertraulichkeit und Integrität ausgetauschter Daten, zur Authentifizierung und Autorisierung von Nutzern und zur Umsetzung verbindlicher, nachvollziehbarer Abläufe sind verpflichtend für jeden P23R umzusetzen.

In diesem Dokument werden keine NORMATIVEN technischen Maßnahmen zur Umsetzung der von einem P23R-Nutzer ggf. geforderten Verfügbarkeitsanforderungen definiert; dieses liegt in der Verantwortung des P23R-Herstellers und des P23R-Providers und kann z. B. über Service Level Agreements eines P23R-Providers gegenüber seinen Kunden abgesichert werden.

1.2 LESERKREIS

Das Dokument richtet sich an Hersteller von P23R und P23R-Provider.

1.3 KONTEXT, INHALTE UND STRUKTURIERUNG

In diesem Dokument werden das Design der P23R-Sicherheitsarchitektur und der Sicherheitsdienste, die sie aufspannen, beschrieben. Zudem werden die zur Umsetzung der Sicherheitsdienste erforderlichen Komponenten funktional spezifiziert. Die technische Spezifikation der Sicherheitsdienste sowie Sicherheitsmechanismen und -objekte über eine Profilierung existierender Standards ist Gegenstand eines separaten Dokuments [5].

In Kapitel 2 des vorliegenden Dokuments werden die primären Herausforderungen des P23R in Bezug auf Sicherheit und Datenschutz beschrieben, mithin solche Fragestellungen behandelt, die sich nicht mit organisatorischen Vorgaben oder einfachen technischen Maßnahmen (z. B. Transportverschlüsselung) adressieren lassen und deren Lösung potenziell auf das Design der gesamten Architektur des P23R und die darauf aufsetzenden Abläufe ausstrahlt. Aus diesen Fragestellungen werden sogenannte „Essentials" des Sicherheitskonzepts und der Sicherheitsarchitektur abgeleitet, die quasi als „Leitplanken" der technischen Spezifikationen von Anwendungs- und Sicherheitsdiensten dienen und deren Einbettung in ein übergreifendes Sicherheitsmanagement beschreiben.

Ausgehend von einer Überblicksdarstellung der P23R-Sicherheitsarchitektur in Kapitel 3 werden die einzelnen Subsysteme (Authentifizierung, Autorisierung und Berechtigungsprüfung, Sicherung von Daten und Nachrichten, Austausch von Adressen und Zertifikaten) in den nachfolgenden Abschnitten 4-7 funktional spezifiziert.

In Kapitel 8 werden die zum Aufbau der P23R-Sicherheitsarchitektur verwendeten Standards beschrieben. Es folgen Glossar, Abkürzungsverzeichnis und Referenzen.

1.4 KONVENTIONEN

Die Verwendung der Schlüsselwörter MUST (MUSS), SHOULD (SOLL / SOLLTE), MAY (KANN / DARF) und MUST NOT (DARF NCHT) entspricht den in RFC 2119 [6] spezifizierten Konventionen.

Über XML-Schemata spezifizierte Typen sowie einzelne Elemente und Attribute dieser Typen werden im Text in *kursiver* Schrift gekennzeichnet.

Alle in diesem Dokument spezifizierten Schnittstellen basieren auf internationalen Standards bzw. lehnen sich an diese an. Für die P23R-Sicherheitsarchitektur erforderliche zusätzliche Schnittstellen und Elemente werden mit englischen Namen belegt, um eine Einheitlichkeit zu wahren.

Generell wird im Kontext des P23R zwischen Benachrichtigungssender und Benachrichtigungsempfänger unterschieden. Üblicherweise werden Benachrichtigungen von Unternehmen an Verwaltungen gesendet. Da in diesem Dokument hauptsächlich die Sicherheit sowie Hoheit des Unternehmens betrachtet werden sollen, werden im weiteren Verlauf abweichend von der Verwendung der Begriffe in den sonstigen Dokumenten zur P23R-Rahmenarchitektur konkret die Begriffe „Unternehmen" und „Verwaltung" benutzt.

2 GRUNDZÜGE DER SICHERHEITSARCHITEKTUR

Die Sicherheitsarchitektur des P23R muss die Durchsetzung der elementaren Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sicherstellen. Darüber hinaus müssen Zugriffe auf Daten und nach außen gerichtete Kommunikationsvorgänge verbindlich, nachvollziehbar und nicht abstreitbar sein (für eine Herleitung der Schutzziele siehe [3]).

2.1 HERAUSFORDERUNGEN

In diesem Abschnitt werden die zentralen Herausforderungen beim Design einer Sicherheitsarchitektur für den P23R beschrieben. Diese Herausforderungen sind diejenigen, die potenziell nicht durch technische Maßnahmen „von der Stange“ gelöst werden können, sondern deren Lösung auf die gesamte Architektur des P23R und auch das Design einzelner Systemkomponenten ausstrahlt. Während z. B. die Herausforderung einer Integritätssicherung vergleichsweise einfach durch Signaturen adressiert werden kann, müssen zur Wahrung der Unternehmenshoheit eines P23R-Nutzers, zum Schutz von zur Benachrichtigungserzeugung genutzten Unternehmensdaten und zur Herstellung eines durchgängigen Schutzniveaus im Systemdesign verankerte Basiskonzepte gefunden werden, um die herum dann die restliche Architektur entwickelt wird. Dieser auch als „privacy by design“ bzw. „security by design“ bezeichnete Ansatz stellt sicher, dass insbesondere an den sicherheitskritischen Stellen einer Lösung Anwendungsarchitektur, Sicherheitskonzept und Sicherheitsarchitektur optimal aufeinander abgestimmt sind [7].

2.1.1 WAHRUNG DER UNTERNEHMENSHOHEIT

Der P23R läuft in der Hoheit und in der organisatorisch-technischen Infrastruktur eines Unternehmens. Dies bedeutet, dass Redundanzen mit bereits bestehenden Systemen gering zu halten sind und dass keine Vorgaben gemacht werden können, die die Organisationshoheit des Unternehmens beschneiden.

CH.P23R.Sec.01:[1] Identifizierung und Authentifizierung

In den meisten Unternehmen existieren Verfahren und technische Systeme zur Pflege des Lebenszyklus der digitalen Identitäten der Mitarbeiter sowie zur Authentifizierung von Mitarbeitern gegenüber IT-Systemen. Das Unternehmen ist frei in der Wahl des Authentifizierungsmechanismus, solange dieser in Bezug auf den Schutzbedarf der für den authentifizierten Mitarbeiter zugänglichen Ressourcen angemessen ist. Die P23R-Sicherheitsarchitektur MUSS diese Vorgaben akzeptieren und SOLL NICHT Ersatzsysteme und -verfahren für bestehende Systeme und Verfahren einführen. Die Verwaltung von Nutzern MUSS in der Hoheit des Unternehmens verbleiben und MUSS über die bestehenden Systeme und Verfahren des Unternehmens erfolgen.

[1] Die Notation CH.P23R.Sec steht für engl. Challenge (Herausforderung) P23R Security und wird fortlaufend nummeriert. Diese Codes werden sowohl in diesem Dokument als auch im Dokument zum übergreifenden Sicherheitskonzept des P23R verwendet, um sowohl Sicherheitsanforderungen als auch -maßnahmen auf zugrunde liegende konzeptionelle Fragestellungen beziehen zu können.

CH.P23R.Sec.02: Rollen und Rechte

Welche Personen welche Benachrichtigungen erstellen und / oder freigeben dürfen, obliegt der Festlegung des Unternehmens. Ob Berechtigungen an Personen oder Rollen geknüpft sind, ist ebenfalls eine aus der Organisationsstruktur abgeleitete Festlegung des Unternehmens. Die P23R-Sicherheitsarchitektur DARF hier NICHT von einem bestimmten Modell einer Autorisierung ausgehen, sondern MUSS die vom Unternehmen getroffenen Festlegungen umsetzen.

CH.P23R.Sec.03: Freigabe-Policy

Die Freigabe einer Benachrichtigung an eine Verwaltung ist ein formaler Akt, der ggf. rechtliche Konsequenzen nach sich ziehen kann. Zur Absicherung der handelnden Personen und des Unternehmens als Organisation wird jedes Unternehmen hierzu bereits Verfahrensweisen festgelegt haben (z. B. in einer Unterschriftenordnung). Typische Beispiele sind das Vier-Augen-Prinzip (eine Meldung muss von mindestens zwei Personen freigegeben werden) und geteilte Verantwortlichkeiten (jemand, der eine Meldung erstellt hat, darf diese nicht anschließend freigeben). Es ist darüber hinaus zu gewährleisten, dass auch per Fax oder Post übermittelte Benachrichtigungen auf Papier mit konventionellen Unterschriften freigegeben werden können. Die P23R-Sicherheitsarchitektur MUSS die im Unternehmen geltenden Regeln akzeptieren und DARF NICHT verlangen, dass ein unternehmensübergreifend einheitlicher Mechanismus vorausgesetzt wird.

2.1.2 Schutz der Unternehmensdaten

Im Datenpool[2] und im Benachrichtigungspool werden Informationen gebündelt, aus denen potenziell schützenswerte Informationen zum Unternehmen oder seinen Mitarbeitern ableitbar sind. Sofern der Nutzungszweck der Daten nicht vorab und vollständig erfasst werden kann, ist per se zunächst, quasi bis zum Nachweis des Gegenteils, ein hoher Schutzbedarf in Bezug auf die Vertraulichkeit der Daten anzunehmen. Dieses gilt insbesondere auch für Fälle, in denen im Datenpool des P23R Daten zusammengeführt werden, die ansonsten im Unternehmen unter der Hoheit getrennter Untereinheiten stehen – ggf. erfordern diese Fälle sogar einen sehr hohen Schutzbedarf, was in einer den Einzelfall betrachtenden Sicherheitsanalyse zu prüfen ist.

[2] Ob das Anlegen von Datenkopien im Datenpool des P23R die zu bevorzugende Umsetzungsoption eines P23R ist, kann nur im Einzelfall unter Betrachtung der Einsatzumgebung des P23R bewertet werden. Aus Datenschutzsicht werden redundante Daten angelegt, d. h. das Gebot der Datensparsamkeit wird verletzt. Aus Sicherheitssicht wird so jedoch ein Zugriff auf die Produktivsysteme des Unternehmens ausgeschlossen, wodurch diese vor Angriffen aus dem P23R heraus geschützt werden. In diesem Dokument wird angenommen, dass in den meisten Fällen der Schutz der Unternehmensdaten eine höhere Priorität besitzt als die vollständige Vermeidung von redundanten Daten (die zusätzlich auch noch gut gekapselt werden können). Daher wird davon ausgegangen, dass Kopien von Unternehmensdaten im Datenpool des P23R verwaltet werden. Dieses schließt jedoch andere Umsetzungsoptionen nicht grundsätzlich aus.

CH.P23R.Sec.04: Vertraulichkeit des Datenpools

„Daten im Datenpool müssen [zur Laufzeit des P23R, d. Verf.] ausgewählt, transformiert und ggf. aggregiert werden, um Benachrichtigungen zu generieren. Dieses Erfordernis einer Verarbeitung im P23R macht eine durchgängige Verschlüsselung unmöglich." [8] Das P23R-Sicherheitskonzept MUSS Lösungen zur Sicherung der Vertraulichkeit der Daten im Datenpool aufzeigen und entsprechende Anforderungen an die Umsetzung des Datenpools und der darauf arbeitenden Systemkomponenten formulieren. *„Die P23R-Sicherheitsarchitektur MUSS ggf. aus diesen Anforderungen abgeleitete Einschränkungen berücksichtigen und sicherstellen, dass Angriffe auf den Datenpool auch ohne eine durchgängige Verschlüsselung der Daten soweit als möglich ausgeschlossen werden."* [8]

CH.P23R.Sec.05: Nicht-Verknüpfbarkeit

„Im Datenpool und im Benachrichtigungspool werden potenziell Daten aus unterschiedlichen Unternehmensteilen zusammengeführt. Hierdurch können Möglichkeiten der Verknüpfung und Auswertung von Daten (z. B. von Mitarbeiterdaten) entstehen, die dem ursprünglichen Zweck der Erhebung dieser Daten widersprechen oder die sogar gesetzlich nicht zulässig sind, da sie z. B. Profilbildungen erlauben." [8]

Das P23R-Sicherheitskonzept MUSS Maßnahmen beschreiben, die eine solche unzulässige Zweitnutzung von Daten ausschließen. Die P23R-Rahmenarchitektur MUSS diese Maßnahmen technisch unterlegen.

CH.P23R.Sec.06: Vertraulichkeit des Benachrichtigungspools

„Im Benachrichtigungspool werden erstellte Meldungen bis zur Freigabe zwischengespeichert. Da die Freigabe eine Sichtprüfung erfordert und auch Änderungen der Benachrichtigungen zu diesem Zeitpunkt noch möglich sein sollen, ist hier eine durchgängige Verschlüsselung nicht möglich." [8]

Analog zu CH.P23R.Sec.04 MÜSSEN entsprechend im Sicherheitskonzept und in der Sicherheitsarchitektur geeignete Schutzmaßnahmen definiert werden.

CH.P23R.Sec.07: Signaturerzeugung

„Im Idealfall kann der P23R als ein abgeschlossener Sicherheitskontext angesehen werden, der Datenschnittstellen nach außen nur an den Verbindungspunkten zu vor- und nachgelagerten Teilprozessen besitzt. Dieser Sicherheitskontext muss jedoch [Wie bereits in CH.P23R.Sec.03 beschrieben, d. Verf.] im Rahmen der Benachrichtigungsfreigabe durchbrochen werden. Ein zweites Szenario, bei dem der Datenfluss einer Benachrichtigungsgenerierung den Sicherheitskontext des P23R verlässt, ist die Aufbringung von qualifizierten Signaturen: Die qualifiziert zu signierenden Daten verlassen den P23R und durchlaufen eine außerhalb der Kontrolle des P23R liegende Signaturanwendung." [8]

Im Sicherheitskonzept [3] und der Sicherheitsarchitektur des P23R MÜSSEN Maßnahmen zur Absicherung der freizugebenden Benachrichtigungen definiert werden, die auch außerhalb des Sicherheitskontexts des P23R durchsetzbar sind.

2.1.3 DURCHGÄNGIGKEIT

Der P23R bildet nur einen Teilprozess einer Prozesskette ab. Sowohl für die Erbringung der geforderten Funktionalität als auch für die Sicherheit der Prozesskette gilt jedoch, dass diese so stark ist wie ihr schwächstes Glied.

CH.P23R.Sec.08: Needs-to-Know-Prinzip

„Die Erstellung einer Benachrichtigung erfordert den Zugang zu Ressourcen innerhalb und ggf. auch außerhalb des P23R. Sofern ein beim Benachrichtigungssender (z. B. im Unternehmen) zur Generierung einer Benachrichtigung grundsätzlich autorisierter Mitarbeiter nicht ausreichende Zugriffsrechte auf alle benötigten Ressourcen besitzt, kann die Benachrichtigung nicht erstellt werden." [8] Dieses Erfordernis der Synchronität von Rechten auf Prozessen und Ressourcen ist umso schwieriger herzustellen, wenn unterschiedliche Schutzbedarfe für Quelldaten und daraus über den P23R abgeleitete verdichtete Daten bestehen[3], oder wenn Prozessketten zwischen Unternehmen aufgebaut werden sollen.

Die P23R-Sicherheitsarchitektur MUSS Mechanismen anbieten, die eine durchgängige und ggf. auch organisationsübergreifende Durchsetzung von Prozessrechten gegenüber Berechtigungen auf Ressourcen erlauben.

CH.P23R.Sec.09: Semantische Integrität von Benachrichtigungen

Konzeptuell wird eine durchgängige Integrität angestrebt, d. h. eine integre, von einer Verwaltung freigegebene Benachrichtigungsregel (BR) führt zu integren Benachrichtigungen. Änderungen an Regeln oder Benachrichtigungen verletzen diese „semantische" Integrität. Auch wenn ggf. nicht semantisch integre Benachrichtigungen von einer Verwaltung akzeptiert werden sollten, so SOLL doch erkennbar sein, dass die durchgängige semantische Integrität nicht gegeben ist. Solche Anforderungen führen üblicherweise zu der Einführung eines gehärteten, gegen ein Schutzprofil (Protection Profile) zertifizierten Anwendungskerns (letzten Endes muss in einer gegen äußere Manipulation abgesicherten Umgebung die Authentizität und Integrität einer Regel geprüft, die Benachrichtigung generiert und unmittelbar integritätsgesichert werden). Durch die Verankerung der Regelausführung in einer gesicherten Umgebung müssen jedoch auch alle Außenschnittstellen der Regelverarbeitung mit abgesichert werden. Hierdurch wird schließlich die gesamte technische Basis des P23R normiert, d. h. Hersteller können z. B. nicht mehr frei wählen, welche Datenbanktechnologie sie im P23R einsetzen. Im P23R-Sicherheitskonzept MUSS analysiert werden, welche Möglichkeiten bestehen, ausreichende Sicherheit auch ohne einen gehärteten Kern herzustellen (insbesondere MUSS auch geklärt werden, was in diesem Fall eine ausreichende Sicherheit ist). Parallel ist zu analysieren, welche Auswirkungen der Verzicht auf einen gehärteten Kern auf die Nutzungsszenarien des P23R hätte.

[3] Ein Beispiel hierfür ist eine Meldung, in der Gesamtsumme der von einem Unternehmen in einem Jahr für seine Mitarbeiter gezahlten Sozialbeiträge enthalten ist. Um diese Zahl zu berechnen, müssen im P23R die für die einzelnen Mitarbeiter gezahlten Beiträge summiert werden. Das angesprochene Problem tritt auf, wenn der für die Meldung zuständige Mitarbeiter zwar die Gesamtsumme sehen darf, aber keine Berechtigung besitzt, auf die einzelnen Mitarbeiterdatensätze zuzugreifen.

CH.P23R.Sec.10: Ende-zu-Ende-Sicherheitsniveau

„Der P23R kann nur Daten und Nachrichten aus Quellen akzeptieren, die das für den P23R geforderte Schutzniveau ebenfalls umsetzen. Genauso kann der P23R nur Daten und Benachrichtigungen an Zielsysteme weitergeben, wenn er einerseits deren gefordertes Schutzniveau realisiert, andererseits aber durch die Weitergabe das eigene Schutzniveau nicht unterlaufen wird (es ist wenig sinnvoll, wenn innerhalb des P23R eine Benachrichtigung mit starken Mechanismen signiert und verschlüsselt wird, nur um anschließend ausgedruckt und per Fax an die Poststelle einer Verwaltung geschickt zu werden). Die Verantwortlichkeit des P23R für zu schützende Daten endet damit nicht an den Außenschnittstellen des P23R, sondern wirkt auch in die unmittelbar angebundenen Systemkomponenten anderer Organisationen hinein.“ [8]

Die P23R-Sicherheitsarchitektur MUSS Mechanismen bereitstellen, die eine Transparenz hinsichtlich der zum Einsatz kommenden Sicherheitsmechanismen und Sicherheitsobjekte von an den P23R angebundenen Systembausteinen herstellen und einen Abgleich mit den für eine Prozesskette geforderten Schutzniveaus erlauben.

2.2 Essentials des Sicherheitskonzepts und der Sicherheitsarchitektur

In diesem Abschnitt werden die Strategien und Designprinzipien beschrieben, mit denen die im vorangegangenen Abschnitt skizzierten Herausforderungen adressiert werden. Die aus den Prinzipien abgeleiteten Konzepte werden im Sicherheitskonzept [3] konsolidiert und in der Sicherheitsarchitektur auf eine in sich konsistente, ein durchgängiges Sicherheitsniveau sicherstellende Dienstelandschaft abgebildet.

2.2.1 Wahrung der Unternehmenshoheit

Das durchgängig angelegte Designprinzip zur Wahrung der Unternehmenshoheit ist die Auslagerung entsprechender Sicherheitsfunktionen aus dem P23R. Grundidee ist, dass Authentifizierungen, Rollenzuweisungen und Definitionen von Berechtigungsregeln im Unternehmen durch die dort für diesen Zweck bereits bestehenden Systeme erfolgen. Die entsprechenden Sicherheitsobjekte werden außerhalb des P23R erstellt und in geeigneter Weise in den P23R eingespielt.

CM.P23R.Sec.01:[4] Externe Verwaltung und Authentifizierung von Nutzern

Die Identifizierung und Authentifizierung von Nutzern erfolgt grundsätzlich außerhalb des P23R. Diese externen Authentifizierungen müssen durch einen vertrauenswürdigen Security Token Service (STS, deutsch: Sicherheitstokendienst) der den Nutzer authentifizierenden Organisation auf interoperable Identitätsnachweise abgebildet werden. Der P23R enthält einen eigenen STS, der die Vertrauenswürdigkeit externer Sicherheitstoken und vom Nutzer beigefügter Besitznachweise prüfen kann und alle externen Sicherheitstoken in ein einheitliches internes Format überführt. Ein analoges Modell wird auch für die Authentifizierung von Verwaltungen und Verwaltungsmitarbeitern genutzt;

[4] Die Notation CM.P23R.Sec steht für engl. Counter Measure (Gegenmaßnahme) P23R Security und wird fortlaufend nummeriert. Im übergreifenden Sicherheitskonzept des P23R [3] werden die entsprechenden Kürzel aufgegriffen, um Bezüge zwischen konkreten Maßnahmen des IT-Grundschutzes [4] und Designprinzipien des P23R herzustellen.

auch hier werden über einen dedizierten STS in der Verwaltung durchgeführte und z. B. über OSCI Transport 2.0 [9] vermittelte Authentifizierungen und Rollenzuordnungen verifiziert und in das generische, für den P23R verständliche Format überführt.

CM.P23R.Sec.02 Freigaben über externen Workflow

Generierte und in den Benachrichtigungspool eingestellte Benachrichtigungen können von berechtigten Personen ausgelesen, modifiziert und wieder in den Pool zurückgeschrieben werden. Mit dem Zurückschreiben kann die Freigabe zum Versand an den Empfänger erteilt werden.

Mögliche Modifikationen der Benachrichtigung können sein:

- Anlegen einer oder mehrerer elektronischer Signaturen unterschiedlichen Niveaus (einfache, fortgeschrittene sowie qualifizierte Signaturen)
- Manuelle Nachbearbeitung
- Ausdrucken, Unterschreiben, Scannen

Die Aufrechterhaltung des erforderlichen Schutzniveaus für die außerhalb des P23R liegenden Bearbeitungen einer Benachrichtigung ist durch ein spezifisches Sicherheitskonzept des Unternehmens sicherzustellen. Der P23R muss lediglich sicherstellen, dass (händisch oder elektronisch) signierte Benachrichtigungen nicht mehr verändert werden bzw. bei Veränderung vor der Weitergabe neu signiert werden.

CM.P23R.Sec.03: Externe Definition und Bindung von Rechten

Autorisierungen zur Generierung, zum Verarbeiten und zur Freigabe von Benachrichtigungen (Prozessautorisierungen) werden von Autorisierungen zum Zugriff auf den Datenpool (Datenautorisierungen) getrennt. Prozessautorisierungen werden von den Unternehmen formuliert und geben an, welche Mitarbeiter welche Aktionen auf dem P23R durchführen dürfen. Die Bindung einer Prozessautorisierung an eine Person kann sowohl im Unternehmen als auch innerhalb des P23R erfolgen. Die Pflege der Berechtigungen soll im Unternehmen erfolgen; die Vorhaltung der daraus abgeleiteten Zugriffsregeln (Access Policies) soll sowohl im P23R als auch im Unternehmen erfolgen können.

Eine Autorisierung zur Erstellung einer Benachrichtigung erfordert immer auch eine Datenautorisierung. Diese wird nicht an eine Person, sondern an einen Dienst gebunden, der die Daten komplett kapselt (complete mediation, siehe Abschnitt 3.2). Der Dienst stellt sicher, dass Datenzugriffe nicht zu einer Offenbarung geschützter Informationen führen (siehe CM.P23R.Sec.08).

2.2.2 Schutz der Unternehmensdaten

Zum Schutz der Unternehmensdaten wird eine Sicherheitsstrategie verfolgt, die auf der 80-zu-20-Regel basiert (d. h. 80 v. H. der Vorfälle folgen einer kleinen Menge generalisierbarer Abläufe, während 20 v. H. der Vorfälle eine Vielzahl von Ausnahmen abbilden, die sich aus unternehmensspezifischen Besonderheiten ergeben). Die Sicherheitsstrategie des P23R fokussiert technische Maßnahmen auf die Regelfälle, um die Komplexität der Sicherheitsarchitektur so gering wie möglich zu halten und damit Angriffspotenziale zu minimieren sowie die Fehleranfälligkeit der implementierten Sicherheitsmechanismen gering zu halten. Für spezifische, potenziell nur wenige Unternehmen, Benach-

richtigungen und Anwendungsfälle betreffende Schutzbedarfe und Risiken werden auf Vermeidung und Auslagerung ausgerichtete Maßnahmen ergriffen:

- Bestimmte Ausnahmeszenarien, die nur mit extrem hohem Aufwand und korrespondierenden Ausnahmemaßnahmen in der Sicherheitsarchitektur abzusichern wären, SOLLEN explizit ausgeklammert werden, d. h. können nicht über den P23R realisiert werden. In diesen Fällen MÜSSEN die auch aktuell ohne P23R in den Unternehmen genutzten Verfahren als Ersatzverfahren weiterlaufen (was aber in jedem Fall – insbesondere beim Einsatz einer neuen Technologie – empfehlenswert ist).
- Bedrohungen des P23R und seiner Daten, die durch konzeptionelle Maßnahmen des Unternehmens im Vorfeld der P23R-Nutzung ausgeschlossen werden könnten, SOLLEN durch entsprechende Vorgaben an das Aufsetzen und Betreiben eines P23R adressiert werden.
- Sofern eine Bedrohung nicht zwingend proaktive technische Maßnahmen erfordert, MUSS immer eine Kombination aus organisatorischen und reaktiven technischen Maßnahmen (d. h. Verbot mit Nachweisbarkeit einer Überschreitung) als Alternative in Erwägung gezogen werden.

Nachfolgend sind die aus dieser Strategie abgeleiteten Konzepte zum Schutz der im P23R verarbeiteten Unternehmensdaten im Detail dargestellt.

CM.P23R.Sec.04: Ausklammern sehr hoher Schutzbedarfe

Daten, die gemäß den Kriterien im BSI-Standard 100-2 [10] einen sehr hohen Schutzbedarf besitzen, DÜRFEN NICHT im Datenpool gespeichert werden, sofern hierdurch zusätzliche, nicht mit bestehenden Maßnahmen abgedeckte Bedrohungen gegen diese Schutzbedarfe entstehen.[5]

CM.P23R.Sec.05: Separierte Nutzergruppen und Chinese Wall Policies

Sofern im P23R Daten aus verschiedenen Unternehmensbereichen zusammengeführt und hierdurch in potenziell unzulässiger Weise – z. B. über die generierten Benachrichtigungen - verknüpfbar werden, MUSS über geeignete Zugriffsregeln auf dem Daten- und Benachrichtigungspool eine Separierung von Nutzergruppen gemäß den im Unternehmen geltenden Regelungen umgesetzt werden (d. h. kein Nutzer hat gleichzeitig Zugriffsrechte auf voneinander zu trennende Daten und/oder Benachrichtigungen). Alternativ KANN diese Separierung auch durch Aufsetzen mehrerer gegeneinander abgeschotteter Instanzen eines P23R mit jeweils unterschiedlichen Quelldaten und Nutzergruppen erfolgen (Z. B. Aufsetzen einer eigenen P23R-Instanz für Personalmeldungen zu der nur Mitarbei-

[5] Beispiel: Ein Steuerbüro nimmt für ein KMU im Rahmen einer Datenverarbeitung im Auftrag die Lohnabrechnung vor. Nun sollen auf den Gehaltsdaten der Mitarbeiter des KMU durch das Steuerbüro zusätzlich bestimmte Meldungen an eine Finanzbehörde erzeugt werden. Wenn der P23R in einem Netzsegment aufgesetzt wird, zu dem nur Mitarbeiter des Steuerbüros Zugang haben, die im Rahmen ihrer berufsmäßigen Tätigkeit bereits Zugang zu den Quelldaten haben, besteht zwar ein sehr hoher Schutzbedarf, es liegt aber keine zusätzliche Bedrohung der Vertraulichkeit dieser Daten vor (alle potenziellen Angreifer sind berechtigte Nutzer dieser Daten und eine Verletzung der Zweckbindung ist durch die Nutzung zur Erzeugung von Meldungen an eine Finanzbehörde auch nicht gegeben). Eine Verarbeitung dieser Daten im P23R ist somit zulässig.

ter der Personalabteilung Zugang haben). Wesentlich ist jeweils die Umsetzung einer vollständigen Separierung (Complete Mediation, siehe Abschnitt 3.2), die auch Administratoren mit einschließen MUSS.

In Ausnahmefällen kann darüber hinaus die Umsetzung von Regelungen erforderlich sein, die sicherstellen, dass eine Person, die einen Teil des geschützten Datenbestands einsehen konnte, keine Zugriffsrechte auf mit diesen Daten nicht zu verknüpfende andere Teile des Datenbestands mehr erhalten kann (z. B. Trennung von Investmentbanking und Aktien-Emission bei Banken). Eine solche Chinese Wall Policy kann nicht isoliert auf einem P23R implementiert werden, da zur Durchsetzung einer solchen Regelung auch die Zugriffshistorie der unternehmensinternen Daten berücksichtigt werden muss. Unternehmen, die eine Chinese Wall Policy technisch durchsetzen (Brewer-Nash-Modell [11]) SOLLEN von der Möglichkeit Gebrauch machen, einen P23R mit dem internen Berechtigungsmanagement zu koppeln (siehe Abschnitte 5.4 und 5.5). Ist dies nicht möglich, MUSS eine organisatorische Regelung durchgesetzt werden, die technisch durch eine Separierung von Nutzerkreisen abgesichert sein MUSS.

CM.P23R.Sec.06: Datensparsamkeit und Auslagerung von kritischen Daten

Anforderungen an Nichtabstreitbarkeit und Nachweisbarkeit erfordern die langfristige Speicherung von Benachrichtigungen und die Protokollierung des Lebenszyklus einer Benachrichtigung. Die Anforderung nach Nachvollziehbarkeit erfordert eine Versionierung aller zur Erzeugung einer Nachricht verwendeten Daten und Benachrichtigungsregeln. Hierdurch werden Kopien geschützter Daten geschaffen, die ebenfalls zu schützen sind. Um die Anzahl der Kopien zu minimieren und möglichst wenige kritische Daten im P23R vorhalten zu müssen, werden die folgenden Maßnahmen vorgeschlagen:

- Eine Versionierung von Daten findet im P23R nicht statt. Die Anforderung der Nachvollziehbarkeit wird hiermit in ihrem Umfang eingeschränkt bzw. in die organisatorische Verantwortung des Unternehmens verlagert. Da es insbesondere auch möglich sein muss, Daten manuell nachzubearbeiten, wäre eine vollständige Nachvollziehbarkeit innerhalb des P23R nur durch eine durchgängige Versionierung des Datenpools und eine durchgängige Protokollierung aller – auch in den internen Systemen vorgenommenen – Veränderungen der in den Pool eingestellten Daten möglich. Der mit der Absicherung dieser zusätzlichen Daten verbundene administrative und technische Aufwand ist nicht zu rechtfertigen. Dies gilt umso mehr, als dass in der Außenkommunikation nur die Freigabesignatur verbindlich ist; d. h. die Nachvollziehbarkeit primär dem Schutz des die Freigabe Erteilenden dient. Da für eine solche Absicherung neben außerhalb des P23R laufenden Prozessen (z. B. zur Datenerfassung) auch das unternehmensspezifische Risikoverhalten zu berücksichtigen ist, erscheint es konsequent, ggf. gewünschte technische Maßnahmen zur Nachvollziehbarkeit einer Benachrichtigungserstellung bevorzugt auch in der Infrastruktur und Zuständigkeit des Unternehmens umzusetzen (z. B. durch Versionierung von Quelldaten, genutzten/angepassten Benachrichtigungsregeln und P23R-Instanzen, worüber ebenfalls eine nachträgliche, vollständige Rekonstruktion einer Benachrichtigungserzeugung möglich ist).

- Benachrichtigungen werden nach ihrem erfolgreichen Versand an die adressierte Verwaltung aus dem Benachrichtigungspool des P23R entfernt und können im Unternehmen in einem geeigneten System archiviert werden. Dies kann sowohl ein dediziertes Archivsystem als auch z. B. eine speziell abgesicherte Dateiablage sein.
- Der Lebenszyklus einer Benachrichtigung wird in einem im P23R fest an die Benachrichtigung gebundenen Protokolldatensatz protokolliert. Hier wird z. B. vermerkt, wer die Erstellung der Benachrichtigung angestoßen hat, welche Benachrichtigungsregeln benutzt wurden und wer die Benachrichtigung zum Versand freigegeben hat. Nach dem erfolgreichen Versand der Benachrichtigung wird der Protokolldatensatz zusammen mit der Benachrichtigung archiviert.

CM.P23R.Sec.07: Entkopplung von Quellsystemen und Datenpool

Der Datenpool ist in Bezug auf Sicherheit und Datenschutz die kritischste Komponente des P23R. Um Bedrohungen der Integrität und Vertraulichkeit der im Datenpool gespeicherten Daten wirksam begegnen zu können, MÜSSEN die Schnittstellen in den Datenpool hinein minimiert und geeignet abgesichert werden. Lesezugriffe erfolgen daher ausschließlich über die Schnittstelle zwischen Benachrichtigungsgenerator (Notification Generator) und Datenpool (siehe CM.P23R.Sec09). Schreibzugriffe von außen werden grundsätzlich nicht zugelassen. Die Synchronisation mit den Quelldaten im Unternehmen erfolgt über einen Pull-Mechanismus, d. h. der Datenpool liest die benötigten Daten aktiv aus im Unternehmen angesiedelten Datenquellen aus. Um die Anforderung nach einer Möglichkeit der manuellen Nachbearbeitung von Quelldaten zu erfüllen, können Quellsysteme und Datenpool durch Transferdatenbanken entkoppelt werden. Quellsysteme (z. B. zur Verwaltung von Mitarbeiterdaten des Unternehmens) exportieren hierbei die vom P23R benötigten Daten in eine oder mehrere Transferdatenbanken. Auf diesen Datenbanken können autorisierte Nutzer ggf. Ergänzungen und Bereinigungen der Daten vornehmen. Der Datenpool importiert anschließend die von ihm benötigten Daten aus den Transferdatenbanken.

CM.P23R.Sec.08: Separation von Nachrichtenerzeugung und Nachrichteneinsicht

Alle internen Datenbanken des P23R (Datenpool, Benachrichtigungspool und Benachrichtigungsregelpool) MÜSSEN im Rahmen der regelgesteuerten Generierung einer Benachrichtigung ausschließlich über P23R-interne Dienste angesprochen werden. Ein Auslösen der Generierung einer Benachrichtigung kann entweder über einen externen Nutzer (über einen P23R Entry Point) oder durch einen P23R-internen, zeit- oder ereignisgesteuerten Prozess automatisiert erfolgen.

Im Kern wird der folgende Ablauf realisiert:

- Lesen der für die Generierung der angeforderten Benachrichtigung benötigten Benachrichtigungsregeln aus dem Benachrichtigungsregelpool durch die Komponente Model and Rule-Management (MARM)
- Verifizieren der Authentizität und Integrität der Benachrichtigungsregeln durch das MARM
- Anstoßen des Notification Generators zur Erzeugung der Benachrichtigung
- Speichern der erzeugten Benachrichtigung im Benachrichtigungspool

Eine Einsichtnahme in die erzeugte Benachrichtigung MUSS nur unter Nutzung der Schnittstelle zum Benachrichtigungspool möglich sein. Diese ist über einen Policy Enforcement Point (siehe Abschnitt 3.1) abgesichert, der die vom Unternehmen definierten Berechtigungen zum Zugriff auf Benachrichtigungen durchsetzt.

2.2.3 DURCHGÄNGIGKEIT

Analog zur der bereits zum Schutz der Unternehmensdaten verfolgten Strategie wird auch in Bezug auf die Herstellung von durchgängiger Sicherheit eine Lösung konzipiert, bei der die Beherrschbarkeit der Sicherheit im Mittelpunkt steht. Hierzu werden ggf. auch Abstriche bei der Umsetzung einzelner Anforderungen in Kauf genommen, um die Verhältnismäßigkeit von Aufwand und Nutzen zu wahren und insbesondere nicht zusätzliche Bedrohungspotenziale zu eröffnen.

CM.P23R.Sec.09: Tracking des Lebenszyklus einer Benachrichtigung

Gemäß Anforderung MUSS eine Verwaltung erkennen können, ob ein Unternehmen die zur Generierung einer Benachrichtigung benutzte BR und/oder die erzeugte Benachrichtigung nachbearbeitet hat. Hierzu werden in dem Protokolldatensatz zu einer Benachrichtigung nach jedem Bearbeitungsschritt „Fingerabdrücke“ (z. B. Hashwerte) der Benachrichtigung und der angewendeten Benachrichtigungsregeln und Filter vermerkt. Bei der Ablage einer Benachrichtigung im Benachrichtigungspool kann der P23R so prüfen, ob die Originalregeln genutzt wurden und ob die Benachrichtigung außerhalb der regelbasierten Transformationen manuell verändert wurde. Der beim Einstellen in den Benachrichtigungspool erstellte „Fingerabdruck“ wird an die Verwaltung übermittelt; diese kann so prüfen, ob der Kern der Benachrichtigung während des Freigabeprozesses verändert wurde. Dieses Verfahren ist nicht verbindlich, d. h. es kann nicht 100-prozentig sichergestellt werden, dass der Fingerabdruck nicht verändert wurde. Um dem entgegen zu wirken, müssen relevante Komponenten zertifiziert werden.

CM.P23R.Sec.10: Einführung von Security Service Levels

Zu jeder Benachrichtigungsdefinition müssen die Konnektoren definiert werden, über die diese Benachrichtigung an eine Verwaltung übermittelt werden können. Alle definierten Konnektoren MÜSSEN den erforderlichen Schutzbedarf der Benachrichtigung erfüllen. Alle Konnektoren SOLLEN zur Übermittlung von Benachrichtigungen mit einem hohen Schutzbedarf geeignet sein. Zu Konnektoren für die elektronische Übermittlung von Benachrichtigungen SOLL die Verwaltung ein Verschlüsselungszertifikat bekannt geben, mit dem die Benachrichtigung für einen berechtigten Empfänger verschlüsselt werden kann. Es MUSS ein Signaturzertifikat bekannt gegeben werden, um eine Dienstauthentifizierung eines Konnektors zu ermöglichen.

3 DIE P23R-SICHERHEITSARCHITEKTUR

Die P23R-Sicherheitsarchitektur ist nur lose an die P23R-Anwendungsarchitektur gekoppelt, wodurch Sicherheitsdienste und Anwendungsdienste weitgehend unabhängig voneinander umgesetzt und weiterentwickelt werden können. Die lose Kopplung wird dadurch realisiert, dass erforderliche Sicherheitsprüfungen (Authentizität und Autorisierung von Nutzern, Integrität von Nachrichten etc.) schon vor dem Aufruf einer Verarbeitungslogik bei der Abarbeitung des vorgeschalteten Protokoll-Stack durchgeführt werden. Die Verarbeitungslogik kann damit davon ausgehen, dass sie immer innerhalb des definierten Sicherheitskontextes ausgeführt wird. Abbildung 2 stellt dieses Muster am Beispiel des externen Aufrufs einer P23R-Funktion dar.

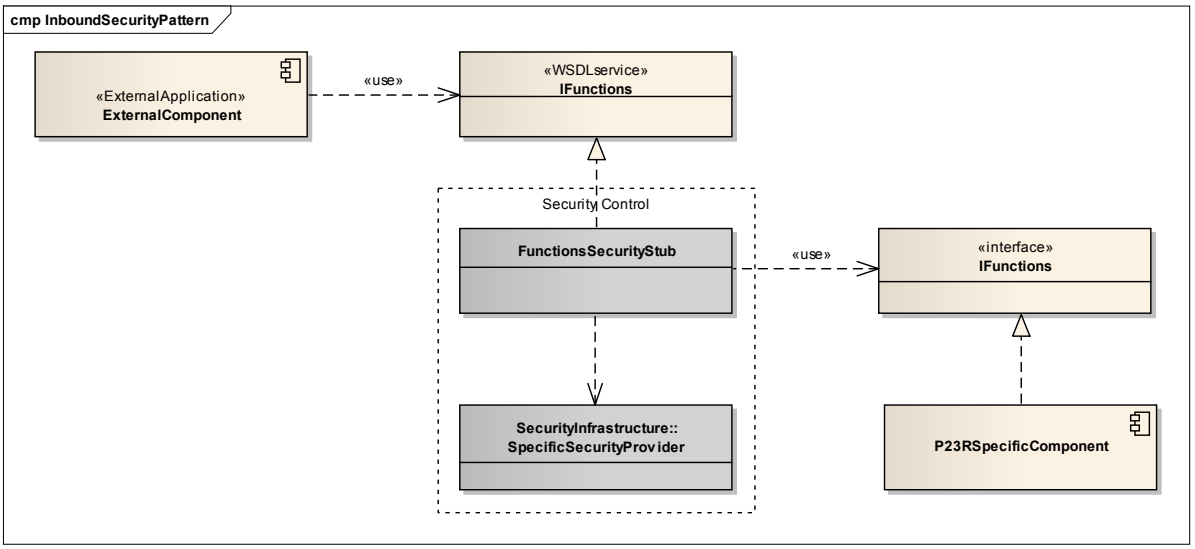


ABBILDUNG 2: SICHERHEITSMUSTER FÜR EINEN DIENST BEI EINGEHENDEN ANFRAGEN (UML)

In diesem Beispiel ist die Herstellung bzw. Verifizierung des für eine P23R-Komponente definierten Sicherheitskontexts in die Abarbeitung des Web Service Stack integriert (z. B. durch Einhängen eines entsprechenden Handlers, der aus dem verwendeten Framework heraus aufgerufen wird) und findet damit bereits zwischen der Annahme einer SOAP-Nachricht an der externen Dienstschnittstelle des P23R und dem Aufruf der internen Schnittstelle der Komponente statt. Diese „Sicherheitsüberprüfung“ (Security Control) umfasst die Umsetzung der Maßnahmen zur Nachrichtensicherheit, die Verifizierung mitgelieferter Sicherheitsobjekte sowie die Prüfung der Identität, Authentizität und Autorisierungen des Nutzers. Ein „Functions Security Stub“ bereitet dabei die in der Anfrage enthaltenen, potenziell für jede Nachricht individuell kodierten Informationen so auf, dass diese anschließend von den spezifischen Sicherheitsdiensten der P23R-Sicherheitsarchitektur verarbeitet werden können.

In diesem Kapitel wird die Sicherheitsarchitektur des P23R im Überblick dargestellt. Hierbei u. a. beschrieben, welche Anforderungen die konkrete Ausgestaltung der „Security Control“ bestimmen, aus welchen elementaren Bausteinen diese zusammengesetzt ist und wie das oben skizzierte Muster in der P23R-Sicherheitsarchitektur auf bestehende Standards abgebildet wurde.

3.1 AUFBAU DER P23R-SICHERHEITSARCHITEKTUR

Die P23R-Sicherheitsarchitektur basiert auf dem Muster einer serviceorientierten Architektur (SOA) und zeichnet sich durch die folgenden Eigenschaften aus (siehe Dokument [12]):

- Lose Kopplung von Sicherheitsdiensten: Dienste zur Authentifizierung und Autorisierung sind voneinander entkoppelt, wodurch P23R-Umsetzungen unterschiedliche Authentisierungsmethoden mit unterschiedlichen Autorisierungsparadigmen kombinieren können. Dienste sind modular aufgebaut und erlauben ein flexibles Deployment der einzelnen Bausteine der Sicherheitsarchitektur (siehe Abschnitt 3.3).
- Zustandslosigkeit von Sicherheitsdiensten: Die P23R-Sicherheitsarchitektur kapselt Sicherheitskontexte in Sicherheitstoken, die von dedizierten STS ausgestellt werden. Die Sicherheitstoken konsumierenden Dienste sind zustandslos, da sie ihren Sicherheitskontext unter Nutzung der übergebenen Token erst beim Dienstaufruf aufbauen. Dieser Mechanismus erlaubt es, Sicherheitskontexte auch organisationsübergreifend auszutauschen und damit einen „Circle of Trust“ aufzuspannen.
- Dedizierte Dienste zur Kapselung von persistenten Daten:[6] Persistente Daten werden über dedizierte Dienste bereitgestellt, die zur Laufzeit von den Sicherheitsdiensten angefragt werden. Durch die Trennung von Funktionalität und Daten können z. B. Quellsysteme für Attribute von Nutzern und Berechtigungsregeln außerhalb des P23R angesiedelt und eng an den Lebenszyklus dieser Informationen in Unternehmen und Verwaltungen gekoppelt werden.

Die Sicherheitsarchitektur des P23R besteht aus zwei lediglich über die Semantik der ausgetauschten Identitätsinformationen lose gekoppelten Subsystemen, die ihrerseits aus lose gekoppelten Diensten aufgebaut sind. Die Subsysteme bilden die für serviceorientierte Sicherheitsarchitekturen typische Entkopplung von Authentifizierung und Autorisierung ab:

- Authentifizierungs-Subsystem (engl. Identity Management Subsystem): Stellt sicher, dass nur identifizierte und authentifizierte Nutzer Zugang zu Diensten des P23R erlangen können.
- Autorisierungs-Subsystem (engl. Access Management Subsystem): Bietet Dienste zur Berechtigungsprüfung an, um geschützte Ressourcen vor unberechtigtem Zugriff zu schützen.

In Abbildung 3 ist das prinzipielle Zusammenspiel der Sicherheits-Subsysteme mit den P23R-Anwendungsdiensten skizziert.

[6] Persistente Daten der Sicherheitsarchitektur sind Sicherheitsobjekte, wie z. B. Nutzerattribute und Berechtigungsregeln.

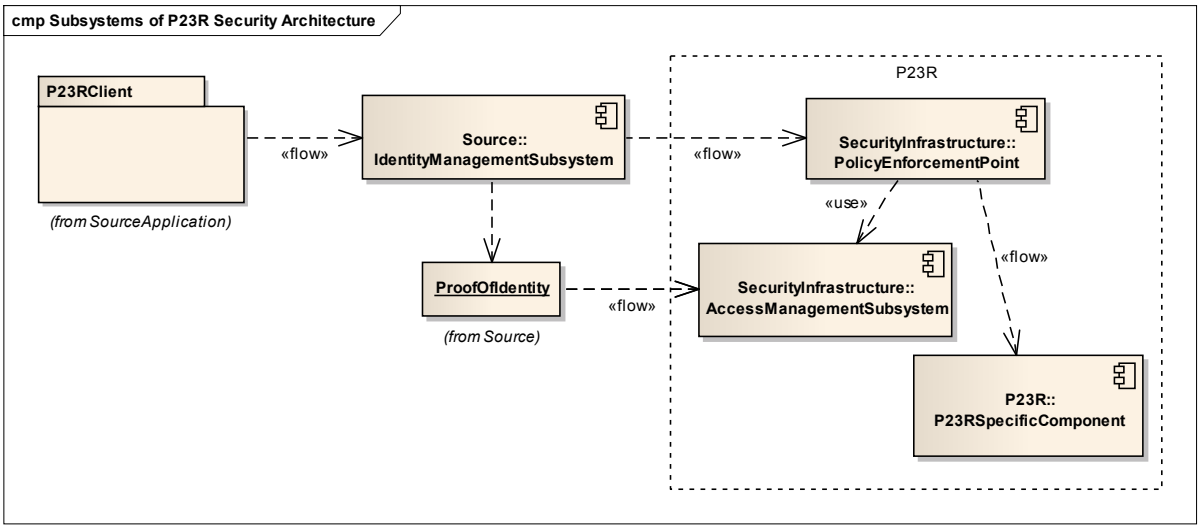


ABBILDUNG 3: SUBSYSTEME DER P23R-SICHERHEITSARCHITEKTUR (UML)

Jeder externe Aufruf eines P23R-Fachdienstes wird durch das Identity Management Subsystem des Quellsystems (engl. Source) geleitet, welches die Identität und Authentizität des Aufrufenden festgestellt. Informationen zur Nutzeridentität werden als Sicherheitstoken gekapselt und über die normalen Dienstaufrufe für das Access Management Subsystem zur Verfügung gestellt („piggybacking-Verfahren"). In die Abläufe der Fachdienste sind vor Zugriffen auf geschützte Ressourcen (Funktionalitäten und Daten) sogenannte Policy Enforcement Points eingebettet, die den Kontrollfluss unterbrechen und eine Autorisierungsprüfung anstoßen. Dies Muster ist auch als „Reference Monitor" [13] bekannt. Im Access Management Subsystem wird anhand von Berechtigungsregeln geprüft, ob der identifizierte Nutzer die gewünschte Aktion ausführen darf. Je nach Entscheidung wird der Kontrollfluss des Fachdienstes fortgesetzt (P23R Specific Component) oder abgebrochen.

3.2 Principles of Secure Design

Sicherheitsarchitekturen zur Herstellung von Sicherheitszielen, wie z. B. Vertraulichkeit, Integrität, Nichtabstreitbarkeit etc., sind Bestandteil jeglicher Systeme, mit denen schützenswerte Daten verarbeitet werden. Entlang der Entwicklungslinien der IT-Nutzung in Unternehmen und Verwaltungen haben sich hier über die Jahre sogenannte „Principles of Secure Design" herausgebildet, die mittlerweile als unbedingt zu verfolgende „Leitlinien" für das Design von Sicherheitsarchitekturen und deren Anbindung an Anwendungsarchitekturen anzusehen sind.

Nachfolgend wird auf Basis der in [14]-[18] ausgeführten „Principles of Secure Design" dargestellt, wie diese Prinzipien in der Sicherheitsarchitektur des P23R umgesetzt sind:

- Economy of Mechanism: Das Berechtigungskonzept muss so einfach wie möglich sein. Es muss ein abgrenzbares Problem adressieren.
  - Die P23R-Sicherheitsarchitektur ist unabhängig von einem konkreten Berechtigungskonzept. Sie erlaubt eine direkte Abbildung von Zuständigkeiten und Verantwortlichkeiten eines Unternehmens bzw. einer Verwaltung auf Berechtigungsregeln.

  - Die Trennung der Sicherheitsarchitektur in zwei Subsysteme erlaubt eine separate Behandlung von Fragen des Identitätsmanagements (engl. Identity Management) und des Berechtigungsmanagements (engl. Access Management).

- Complete Mediation: Jeder Zugriff auf eine Ressource muss durch ein Zugriffsberechtigungssystem geschützt sein. Es darf (auch für Administratoren) keine Möglichkeit geben, am Access Management vorbei auf eine Ressource zuzugreifen.
  - Durch Umsetzung des Musters eines Reference Monitor [13] ermöglicht die P23R-Sicherheitsarchitektur einen vollständigen Schutz von Ressourcen. Die erforderlichen Zugänge zu Ressourcen werden auf ein Minimum reduziert und erlauben damit die Umsetzung eines hohen Schutzniveaus mit punktuell eingebetteten Policy Enforcement Points (siehe Abschnitt 5.3).
  - Berechtigungsregeln können für jeden Zugriff definiert werden. Hiermit kann auch die Einhaltung von Berechtigungen der Administratoren technisch durchgesetzt werden.
- Open Design: Die genutzten Mechanismen und Algorithmen müssen offen und überprüfbar sein.
  - Die P23R-Sicherheitsarchitektur nutzt ausschließlich offene Standards, für die auch Open Source Software zur Verfügung steht.
  - Erfahrungen mit dem Einsatz der genutzten Standards in anderen Projekten (elektronische FallAkte [19], epSOS [20], STORK [21] etc.) wurden beim Design der P23R-Sicherheitsarchitektur berücksichtigt.
- Least-Common Mechanism: Zwischen Anwendungen bzw. Nutzern geteilte Objekte und Zustände der Ablaufumgebung sollten auf das notwendige Minimum reduziert werden.
  - Sicherheitskontexte werden in der P23R-Sicherheitsarchitektur als Sicherheitstoken gekapselt. Zustandsinformationen sind damit immer eindeutig an einer Stelle kodiert.
  - Sicherheitstoken werden über den SOAP Header kommuniziert, während Anwendungsdaten im SOAP Body enthalten sind. Sicherheitstoken werden ausschließlich in den Subsystemen der Sicherheitsarchitektur verarbeitet, während Anwendungsdaten nur von Fachdiensten der Anwendungsarchitektur verarbeitet werden.
- Fail-Safe Defaults: Zugriffe, die nicht explizit als erlaubt verifiziert werden können, sind verboten. Privilegien werden immer nur zu einer initial leeren Menge von Berechtigungen hinzugefügt („opt-in“ statt „opt-out“).
  - Alle Policy Enforcement Points des P23R verfolgen eine sogenannte „deny-based policy“, mit der Zugriffe nur bei einer eindeutig positiven Regelauswertung zugelassen werden.
- Separation of Privilege: Schutzmechanismen sollten soweit als möglich auf der Erfüllung mehrerer unabhängiger Bedingungen basieren.
  - Die P23R-Sicherheitsarchitektur bietet technische Mechanismen zum dynamischen Abruf von Informationen zu Nutzern, Umgebungsbedingungen und Ressourcen an. Dies erlaubt

die Definition von Berechtigungsregeln, die über eine einfache Auswertung von Rollenrechten hinausgehen und auch Kontextbedingungen berücksichtigen.

  - Das Identity Management Subsystem unterstützt alle gängigen Authentifizierungsmechanismen und damit auch solche, die auf mehreren Faktoren (z. B. „Besitz und Wissen“) beruhen.

- Least Privileges: Ein Nutzer / Prozess greift immer nur mit den Privilegien (Berechtigungen) auf eine Ressource zu, die für die Erfüllung der Aufgabe gerade ausreichend sind.
  - Die P23R-Sicherheitsarchitektur unterstützt neben einem Perimeterschutz vor allem die feingranulare Absicherung einzelner Dienste und Ressourcen. Berechtigungen werden immer nur für eine Aktion auf einer Ressource erteilt.
- Privacy Consideration: Es sollte immer nur der Anteil eines Datensatzes herausgegeben werden, der für die Erfüllung der aktuellen Aufgabe zwingend benötigt wird.
  - Die in der P23R-Sicherheitsarchitektur eingesetzten Standards erlauben eine nutzerindividuelle Filterung von Datensätzen, d. h. zur Laufzeit können bei Bedarf einzelne Datenelemente für den aktuellen Nutzer ausgeblendet werden.
- Psychological Acceptability: Mechanismen der Zugriffskontrolle dürfen den Datenzugriff für berechtigte Nutzer nicht komplizierter und unvertretbar aufwändiger machen, als dies ohne Zugriffskontrolle der Fall wäre.
  - Das P23R-Authentifizierungs-Subsystem ist in der Lage, im Unternehmen oder in einer Verwaltung vorgenommene Authentifizierungen in den P23R einzuspielen. Hierdurch können Dienste eines P23R über ein Single Sign-On in bestehende Fachverfahren eingebunden werden.
  - Nutzerattribute können on-demand aus der Unternehmens-IT abgefragt werden, d. h. die Auswertbarkeit von Regeln muss nicht zwingend bei deren Design abgesichert werden.
- Reluctance to Trust: Externe Systeme müssen immer als unsicher angesehen werden, es sei denn, dass durch eine angemessene Sicherheitszertifizierung (z. B. nach Common Criteria [22]) das Gegenteil angenommen werden kann. Die Zahl der Systemelemente, auf deren fehlerfreies und sicheres Funktionieren bei der Zugriffssicherung vertraut werden muss, sollte minimal sein.
  - Ein P23R kann mitsamt aller Sicherheitsdienste komplett gekapselt werden („P23R-in-a-Box“), um auch Einsatzszenarien in unsicheren Umgebungen umzusetzen (siehe Abschnitt 3.4).
  - Die P23R-Sicherheitsarchitektur nutzt in hohem Maße eine deklarative Sicherheit (siehe Abschnitt 3.3). Hierdurch sind keine Eigenentwicklungen von Sicherheitskomponenten erforderlich.
- Isolation: Die Sicherheitsdienste sollten von anderen Systemfunktionalitäten isoliert sein und besonders geschützt werden können.

- Sicherheitsdienste sind lose gekoppelt und bilden eine von der Anwendungsebene unabhängige Sicherheitsarchitektur.
- Die zentralen Sicherheitsfunktionen zur Authentifizierung und Berechtigungsprüfung können über verfügbare Hardware-Lösungen gekapselt werden.

- Conceptual Integrity: Die zur Authentisierung und Autorisierung eingesetzten Mechanismen und Abläufe sollten für alle Akteure identisch sein. Die technische Lösung muss sich auf die etablierten Konzepte zur Zugriffskontrolle abbilden und über darauf aufbauende Standards umsetzen lassen.
  - Das Identity Management Subsystem bildet verschiedene Mechanismen der Nutzerauthentifizierung auf einen einheitlich kodierten Identitäts- und Authentizitätsnachweis ab. Alle Autorisierungen werden über Regeln kodiert und können gegen Attribute ausgewertet werden, die über einen einheitlichen Mechanismus abgefragt werden.
  - Die P23R-Sicherheitsarchitektur nutzt ausschließlich offene Standards, die bereits erfolgreich in komplexen Anwendungsszenarien – z. B. im Gesundheitswesen (elektronische FallAkte [19]) und eGovernment (OSCI Transport 2.0 [9]) – im Einsatz sind.[7]

3.3 Deklarative Sicherheit

Eine wesentliche, mittlerweile auch gut mit Standards abgedeckte Entwicklungstendenz der letzten Jahre ist die Abkehr von einer programmierten Sicherheit hin zu einer deklarativen Sicherheit [23]. Während bei programmierter Sicherheit Sicherheitsmechanismen gemäß den Vorgaben einer konkreten Sicherheitsarchitektur in Programmcode übersetzt und als Sicherheitsdienste kompiliert werden, ist es das Ziel deklarativer Sicherheit, die für eine Komponente oder Kommunikationsbeziehung geltenden Sicherheitsziele in einem menschen- und maschinenlesbaren Dokument zu beschreiben, um damit das Verhalten eines Sicherheits-Frameworks zu steuern.

Deklarative Sicherheit erhöht damit nicht nur die Flexibilität einer Lösung, sondern erleichtert insbesondere auch die Nutzung von bestehenden Produkten. Es muss nichts neu programmiert werden, sondern nur ein erprobtes System neu konfiguriert werden. Ein weiterer Vorteil in Bezug auf Sicherheit und Datenschutz ist die erhöhte Sichtbarkeit von zentralen Sicherheitsmaßnahmen. Diese sind nicht mehr im Programmcode verborgen, sondern in Form einer Deklaration festgehalten, deren Konformität zu einem Sicherheits- und Datenschutzkonzept leicht verifizierbar ist.

In der Sicherheitsarchitektur des P23R spielen Konzepte und Standards einer deklarativen Sicherheit eine wichtige Rolle:

- Die Abläufe im Identity Management Subsystem und deren Anbindung an den P23R sind so gestaltet, dass sie über WS-Policy [24] und WS-SecurityPolicy [25] gesteuert werden können (siehe Abschnitt 4.4). Hierdurch kann z. B. konfiguriert werden, welche Sicherheitsnachweise in einen P23R eingespielt werden dürfen.

[7] Die in der Sicherheitsarchitektur verwendeten Standards werden in Form von Steckbriefen in Kapitel 8 vorgestellt.

- Berechtigungen werden durchgängig deklarativ als XACML Policies [26] kodiert. Hiermit ist ein P23R in der Lage, unternehmensspezifische Rollen zu verarbeiten und unterschiedlichste Berechtigungsparadigmen umzusetzen. Faktisch kann so jedes Unternehmen seine bestehenden, auf der individuellen Organisationsstruktur basierenden Rollen und Rechte per Rechtedeklaration in einen P23R einbringen.
- Ein Unternehmen oder eine Verwaltung beschreiben in einer TSL (siehe Abschnitt 7.1), welche für die Sicherheitsdienste relevanten Funktionalitäten und Daten (Attribute und Regeln) sie selber umsetzen. Beispiele hierfür sind ein Unternehmen, welches Berechtigungsregeln aus seinem Berechtigungsmanagement für einen P23R bereitstellt, oder eine Verwaltung, die ihre an die Verwaltungs-Public Key Infrastructure [27] angebundenen Nutzerzertifikate für eine Anmeldung am P23R eines Unternehmens nutzen möchte.

Grundsätzlich soll es hierdurch möglich sein, die P23R-Sicherheitsarchitektur mit minimalem Programmieraufwand über bestehende und standardmäßig integrierbare WS-*-, SAML- und XACML-Frameworks umzusetzen.

3.4 Integration in bestehende IT-Infrastrukturen

In den Machbarkeitsstudien (siehe [28]-[30]), im Dokument [8] sowie im informellen Dokument zur Rahmenarchitektur (siehe [1]) werden je nach Einsatzkontext verschiedene zu unterstützende Deployments eines P23R beschrieben. Diese reichen von der Umsetzung eines P23R als isoliertes, alle Funktionalitäten und Daten vollständig kapselndes Produkt („P23R-in-a-Box“) bis hin zur Integration von P23R-Funktionalitäten in ein bestehendes Human-Resources-System oder Fachverfahren („P23R Inside“). Analog hierzu MUSS auch die P23R-Sicherheitsarchitektur so flexibel aufgebaut sein, dass sie sowohl als abgeschlossenes System umsetzbar ist als auch sehr eng mit im Unternehmen bereits vorhandenen Funktionalitäten interagieren kann. Die in diesem Dokument spezifizierte P23R-Sicherarchitektur ist so konzipiert, das jede spezifikationskonforme P23R-Umsetzung durch eine geeignete Konfiguration die komplette Spannbreite von einem P23R-in-a-Box bis zu einer engen Bindung an bestehende IT-Infrastrukturen abdecken kann. Viele dieser Konfigurationen sind dynamisch, wodurch sich z. B. ein von einem P23R-Provider für mehrere Unternehmen betriebener P23R gegenüber einem angebundenen Unternehmen als P23R-in-a-Box verhalten kann, während ein anderes angebundenes Unternehmen wesentliche Sicherheitsfunktionalitäten über seine bestehenden Systeme abdeckt.

3.4.1 P23R-in-a-Box

In dieser Konfiguration sind alle Sicherheitsdienste voll in den P23R integriert. Die Authentifizierung des Nutzers erfolgt über einen integrierten Client (siehe Abschnitt 4.5) gegen den P23R-Identity-Provider. Berechtigungsregeln werden im P23R verwaltet und können über eine Schnittstelle des P23R-Herstellers gepflegt werden. Eine Übersicht dieses Konzepts gibt Abbildung 4.

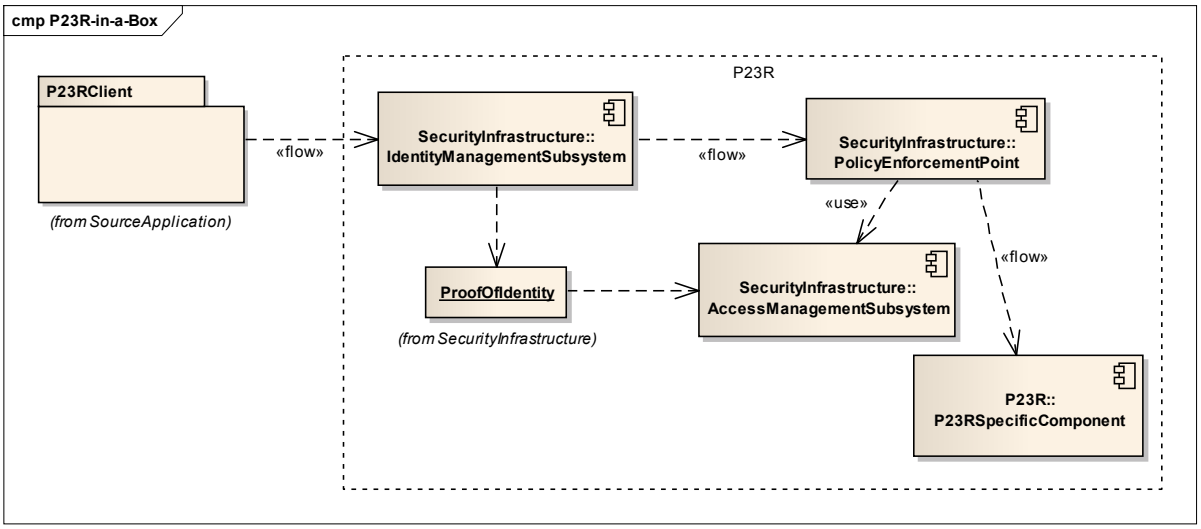


ABBILDUNG 4: P23R-IN-A-BOX (UML)

Diese Konfiguration eignet sich vor allem für (kleine) Unternehmen, die kein internes Identitäts- und / oder Berechtigungsmanagement betreiben oder für die aufgrund nur weniger zu generierender Benachrichtigungen eine Anbindung des P23R an bestehende Fachverfahren nicht wirtschaftlich ist.

3.4.2 VERNETZUNG MIT IT-SYSTEMEN IN UNTERNEHMEN UND VERWALTUNG

Viele zur Umsetzung der Sicherheitsdienste des P23R genutzte Komponenten können aus dem P23R ausgelagert werden. Dies betrifft insbesondere Komponenten, welche Daten kapseln, die in der Hoheit des Unternehmens gepflegt werden. Hierzu zählen z. B. Nutzerattribute und Berechtigungsregeln.

Die P23R-Sicherheitsarchitektur kann so konfiguriert werden, dass

- im Unternehmen durchgeführte Authentifizierungen in den P23R eingespielt werden,
- in einer Verwaltung durchgeführte Authentifizierungen über die im OSCI Transport 2.0 Protokoll definierten Mechanismen an den P23R vermittelt werden können,
- Nutzerattribute (Rollen, Zugehörigkeit zu Organisationseinheiten, etc.) ausschließlich außerhalb des P23R verwaltet werden und bei Bedarf vom P23R aus bestehenden Verzeichnisdiensten des Unternehmens abgefragt werden,
- Berechtigungsregeln im Unternehmen (z. B. in einem Access Management System) gepflegt und vom P23R importiert werden,
- Protokolle zu Zugriffen auf geschützte Funktionen oder Daten in ein im Unternehmen angesiedeltes System geschrieben werden.

Konfigurationen, in denen nur einige dieser Optionen genutzt werden und bei denen die restlichen Funktionalitäten im P23R verbleiben, sind möglich. Die Übernahme externer Authentifizierungen und der ggf. für die Autorisierung benötigte On-demand-Abruf von Nutzerattributen können per Konfiguration auch für Verwaltungen aktiviert werden. Hiermit können nicht nur von Verwaltungen an einen P23R gesandte Nachrichten innerhalb des P23R mit den gleichen Sicherheitsmechanismen wie bei der Kommunikation aus einem Unternehmen heraus behandelt werden, sondern es werden auch

perspektivisch sehr flexible Möglichkeiten des Zusammenspiels von mehreren P23Rs (z. B. in Unternehmen und Verwaltungen) umsetzbar.

Wie die Abbildung 5 zeigt, kann individuell aus dem P23R heraus auf bestehende, unternehmensinterne Identitäts- und / oder Berechtigungsmanagementsubsysteme zugegriffen werden.

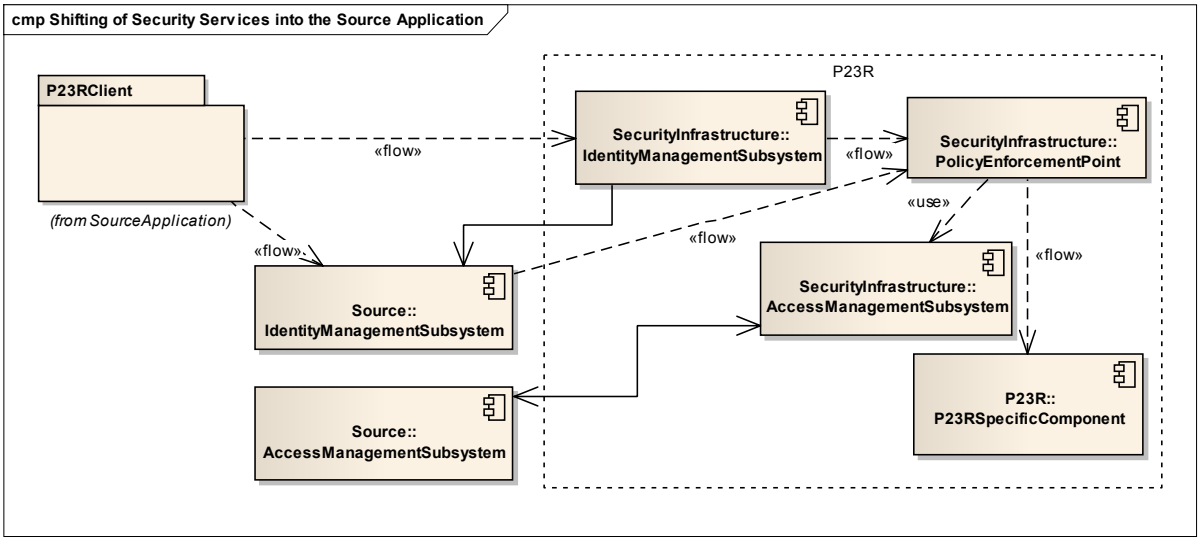


ABBILDUNG 5: VERLAGERUNG VON SICHERHEITSKOMPONENTEN IN DIE UNTERNEHMENS-IT (UML)

Diese Konfiguration ist vor allem für Unternehmen geeignet, die Identitätsdaten und Berechtigungen in elektronischer Form pflegen, intern bereits ein Single Sign-On nutzen und / oder den P23R eng mit bestehenden Fachverfahren koppeln wollen.

4 AUTHENTIFIZIERUNG

Abbildung 6 stellt die technischen Bausteine (engl. building blocks) und Abläufe zur Nutzerauthentifizierung im Überblick dar. Komponenten der Sicherheitsarchitektur sind mit dem Paketnamen „Security Infrastructure“ besonders gekennzeichnet.

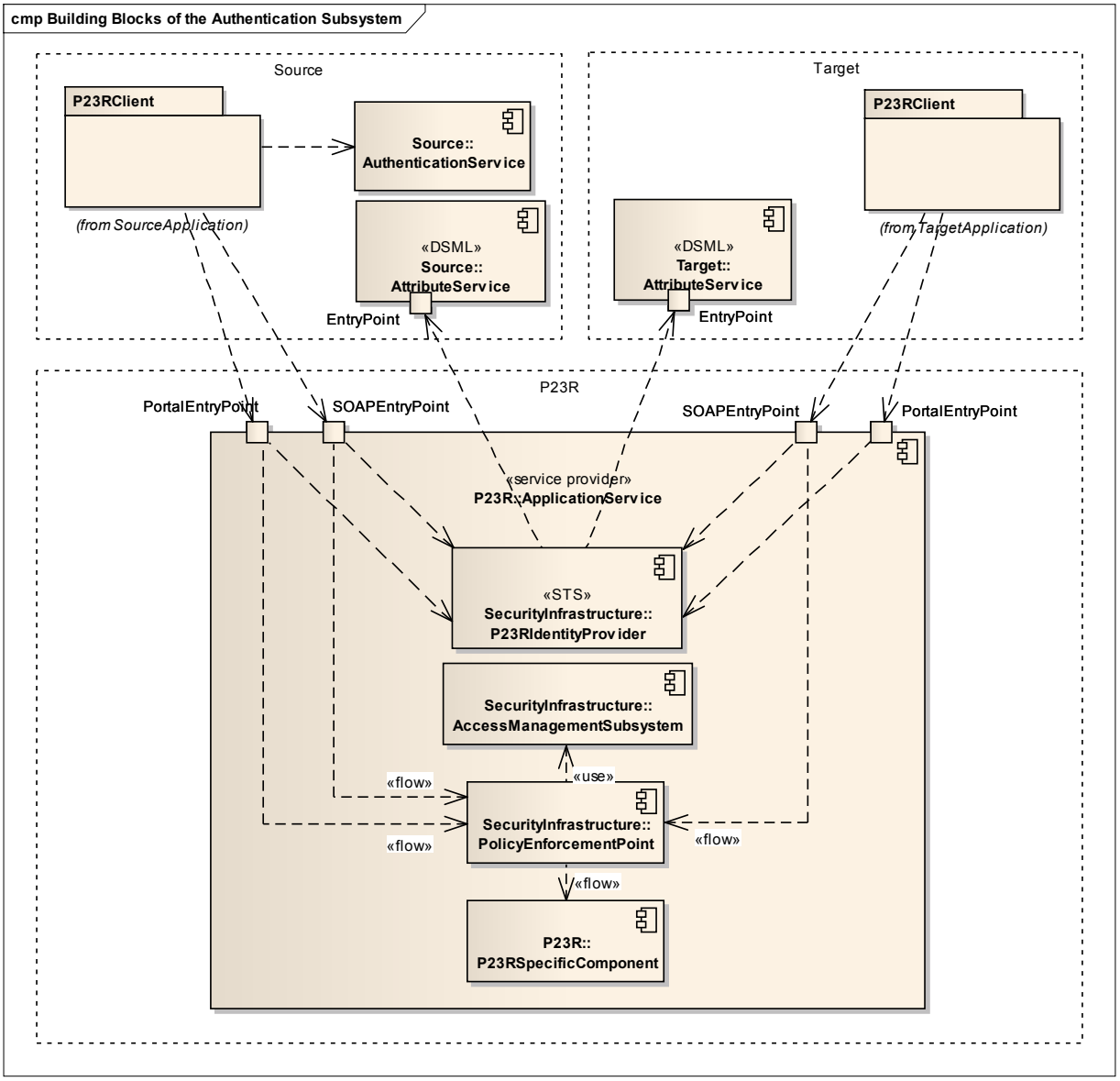


ABBILDUNG 6: BAUSTEINE UND ABLÄUFE DES IDENTITY MANAGEMENT SUBSYSTEMS (UML)

Der grundsätzliche Gedanke des Identity Management Subsystems des P23R ist es, einheitliche Muster für die Authentifizierung von P23R-Nutzern aus Unternehmen (P23R-Client) und Verwaltung (Target Application) zu nutzen und diese innerhalb des P23R auch auf eine einheitliche Technologie abzubilden. Hierdurch ist es für die internen Abläufe innerhalb des P23R und speziell innerhalb des Access Management Subsystems des P23R irrelevant, ob ein Nutzer Mitarbeiter eines Unternehmens

oder einer Verwaltung ist. Wichtig ist nur, dass sich eine Regel finden und ausführen lässt, anhand derer die Autorisierung des Nutzers für die gewünschte P23R-Operation verifizierbar ist.[8]

Zur Berücksichtigung der Anforderungen und Rahmenbedingungen sowohl von Großunternehmen als auch von KMU und Verwaltungen müssen vom P23R zwei Formen der Authentifizierung unterstützt werden:

- Authentifizierung im Unternehmen oder einer Verwaltung: Ein Mitarbeiter eines Unternehmens oder einer Verwaltung meldet sich innerhalb seiner Organisation über die dort üblichen Mechanismen an, ein System innerhalb der Organisation bestätigt gegenüber dem P23R die Identität des Nutzers sowie die erfolgreiche Authentifizierung. Der Nutzer kann gegenüber dem P23R einen Nachweis führen, dass er derjenige ist, dessen Identität und Authentizität bestätigt wurde (in Abbildung 5: Verlagerung von Sicherheitskomponenten in die Unternehmens-IT (UML) exemplarisch für „Source“ dargestellt). Diese Form der Authentifizierung ist vor allem für Großunternehmen und Verwaltungen sinnvoll, die über ein internes Identitäts- und Berechtigungsmanagement verfügen und sich über ein Single Sign-On an den P23R anbinden wollen. Die Umsetzung dieses Verfahrens ist in Abschnitt 4.3 spezifiziert. Abschnitt 4.6 beschreibt ergänzend hierzu, wie OSCI Transport 2.0 genutzt werden kann, um in einer Verwaltung vorgenommene Authentifizierungen an einen P23R zu vermitteln.
- Authentifizierung über P23R-Client (Web Portal): Ein P23R-Nutzer aus einem Unternehmen oder einer Verwaltung meldet sich an einem dem P23R vorgeschalteten, dedizierten Client (z. B. einem Web Portal) an. Der P23R-Client bestätigt gegenüber dem P23R die Identität des Nutzers und dessen erfolgreiche Authentifizierung. Durch die Entkopplung von Nutzer und P23R über den P23R-Client kann der Nutzer keinen direkten Nachweis seiner Identität und Authentizität erbringen; diese Vertrauensstellung wird daher über den Client vermittelt. Diese Form der Authentifizierung ist vor allen dann sinnvoll, wenn ein P23R nur von sehr wenigen Personen genutzt wird und ein Single Sign-On nicht gewünscht oder realisierbar ist. Auch die Anbindung des OSCI Transport 2.0 Protokolls erfolgt technisch über diesen Mechanismus, wobei die Vermittlung der Vertrauensstellung zwischen P23R und Nutzer über ein vorgeschaltetes OSCI-Gateway erfolgt. Die Umsetzung einer Authentifizierung unter Vermittlung der Vertrauensbeziehung über ein Portal oder ein Gateway ist in den Abschnitten 4.5 und 4.6 beschrieben.

Um die Art der Authentifizierung und die Auswirkungen der verschiedenen P23R-Zugangswege auf die Erbringung von Authentizitätsnachweisen möglichst vor den P23R-Diensten zu verbergen, enthält der P23R einen eigenen Identity Provider. Dieser nimmt externe (d. h. im Unternehmen bzw. einer Verwaltung erstellte oder vom P23R-Client verbürgte) Authentisierungsnachweise entgegen und bildet diese auf ein einheitliches Profil ab. Zusätzlich führt er bei Bedarf eine Transformation von Attri-

[8] Die Authentifizierung von Verwaltungsmitarbeitern gegen einen P23R wird hier ausschließlich im Kontext von Nachrichten betrachtet, die aus einer Verwaltung – z. B. als Reaktion auf eine Benachrichtigung – an einen P23R gesandt werden. Perspektivisch erlauben es die in diesem Dokument spezifizierten Mechanismen jedoch auch, eine Authentifizierung durch eine gesamte, potenziell mehrere Verwaltungen durchlaufende Prozesskette zu ziehen.

buten auf ein einheitliches Format durch und / oder ruft fehlende Nutzerattribute von einem Attribute Service innerhalb des Unternehmens oder einer Verwaltung ab.

Alle Zugänge zu P23R-Diensten sind über Policy Enforcement Points abgesichert. An diesen Punkten wird die Ausführung einer Operation unterbrochen und eine Berechtigungsprüfung durchgeführt. Hierbei wird der vereinheitlichte, vom P23R-internen Identity Provider ausgestellte Identitäts- und Authentizitätsnachweis an das Access Management Subsystem des P23R übergeben.

4.1 P23R-IDENTITY-PROVIDER: FUNKTION UND SCHNITTSTELLEN

Der P23R-Identity-Provider ist die zentrale Komponente des Identity Management Subsystems des P23R. Der P23R-Identity-Provider ist ein WS-Trust 1.3 [31] Sicherheitstokendienst (Security Token Service, STS). Seine Aufgabe ist es, von externen Systemen (Authentifizierungsdienst im Unternehmen, P23R-Client etc.) vorgenommene Authentifizierungen in ein Format zu überführen, das von den Diensten des P23R-Berechtigungssystems interpretiert werden kann. Die entsprechenden Nachweise zur Identität des Nutzers und seiner Authentifizierung werden vom P23R-Identity-Provider in Form einer P23R-Identity-Assertion ausgegeben. Eine P23R-Identity-Assertion ist eine SAML 2.0 [32] Authentication Assertion, in der Informationen zur Organisationszugehörigkeit und den Rollen des Nutzers kodiert sind (siehe Abschnitt 4.2).

Jedem Aufruf eines P23R-Dienstes MUSS im WS-Security Header eine gültige P23R-Identity-Assertion mitgegeben werden. Daher MUSS ein P23R-Nutzer vor dem ersten Aufruf eines P23R-Dienstes eine entsprechende Assertion vom P23R-Identity-Provider anfordern. Dieser Ablauf KANN durch eine WS-Policy bzw. WS-Security Policy für die Dienste des P23R automatisiert werden (siehe Abschnitt 4.4).

Zum Abruf von P23R-Identity-Assertions implementiert der P23R-Identity-Provider drei Schnittstellen:

- Externe Systeme können über eine Webservice-Schnittstelle eine P23R-Identity-Assertion für einen zuvor authentifizierten Nutzer abrufen. Hierzu implementiert der P23R eine logische Operation „Authenticate“ am Port „P23RIdentityProviderAuthenticatedClient“. Diese Operation wird auf eine WS-Trust 1.3 Request Security Token Nachricht abgebildet. Der Port „P23RIdentityProviderAuthenticatedClient“ KANN über eine WS-SecurityPolicy abgesichert werden, die auf den zur initialen Authentifizierung zu verwendenden Dienst des Unternehmens verweist (siehe Abschnitt 4.4). Diese Schnittstelle ist NORMATIV und in Abschnitt 4.3 beschrieben.
- Ein direkt an den P23R angebundener Client (z. B. ein Web Portal) KANN ebenfalls die externe Schnittstelle nutzen. Um jedoch die Abläufe in diesem Deployment-Szenario zu vereinfachen und die Vertrauensstellung des Clients zu nutzen, SOLL ein solcher Client über eine interne Schnittstelle direkt auf den P23R-Identity-Provider zugreifen können. Die entsprechende Schnittstelle ist NICHT NORMATIV festgelegt, eine Umsetzungsempfehlung ist jedoch in Abschnitt 4.5 beschrieben.
- Ein dem P23R vorgeschaltetes OSCI-Gateway kann über den Port „P23RIdentityProvider-OSCIGateway“ einen OSCI-konformen Identitäts- und Authentizitätsnachweis in den P23R einspielen. Intern wird dieses auf die hinter der oben skizzierten Operation „Authenticate“ stehende Funktionalität abgebildet. Durch die Nutzung eines dedizierten Ports ist es jedoch

möglich, über WS-SecurityPolicy spezifische Vorgaben zu dem zwischen P23R und OSCI-Gateway herzustellenden Vertrauensverhältnis zu definieren und über das genutzte Framework durchzusetzen. Diese Schnittstelle ist NORMATIV und in Abschnitt 4.6 beschrieben.

- Für die Berechtigungsprüfung bei zeitgesteuerten, internen Aktionen MÜSSEN auch diese mit einem die Aktion verantwortenden Nutzer verknüpft werden. Der P23R-Identity-Provider bietet eine interne Schnittstelle an, mit der eine P23R-Identity-Assertion an eine zeitgesteuerte Aktion gebunden werden kann. Als Identität wird in der Assertion der Nutzer registriert, der das zeitgesteuerte Ereignis am P23R registriert hat. Die funktionale Spezifikation dieser Schnittstelle ist NORMATIV und in Abschnitt 4.7 beschrieben.

4.2 P23R-IDENTITY-ASSERTION

Eine P23R-Identity-Assertion bestätigt gegenüber Diensten des P23R die Identität und Authentizität eines Nutzers. Hierzu verkapselt sie in einer SAML 2.0 [32] Authentication Assertion die folgenden Informationen:

- Eindeutige ID des Nutzers: Diese Angabe wird u. a. zu Zwecken der Protokollierung und zum ggf. erforderlichen Abruf weiterer Nutzerdaten benötigt. Ferner ist es möglich, personenbezogene Berechtigungen zu vergeben, die über die Nutzer-ID ausgewertet werden. Die ID des Nutzers MUSS innerhalb eines Unternehmens (durch die Organisationszuordnung des Nutzers eingegrenzter Kontext) eindeutig sein.
- Authentizitätsnachweis: Je nach Vertrauensstellung des P23R-Client kann der Nachweis der Authentizität entweder direkt vom Nutzer über einen Besitznachweis (z. B. Zugang zu einem privaten Schlüssel) oder indirekt über die Vertrauensstellung zwischen Nutzer, P23R-Client und P23R geführt werden (Aus Sicht des P23R ist ein OSCI-Gateway hierbei nur eine spezifische Ausprägung eines P23R-Clients). Ein indirekter Nachweis SOLL verwendet werden, wenn alle drei benannten Akteure in einem direkten, gegenseitigen und technisch abgesicherten Vertrauensverhältnis stehen. Dieses kann z. B. durch Nutzung von TLS (siehe Kapitel 7 und [33]) realisiert werden. In allen anderen Szenarien MUSS der direkte Besitznachweis erfolgen, d. h. der P23R besitzt keine implizite Vertrauensstellung zum P23R-Client, sondern fordert diese explizit vom Nutzer.
- Organisationszugehörigkeit: Insbesondere in Szenarien, in denen ein P23R für mehrere Unternehmen bzw. Organisationseinheiten eines Unternehmens Benachrichtigungen generiert, MUSS eine eindeutige Zuordnung von Nutzern zu Unternehmen oder Unternehmensteilen möglich sein. Hierdurch werden auch die Sicherheitsdienste des P23R erst in die Lage versetzt, die richtigen Verzeichnisdienste für die Abfrage von Berechtigungsregeln und ggf. erforderlichen weiteren Nutzerinformationen zu lokalisieren. Die Organisationszugehörigkeit SOLL über die X.500-Attribute *organizationName* (oid:2.5.4.10) und *organizationalUnitName* (oid:2.5.4.11) ausgedrückt werden (Definitionen gegeben in [34]).
- Rollenzuweisungen: Sofern der Zugriff auf einen P23R und die dort verwalteten Daten über ein rollenbasiertes Berechtigungsmanagement abgesichert ist, MÜSSEN Angaben zu den Rollen des Nutzers im Unternehmen oder in einer Verwaltung in der P23R-Identity-Assertion

kodiert werden. Hierzu SOLL das X.500-Attribut *roleOccupant* (oid:2.5.4.33) verwendet werden.

- Weitere Zuordnungen: Sofern für die Auswertung von Berechtigungsregeln über reine Funktionsrollen und organisatorische Verankerungen hinausgehende Gruppenzuordnungen eines Nutzers relevant sind, SOLLEN auch diese bereits über die P23R-Identity-Assertion verfügbar gemacht werden. Hierzu SOLL das X.500-Attribut *member* (oid:2.5.4.31) verwendet werden.
- Weitere Attribute: Grundsätzlich KANN ein Unternehmen zur Beschreibung von Mitarbeitern beliebige weitere Attribute in eine P23R-Identity-Assertion einbetten und in Berechtigungsregeln einfließen lassen. Hierbei SOLLEN nach Möglichkeit an X.500 angelehnte Attributnamen verwendet werden (siehe SAML Assertion-Profil in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Kapitel 4 in [5]).

Prinzipiell liegt es in der Entscheidung eines Unternehmens, welche Attribute mit welchen Wertebereichen für die nähere Beschreibung eines Nutzers verwendet werden. Wesentlich ist lediglich, dass in einer P23R-Identity-Assertion kodierte Attributnamen und -werte mit den in den Berechtigungsregeln verwendeten Attributnamen und -werten übereinstimmen. Für die Definition der Nutzerattribute bietet sich daher das in [35] beschriebene Vorgehen an:

- Definition der Berechtigungsregeln
- Identifizieren der für die Auswertung der Berechtigungsregeln benötigten Nutzerattribute
- Definition von „Attribute Stubs“, die für jedes Attribut die Semantik (Bedeutung), den Namen und den Wertebereich festlegen
- Abbilden der „Attribute Stubs“ auf in internen Verzeichnisdiensten abrufbare Nutzerinformationen
- Ggf. Anpassen der „Attribute Stubs“ und Regelwerke auf die intern genutzten Attributnamen und Wertebereiche

Für Nutzer aus Verwaltungen wird hingegen ein fester Satz von zulässigen Attributen vorgegeben. Hierdurch wird sichergestellt, dass Identitäts- und Authentifizierungsnachweise von jedem P23R verarbeitet werden können.

Die technische Spezifikation der P23R-Identity-Assertion und der ausgetauschten Nutzerattribute ist Gegenstand der technischen Spezifikationen zur Sicherheitsarchitektur (vgl. Kapitel 2 in [5]).

4.3 Guarantor Assertion: Schnittstelle und Ablauf (NORMATIV)

Das Guarantor Assertion-Verfahren ist ein etabliertes Muster, um eine im Unternehmen oder einer Verwaltung erfolgte Nutzerauthentifizierung in einen Anwendungskontext einzuspielen. Die Grundidee ist, dass eine Anwendung einen spezifischen Identity Provider nutzt, dieser aber die Authentifizierung des Nutzers an einen vertrauenswürdigen Authentifizierungsdienst delegiert (der die sichere Durchführung der Authentifizierung garantiert und in einem entsprechenden Nachweis verbürgt, daher der Name Guarantor Assertion). Abbildung 7 stellt das Verfahren im Überblick dar.

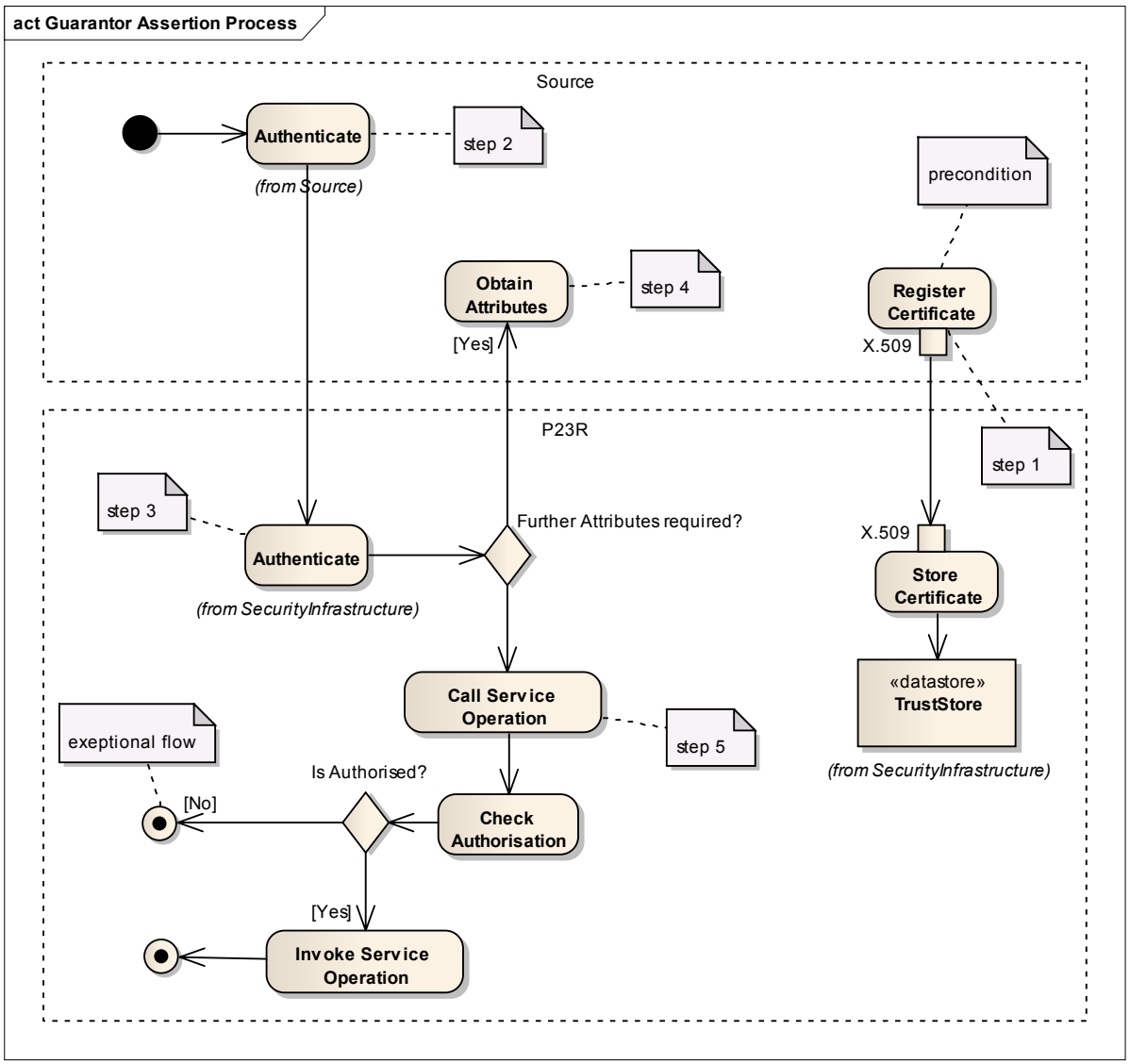


ABBILDUNG 7: GUARANTOR ASSERTION-VERFAHREN (UML)

Voraussetzung für das Einspielen einer im Unternehmen oder einer Verwaltung erfolgten Authentifizierung in den P23R ist, dass der außerhalb des P23R angesiedelte Authentifizierungsdienst dem P23R-Identity-Provider bekannt ist und von diesem als vertrauenswürdig angesehen wird. Diese Herstellung eines Vertrauensverhältnisses erfolgt durch Registrierung des X.509-Zertifikats des Authentifizierungsdienstes am Trust Store des P23R-Identity-Provider (step 1 bzw. Schritt 1). Hier SOLL der in Kapitel 7 beschriebene Mechanismus einer TSL genutzt werden.

Ein Nutzer kann sich nun zunächst gegenüber einem System innerhalb des Unternehmens oder einer Verwaltung anmelden (Schritt 2). Als Nachweis der erfolgreichen Authentifizierung stellt dieses System eine sogenannte Guarantor Assertion aus und signiert diese. In der Guarantor Assertion ist u. a. ein Zertifikat des Nutzers enthalten, so dass dieser über einen Besitznachweis des zugehörigen privaten Schlüssels seine Authentizität nachweisen kann. Sobald ein Nutzer einen Dienst des P23R nutzen will, wird der entsprechende Aufruf zunächst auf den P23R-Identity-Provider umgeleitet (Schritt 3). Dieser prüft die Authentizität der mitgelieferten Guarantor Assertion und des aufrufenden Nutzers und stellt eine P23R-Identity-Assertion in einem Format aus, das von allen Diensten des P23R (und

insbesondere vom Berechtigungsmanagement des P23R) verarbeitet werden kann. Sofern für die Auswertung von Berechtigungen erforderliche Informationen nicht (vollständig) in der Guarantor Assertion enthalten sind, KANN der P23R-Identity-Provider auf Verzeichnisdienste im Unternehmen oder einer Verwaltung zugreifen, um die erforderlichen Nutzerattribute abzufragen (Schritt 4). Unter Beigabe der vom P23R-Identity-Provider ausgestellten P23R-Identity-Assertion kann der Nutzer nun über die definierten Webservice-Endpunkte des P23R (Schritt 5) auf Dienste innerhalb des P23R zugreifen. Diese sind jeweils durch einen Policy Enforcement Point abgesichert, der dafür sorgt, dass vor dem Zugriff auf geschützte Daten oder Funktionen eine Berechtigungsprüfung erfolgt (siehe Kapitel unten).

Für die Anbindung eines OSCI-Gateways (siehe auch Abschnitt 4.6) wird der gleiche Mechanismus genutzt. Hierbei fungiert die über das OSCI Transport 2.0 Protokoll vermittelte OSCI-konforme SAML Identity Assertion als Guarantor Assertion. Der einzige Unterschied ist, dass die Verifizierung der Nutzerauthentizität auf das OSCI-Gateway verlagert wird (die Ende-zu-Ende-Sicherheit von OSCI-terminiert am Gateway und kann nicht in den P23R hinein verlängert werden!) und dieses damit gegenüber dem P23R-Identity-Provider die Authentizität des Nutzers verbürgt.

4.3.1 AUFBAU

Die Guarantor Assertion ist eine SAML Assertion [32] und enthält die Aussage einer erfolgreichen Authentisierung. Das Subjekt der Guarantor Assertion kodiert den erfolgreich authentisierten Nutzer (siehe Abbildung 8 für das Beispiel einer Authentifizierung über einen privaten Schlüssel, bei der der zur Verifizierung des Besitzers benötigte öffentliche Schlüssel ebenfalls in die Guarantor Assertion übernommen wird). Die Nutzeridentifizierung wird später für die Attributanfrage des P23R-Identity-Provider genutzt und 1:1 in die P23R-Identity-Assertion übernommen.

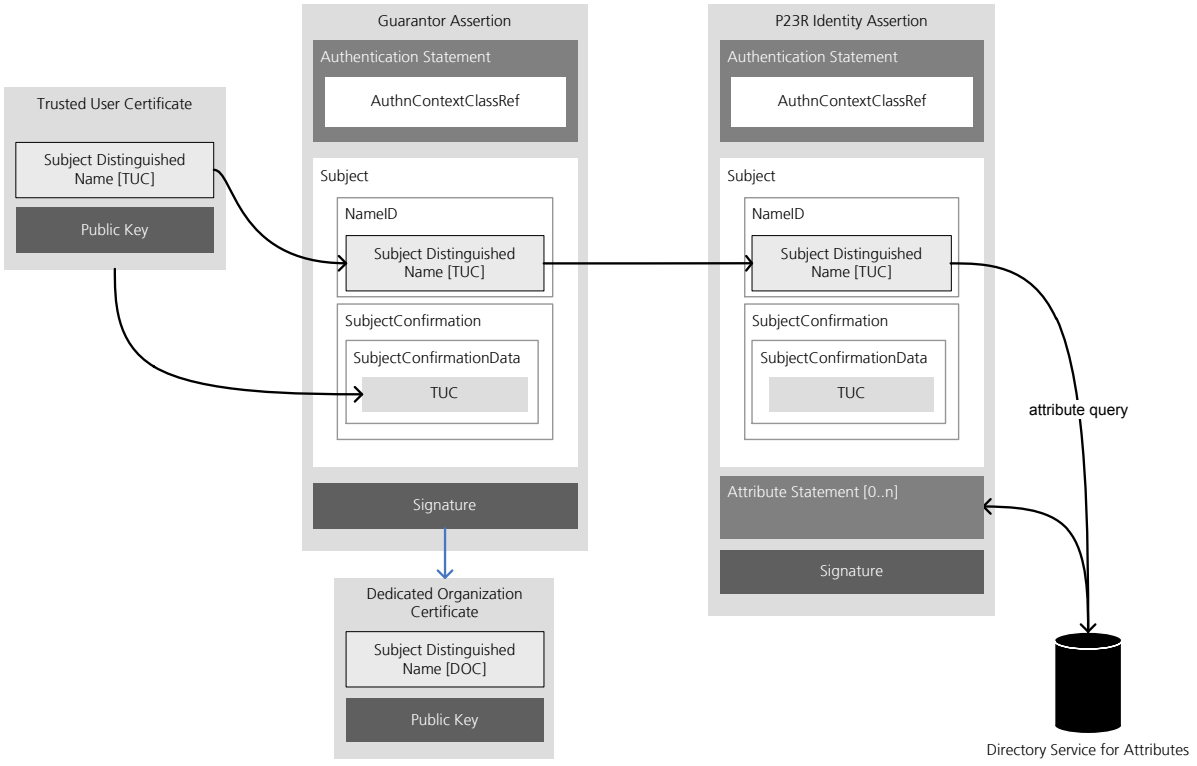


ABBILDUNG 8: GUARANTOR ASSERTION UND IDENTITY ASSERTION (BLOCKDIAGRAMM)

Grundsätzlich kann der als Guarantor Token Service fungierende Authentisierungsdienst eines Unternehmens oder einer Verwaltung als Aussteller der Guarantor Assertion verschiedene Authentisierungsmethoden unterstützen, um auf einen P23R zugreifen zu können bzw. um sich am P23R-Identity-Provider zu authentisieren. Als Beispiele sind neben einer Authentifizierung über eine Chipkarte (Smartcard) vor allem die weit verbreitete Authentisierung über Benutzername und Passwort oder über das Kerberos-Protokoll [36] praxisrelevant. Die Guarantor Assertion vereinheitlicht diese Verfahren durch ein standardisiertes Profil. Die SAML-Spezifikation sieht vor, dass die verschiedenen Kontexte der Authentisierung als Attribut (a*uthentication context class*) bzw. URI-Referenz in einer SAML Assertion festgehalten werden können [37]. Diese Angabe ist für die Guarantor Assertion bindend, sodass dem Konsumenten der Guarantor Assertion (in diesem Fall dem P23R-Identity-Provider) die Entscheidung obliegt, welche Stärke der lokalen Authentisierungsmethode für den P23R als angemessen erachtet wird. In [23] wird ein Verfahren aufgezeigt, wie eine Festlegung zu zugelassenen Authentifizierungsmethoden deklarativ erfolgen kann und damit frei konfigurierbar ist.

4.3.2 Schnittstelle zum P23R-Identity-Provider

Die Abbildung der funktionalen Schnittstellen auf WS-Trust 1.3 RST/RSTR-Nachrichten ist in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 2.1.1 in [5]) gesondert beschrieben.

4.3.3 Ablauf

Die folgenden Ausführungen gehen davon aus, dass ein Unternehmen einen eigenen Authentifizierungsdienst betreibt, der SAML-konforme Authentifizierungsnachweise generieren kann, die als Guarantor Assertions an den P23R-Identity-Provider übergeben werden können. Hiermit können lokale Authentisierungsmethoden (Zertifikat, Kerberos etc.) gegenüber dem P23R gekapselt werden. Die Anbindung von Verwaltungen an einen P23R-Identity-Provider KANN analog umgesetzt werden bzw. über ein vorgeschaltetes OSCI-Gateway erfolgen (siehe Abschnitt 4.6).

Im Einzelnen werden die folgenden Ablaufschritte im Zusammenspiel vom unternehmens- bzw. verwaltungsinternen Authentisierungsdienst (Guarantor Token Service) und P23R-Identity-Provider durchlaufen:

- Der P23R Nutzer authentisiert sich lokal an einem Guarantor Token Service (Abbildung 9). Als übertragbarer Authentisierungsnachweis wird die Guarantor Assertion erzeugt (siehe Abschnitt 4.3.1).

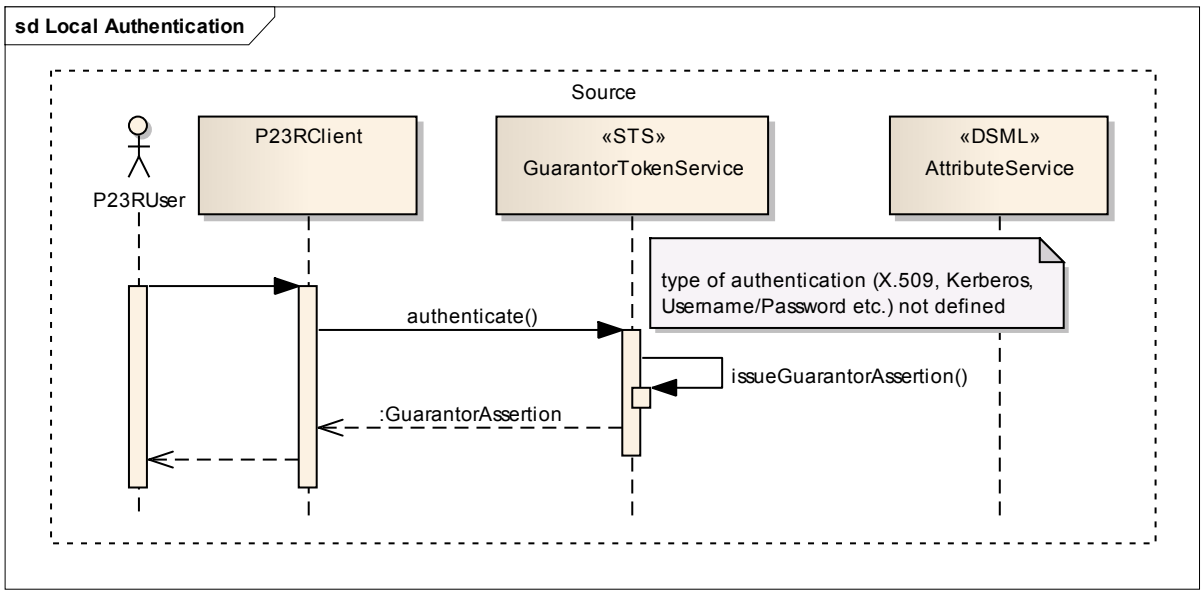


ABBILDUNG 9: LOKALE AUTHENTISIERUNG IM UNTERNEHMEN (UML)

- Als Nächstes wird der lokale Authentisierungsnachweis dem P23R-Identity-Provider vorgelegt (Abbildung 10). Über das WS-Trust-Protokoll wird zugleich der Besitznachweis der Guarantor Assertion durch Signatur der Nachricht erbracht und damit die Prüfung der Authentizität des Nutzers ermöglicht. Der P23R-Identity-Provider verifiziert die Signatur der Guarantor Assertion und überprüft die Nachrichtensignatur auf ihre Konformität zur Subject Confirmation aus der Guarantor Assertion. Im Erfolgsfall KANN der Subject Distinguished Name für eine Attributanfrage an einen Attribute Service im Unternehmen oder in einer Verwaltung genutzt werden (siehe Abschnitt 4.8). Diese Attribute werden für die spätere Autorisierungsprüfung verwendet. Der P23R-Identity-Provider bezeugt die ordnungsgemäße Authentifizierung und die Authentizität der Attribute durch Signatur der P23R-Identity-Assertion, die dem Client in der Antwort auf die ursprüngliche Anfrage zurückgeschickt wird.

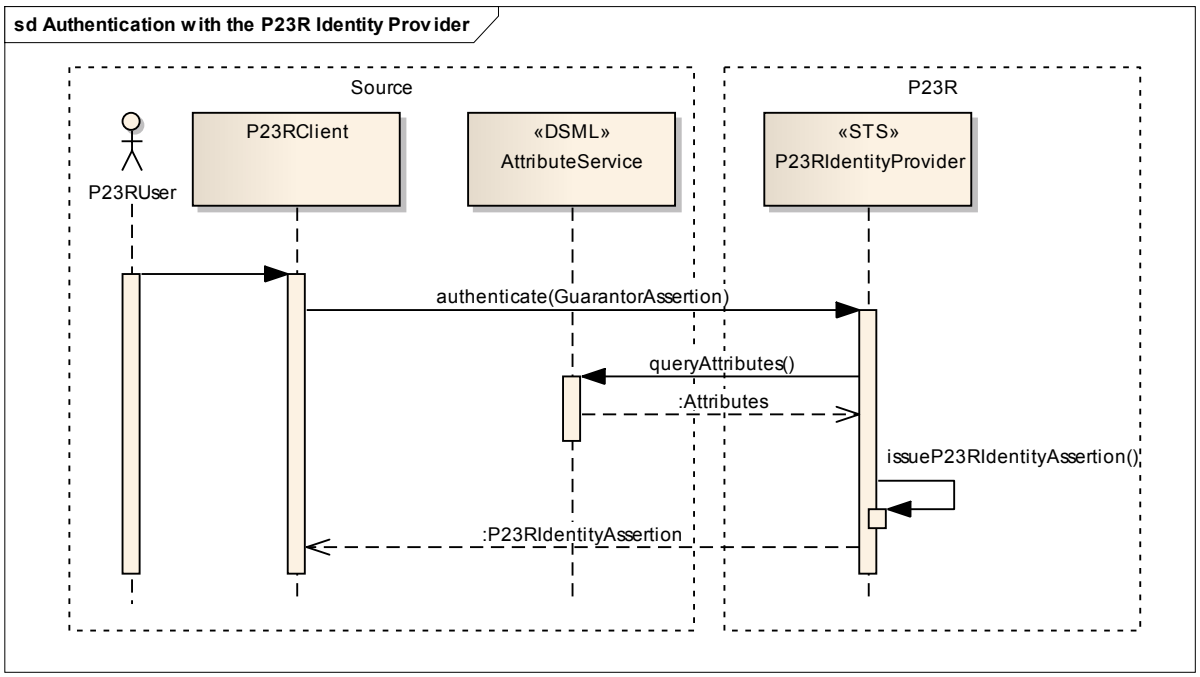


ABBILDUNG 10: AUTHENTISIERUNG AM P23R-IDENTITY-PROVIDER (UML)

- Mit dem erworbenen Authentisierungsnachweis in standardisierter und vereinheitlichter Form können die P23R-Dienste genutzt werden. Diese Dienste konsumieren eine P23R-Identity-Assertion, wobei für Nutzer mit gültigem Authentisierungsnachweis gleichzeitig der initiale Dienstzugang gewährt wird (Abbildung 11). Der Zugriff auf die vom Dienst verwalteten Ressourcen wird in einer gesonderten Autorisierungsprüfung gegen die in der P23R-Identity-Assertion kodierten Nutzerattribute verifiziert.

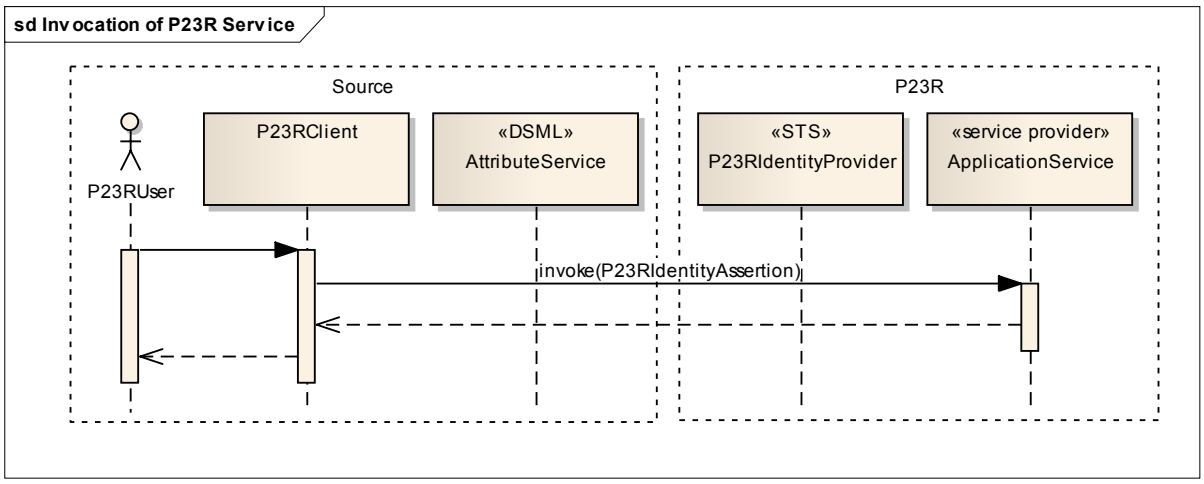


ABBILDUNG 11: NUTZUNG EINES P23R-DIENSTES MITTELS EINES AUTHENTISIERUNGSNACHWEISES (UML)

4.4 NUTZUNG VON WS-SECURITY POLICY (NICHT NORMATIV)

Der in Abschnitt 4.3.3 geschilderte Ablauf kann per WS-Policy [24] und WS-SecurityPolicy [25] deklarativ gesteuert werden (siehe auch Abschnitt 3.3). Dazu muss jeder in WSDL kodierten Dienstbeschreibung eine WS-Policy beigefügt werden. Diese beschreibt die lokalen Sicherheitsanforderungen, um den Dienst nutzen zu können. Wird von einem initialen Dienstaufruf ausgegangen, so lädt sich der Client das WSDL-Dokument mit der entsprechenden WS-Policy und überprüft die Sicherheitsanforderungen, die an die aufgerufene Operation gestellt werden. Darin wird bspw. festgelegt, dass ein Authentisierungs-Token (*Issued Token*) in Form einer SAML Assertion von einem vertrauten Identity Provider (in diesem Fall dem P23R-Identity-Provider) dem Dienstaufruf beigelegt werden muss. Neben weiteren Konfigurationen enthält diese Anweisung auch die URL des P23R-Identity-Providers. Anhand dieser URL kann der P23R-Client sich das WSDL-Dokument mit der entsprechenden WS-Policy des P23R-Identity-Providers herunterladen und auswerten. Die WS-Policy des P23R-Identity-Providers erlaubt für die in Abschnitt 4.3 spezifizierte Webservice-Schnittstelle die Authentisierung per Guarantor Assertion. Diese Sicherheitsanforderungen werden in der WS-Policy als *Issued Token* (SAML Assertion) kodiert. Der P23R-Client kann diese Anforderung abermals auswerten und somit – im Falle einer lokalen Authentisierung – an einen lokalen Authentisierungsdienst im Unternehmen weiterleiten. Werden alle Abhängigkeiten der beteiligten Dienste erfüllt, kann der eigentliche Dienstaufruf am P23R erfolgen.

Ein Beispiel für eine als WS-SecurityPolicy kodierte Dienst-Policy ist in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 7.5 in [5]) angegeben.

4.5 PORTAL VOUCHES: SCHNITTSTELLE UND ABLAUF (NICHT NORMATIV)

Die oben beschriebene NORMATIVE, zwingend umzusetzende Webservice-Schnittstelle zur Authentifizierung von Nutzern erlaubt eine direkte Anbindung des P23R an Systeme in Unternehmen und Verwaltung und damit eine Integration von P23R-Aufrufen in die Ablaufsteuerung von bestehenden Fachverfahren.

Insbesondere für kleine Unternehmen oder für Szenarien, in denen eine Anbindung des P23R an Fachverfahren für die Hersteller der entsprechenden Systeme nicht wirtschaftlich ist, MÜSSEN auch P23R-Konfigurationen unterstützt werden, bei denen die Authentifizierung des Nutzers über ein Web Portal realisiert ist. Diese optional zu realisierende Variante sieht vor, dass der P23R-Client als Web Portal für jeden authentifizierten Nutzer eine Guarantor Assertion ausstellt bzw. von einer Authentifizierungskomponente ausstellen lässt, sofern weitere, dem Portal nicht bekannte Attribute notwendig sind. Der P23R-Client bürgt demzufolge für die Authentifizierung eines Nutzers. Dieses Verfahren erfordert weitere Absicherungen, da der Besitznachweis der Guarantor Assertion (nach SAML Sender Vouches-Profil) gegenüber dem P23R-Identity-Provider nicht erbracht werden kann. Das Clientsystem MUSS daher eine durchgängig authentische und integritätsgesicherte Kommunikationsstrecke zwischen dem Desktop des Nutzers und dem P23R aufbauen. Dies kann z. B. über einen beidseitig authentifizierten TLS-Tunnel zwischen Desktop des Nutzers und Clientsystem (insb. Web Portal) erfolgen. In diesem Fall bürgt das Clientsystem gegenüber dem P23R-Identity-Provider für die durchgeführte Authentifizierung und die Authentizität des Nutzers bei allen P23R-Dienstaufrufen.

Eine mögliche Umsetzung der Anbindung eines P23R-Clientsystems an den P23R-Identity-Provider ist in Abbildung 12 am Beispiel eines Web Portal skizziert.

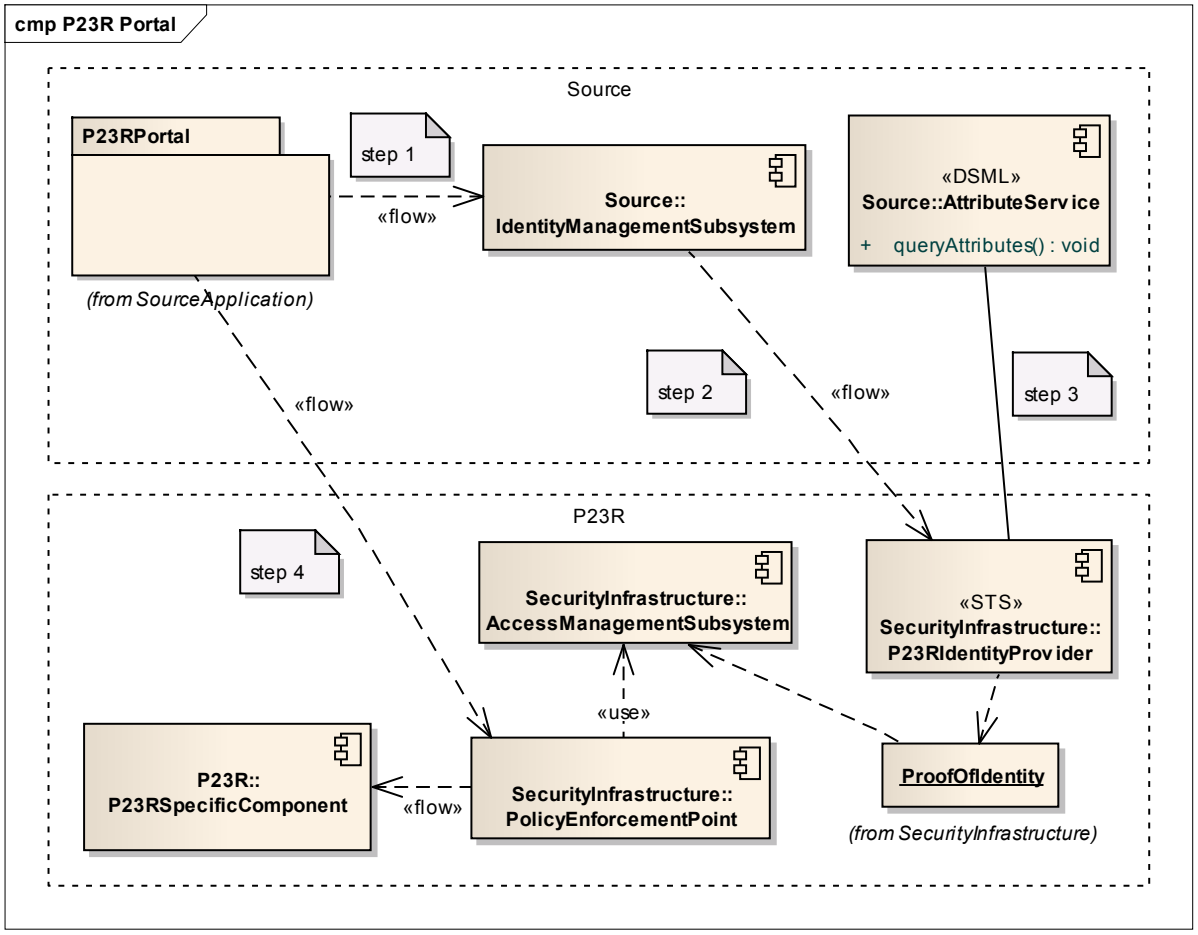


ABBILDUNG 12: P23R MIT ENG GEKOPPELTER CLIENT-KOMPONENTE (UML)

Bei der in der Abbildung dargestellten Kapselung des P23R über ein Web Portal meldet sich der Nutzer zunächst über einen in das Web Portal (P23R Portal) integrierten Authentifizierungsdienst an (step 1 bzw. Schritt 1). Grundsätzlich kann ein Web Portal hierzu einen beliebigen Mechanismus nutzen. Das Access Management Subsystem des P23R MUSS jedoch Authentisierungsnachweise ablehnen, die sich unterhalb eines im spezifischen Sicherheitskonzept des P23R-Betreibers festgeschriebenen Sicherheitsniveau bewegen.

Der Authentifizierungsdienst des Portals sendet die im Rahmen der Authentifizierung gesammelten Informationen an den P23R-Identity-Provider (Schritt 2), der diese Angaben in einer P23R-Identity-Assertion kapselt. Sofern erforderlich fragt der P23R-Identity-Provider bei einem Attribute Service des Unternehmens weitere Informationen zum Nutzer ab (Schritt 3). Die P23R-Identity-Assertion wird im Portal der Nutzer-Session zugeordnet und allen im Rahmen dieser Session ausgelösten Aufrufen von P23R-Diensten mitgegeben. Es folgt zudem die Berechtigungsprüfung in Folge von Zugriffen auf über Policy Enforcement Points abgesicherte Ressourcen (Schritt 4).

4.6 Anbindung eines OSCI-Gateways (NORMATIV)

Verwaltungen können Nachrichten über das OSCI Transport Protokoll an einen P23R senden. Hierzu kann dem P23R ein OSCI-Gateway vorgeschaltet werden, an dem das OSCI Transport Protokoll terminiert und das die im OSCI-Standard definierten Maßnahmen zur Ende-zu-Ende-Sicherheit unterstützt. Das P23R-Protokoll [1] definiert hierzu das OSCI Transport Protokoll als einen Mechanismus, um die Nutzlast einer Nachrichten zu sichern.

Technisch erfolgt die Anbindung des Gateways auf der Ebene der Sicherheitsarchitektur durch eine Kombination der in den Abschnitten 4.3 und 4.5 beschriebenen Verfahren:

- In der Kommunikation des OSCI-Gateways mit den P23R-Sicherheitsdiensten MUSS das in Abschnitt 4.5 beschriebene Verfahren gemäß Abbildung 12 umgesetzt werden, wobei das OSCI-Gateway die Rolle des Web Portals einnimmt. Hierbei entfällt lediglich Schritt 1 (Authentifizierung am Portal), da die Authentifizierung bereits in der Verwaltung erfolgt ist und ein entsprechender, authentifizierbarer Nachweis in Form einer OSCI-konformen Identity Assertion am OSCI-Gateway vorliegt.
- Für die Kommunikation mit dem P23R-Identity-Provider MUSS das in (siehe Abschnitt 2.4 in [5]) beschriebene Profil des WS Trust 1.3 RST/RSTR Protokolls genutzt werden. Hierbei wird der in der OSCI Transportnachricht übermittelte Identitätsnachweis als Guarantor Assertion gemäß Abschnitt 4.3 an den P23R-Identity-Provider übergeben.

Die Kommunikation zwischen der Verwaltung und dem OSCI-Gateway erfolgt über die im OSCI Transport 2.0 Standard beschriebenen Mechanismen. Für verwendete SAML 2.0 Identity Assertion MUSS hierbei die in (siehe Abschnitt 4.5 in[5]) festgeschriebenen Vorgaben umsetzen.

4.7 Authentifizierung bei internen Triggern (NORMATIV)

Aktionen des P23R können durch externe oder interne Ereignisse angestoßen werden. Bei einem externen Ereignis MUSS es immer einen auslösenden Nutzer geben, der über einen der oben beschriebenen Mechanismen authentifiziert wurde. Interne Ereignisse, wie z. B. die zeitgesteuerte Auslösung einer Benachrichtigungsgenerierung, werden vom P23R ausgelöst. Zwischen Auslösen des Ereignisses und Ausführen der Aktion ist häufig keine Nutzerinteraktion möglich oder gewünscht.

Interne Trigger laufen innerhalb des P23R mit der Autorisierung des Nutzers, der diesen Trigger registriert hat. Es werden also an die durch den Trigger ausgelösten internen Nachrichten Identitätsinformationen gebunden, die aus der Authentifizierung des Nutzers abgeleitet sind, der diesen Trigger am P23R registriert hat. Die oben beschriebenen Mechanismen beinhalten alle hierzu benötigten Informationen, so dass auch zeitgesteuerte Ereignisse mit einer P23R-Identity-Assertion verknüpft werden können, wodurch eine durchgängige Einheitlichkeit der Bereitstellung von Identitäten und Attributen hergestellt wird. Das Grundprinzip ist hierbei das gleiche wie bei dem Guarantor Assertion-Verfahren, nur dass hier die für die Registrierung des Triggers genutzte P23R-Identity-Assertion als Guarantor Assertion verwendet wird, aus der der P23R-Identity-Provider eine neue P23R-Identity-Assertion ableitet, die nur im Rahmen der Abarbeitung des Triggers genutzt werden kann.

4.7.1 Schnittstelle zum P23R-Identity-Provider

Die funktionale Beschreibung dieser Schnittstelle ist in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 2.2 in [5]) gesondert aufgeführt. Der Hersteller eines P23R kann diese funktionale Schnittstelle – ggf. auch mit eigenen Erweiterungen – auf die in seiner Implementierung gewählte Plattform übertragen. Wesentlich ist lediglich, dass die Durchgängigkeit von der initialen Authentifizierung bis zur Verwertung der Identitätsinformationen gewahrt ist.

4.7.2 Ablauf

Die folgende Ausführung geht vom dem Fall aus, dass eine lokale Authentisierung des Mitarbeiters im Unternehmen stattfindet. Der generierte Authentisierungsnachweis (Guarantor Assertion) wird für die Authentisierung am P23R eingesetzt. Der Ablauf ist in Abbildung 13 dargestellt, wobei die eigentliche Registrierung und Aktivierung einer Regel in der ScheduleTable über das Model And Rule Management (siehe Abschnitt 3.11 in [38]) geschieht und implementierungsspezifisch ist.

- Der P23R-Identity-Provider stellt auf Grundlage der Guarantor Assertion die P23R-Identity-Assertion aus und sendet sie an den P23R-Client zurück.
- Der P23R-Client registriert die Erzeugung einer Benachrichtigung am ScheduleManager und legt die P23R-Identity-Assertion als Authentisierungsnachweis vor.
- Der ScheduleManager ruft über eine interne Schnittstelle des P23R-Identity-Providers eine P23R-Trigger-Identity-Assertion auf Grundlage der vorliegenden P23R-Identity-Assertion ab.
- Mit der P23R-Trigger-Identity-Assertion wird der Trigger für die Benachrichtigungserzeugung generiert.

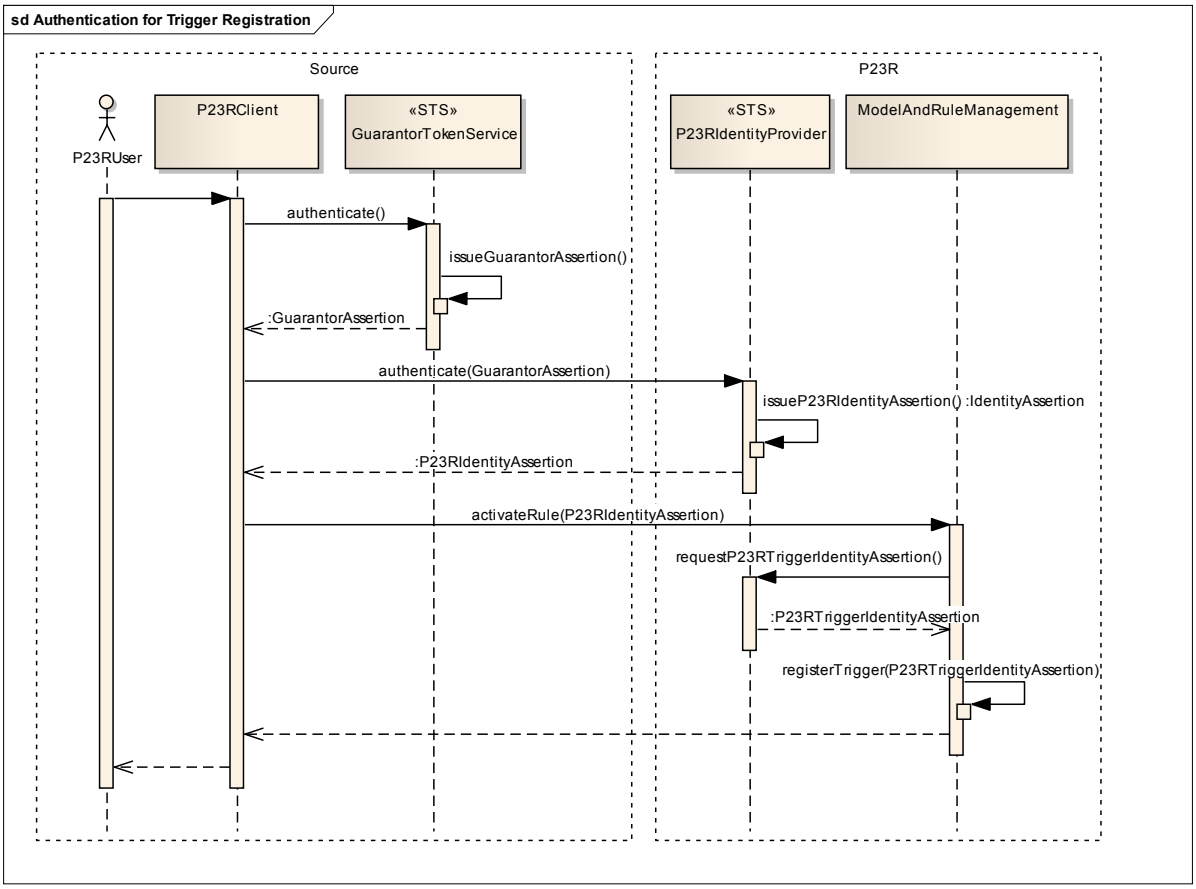


ABBILDUNG 13: AUTHENTISIERUNG BEI INTERNEN TRIGGERN (UML)

4.8 ABRUF VON NUTZERATTRIBUTEN (NORMATIV)

Zur Prüfung von Berechtigungen müssen dem Access Management Subsystem des P23R über die P23R-Identity-Assertion Angaben zur Organisationszugehörigkeit und ggf. auch zu den Rollen eines Nutzers verfügbar gemacht werden.[9]

4.8.1 ERMITTELN DER ORGANISATIONSZUGEHÖRIGKEIT EINES NUTZERS

Die Organisationszugehörigkeit kann vom P23R-Identity-Provider anhand verfügbarer Informationen ermittelt und als Attribut in die P23R-Identity-Assertion eingetragen werden:

- Sofern der P23R-Identity-Provider direkt (z. B. von einem dem P23R vorgeschalteten Web Portal) aufgerufen wird, MUSS die Organisationszuordnung als Parameter übergeben werden.
- Sofern der P23R-Identity-Provider über die WS-Trust-Schnittstelle mit einer Guarantor Assertion aufgerufen wird, prüft der P23R-Identity-Provider zunächst, ob Angaben zur Organisationszugehörigkeit in der Guarantor Assertion enthalten sind und von dort übernommen

[9] Rolleninformationen sind nur erforderlich, wenn der Zugang zu P23R-Diensten und -Daten über ein rollenbasiertes Berechtigungsmanagement abgesichert wird. Insbesondere für Kleinunternehmen ist jedoch auch eine Autorisierung von Einzelpersonen denkbar. In diesem Fall sind die in der P23R-Identity-Assertion enthaltenen Identitätsdaten (Nutzer und Organisation) ausreichend.

werden können. Ist dies nicht der Fall, übernimmt der P23R-Identity-Provider die Organisationsangabe des *Subject DN* des Signaturzertifikats, mit dem die Guarantor Assertion signiert wurde.

4.8.2 Anbindung an einen Attribute Service

Sofern Rolleninformationen nicht beim Aufruf des P23R-Identity-Providers – z. B. als Teil einer Guarantor Assertion – mitgegeben wurden, SOLL der P23R-Identity-Provider eine Anfrage an den Attribute Service der Organisation stellen, der der Nutzer zugeordnet ist. Hierzu verfährt der P23R-Identity-Provider wie folgt:

- Anhand der Organisationszuordnung des Nutzers ermittelt der P23R-Identity-Provider die TSL des Unternehmens bzw. der Verwaltung, der der Nutzer angehört (siehe Kapitel 7). Sofern die Organisation keine TSL am P23R registriert hat, wird eine P23R-Identity-Assertion ohne Rolleninformationen ausgestellt.
- Aus der TSL ermittelt der P23R-Identity-Provider die Adresse des Attribute Service des Unternehmens bzw. der Verwaltung. Sofern die Organisation keinen Attribute Service in der TSL registriert hat, wird eine P23R-Identity-Assertion ohne Rolleninformationen ausgestellt.
- Der P23R-Identity-Provider fragt beim Attribute Service die Rollenzuweisungen des identifizierten Nutzers ab (siehe Kapitel unten) und trägt diese in die P23R-Identity-Assertion ein.

Wie aus diesen Ausführungen zu ersehen ist, erfolgt die Konfiguration, ob ein externer Attribute Service abgefragt werden soll, über die TSL der Organisation, der der Nutzer angehört. Ist in der TSL ein Attribute Service vermerkt, so wird dieser nach Rolleninformationen zum Nutzer angefragt. Ist kein Attribute Service registriert, arbeitet der P23R einzig auf den über die Authentifizierung verfügbar gemachten Nutzerinformationen.

4.8.3 Attribute Service: Schnittstelle und Schema (NORMATIV)

Die Abbildung der funktionalen Schnittstellen auf DSML [39] ist in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 2.3 in [5]) gesondert beschrieben. Als Attribute Services können beliebige Verzeichnisdienste im Unternehmen angebunden werden, die

- eine NORMATIVE LDAP-Anfrage über DSMLv2 erlauben oder aber
- ein Personenschema gemäß RFC 2798 [40] verarbeiten können.

Der Verbindungsaufbau vom P23R-Identity-Provider zum Attribute Service MUSS über HTTPS erfolgen. Sofern eine gegenseitige Authentifizierung der Dienste verlangt wird, MÜSSEN die in den jeweiligen TSLs publizierten TLS-Zertifikate verwendet werden. Andere Zertifikate DÜRFEN NICHT akzeptiert werden.

5 AUTORISIERUNG UND BERECHTIGUNGSPRÜFUNG

Durch die Trennung von Authentifizierung und Autorisierung können standardisierte Verfahren und Technologien zur Prüfung einer Berechtigung eingesetzt werden. Abbildung 14 stellt eine Übertragung der Abläufe und Bausteine des XACML-Standards [26] auf den P23R dar. Eine Besonderheit ist dabei, dass die Flexibilität des Standards genutzt wird, um einzelne Bausteine – und damit auch die von diesen Bausteinen verwalteten Daten – alternativ in der Unternehmensinfrastruktur oder im P23R anzusiedeln.

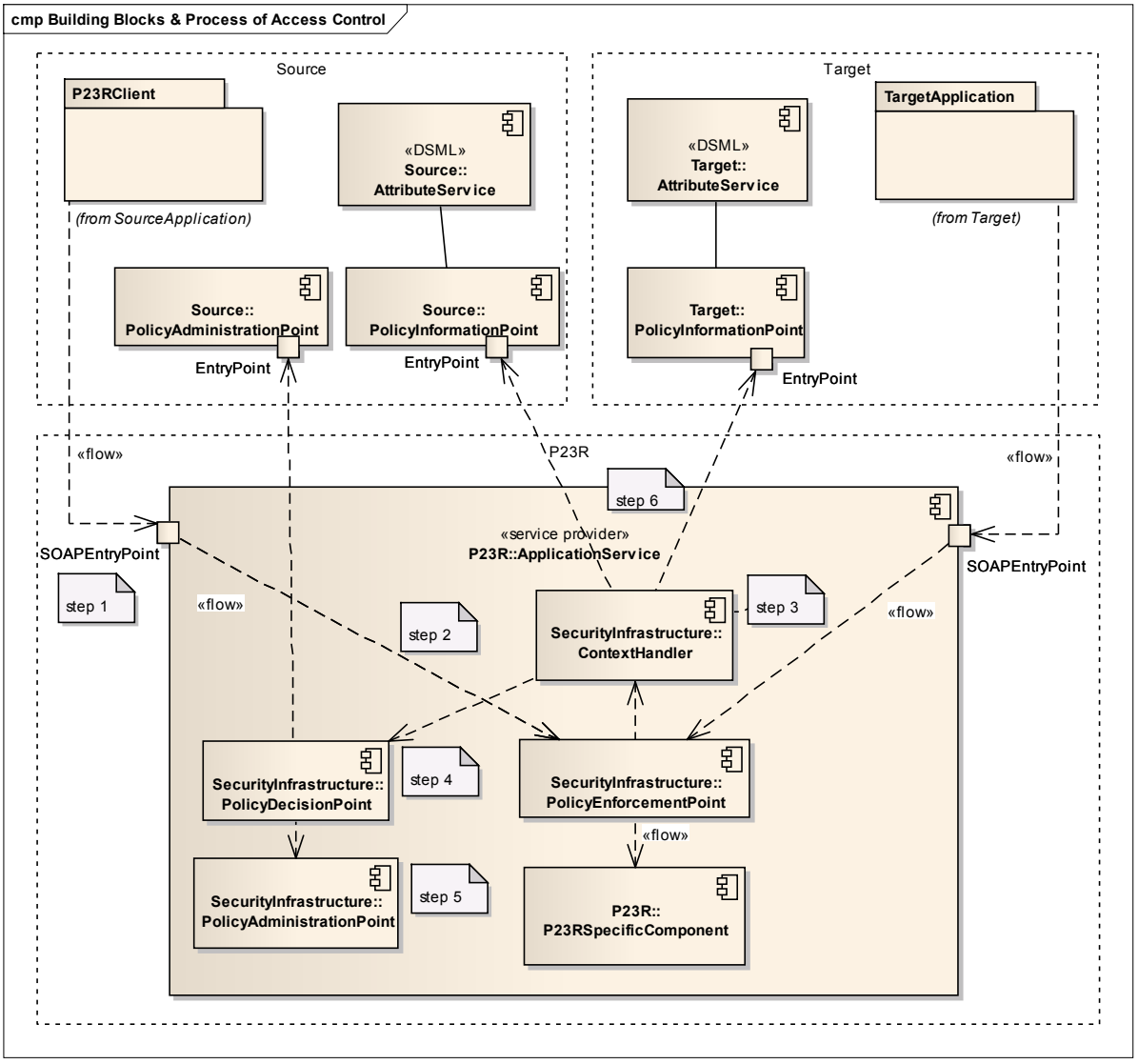


ABBILDUNG 14: BAUSTEINE UND ABLÄUFE DES AUTORISIERUNGSDIENSTES (UML)

Der Zugang zu Daten und Diensten des P23R erfolgt ausschließlich über dedizierte Zugangspunkte (step 1 bzw. Schritt 1). Hierbei muss ein vom P23R-internen Identity Provider ausgestellter Identitätsnachweis mitgeliefert werden (siehe Kapitel 4). Dieses geschieht durch Einbettung der entsprechenden P23R-Identity-Assertion in den administrativen Teil der Anfragenachricht (konkret: SOAP Security Header), mithin unsichtbar für die eigentliche Anwendungskommunikation zwischen Nutzer(-system) und P23R.

Jeder Zugang zu einem P23R-Dienst ist durch einen Policy Enforcement Point (PEP) abgesichert (Schritt 2). Der PEP ist eine logische Entität[10] der Sicherheitsarchitektur, die (logisch) in den Kontrollfluss eines Ressourcen- bzw. Dienstzugangs eingebettet ist und das Ergebnis einer Berechtigungsprüfung (Berechtigungsentscheidung) durchsetzt (Reference Monitor Pattern) (Schritt 3). Die Steuerung der Berechtigungsprüfung liegt bei einem sogenannten Context Handler, der die Berechtigungsprüfung durch einen Policy Decision Point (PDP) anstößt (Schritt 4). Der Policy Decision Point identifiziert die für den Dienstaufruf gültigen Berechtigungsregeln. Hierzu greift er auf Policy Administration Points (PAP) zu, die sowohl im P23R als auch außerhalb des P23R im Unternehmen angesiedelt sein können (Schritt 5). Durch Anbindung eines eigenen PAP kann ein Unternehmen die seine Mitarbeiter und Daten betreffenden Regeln über seine internen Systeme pflegen und dem P23R zur Verfügung stellen.

Sofern zur Auswertung einer Berechtigungsregel über die im P23R verfügbaren Daten zusätzliche Informationen über den Nutzer oder die zu schützende Ressource benötigt werden, kommuniziert der Context Handler mit einem oder mehreren Policy Information Points (PIP), die die geforderten Informationen bereitstellen (Schritt 6). Die Auswertung der Berechtigungsregeln gegen die Attribute des Nutzers und der zu schützenden Ressource durch den Policy Decision Point (PDP) liefert ein *permit* (Nutzer ist zum Zugriff auf die Ressource bzw. den Dienst berechtigt) oder ein *deny* (Nutzer ist nicht berechtigt). Im Fall eines *permit* gibt der PEP den Zugang zu dem Dienst bzw. der Ressource frei, andernfalls wird der Zugriffsversuch auf die geschützte Ressource bzw. den geschützten Dienst mit einer Fehlermeldung abgebrochen. Die zwei weiteren Ergebnistypen *not applicable* und *indeterminate* von einem PDP werden durch den PEP als *deny* interpretiert („deny-based PEP“).

Dadurch dass Policy Administration Points und Policy Information Points sowohl innerhalb des P23R als auch in der Unternehmensinfrastruktur angesiedelt sein können, kann beim Aufsetzen eines P23R sehr flexibel auf die vorhandenen Systeme und Abläufe reagiert werden. Falls z. B. ein Unternehmen bereits ein Produkt zum Identitäts- und Berechtigungsmanagement einsetzt, kann dieses als im Unternehmen befindlicher PAP an den P23R angebunden werden. Rollen und Rechte müssen somit nicht mehrfach verwaltet werden, sondern werden weiterhin über die bestehenden Systeme und Abläufe gepflegt. Auch eine in ein Fachverfahren integrierte „P23R-Inside“ Lösung kann analog umgesetzt werden, wobei hier Nutzerattribute und Berechtigungsregeln nicht aus zentralen Systemen, sondern über das Fachverfahren (vermittelt) an den P23R übergegeben werden. Ein Unternehmen, das aktuell Meldungen außerhalb bestehender Fachverfahren vorwiegend manuell erstellt, wird hingegen einen P23R potenziell eher als Stand-Alone-Lösung einsetzen und Nutzerprofile sowie Berechtigungen über einen P23R-Client innerhalb des P23R pflegen wollen (insbesondere in Szenarien, in

[10] Siehe Definition eines Policy Enforcement Point als „logical entity“ in RFC 3198. In der Definition eines PEP im XACML-Standard wird abweichend der Begriff „system entity“ verwendet. In XACML-Frameworks (z. B. SUN’s XACML) ist der PEP eine anwendungsspezifische Funktionalität, die die aus dem Kontext eines Aufrufs heraus verfügbaren Informationen in normierter Form packt und an die Berechtigungsprüfung weiterleitet. Für dieses Dokument wird der PEP als der Punkt angesehen, an dem aus einem Kontrollfluss der Anwendungsarchitektur heraus Funktionen des Autorisierungs-Subsystems angesprungen werden. Der Kontrollfluss der Anwendungsarchitektur wird nur bei einer positiven Berechtigungsentscheidung fortgesetzt. In den UML-Modellen wird dieser Punkt als Komponente dargestellt, um den Übergang zwischen Anwendungs- und Sicherheitsarchitektur an einen Modell-Baustein knüpfen zu können.

denen z. B. nur der Geschäftsführer oder wenige Verwaltungsmitarbeiter des Unternehmens mit dem P23R arbeiten, ist dies sicherlich auch unabhängig von den bestehenden Abläufen eine pragmatische Verfahrensweise). In diesem Fall wird ein PAP innerhalb des P23R genutzt. Denkbar sind jedoch auch Mischlösungen, in denen z. B. die Rechte von für den P23R-Betrieb verantwortlichen Personen von der IT-Abteilung des Unternehmens im P23R gepflegt werden, während die auch für Fachverfahren in den Geschäftsabläufen geltenden Berechtigungen von Mitarbeitern aus den Geschäftsbereichen zentral im Unternehmen verwaltet werden.

5.1 Absicherung des Datenpools

Abbildung 15 stellt die in Abschnitt 2.2.2 beschriebenen Einzelmaßnahmen zur Absicherung des Datenpools und der generierten Benachrichtigungen im Überblick dar.

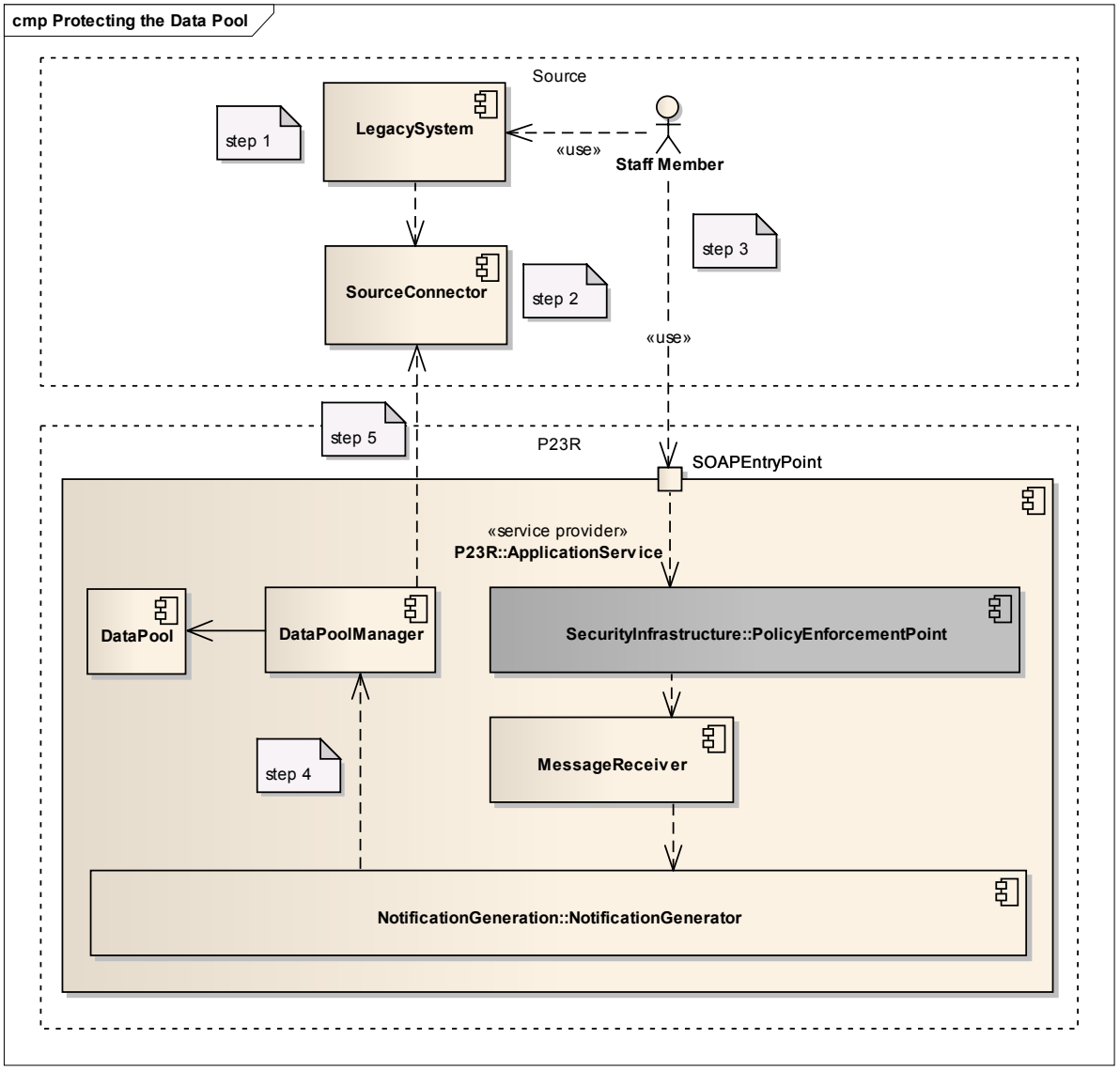


ABBILDUNG 15: ABSICHERUNG DES DATENPOOLS (UML)

Wie aus der Abbildung zu ersehen, schlagen sich die Maßnahmen in stark regulierten Kontroll- und Datenflüssen nieder:

- Innerhalb des Berechtigungskontexts des Unternehmens wird der Export von Daten aus dem Bestandssystem (engl. Legacy System) freigegeben (step 1 bzw. Schritt 1). Die Daten werden im vom P23R vorgegebenen Schema in den SourceConnector exportiert (Schritt 2), welcher eine Transferdatenbank – z. B. zur Anpassung des Datenmodells an das Pivot-Datenmodell – implementieren kann.
- Ein im Unternehmen authentifizierter Mitarbeiter (engl. Staff Member) löst über einen P23R Zugangspunkt (engl. SOAP Entry Point) die Benachrichtigungsgenerierung aus (Schritt 3). Hierzu wird als erster Dienst der MessageReceiver angesprungen, der die Benachrichtigungsgenerierung über den NotificationGenerator anstößt. Der MessageReceiver ist über einen Policy Enforcement Point abgesichert, wodurch sichergestellt ist, dass der Mitarbeiter berechtigt ist, die Generierung der angeforderten Benachrichtigung auszulösen (Schritt 3).
- Der NotificationGenerator liest die für die Generierung benötigten Daten aus dem DataPool (Datenpool) über den entsprechenden Manager (Schritt 4). Sollten die benötigten Daten nicht vorhanden oder nicht mehr aktuell sein, werden die Daten über den SourceDataConnector (Konnektor für Quelldaten) ausgelesen (Schritt 5).

Die Abbildung zeigt die Absicherung des Datenpools für die manuelle Erzeugung einer Benachrichtigung über den MessageReceiver. Die zeitgesteuerte Erzeugung geschieht über das Model and Rule-Management (MARM). Auch hier wird die Aktivierung einer BR analog zum MessageReceiver über einen Policy Enforcement Point abgesichert.

5.2 Kodierung von Access Policies

Access Policies SOLLEN in XACML 2.0 [26] kodiert sein.[11] Die Vorgaben in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 3.1 in [5]) zur Umsetzung von „Fail-Safe Defaults“ (siehe Abschnitt 3.2) MÜSSEN bei der Kodierung von XACML Policies berücksichtigt werden.

XACML Policies sind hierarchisch aufgebaut:

- Eine Policy besteht aus
  - einer oder mehreren Regeln (*Rules*),
  - einem Rule-Combining-Algorithmus, der festlegt, wie vorzugehen ist, wenn die Regeln der Policy zu unterschiedlichen Berechtigungsentscheidungen kommen. Für den P23R MUSS immer festgelegt sein, dass eine Policy den Zugriff auf eine Ressource oder die Ausführung einer Aktion untersagt, sobald eine der enthaltenen Regeln die gewünschte Aktion als unzulässig bewertet.

[11] Andere Policy-Sprachen KÖNNEN von einer P23R-Implementierung eingesetzt werden, dieses DARF aber NICHT zu Änderungen an den NORMATIVEN Schnittstellen zum Abruf von Policies und Policy-Informationen führen (siehe Abschnitte 5.4 und 5.5). Die Ausführungen in diesem Kapitel beziehen sich ausschließlich auf XACML-kodierte Policies.

- einem Gegenstand der Policy (*Target*), in dem beschrieben ist, was der Aufhänger der Policy ist. Zum Beispiel kann eine Policy die Rechte eines Subjekts oder die Zugriffsregeln auf eine Ressource definieren.
- beliebig vielen Nachbedingungen (*Obligations*). Zu jeder Nachbedingung ist vermerkt, ob sie relevant für den Fall einer positiven oder negativen Zugriffsentscheidung ist. Relevante Nachbedingungen werden an den PEP zurückgespielt, der die in der Nachbedingung benannte Aktion (z. B. Schreiben eines Protokolleintrags) ausführen SOLL.

- Eine Regel definiert, unter welchen Umgebungsbedingungen ein bestimmtes Subjekt (Nutzer) eine bestimmte Aktion auf einer bestimmten Ressource ausführen darf. Subjekte und Ressourcen werden über Attribute beschrieben. Über ein Attribut (*effect*) ist definiert, ob ein Zutreffen der Regel eine positive (*permit*) oder negative (*deny*) Zugriffsentscheidung bedeutet.
- Policies können zu *PolicySets* zusammengefasst werden.

5.2.1 Festlegen von Policies

Die Verantwortung für die Kodierung der P23R-Policies liegt bei den Unternehmen, aus deren Daten heraus Benachrichtigungen generiert werden. Das heißt, jedes Unternehmen legt über Policies fest, welche Rechte seine Mitarbeiter auf den das Unternehmen betreffenden Ressourcen (Benachrichtigungsregeln, Benachrichtigungen etc.) haben. Prinzipiell bieten sich zwei Möglichkeiten zur Definition von Policies an:

- Eine Policy fasst Regeln zusammen, die festlegen, welche Aktionen bestimmte Mitarbeiterrollen ausführen dürfen. Es gibt somit (mindestens) eine Regel pro Mitarbeiterrolle. Dieses Vorgehen wird empfohlen, wenn die Berechtigungsregeln unabhängig von der konkreten Benachrichtigung sind (z. B. jeder Verwaltungsmitarbeiter darf die Generierung einer Benachrichtigung auslösen und der Geschäftsführer darf jede Benachrichtigung freigeben).
- Eine Policy fasst Regeln zusammen, die festlegen, welche Zugriffsbeschränkungen für welche Ressourcen gelten. Es gibt somit (mindestens) eine Regel pro Nachrichtentyp. Dieses Vorgehen wird empfohlen, wenn für die einzelnen Arten von Nachrichten (Personenmeldungen, Umweltmeldungen etc.) unterschiedliche Rollenrechte gelten sollen.

5.2.2 Benachrichtigungs-Policies

Zusätzlich KANN für jeden Benachrichtigungstyp eine Policy definiert werden, die den Lebenszyklus der Benachrichtigung steuert, d. h. in der definiert ist, welche Bedingungen erfüllt sein müssen, damit der nächste Bearbeitungsschritt eingeleitet werden kann. Beispielsweise kann über eine solche Policy definiert werden, dass eine Benachrichtigung von zwei Personen signiert sein muss, bevor sie an eine Verwaltung übermittelt werden darf.

Sofern es gesetzliche Vorgaben zum Generierungs-, Freigabe- und Übermittlungsprozess einer Benachrichtigung gibt, MÜSSEN diese in Form einer Policy von der Öffentlichen Leitstelle zusammen mit dem Benachrichtigungsregelpaket (BRP) verteilt werden. Eine solche Policy MUSS im PAP des P23R registriert werden und MUSS bei jedem Bearbeitungsschritt ausgeführt werden.

5.2.3 Subjekte und Ressourcen

Zu kodierende Subjekte bzw. Subjektattribute in den Access Policies müssen konform zu den Vorgaben zur P23R-Identity-Assertion sein. Nur so stehen zur Laufzeit alle notwendigen Identitätsinformationen zur Verfügung, die für die Berechtigungsprüfung erforderlich sind.

Für den P23R sind zunächst über *Resource*-Attribute die folgenden Ressourcen aus der Rahmenarchitektur [1] definiert, über die Access Policies definiert werden können:

- Benachrichtigung (*Notification*)
- Benachrichtigungsprofil (*NotificationProfile*)

Diese Attribute werden standardmäßig auf *urn:oasis:names:tc:xacml:1.0:resource:resource-id* abgebildet und sind in den Policies entsprechend zu berücksichtigen.

Die konkrete technische Spezifikation der *Resource*-Attribute für Benachrichtigungs-Policies ist in den Nutzungsvorgaben zu XACML in der technischen Spezifikationen zur Sicherheitsarchitektur(siehe Abschnitt 3.2 in [5]) enthalten. Die folgenden internen Ressourcen des P23Rs können somit ebenfalls über Policies geschützt werden:

- Benachrichtigungsregel *(NotificationRule*)
- Benachrichtigungsregelgruppe (*NotificationRuleGroup*)
- Benachrichtigungsregelpaket (*NotificationRulePackage*)
- Benachrichtigungsregelvariante (*NotificationRuleVariant*)
- Nachricht (*Message*) als Teil einer BR

5.2.4 Aktionen

Auszuführende Aktionen auf den Ressourcen spiegeln sich in den Dienstschnittstellen der Rahmenarchitektur wider. Die darin definierten Operationen werden im XACML-Kontext als Aktion behandelt, so dass diese standardmäßig auf *urn:oasis:names:tc:xacml:1.0:action:action-id* abgebildet werden.

5.3 Einbettung der Policy Enforcement Points

In der nachfolgenden Tabelle 1 und Tabelle 2 ist angegeben, welche der in der P23R-Rahmenarchitektur definierten Operationen auf welchen P23R-Diensten über Policy Enforcement Points abgesichert werden SOLLEN. Die Berechtigungsprüfung MUSS vor Ausführung der Operation erfolgen, d. h. direkt als erste Aktion nach dem Operationsaufruf. Zu jeder Operation ist angegeben, über welche Ressource und Aktion eine entsprechende Policy definiert sein SOLL, um Zugriffsbeschränkungen durchzusetzen.

TABELLE 1: AUFRUFBARE AKTIONEN AM P23R AUS DER SOURCE APPLICATION

P23R-Dienst	Aktion	Ressource
IRuleActivate	updateNotificationRulePackages	NotificationRulePackage
IRuleActivate	getNotificationRulePackageStates	NotificationRulePackage
IRuleActivate	isUpToDate	NotificationRule
IRuleActivate	setNotificationRulePackageStates	NotificationRulePackage
IMessageDeliverLocal	deliverMessage	Message
IExtMessageDeliverTest	deliverMessage	Message
IMessageDeliverScheduled	deliverMessage	Message
IProtocolQuery	queryProtocol	ProtocolEntry
INotificationApprove	getNotification	Notification
INotificationApprove	getMessage	Notification
INotificationApprove	approveNotification	Notification
IImportExportTransfer	activate	*P23R-Instanz*
IImportExportTransfer	block	*P23R-Instanz*
IImportExportTransfer	create	*P23R-Instanz*
IImportExportTransfer	deactivate	*P23R-Instanz*
IImportExportTransfer	export	*P23R-Inhalte*
IImportExportTransfer	Import	*P23R-Inhalte*

TABELLE 2: AUFRUFBARE AKTIONEN AM P23R AUS DER TARGET APPLICATION

P23R-Dienst	Aktion	Ressource
IMessageDeliverExternal	deliverMessage	Message

Ein P23R-Dienst ist immer durch seinen Namen sowie den Port, welche jeweils mit einem gemeinsamen Namensraum (TargetNamespace) versehen sind, beschrieben.

PEPs KÖNNEN an weitere interne, hier nicht aufgeführte Schnittstellen gebunden werden. Wenn Erweiterungen für interne Zugriffspunkte notwendig sind, dann MÜSSEN weitere PEPs gemäß den Vorgaben der Schutzbedarfsfeststellung des Sicherheitskonzepts [3] definiert werden.

5.4 Abfrage von Access Policies

Das Datenhaltungssystem für Access Policies ist das Policy Repository. Die Access Policies werden über die an das Policy Repository angeschlossene PAP-Komponente erstellt und verwaltet.[12] Wird ein PAP nicht gemäß des in XACML definierten Ablaufs (siehe Abschnitt 5.4.2 und (Abschnitt 3.3 in [5])) aus einem standardisierten PDP heraus angesprochen, so MUSS die Abfrage der Access Policies aus einem P23R-externen PAP über eine alternatives, vom P23R-Anbieter offen zu legendes Protokoll möglich sein.

Funktional wird eine Policy-Abfrage durch Kontextattribute begleitet. Diese können z. B. das Subjekt, die Ressource oder die auszuführende Aktion sein. Die Kontextattribute sind in Tabelle 3 aufgelistet.

[12] Im weiteren Verlauf wird nur noch von einem PAP gesprochen, welcher ein Policy Repository subsumiert.

TABELLE 3: KONTEXTATTRIBUTE EINER POLICY-ABFRAGE

Parameter	Beschreibung
Subject	Das Subjekt, welches auf eine Ressource eines P23R-Dienstes zugreifen möchte. Es korrespondiert mit dem Subjekt, welches in einer P23R-Identity-Assertion festgelegt wurde, bzw. wird direkt übernommen (SubjectDN).
Resource	Eine Ressource identifiziert bestimmte Objekte, auf welche zugegriffen werden soll.
Action	Legt die gewünschte Operation fest, welche auf der Ressource ausgeführt werden soll.

5.4.1 SCHNITTSTELLE ZUM POLICY ADMINISTRATION POINT

Die Abbildung der Schnittstellen auf das XACML Policy Query Profile ist in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 3.3 in [5]) gesondert beschrieben.

5.4.2 ABLAUF

Die folgenden Ausführungen (vgl. Abbildung 16) gehen von dem Fall aus, dass Access Policies von einem PAP im Unternehmen verwaltet werden und dass diese zur Laufzeit vom PDP abgerufen werden sollen. Der PDP sendet per SAML-Protokoll eine *XACMLPolicyQuery* an den in der TSL konfigurierten PAP des Unternehmens. In einer Antwortnachricht können eine oder mehrere Policies enthalten sein.

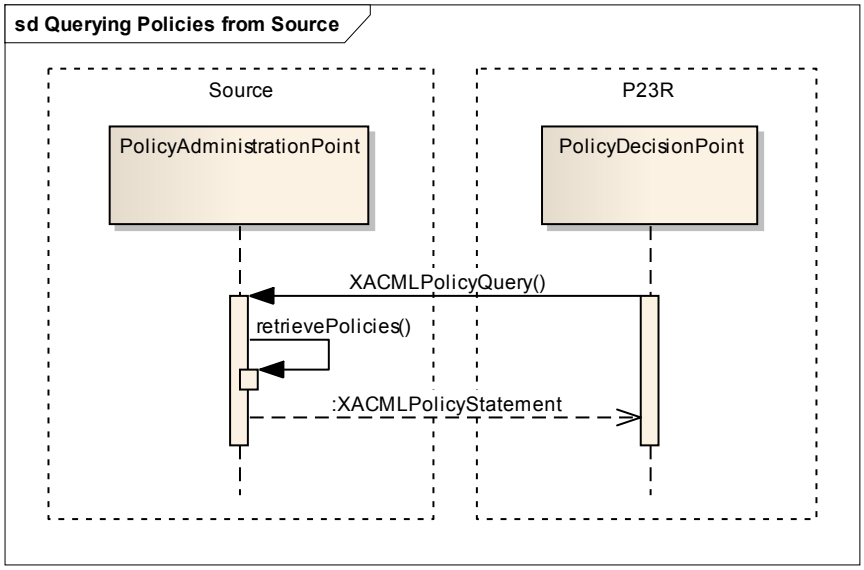


ABBILDUNG 16: ABRUF EINER ODER MEHRERER ACCESS POLICIES VOM UNTERNEHMEN (UML)

5.5 ABFRAGE VON POLICY-INFORMATIONEN

Zur Evaluierung einer Autorisierungsentscheidung können weitere Attribute erforderlich sein. Policy Information Points in einem Unternehmen oder einer Verwaltung können diese Attribute in Verzeichnisdiensten bereitstellen. Die Sicherheitsarchitektur des P23R legt zwei Möglichkeiten eines standardisierten Abrufs von Policy-Informationen oder weiteren Attributen fest:

- Directory Services Markup Language (DSML v2) über SOAP (NORMATIV)
- SAML Attribute Query (NICHT NORMATIV).

DSML-basierte Anfragen an Verzeichnisdienste wurden bereits bei der Ausstellung der P23R-Identity-Assertion durch den P23R-Identity-Provider spezifiziert, um Nutzerattribute z. B. aus dem Unterneh-

men abzurufen. Derselbe Mechanismus wird auch für die Aufbereitung des Autorisierungskontextes verwendet (siehe Abschnitte 5.5.1 und 4.7). Liefert der PDP als Ergebnis einer Autorisierungsanfrage die Meldung zurück, dass weitere Attribute für die Policy-Evaluierung fehlen [26, Abschnitt 6.16], so werden die erforderlichen Attribute über die registrierten Policy Information Points angefragt. Die Schnittstelle eines Policy Information Points KANN auch das SAML-Protokoll mit der HTTP-Bindung unterstützen (siehe Abschnitt 3.2.3 in [5]). In (Abschnitt 3.3.2.3 in [5]) wird festgelegt, wie Attributanfragen definiert sein können. Spezifische Vorgaben werden hierbei nicht gemacht.

5.5.1 SCHNITTSTELLE ZUM POLICY INFORMATION POINT

Neben der NORMATIVEN DSML-Schnittstelle wird auch die SAML-Schnittstelle gesondert in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 3.4 in [5]) spezifiziert.

5.5.2 ABLAUF

Die folgenden Ausführungen (vgl. Abbildung 17) gehen davon aus, dass zur Auswertung einer Access Policy erforderliche Attributwerte nicht über die P23R-Identity-Assertion verfügbar sind und daher zur Laufzeit von einem PIP im Unternehmen (oder einer Verwaltung) abgerufen werden sollen.

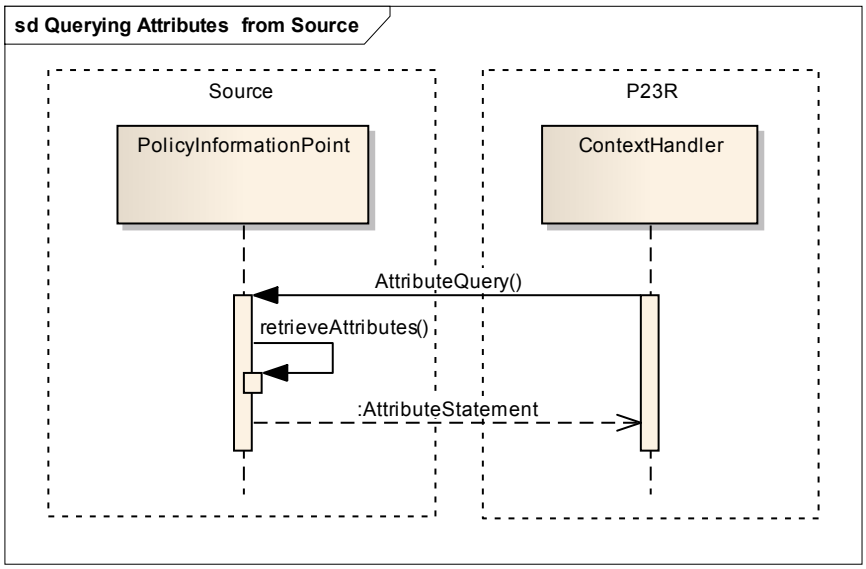


ABBILDUNG 17: ABRUF WEITERER ATTRIBUTE PER SAML-PROTOKOLL (UML)

Hierbei erstellt die Autorisierungskomponente Context Handler eine Attribut Anfrage und sendet diese an einen PIP im Unternehmen, welches die erforderlichen Attribute für die Autorisierungsentscheidung über ein Attribute Statement zur Verfügung stellen kann. Je nach Bedarf können Attribute vor der Evaluierung einer Autorisierungsentscheidung oder nach einer fehlgeschlagenen Evaluierung aufgrund fehlender Attribute abgerufen werden. Im letzteren Fall wird nach der Attributabfrage erneut eine Autorisierungsentscheidung mit den fehlenden Attributen evaluiert.

6 SICHERUNG VON DATEN UND NACHRICHTEN

Die Identity- und Access Management Subsysteme der P23R-Sicherheitsarchitektur stellen die Vertraulichkeit und Integrität von Daten innerhalb des P23R sicher. Die hier definierten Maßnahmen greifen jedoch nur bedingt auch für die Außenkommunikation des P23R mit Unternehmen, Verwaltungen und der Öffentlichen Leitstelle.

In diesem Kapitel sind die technischen Sicherheitsmaßnahmen beschrieben, über die die Außenkommunikation des P23R und die über Außenschnittstellen ausgetauschten Daten in ihrer Integrität, Authentizität und ggf. auch Vertraulichkeit gesichert werden. Diese technischen Maßnahmen werden durch im P23R-Sicherheitskonzept [3] beschriebene organisatorische Sicherheitsmaßnahmen ergänzt und unterfüttert. .

6.1 KOMMUNIKATION P23R – ÖFFENTLICHE LEITSTELLE

Gemäß den Anforderungen an das P23R-Prinzip [8] MUSS ein P23R Daten, wie z. B. Benachrichtigungsregelpakete, anonym von der Leitstelle abrufen können. Da eine vollständige Anonymität alleine schon aufgrund der auf den unteren Kommunikationsebenen offenbarten Verbindungsparameter (z. B. IP-Adresse des P23R) nicht mit vertretbarem Aufwand herstellbar ist, zielen die in diesem Abschnitt beschriebenen Maßnahmen ausschließlich darauf ab, eine Zuordnung von Personen / Organisationen zu Kommunikationsinhalten verschleiern zu können. Im Wesentlichen soll verhindert werden, dass identifizierende Daten eines Aufrufers oberhalb der Transportschicht sichtbar sind und dass unberechtigte Dritte durch Abhören von Kommunikationsleitungen Rückschlüsse auf den Inhalt einer Kommunikation zwischen einem P23R und einer Öffentlichen Leitstelle ziehen können.

Zur Sicherung einer von einem Unternehmen über einen P23R initiierten Kommunikation mit der Öffentlichen Leitstelle MÜSSEN die folgenden Vorgaben umgesetzt werden:

- Der P23R MUSS in der Lage sein, eine gesicherte (verschlüsselte) Verbindung zu der Öffentlichen Leitstelle aufzubauen. Der Aufbau der Transportverbindung MUSS eine Authentifizierung der Öffentlichen Leitstelle einschließen (TLS Server Authentication).
- Die Öffentliche Leitstelle MUSS sich beim Verbindungsaufbau über ein Zertifikat authentifizieren, das dem Zertifikatsprofil „Service Provider Node Authenticity“ gemäß der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Kapitel 6 in [5]) entspricht.
- Eine Öffentliche Leitstelle KANN eine TLS Mutual Authentication verlangen. In diesem Fall SOLL sich der P23R beim Verbindungsaufbau über ein Zertifikat authentifizieren, das dem Zertifikatsprofil „Service Consumer Node Authenticity“ gemäß der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Kapitel 6 in [5]) entspricht.

Die Rahmenarchitektur des P23R sieht keine von der Öffentlichen Leitstelle initiierten Kommunikationen zu einem P23R vor. Eine Leitstelle KANN ihren Kunden jedoch individuelle Kommunikationsdienste – z. B. zur Benachrichtigung über neue oder geänderte Benachrichtigungsregelpakete – anbieten. Die Sicherung dieser Kommunikation unterliegt einem spezifischen Sicherheitskonzept der Leitstelle und ist nicht Betrachtungsgegenstand dieser Spezifikation.

6.2 KOMMUNIKATION P23R – VERWALTUNG

Die Sicherung der Kommunikation zwischen einem P23R und einer Verwaltung MUSS unabhängig vom Initiator des Verbindungsaufbaus die folgenden Maßnahmen umfassen:

- Der Initiator des Verbindungsaufbaus MUSS in der Lage sein, eine gesicherte (verschlüsselte) Transportverbindung zum Endpunkt der Verbindung aufzubauen. Der Aufbau der Transportverbindung MUSS eine Authentifizierung des Endpunkts einschließen (TLS Server Authentication).
- Der Endpunkt der Verbindung MUSS sich beim Verbindungsaufbau über ein Zertifikat authentifizieren, das dem Zertifikatsprofil „Service Provider Node Authenticity“ gemäß der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Kapitel 6 in[5]) entspricht.
- Der Endpunkt KANN eine TLS Mutual Authentication verlangen. In diesem Fall SOLL sich der Initiator des Verbindungsaufbaus über ein Zertifikat authentifizieren, das dem Zertifikatsprofil „Service Consumer Node Authenticity“ gemäß der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Kapitel 6 in [5]) entspricht.

Die beschriebenen Maßnahmen stellen eine Vertraulichkeit der Kommunikation zwischen P23R und Verwaltung sowie die Authentizität der kommunizierenden Systeme sicher. Die Vertraulichkeit, Integrität und Authentizität der ausgetauschten Daten (Benachrichtigungen bzw. Nachrichten) wird auf der Anwendungsebene und in Abhängigkeit vom verwendeten Kommunikationsprotokoll (z. B. SOAP oder E-Mail) gesichert (siehe Abschnitt 6.4).

6.3 INTEGRITÄT UND AUTHENTIZITÄT VON BENACHRICHTIGUNGSREGELN

Regeln zur Generierung von Benachrichtigungen müssen gesetzliche Vorgaben inhaltlich-semantisch richtig abbilden. Formalisierungen von gesetzlichen Vorgaben müssen inhaltlich-syntaktisch richtig auf die T-BRS des P23R abgebildet werden.

Zur Sicherung der Integrität und Authentizität von Benachrichtigungsregelwerken MÜSSEN von Öffentlicher Leitstelle und P23R die folgenden Vorgaben umgesetzt werden:

- Der Abruf und der Empfang von Benachrichtigungsregelwerken MÜSSEN auf Seite des P23R protokolliert werden. Aus den Protokolldaten MUSS ersichtlich sein, welche Person wann welche Benachrichtigungsregelpakete von welcher Leitstelle abgerufen hat. Die Integrität der Protokolldaten MUSS mit im spezifischen Sicherheitskonzept eines P23R zu definierenden Maßnahmen sichergestellt werden.
- Von der Öffentlichen Leitstelle zum Abruf bereitgestellte oder übermittelte Paketlisten mit enthaltenen Benachrichtigungsregelwerken MÜSSEN von der Öffentlichen Leitstelle digital signiert werden. Hierzu MUSS eine „Detached Signature“ gemäß [42] verwendet werden. Das zugrunde liegende Signaturzertifikat MUSS den Vorgaben des Zertifikatprofils in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Kapitel 6 in [5]) entsprechen. Ein P23R MUSS die Integrität der Daten sowie die Gültigkeit und Authentizität des zur Signatur gehörigen Zertifikats prüfen. Ein P23R DARF Benachrichtigungsregelwerke aus Paketlisten, deren

Signaturprüfung nicht erfolgreich war, NICHT in den Benachrichtigungsregelpool übernehmen.

6.4 Integrität, Authentizität und Vertraulichkeit von Benachrichtigungen

Von einem P23R an eine Verwaltung übermittelte Benachrichtigungen MÜSSEN von einem berechtigten Mitarbeiter des Unternehmens freigegeben sein. Hierzu SOLL – je nach Unterschriftenregelung des Unternehmens – eine einfache oder fortgeschrittene Signatur auf einem Freigabedatensatz eingesetzt werden. Dieser ist lokal zu Nachweiszwecken zu protokollieren und SOLL NICHT mit der Benachrichtigung an die Verwaltung versandt werden.

Die Benachrichtigung selber MUSS gemäß den Vorgaben der zugrunde liegenden, für die Benachrichtigung geltenden gesetzlichen Bestimmungen signiert sein. In den meisten Fällen wird hier eine fortgeschrittene Signatur ausreichend sein, die mit einem Zertifikat des die Benachrichtigung sendenden Unternehmens verknüpft ist. Die qualifizierte Signatur MUSS nur dann verwendet werden, wenn der Gesetzgeber dies explizit vorschreibt. Dieses Verfahren trennt die teilweise erforderliche elektronische qualifizierte Dokumentensignatur (Signatur der eigentlichen Benachrichtigung) von der „Freigabe-Signatur“, so dass immer eine einfache oder fortgeschrittene Signatur für die Freigabe ausreicht. Hierdurch müssen lediglich die unterschriftsberechtigten, das Unternehmen rechtlich vertretenden Personen über qualifizierte Signaturen verfügen.

Wenn eine Benachrichtigung datenschutzrelevante, z. B. personenbezogene Daten enthält, MUSS sie verschlüsselt werden. Die Verschlüsselung MUSS auf einen vom Benachrichtigungsempfänger publizierten öffentlichen Schlüssel erfolgen (siehe Kapitel 7 für Verfahren zur Bekanntgabe von Zertifikaten). Das Verschlüsselungszertifikat MUSS den Vorgaben aus der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 6.7 in [5]) entsprechen. Das Erfordernis einer Verschlüsselung kann aus den beschreibenden Daten des zur Generierung der Benachrichtigung genutzten Benachrichtigungsregelpakets abgeleitet werden. Die konkrete Umsetzung der Verschlüsselung einer versandten Benachrichtigung hängt von dem gewählten Protokoll zur Übermittlung von Benachrichtigungen ab:

- Bei Übermittlung über eine SOAP-Schnittstelle MUSS die Verschlüsselung des vollständigen SOAP-BODY gemäß den Vorgaben aus [43] über XML Encryption [44] erfolgen.
- Bei Übermittlung über E-Mail MUSS die Verschlüsselung per S/MIME-Verschlüsselung [45], [46] erfolgen

Bei Übermittlung über OSCI-2 [1], [8] MÜSSEN die für dieses Protokoll definierten Mechanismen zur Ende-zu-Ende-Verschlüsselung genutzt werden.

6.5 Integrität, Authentizität und Vertraulichkeit von Nachrichten

Von einer Verwaltung an einen P23R übermittelte Nachrichten SOLLEN von einem berechtigten Mitarbeiter der Verwaltung freigegeben und signiert sein. Die sichere Übermittlung der Nachricht SOLL über OSCI Transport 2.0 erfolgen. Hierbei müssen die für OSCI Transport 2.0 spezifizierten Mechanismen zur Vermittlung einer authentischen Nutzeridentität (siehe Abschnitt 4.6), zur Integritätssicherung und – falls erforderlich – zur Sicherung der Vertraulichkeit genutzt werden.

Sofern ein anderes Protokoll als OSCI verwendet wird, MUSS die Authentizität der sendenden Verwaltung über das Kommunikationsprotokoll abgesichert werden:

- Bei Übermittlung über eine SOAP-Schnittstelle MUSS der vollständige SOAP-BODY gemäß den Vorgaben aus [43] über XML Signature [42] signiert sein. Das genutzte Zertifikat MUSS den Vorgaben aus der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 6.5 in [5]) entsprechen.
- Bei Übermittlung über E-Mail MÜSSEN die Nutzdaten (einschließlich aller Anhänge) per S/MIME Signatur [45][46] signiert werden. Das genutzte Zertifikat MUSS den Vorgaben aus der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 6.5 in [5]) entsprechen.

Eine Nachricht MUSS auf den vom empfangenden P23R in seiner TSL (siehe Kapitel 7) publizierten öffentlichen Schlüssel verschlüsselt werden.[13] Das Verschlüsselungszertifikat MUSS den Vorgaben aus der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Abschnitt 6.7 in [5]) entsprechen. Die konkrete Umsetzung der Verschlüsselung einer versandten Nachricht hängt von dem gewählten Protokoll zur Übermittlung von Nachrichten ab:

- Bei Übermittlung über das OSCI Transport 2.0 Protokoll MÜSSEN die dort spezifizierten Mechanismen genutzt werden. Die Verschlüsselung der Nachricht MUSS am OSCI-Gateway des P23R terminieren. Eine (zusätzliche) Verschlüsselung von Nachrichteninhalten KANN erfolgen, MUSS dann aber erst im P23R terminieren.
- Bei Übermittlung über eine SOAP-Schnittstelle MUSS die Verschlüsselung des vollständigen SOAP-BODY gemäß den Vorgaben aus [43] über XML Encryption [44] erfolgen.
- Bei Übermittlung über E-Mail MUSS die Verschlüsselung per S/MIME Verschlüsselung [45][46] erfolgen.

[13] Falls der P23R kein Verschlüsselungszertifikat angegeben hat, wird die Nachricht unverschlüsselt übertragen (in diesem Fall greift lediglich die TLS-Verschlüsselung auf der Transportebene).

7 AUSTAUSCH VON ADRESSEN UND ZERTIFIKATEN

Das Konzept des P23R sieht vor, dass mindestens drei Akteure über definierte Verfahren sicher mit Hilfe des P23R miteinander kommunizieren müssen:

- Unternehmen, die über einen P23R Benachrichtigungen für Verwaltungen generieren und Nachrichten von Verwaltungen entgegennehmen.
- Verwaltungen, die Benachrichtigungen von Unternehmen entgegennehmen und Nachrichten an Unternehmen versenden.
- Eine Öffentliche Leitstelle, die gemeinsam mit Verwaltungen Benachrichtigungsregelwerke erstellt, deren Lebenszyklus steuert und Benachrichtigungsregelwerke für Unternehmen zum Abruf vorhält.

Um die sichere Kommunikation zwischen diesen Akteuren zu ermöglichen, müssen alle Akteure die Dienst-Endpunkte und digitalen Zertifikate all ihrer Kommunikationspartner kennen. Hierzu sind verschiedene Lösungsansätze denkbar:

- In einer zentral vorgehaltenen Konfiguration sind die Dienst-Endpunkte und Zertifikate aller an der über den P23R vermittelten Kommunikation beteiligten Akteure vermerkt. Es gibt einen definierten Prozess, nach dem eine zentrale Stelle den Lebenszyklus dieser Konfiguration steuert und allen Akteure diese Konfiguration bereitstellt. Der Vorteil dieses Ansatzes ist, dass mit der Öffentlichen Leitstelle bereits eine Stelle existiert, die eine zentrale Bereitstellung von Konfigurationsdaten realisieren kann. Der Nachteil dieses Ansatzes ist, dass er normierte Prozesse zwischen Unternehmen und Verwaltungen auf der einen Seite und Öffentlicher Leitstelle auf der anderen Seite erfordert, die den kompletten Lebenszyklus einer Konfiguration (insb. Änderungen) abdecken. Da diese Lebenszyklen organisationsübergreifend ablaufen, müssen zusätzliche Mechanismen zur Absicherung von Authentizität, Verfügbarkeit, Nachvollziehbarkeit und Vertraulichkeit zwischen interagierenden Organisationen normiert, implementiert und betrieben werden.
- Für den P23R-Einsatz zuständige Systemadministratoren in Unternehmen und Verwaltungen rufen die erforderlichen Konfigurationsdaten aus bestehenden Verzeichnisdiensten, wie z. B. dem Deutschen Verwaltungsdiensteverzeichnis (DVDV) und dem LDAP-Dienst der Verwaltungs-PKI (ldap://x500.Bund.de) ab und pflegen diese manuell[14] in die P23R-Konfiguration ein. Der Vorteil dieses Verfahrens ist die geringe Redundanz, d. h. bestehende Systeme und Prozesse können für den P23R genutzt werden. Nachteilig sind die mit manuellen Prozessen zwangsläufig verbundenen Sicherheitsrisiken, die Verteilung benötigter Daten auf verschiedene Stellen sowie das Erfordernis einer Anpassung bzw. Erweiterung der genutzten Systeme an die Anforderungen des P23R.
- Jeder Akteur macht die Adressen seiner Dienst-Endpunkte und seine P23R-relevanten Zertifikate über einen eigenen Dienst verfügbar, der über ein Standard-Protokoll (FTP) abgefragt

[14] DVDV und LDAP-Dienst sind für einen P23R-Betrieb derzeit nicht vollständig, sodass die aggregierten Daten dieser Verzeichnisdienste zu einer P23R-Konfiguration aufbereitet werden müssen.

werden kann. Der Vorteil dieses Ansatzes ist die hohe Autonomie der Akteure. Es müssen jedoch einheitliche Vorgaben zum sicheren Umgang mit den Konfigurationsdaten in einer für alle Akteure umsetzbaren Form definiert und vor allem auch durchgesetzt werden.

Die nachfolgend beschriebene Lösung kann sowohl den ersten als auch den dritten der beschriebenen Ansätze sowie Mischformen zwischen diesen Ansätzen umsetzen. Ein Akteur aus dem P23R-Kontext kann frei entscheiden, ob er seine Konfigurationsinformationen selbst vorhält und zum Abruf bereitstellt oder ob diese Daten zusätzlich über eine zentrale Leitstelle verteilt werden sollen. Es ist auch möglich, dass P23R-Akteure als Konfigurations-Provider für andere Akteure agieren; beispielsweise kann auf diese Weise ein Ministerium die Konfigurationsdaten für alle nachgeordneten Verwaltungen bereitstellen (was insbesondere dann Sinn macht, wenn alle P23R-Endpunkte im gleichen Rechenzentrum angesiedelt sind).

7.1 Trusted Service Lists

Zum Aufbau sicherer Kommunikationsbeziehungen zwischen Unternehmen, P23R und Verwaltung werden Trusted Service (Status) Lists (TSLs) in der Syntax des ETSI-Standards zu Trust Service Provider Status Informationen [47] verwendet.[15]

Eine TSL kann je nach Profil (s. u.) die folgenden Informationen für von einem P23R-Akteur angebotene Dienste enthalten:

- Endpunktadresse (definierbares Format, d. h. auch Fax-Nummern sind als Endpunkte zulässig)
- Zertifikate für den Aufbau einer TLS-Verbindung zu diesem Dienst
- Zertifikate zur Verschlüsselung von über diesen Dienst vermittelten Daten
- Zertifikate zur Verifizierung von Signaturen auf über diesen Dienst vermittelte Daten

Welche dieser Angaben von einem P23R-Akteur bereitgestellt werden müssen, wird in fünf unterschiedlichen TSL-Profilen definiert (siehe Kapitel 5 in [5]). Diese bilden die Anforderungen an die unterschiedlichen Kommunikationsbeziehungen zwischen den Akteuren ab:

- P23R-Callback: Ein Unternehmen oder eine Verwaltung publiziert Adressen und Zertifikate von Callback-Diensten (Attribute Service, Policy Information Point, Policy Administration Point, Identity Provider). Da die aktuell von P23R umzusetzenden Szenarien keine Autorisierung von Verwaltungsmitarbeitern an einem P23R eines Unternehmens erfordern, sind zunächst nur P23R-Callback-TSLs für Unternehmen definiert.
- P23R-External: Ein Unternehmen publiziert die zur Kommunikation mit diesem Unternehmen benötigten Adressen (URIs) und Zertifikate.

[15] Der ETSI-Standard definiert Syntax und Semantik einer Trust Service Status List, über die Informationen zu von einem Trust Service Provider angebotenen Diensten publiziert werden können. Auch wenn der Standard als Trust Service Provider vor allem Zertifikatsherausgeber im Fokus hat, ist er doch bewusst für weitere Verwendungszwecke offen gehalten. Im Rahmen des P23R wird der Standard für die Bekanntgabe von Zertifikaten und Schnittstellen vertrauenswürdiger Dienste genutzt; die entsprechenden Dokumente werden daher als Trusted Service Lists (TSLs) bezeichnet.

- GOV-External: Eine Verwaltung publiziert die zur Kommunikation mit dieser Verwaltung benötigten Adressen (URIs) und Zertifikate.
- CTRLCTR-External: Die Öffentliche Leitstelle publiziert die zur Kommunikation mit der Leitstelle benötigten Adressen und Zertifikate.

Abbildung 18 gibt einen Überblick, welche TSL-Profile zwischen welchen Akteuren ausgetauscht werden.

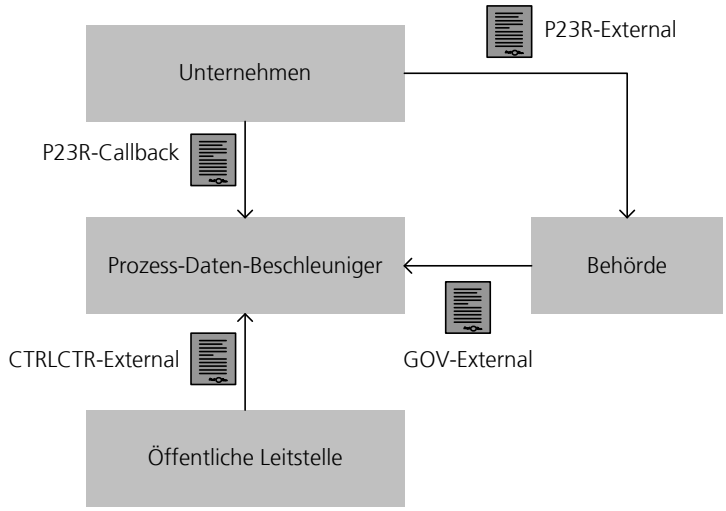


ABBILDUNG 18: AUSTAUSCH VON TRUSTED SERVICE LISTS (BLOCKDIAGRAMM)

Wie in der Rahmenarchitektur [1] beschrieben, muss ein P23R während des Bootstrapping-Prozesses den Abruf von TSLs von der Öffentlichen Leitstelle per HTTP(S) unterstützen.

Im folgenden Abschnitt 7.2 ist beschrieben, wie die einzelnen TSLs publiziert, verteilt und gepflegt werden. Abschnitt 7.3 beschreibt die als Vertrauensanker genutzten Zertifikate und die Anforderungen zur Prüfung von Signaturen auf TSLs. Die Abbildung der in den einzelnen Profilen publizierten Informationen zu Adressen und Zertifikaten auf die Syntax des ETSI TS 102231 Standards ist gesondert in der technischen Spezifikationen zur Sicherheitsarchitektur (siehe Kapitel 5 in [5]) spezifiziert.

7.2 Pflege und Verteilung von Trusted Service Lists

Die folgenden vier Abschnitte beschreiben die Publikation, Verteilung und Pflege aus den verschieden Kommunikationsbeziehungen heraus.

7.2.1 P23R-Callback TSL

Eine P23R-Callback TSL MUSS angelegt werden, wenn ein P23R auf Dienste in der IT-Infrastruktur eines Unternehmens zugreifen soll (z. B. zum Abruf von Nutzerattributen). Eine P23R-Callback TSL wird in der Regel vom Systemadministrator des Unternehmens angelegt und enthält die Endpunkt-Adressen und -Zertifikate der Dienste, die für den P23R sichtbar und nutzbar sein sollen.

P23R-Callback TSLs für die einzelnen Mandanten eines P23R sind Bestandteil der Konfiguration des P23R. Es ist dem P23R-Provider überlassen, wie er die Authentizität von P23R-Callback TSLs prüft[16] und diese in eine P23R-Instanz einspielt.

7.2.2 GOV-EXTERNAL TSL

Jede Verwaltung, die über einen P23R generierte Benachrichtigungen entgegennimmt, MUSS die Adressen und Zertifikate der Annahmepunkte (Trusted Proxies, Postfächer, Faxgeräte etc.) in einer GOV-External TSL publizieren. GOV-External TSLs werden vom für die IT-Infrastruktur der Verwaltung verantwortlichen Systemadministrator erstellt und gepflegt. Die Bereitstellung der TSL seitens der Verwaltung kann entweder dezentral oder zentral über die Öffentliche Leitstelle erfolgen. Eine GOV-External TSL MUSS mit einer fortgeschrittenen Signatur versehen sein, anhand derer die Integrität und Authentizität der TSL verifizierbar ist.

Der CompetenceFinder (P23R-Zuständigkeitsverzeichnis) auf Seite der P23R-Leitstelle [1] liefert Adressen und weitere notwendige Informationen eines Benachrichtigungsempfängers und KANN daher Teile dieser benötigten Informationen aus einer GOV-External TSL beziehen.[17] Der CompetenceFinder DARF NUR GOV-External TSLs in seine statische Konfiguration übernehmen, deren Integrität und Authentizität er vollständig prüfen konnte. Die GOV-External TSL MUSS neu geladen werden, wenn

- eine der darin benannten Endpunktadressen nicht mehr verfügbar ist
- eines der darin enthaltenen Zertifikate nicht mehr gültig ist bzw. gesperrt wurde
- das zur Signatur der TSL genutzte Zertifikat gesperrt wurde. Um dies zu prüfen, MUSS die Gültigkeit des Zertifikats vor jeder Nutzung der in der TSL enthaltenen Daten geprüft werden.

7.2.3 P23R-EXTERNAL TSL

Ein P23R, der von Verwaltungen versandte Nachrichten entgegennimmt, MUSS die Adressen und Zertifikate seiner Annahmepunkte (Trusted Proxies, Postfächer, Faxgeräte etc.) in einer P23R-External TSL publizieren. P23R-External TSLs werden vom für den Betrieb eines P23R verantwortlichen Systemadministrator erstellt und gepflegt. Die Bereitstellung der TSL eines P23R erfolgt dezentral über ein vom P23R-Provider gewähltes, standardisiertes Protokoll (HTTPS oder SFTP). Die Adresse, unter der eine P23R-External TSL eines P23R bereitgestellt wird, ist als vollständige URL in allen von diesem P23R generierten Benachrichtigungen kodiert. Ein P23R Betreiber KANN unterschiedliche Endpunkte – und damit auch unterschiedliche TSLs – für an verschiedene Mandanten gerichtet Nachrichten bereitstellen.

Eine P23R-External TSL MUSS mit einer fortgeschrittenen Signatur versehen sein, anhand derer die Integrität und Authentizität der TSL verifizierbar ist. Eine Verwaltung DARF für den Versand von Nachrichten nur Angaben aus einer TSL nutzen, deren Integrität und Authentizität sie vollständig prüfen konnte.

[16] Die Spannbreite der Mechanismen reicht hierbei von der persönlichen Übergabe auf einem Datenträger bis zu einer Schnittstelle zum dynamischen Import signierter TSL-Dateien.

[17] Weiterentwicklungen der P23R-Architektur werden Erfahrungen aus dem P23R-Betrieb bzgl. der Synchronisation von P23R-Zuständigkeitsverzeichnis und GOV-External TSL berücksichtigen, um weitere Synergiepotenziale zu nutzen.

Ein Fachsystem in einer Verwaltung KANN eine P23R-External TSL in seine Konfiguration übernehmen. Die TSL MUSS neu geladen werden, wenn eine der darin benannten Endpunkt-Adressen nicht mehr verfügbar ist oder wenn eines der darin enthaltenen Zertifkate nicht mehr gültig ist bzw. gesperrt wurde. Die Signatur der TSL MUSS vor jeder Nutzung der in der TSL enthaltenen Daten geprüft werden.

7.2.4 CTRLCTR-EXTERNAL TSL

In einer CTRLCTR-External TSL publiziert eine Leitstelle die Endpunkt-Adressen und -Zertifikate ihrer Dienste (z. B. zum Abruf von Benachrichtigungsregelpaketen).

Die CTRLCTR-External TSL einer Leitstelle ist der Vertrauensanker des gesamten von dieser Leitstelle bedienten P23R-Netzwerks. Die Abrufadresse dieser TSL sowie das zur Prüfung der Signatur auf der TSL benötigte Zertifikat sind Bestandteil der Konfiguration eines jeden P23R. Die Öffentliche Leitstelle MUSS einen Abruf über HTTPS ermöglichen, zusätzlich KANN eine Bereitstellung über SFTP unterstützt werden. Jeder P23R-Provider MUSS die Authentizität des Zertifikats vor der Übernahme in die P23R-Konfiguration verifizieren (z. B. durch manuellen oder automatischen Vergleich gegen einen auf anderem Wege übermittelten Fingerprint).

7.3 SIGNATUREN AUF TRUSTED SERVICE LISTS

Alle TSL Dateien (mit Ausnahme der P23R-Callback TSL) sind mit einer fortgeschrittenen Signatur versehen. Das Signaturzertifikat der Leitstelle ist Bestandteil der Konfiguration eines jeden P23R. Hierüber kann die Authentizität einer CTRLCTR-External TSL sicher geprüft werden.

Alle Zertifikate zu Schlüsseln, die für die Signierung von TSLs und Benachrichtigungsregelpaketen genutzt werden, MÜSSEN in einer Sub-Zertifizierungsstelle (engl. Certification Authority, CA) verankert sein. Diese Sub-CA MUSS ausschließlich Zertifikate ausstellen, die zum Betrieb des P23R-Netzwerks genutzt werden (Zweckbindung). Dies KANN bspw. in einer Certificate Policy gefordert werden; weitere Festlegungen werden hierzu nicht getroffen. Das Zertifikat der Sub-CA ist in der CTRLCTR-External TSL der Öffentlichen Leitstelle angegeben und wird von jedem P23R in den lokalen Trust Store übernommen.

8 ANHANG: VERWENDETE STANDARDS

8.1 SECURITY ASSERTION MARKUP LANGUAGE (SAML)

Die Security Assertion Markup Language (SAML) spezifiziert einen Rahmen, in dem vertrauenswürdige Aussagen zu Identitäten dargestellt und ausgetauscht werden können. Die primären Anwendungsszenarien, in denen SAML eingesetzt wird, sind Single Sign-On sowie Identity Federation (Verknüpfung und Austausch von Identitätsinformationen über Organisationsgrenzen hinweg).

Den zentralen Bestandteil des Standards bilden die in [32] spezifizierten abstrakten Nachweise (Assertions) und Protokolle. Während die Assertions vertrauenswürdige Aussagen zur Authentifizierung und Autorisierung einer Identität sowie einer Identität zugeordnete Attribute kapseln, erlauben es die Protokolle, solche Assertions anzufragen und zu transportieren (siehe Tabelle 4).

TABELLE 4: STECKBRIEF „SAML CORE“

SAML Core	
Organisation	OASIS
Version	2.0 (März 2005)
Zweck	Abstrakte, XML-basierte Darstellung von vertrauenswürdigen Aussagen in Form von SAML Assertions
	Abstrakte Protokolle für den Transport der SAML Assertions

Die SAML-Protokolle und deren Nachrichten werden in [32] zunächst abstrakt spezifiziert. Wie die Protokolle an ein konkretes Nachrichten- oder Transportprotokoll, beispielsweise SOAP oder HTTP, gebunden werden, wird in [41] spezifiziert. Abhängig vom mit SAML umzusetzenden Anwendungsszenario können Assertions und Protokolle zusätzlich in Form einer Profilierung konkretisiert werden. Für typische Anwendungsszenarien gibt der SAML-Standard bereits Profilierungen in [48] vor. Diese umfassen u. a. Single Sign-On-Szenarien für Web Browser und für erweiterte Clients sowie Identity-Federation-Szenarien in verschiedenen Varianten.

Für den P23R werden nach diesem Muster zwei Profile über dem SAML 2.0 Assertion-Format definiert (siehe Kapitel 4 in [5]). Diese erlauben eine auf die Szenarien der P23R-Nutzung durch Unternehmen und Verwaltungen abgestimmte Kodierung von Identitäts- und Authentifizierungsnachweisen. Die SAML 2.0 Protokolle werden in der P23R-Sicherheitsarchitektur nicht genutzt, da sie vielfach auf eher leichtgewichtige Szenarien abzielen (z. B. Zugriff über Web Browser). Stattdessen werden WS-Trust zum Abruf von Assertions und DSML zur Abfrage von zusätzlichen Nutzerattributen verwendet.

8.2 EXTENSIBLE ACCESS CONTROL MARKUP LANGUAGE (XACML)

XACML [26] erlaubt die XML-basierte Beschreibung von Regeln für den Zugriff auf Ressourcen und spezifiziert Protokolle, mit denen Autorisierungsentscheidungen angefordert und ausgegeben werden können (siehe Tabelle 5). Der Standard verfolgt einen generischen Ansatz, sodass mit XACML verschiedenartige Ansätze für Berechtigungssysteme (z. B. rollenbasierte Berechtigungen) realisiert werden können.

TABELLE 5: STECKBRIEF „XACML“

XACML		
Organisation	OASIS	
Version	2.0 (Februar 2005)	
Zweck	Autorisierung	
	Beschreibung von Zugriffsregeln	
	Protokoll zur Anforderung und Herausgabe von Autorisierungsentscheidungen	

Der Standard besteht in seinem Kern aus den Systembausteinen Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Information Point (PIP) sowie Policy Administration Point (PAP). Diese Systembausteine werden durch weitere periphere Informationssysteme (z. B. Verzeichnisdienste) unterstützt. Weitere von OASIS herausgegebene Profile adressieren das Zusammenspiel mit anderen Standards (z. B. SAML) oder die Implementierung spezifischer Berechtigungsmodelle über die Konstrukte von XACML.

XACML spezifiziert – wie SAML auch – zunächst lediglich die Schemata für Protokollnachrichten. Der Transport dieser Nachrichten wird vom Standard nicht adressiert und ist Gegenstand einer Profilierung. Die Spezifikation zur P23R-Sicherheitsarchitektur nimmt solche Profilierungen lediglich dort vor, wo Nachrichten zwischen P23R und Unternehmen / Verwaltung ausgetauscht werden und somit einheitlich umzusetzende Außenschnittstellen existieren. Für den P23R-internen Fluss von Nachrichten zwischen PEP, PDP, PAP und PIP werden lediglich Umsetzungsbeispiele gegeben (siehe Kapitel 7 in [5]). Hersteller können hier jedoch mit großen Freiheitsgraden auch auf die spezifischen Einsatzszenarien eines P23R zugeschnittene Lösungen umsetzen.

8.3 Web Services Security (WS-Security)

WS-Security [43] erlaubt es, SOAP-Nachrichten auf der Nachrichtenebene zu signieren und zu verschlüsseln. Es bietet außerdem einen Rahmen, in dem verschiedene Sicherheitstoken übertragen werden können. Der Standard wird daher von weiteren Token-Profilen begleitet, die etwa die Nutzung von X.509-basierten Zertifikaten, SAML-Token oder Kerberos-Tickets als Sicherheitstoken spezifizieren (siehe Tabelle 6).

TABELLE 6: STECKBRIEF „WS-SECURITY“

WS-Security		
Organisation	OASIS	
Version	1.1 (Februar 2006)	
Zweck	Nachrichtensicherheit auf Nachrichtenebene, Bereitstellung von Mechanismen für höhere Sicherheitsprotokolle	
Erweiterungen	Tokenprofile:	Username Token Profile 1.1
		X.509 Token Profile 1.1
		SAML Token Profile 1.1
		Kerberos Token Profile 1.1

Im Rahmen der P23R-Sicherheitsarchitektur wird WS-Security genutzt, um Sicherheitstoken zwischen Unternehmen / Verwaltung und Systemkomponenten des P23R auszutauschen. So wird z. B. bei jedem Aufruf eines P23R-Dienstes über das WS-Security SAML Token Profile die vom P23R-Identity-Provider ausgestellte P23R-Identity-Assertion in die Nachricht eingebettet. Die WS-Security Profile zur Vermittlung von Authentifizierungsinformationen werden vom P23R-Identity-Provider genutzt, um verschiedene Arten der Nutzeranmeldung gegenüber der Berechtigungsprüfung auf einen einheitlichen Mechanismus abzubilden.

8.4 Web Services Trust Language (WS-Trust)

WS-Trust [31] erweitert WS-Security um ein nachrichtenbasiertes Protokoll, das das Anfragen und Ausstellen von Sicherheitstoken sowie die Delegation von Vertrauensbeziehungen erlaubt. WS-Trust führt dazu ein aus drei Rollen bestehendes Modell ein, in dem ein Webservice-Nutzer bei einem Sicherheitstokendienst (Security Token Service, STS) ein Sicherheitstoken anfragt, welches dieser anschließend bei einem Webservice-Anbieter einlösen kann. Die vom Webservice-Nutzer so vorgelegten Behauptungen zur Nutzeridentität sind durch die Vertrauensbeziehung zwischen Webservice-Anbieter und STS mithilfe von kryptographischen Methoden verifizierbar.

WS-Trust (siehe Tabelle 7) ist funktional dem SAML 2.0 Protokoll sehr ähnlich, wobei SAML eher in browserbasierten Lösungen zum Einsatz kommt, während WS-Trust vorwiegend in Fat-Client-Umgebungen genutzt wird, bei denen auch über eine rein textbasierte HTTP-Kommunikation hinausgehende Protokolle wie z. B. SOAP zur Kommunikation zwischen Systemkomponenten genutzt werden. Hersteller von Identitäts- und Berechtigungsmanagement-Lösungen unterstützen üblicherweise beide Protokolle.

TABELLE 7: STECKBRIEF „WS-TRUST“

WS-Trust	
Zuständigkeit	OASIS
Version	1.3 (März 2007)
Zweck	Anfragen und Ausstellen von Sicherheitstoken (z. B. SAML Assertions), Konzept des direkt vermittelten Vertrauens

Der P23R-Identity-Provider ist ein WS-Trust 1.3 STS. Er erlaubt einen Abruf von P23R-Identity-Assertions über das WS-Trust-Protokoll.

8.5 Web Services Security Policy Language (WS-SecurityPolicy)

WS-SecurityPolicy [25] spezifiziert eine Erweiterung des Web Services Policy Framework Standards (WS-Policy) [24]. WS-SecurityPolicy erlaubt es, die Sicherheitsrichtlinien eines Webservices als Teil des Dienstvertrags abzubilden. Mit dieser Erweiterung ist es beispielsweise möglich, die zu verwendenden Sicherheitstoken festzulegen oder anzuzeigen, welche Nachrichtenteile zu signieren oder zu verschlüsseln sind. WS-SecurityPolicy gibt dafür die Syntax und Semantik von sogenannten Policy Assertions vor, die auf die Standards WS-Security, WS-Trust sowie WS-SecureConversation abgestimmt sind. Der Kurzsteckbrief ist in Tabelle 8 zu finden.

TABELLE 8: STECKBRIEF „WS-SECURITYPOLICY“

WS-SecurityPolicy	
Zuständigkeit	OASIS
Version	1.2 (Juli 2007)
Zweck	Beschreibung von Sicherheitsrichtlinien im Dienstvertrag

Im Rahmen des Deployments der P23R-Systemkomponenten KANN WS-SecurityPolicy genutzt werden, um die Ablaufsequenz zur Nutzerauthentifizierung durch das verwendete WS-Framework zu steuern (siehe Abschnitt 4.4). So kann z. B. ein Nutzer direkt einen Dienst des P23R aufrufen und das WS-Framework ist anhand von WS-SecurityPolicy in der Lage, selbständig mit den Sicherheitsdiensten zu kommunizieren, die für den Nutzer die zum Dienstaufruf beizubringenden Sicherheitstoken ausstellen.

8.6 DIRECTORY SERVICES MARKUP LANGUAGE (DSML)

Die Directory Services Markup Language 2.0 (DSMLv2) [39] ist eine standardisierte, XML-basierte Beschreibungssprache für den Zugriff auf Verzeichnisdienste (siehe Tabelle 9). Anders als die erste Fassung des Standards ist DSMLv2 keine Beschreibungssprache für den Zustand eines Verzeichnisses (der Ausprägung eines konkreten Verzeichnisbaums (Directory Information Tree, DIT)). Stattdessen spezifiziert DSMLv2 eine XML-Grammatik, welche die vom Quasi-Standard LDAP bekannten Operationen eines Verzeichnisdienstes beschreibt.

DSMLv2 erlaubt es, Verzeichnisdienste mithilfe von Webservices-Technologien bereitzustellen. Der Standard spezifiziert dazu ein SOAP-Binding, welches zusammen mit http / HTTPS eingesetzt werden kann. Durch eine Kapselung von LDAP-Verzeichnisdiensten mit einer DSMLv2-Schnittstelle ist es möglich, Fach- und Verzeichnisdienste mit einheitlichen Sicherheitsmechanismen zu schützen.

TABELLE 9: STECKBRIEF „DIRECTORY SERVICES MARKUP LANGUAGE“

DSML	
Zuständigkeit	OASIS
Version	2.0 (April 2002)
Zweck	XML-basierter Zugriff auf Verzeichnisdienste

Im Rahmen der P23R-Sicherheitsarchitektur wird DSML zur Abfrage von Nutzerattributen aus einem Attribute Service verwendet. DSML bildet hier die Brücke zwischen den serviceorientierten, auf XML-Datenstrukturen aufbauenden P23R-Sicherheitsdiensten und in Unternehmen weit verbreiteten LDAP- bzw. ActiveDirectory-basierten Verzeichnisdiensten.

8.7 TRUSTED SERVICE LIST (TSL)

Der Standard ETSI TS 102 231 [47] definiert ein logisches Modell, um dienstspezifische Informationen zu Schnittstellen und digitalen Zertifikaten interoperabel austauschen zu können. Dafür wurden vier logische Komponenten definiert:

- Schlüsselinformationen über die TSL selbst (Verweise auf weitere Informationen etc.)
- Informationen über einen vertrauenswürdigen Diensteanbieter (Trusted Service Provider, TSP)
- Informationen über spezifische Dienste eines TSP
- Historie über Statusinformationen der Dienste

Dies wird in einer sogenannten „Trust-Service Status List“ festgehalten, welche in ASN.1 [49] oder XML implementiert sein kann.

TABELLE 10: STECKBRIEF „TRUSTED SERVICE LIST“

TSL	
Zuständigkeit	ETSI
Version	3.1.2 (Dezember 2009)
Zweck	Standard für die Provisionierung von Informationen zur Etablierung von Vertrauensverhältnissen zwischen Kommunikationspartnern

Im Rahmen des P23R werden TSLs benutzt, um die zum Aufbau sichererer Kommunikationsbeziehungen zwischen Unternehmen, P23R, Öffentlicher Leitstelle und Verwaltungen erforderlichen Informationen – wie z. B. Dienstschnittstellen und Zertifikate – zu publizieren (siehe Kapitel 7).

9 GLOSSAR

Access Policy

Eine Access Policy ist ein Regelwerk, aus dem sich Entscheidungen über die Zulässigkeit von Ressourcenzugriffen herleiten lassen. Im Rahmen der P23R-Sicherheitsarchitektur werden Access Policies zur Kodierung von Berechtigungen (Berechtigungs-Policies) und zur Steuerung des Dienstzugangs (Sicherheits-Policies) verwendet.

Adapter

Adapter sind interne Komponenten, um unterschiedliche interne oder externe Implementierungen einer Schnittstelle zu nutzen, bspw. um Datenformate oder Übertragungsprotokolle anzupassen.

Antrag

Ein Antragsprozess stellt einen Typ von Prozessketten zwischen Wirtschaft und Verwaltung dar, der dadurch gekennzeichnet ist, dass ein Antragsteller bei der zuständigen Behörde eine Genehmigung für eine bestimmte Tätigkeit oder auch eine Unterstützungsleistung einholt bzw. nachfragt. Die verschiedenen Typen von Prozessketten zwischen Wirtschaft und Verwaltung werden durch die Merkmale Auslöser und Richtung des Informationsflusses unterschieden. Anträge werden durch ein bestimmtes Anliegen des Antragstellers (eine bestimmte Tätigkeit bspw. ein Bau einer Fabrikhalle soll durchgeführt werden oder Unterstützungsleistungen bspw. in Form von Subventionen sollen in Anspruch genommen werden) ausgelöst. Im Lauf des Antragsprozesses oder Antragsverfahrens werden Informationen zwischen Antragsteller und Genehmigungsbehörde in beide Richtungen ausgetauscht, d. h. der Informationsfluss ist bidirektional.

Arbeitgebermeldepflichten

Der Sammelbegriff Arbeitgebermeldepflichten (kurz AGM) umfasst alle Informations- und Meldepflichten, die ein Unternehmen in seiner Funktion als Arbeitgeber erfüllen muss.

Assertion

Eine Assertion ist eine Zusicherung über einen durchgeführten Prozess und / oder Eigenschaften eines Objekts. Im Rahmen der P23R-Sicherheitsarchitektur werden sog. Identity Assertions genutzt, um von einem vertrauenswürdigen Dienst beglaubigte Zusicherungen über die Identität von Nutzern auszutauschen.

Attribut

Ein Attribut ist ein beschreibendes Merkmal einer Entität, das über einen Namen, eine Bedeutung, eine Struktur und einen Definitionsbereich verfügt. Im Rahmen der P23R-Sicherheitsarchitektur werden Attribute z. B. für Nutzer, Regeln und Ressourcen definiert.

Attribute Service

Ein Attribute Service ist ein Dienst, über den Attributwerte zu einer identifizierten Entität – z. B. die E-Mail-Adresse eines Nutzers – abgefragt werden können.

Audit

Protokollierung von fachlichen Ereignissen, z. B. zum Zweck des Datenschutzes oder zur Wahrung der Betroffenenrechte.

Authentifizierung

Unter einer Authentifizierung versteht man die Prüfung einer Authentisierung, d. h. die Überprüfung, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein.

Authentizität

Unter dem Begriff Authentizität (engl. authenticity) versteht man die Eigenschaft, die gewährleistet, dass der Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein, bzw. dass die vorliegenden Informationen von der angegebenen Quelle erstellt wurden.

Autorisierung

Eine Autorisierung ist eine Einräumung von Rechten. Rechte können dabei sowohl an Individuen und abgegrenzte Gruppen vergeben werden als auch an offene Gruppen, die lediglich über Eigenschaften ihrer Mitglieder beschrieben sind (z. B. rollenbasierte Berechtigungsvergabe).

Benachrichtigung (Notification)

Eine Benachrichtigung ist ein Sammelbegriff für die technische Darstellung im P23R für einen Antrag, einen Bericht, eine Meldung oder eine Statistik, der bzw. die an einen Benachrichtigungsempfänger gesendet wird. Eine Benachrichtigung, die ein Benachrichtigungssender an den Benachrichtigungsempfänger übermittelt, ergibt sich bspw. aus juristischer Sicht aus den Benachrichtigungspflichten der Unternehmen gegenüber der Verwaltung.

Benachrichtigung, Öffentliche (Legal Notification)

Eine Öffentliche Benachrichtigung ist der Spezialfall einer Benachrichtigung, deren zugeordnete Öffentliche Benachrichtigungsregel ausdrücklich vom Vorschriftengeber freigegeben ist. Öffentliche Benachrichtigungen sind insbesondere:

- Meldungen (periodisch und anlassbezogen),
- Berichte,
- Anträge.

Benachrichtigungsempfänger (Notification Receiver)

Der Benachrichtigungsempfänger (beispielsweise ein Unternehmen, eine Organisation oder eine Verwaltung) benötigt von einem Benachrichtigungssender (beispielsweise ein Unternehmen, eine Organisation oder eine Verwaltung) Informationen, die er in Form von Benachrichtigungen erhält.

Benachrichtigungsempfänger für eine Öffentliche Benachrichtigung bezeichnet eine Behörde oder eine andere Stelle auf Vollzugsebene mit einem gesetzlichen Auftrag, dessen Rahmen eine Öffentliche Benachrichtigung zu empfangen oder anzufordern ist.

Benachrichtigungspool (Notification Pool)

Speicher und Archiv für die Benachrichtigungen, in dem alle generierten Benachrichtigungen nachweisbar abgelegt werden. Die freigegebenen Benachrichtigungen werden aus dem Pool an den ermittelten Benachrichtigungsempfänger versendet.

Benachrichtigungsregel (Notification Rule)

Eine Benachrichtigungsregel (BR) beschreibt, wie technisch aus den Daten des Benachrichtigungssenders (z. B. ein Unternehmen) genau eine Benachrichtigung für den Benachrichtigungsempfänger (z. B. eine Verwaltung) generiert wird. Eine BR enthält vor allem verschiedene Berechnungen zur Selektion, Aggregation, Transformation, Validierung und Repräsentation sowie weitere vom P23R benötigte Metainformationen. Für die technische Umsetzung werden die Benachrichtigungsregeln aus den rechtlichen Vorgaben durch den Gesetzgeber bzw. der Verwaltung abgeleitet.

Dabei wird zwischen technischen und fachlichen Benachrichtigungsregeln unterschieden. Technische Benachrichtigungsregeln werden in einer Technischen Benachrichtigungsregelsprache (T-BRS) definiert, direkt durch den P23R verstanden und sind auf allen P23Rs ausführbar. Um die Entwicklung und Überprüfung der Benachrichtigungsregeln für Fachleute zu vereinfachen, gibt es fachliche Benachrichtigungsregeln, die in einer Fachlichen Benachrichtigungsregelsprache (F-BRS) definiert werden, durch Fachleute relativ einfach verstanden und geschrieben werden können sowie automatisch in die technischen Benachrichtigungsregeln übersetzbar sind.

Benachrichtigungsregel, Öffentliche (Legal Notification Rule)

Eine Öffentliche Benachrichtigungsregel ist ein Spezialfall der Benachrichtigungsregel. Sie basiert auf der Modellierung einer gesetzlichen Vorgabe (der Benachrichtigungspflicht). Die Öffentliche Benachrichtigungsregel wird vom Vorschriftengeber geprüft und als korrekt freigegeben. Während software-technisch keine Unterschiede zur (allgemeinen) Benachrichtigungsregel bestehen, unterscheidet sich die rechtliche Beurteilung der Öffentlichen Benachrichtigungsregel von derjenigen der allgemeinen Benachrichtigungsregel. Die unveränderte Anwendung der Öffentlichen Benachrichtigungsregel im P23R begründet z. B. eine ausreichende Ausübung der Sorgfaltspflicht bei der Erzeugung bzw. Zusammenstellung einer Benachrichtigung mit Hilfe des P23R. Die Richtigkeit der verwendeten Daten bleibt

Benachrichtigungsregelgruppe (Notification Rule Group)

Eine Benachrichtigungsregelgruppe (BRG) enthält alle diejenigen Benachrichtigungsregeln, die zur Unterstützung einer Meldung, einer Statistik, eines Berichts usw. benötigt werden. Die Benachrichtigungssender können nur Benachrichtigungsregelgruppen in Benachrichtigungsregelpaketen von einer P23R-Leitstelle beziehen. Die Aktivierung von Benachrichtigungsregeln im P23R erfolgt immer im Rahmen einer Benachrichtigungsregelgruppe. Welche Benachrichtigungsregelgruppen für einen Benachrichtigungssender tatsächlich erforderlich bzw. sinnvoll sind, wird bei der Aktualisierung von Benachrichtigungsregelpaketen mittels spezifischer Entscheidungskriterien für eine Benachrichtigungsregelgruppe überprüft.

Es kann für eine Meldepflicht innerhalb einer Benachrichtigungsregelgruppe zum einem verschiedene Varianten einer Benachrichtigung geben, beispielsweise bedingt durch unterschiedliche Unternehmensgrößen. Zum anderen kann es auch mehrere verschiedene, aber zusammengehörende Benachrichtigungen geben, die zur Umsetzung der Meldepflicht benötigt werden, beispielsweise neben der eigentlichen Meldung auch die Anmeldung bei einer Behörde bzgl. der Meldepflicht.

Benachrichtigungsregelpaket (Notification Rule Package)

Ein Benachrichtigungsregelpaket (BRP) ist eine Menge von technischen Benachrichtigungsregelgruppen sowie den dazugehörigen Teildatenmodellen, wie sie technisch durch eine Leitstelle bereitgestellt werden. Ein BRP könnte beispielsweise alle benötigten Benachrichtigungsregelgruppen für eine Fachdomäne enthalten.
Darüber hinaus gibt es ein Basis-Benachrichtigungsregelpaket, das die Benachrichtigungsregelgruppen enthält, die grundsätzlich jeder P23R insbesondere für seine Initialisierung benötigt.

Die Benachrichtigungsregelgruppen in einem BRP werden nach Gesichtspunkten der technischen Verwandtschaft und des Anwendernutzens zusammengestellt. Sie sind in der Regel nicht deckungsgleich mit der Gruppierung in einem Benachrichtigungsregelwerk.

Benachrichtigungsregelsprache (Notification Rule Language)

Eine Benachrichtigungsregelsprache (BRS) beschreibt die Rechtschreibung und Grammatik, wie Benachrichtigungsregeln, -gruppen und -pakete zu spezifizieren sind. Die Technische Benachrichtigungsregelsprache (T-BRS) wird für die Verteilung der Benachrichtigungsregelpakete genutzt, um sicherzustellen, dass jeder P23R unabhängig vom Hersteller die Benachrichtigungsregeln identisch interpretiert.

Die Fachliche Benachrichtigungsregelsprache (F-BRS) soll dagegen den Fachexperten, die die fachlichen Benachrichtigungsregelwerke entwickeln und spezifizieren müssen, eine möglichst einfach zu erstellende, leicht verständliche und fachlich angepasste Beschreibungsform zur Verfügung stellen, die dann letztlich aber automatisch in die T-BRS übersetzt wird.

Siehe auch *Benachrichtigungsregel.*

Benachrichtigungsregelwerk (Notification Rule Set)

Ein Benachrichtigungsregelwerk (BRW) ist eine logisch oder fachlich abgeschlossene Menge von Benachrichtigungsregeln. Dies könnten beispielsweise alle Benachrichtigungsregeln zu einem Gesetz, einem Rechtsgebiet, einer Fachdomäne oder einer Organisationseinheit sein. Die Kriterien der Zusammenfassung sind rein fachlicher Art. Es gibt keine zwingende Deckungsgleichheit mit den Begriffen „Benachrichtigungsregelpaket“ oder „Benachrichtigungsregelgruppe“.

Benachrichtigungssender (Notification Sender)

Der Benachrichtigungssender (beispielsweise ein Unternehmen, eine Organisation oder eine Verwaltung) sendet Informationen, in Form von Benachrichtigungen, an einen Benachrichtigungsempfänger (beispielsweise ein Unternehmen, eine Organisation oder eine Verwaltung).

Benachrichtigungstyp (Notification Type)

Die Benachrichtigungsregeln generieren eine Benachrichtigung in einem internen, empfängerunabhängigen XML-Format. Jedem dieser XML-Formate kann ein Benachrichtigungstyp zugeordnet werden. Ein Benachrichtigungstyp wird durch einen eindeutigen Namen in Form des standardmäßigen XML-Namensraums identifiziert, der in dem XML-Dokument verwendet wird.

Berechtigung

Siehe *Autorisierung*.

Bericht

Ein Bericht stellt einen Typ von Prozessketten zwischen Wirtschaft und Verwaltung dar, der dadurch gekennzeichnet ist, dass ein Unternehmen vorgegebene Informationen über eine bestimmte Tätigkeit bspw. die mit der Verbrennung von Abfällen verbundenen Emissionen abgeben muss. Die verschiedenen Typen von Prozessketten zwischen Wirtschaft und Verwaltung werden durch die Merkmale Auslöser und Richtung des Informationsflusses unterschieden. Berichte sind dadurch charakterisiert, dass sie neben festgelegten Inhalten einen vorgegeben Fälligkeitstermin und eine vorgegebene Frequenz haben, d.h. sie werden durch das Eintreffen des Fälligkeitstermins ausgelöst. Informationen fließen im Wesentlichen in eine Richtung, vom Unternehmen zur zuständigen Überwachungsbehörde.

Betreibermodell

Ein Betreibermodell ist ein Geschäftskonzept für die Bereitstellung von Gütern und Dienstleistungen, bei dem diese nicht mehr an Kunden verkauft, sondern gegen ein leistungsabhängiges Entgelt zur Nutzung angeboten werden. Betreibermodelle können somit für die Bereitstellung von physischen Produkten und / oder immateriellen Dienstleistungen gestaltet und etabliert werden. Betreibermodelle können gemäß den folgenden Kriterien klassifiziert, beschrieben und gestaltet werden: Leistungsfokus, Organisationsform, Koordinationsform, Kundenfokus, Gegenstand, Leistungsverrechnung, Preismodell, Absatzmarkt, Kontrahierungsform, Center-Konzept und Mitarbeiter.

Betreiber- und Geschäftsmodell

Ein Betreibermodell im Kontext des P23R ist ein Geschäftskonzept für die Bereitstellung von Gütern und Dienstleistungen gegen ein leistungsabhängiges Entgelt. Betreibermodelle können somit für die Bereitstellung von physischen Produkten und / oder immateriellen Dienstleistungen gestaltet und etabliert werden. Betreibermodelle können gemäß der folgenden Kriterien klassifiziert, beschrieben und gestaltet werden: Zielgruppe, Zielbranche, Anbieter / Provider, Geschäftsfelder, P23R-Lösung, Musterimplementierung, Make-or-Buy-Entscheidung, Betrieb, Preismodell, Abrechnungsmöglichkeiten.

Datenmodell

Als Datenmodell wird das in den Benachrichtigungsregeln verwendete logische, von der konkreten Implementierung unabhängige Pivot-Datenmodell bezeichnet, um auf die Daten des Benachrichtigungssenders (z. B. eines Unternehmens), die im Datenpool zugänglich sind, zuzugreifen. Aus technischen Gründen wird das Datenmodell noch in Teildatenmodelle unterglie-

dert, gepflegt und verteilt. Ein Teildatenmodell entspricht technisch einem XML-Schema mit einem spezifischen XML-Namensraum.

Das Mapping eines logischen Teildatenmodells in ein konkretes Datenmodell des Quellsystems erfolgt beim zugehörigen SourceConnector.

Datenmodellpaket (Model Package)

Ein Datenmodellpaket (MP) ist eine Menge von Teildatenmodellen, wie sie technisch durch eine P23R-Leitstelle bereitgestellt werden. Ein Datenmodellpaket könnte beispielsweise alle benötigten Teildatenmodelle für eine Fachdomäne enthalten. Darüber hinaus gibt es ein Basis-Datenmodellpaket, das die Teildatenmodelle enthält, die grundsätzlich jeder P23R insbesondere für seine Initialisierung benötigt.

Die Teildatenmodelle in einem Datenmodellpaket werden nach Gesichtspunkten der technischen Verwandtschaft und des Anwendernutzens zusammengestellt. Sie sind in der Regel nicht deckungsgleich mit der Gruppierung in einem fachlichen Benachrichtigungsregelwerk.

Datenpool

Der Datenpool ist die logische Komponente im P23R, die das Abfragen und Zwischenspeichern der Quelldaten (Unternehmensdaten) sowie den Zugriff auf diese regelt. Dazu kann ein Cache genutzt werden, der die Anfragen mit ihren Antworten zwischenspeichert. Alternativ können die Quelldaten im P23R teilweise gespiegelt werden.

Datenschutz

Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch bezeichnet (nicht zu verwechseln mit Datensicherheit).

Datensicherheit

Datensicherheit beziehungsweise IT-Sicherheit bedeutet „die Durchführung aller organisatorischen und technischen Maßnahmen, um das in der Organisation von Unternehmen und Behörden benötigte Niveau an Vertraulichkeit, Verfügbarkeit, Integrität“ und Prüfbarkeit aller verarbeiteten Daten, einschließlich der Programme, sicherzustellen. Für den Bereich des Datenschutzes sind die korrespondierenden Pflichten in der Anlage zu § 9 Satz 1 BDSG konkretisiert.

Quelle: [51]

Domäne (Fachdomäne)

Die Abgrenzung eines Themenbereiches für die Regelerstellung wird im Kontext des P23R-Prinzips als „Fachdomäne“ (kurz: „Domäne“) bezeichnet. Die Abgrenzungskriterien sind unterschiedlicher Art; sie können auf Rechtsgebieten, Verwandtschaft durch Nutzung stark überschneidender Datenmengen, gleichen oder verwandten Überwachungsgegenständen, verwandten Geschäftsprozessen, dem spezifischen Bedarf einer bestimmten Branche oder anderen rationalen Kriterien basieren.

Elektronische Signatur

Die elektronische Signatur beschreibt ein asymmetrisches Verschlüsselungsverfahren zur Gewährleistung der Authentizität und Integrität elektronischer Daten und zur Überprüfung der Identität des Benutzers. Sie ist praktisch mit einer handschriftlichen Unterschrift oder der Möglichkeit, sich eindeutig gegen Vorlage einer Unterschrift auszuweisen, zu vergleichen. Die Rechtswirksamkeit der elektronischen Signaturen wird in Deutschland durch das Signaturgesetz (SigG) geregelt. Hiernach gibt es drei Arten: Die (allgemeine) elektronische Signatur, die fortgeschrittene elektronische Signatur und die qualifizierte elektronische Signatur. Hierbei hat jede Signatur eine bestimmte Qualitätsstufe. Je höherwertiger die Signatur, desto größer ist ihre Bedeutung für den Rechtsverkehr und desto größer ist ihre Funktionalität.

Empfänger

Empfänger bezeichnet eine Behörde oder eine andere Stelle auf Vollzugsebene mit einem gesetzlichen Auftrag, in dessen Rahmen eine Benachrichtigung zu empfangen oder anzufordern ist.

Fachliche Beratungsstellen

Fachliche Beratungsstellen können die Ersteller von Benachrichtigungsregeln methodisch unterstützen sowie bei Bedarf die Entwicklung fachlicher Benachrichtigungsregelsprachen (F-BRS) betreuen. Die Einrichtung und der Betrieb Fachlicher Beratungsstellen liegen in der Verantwortung interessierter Vorschriftengeber bzw. Vorschriftengebergruppen.

Fachübergreifende Koordinierungsaufgaben

Durch das Konzept der Autonomie für die einzelnen P23R-Installationen besteht in einigen Bereichen ein übergreifender Koordinierungsbedarf. Dies kann bspw. folgende Koordinierungsaufgaben betreffen:

- Betrieb des P23R-Depots bei einer Öffentlichen Leitstelle für die Bereitstellung von Benachrichtigungsregel- und Datenmodellpaketen
- Prüfung von Benachrichtigungsregeln und Pflege des Pivot-Datenmodells
- Weiterentwicklung der Technischen Benachrichtigungsregelsprache (T-BRS) bei Bedarf
- Einbindung externer Verzeichnisdienste, wie z. B. „Leistungsverzeichnisse“ und „Zuständigkeitsverzeichnisse“, und weiterer Quellen zur Bereitstellung von Zuständigkeitsinformationen über das P23R-Zuständigkeitsverzeichnis
- Angebot eines Online-Entwickler-Portals, um die Entwicklung der fachlichen Benachrichtigungsregeln zu unterstützen
- Angebot eines Online-Service-Portals, um die Kommunikation mit den P23R-Anbietern und P23R-Betreibern zu unterstützen
- Organisation von Präsenzveranstaltungen zum fachlichen Austausch in und zwischen Interessengruppen, wie z. B. Stakeholdergremien, Communities, fachliche Arbeitsgruppen
- Organisation von Kontakten zu anderen Gremien, die für das P23R-Konzept von Interesse sind.

Fachübergreifende Koordinierungsstelle

Die Fachübergreifende Koordinierungsstelle ist in ihrer Rolle als Dienstleister für den P23R für die Umsetzung der Ziele und Anforderungen des P23R-Prinzips verantwortlich.

Sie übernimmt die zentrale Koordination aller Aufgaben, die über die Erstellung einzelner Benachrichtigungsregeln und -regelgruppen hinausgehen.

Siehe auch *Fachübergreifende Koordinierungsaufgaben*.

Identität

Eine Identität im Sinne der IT-Sicherheit ist die Summe der die Eigentümlichkeit einer Entität erfassenden Merkmale (Attribute und Werte). Die Identität eines Nutzers kann so z. B. über eine eindeutige Nummer innerhalb eines definierten Wertesystems (z. B. Sozialversicherungsnummer) oder über demografische Attribute (Name, Geburtstag, Geburtsort etc.) erfasst werden.

Identitäts- und Berechtigungsmanagement

Das Identitäts- und Berechtigungsmanagement bildet systemübergreifend den Lebenszyklus von Identitäten und Berechtigungen in einem Unternehmen bzw. einer Behörde ab.

Identity Provider

Ein Identity Provider ist ein Infrastrukturdienst, der Zusicherungen über die Authentizität und Identität von Entitäten (i. Allg. Systemnutzern) in einem standardisierten Format bereitstellt.

Informations- und Meldepflichten

Informations- und Meldepflichten sind der Sammelterm für die unterschiedlichen Typen von Prozessketten zwischen Wirtschaft und Verwaltung. Sie umfassen Antragsprozesse, Archivpflichten, Berichte, Meldungen.

Integrität

Bei der elektronischen Kommunikation ist damit die Unversehrtheit von Informationen und Daten gemeint, d. h. dass die Daten bei der Übertragung nicht verändert wurden.

Quelle: [50]

Intermediär

Ein Intermediär ist ein vom Unternehmen beauftragter Dienstleister, der Prozesse für das Unternehmen ganz oder teilweise durchführt. Er wird im P23R repräsentiert durch die Rolle Intermediär. Der Intermediär ist keine globale Rolle (z. B. Steuerberater, Buchhaltungsservice).

IT-Grundschutz

IT-Grundschutz bezeichnet eine Methodik zum Aufbau eines Sicherheitsmanagementsystems sowie zur Absicherung von Informationsverbünden über Standard-Sicherheitsmaßnahmen. Außerdem wird mit IT-Grundschutz der Zustand bezeichnet, in dem die vom BSI empfohlenen Standard-Sicherheitsmaßnahmen umgesetzt sind, die als Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Sicherheitsmaßnahmen, Institutionen mit normalem Schutzbedarf hinreichend absichern.

Quelle: [52]

IT-Sicherheit

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

Quelle: [52]

Kommunikationskanal

Als Kommunikationskanal bezeichnet man die physische Kommunikationsverbindung zwischen dem P23R und dem Benachrichtigungsempfänger, über die Benachrichtigungen versendet werden. Die physische Kommunikation erfolgt im P23R durch die verschiedenen Kommunikationsadapter, die die Protokolle, wie Webservices, E-Mail, Fax usw., implementieren.

Kommunikationsmaßnahmen

Kommunikationsmaßnahmen sind als Aktivitäten definiert, die von einem kommunikationstreibenden Unternehmen bewusst zur Erreichung kommunikativer Zielsetzungen eingesetzt werden.

Quelle: [53]

Kommunikationsmatrix

Die Kommunikationsmatrix ist eine Darstellungsform der Kommunikationsstrategie bei der Kommunikationsinstrumente und -maßnahmen zeitlich integriert und auf konkrete Zielgruppen abgestimmt werden.

Kommunikationsstrategie

Unter einer Kommunikationsstrategie werden Maßnahmen grundsätzlicher Art zur Erreichung von Kommunikationszielen verstanden. Kommunikationsstrategien können sich in Verwendung einzelner, als auch in Kombination mehrerer Kommunikationsinstrumente niederschlagen.

Quelle: [54]

Komponente

Als Komponenten werden im IT-Grundschutz technische Zielobjekte (siehe dort) oder Teile von Zielobjekten bezeichnet.

Quelle: [52]

Konnektor

Ein Konnektor ist eine Komponente ohne eigene Geschäftslogik, die in die Kommunikation zwischen zwei Anwendungen (Systemkomponenten) eingefügt wird, um Datenformate oder Übertragungsprotokolle zwischen unterschiedlichen Schnittstellen anzupassen.

Leitstelle, Öffentliche

Eine Öffentliche Leitstelle ist eine P23R-Leitstelle, die für die Bereitstellung von Öffentlichen Benachrichtigungsregel- und Datenmodellpaketen sowie des Öffentlichen P23R-Zuständigkeitsverzeichnisses zuständig ist. Im Idealfall gibt es genau eine Öffentliche Leitstelle.

Siehe auch *P23R-Leitstelle.*

Meldung

Eine Meldung ist eine Informationsübermittlung von einem Unternehmen an einen Meldungsempfänger im Rahmen einer Prozesskette. Das sind im juristischen Sinne Meldungen, die sich aus den Meldepflichten des Unternehmens ergeben.

Methodenleitfaden (MLF)

Der Methodenleitfaden bildet ein Kompendium aus unterschiedlichen Modulen. Die einzelnen Module des Methodenleitfadens richten sich an Entscheider und Experten, die an der Schnittstelle zwischen Wirtschaft und Verwaltung wirken. Sie unterstützen diese in ihren fachlichen, IT-architektonischen, sicherheitstechnischen, wirtschaftlichen und juristischen Analyse- und Gestaltungsaufgaben. In digitaler Form gibt es einen Methodenleitfaden-Online.

Methodenleitfaden-Online (MLF-Online)

Der Methodenleitfaden Online ist die webbasierte Variante des Methodenleitfadens, der im Projekt Prozess-Daten-Beschleuniger entsteht. Der Methodenleitfaden kann von den Nutzern aus der Öffentlichkeit und Fachöffentlichkeit in rollengeführter Anwendung eingesetzt werden.

Modellierung

Bei der Vorgehensweise nach IT-Grundschutz wird bei der Modellierung der betrachtete Informationsverbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus den IT-Grundschutz-Katalogen nachgebildet. Hierzu enthält Abschnitt 2.2 der IT-Grundschutz-Kataloge für jeden Baustein einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind.

Quelle: [52]

Nachricht (Message)

Eine Nachricht löst die Generierung einer Benachrichtigung aus. Im Standardfall werden interne Nachrichten innerhalb des P23R zeitgesteuert erzeugt, z. B. um gesetzlichen Meldepflichten fristgerecht nachzukommen. Daneben kann auch ein Benachrichtigungsempfänger eine externe (Öffentliche) Nachricht an den P23R senden und damit gezielt eine Benachrichtigung anfordern.

Eine Nachricht bezieht sich immer auf eine Benachrichtigung. Eine Nachricht kann aus zwei Gründen erzeugt werden:

- Die Nachricht fordert ein Unternehmen auf, eine Benachrichtigung zu erzeugen.
- Die Nachricht ist eine Reaktion auf eine vorhergehende Benachrichtigung. Die Nachricht kann eine Eingangsbestätigung, eine Rückfrage, eine Aufforderung zur Korrektur, eine Genehmigung oder Ablehnung eines Antrags oder Ähnliches enthalten.

Art und Form einer Nachricht werden im Rahmen der BR definiert.

Nichtabstreitbarkeit

Nichtabstreitbarkeit ist ein Sicherheitsziel zur Herstellung von Verbindlichkeit in der elektronischen Kommunikation. Nichtabstreitbarkeit stellt sicher, dass ein Kommunikationspartner seine Teilnahme an einem Kommunikationsvorgang (z. B. Senden einer Benachrichtigung) nicht in Abrede stellen kann.

Quelle: [50]

Notfall

Ein Notfall ist ein Schadensereignis, bei dem Prozesse oder Ressourcen einer Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforderten Zeit nicht wieder hergestellt werden. Der Geschäftsbetrieb ist stark beeinträchtigt. Eventuell vorhandene Service Level Agreements können nicht eingehalten werden. Es entstehen hohe bis sehr hohe Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf das Gesamtjahresergebnis eines Unternehmens oder die Aufgabenerfüllung einer Behörde auswirken. Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation.

Quelle: [55]

Notfallkonzept

Das Notfallkonzept umfasst das Notfallvorsorgekonzept und das Notfallhandbuch.

Quelle: [55]

Öffentliche Benachrichtigung (Legal Notification)

Siehe *Benachrichtigung, Öffentliche (Legal Notification).*

Öffentliche Benachrichtigungsregel (Legal Notification Rule)

Siehe *Benachrichtigungsregel, Öffentliche (Legal Notification Rule)*.

Öffentliche Leitstelle

Siehe *Leitstelle, Öffentliche*.

P23R

Unter der Bezeichnung „P23R“ ist derjenige Teil einer P23R-Lösung zu verstehen, der die Generierung und den Versand von Benachrichtigungen über die von der Leitstelle bereitgestellten Regelwerke realisiert. Der Name „P23R“ leitet sich von „Prozess-Daten-Beschleuniger“ ab. P

steht dabei für den ersten Buchstaben, R für den letzten Buchstaben. Dazwischen befinden sich 23 Buchstaben.

P23R-Anwender

Ein P23R-Anwender ist jede natürliche oder juristische Person, die eine P23R-Lösung zur Abwicklung von Informations- und Meldepflichten einsetzt.

P23R-Client

Der P23R selbst stellt ausschließlich Dienstschnittstellen (SOA) zur Verfügung, über die auf seine Funktionalität zugegriffen werden kann. Eine ggf. ergänzende Komponente, die als P23R-Client bezeichnet wird, stellt eine grafische Oberfläche zur Bedienung des P23R bereit. Diese Funktionalität des P23R-Client kann auch direkt in der Unternehmenssoftware integriert sein.

P23R-Depot

Das P23R-Depot stellt Benachrichtigungsregelpakete, die Liste aller Benachrichtigungsregelpakete und die Trusted Service Lists den P23R-Instanzen zur Verfügung. Die Öffentliche Leitstelle hält (mindestens) alle Öffentlichen Benachrichtigungsregeln auf einem Server zum anonymen Download bereit.

P23R-Identity-Assertion

Siehe *Assertion*.

P23R-Identity-Provider

Siehe *Identity Provider*.

P23R-in-a-Box

„P23R-in-a-Box“ ist eine Form der Umsetzung eines Prozessdatenbeschleunigers mit einem eng gekoppelten P23R-Client, bei der auch alle Sicherheitsdienste und die von diesen verarbeiteten Sicherheitsobjekte (Nutzeridentitäten, Nutzerattribute, Berechtigungsregeln) im P23R bzw. im P23R-Client gekapselt sind. Damit bleibt die komplette Sicherheitsarchitektur nach außen verborgen und die Integration erfolgt allein über die in der P23R-Rahmenarchitektur beschriebenen fachlichen Schnittstellen.

P23R-Infrastruktur

Die P23R-Infrastruktur umfasst neben der zentralen Systemkomponente P23R auch den optionalen P23R-Client, die P23R-Leitstelle und den optionalen P23R-TrustedProxy sowie die Definition des P23R-Protokolls.

P23R-inside

Unter einer P23R-inside-Lösung versteht man eine P23R-Lösung, bei der relevante P23R-Architekturelementen in eine bestehende IT-Lösung integriert werden. Solche Lösungen setzen ein gutes Verständnis der Rahmenarchitektur voraus und können diese in unterschiedlichen Ausprägungen implementieren.

P23R-Instanz

Die P23R-Instanz ist eine in Betrieb befindliche Instanziierung des P23R.

P23R-Leitstelle

Eine P23R-Leitstelle ist eine Organisationseinheit, die den Betrieb der P23Rs technisch unterstützt. Sie generiert die Benachrichtigungsregelpakete sowie die Datenmodellpakete und weitere technische Artefakte und stellt diese für den P23R bereit. Darüber hinaus betreibt sie noch weitere Dienste für den P23R, z. B. das P23R-Zuständigkeitsverzeichnis.

Neben einer oder mehreren Öffentlichen Leitstellen kann es in jedem Unternehmen eigene Unternehmensleitstellen geben, die eigene Benachrichtigungsregelpakete und Datenmodellpakete sowie weitere Dienste für das Unternehmen bereitstellen.

Siehe auch *Leitstelle, Öffentliche.*

P23R-Lösung

Eine P23R-Lösung ist eine mögliche Umsetzung der P23R-Rahmenarchitektur durch einen Softwareanbieter oder IT-Dienstleister im Rahmen eines Betreiber- und Geschäftsmodells. Wie diese jeweils ausgestaltet ist, darf im Rahmen der Architektur frei entschieden werden und basiert in der Regel auf einem der beiden Lösungskonzepte P23R-inside und P23R-standalone.

P23R-Lösungsanbieter

Ein P23R-Lösungsanbieter ist ein Softwareanbieter oder IT-Dienstleister, der eine spezifische P23R-Lösung auf Basis der P23R-Rahmenarchitektur einem definierten Kundenkreis im Rahmen eines Betreiber- und Geschäftsmodells anbietet. Der P23R-Provider stellt hierbei eine Sonderform des P23R-Lösungsanbieters dar.

P23R-Mandant

Der P23R-Mandant, in der Regel eine Organisation oder ein Unternehmen (juristische Person) oder eine natürliche Person, ist eine Rolle im organisatorischen und juristischen Verhältnis zwischen dem Nutzer eines P23R und einem P23R-Provider. Der P23R-Mandant nutzt eine vom Provider bereitgestellte P23R-Instanz, genauer gesagt eine P23R-Mandanteninstanz eines P23R.

P23R-Mandanteninstanz

Die P23R-Mandanteninstanz ist ein Nutzer einer P23R-Instanz, der eigene getrennte Ressourcen besitzt, bspw. eigene Datenhaltung und eigene aktivierte Benachrichtigungsregeln. Die P23R-Mandanteninstanz fasst alle Aspekte einer P23R-Instanz zusammen, die genau einen Mandanten betreffen. Man kann sie so betrachten, als ob die P23R-Instanz einzeln genau nur für diesen Mandanten betrieben würde. Das betrifft vor allem die getrennte Datenhaltung und die Unabhängigkeit der Verarbeitungsprozesse.

P23R-Musterimplementierung

Die P23R-Musterimplementierung ist die im Rahmen des Projekts „Pilotierung und Realisierung eines Prozess-Daten-Beschleunigers (P23R) für den Datenaustausch zwischen Wirtschaft und Verwaltung“ entstandene Open-Source-Musterimplementierung einer P23R-standalone-Lösung. Diese umfasst eine Umsetzung des P23R (inkl. pilotrelevanter Kommunikationskonnektoren), des P23R-Client, sowie einer Laborleitstelle mit Zuständigkeitsverzeichnis.

P23R-Prinzip

Das Prinzip Prozess-Daten-Beschleuniger (P23R-Prinzip) beschreibt Methoden und Architekturkonzepte zur effizienten Gestaltung von Prozessen zwischen Wirtschaft und Verwaltung. Es zielt darauf ab, Prozessketten zwischen Wirtschaft und Verwaltung sinnvoll zu bündeln und zentral bereitgestellte Regelwerke für die automatisierte Abwicklung von Informations- und Meldepflichten zu nutzen.

P23R-Provider

Ein P23R-Provider stellt einem P23R-Mandanten die technische Infrastruktur zur Verfügung, mit der der Mandant in der Lage ist, die Funktionalität des P23R zu nutzen. Der P23R-Provider hat keinen Einblick in die im P23R enthaltenen Daten und Profile.

Es wird nicht zwischen internen und externen P23R-Providern unterschieden, da beide als Dienstleister gemäß IT Infrastructure Library (ITIL) zu betrachten sind.

P23R-Rahmenarchitektur

P23R-Rahmenarchitektur ist ein Dokument, das einen konzeptionellen Überblick über die vollständige Infrastruktur des Prozess-Daten-Beschleunigers (P23R) und deren Systemkomponenten, die Schnittstellen und die verwendeten Datenstrukturen in den Teilkomponenten des P23R sowie ihr Zusammenspiel liefert. Sie soll den Entwicklern eine klare Vorstellung davon geben, welche Funktionalität jede Teilkomponente des P23R bzw. Systemkomponente der P23R-Infrastruktur haben sollte und wie ein mögliches Systemdesign aussehen könnte.

P23R-Sicherheitsarchitektur

P23R-Sicherheitsarchitektur ist ein Dokument, das einen konzeptionellen Überblick über die vollständige Sicherheitsinfrastruktur des Prozess-Daten-Beschleunigers (P23R) und den Systemkomponenten der Sicherheitsarchitektur, die Schnittstellen und die verwendeten Datenstrukturen in den Sicherheits-Teilkomponenten des P23R sowie ihr Zusammenspiel im Kontext der P23R-Rahmenarchitektur liefert. Sie soll den Entwicklern eine klare Vorstellung davon geben, welche Funktionalität jede Teilkomponente der P23R-Sicherheitsarchitektur im Kontext der P23R-Rahmenarchitektur bzw. der zu implementierenden bzw. zu nutzenden Systemkomponenten der P23R-Infrastruktur haben sollte und wie ein mögliches Systemdesign aussehen könnte.

P23R-standalone

Unter einer P23R-standalone-Lösung versteht man eine P23R-Lösung, die einen eigenständigen P23R – sprich nicht in eine vorhandene IT-Lösung integrierte P23R-inside-Lösung – realisiert.

P23R-TrustedProxy

Standardmäßig kommunizieren der P23R und das Fachverfahren direkt über ein eigenes Protokoll. Der P23R-TrustedProxy als optionale Komponente der P23R-Infrastruktur bietet eine besonders sichere und vertrauenswürdige Kommunikation. Er wird direkt in der internen Infrastruktur bereitgestellt und erlaubt eine vereinfachte Kommunikation im Intranet mit dem P23R.

Der P23R-TrustedProxy ist der Stellvertreter des P23R in der eigenen Infrastruktur und realisiert alle Sicherheitsfunktionen zwischen P23R und Proxy. Ein P23R-TrustedProxy kann durch ein spezielles Deployment eines P23R realisiert werden.

P23R-Unterstützungsstellen

P23R-Unterstützungsstellen ist ein Begriff für die Gesamtheit föderativ verteilter Organisationseinheiten. Diese führen Koordinationsaufgaben durch, die einerseits den Betrieb der P23R-Infrastruktur operativ und andererseits die Erstellung der benötigten Benachrichtigungsregeln unterstützen sowie ggf. deren Konzepte weiterentwickeln. Möglich sind eine Öffentliche Leitstelle, eine Fachübergreifende Koordinierungsstelle sowie eine dem Bedarf anpassbare Anzahl von Fachlichen Beratungsstellen.

P23R-Zuständigkeitsverzeichnis

Ein P23R-Zuständigkeitsverzeichnis ist erforderlich, um eine Benachrichtigungsregel im P23R eines Unternehmens zu konkretisieren. Mit seiner Hilfe wird anhand der aktuellen Unternehmenscharakteristik und entsprechend den Vorgaben in der Benachrichtigungsregel ein zuständiger Benachrichtigungsempfänger zugeordnet. Weitere Informationen sind Angaben zur Kommunikation mit dem Benachrichtigungsempfänger und zur erforderlichen Darstellung der Benachrichtigung.

Die Öffentliche Leitstelle ist für die technische Verfügbarkeit der Informationen verantwortlich. Der Betreiber des P23R-Zuständigkeitsverzeichnisses ist nicht notwendigerweise auch der Betreiber der erforderlichen Original-Verzeichnisse. Die erforderlichen Zuständigkeitsinformationen können aus einem zentralen oder aus einem verteilten, föderativen System stammen oder speziell für die Benachrichtigungsregel erstellt werden. Die für die Funktion des P23R erforderlichen Informationen müssen jedoch über das P23R-Zuständigkeitsverzeichnis in einem einheitlichen Format bereitgestellt werden.

Die Anbindung von externen Verzeichnissen an das P23R-Zuständigkeitsverzeichnis ist eine der Unterstützungsaufgaben.

Pivot-Datenmodell

Das Pivot-Datenmodell vermittelt die Semantik zwischen den verschiedenen Semantiken der Quelldatenmodelle (Unternehmensdatenmodelle) zu den verschiedenen Semantiken der Benachrichtigungstypen im P23R (Mapping). Es dient gleichzeitig der Definition des internen Datenmodells. Es ist nicht notwendigerweise ein kanonisches oder normalisiertes Datenmodell.

Siehe auch *Datenmodell.*

Policy

Eine Policy ist ein Regelwerk, aus dem sich Entscheidungen herleiten lassen. Im Rahmen der P23R-Sicherheitsarchitektur werden Policies zur Kodierung von Berechtigungen (Berechtigungspolicies) und zur Steuerung des Dienstzugangs (Sicherheitspolicies) verwendet.

Policy Administration Point (PAP)

Über einen Policy Administration Point wird der Lebenszyklus einer Policy gesteuert. Insbesondere erfolgt über den Policy Administration Point als Teil des Berechtigungsmanagements auch die Bereitstellung von Policies zur Nutzung im Rahmen einer Berechtigungsprüfung.

Policy Decision Point (PDP)

Ein Policy Decision Point kapselt die Funktionalität zur Prüfung einer Zugriffsanfrage gegen Berechtigungspolicies.

Policy Enforcement Point (PEP)

Ein Policy Enforcement Point setzt das Designmuster eines Reference Monitors um, der Kontrollflüsse vor dem Zugriff auf geschützte Ressourcen unterbricht, um von einem Policy Decision Point eine Berechtigungsentscheidung abzufragen.

Policy Information Point (PIP)

Ein Policy Information Point erlaubt einen on-demand Abruf von Attributwerten, die zur Auswertung einer Policy erforderlich sind. Ein Policy Information Point fungiert dabei als Zugang zu bestehenden Informationssystemen im Unternehmen.

Pool

Ein Pool ist die allgemeine Bezeichnung für Daten- und Informationssammlungen. Ob die Daten dabei in einer Datenbank, in XML-Dateien oder anders abgelegt werden, spielt keine Rolle.

Protokollierung (Logging)

Protokollierung von technischen Ereignissen, z. B. zur Erleichterung einer Fehlerdiagnose oder zur Überwachung der Systemauslastung.

Prozess

Ein Prozess ist eine logische, zielgerichtete Folge von Funktionen, die zur Schaffung eines Produktes oder einer Dienstleistung dienen und in einem direkten Zusammenhang stehen. Prozesse transformieren Inputfaktoren zu einem Outputfaktor.

Prozess-Daten-Beschleuniger

Der Prozess-Daten-Beschleuniger (P23R) ist die zentrale Komponente der P23R-Infrastruktur. Der P23R generiert auf Anforderung automatisch eine Benachrichtigung gemäß den vorliegenden Regeln. Er verwendet dazu die vorab vom Unternehmen bereitgestellten Daten. Bevor eine Benachrichtigung an den Benachrichtigungsempfänger versendet wird, muss diese durch das Unternehmen freigegeben werden. Der P23R stellt nur Webservices im Sinne einer SOA bereit.

Prozesskette

Eine Prozesskette kann als eine logische Verknüpfung von Prozessen gesehen werden. Prozessketten stellen damit eine Kette zusammenhängender Prozesse dar, die zur Erstellung einer Dienstleistung oder eines Produkts (Wertschöpfungsorientierung) sowie zu einem gemeinsamen (Geschäfts-)Prozessziel führen sollen.

PRK-Typ I Wertschöpfungsorientierte Prozessketten: Diese Prozessketten beschreiben Wertschöpfungsprozesse, bei denen ein Unternehmen mit mehreren anderen Unternehmen und Verwaltungen interagieren muss. Sie zeichnen sich in der Regel durch eine hohe Anzahl an Prozessteilnehmern sowie durch eine komplexe Ablauflogik aus.

PRK-Typ II Datenorientierte Prozessketten: Diese Prozessketten beschreiben Prozesse, deren zentrales Element die daten- und ereignisgetriebene Übermittlung von Daten von den Unternehmen an die Verwaltung ist. Die in einer Prozesskette zwischen den Teilnehmern ausgetauschten Daten und Dokumente fließen oftmals auch in weitere Prozesse, so dass es zu Datenredundanzen kommt. Prozessketten vom Typ II zeichnen sich in der Regel durch eine geringe Anzahl an Prozessteilnehmern und durch eine einfache Ablauflogik aus. Die auszutauschenden Daten und Dokumente müssen im Prozess aufbereitet und an spezifische Formate angepasst werden. Sie weisen i. Allg. einen hohen Grad an Komplexität und Vertraulichkeit auf.

Prozesskettenbündel

Prozesskettenbündel bezeichnen die systematische Verbindung von mehreren Prozessketten zwischen Wirtschaft und Verwaltung mit dem Ziel, Effizienz, Effektivität sowie die Qualität von Informationen für alle Beteiligten zu verbessern. Es gibt unterschiedliche Kriterien, nach denen Prozesskettenbündel gebildet werden können.

In Abhängigkeit der angewendeten Kriterien unterscheidet man in Prozesskettenbündelung vom Typ I und Prozesskettenbündelung vom Typ II. Das Architekturkonzept des Prozess-Daten-Beschleunigers beschreibt technische Komponenten, die zur effizienten IT-Unterstützung von Prozesskettenbündeln eingesetzt werden können.

Prozesskettenbündelung Typ I

Bei der Prozesskettenbündelung vom Typ I werden Prozessketten zwischen Wirtschaft und Verwaltung mit einander verbunden, die entlang einer Wertschöpfungskette im Unternehmen auftreten. Solche Prozesskettenbündel sind durch eine hohe Anzahl von Akteuren und hohe Frequenz gekennzeichnet, da sie jedes Mal im Zusammenhang mit der Wertschöpfungskette im Unternehmen auftreten. Ziel der Bündelung ist eine möglichst reibungslose, medienbruchfreie Abwicklung der Wertschöpfungskette im Unternehmen sowie die effiziente Erfüllung gesetzlicher Informationspflichten. Ein Beispiel für eine derartige Prozesskettenbündelung vom Typ I ist die Vergabe von privaten Immobilienkrediten (vgl. [30]). Analysekriterien für die Identifikation von Prozessketten, die nach Typ I gebündelt werden können sind: Zugehörigkeit zu einem Wertschöpfungs- bzw. zu einem Prozess-Cluster Die Prozesskette wird ausgelöst durch den Wertschöpfungsprozess im Unternehmen, wie z. B. Meldung, Antrag, Registerauskunft.

Prozesskettenbündelung Typ II

Bei der Prozesskettenbündelung vom Typ II werden Prozessketten zwischen Wirtschaft und Verwaltung mit einander verbunden, die durch eine inhaltliche Überschneidung gekennzeichnet sind. Prozessketten, die gleiche oder ähnliche Inhalte zum Gegenstand haben werden mit einander so verbunden, dass sie nur noch eine gemeinsame Informationsbasis nutzen. Berichts- oder Meldedaten müssen auf diese Weise nicht mehr redundant ermittelt, gepflegt und archiviert werden. Ziel ist es, Berichts- und Meldepflichten an unterschiedliche Adressaten auf Verwaltungsseite möglichst effizient und mit hoher Informationsqualität abwickeln zu können. Analysekriterien für die Identifikation von Prozessketten, die nach Typ II gebündelt werden können, sind: Übereinstimmung von Inhalt, Unternehmenstyp des Informationspflichtigen und Richtung des Informationsflusses (von Wirtschaft zu Verwaltung).

PRTR

Das PRTR (Pollutant Release and Transfer Register) ist ein Register für Schadstoffemissionen in der Luft, in den Böden, in Gewässern, in externen Kläranlagen sowie für entsorgte, gefährliche und nicht-gefährliche Abfälle. Das Register ist öffentlich im Internet zugänglich und informiert über insgesamt 91 Schadstoffe, die von großen Industriebetrieben freigesetzt werden. das PRTR verfolgt das Ziel, die Öffentlichkeit für Umweltfragen zu sensibilisieren und an der Entscheidungsfindung im Umweltbereich zu beteiligen. Darüber hinaus soll die Umweltleistung von Unternehmen verbessert werden.

Quelle: [56]

Public Key Infrastruktur (PKI)

Eine Public Key Infrastruktur umfasst alle Systeme zur Steuerung und Abwicklung des Lebenszyklus digitaler Zertifikate. Hierzu zählen z. B. die Ausstellung von Zertifikaten über eine Certificate Authority und die Prüfung der Gültigkeit von Zertifikaten gegen eine Sperrliste.

Quellsystem (Source Application)

Mit Quellsystem wird das Softwaresystem beim Benachrichtigungssender bezeichnet, das die Daten für die Generierung der Benachrichtigungen in einem P23R bereitstellt.
Das kann bspw. das IT-Fachsystem eines Unternehmens sein.

Reference Monitor

Ein Reference Monitor ist ein Designmuster für die Kontrolle und Durchsetzung von Zugriffsberechtigungen. Ein Reference Monitor kapselt eine zu schützende Ressource vollständig (complete mediation) und stellt sicher, dass jeder Zugriffsversuch auf diese Ressource mit definierten Zugriffsregeln abgeglichen wird. In der P23R Sicherheitsarchitektur wird ein Reference Monitor durch das Access Control Subsystem realisiert. Die Anbindung an die Anwendungsarchitektur erfolgt über Policy Enforcement Points (PEPs), die aus den Abläufen der Anwendung heraus den Übergang zum Access Control Subsystem der Sicherheitsarchitektur bilden.

Rollen

Jeder Mitarbeiter erfüllt innerhalb seines Tätigkeitsprofils bestimmte Aufgaben, die Rollen definieren. Rollen können auch im Zusammenhang mit Anwendungsfällen definiert werden. Über diese Rollen werden Berechtigungen definiert, z. B. Zugriffsrechte auf Daten oder Schnittstellen einer Anwendung.

Schutzbedarf

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Quelle: [52]

Schutzbedarfsfeststellung

Bei der Schutzbedarfsfeststellung wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen und der IT-Komponenten bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der Grundwerte der Informationssicherheit – Vertraulichkeit, Integrität oder

Verfügbarkeit – entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“.

Quelle: [52]

Security Token

Ein Security Token (Sicherheitstoken) kodiert eine Assertion (Zusicherung) in einer Form, die die Integrität der Assertion und die Authentizität des Erstellers sichert und für den Nutzer der Assertion überprüfbar macht.

Security Token Service (STS)

Ein Security Token Service stellt Security Token aus. Ein Beispiel für einen Security Token Service ist ein Identity Provider, der Identity Assertions in Form von Sicherheitstoken erstellt.

Serviceorientierte Architektur

Serviceorientierte Architekturen (SOA) beschreiben fachliche Architekturkonzepte zur Vernetzung und Verwendung verteilter Dienste bzw. Services (meist Webservices). Dabei werden die Anwendungsbausteine (Services) lose miteinander gekoppelt und je nach Bedarf zu umfassenden Diensten und Dienstleistungen verbunden (Service-Orchestrierung). E-Government-Architekturen basieren zunehmend auf SOA-Konzepten.

Sicherheitsdienst

Ein Sicherheitsdienst trägt innerhalb einer Sicherheitsarchitektur zur Umsetzung von einem oder mehreren Sicherheitszielen (Vertraulichkeit, Integrität, Verfügbarkeit) bei. Beispiele für Sicherheitsdienste sind Nutzerauthentifizierung und Zugriffskontrolle.

Sicherheitskonzept

Ein Sicherheitskonzept dient zur Umsetzung der Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele einer Institution zu erreichen. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

Quelle: [52]

Sicherheitsmaßnahme

Mit Sicherheitsmaßnahme (kurz Maßnahme) werden alle Aktionen bezeichnet, die dazu dienen, um Sicherheitsrisiken zu steuern und um diesen entgegenzuwirken. Dies schließt sowohl organisatorische, als auch personelle, technische oder infrastrukturelle Sicherheitsmaßnahmen ein. Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt. Als englische Übersetzung wurde „safeguard“, „security measure“ oder „measure“ gewählt. Im englischen Sprachraum wird neben „safeguard“ außerdem häufig der Begriff „control“ verwendet.

Quelle: [52]

Sicherheitsobjekt

Sicherheitsobjekte sind in Bezug auf ihre Integrität, Authentizität und ggf. auch Vertraulichkeit besonders abgesicherte Objekte, die als Ankerpunkte für darauf aufsetzende Sicherheitsmechanismen dienen. Beispiele für Sicherheitsobjekte sind kryptografische Schlüssel und Identifizierer.

Single Sign-On

Bei einem Single Sign-On wird eine einmalig durchgeführte, über ein Sicherheitstoken bestätigte Authentifizierung von mehreren Systemen akzeptiert. Ein Nutzer kann so mit einer Anmeldung auf durch verschiedene Systeme verwaltete Ressourcen zugreifen.

SourceConnector (Quelldatenkonnektor)

Der SourceConnector ist eine externe Systemkomponente, die nicht zum P23R gehört, und typischerweise vom Hersteller der SourceApplication oder dem P23R-Betreiber bereitgestellt wird. Der SourceConnector muss die normative Schnittstelle ISourceDataRead für den P23R bereitstellen, damit dieser auf die Daten der SourceApplication zugreifen kann. Ob der SourceConnector eine separate Systemkomponente oder eine in die SourceApplication integrierte Schnittstelle ist, ist der Implementierung selbst überlassen, solange die Schnittstelle realisiert wird.

Stakeholder

Als Stakeholder wird eine natürliche Person (der Mensch in seiner Rolle als Rechtssubjekt) oder eine juristische Person (z. B. eine Institution) bezeichnet, die ein Interesse am Verlauf oder Ergebnis des P23R-Projekts hat.

Quelle: [57]

Trust Store

In einem Trust Store verwaltet ein System als vertrauenswürdig deklarierte Zertifikate. Signaturen, die auf Zertifikate verweisen, die nicht im Trust Store enthalten sind bzw. über ihre Zertifikatskette nicht auf ein im Trust Store registriertes Zertifikat zurückgeführt werden können, DÜRFEN von dem System NICHT akzeptiert werden.

Trusted Service List (TSL)

Zur Bekanntgabe von Zertifikaten und Schnittstellen vertrauenswürdiger Dienste werden entsprechende Dokumente als Trusted Service List publiziert. Syntax und Semantik dieser Dokumente werden durch den Standard ETSI TS 102 231 [47] definiert.

Unternehmenscharakteristik

Die Unternehmenscharakteristik ist die Menge aller relevanten Eigenschaften eines Unternehmens, die zur Bestimmung der durch den P23R zu empfehlenden Benachrichtigungsregelgruppen und -regeln erforderlich sind.

Unterstützungsaufgaben

Hier handelt es sich um die Gesamtheit an Aufgaben, die die erfolgreiche Umsetzung des P23R-Prinzips unterstützen. Dies sind bspw. die Fachübergreifende Koordinierungsaufgaben,

die technische Bereitstellung der Benachrichtigungsregel- und Datenmodellpakete sowie Beratungsaufgaben bei der Erstellung von Benachrichtigungsregeln.

Siehe *Fachübergreifende Koordinierungsaufgaben*.

Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Quelle: [52]

Version

Der Begriff Version wird verwendet, um verschiedene zeitliche Zustände der gleichen Daten zu beschreiben. Jede Änderung von Daten erzeugt eine neue Version (eine neue Instanz) dieser Daten. Beim P23R müssen ältere Versionen archiviert werden, d. h. sie dürfen nicht verloren gehen oder gelöscht werden. Änderungen, z. B. die Beseitigung eines Schreibfehlers in einem Attribut, Datenergänzungen etc., werden vom Unternehmen angestoßen und vom Datenpool erzeugt.

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

Quelle: [52]

Verzeichnisdienst

Ein Verzeichnisdienst ist ein Infrastrukturdienst, der Informationen (Attributwerte) zu hierarchisch strukturierten Entitäten eines Typs zur Verfügung stellt.

Vorschriftengeber

Vorschriftengeber ist in der Regel der Gesetzgeber. In einigen Fällen ist die Situation komplexer. Dies gilt dann, wenn der Gesetzgeber nur einen Rechtsrahmen schafft, der von einer anderen Körperschaft auszugestalten ist (z. B. Rechtsrahmen für die Berufsgenossenschaften oder die Ausgestaltung von Durchführungsverordnungen). In solchen Fällen müssen alle beteiligten Stellen an den Aufgaben des Vorschriftengebers mitwirken. Nur indirekt betroffen sind die Empfänger auf Vollzugsebene.

Webservice

Ein Webservice ist eine interoperable Softwareschnittstelle, die über XML beschrieben ist und die über in XML kodierte Nachrichten angesprochen wird.

Wert

Werte sind alles, was wichtig für eine Institution ist (Vermögen, Wissen, Gegenstände, Gesundheit).

Quelle: [52]

Zertifikat

Ein (digitales) Zertifikat bindet mit Hilfe einer digitalen Signatur einen öffentlichen Schlüssel an eine Identität. Eine digitale Signatur, die gegen diesen öffentlichen Schlüssel geprüft werden kann, ist damit der an diesen Schlüssel gebundenen Identität zuzuordnen. Zertifikate bilden Hierarchien, an deren Spitze ein von einer vertrauenswürdigen Stelle selbst zertifiziertes Zertifikat steht.

Zertifizierung

Als Zertifizierung wird die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz bezeichnet.

Zielgruppe

Als Zielgruppen wird eine bestimmte Menge von Stakeholdern bezeichnet, die auf kommunikationspolitische Maßnahmen homogener reagieren als die Gesamtmenge aller Stakeholder.

Quelle: [54]

Zugang

Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen, wie IT-Systeme bzw. System-Komponenten und Netze, zu nutzen.

Quelle: [52]

10 ABKÜRZUNGSVERZEICHNIS

BMI	Bundesministerium des Innern
BR	Benachrichtigungsregel
BRP	Benachrichtigungsregelpaket
BRW	Benachrichtigungsregelwerk
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
DIT	Directory Information Tree
DSML	Directory Services Markup Language
DVDV	Deutsches Verwaltungsdiensteverzeichnis
EP	Entry Point (Einsprungspunkt)
ETSI	European Telecommunications Standards Institute
F-BRS	Fachliche Benachrichtigungsregelsprache
FTP	File Transfer Protocol
IP	Internet Protocol
HR	Human Resources
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
KMU	Kleine und mittlere Unternehmen
LDAP	Lightweight Directory Access Protocol
MARM	Model and Rule Management
OASIS	Organization for the Advancement of Structured Information Standards
OSCI	Online Services Computer Interface
P23R	Prozess-Daten-Beschleuniger
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PKI	Public Key Infrastructure
PRK	Prozesskette
RFC	Request for Comments
RST	Request Security Token
RSTR	Request Security Token Response
SAML	Security Assertion Markup Language
SFTP	Secure File Transfer Protocol
SigG	Signaturgesetz
SOA	Serviceorientierte Architektur
SOAP	Simple Object Access Protocol
STS	Security Token Service
S/MIME	Secure / Multipurpose Internet Mail Extensions

T-BRS	Technische Benachrichtigungsregelsprache
TLS	Transport Layer Security
TSL	Trusted Service List
TSP	Trusted Service Provider
UML	Unified Modeling Language
URL	Uniform Resource Locator
WS	Webservice
WSDL	Web Services Description Language
WSS	Web Services Security
WS-*	Sammelbegriff für auf WSS aufbauende Standards, wie z. B. WS-Trust und WS-SecureConversation
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

11 REFERENZEN

Alle in diesem Kapitel aufgeführten Ergebnisdokumente des P23R-Projekts werden unter www.p23r.de bereitgestellt werden.

[1] J. Baum et al. (2012), *P23R: Rahmenarchitektur.* (Ergebnisdokument des P23R-Projekts)

[2] ISO - International Organization for Standardization (2000), ISO 7498-2:1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2,* Security Architecture.

[3] J. Baum et al. (2012), *P23R: Sicherheitskonzept.* (Ergebnisdokument des P23R-Projekts)

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI), *IT-Grundschutz-Kataloge: 11. Ergänzungslieferung.* Verfügbar unter: https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/kataloge.html (zuletzt abgerufen am 07.11.2012).

[5] J. Baum et al. (2012), *P23R: Spezifikationen zur Sicherheitsarchitektur.* (Ergebnisdokument des P23R-Projekts)

[6] S. Bradner (1997), *Key words for use in RFCs to Indicate Requirement Levels (RFC 2119).* Verfügbar unter: http://tools.ietf.org/html/rfc2119 (zuletzt abgerufen am 07.11.2012).

[7] P. Schaar (2010), *Privacy by Design,* Identity in the Information Society, Bd. 3, Nr. 2, S. 267-274.

[8] J. Gottschick, H. Hartenstein und R. Rosenmüller (2012), *Anforderungen an die Ausgestaltung und Umsetzung des P23R-Prinzips.* (Ergebnisdokument des P23R-Projekts)

[9] J. Apitzsch (2009), *OSCI-Transport, Version 2.0* - Technical Features Overview. OSCI-Leitstelle.

[10] Bundesamt für Sicherheit in der Informationstechnik (BSI), *BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise*. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html (zuletzt abgerufen am 07.11.2012).

[11] D. F. C. Brewer und M. J. Nash (1989), *The Chinese Wall Security Policy,* in IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, S. 206-214.

[12] O. Boehm et al. (2008), *Federated Authentication and Authorization: A Case Study,* Enterprise Distributed Object Computing Conference, S. 356-362.

[13] J P. Anderson (1972), *Computer Security Technology Planning Study Volume II.*

[14] J. H. Saltzer und M. D. Schroeder (1975), *The Protection of Information in Computer Systems,* Proceedings of the ACM, Bd. 63, Nr. 9, S. 1278-1308.

[15] D. S. Wallach et al. (1997), *Extensible security architectures for Java,* in Proceedings of the sixteenth ACM symposium on Operating systems principles - SOSP 97, S. 116-128.

[16] M. Benantar (2009), *Access Control Systems: Security, Identity Management and Trust Models,* Springer US.

[17] D. F. Ferraiolo, D. R. Kuhn und R. Chandramouli (2007), *Role-Based Access Control,* 2. Auflage, Artech House Inc, London.

[18] U.S. Department of Homeland Security, *Build Security In - Principles.* Verfügbar unter: https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/principles.html (zuletzt abgerufen am 07.11.2012).

[19] Verein elektronische FallAkte e.V. (2011), *Elektronische FallAkte*. Verfügbar unter: http://www.fallakte.de/ (zuletzt abgerufen am 07.11.2012).

[20] epSOS, *epSOS - Smart Open Services for European Patients*. Verfügbar unter: http://www.epsos.eu/ (zuletzt abgerufen am 07.11.2012).

[21] STORK, *STORK - Secure Identity Across Borders Linked*. Verfügbar unter: https://www.eid-stork.eu/ (zuletzt abgerufen am 07.11.2012).

[22] CCRA (2009), *Common Criteria and Common Evaluation Methodology Version 3.1 Release 3*. Verfügbar unter: http://www.commoncriteriaportal.org/cc/ (zuletzt abgerufen am 22.11.2012)

[23] R. Kuhlisch, J. Caumanns und O. Boehm (2010), *Deklarative Sicherheit zur Spezifikation und Implementierung der elektronischen Fallakte,* in 55. GMDS-Jahrestagung, Mannheim.

[24] A. S. Vedamuthu et al. (2007), *Web Services Policy 1.5 - Framework.* W3C.

[25] A. Nadalin et al. (2007), *WS-SecurityPolicy 1.2. OASIS*.

[26] T. Moses (2005), *eXtensible Access Control Markup Language (XACML)* Version 2.0. OASIS.

[27] KoopA ADV, *Verwaltungs-PKI*. Verfügbar unter: http://www.koopa.de/projekte/pki.html (zuletzt abgerufen am 21.03.2011).

[28] H. Krcmar et al. (2009), *Machbarkeitsstudie Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung: Umwelt.* Verfügbar unter: http://www.p23r.de/publikationen/ (zuletzt abgerufen am 17.11.2011).

[29] K.-P. Eckert et al. (2009), *Machbarkeitsstudie Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung: Informations- und Meldepflichten für Arbeitgeber.* Verfügbar unter: http://www.p23r.de/publikationen/ (zuletzt abgerufen am 17.11.2011).

[30] N. Fröschle et al. (2009), *Machbarkeitsstudie Entwicklung von Prozessketten zwischen Wirtschaft und Verwaltung: Finanzdienstleistungen.* Verfügbar unter: http://www.p23r.de/publikationen/ (zuletzt abgerufen am 17.11.2011).

[31] A. Nadalin et al. (2007), *WS-Trust 1.3.* OASIS.

[32] S. Cantor et al. (2005), *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.*

[33] C. Allen und T. Dierks (1999), *The TLS Protocol Version 1.0 (RFC 2246)*. Verfügbar unter: http://tools.ietf.org/html/rfc2246 (zuletzt abgerufen am 07.11.2012).

[34] M. Wahl (1997), *A Summary of the X.500(96) User Schema for use with LDAPv3 (RFC 2256)*. Verfügbar unter: http://tools.ietf.org/html/rfc2256 (zuletzt abgerufen am 07.11.2012).

[35] J. Caumanns et al. (2009), *IHE White Paper on Access Control*. Verfügbar unter: http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf (zuletzt abgerufen am 07.11.2012).

[36] C. Neuman et al. (2005), *The Kerberos Network Authentication Service (V5) (RFC 4120)*. Verfügbar unter: http://tools.ietf.org/html/rfc4120 (zuletzt abgerufen am 07.11.2012).

[37] J. Kemp et al. (2005), *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*.

[38] F. Clauder, H. Hartenstein und R. Rosenmüller (2012), *P23R: Spezifikationen zur Rahmenarchitektur*. (Ergebnisdokument des P23R-Projekts)

[39] OASIS (2002), *Directory Services Markup Language v2.0*. Verfügbar unter: http://www.oasis-open.org/committees/dsml/docs/DSMLv2.doc (zuletzt abgerufen am 20.11.2012).

[40] S. Mark (2000), *Definition of the inetOrgPerson LDAP Object Class (RFC 2798)*. Verfügbar unter: http://tools.ietf.org/html/rfc2798 (zuletzt abgerufen am 07.11.2012).

[41] S. Cantor et al. (2005), *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*.

[42] D. Eastlake et al. (2008), *XML Signature Syntax and Processing (Second Edition). W3C*.

[43] A. Nadalin et al. (2006), *Web Service Security: SOAP Message Security 1.1. OASIS*.

[44] T. Imamura, B. Dillaway und E. Simon (2002), *XML Encryption Syntax and Processing. W3C*.

[45] S. Turner und B. Ramsdell (2010), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification (RFC 5751)*. Verfügbar unter: http://tools.ietf.org/html/rfc5751 (zuletzt abgerufen am 07.11.2012).

[46] S. Murphy et al. (1995), *Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted (RFC 1847)*. Verfügbar unter: http://tools.ietf.org/html/rfc1847 (zuletzt abgerufen am 07.11.2012).

[47] ETSI Technical Committee Electronic Signatures and Infrastructures (2009), *ETSI TS 102 231 Version 3.1.2 - Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status Information*. Verfügbar unter: http://www.etsi.org/deliver/etsi_ts/102200_102299/102231/03.01.02_60/ts_102231v030102p.pdf (zuletzt abgerufen am 13.08.2011).

[48] J. Hughes et al. (2005), *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.*

[49] ITU-T Recommendation X.680 (2008), *Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[50] Bundesamt für Sicherheit in der Informationstechnik (2006), *Das E-Government-Glossar*. Verfügbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/476872/publicationFile/31173/6_EGloss_pdf.pdf (zuletzt abgerufen am 07.11.2012).

[51] P. Kramer und M. Meints, „Datenschutz“, in: *Handbuch Multimedia-Recht,* T. Hoeren und U. Sieber (Hrsg.), 23. Auflage. München: Beck, 19. Einzellieferung vom 19. März 2008., Teil 16.5, Rn. 3 ff.

[52] Bundesamt für Sicherheit in der Informationstechnik (BSI), *IT-Grundschutz-Glossar*. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html (zuletzt abgerufen am 31.10.2012).

[53] M. Bruhn (2007), *Kommunikationspolitik*, 4. überarbeitete Auflage, Verlag Franz Vahlen GmbH, München.

[54] Gabler Verlag (Hrsg.), *Gabler Wirtschaftslexikon*, Verfügbar unter: http://wirtschaftslexikon.gabler.de/Archiv/81506/kommunikationsstrategie-v5.html (zuletzt abgerufen am 07.11.2012).

[55] Bundesamt für Sicherheit in der Informationstechnik (BSI), *BSI Standard 100-4: Notfallmanagement.* Verfügbar unter: https://www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf (zuletzt abgerufen am 29.10.2012).

[56] Umweltbundesamt (2010), *Leitfaden für die Durchführung der PRTR-Berichtspflicht*. Verfügbar unter: http://www.umweltbundesamt.at/fileadmin/site/publikationen/REP0164.pdf (zuletzt abgerufen am 29.11.2012).

[57] R. Olbrich (2009), *Marketing – Eine Einführung in die marktorientierte Unternehmensführung*, 2. Auflage, Springer-Verlag GmbH, Heidelberg.

Herausgeber
Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

Kontakt
info@p23r.de
www.p23r.de

Redaktion
Johannes Einhaus, Fraunhofer FOKUS
Dominique Leikauf, :::tsm total-sourcing-management
Petra Steffens, Fraunhofer FOKUS

Layout und Satz
Marie Luise Birkholz, Fraunhofer FOKUS
Simone Geppert, Fraunhofer FOKUS

www.p23r.de