Technologieintegrierte Datensicherheit bei RFID-Systemen

Ulrich Waldmann, Fraunhofer Institut für Sichere Informationstechnologie (SIT), Darmstadt

Kurzfassung

Die Pharmaindustrie spielt eine Vorreiterrolle bei der Einführung von RFID auf der Ebene von Einzelpackungen in der Lieferkette. Dabei kann das mittelfristig zu erwartende RFID-Anwendungsszenario "Fälschungssicherheit von Medikamenten" einen Mehrwert gegenüber den heutigen Barcode-Anwendungen bringen. Dieser Beitrag betrachtet ein speziell für den Pharmabereich entwickeltes RFID-System, das auf Basis der EPCglobal-Architektur den elektronischen Herkunftsnachweis und die Produktauthentisierung unterstützt. Mit Blick auf die Medikamentensicherheit werden weitergehende Sicherheitsanforderungen definiert und als Sicherheitsmaßnahmen die Überprüfung der Tag-Kennungen und des Herkunftsnachweises, die kryptographische Authentisierung des Tags und die Überprüfung des Produktes anhand einer nachweislichen Tag/Produkt-Beziehung gefordert. Dazu sind neue Verfahren der Produktauthentisierung gefragt, wobei One-Time-Codes und physikalische Fingerprints entwicklungsfähige Ansätze sind, die langfristig gute Lösungen für den Fälschungsschutz bringen könnten.

1 Sicherheit von RFID-Systemen

Dieser Beitrag konzentriert sich auf die Sicherheit an der RFID-Luftschnittstelle zur drahtlosen Informationsübertragung, da die Sicherheitsaspekte der anderen Systemkomponenten wie RFID-Middleware, Datenbanken und Backend-Systeme bereits ausführlich in Verbindung mit den Internet-Technologien betrachtet werden. Die RFID-Frontends sind vor allem den folgenden Angriffen ausgesetzt [3], [9]:

- Sniffing
- Spoofing
- Replay-Angriffe
- Denial-of-Service-Angriffe
- Relay-Angriffe
- Unautorisiertes Tracking.

Angreifer können die Angriffe kombinieren, um z.B. Leseprozesse zu verhindern (z.B. in automatisierten Prüfsystemen), Diebstahl zu vertuschen, Produktionsdaten zu manipulieren oder RFID-Transponder zu klonen und für Produktfälschungen zu verwenden. Um einen Missbrauch der RFID-Technologien zu vermeiden, muss daher die Sicherheit von RFID-Systemen optimiert werden, wobei neben der Funktionssicherheit Aspekte der Datensicherheit (Echtheit, Integrität, Vertraulichkeit, Verfügbarkeit, Verbindlichkeit) und der Datenschutz wichtig sind.
Die zurzeit erhältlichen RFID-Transponder besitzen nur sehr begrenzte Sicherheitsfunktionalität. Die EPC Class1 Generation2 Tags sind passive Low-Cost Tags und die EPCglobal-Spezifikationen bieten noch kein übergreifendes Sicherheitskonzept [7]. Zukünftige Spezifikationen von RFID-Tags sowie entsprechende Daten- und Kommunikationsstandards (z.B. EPC Class2) werden jedoch die Ziele der Datensicherheit und des Datenschutzes berücksichtigen müssen. Neue Methoden zur Authentisierung und Autorisierung, Verschlüsselung, Integritätsschutz, Pseudonymisierung, Deaktivierung von Tags und Verhinderung von nicht autorisierten Lese- und Schreibzugriffen sind Gegenstand aktueller Forschung. Da die Tagkosten niedrig zu halten sind, müssen neue effektive Methoden für eine gegenseitige Authentisierung von Transponder und Lesegerät entwickelt werden. Für die Kommunikation steht nur ein begrenzter Zeitrahmen zur Verfügung. Klassische Methoden wie hash-basierte starke Authentisierung erfordern viel Rechenleistung und komplizierte Hardware. Die bekannten symmetrischen und asymmetrischen Verschlüsselungsverfahren sind schlecht einsetzbar, da der Aufwand für ein sicheres Schlüsselmanagement in offenen Lieferketten unverhältnismäßig hoch ist. Zudem besteht bei ungenügend manipulationsgeschützten Low-Cost Tags z.B. die Gefahr, dass ein Angreifer durch physikalische Analysen der Tags die geheimen Schlüssel ermittelt, wodurch ganze Sicherheitskonzepte kompromittiert werden können. Folglich werden sichere Verfahren der Lightweight-Kryptographie gebraucht, einschließlich effektiver Methoden für die Generierung von Zufallszahlen und Hashwerten auf Tags. Neue Konzepte wie die Physical Uncloneable Functions (PUFs) könnten einen Ausweg aus dem Kostendilemma zeigen, in das die Implementierung von Sicherheit bisher steckt.
Dieser Beitrag fasst einige Ergebnisse der gleichnamigen RFID-Sicherheitstudie zusammen, die vom Bundesministerium für Bildung und Forschung (BMBF) gefördert und im Frühjahr 2007 veröffentlicht wurde [23]. In der Studie werden drei RFID-Anwendungsszenarien behandelt: "Identifikation von Bauteilen in der Automobilproduktion", "Identifikation von Konsumgütern in der Lieferkette des Einzelhandels" und die "Fälschungssicherheit von Medikamenten in der pharmazeutischen Lieferkette". Die folgenden Abschnitte fassen die Untersuchung des dritten Szenarios zusammen.

2 Fälschungssicherheit von Medikamenten mit RFID

2.1 Motivation

In diesem Anwendungsszenario soll mittels RFID nicht nur die Effizienz der Medikamentenlieferkette verbessert, sondern auch die Fälschungssicherheit von Medikamenten erhöht werden. Die WHO schätzt den Anteil von Fälschungen am Gesamtumsatz, der mit Medikamenten erzielt wird, auf 10-30% in den Entwicklungsländern und mindestens 1% in den Industrieländern, wobei Fälschungen aufgrund zunehmender Importe, Reimporte und Parallelimporte und aufgrund des Internet-Handels stark zunehmen (siehe **Bild 1**). So sind mehr als 50% der im Internet ohne Adressangabe angebotenen Medikamente Fälschungen.

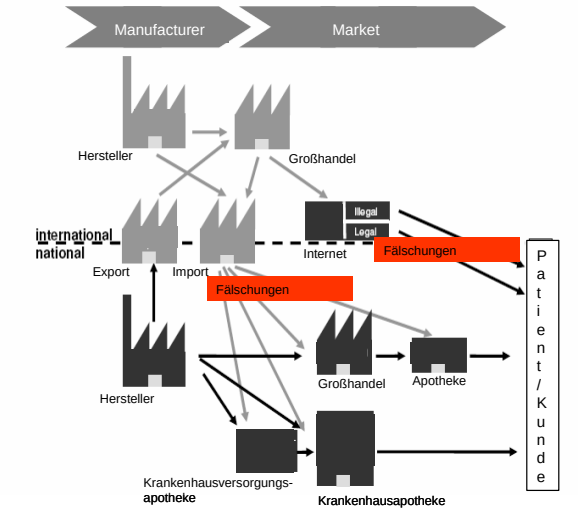

Bild 1 Komplexität der Medikamentenlieferkette [19]

Der Kampf gegen Fälschungen wird zurzeit mit Informationskampagnen, politischen Richtlinien und speziellen Verpackungslösungen geführt. Um die Echtheit nachzuweisen, müssen pharmazeutische Wirkstoffe oder für diesen Zweck zugesetzte geheime Marker aufwändig geprüft werden. Neue Maßnahmen wie aufwändiges Verpackungsdesign, Hologramme oder neue Barcodeverfahren können innerhalb kurzer Zeit professionell nachgeahmt werden [19].
Die US-amerikanische Food and Drug Administration (FDA) empfiehlt daher den Einsatz des elektronischen Herkunftsnachweises auf Basis von RFID für jede gehandelte Verpackungseinheit [5]. Den Konzepten von EPCglobal als standardisierte RFID-Gesamtlösung werden die größten Chancen eingeräumt [4], [11], [13], [15].
Im Gegensatz zu den Entwicklungen in den USA streben die europäische Pharmaindustrie und der Großhandel die Einführung des zweidimensionalen Barcodes (Data Matrix) auf Basis der EAN 128-Daten an. Zudem existieren nationale Kodierungen für Medikamente, die sich nicht auf die EPC abbilden lassen, z.B. in Deutschland die Pharmazentralnummer (PZN). Der Großhandel hält die heutigen RFID-Lösungen für technisch unausgereift und ungeeignet für die Lagerverwaltung, für die das Haltbarkeitsdatum und die Chargennummer auch offline wichtig wären. Folgende Argumente werden gegen RFID und die EPCglobal-Architektur genannt: Hohe Kosten und ungeklärte Zuständigkeiten für die RFID-Infrastruktur (Datenbanken, Netzwerke), Existenz unterschiedlicher inkompatibler Technologien (z.B. verschiedene Frequenzen), mangelnde Funktionssicherheit (Leseraten, Übetragungsgeschwindigkeiten), die noch undefinierten Anwendungsfälle für die RFID-Daten und nicht zuletzt die noch unerforschten Auswirkungen, die RFID auf Menschen und Substanzen haben könnte.
Daher gibt es bis heute in Europa keinen ernsthaften Ansatz, RFID flächendeckend in die pharmazeutischen Lieferketten zu integrieren. Dennoch scheint gerade die pharmazeutische Lieferkette für RFID qualifiziert zu sein: Ein vorteilhaftes Verhältnis von hohen Produktwerten zu den entstehenden RFID-Kosten und der Einfluss höherer Werte wie Gesundheit [24], welche der Echtheitsprüfung von Medikamenten einen hohen Stellenwert einräumen. Der RFID-basierte Schutz gegen Fälschungen könnte daher trotz der nicht hundertprozentigen Leseraten gegenüber den heutigen Barcode-Anwendungen einen Mehrwert bringen.

2.2 RFID-basierte pharmazeutische Lieferkette

Betrachtet wird eine RFID-Lösung von IBM, die zur Absicherung von pharmazeutischen Lieferketten in den USA bereits im Einsatz ist. Andere Technologiehersteller (wie SAP) stellen ähnliche Systeme her. Das Ziel der Implementierungen ist der Echtheitsnachweis der Medikamente und die Möglichkeit, die Medikamentenpackungen an jeder Stelle der Lieferkette orten und zurückverfolgen zu können (Tracking and Tracing). Das System basiert auf der EPCglobal Architektur, die den Electronic Product Code (EPC) verwendet. Mit dem EPC ist eine eindeutige Identifikation jeder Produkteinheit möglich (siehe **Bild 2**).

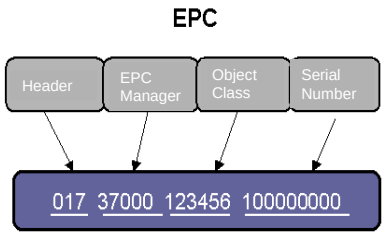

Bild 2 Electronic Product Code nach EPCglobal

Auf Basis des EPC werden in EPC Information Services (EPCIS) die Produkt- und Transaktionsinformationen gespeichert und können von anderen Teilnehmern der Lieferkette abgerufen werden (siehe **Bild 3**).

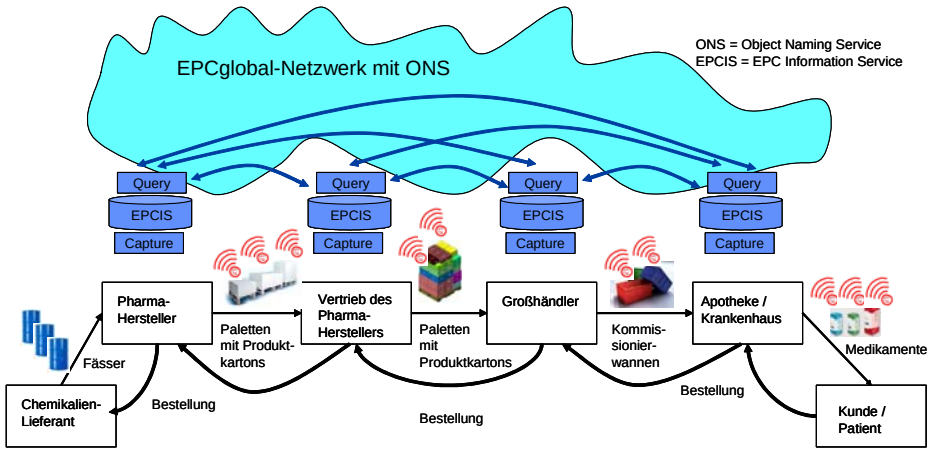

Bild 3 RFID-basierte Medikamentenlieferkette (IBM)

Jeder Partner in der Lieferkette legt dazu selbst fest, welche Informationen er auf seinem lokalen EPCIS-Server zur Verfügung stellt und welche Partner er mit rollenbasierten oder individuellen Zugriffsrechten ausstattet. Der Zugang zu den EPCIS-Servern erfolgt mittels XML-Anfragen über das EPC-Netzwerk. Die auf den Tags gespeicherten Daten sind dabei auf ein Minimum beschränkt: Eine eindeutige Chipkennung (Tag-ID), die vom Chiphersteller eingeschrieben und gegen Überschreiben geschützt ist ("Burnt-In Code") und dem EPC. Der Pharmahersteller schreibt den EPC in den Tag und registriert das Produkt unter der Kombination beider Kennungen. Das System realisiert mittels RFID-Middleware eine strikte Trennung von Datenerfassung (durch die RFID-Hardware), Datenabfrage (durch den externen Zugang zum EPCIS) und den firmeninternen Anwendungen (z.B. ERP-Systemen). Die EPCIS-Daten werden nicht unter den Netzteilnehmern verteilt oder synchronisiert, sondern bleiben an ihrem lokalen Entstehungsort. Ausgewählte Daten werden nur auf Nachfrage übermittelt, können aber abonniert werden, so dass Teilnehmer die Lieferdaten vor der eigentlichen Produktlieferung erhalten. Ein weiteres Prinzip ist die Verwendung des elektronischen Herkunftsnachweises, der sich aus Informationen der einzelnen EPCIS-Quellen zusammensetzt und noch von dort einzeln abgerufen werden muss. Geplant ist der Abruf der gesamten Information in einem Schritt geschützt mit digitalen Signaturen.

2.3 Sicherheitsbetrachtung der Echtheitsprüfung

Das vorgestellte System unterstützt den Nachweis der Produktechtheit. Dieser Nachweis beruht auf dem Auslesen der Tag-ID und des EPC und der Anfrage an den Produkthersteller, ob das Produkt unter der Kombination beider Kennungen registriert ist. Ist die Antwort negativ, gehören die Kennungen vermutlich zu einem gefälschten Produkt. Das System meldet auch das Vorhandensein von Duplikaten, falls mehrere Anfragen die gleichen Kennungen enthielten und offensichtlich auf verschiedenen unvereinbaren Lieferwegen gestellt wurden. Auf Grundlage einer solchen Anfrage kann jedoch nicht entschieden werden, welches der Produkte echt und welches eine Fälschung ist.

Die Sicherheit der Echtheitsprüfung basiert auf der Annahme, dass die "Burnt-In" Chip-Kennungen nicht kopiert werden können. Da die industriellen Anwender vor allem an der Leistungsfähigkeit und Funktionssicherheit der RFID-Systeme interessiert sind wurden Aspekte der Datensicherheit weniger beachtet. Die Gründe hierfür sind vorrangige Probleme der Funktionssicherheit: Die schwierigen Lesebedingungen an der Luftschnittstelle, die hohen Geschwindigkeiten der Verpackungslinien, die hohen Aggregatdichten, die heterogenen Materialien (Flüssigkeiten, Metalle) und Verpackungsformen der pharmazeutischen Produkte und nicht zuletzt die gewünschte Minimierung der Kosten. Welche Frequenz (HF oder UHF) auf der Ebene von Einzelpackungen verwendet werden sollte, ist noch immer eine offene Frage unter den Anwendern und sollte weiter untersucht werden [1], [17], [18], wobei die im Vergleich jüngere UHF-Technologie noch großes Entwicklungspotential besitzt. Das vorgestellte System verwendet preiswerte HF-Tags auf Ebene der Einzelpackungen und UHF-Tags auf Ebene der Produktkartons und Paletten.

Das folgende Beispiel eines Angriffsszenarios soll verdeutlichen, dass die Sicherheit, die der Echtheitsprüfung zugrunde liegt, noch verbesserungsfähig ist. Ein Fälscher könnte die Kommunikation zwischen Tag und Lesegerät mithören oder gültige Tags aktiv auslesen (Sniffing), um Tags zu klonen und diese für gefälschte Produkte zu verwenden. Jeder RFID-Leser, der das EPC-Protokoll der Luftschnittstelle unterstützt, kann die EPC-Daten von Low-Cost Tags auslesen. Fälscher könnten außerdem Zugang zu frei pro-

grammierbaren Tags oder zur Chipherstellung gewinnen, so dass auch die Tag-IDs nicht wirklich sichere Einträge darstellen.
Ebenso wenig bietet der elektronische Herkunftsnachweis genügend Sicherheit für Echtheitsprüfungen, da die nachweisbar authentische Information kopierbar ist bzw. die gleiche Information von mehreren gefälschten Produkten mit dem gleichen duplizierten EPC referenziert werden kann. Zudem bleibt die Information verteilt in den originalen EPCIS, so dass beispielsweise ein betrügerischer Großhändler seine EPCIS-Daten nach einer Produktlieferung manipulieren (und wiederum signieren) könnte, ohne dass die anderen Teilnehmer imstande sind, diese als gefälschte Information zu identifizieren.
Eine weitere Sicherheitslücke der Echtheitsprüfung würde bestehen, falls die Verbindung zwischen Tag und Produkt nicht manipulationssicher ist: Angreifer könnten Tags von abgelaufenen oder zurückgezogenen Produkten entfernen und die Tags zur Kennzeichnung gefälschter Medikamente verwenden. Eine gesicherte physische und logische Verknüpfung von Tag und Produkt ist daher wichtig.
Die folgenden Sicherheitsstufen stellen ein Vorschlag für eine umfassende Sicherheitslösung der Echtheitsprüfung dar, wobei jeder Schritt das Sicherheitsniveau der voran gegangenen Schritte erweitert [6],[14],[16]:

- **Sicherheitsstufe 1**: Prüfung der Tag-Kennungen
- **Sicherheitsstufe 2**: Prüfung anhand eines elektronischen Herkunftsnachweises
- **Sicherheitsstufe 3**: Prüfung mittels kryptographischer Tag-Authentisierung
- **Sicherheitsstufe 4**: Prüfung des Produktes anhand einer gesicherten Tag / Produkt-Beziehung

Der folgende Abschnitt beschreibt entsprechende Sicherheitsmaßnahmen, die zur Erreichung dieser Sicherheitsstufen eingesetzt werden können.

2.4 Sicherheitsmaßnahmen der Echtheitsprüfung

Zur Erreichung der **Sicherheitsstufe 1** ist eine Registrierung und Abfrage von Tag-Kennungen notwendig, die bereits realisierbar ist (siehe oben).
Die **Sicherheitsstufe 2** beinhaltet den Vergleich dieser Kennungen mit den Angaben im Herkunftsnachweis und eine Plausibilitätsprüfung des Lieferweges, den das getaggte Produkt genommen hat. Im Gegensatz zu den verteilten Informationen der IBM-Lösung, sollte der Herkunftsnachweis als ganzes erweiterbares Dokument parallel zum Weg, den das Produkt nimmt, an die Partner der Lieferkette gesendet werden [12]. Die Datenstruktur eines solchen Herkunftsnachweises wurde bereits bei EPCglobal spezifiziert [8], siehe **Bild 4**. Jeder Teilnehmer fügt seine Informationen hinzu und signiert den gesamten Herkunftsnachweis einschließlich aller bereits vorhandenen Signaturen. Alle enthaltenen digitalen Signaturen sind nacheinander überprüfbar, so dass Teile der Information nicht nachträglich geändert werden können.

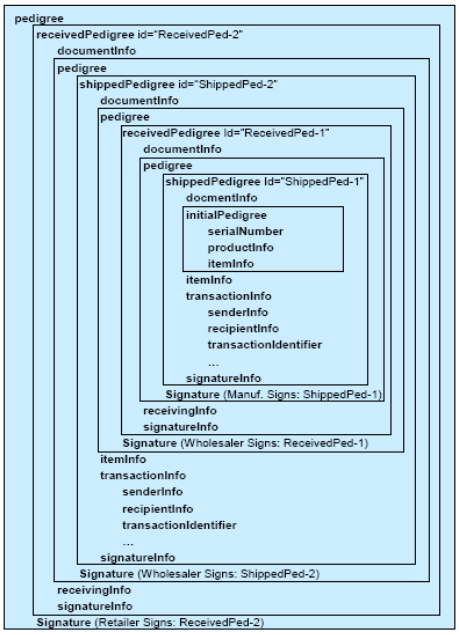

Bild 4 Struktur eines Herkunftsnachweises (Beispiel)

Die **Sicherheitsstufe 3** wird durch eine Authentisierung des Tags erreicht, durch welche der originale Speicherort der in Sicherheitsstufe 1 geprüften Kennungen und andere Tagdaten nachgewiesen wird. Eine starke Authentisierung nach einem Challenge-Response Protokoll mit tag-individuellen nicht kopierbaren kryptographischen Schlüsseln stellt aus der Perspektive der Sicherheit eine wirksame Lösung gegen das Klonen von Tags dar.
Jedoch wird dazu die kryptographische Funktionalität von Mikroprozessorchips benötigt, welche mit der geforderten Beschränkung auf Low-Cost Tags kaum vereinbar ist. Die gesetzlichen Regelungen hinsichtlich der vom Lesegerät ausgestrahlten Leistung, der nutzbaren Frequenzen und Bandbreiten sowie die erwartete Gesamtleistung des Systems schränken zusätzlich die zulässige Rechenzeit und den Stromverbrauch kryptographischer Tags stark ein [21].
Die Leistungsaufnahme der Tags kann durch ein intelligentes Chip-Design verringert werden [20]. Heutige Low-Cost Tags besitzen aber nur etwa 5.000-10.000 elektronische Gatter, von denen maximal 3.000 für Sicherheitsfunktionen zur Verfügung stehen. Das ist nicht genug, um die bekannten kryptographischen Algorithmen zu unterstützen [26]. Hardware-basierte Implementierungen von RSA (1024 Bit) oder AES (128 Bit) brauchen ca. 67.000 bzw. 20-30.000 Gatter. Für Geräte mit beschränkten Ressourcen existieren aber bereits Lightweight-Implementierungen, die einen Großteil der Berechnungen in die Software verlegen. Lightweight-ECC (163 Bit), Lightweight-AES (128 Bit) und Lightweight-DES (112 Bit) kommen

inzwischen mit 15.094, 3.595 bzw. 2.168 Gattern aus und zeigen, dass weiter optimiert werden kann.
Andere Verfahren der Lightweight- und Minimalist-Cryptography beschränken sich auf einfache XOR-Bit-Operationen und sind damit aus Sicht des Tags sehr effizient. Sie entlasten die Tags, sind aber in Bezug auf die Generierung, Diversifikation und Synchronisation von kryptographischen Schlüsseln und den notwendigen Datenbank- und Serverzugriffen ähnlich komplex wie die mathematisch-anspruchsvollen Algorithmen [21],[26]. Die meisten dieser Verfahren scheinen ungeeignet für offene Lieferketten, wenn jede Medikamentenpackung mit ihrem Tag einen individuellen Schlüssel besitzen soll, welcher jedem Teilnehmer der Lieferkette bekannt bzw. in Echtzeit verfügbar sein muss. Zudem stellen Low-Cost Tags keine sicheren Speicherorte für Schlüssel dar.
One-Time-Codes wären für preiswerte Tags ideal, da sie ebenfalls nur einfache XOR-Operationen zur Verschlüsselung und Entschlüsselung von Daten benötigen und zudem eine unübertreffliche Sicherheit bieten, solange der Code wirklich zufällig und geheim ist und nur einmal verwendet wird. Die Forschung befasst sich mit der Generierung und Synchronisierung dieser Codes für langfristig sichere und preiswerte Lösungen [10].
Die Suche nach neuen Verfahren z.B. im Bereich der Physical Uncloneable Functions (PUFs) könnte langfristig Authentisierungsverfahren bringen, die ganz ohne kryptographische Schlüssel auskommen. PUFs nutzen winzige Materialunterschiede aus, die aus unkontrollierbaren oder unbekannten Abweichungen im Herstellungsprozess stammen. Beispielsweise zeigt eine PUF-Schaltung auf bestimmte Eingabedaten charakteristische Antworten ganz ähnlich der Funktionalität eines geheimen Schlüssels (siehe **Bild 5**).

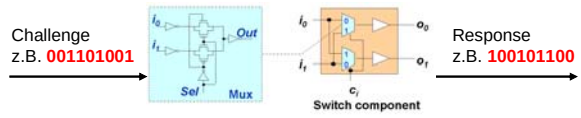

Bild 5 PUF-Schaltung

Das individuelle Verhalten einer PUF-Schaltung lässt sich nicht kopieren und es gibt keine Schlüsseldaten, die geschützt werden müssten. Eine solche Schaltung kann in einen Tag integriert werden, wobei die individuellen Antworten auf ausgewählte Challenges gemessen und gespeichert werden müssen, um als Referenzdaten für Authentisierungsverfahren zur Verfügung zu stehen. Auftretende Spannungseffekte, welche die PUF-Antwort teilweise unzuverlässig machen, und geeignete Protokolle zur Tag-Authentisierung sind Gegenstand aktueller Forschung [21].
Produktfälschungen werden bereits durch das bloße Vorhandensein von Tags und vor allem durch eine Authentisierung des Tags erschwert. Die **Sicherheitsstufe 4** aber erfordert zusätzlich den Nachweis, dass der authentisierte Tag auch wirklich zur Produktpackung gehört, welche mit den beglaubigten Tag-Daten referenziert wird. Der Tag sollte manipulationssicher am Produkt befestigt oder in das Verpackungsmaterial eingelassen sein, z.B. als Inlay in Behältern mit Siegelverschluss.
Neue Verfahren der Produktauthentisierung sollten äußere Sicherheitsmerkmale des Produkts, z.B. optische Eigenschaften oder sensor-basierten Manipulationsschutz, in RFID-Systeme integrieren. Eine Produktauthentisierung könnte sich z.B. auf maschinenlesbaren Barcode, aufgedruckte Tag-Daten, Produktbilder, Copy Detection Pattern oder Hologramme stützen, die mittels EPC und Herkunftsnachweis dem Anwender mitgeteilt werden, um z.B. für eine manuell-unterstützte Echtheitsprüfung des Medikaments in der Apotheke zur Verfügung zu stehen.
Die so genannten Physical One-Way Functions (POWFs) können mittelfristig gute Lösungen bieten. Die am MIT entwickelten Prototypen verwenden Laserlicht als Eingabe zu einem optischen Medium, einer dreidimensionalen Mikrostruktur mit zufällig eingeschlossenen Partikeln [22]. Jede dieser Mikrostrukturen erzeugt unter Bestrahlung ein individuelles Interferenzmuster, das in ein charakteristisches Bitmuster umgewandelt werden kann (siehe **Bild 6**).

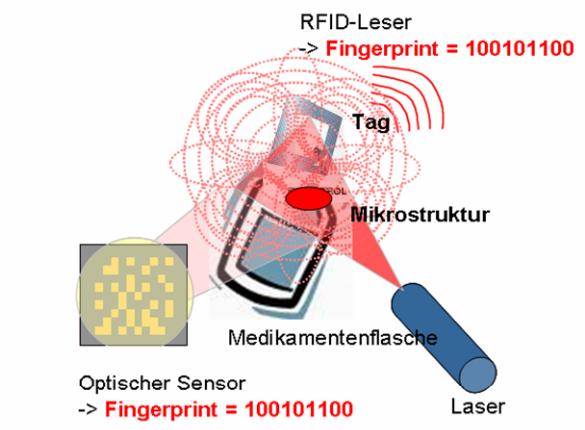

Bild 6 Produktauthentisierung mittels POWF

Die Interferenzmuster stellen physikalische Fingerprints dar, deren Daten auf dem jeweiligen Produkttag gespeichert werden können, um für die folgenden Schritte der Produktauthentisierung verfügbar zu sein:

- **Schritt 1**: Tag-Authentisierung
- **Schritt 2**: Lesen der Fingerprint-Daten (Tag)
- **Schritt 3**: Messen d. Fingerprints (Mikrostruktur)
- **Schritt 4**: Vergleich beider Datensätze

Eine elegante POWF-Lösung bietet die "Laser Surface Authentication"-Technologie, die zur fälschungssicheren Authentisierung von Verpackungen entwickelt wurde und bereits industrietauglich ist [2]. Mittels Laserlicht wird ein Objekt, z.B. eine Produktverpackung, anhand seiner individuellen nicht kopierbaren

Oberflächenstruktur (Pappe, Kunststoff oder Metall) eindeutig erkannt und ist anschließend anhand der in einer Datenbank hinterlegten Scan-Daten (125-750 Bytes) verifizierbar. Eine Kombination mit RFID-Technologien wäre vielversprechend.

3 Ausblick

Die Forschung sollte sich hinsichtlich RFID-basierter Verfahren zur Fälschungssicherheit auf Verfahren konzentrieren, welche mit preiswerten Tags vereinbar sind, allerdings ohne sich auf Anforderungen von EPCglobal zu beschränken. Aktuelle Forschungsgebiete sind z.B. die Interoperabilität der RFID-Komponenten, die Verbesserung der RFID-Hardware (insbesondere UHF-Tags und Leser), die Entwicklung geeigneter kryptographischer Lightweight-Verfahren und die Schaffung von anwendungsspezifischen Sicherheitsprotokollen für die Authentisierung von Tags und Produkten. Das Potential preiswerter physikalischer Fingerprints sollte in den Sicherheitsprotokollen der Echtheitsprüfung genutzt werden. Eine erste Kombination von physikalischen Fingerprints (auf Grundlage von PUFs), digitaler Signaturen und ECC-basierter Authentisierung wurde bereits realisiert [25]. Die Entwicklung von Sensoren für passive Tags, welche Manipulationen am Produkt erkennen und dem RFID-System melden, wird weitere Möglichkeiten der automatischen Echtheitsprüfung von Produkten eröffnen.

4 Literatur

[1] ADT/Tyco Fire & Security, Alien Technology, Impinj, Intel, Symbol, Xterprise: RFID and UHF: A prescription for RFID success in the pharmaceutical industry, June 2006

[2] Bayer Technology Services; Ingenia Technology: Hermes Award für Identifikationstechnologie ProteXXion, www.bayertechnology.com

[3] BSI: Risiken und Chancen des Einsatzes von RFID-Systemen, 2004

[4] Büchel, P. B.; Platzen, O.: RFID-Technologie zur Verhinderung von Arzneimittelfälschungen, Pharm. Ind. 68, Nr. 10, 1153-1157, 2006

[5] Combating Counterfeiting Drugs: A Report of the Food and Drug Administration Annual Update, US Department of Health and Human Services, 2005

[6] Duc, D. N.; Lee, H.; Kim, K.: Enhancing security of EPCglobal Gen-2 RFID against traceability and cloning, Auto-ID Labs Information and Communication University, 2006

[7] EPCglobal: EPC Class-1 Generation-2 UHF RFID Protocol for Communication at 860 MHz – 960 MHz, Version 1.0.9, January 2005

[8] EPCglobal: Pedigree Ratified Standard, Version 1.0, January 2007

[9] Garfinkel, S.; Rosenberg, B.: RFID – Applications, Security, and Privacy, Addison-Wesley, 2006

[10] Ghosal, R.; Jantscher, M.; Grasso, A. R.; Cole, P. H.: One time codes, Auto-ID Labs University of Adelaide, 2006

[11] GS1 Germany: Fälschungssicherheit per EPC, Über EPC und EPCglobal-Netzwerk Warenechtheit gewährleisten, März 2006

[12] Harrison, M.; Inaba, T.: Improving the safety and security of the pharmaceutical supply chain, Auto-ID Labs, 2006

[13] Healthcare Distribution Management Association (HDMA): EPC and Healthcare Distribution: Current State of the Industry, November 2004

[14] Inaba, T.: EPC System for safe & secure supply chain and How it is applied, Auto-ID Labs Keio University, 2006

[15] Koh, R.; Staake, T.: Nutzen von RFID zur Sicherung der Supply Chain d. Pharmaindustrie, 2005

[16] Lehtonen, M.; Staake, T.; Michahelles, F.; Fleisch, E.: The potential of RFID and NFC in anti-counterfeiting, Auto-ID Labs ETH Zürich und Uni St. Gallen, 2006

[17] Magellan technology: A comparison of RFID frequencies and protocols, March 2006

[18] ODIN technologies laboratories: Pharmaceutical item level RFID: Battle of the frequencies, March 2006

[19] Platzen, O.: Die Eignung eines Auto-ID-Systems zur Reduzierung von Arzneimittelfälschung im Auftragsabwicklungsprozess zwischen Hersteller und Handel in Deutschland, Diplomarbeit Uni Regensburg, 3.2.2006

[20] Rabaey, J.; Pedram, M.: Low-Power Design Methodologies, Kulwer Academic Publishers, 1996

[21] Ranasinghe, D. C.; Cole, P. H.: Security in low cost RFID, Auto-ID Labs University of Adelaide, 2006

[22] Ravikanth, P. S.: Physical One-Way Functions, MIT, March 2001

[23] Sohr, K.; Hollstein, T.; Waldmann, U.: Technologieintegrierte Datensicherheit bei RFID-Systemen, Studie gefördert vom BMBF, Kz. 16SV3505, Mai 2007

[24] Stiehler, A.; Wichmann, T.: RFID im Pharma- und Gesundheitssektor, Berlecon, 2005

[25] Tuyls, P.; Batina, L.: RFID-Tags for Anti-counterfeiting, CT-RSA 2006, LNCS 3860, pp. 115-131, Springer-Verlag, 2006

[26] Yu, Y.; Yang, Y., Fan, Y., Min, H.: Security scheme for RFID tag, Auto-ID Labs Fudan University, 2006