Trusted EPC Administration*

- RFID SysTech 2009 (final paper) -

Peter Sakal, Benedikt Iltisberger, Thomas Stein, Micha Hastrich, Hartmut Pohl
Informationssicherheit, Fachbereich Informatik, Hochschule Bonn–Rhein–Sieg

08.05.2009

1 Einleitung

RFID-Transponder dienen der Identifizierung von Produkten, der Zuordnung von Produkten zu Personen, der Fälschungssicherheit und weiteren Anwendungsgebieten [18]. Durch RFID-Transponder sollen Technologien wie z.B. der Barcode (teilweise) abgelöst werden. Einige Unternehmen sehen eine Koexistenz zwischen den Technologien, da die alte Technologie zur Zeit noch kostengünstiger ist.

Einige Branchen, wie z.B. Produktion, Logistik und Handel, können von der Technologie profitieren. Die RFID-Transponder bringen gegenüber alten Technologien viele Vorteile. RFID ermöglicht die Verarbeitung eines größeren Datenvolumens, es ist kein direkter Sichtkontakt zum Lese-/Schreibgerät erforderlich und mehrere Transponder können gleichzeitig ausgewertet werden [14]. Business-to-Business (B2B) Anwender erhoffen sich einen effizienteren und transparenteren Beschaffungsprozess, welcher im Rahmen des Supply-Chain-Managements Vorteile bringen kann.

Diese Arbeit legt ihren Schwerpunkt auf die Echtzeitüberwachung während des gesamten Produktlebenszyklus. Zur weltweit eindeutigen Identifikation von Objekten werden dazu in RFID-Transpondern item-level Identifikationsnummern wie der EPC (Electronic Product Code) verwendet [7].

* Gefördert vom Bundesministerium für Bildung und Forschung im Rahmen des Programms 'KMU-innovativ': Verbundprojekt EOMS: RFID in der Logistik - Offene Systeme auf der Basis von EPC und ONS'. Teil des Forschungsschwerpunkts 'NEGSIT - Next Generation Services in Heterogeneous Network Infrastructures' der Hochschule Bonn-Rhein-Sieg

Datenbanken von Produktherstellern referenzieren auf diesen EPC. Dadurch sollen Geschäftspartner und Endverbraucher in die Lage versetzt werden Informationen über das Produkt abfragen zu können. Dies können z.B. Produktbestandteile, Herstellungs- und Vertriebsdaten, sowie Informationen über den Stammbaum sein.

Bisher erarbeitete RFID Standards, Protokolle und proprietäre Lösungen beinhalten nur unvollständige Implementierungen von Sicherheitsaspekten [19]. Dies führt für viele Anwendungsbereiche, einschließlich des hier betrachteten Szenarios, zu einer unzureichenden Widerstandsfähigkeit im Hinblick auf Angriffe gegen die Integrität, Vertraulichkeit und Verfügbarkeit, sowie gegen die Anonymität der RFID-Lösung. Angriffsmöglichkeiten sind dabei auf verschiedenen Schichten und Objekten gegeben [6].

2 EPC-/ONS-Managementsystem (EOMS)

Im Projekt EOMS wird ein offenes System für die Logistik entwickelt; auf Basis des EPC und dem Object Naming Service (ONS), wird ein eindeutiges Mapping zwischen EPC-Nummern und DNS-Namen (Domain Name System) durchführt.

Es wird eine standardisierte Architektur realisiert, die es allen am Produktions- und Lieferprozess Beteiligten erlaubt, den Lebenszyklus eines Produktes weltweit vertrauenswürdig (integer, vertrau-

lich, authentisch und verfügbar) nachverfolgen zu können.

Hierzu wird eine standardkonforme, softwaregestützte IT-Infrastruktur aufgebaut, die den unternehmensübergreifenden Informationsaustausch über Produkte erlaubt. Sie wird die Verknüpfung zwischen Transpondern, Lese-/ Schreibgeräten und IT-Systemen mit verteilten Datenbanken verschiedener Instanzen herstellen.

Relevante Standards sind bereits im umfassenden EPC Architecture Framework [10] von EPCglobal Inc. implementiert. Das EPC Architecture Framework ist in Abbildung 1 dargestellt.

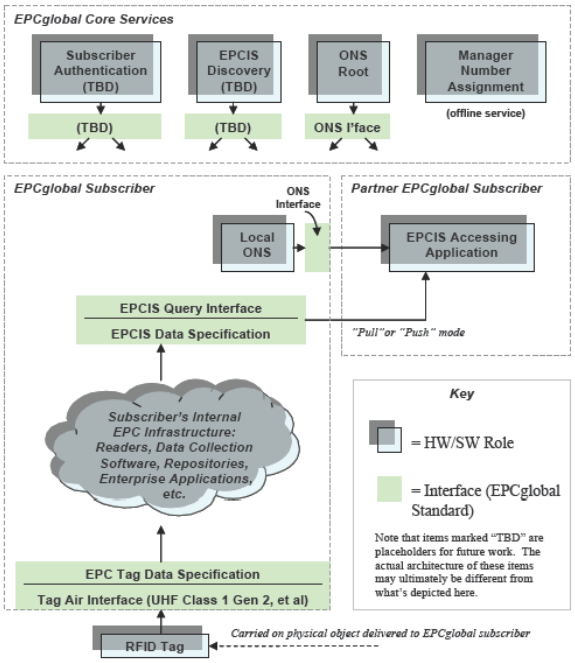

Abbildung 1: EPC Architektur [10]

Die EPC Information Services (EPCIS) [9] bieten eine standardisierte Möglichkeit um Produktinformationen entlang der Supply-chain unternehmensübergreifend austauschen zu können. Der Zugriff auf diese dezentralen, von den Herstellern selbst verwalteten und bereitgestellten Informationen, erfolgt über das EPCIS Query Interface (vgl. Abb. 1). Die Zusammenstellung von Informationen verschiedener an der Supply-chain beteiligter Instanzen soll zukünftig über den EPCIS Discovery Service (DS) realisiert werden. Dabei wird die Auflösung von EPC's zu den EPCIS-Servern der beteiligten Instanzen mittels des ONS [11] realisiert.

3 Trusted EPC Administration (TEA)

Auf Basis der EPCglobal-Standards soll die übergreifende Software-Architektur im Rahmen des Teilprojektes TEA prototypisch designed und implementiert werden - das EOMS.

Hier werden sicherheitsrelevante Aspekte der EOMS-Architektur im Hinblick auf ein vorgegebenes Sicherheitsniveau untersucht und erweitert, sowie ein Sicherheitsmodell für die vertrauenswürdige Verwaltung von EPC entwickelt.

Zudem wird ein Sicherheitsmodell zur Identifizierung und Authentifizierung von Benutzern des EPCIS Query Interface, sowie des DS realisiert.

Es soll nur berechtigten Subjekten (also autorisierten Geschäftspartnern) der Zugriff auf die in den Hersteller-Datenbanken hinterlegten Produktinformationen gewährt werden. Dieser Aspekt wird unter dem Sachziel Vertraulichkeit zusammengefasst.

Ein weiterer Kernaspekt ist die Konzeption eines Modells zur Counterfeit Security für EPC. Es soll auch nicht möglich sein, RFID-Transponder zu clonen [18]. Produktfälscher sollen nicht in der Lage sein die Identifikationsnummer eines originalen RFID-Transponders in einen Anderen zu kopieren. Ziel ist es zu verhindern, dass ein gültiger Verweis zwischen einem gefälschten RFID-Transponder (bzw. des enthaltenen EPC) und der Produktdatenbank des Herstellers aufgebaut werden kann. Somit kann die Erkennung von Fälschungen forciert werden. Dies kann durch die Verknüpfung von RFID mit PKI-Technologie erreicht werden [22].

Darüber hinaus sollen RFID-Transponder ausschließlich mit berechtigten Lesegeräten kommunizieren, um so eine nachweisbar authentische Kommunikation zu gewährleisten.

Die Entwicklung einer widerstandsfähigen und somit sichereren Architektur soll mittels marktüblichen Mechanismen erreicht werden. Dabei soll die Art des einzusetzenden RFID-Systems evaluiert werden, da diese einen Rahmen für die Realisierbarkeit von Sicherheitsmechanismen bildet [15].

Bei der Wahl eines RFID-Transponders muss neben dem sicherheitstechnischen auch der wirtschaftliche Aspekt betrachtet werden. Der Transponder muss eine kosteneffiziente Sicherheitslösung mit einem Widerstandswert bieten, welcher ausreicht um Fälschungen zu verhindern. Durch den hohen Rechenaufwand der bekannten Verschlüsselungsalgorithmen müssen sichere RFID-Transponder leistungsfähig sein, was ihre Produktionskosten erhöht und sie folglich für den EPC unattraktiv macht [16].

Daher werden Sicherheitslösungen, welche kostengünstig ein hohes Maß an Sicherheit bieten, untersucht und bewertet. Mögliche Ansätze könnten Physical Unclonable Functions (PUF) oder Algorithmen auf der Basis von elliptischen Kurven sein [5; 21].

3.1 Darstellung des Standards

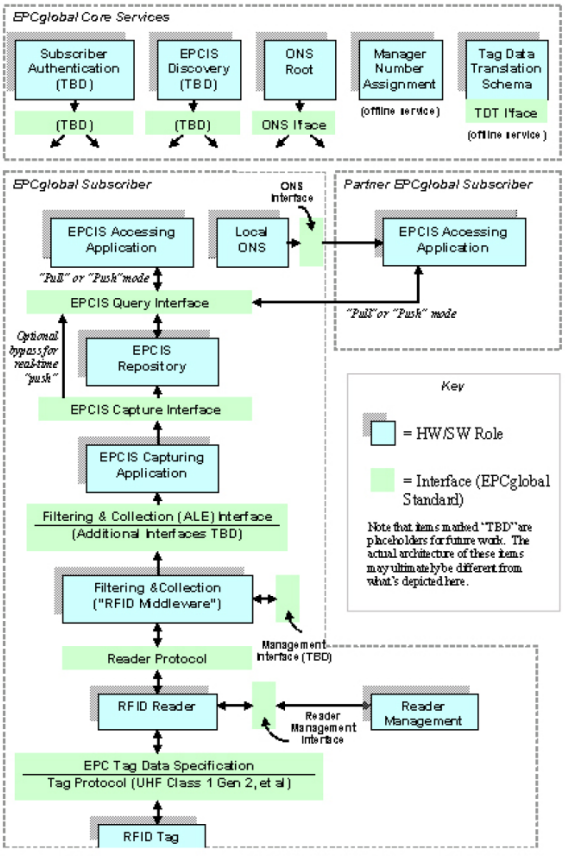

Abbildung 2: EPCglobal Network Software Architecture Components [10]

Um eine Verfolgung von Produktlebenszyklen anhand eines zugehörigen EPC zu ermöglichen, ist eine offene und anbieter-neutrale Architektur beabsichtigt, die eine weltweite und unternehmensübergreifende Lösung bereitstellt. Für diesen Zweck stellt das EPCglobal Architecture Framework [10] der EPCglobal Inc. eine plattformunabhängige Zusammenstellung von Hard-, Software und Datenstandards zur Verfügung. Bereits etablierte Standards wurden hierbei in das Framework einbezogen, soweit dies sinnvoll möglich war.

Um zu einem gegebenen EPC Meta-Informationen – z.B. für die Darstellung des Lebenszyklus – zu erhalten, wird der DS verwendet, welcher auch als Lookup Service bezeichnet wird. Der DS kann Verknüpfungen (Pointer) zu Entitäten (Repositorys) enthalten, welche relevante Daten zum angefragten EPC enthalten. Diese können z.B. generiert werden, wenn ein Application Layer Event (ALE) erzeugt wird – also ein RFID-Tag durch ein RFID-Lesegerät erkannt wird und an die Middleware gemeldet wird. Als Anfrage wird ein EPC an den DS übergeben, welcher mittels der gespeicherten Pointer als Ergebnis eine oder mehrere Lokationen in Form einer Liste von EPCIS Repository-Adressen zurückliefert, die Meta-Informationen zu dem jeweiligen EPC enthalten. Die in der Liste enthaltenen Adressen werden mittels dem ONS aufgelöst [9]. Die Auflösung durch das ONS erfolgt hierarchich nach dem Schema des DNS. Anstatt DNS Einträge enthält das ONS so genannte Naming Authority Pointer (NAPTR).

Der ONS stellt selber keine EPC Daten zur Verfügung, sondern verweist lediglich auf Netzadressen der Dienste, welche die benötigten EPC Daten vorhalten [8]. Zur Erlangung der Meta-Informationen zum angefragten EPC werden abschließend die ermittelten Repositorys einzeln abgefragt.

Das EPCglobal Architecture Framework schließt nicht aus, dass mehrere DS existieren können, welche jeweils unterschiedliche – z.B. regionale oder überregionale – Bereiche abdecken. Weiterhin ist der Standard zur Spezifikation des DS nicht abschließend fertiggestellt.

Angriff	Erläuterung	Zusammenhang zu EOMS	Betroffene Sachziele
Sniffing	Unbefugtes mitlesen/mithören oder auslesen von Daten	Fälschung der Lesegeräte oder Mithören der Funkübertragung	Vertraulichkeit, Verbindlichkeit
Spoofing	Verschleierung, Manipulation der eigenen Identität	Autorisierung und Zugriff der einzelnen Dienste untereinander	Vertraulichkeit, Authentizität, Verbindlichkeit
Replay	Aufzeichnung und Wiederholung eines erfolgreichen Informationsaustausches	Auslesen von Tags oder Kommunikation zwischen der ONS- oder EPCIS-Systemen	Vertraulichkeit, Verbindlichkeit
Man-in-the-Middle	Kommunikation zwischen zwei Knoten manipulieren indem ein weiterer Knoten eingefügt wird	Datenübertragung zwischen EPCIS, ONS oder Discovery-Service	Vertraulichkeit, Authentizität, Integrität, Verfügbarkeit
Denial of Service	Störung der Infrastruktur oder Komponenten durch die Verweigerung des Dienstes	Überlastung durch DDoS-Attacken, phys. Störung der Tags oder der Lesegeräte	Verfügbarkeit
Cloning	Nachbau von Tags durch „Reverse Engineering“ oder erfolgreiches Spoofing	Doppelte Tags lösen ggf. Fehler im System aus. Datenherausgabe an Unbefugte	Vertraulichkeit, Verbindlichkeit
Tracking	Erstellung von Bewegungsprofilen	Besondere Beachtung bzgl. Datenschutzregelungen	Vertraulichkeit
Relay	Vergrößerung der Lesereichweite von Tags	Unerkannte Verbesserung der Spoofing-bedingungen	Vertraulichkeit, Verbindlichkeit

Tabelle 1: Beispiele für Angriffe auf das EOMS und der zugehörigen Sachziele

3.2 Marktanalyse mit Abgrenzung des Projektrahmens

Das betrachtete EPC Architecture Framework beinhaltet neben den Kernkomponenten einige benachbarte Systeme (vgl. Abb. 1 und Abb. 2). Die Betrachtung der Sicherheitsaspekte tangiert in diesem Projekt die Kernkomponenten ONS, EPCIS und den DS.

Der Fokus des Projektes liegt insbesondere auf dem Bereich EPCIS und ONS. Die Bereiche RFID-Tag und Lesegerät werden nur in relevanten Zusammenhängen betrachtet. Allerdings lassen sich viele Überlegungen und grundsätzliche Aussagen auf diese Ebene übertragen und anwenden.

Im Bereich der physikalischen Sicherheit von RFID-Tags wird insbesondere die Fälschungssicherheit betrachtet.

Im Bereich EPCIS gibt es Unternehmen wie z.B. Oracle, SAP oder IBM, die standardkonforme EPCIS-Lösungen anbieten. Dabei werden Sicherheitsaspekte im Bezug auf die Repositorys zumeist auf der Basis von Best-Practice Lösungen realisiert.

Einige Lösungen der Anbieter zeichnen sich durch die Einbettung in bestehende Geschäftsprozesse aus. Der große Erfolg der European Article Number (EAN, heute GTIN) [12] scheint ein wichtiger Faktor zu sein, der zur Akzeptanz des EPCIS-Standards beiträgt.

Siemens hat in diesem Kontext eine PKI [20] entwickelt, die sowohl die Tags (Hardware) als auch die Software mit einbezieht. So werden die Güter - laut dem Hersteller - nach der Produktion „untrennbar“ mit einem Tag verbunden, auf dem ein Private-Key gespeichert wird. Mit Hilfe des Public-Keys, der beim Hersteller abrufbar ist, soll eine zuverlässige Echtheitsüberprüfung möglich sein. Die Tags sollen trotz der komplexen Krypto-Features wie elliptische Kurven preiswert sein und über eine kompakte Bauform verfügen. Das System soll sich zur Zeit noch in einem prototypischen Einsatz befinden.

3.3 Bedrohungsanalyse

Zu Bedrohungen oder Angriffen kommt es, sobald ein Sachziel der Informationssicherheit gefährdet ist. Wichtige Sachziele sind in diesem Zusammenhang:

- Authentizität:
  Nachgewiesene Identität.

Bedrohung	Lösungsansatz
Fälschung der Lesegeräte oder Mithören der Funkübertragung (Sniffing)	Digitale Signatur, Verschlüsselung , organisatorische Kontrollmaßnahmen
Auslesen von Tags oder Kommunikation zwischen der ONS- oder EPCIS-Systemen (Replay)	Timestamping, bekannt aus PKI, Verschlüsselung
Datenübertragung zwischen EPCIS, ONS oder Discovery-Service (Man-in-the-Middle)	Authentifizierung der Kommunikationsteilnehmer und Verschlüsselung der Kommunikationsstrecken
Überlastung durch DDoS-Attacken, Phys. Störung der Tags oder Lesegeräte (Denial of Service)	Erkennung von Angriffsmustern, Filtern der Kommunikation, ggf. Ansätze aus dem Cloudcomputing zur Verwaltung von Datenströmen
Doppelte Tags lösen ggf. Fehler im System aus. Datenherausgabe an Unbefugte (Cloning)	Erkennung von Clones durch digital signierte Tags, organisatorische Maßnahmen zur Behandlung von Plagiaten
Besondere Beachtung von Datenschutzregelungen (Tracking)	Datenschutzregelungen und gesetzliche Vorschriften anwenden und überwachen
Unerkannte Verbesserung der Spoofingbedingungen (Relay)	Regelmäßige Umgebungsprüfungen, Protokolle und Checklisten

Tabelle 2: Bedrohungen und Lösungsansätze für das EOMS-Projekt

- Vertraulichkeit:
  Daten sind für Berechtigte zugreifbar und für Unberechtigte nicht zugreifbar.
- Integrität:
  Daten sind vollständig, korrekt und unverändert.
- Verfügbarkeit:
  Wahrscheinlichkeit, ein System zu einem vorgegebenen Zeitpunkt, in einem funktionsfähigen Zustand anzutreffen.
- Verbindlichkeit:
  Ausgeführte Aktivitäten sind nichtabstreitbar.

Das Erfüllen der Sachziele kann durch den Einsatz verschiedener Methoden, Maßnahmen und Mechanismen erreicht werden. Es gibt darüber hinaus Überschneidungen bei der Erfüllung von Sachzielen. Ein Beispiel für eine solche Überschneidung ist die digitale Signatur, welche neben der Integrität auch die Vertraulichkeit gewährleistet [20].

In Tabelle 1 werden Beispiele möglicher Angriffe, das betroffene Sachziel und deren Zusammenhang mit den Schnittstellen des EOMS (vgl. Abb. 1 und Abb. 2) dargestellt.

3.4 Grundfunktionen und Mechanismen

Das Auffinden und Beschreiben von potentiellen Angriffen ist nur der erste Schritt bei der Bekämpfung von Bedrohungen. Daher ist ein systematisches Vorgehen von besonderer Bedeutung. Dazu werden die im Vorfeld analysierten Bedrohungen (vgl. Tabelle 2) zusammengetragen und Lösungsansätze dargestellt.

Abschließend sind die Verbindungen zwischen Kunde (Customer) und DS, DS und ONS, sowie ONS und EPCIS besonders im Blick der Securityanalyse.

Da das ONS große Ähnlichkeiten zum DNS aufweist [11] sollten hier sicherheitskritische Probleme, die vom DNS bereits bekannt sind, vermieden werden. Ziel ist daher die Wahl einer sicheren, vertraulichen, authentischen und integeren DNS-Implementierung.

In diesem Zusammenhang ist der Ansatz der Domain Name System Security Extension (DNSSEC) [1; 3; 2] von großer Bedeutung. Die abgelegten Daten werden mittels eines geheimen Schlüssels signiert und können mit einem öffentlichen Schlüssel auf Integrität und Authentizität geprüft werden. DNSSEC nutzt asymmetrische Kryptographieverfahren [20]. Diese haben einen, im Vergleich zu symmetrischen Verschlüsselungsverfahren, höheren Verwaltungsaufwand, da ein Keymanagement erforderlich ist. Hinzu kommen Konzepte wie die Chain-of-Trust, welche den Aufwand ebenfalls erhöhen.

Auch die Tatsache, dass DNS ein zumeist öffentlicher Dienst ist, ist im Bezug auf die Gefahr von

Angriff	Erläuterung
Zone Walking	Durchtesten vollständiger signierter Zonen, da nicht vorhandene Namen immer mit sortierten Listen bewiesen werden. (Bsp.: Zonenlist [001, 002, 004]. Eintrag 003 wird angefordert. Der Server antwortet also mit [002, 004]. So können alle Informationen einer Zone iterativ abgefragt werden).
DNS-Spoofing [17]	Fälschung der Zuordnung von IP und URL (z.B. durch Cache Poisoning usw.).
Cache Poisoning	Temporäre Manipulation des DNS-Server Caches um Anfragen an einen manipulierten Server umzuleiten.
Denial of Service bei DNSSEC	Durch die Generierung, Berechnung und andere Operationen, die durch das Public-Key-Verfahren anfallen ist DNSSEC besonders gefährdet was DoS-Attacken betrifft
DNS-Amplification	Manipulierte Anfragen werden genutzt um besonders lange Antworten eines DNS-Servers zu provozieren, welche dann an das Opfer weitergeleitet werden. Die Folge ist eine Auslastung der Bandbreite des Zielsystems.

Tabelle 3: Bekannten Sicherheitslücken im Bereich DNS

existierenden Sicherheitslücken von hoher Bedeutung. Dienste wie DNS und HTTP sind dadurch besonders stark im Interesse von Angreifern.

Eine sicheres Softwaredesign und eine adäquate Verifikation des Sicherheitsniveaus müssen bei der Entwicklung des ONS in besonderem Maße berücksichtigt werden. Tabelle 3 stellt bekannte Sicherheitslücken von DNS und DNSSEC dar.

DNSSEC und dessen Schwachstellen können wichtige Hinweise bei der Konzeption von sicheren ONS-Implementierungen geben. Auf Basis solcher Projekt-Retrospektiven können Fehler vermieden werden und die Sicherheit des Systems maßgeblich verbessert werden.

Neben der Integrität und Authentizität, welche durch DNSSEC erreicht werden kann, kann der Einsatz von DNSCurve [4] empfohlen werden, um auch das Sachziel Vertraulichkeit zu erreichen und den unberechtigten Zugriff auf Daten zu verhindern.

4 Fazit

Die RFID Technologie kann in vielen Branchen sinnvoll eingesetzt werden. Relevante Objekte eines RFID-Systems lassen sich mittels Softwarearchitekturen derart verbinden, dass sie sich zur weltweiten Verfolgung von Produktlebenszyklen eignen. Hierzu existieren Architekturen, wie das EPC Architecture Framework der EPCglobal Inc.. Eine unternehmensübergreifende Lösung wird dabei durch den Einsatz von Standards erreicht.

Aktuelle Softwarelösungen weisen einen geringen Widerstandswert auf. Dies ist in nicht genutzten oder schwachen Sicherheitsmechanismen begründet [13]. Das Projekt TEA beschäftigt sich mit der Erweiterung von EOMS um sicherheitsrelevante Aspekte, die einen vertrauenswürdigen Betrieb des Frameworks unter einem tolerierbaren Restrisiko ermöglichen. Das Projekt ist noch nicht abschließend bearbeitet.

Literatur

[1] Arends, R. ; Austein, R. ; Larson, M. ; Massey, D. ; Rose, S. : *DNS Security Introduction and Requirements.* `http://www.ietf.org/rfc/rfc4033.txt`. Version: 2005

[2] Arends, R. ; Austein, R. ; Larson, M. ; Massey, D. ; Rose, S. : *Protocol Modifications for the DNS Security Extensions.* `http://www.ietf.org/rfc/rfc4035.txt`. Version: 2005

[3] Arends, R. ; Austein, R. ; Larson, M. ; Massey, D. ; Rose, S. : *Resource Records for the DNS Security Extensions.* `http://www.ietf.org/rfc/rfc4034.txt`. Version: 2005

[4] Bernstein, D. J.: *DNSCurve: Usable security for DNS.* o.O., 2008 `http://www.dnscurve.org/dnssec.html`

[5] Braun, M. ; Hess, E. ; Meyer, B. : *Using Elliptic Curves on RFID Tags,.* Munich : Siemens AG, Corporate Technology, 2008

[6] BSI (Hrsg.): *TR 03126-1 - Technische Richtlinie für den sicheren RFID-Einsatz.* Bonn, 2008 http://www.bsi.de/literat/tr/tr03126/BSI-TR-03126-1.pdf

[7] EPCglobal Inc. (Hrsg.): *Electronic Product Code (EPC) Version 1.0 Specifications.* Lawrenceville, 2002 – 2004 http://www.epcglobalinc.org/standards_technology/specifications.html

[8] EPCglobal Inc. (Hrsg.): *Object Naming Service (ONS) Standard - Version 1.0.* o.O., 2005 http://www.epcglobalus.org/dnn_epcus/KnowledgeBase/Browse/tabid/277/DMXModule/706/Command/Core_Download/Default.aspx?EntryId=299

[9] EPCglobal Inc. (Hrsg.): *EPC Information Services (EPCIS) Version 1.0.1 Specification.* o.O., 2007 http://www.epcglobalinc.org/standards/epcis/epcis_1_0_1-standard-20070921.pdf

[10] EPCglobal Inc. (Hrsg.): *The EPCglobal Architecture Framework - EPCglobal Final Version 1.2.* o.O., 2007 http://www.epcglobalinc.org/standards/architecture/architecture_1_2-framework-20070910.pdf

[11] EPCglobal Inc. (Hrsg.): *The EPCglobal Architecture Framework - EPCglobal ONS Standard v. 1.0.1.* o.O., 2008 http://www.epcglobalinc.org/standards/ons/ons_1_0_1-standard-20080529.pdf

[12] Fleisch, E. ; Friedmann, M. : *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis.* Berlin et al., 2005

[13] Heise Zeitschriften Verlag (Hrsg.): *Mangelhafte Verschlüsselung bei vielen RFID-Karten.* Hannover, 2008 http://www.heise.de/newsticker/meldung/print/121028

[14] Kaminsky, D. (Hrsg.): *An Attack Surface Analysis of RFID.* o.O., 2007 http://www.law.washington.edu/lct/events/rfid/Dan_Kaminsky-RFID-Attack-Surface.pdf

[15] Knospe, H. ; Pohl, H. : *RFID Security.* Bd. Information Security Technical Report: 9, 4, 39 - 50, http://www.inf.fh-bonn-rhein-sieg.de/informatikmedia/Downloads/fb_informatik/personen/pohl/Aufsaetze/Pohl_Knospe_RFID_Security_050126.pdf

[16] Lehtonen, M. ; Staake, F. ; Michahelles, F. ; E., F. ; Auto-ID Labs ETH Zürich und Uni St. Gallen (Hrsg.): *From identification to authentication, White Paper.* 2006

[17] Müller, B. : *Improved DNS spoofing using node re-delegation.* Vienna, 2008

[18] Pohl, H. : *Sicherheitsrisiken von Transpondern – Schutzmaßnahmen und Handlungsbedarf. Eingeladener Vortrag. VDE/ITG Workshop RFID: Intelligente Funketiketten - Chancen und Herausforderungen.* Darmstadt, 2005 http://www.inf.fh-bonn-rhein-sieg.de/informatikmedia/Downloads/fb_informatik/personen/pohl/Aufsaetze/Pohl_RFID_Risiken_VDE_ITG_WS_Darmstadt_050215.pdf

[19] Pohl, H. ; Jung, N. ; Roth, T. : *Bewertung des Sicherheitsniveaus einiger Mechanismen zur Vertraulichkeit, Verfügbarkeit und Pseudonymität von Transpondern (RFID). In: Hollstein, T.; Wernle, M.E.; Wissendheit, U.: 2. Workshop RFID: Intelligente Funketiketten – Chancen und Herausforderungen. Erlangen 4./5. Juli 2006 VDE/ITG.* Darmstadt, 2006 http://www.inf.fh-bonn-rhein-sieg.de/informatikmedia/Downloads/fb_informatik/personen/pohl/Aufsaetze/Pohl_Jung_Roth_Bewertung_des_Sicherheitsniveaus_von_Transpondern_.pdf

[20] Schmeh, K. : *Kryptographie - Verfahren, Protokolle, Infrastrukturen..* Bd. 3. über und erw. Auflage. Heidelberg, 2007

[21] VERAYO (Hrsg.): *PUF RFID.* San Jose, 2008 http://www.verayo.com/product/pufrfid.html

[22] WALLSTABE, A. ; POHL, H. : *Implementing high-level Counterfeit Security using RFID and PKI. In: Wissendheit, U.; Kolnsberg, S.; Wernle, M.E.; Hollstein, T.: 3rd European Workshop on RFID Systems and Technologies 12.Juni – 13. Juni 2007.* Duisburg, 2007 http://www.inf.fh-bonn-rhein-sieg.de/informatikmedia/Downloads/fb_informatik/personen/pohl/Aufsaetze/Pohl_Wallstabe_High_Level_Counterfeit_Security_2007_.pdf