RFID-Authentisierung in der Lieferkette der Automobilindustrie

Silke Schäfer[1] · Karsten Sohr[2]

[1]Universität Bremen – Technologie-Zentrum Informatik (TZI)
schaefer@tzi.de

[2]Universität Bremen – Technologie-Zentrum Informatik (TZI)
sohr@tzi.de

Zusammenfassung

In der Automobilindustrie besteht eine hohe Motivation für die Nutzung der RFID-Technologie. Der wesentliche Antrieb besteht in den zu erzielenden Effizienzgewinnen, die aus einer geringen Fehlerrate bei automatisierten Abläufen und einer generellen Prozessbeschleunigung resultieren. Dabei gilt der Einsatz von lieferkettenübergreifenden RFID-Anwendungen als wirtschaftlich besonders vielversprechend.
Dieser Artikel stellt eine lieferkettenübergreifende RFID-Anwendung vor, mit der die Produkt- und Produktionsdaten eines Fahrzeugs lebenslang dokumentiert werden können und zeigt auf, wie dem Sicherheitsrisiko „Verlust der Vertraulichkeit“ durch eine Authentisierung mit abgeleiteten Schlüsseln Rechnung getragen werden kann.

1 Einführung

Die RFID-Technologie kommt in letzter Zeit verstärkt in betriebswirtschaftlichen Prozessen wie z. B. in der Automobilproduktion und -logistik, im Einzelhandel und im Pharmaziebereich zum Einsatz. Sie bietet hier ein großes Potential für die Optimierung bisher aufwendiger und fehleranfälliger betriebswirtschaftlicher Abläufe. Insbesondere die Automobilindustrie besitzt eine hohe Motivation, die RFID-Technologie zu nutzen, wobei der wesentliche Antrieb in den zu erzielenden Effizienzgewinnen besteht, die aus einer geringen Fehlerrate bei automatisierten Abläufen und einer generellen Prozessbeschleunigung resultieren. Bereits umgesetzte Lösungen beschränken sich dabei oftmals auf die Verbesserung der Abläufe nur eines Unternehmens [WaHS07].

Die Optimierung der gesamten Lieferkette der Automobilindustrie gilt jedoch als erfolgversprechende Maßnahme zur Steigerung der Wettbewerbsfähigkeit [StPS05]. Die RFID-Technologie besitzt hier das Potential für zahlreiche Verbesserungen entlang der Wertschöpfungskette: Sie ermöglicht neben der automatischen Objektidentifikation auf der Basis von Funktechnologien auch eine lückenlose, lieferkettenübergreifende Dokumentation der Fahrzeughistorie auf RFID-Transpondern. Dies kann erreicht werden, indem jedes Fahrzeug mit einem Transponder versehen wird, auf den neben dem Fahrzeughersteller auch andere Unternehmen der Lieferkette der Automobilindustrie im Rahmen ihrer Aufgaben Lese- und Schreibzugriff erhalten. Diese Art von Anwendung ist damit für eine Industrie, die auf Grund der Tendenz zum kundenindividuellen Fahrzeug vermehrt aufwendige und fehlerträchtige Abläufe aufweist, lieferkettenübergreifend von zunehmendem Interesse.

P. Horster (Hrsg.) · D•A•CH Security 2008 · syssec (2008) 1-10.

Eine derartige Anwendung zeichnet sich zunächst dadurch aus, dass mehrere Partner auf eine Vielzahl von Transpondern zugreifen. Darüber hinaus hinterlegen die verschiedenen Unternehmen in der Lieferkette nicht nur nicht-vertrauliche Daten wie die Lackfarbe oder Produktionsnummer eines Fahrzeugs auf dem Transponder, sondern speichern dort mit dem Ziel einer lückenlosen Fahrzeughistorie auch streng vertrauliche Informationen wie beispielsweise Qualitätsdaten, die nur bestimmten anderen Partnern in der Lieferkette – und keinem Dritten – zugänglich sein dürfen. Um die Informationssicherheit einer derartigen Anwendung zu gewährleisten, sind verschiedene Anforderungen zu erfüllen. So muss ein Fahrzeug über seinen Transponder eindeutig identifizierbar sein, indem der Transponder seine Identität gegenüber einem RFID-Lesegerät eindeutig nachweist; ein Lesegerät eines Partners muss seinerseits seine Identität gegenüber dem Transponder nachweisen und belegen, dass es zum Datenzugriff autorisiert ist; schließlich muss dem Sicherheitsrisiko „Verlust der Vertraulichkeit“ durch entsprechende Maßnahmen Rechnung getragen werden.

Dieser Artikel zeigt auf, wie eine lückenlose Dokumentation der Fahrzeughistorie auf einem RFID-Transponder lieferkettenübergreifend so umgesetzt werden kann, dass die genannten Anforderungen erfüllt werden. Dazu stellen wir im Anschluss an eine kurze Einführung der RFID-Grundlagen zunächst die beteiligten Partner einer derartigen Anwendung vor und begründen ihre Motivation für die Umsetzung einer lieferkettenübergreifenden Dokumentation von Fahrzeugdaten auf einem RFID-Transponder. Anschließend legen wir ein unter den Unternehmen in der Lieferkette abzustimmendes Datenmodell dar, das den Partnern eine gemeinsame Nutzung der Daten auf den Transpondern ermöglicht und dabei jedem Partner mit Hilfe von hierarchischen Zugriffspasswörtern sowohl die Ablage vertraulicher, unternehmensinterner Daten als auch den Datenaustausch mit weiteren Partnern erlaubt. Die Darstellung eines sicheren Protokolls zum Schutz dieser Zugriffspasswörter sowie zusätzlicher Nutzdaten ist ein weiteres Ziel dieses Beitrags.

2 RFID-Grundlagen

RFID-Systeme dienen zur automatischen Identifikation von Objekten über Funk. Sie gehören damit zu den so genannten Auto-ID-Verfahren, die sich dadurch auszeichnen, dass sie das eineindeutige Erkennen einer Person oder eines Objekts automatisiert ermöglichen. Ein RFID-System besteht dabei aus zwei Komponenten: einem Lesegerät und einem Transponder, der den eigentlichen Datenträger darstellt. Er wird an einem Objekt angebracht oder in ein Objekt integriert und dient insbesondere zu dessen Identifikation. Ein Transponder besteht im Wesentlichen aus einem Mikrochip und einer Spule oder Antenne als Kopplungseinheit. Er kann von einem Lesegerät kontaktlos ausgelesen und je nach eingesetzter Technologie auch mit Daten beschrieben werden.

Das RFID-Lesegerät erzeugt die Sendeleistung, die zur Aktivierung und Stromversorgung eines RFID-Transponders benötigt wird und moduliert das Datensignal auf ein magnetisches oder elektromagnetisches Feld, so dass Daten an den Transponder übertragen werden können. Darüber hinaus empfängt und demoduliert es die vom Transponder übermittelten Antwortdaten. Das Lesegerät ermöglicht damit den Datenaustausch zwischen einer Anwendungssoftware einerseits und einem Transponder andererseits. Neben der grundlegenden Aufgabe der Signalkodierung und -dekodierung ist das Lesegerät in komplexeren Systemen auch für die Durchführung einer Authentisierung sowie für die Verschlüsselung bzw. Entschlüsselung der ausgetauschten Daten zuständig.

3 Themennahe Arbeiten

Bono et. al. [BGSJ+05] stellen Untersuchungen zum Thema RFID-Sicherheit im Umfeld der Automobilindustrie an. Die Autoren zeigen die Sicherheitsmängel des Texas Instruments Digital Signature Transponders (DST) auf, der sowohl in elektronischen Wegfahrsperren als auch als elektronisches Zahlungsmittel in Form des ExxonMobil SpeedPass™ zum Einsatz kommt. Es handelt sich dabei um einen höherwertigen Transponder, dessen kryptographische Funktionalität ihn befähigt, ein Challenge-Response-Protokoll zur Transponder-Authentisierung durchzuführen. Diese Authentisierung beruht darauf, dass der Transponder die Kenntnis eines gemeinsamen, 40 Bit langen Schlüssels nachweist, indem er im Wesentlichen eine vom Lesegerät ausgesendete Zufallszahl verschlüsselt zurücksendet. Die Autoren weisen nach, dass die Sicherheitsmängel des DST auf eine unangemessene Schlüssellänge zurückzuführen sind, die es ihnen erlauben, einen voll funktionsfähigen Klon eines DST-Tokens herzustellen.

Waldmann et. al. [WaHS07, Kapitel 4] untersuchen die Sicherheitsanforderungen der Automobilindustrie in geschlossenen und lieferkettenübergreifenden RFID-Anwendungen. Die Autoren stellen fest, dass speziell fehlende Standards, hohe Kosten und Sicherheitsbedenken der Anwender einem lieferkettenübergreifenden Zugriff auf gemeinsame Datenbestände entgegenstehen und machen insbesondere Mechanismen zur Authentisierung und Zugriffskontrolle sowie geringe Transponderkosten als wichtige Anforderungen für den erfolgreichen RFID-Einsatz in der Automobilindustrie aus. Die Transponderkosten werden dabei insbesondere von der Anzahl der Gatter auf dem Transponder bestimmt.[1]

Die Authentisierung von Transpondern und Lesegeräten bildet somit eine wichtige Sicherheitsfunktionalität, die einerseits die Anwendung vor einer Manipulation mit gefälschten Daten sichert und andererseits den Transponder vor unberechtigten Lese- und Schreibzugriffen sowie einem Missbrauch des Kill-Kommandos schützt [Fink06, WaHS07]. Ein angemessen starkes Authentisierungsverfahren, das hinsichtlich des Speicherbedarfs und der Zahl der Gatter auf dem RFID-Transponder optimiert ist, stellen Peris-Lopez et. al. [PLHCETR06] mit dem Lightweight Mutual Authentication Protocol (LMAP), einem Verfahren der Lightweight-Cryptography, vor. Ferner präsentieren Feldhofer et. al. [FeDW04] ein Protokoll zur gegenseitigen Authentisierung nach ISO/IEC 9798-2 unter Verwendung von AES und zeigen in einer Machbarkeitsstudie die Hardware-Umsetzung des Algorithmus, die für einen geringen Energieverbrauch und eine vergleichsweise geringe Gatterzahl optimiert ist. Beide Arbeiten entsprechen damit der oben genannten Anforderung nach geringen Transponderkosten.

Auch Finkenzeller [Fink06] befasst sich mit der (Daten-)Sicherheit von RFID-Systemen durch den Einsatz von Authentisierungsprotokollen auf der Basis von ISO/IEC 9798-2. Die Umsetzung dieses Protokolls für eine lieferkettenübergreifende Anwendung der Automobilindustrie stellt auch das Thema dieses Artikels dar. Wir schlagen den Einsatz von starken kryptographischen Verfahren vor, um eine sichere lieferkettenübergreifende Authentisierung zu erreichen.

4 Die virtuelle Baukarte in der Automobilindustrie

Die Automobilindustrie in Deutschland gilt als einer der Vorreiter auf dem Gebiet der RFID-Technologie. Der Einsatz von RFID gilt hier aufgrund des durchgängigen Waren- und Informationsflusses als besonders vielversprechend; bereits umgesetzte Lösungen beschränken sich jedoch oftmals auf die Verbesserung der Abläufe nur eines Unternehmens und lassen so das

[1] Nach Schätzungen aus dem Jahr 2003 führen 1.000 Gatter zu Mehrkosten von einem US Cent [Weis03].

weitere Potential zur Steigerung der Wettbewerbsfähigkeit durch eine gezielte Optimierung der Lieferkette ungenutzt [StPS05].

Ein Großteil der in Automobilproduktion und -logistik bereits umgesetzten RFID-Anwendungen bildet somit Insellösungen. In diesem Zusammenhang untersuchen Waldmann et. al. [WaHS07] unter anderem Konzepte für die RFID-gestützte Online-Steuerung der Lieferkette. Sie legen ausführlich zwei Pilotprojekte dar, die sich mit der Kontrolle des Produktionsprozesses sowie der Dokumentation von Produkt- und Produktionsdaten befassen. Neben der Identifikation der benötigten Verfahren für eine sichere Anwendung der RFID-Technologie in diesem Umfeld stellen die Autoren den RFID-Einsatz in einer generischen Lieferkette der Automobilindustrie vor und umreißen bereits die Idee einer erweiterten, lieferkettenübergreifenden RFID-Anwendung, die sich mit der automatischen Dokumentation und Archivierung von Produkt- und Produktionsdaten auf RFID-Transpondern befasst.

Diese Anwendung, die bislang nur einen Teil einer lieferkettenübergreifenden Prozesskette – die Automobilproduktion – umfasst, lässt sich derart erweitern, dass sie die gesamte Lieferkette der Automobilindustrie überspannt [Schä07]: Jedes Fahrzeug wird dazu während der Produktion mit einem RFID-Transponder (*virtuelle Baukarte*, kurz Baukarte) ausgestattet, der während des gesamten Produktlebenszyklus zur weiteren Nutzung im Fahrzeug verbleibt. Die Baukarte dokumentiert während der Produktion zunächst die Produkt- und Produktionsdaten und dient zur Steuerung der Prozessabläufe. Im Anschluss an den Fertigungsprozess beim Fahrzeughersteller erhalten auch weitere Unternehmen aus verschiedenen Stufen der Lieferkette im Rahmen ihrer Aufgaben Zugriff auf die auf der virtuellen Baukarte gespeicherten Informationen und hinterlegen dort auch selber Daten. So greifen nach dem Fahrzeughersteller und dessen Zulieferern zusätzlich Logistikdienstleister und Händler sowie Werkstätten und Recycling- und Entsorgungsbetriebe auf die Baukarte zu (vgl. Abb. 1).

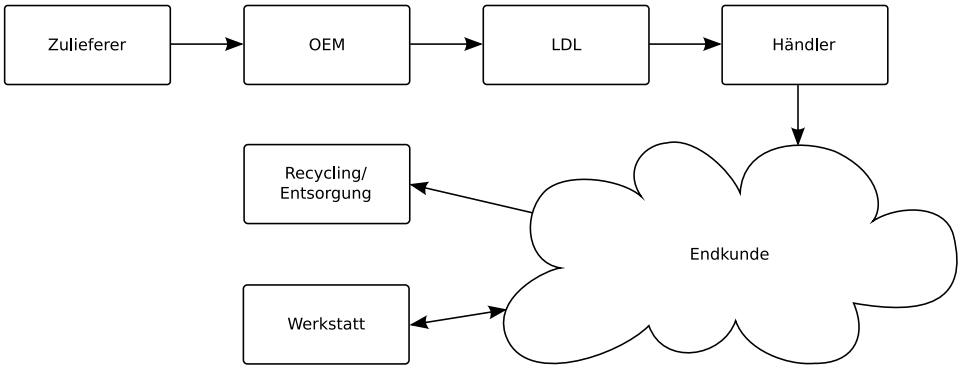

Abb. 1: Die Lieferkette in der Automobilindustrie

Neben der skizzierten Möglichkeit, die zu verarbeitenden Daten auf dem Transponder selbst zu hinterlegen, kommt alternativ die Ablage in einer Datenbank infrage, die allen Wertschöpfungspartnern eine zentrale Sicht auf die Daten ermöglicht. Dabei wird der Transponder als eine Art Zeiger auf den assoziierten Datensatz genutzt. Beide Möglichkeiten unterscheiden sich in ihren Sicherheitsanforderungen und -risiken, da kommerzielle Datenbanken – im Gegensatz zu Transpondern – im Allgemeinen über erprobte Schutzkonzepte verfügen (unter anderem Authentisierung, Zugriffskontrolle, Verschlüsselung), so dass das NIST [NIS07] in der Regel die Ablage von Informationen in einer Datenbank empfiehlt. Heutige Produktionssysteme geben ein homogenes, föderativ genutztes Backend zur Datenablage (vgl. beispielsweise [Erdo06]) je-

doch nicht her [Weig06], so dass bei den der Produktion nachgelagerten Schritten nicht a priori davon ausgegangen werden kann, dass ein Online-Zugriff auf die Daten möglich ist. Aus diesem Grund wird in diesem Szenario abweichend von der NIST-Empfehlung eine transponderbasierte Speicherung angenommen, die auch der aktuellen Tendenz in der Automobilindustrie entspricht und in ähnlicher Form bereits evaluiert wird [WaHS07]. Im Folgenden wird mithin nicht nur ein Datenmodell eingeführt, das die sichere, lieferkettenübergreifende Nutzung der Baukartendaten ermöglicht, sondern ferner ein sicheres Verfahren für die Authentisierung und Verschlüsselung (inkl. Schlüsselverwaltung) vorgestellt, um so den resultierenden Sicherheitsrisiken Rechnung zu tragen.

4.1 Datenmodell der virtuellen Baukarte

Die gemeinsame, sichere Nutzung der vertraulichen Daten auf der virtuellen Baukarte durch mehrere Unternehmen in der Lieferkette macht ein unter den Beteiligten abgestimmtes Datenmodell erforderlich. In Orientierung an der VDA-Empfehlung 5501 [VDA06], die die Datenorganisation auf den Transpondern nach ISO/IEC 18000-6c spezifiziert, nehmen wir eine logische Unterteilung des Transponder-Speichers in vier Bereiche an (vgl. Abb. 2). Die ersten beiden Bereiche beinhalten die eindeutige Kennung des Transponders (TID) sowie einen Unique Item Identifier (UII), der das Fahrzeug, zu dem der Transponder gehört, eindeutig identifiziert – vergleichbar mit der Fahrgestellnummer.

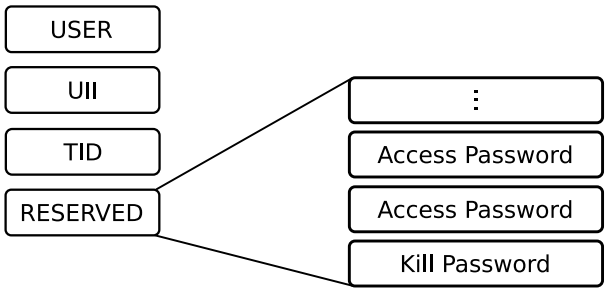

Abb. 2: Datenstruktur der virtuellen Baukarte

Der USER-Bereich der virtuellen Baukarte ist von den an der Wertschöpfungskette beteiligten Partnern mit gewissen Einschränkungen frei zugreifbar. Er dient dem Datenaustausch unter den Partnern einerseits sowie der Ablage unternehmensinterner Daten andererseits und ist dazu in mehrere zugriffsgeschützte Segmente $S_1, \ldots, S_n$ unterteilt [Fink06]. Der Zugriffsschutz eines Segments S_j ($1 \leq j \leq n$) wird mit Hilfe zweier Segment-spezifischer Zugriffspasswörter s_j^r bzw. s_j^w realisiert, denen unterschiedliche Zugriffsrechte (nur Lesen bzw. Lesen und Schreiben) zugewiesen werden. Sie steuern den Zugriff auf die Nutzdaten und werden, wie vom VDA spezifiziert, im schreibgeschützten Transponder-Bereich RESERVED hinterlegt [VDA06]. Mithilfe dieser Vorgehensweise können unterschiedliche Berechtigungsstufen erzielt werden. Finkenzeller [Fink06] bezeichnet sie als *hierarchische Schlüssel*, so dass im Folgenden die Rede von Zugriffsschlüsseln statt -passwörtern sein soll.

Jeder Partner in der Lieferkette erhält zunächst ein privates Segment zur Ablage unternehmensinterner Daten, dessen Schlüssel nur ihm bekannt sind. Weitere Segmente dienen der Kommunikation unter den Partnern; mit ihrer Hilfe können beispielsweise Produktinformationen ausgetauscht oder Aufträge erteilt werden: Will dazu Partner p_1 zwei verschiedene Datensätze

an Partner p_2 übermitteln, von denen einer nur gelesen werden darf, so sind zwei Segmente erforderlich, wobei p_2 von einem den Lese- und vom anderen den Lese-/Schreibschlüssel kennt.

Um eine für den Prozessablauf ausreichende Datenübertragungsrate (vgl. [WaHS07]) sicherzustellen, ist es in den meisten Fällen ausreichend, nur den im jeweiligen Prozess-Kontext benötigten Teil eines Segments auszulesen oder zu schreiben [VDA06]. Ein derartiger differenzierter Zugriff kann durch die Angabe einer dreistufigen Adressierung bei Lese- oder Schreibvorgängen erreicht werden, die die Segmentnummer, die Startposition und eine Längenangabe beinhaltet. Diese Adressierung von Teilsegmenten reduziert die Datenmengen auf das notwendige Minimum, so dass der Einsatz der virtuellen Baukarte, wie er im Folgenden beschrieben wird, mit minimalen Schreib-/Lesezeiten möglich ist.

4.2 Fallbeispiel: Einsatz der virtuellen Baukarte

Der Einsatz der virtuellen Baukarte kann beispielhaft beim Automobilhersteller und Logistikdienstleister wie folgt stattfinden: Im ersten Schritt erstellt der Fahrzeughersteller eine Baukarte für das zu produzierende Fahrzeug und versieht sie mit den benötigten Daten und ihrer Kennung UII. Dabei kommt das oben dargestellte Datenmodell zum Einsatz. Die für den Zugriff auf die Segmente der Baukarte benötigten Schlüssel werden ebenso wie die TID bereits vom Hersteller des Transponders hinterlegt, der als entsprechend vertrauenswürdig angesehen wird.

Während der eigentlichen Fahrzeugproduktion wird die virtuelle Baukarte physisch mit dem Fahrzeug verbunden und für die Dokumentation der durchgeführten Arbeitsschritte genutzt (Verbaudokumentation). Die Endabnahme des Fahrzeugs, die der Qualitätssicherung dient, schließt den Produktionsprozess ab. Während dieses Prozessschrittes werden alle Funktionen und Eigenschaften des Fahrzeugs anhand seiner Baukarte überprüft. Die in diesem Zusammenhang auf der Baukarte hinterlegten Daten unterliegen insbesondere hohen Anforderungen hinsichtlich Vertraulichkeit: Da sie Aufschluss darüber geben, ob verschiedene Qualitätsprüfungen bestanden wurden, droht dem Fahrzeughersteller ein Imageschaden, falls eine zu hohe Fehlerquote in der Produktion publik wird. Auf der Grundlage dieser Daten wird nun entschieden, ob das Fahrzeug für die Übergabe an den Logistikdienstleister bereit ist oder Nachbesserungen erforderlich sind.

Der Logistikdienstleister führt den weiteren Transport des Fahrzeugs zu einem Händler durch und greift als Drittpartei im Zuge seines logistischen Prozesses ebenfalls auf dessen virtuelle Baukarte zu. Er entnimmt ihr zunächst verschiedene Fahrzeug- und Auftragsdaten (z. B. Modellcode, Lieferdatum und Schlüsselnummer) und hinterlegt dort eigene Prozessdaten sowie eine Dokumentation der technischen Bearbeitung und sonstiger Arbeitsschritte. Auch für diese Daten ist die Vertraulichkeit zu gewährleisten.

Dieses Fallbeispiel verdeutlicht, wie der Einsatz der virtuellen Baukarte den Fahrzeughersteller und Logistikdienstleister bei der Durchführung ihrer Geschäftsprozesse unterstützt. Auch im After-Sales-Bereich, der Rückrufe durch den Fahrzeughersteller, Wartung und Reparaturen in Werkstätten sowie Recycling und Entsorgung am Ende des Produktlebenszyklus umfasst (siehe auch Abb. 1), besitzt die Baukarte das Potential für weitere Optimierungen (vgl. auch [WaHS07]):

- Da die Fahrzeugdaten bereits beim Verbau eines Teils erfasst und gespeichert werden, sind später – falls bei der betreffenden Produktionscharge Fehler entdeckt werden – gezielte Rückrufe möglich, die zu einer geringeren öffentlichen Wahrnehmung führen.

- Im Rahmen der Ersatzteildistribution können die Daten auf der Baukarte zur gezielten Steuerung und -optimierung der Prozesse genutzt werden.
- Bei 10% aller als Originalersatzteile vertriebenen Teile handelt es sich in Wirklichkeit um Fälschungen [StPS05] – der gezielte Technologieeinsatz kann einer Werkstatt hier wirtschaftlich sinnvolle Kontrollen ermöglichen, da sie z. B. im Garantiefall anhand der Fahrzeughistorie auf der Baukarte überprüfen kann, ob tatsächlich noch das Originalteil aus dem Werk verbaut ist.
- Die genaue Kenntnis der Fahrzeugkonfiguration erleichtert Werkstattmitarbeitern die Durchführung von Wartungs- und Reparaturaufträgen. Ferner kann für sicherheitsrelevante Bauteile mittels Baukarte gewährleistet werden, dass vorgeschriebene Wartungsvorgänge laut Inspektionsplan durchgeführt werden.
- In Recyclingbetrieben kann eine stoffliche Beschreibung der Bauteile von der Baukarte abgerufen werden. Sie ermöglicht ein sortenreines Trennen und stellt Demontagerelevante Informationen (z. B. für die Wiederverwendung von Bauteilen bei neuen Unfallwagen) bereit, um so der EU-Richtlinie über Altfahrzeuge [EG00] gerecht zu werden, die hohe Wiederverwendungs- und Verwertungsquoten bei allen Altfahrzeugen von mindestens 85% ab 2006 und 95% im Jahr 2015 vorsieht.

Hat die RFID-Technologie erst einmal einen bestimmten Verbreitungsgrad gefunden, so wird die Nutzung der nun vorhandenen RFID-Infrastruktur auch für weitere Anwendungsgebiete interessant, da Investitionen in die Infrastruktur zu einem großen Teil schon getätigt wurden und so Synergieeffekte genutzt werden können.

4.3 Technische Anforderungen an die virtuelle Baukarte

Um die Dokumentation aller im Leben eines Fahrzeugs relevanten Informationen lieferkettenübergreifend auf einer Baukarte zu ermöglichen, sind industrieweit gemeinsam definierte Standards für die benötigten Hardwarekomponenten, Übertragungsprotokolle, Schnittstellen und Datenstrukturen erforderlich. Sie erlauben den Zugriff auf Transponder, die ausreichend mehrfach beschreibbaren Speicherplatz bieten müssen. Einzelne Datenfelder der Transponder, wie beispielsweise das Produktionsdatum oder Recycling-Informationen, sollten als WORM-Felder[2] nach dem einmaligen Beschreiben nur noch für Lesevorgänge zur Verfügung stehen, um eine nachträgliche Manipulation zu verhindern.

Eine weitere Anforderung an die virtuelle Baukarte ergibt sich aus der Notwendigkeit beispielsweise für den Logistikdienstleister, die Transponder aus einer Distanz von mehreren Metern auszulesen, um die Identifikation der Fahrzeuge auch auf einem LKW zu ermöglichen, der ein Antennentor mit stationärem RFID-Lesegerät passiert. Dieser Anforderung entsprechen beispielsweise passive RFID-Systeme, die im Ultrahochfrequenzbereich (868 MHz) arbeiten und ohne Stützbatterie eine Reichweite von etwa drei bis vier Metern erreichen [BSI04].

Darüber hinaus ist aufgrund der langen Nutzungsdauer eines Fahrzeugs von 15 Jahren oder mehr der Einsatz passiver Transponder geboten. Um den verschiedenen Umweltbedingungen gerecht zu werden, muss die Baukarte im Temperaturbereich von etwa -20 bis +50° C arbeiten und vor Staubeintritt geschützt sein. Diese Anforderungen hinsichtlich Energieversorgung, Temperaturbereich und Frequenzbereich (und damit Lesegeschwindigkeit und -abstand) erfüllen beispielsweise Transponder der Norm ISO/IEC 18000-6 [BSI04].

[2] Write once, read multiple times

4.4 Sicherheitsaspekte der virtuellen Baukarte

Die Sicherheitsprobleme der hier dargestellten Anwendung untersucht Schäfer in [Schä07] exemplarisch an einem Ausschnitt der Lieferkette, der den Automobilhersteller sowie Logistikdienstleister umfasst. Die Autorin klassifiziert verschiedene Arten von Bedrohungen, darunter

- Störungen, die den erwartungskonformen Prozessablauf beeinträchtigen. Sie besitzen ein erhebliches Bedrohungspotential, da ein Ausfall im Logistikbereich bzw. ein Produktionsstopp pro Stunde Kosten im sechs- bzw. siebenstelligen Bereich verursachen kann;
- der Verlust von Verfügbarkeit und Integrität der Baukartendaten. Diese Kategorie von Bedrohungen, die zu einer negativen Außenwirkung führen oder finanzielle Auswirkungen besitzen können, resultiert aus der gesetzlichen Anforderung an den Automobilhersteller, die während der Produktion anfallenden Produkt- und Produktionsdaten dauerhaft verfügbar zu halten (Dokumentations- und Archivierungspflicht), so dass später eventuelle Haftungsfragen geklärt werden können;
- der Aspekt der *Location Privacy*, der die Fähigkeit bezeichnet, andere daran zu hindern, den gegenwärtigen oder vergangenen Aufenthaltsort einer Person zu erfahren [BeSt03]. Da die virtuelle Baukarte die automatisierte Erstellung von Bewegungsprofilen ermöglicht, weist sie ein grundsätzliches Bedrohungspotential für den Endkunden auf, der ein damit ausgestattetes Fahrzeug besitzt.

Darüber hinaus wird die Vertraulichkeitseigenschaft der lieferkettenübergreifend verfügbaren Daten auf der Baukarte als essentiell eingestuft und das Ausspähen von Informationen folglich als zentrale Bedrohung identifiziert. Der folgende Abschnitt stellt mithin ein Protokoll dar, dass eine gegenseitige Authentisierung von Transpondern und Lesegeräten sowie eine vertrauliche Kommunikation ermöglicht.

5 Authentisierung mit abgeleiteten Schlüsseln

Die vertraulichen Daten eines Partners in der Lieferkette werden mit Hilfe der Zugriffsschlüssel, die den Zugriff auf die Baukartensegmente steuern, vor dem unautorisierten Zugriff durch Dritte geschützt. Die Schlüssel werden vom Lesegerät über die Luftschnittstelle übertragen, das so seine Autorisierung anzeigt; sie unterliegen damit einem hohen Risiko durch Ausspähen. Diese Tatsache macht ein Verfahren erforderlich, das eine Übertragung der Zugriffsschlüssel derart ermöglicht, dass ihre Vertraulichkeit gewahrt bleibt. Eine einfache Abschirmung, wie sie beispielsweise vom BSI vorgeschlagen wird [BSI04], bietet aufgrund der hohen Vertraulichkeit der Daten keinen ausreichenden Schutz. Eine Lösung besteht in einer ausreichend starken symmetrischen Verschlüsselung der Zugriffsschlüssel in der Luftschnittstelle. Sie birgt im beschriebenen Szenario jedoch zwei wesentliche Probleme:

1. Die Vorgehensweise reicht nicht aus, um ein Aufzeichnen und späteres Wiedereinspielen der *verschlüsselten* Zugriffsschlüssel zu verhindern, durch das ein Angreifer Zugriff auf die als vertraulich klassifizierten USER-Daten erlangen kann.
2. Symmetrische kryptographische Verfahren erfordern ein gemeinsames Geheimnis (symmetrischer Schlüssel) aller Unternehmen in der Lieferkette. Da dieser Schlüssel mit einer gewissen Wahrscheinlichkeit aufgedeckt wird, ist die Verwendung eines identischen Schlüssels für alle Baukarten zu unsicher. Die Verteilung individueller, baukartenspezifischer Schlüssel unter den Unternehmen ist indes zu aufwendig, da bei-

spielsweise allein das Daimler-Werk in Bremen pro Jahr ca. 200.000 Autos produziert [WaHS07]. Somit wird ein Verfahren benötigt, das nur geringe Anforderungen an das Schlüsselmanagement, speziell den Schlüsselaustausch, stellt.

Beide Probleme lassen sich durch eine *Authentisierung mit abgeleiteten Schlüsseln* lösen (vgl. [Fink06]), die auf dem „Three-pass Mutual Authentication Protocol“ (ISO/IEC 9798-2) beruht. Die grundsätzliche Idee besteht darin, jede Baukarte derart mit einem individuellen kryptographischen Schlüssel k_{tid} zu sichern, dass unabhängig von der Anzahl der verwendeten Baukarten nur ein initialer Schlüsselaustausch wie folgt durchgeführt werden muss: Jeder Partner p in der Lieferkette

- erhält die von ihm benötigten Zugriffsschlüssel, die den lesenden bzw. schreibenden Zugriff auf die einzelnen Baukartensegmente steuern und
- bildet seinerseits auf sichere Art und Weise einen Masterschlüssel k_M^p. Diesen teilt er dem Baukartenhersteller mit.

Der Baukartenhersteller verfährt während der Produktion einer Baukarte für jeden Masterschlüssel wie folgt: Er leitet den Baukartenschlüssel k_{tid}^p des Partners p unter Zuhilfenahme von k_M^p aus der Seriennummer *tid* der Baukarte ab und hinterlegt ihn auf der Baukarte. Sie enthält somit für jedes Unternehmen einen mit der eigenen Seriennummer verknüpften Schlüssel. Ferner speichert der Hersteller die Zugriffsschlüssel im RESERVED-Segment der Baukarte (vgl. Abb. 2 auf Seite 5).

Den Protokollablauf zur gegenseitigen Authentisierung und anschließendem Zugriff auf ein Segment einer Baukarte zeigt Abb. 3. Die Authentisierung entspricht im Wesentlichen dem Verfahren nach ISO/IEC 9798-2. Der Unterschied besteht einerseits in der Parametrisierung des `get_challenge`-Kommandos mit der Kennung p des jeweiligen Partners sowie der zusätzlichen Übersendung der Baukartenkennung tid andererseits. Anhand dieser Informationen können die Baukarte beziehungsweise das Lesegerät den richtigen Schlüssel k_{tid}^p auswählen

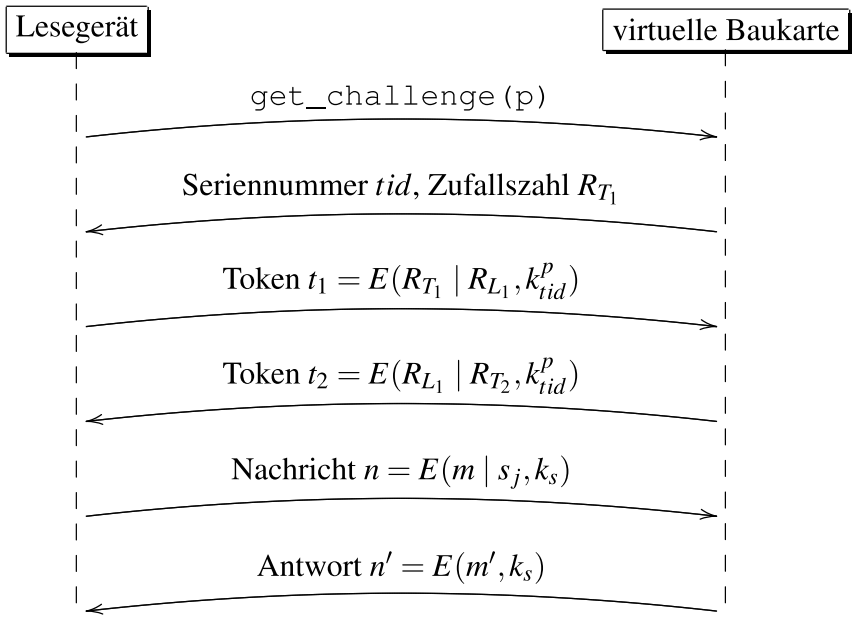

Abb. 3: Authentisierung mit abgeleiteten Schlüsseln und Zugriff auf Segment S_j der Baukarte tid

beziehungsweise berechnen.

Die Authentisierung endet mit dem Empfang des korrekten Tokens t_2 durch das Lesegerät. Um nun auf Segment S_j der Baukarte tid zuzugreifen, überträgt es das entsprechende Kommando (in Abb. 3 als n bezeichnet) und den benötigten Zugriffsschlüssel s_j^r bzw. s_j^w, der seine Autorisierung anzeigt. Diese Nachricht sowie die Antwort n' des Transponders werden mit einem Sitzungsschlüssel k_s (engl. *Session Key*) verschlüsselt, den die Kommunikationspartner aus den während der Authentisierung erzeugten Zufallszahlen berechnen. Er ist spezifisch für eine Kommunikationsverbindung und unterbindet das Wiedereinspielen der Nachrichten.

Die Sicherheit des Verfahrens hängt von der Länge der verwendeten Schlüssel und deren sicherer Verwahrung ab. Grundsätzlich besteht zwar die Möglichkeit, dass ein Angreifer Schlüssel direkt aus dem Speicher der Baukarte ausliest; den Aufwand für die dazu nötigen physikalischen Methoden schätzt das BSI allerdings als unverhältnismäßig hoch ein [BSI04]. Ferner beeinflusst der verwendete kryptographische Algorithmus die Sicherheit des Protokolls. Wir schlagen den Einsatz des Advanced Encryption Standard (AES, Rijndael) vor, der als sehr sicher gilt und sich durch seine geringen Ressourcenanforderungen und geringen Speicherbedarf [DaRi99] auch für den Einsatz in einem RFID-System eignet. Die Authentisierung eines Transponders nach ISO/IEC 9798-2 unter Verwendung von AES kann bereits effizient in RFID-Hardware umgesetzt werden, wie Feldhofer et. al. [FeDW04] zeigen.

Das vorgeschlagene Protokoll zur Authentisierung mit abgeleiteten Schlüsseln sichert die Vertraulichkeit der Zugriffsschlüssel bei geringem Aufwand in Bezug auf das Schlüsselmanagement und bietet zusätzlichen Nutzen in Bezug auf andere Bedrohungen: Wenn die Kommunikation zwischen Lesegeräten und Baukarte anhand des skizzierten Protokolls erfolgt, gelten die obigen Aussagen zur Sicherheit nicht nur für die Zugriffsschlüssel, sondern zusätzlich für die Nutzdaten (n bzw. n' in Abb. 3). Die gegenseitige Authentisierung verhindert ferner ein unautorisiertes Auslesen der virtuellen Baukarte während des Fahrzeuglebenszyklus sowie eine Manipulation der Baukartendaten z. B. durch gefälschte Lesegeräte, indem die Baukarte die Kommunikation mit nicht autorisierten Geräten abblockt.

6 Zusammenfassung und Ausblick

Die virtuelle Baukarte besitzt das Potential, die Dokumentation von Produkt- und Produktionsdaten über die gesamte Lieferkette der Automobilindustrie zu ermöglichen. Diese Anwendung erfordert, dass mehrere Partner auf eine Vielzahl von segmentierten Transpondern sicher zugreifen können, um so den kontrollierten Datenaustausch unter den Partnern einerseits sowie die geschützte Ablage vertraulicher, unternehmensinterner Daten andererseits zu erreichen. Die Basis für die erforderliche sichere Kommunikation bildet das anwendungsspezifische Protokoll zur Authentisierung mit abgeleiteten Schlüsseln. Die Besonderheit dieses Protokolls besteht darin, dass es jede Baukarte mit einem individuellen Schlüssel schützt und dennoch mit nur einem initialen Schlüsselaustausch zwischen den Unternehmen in der Lieferkette auskommt. Es ist damit speziell auf die Anforderungen zugeschnitten, die aus dem lieferkettenübergreifenden Einsatz einer Baukarte mit segmentiertem Speicher resultieren und kann in ein existierendes Sicherheitskonzept integriert werden, um so den bestehenden Sicherheitsbedenken, die den lieferkettenübergreifenden RFID-Einsatz bis dato verzögern, Rechnung zu tragen.

Bislang handelt es sich bei der virtuellen Baukarte um ein fiktives System. In der Automobilindustrie existieren zwar bereits erste – wenn auch in sich geschlossene – Ansätze, eine derartige Anwendung auch lieferkettenübergreifend umzusetzen, wobei sich neben dem Automobilher-

steller auch weitere Unternehmen wie z. B. Logistikdienstleister Zugewinne durch einen lieferkettenübergreifenden RFID-Einsatz [WaHS07] versprechen. Hier ist zukünftig jedoch Abstimmungsbedarf unter den Partnern der Lieferkette erforderlich: Eine Dokumentation der Fahrzeugdaten mittels Baukarte erfordert zunächst eine Festlegung des gewünschten Dokumentationsumfangs. So beinhaltet das in diesem Beitrag vorgestellte Szenario, dass ein Fahrzeug mit nur einem Transponder ausgestattet wird, der die Fahrzeughistorie während und im Anschluss an die Produktion dokumentiert. In einer erweiterten Anwendung könnte z. B. nicht nur das Fahrzeug selbst mit einem Transponder (als virtuelle Baukarte) versehen werden, sondern zusätzliche Komponenten des Fahrzeugs in diesen Prozess einfließen. Dies kann über weitere Transponder für einzelne Bauteile geschehen, auf denen beispielsweise der jeweilige Zulieferer Produktinformationen dokumentiert, die dann jedoch auch zusätzliche Kosten verursachen; eine alternative Möglichkeit besteht in der Nutzung von zusätzlichen EDI-Datenströmen aus den operativen Systemen des Zulieferers, die der Ware „vorauseilen“ [VDA06] und Informationen zu Bauteilen an den Fahrzeughersteller übermitteln, der diese zu Dokumentationszwecken auf der Baukarte vermerkt (vgl. auch [WaHS07]).

Modelle für eine Verteilung von Kosten und Nutzen im Wertschöpfungsnetzwerk ermöglichen, dass alle beteiligten Unternehmen vom Einsatz der virtuellen Baukarte profitieren. Sie wurden in diesem Beitrag bewusst außer Acht gelassen, sollten jedoch Gegenstand zukünftiger Forschungsarbeiten sein, um zu untersuchen, wie ein derartig komplexes System wie die virtuelle Baukarte zukünftig rentabel umgesetzt werden kann. Weiterer Forschungsbedarf besteht hinsichtlich industrieweiter, gemeinsam definierter Standards für die benötigten Hardwarekomponenten, Übertragungsprotokolle, Schnittstellen und Datenstrukturen – dieser Beitrag kann hier zwar einen grundlegenden Diskussionsansatz liefern, im Weiteren sind jedoch eine industrieweite Standardisierung durch die Vermittlung von Automobilverbänden (z. B. VDA oder ODETTE) oder einheitliche Vorgaben der Fahrzeughersteller wünschenswert.

Literatur

[BeSt03] A. R. Beresford, F. Stajano: Location Privacy in Pervasive Computing. In: *IEEE Pervasive Computing*, 2 (2003), Nr. 1, S. 46–55.

[BGSJ+05] S. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, M. Szydlo: Security analysis of a cryptographically-enabled RFID device. *In: SSYM'05: Proceedings of the 14th conference on USENIX Security Symposium*, USENIX Association, Berkeley, CA, USA (2005), S. 1–16.

[BSI04] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Risiken und Chancen des Einsatzes von RFID-Systemen (RIKCHA) – Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Bonn (2004).

[DaRi99] J. Daemen, V. Rijmen: AES Proposal: Rijndael (1999).

[EG00] Richtlinie 2000/53/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über Altfahrzeuge – Erklärung der Kommission (2000)

[Erdo06] M. Erdos: RFID and Authenticity of Goods. *In: S. Garfinkel, B. Rosenberg (Hrsg.), RFID: Applications, Security, and Privacy*, Addison Wesley Professional, Kap. 7 (2006), S. 137–148.

[FeDW04] M. Feldhofer, S. Dominikus, J. Wolkerstorfer: Strong Authentication for RFID

Systems Using the AES Algorithm. In: *Cryptographic Hardware and Embedded Systems - CHES 2004* (2004), S. 357–370.

[Fink06] K. Finkenzeller: RFID Handbuch. Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten. Hanser Fachbuchverlag, 4. Aufl. (2006).

[NIS07] National Institute of Standards and Technology: Guidelines for Securing Radio Frequency Identification (RFID) Systems: Recommendations of the National Institute of Standards and Technology. Gaithersburg (2007).

[PLHCETR06] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, A. Ribagorda: LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags. *In: Proc. of 2nd Workshop on RFID Security*, Graz (2006).

[Schä07] S. Schäfer: Konstruktion von sicheren RFID-Anwendungen. Diplomarbeit, Universität Bremen, Fachbereich 3 – Mathematik und Informatik (2007).

[StPS05] M. Strassner, C. Plenge, S. Stroh: Potentiale der RFID-Technologie für das Supply Chain Management in der Automobilindustrie. *In: E. Fleisch, F. Mattern (Hrsg.), Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis*, Springer-Verlag (2005), S. 177–196.

[VDA06] Norm VDA 5501. RFID im Behältermanagement der Supply Chain (2006).

[WaHS07] U. Waldmann, T. Hollstein, K. Sohr: Technologieintegrierte Datensicherheit bei RFID-Systemen. Bundesministerium für Bildung und Forschung, Bonn, Stand April 2007 (2007).

[Weig06] R. Weigele: Dokumentation von Produkt- und Produktionsdaten. Daimler-Chrysler AG, Rastatt (2006) – Persönliche Kommunikation.

[Weis03] S. A. Weis: Security and Privacy in Radio-Frequency Identification Devices. Masters thesis, Massachusetts Institute of Technology (2003).