

Digitale Wächter garantieren Originalität

Von Volker Klaas, Leiter Global Competence Center AutoID/RFID, Siemens IT Solutions and Services

Radio Frequency Identification (RFID) ist ein Dauerbrenner: Die kleinen, funkenden Chips tauchten erstmals vor über 40 Jahren als klobige Diebstahlsicherungen in Warenhäusern auf und werden heute branchenübergreifend für die unterschiedlichsten Szenarien eingesetzt. Nun können die Daten vom Chip 100% authentisch gemacht werden und zwar mittels Kryptografie, die auf den Gesetzen der Quantenphysik beruht. Damit wird Betrugern und Fälschern, die in lohnenden Fällen, wie bei lohnenden Markenprodukten, identische Klone von handelsüblichen Chips herstellen wollen, von vornherein das Handwerk gelegt.

Das Geschäft blüht: Ob kostspielige Markenkleidung und Schmuck, hochwertige Lebensmittel oder teure Ersatzteile für Maschinen und Autos, Marken- und Produktpiraterie ist schon lange eine lohnende Tätigkeit für Kriminelle. Wie rentabel und vor allem verbreitet sie tatsächlich ist, zeigen folgende Zahlen: So haben die europäischen Zollbehörden 2008 insgesamt 178 Millionen gefälschte Artikel beschlagnahmt. Die von der Europäischen Kommission vorgelegten Zahlen bedeuten eine Verdoppelung gegenüber dem Vorjahr. Besonders beliebt waren bei den Fälschern Elektrogeräte und Arzneimittel.

Ebenfalls zu denken gibt eine aktuelle Studie der Beratungsgesellschaft Ernst & Young, die mit Unterstützung des Mar-

kenverbandes erstellt wurde. Der zufolge entsteht den europäischen Konsumgüterherstellern durch Produkt- und Markenpiraterie jährlich ein Schaden von rund 35 Milliarden Euro. Das entspricht etwa zwei Prozent ihres gesamten Jahresumsatzes. Befragt wurden dafür 2.500 europäische Verbraucher und 27 europäische Konsumgüterhersteller.

Nur noch Rauschen statt Lauschen

Gründe genug also für Hersteller und alle Teilnehmer der Supply Chain, Gegenmaßnahmen zu treffen. Zu den wichtigsten zählen dabei Personalauswahl, Zutrittskontrolle und IT-Sicherheit. Was letztere betrifft, so setzen Siemens IT Solutions and Services und Siemens Corporate Technology dabei auf RFID und auf innovative Wege. Denn während konventionelle Funkchips mit einem geheimen Schlüssel arbeiten, den sowohl das Tag als auch das Lesegerät kennen, ein symmetrisches Verfahren also, sind die neuen Krypto-RFID-Chips zusätzlich mit einer kryptografischen Hardwareeinheit ausgestattet. Diese ermöglicht ein asymmetrisches Verfahren, das um ein Vielfaches sicherer ist.

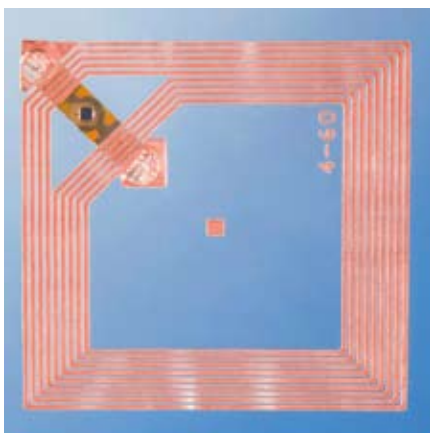
Bisher sind auf den handelsüblichen Transpondern beispielsweise Pro-

duktdaten oder Seriennummern verschlüsselt gespeichert. Per Funk empfängt der Reader diese Informationen und dekodiert und verarbeitet sie mit demselben geheimen Schlüssel, der aus einer Reihe zufällig gewählter Datenbits besteht. In besonders lohnenden Fällen haben es Kriminelle manchmal geschafft, den geheimen Schlüssel zu stehlen oder zu kopieren, um damit identische Klone zu erschaffen. Basierend auf dem Public-Key-Konzept, wie es bereits zur Verschlüsselung von E-Mails oder digitalen Signaturen verwendet wird, haben die RFID-Experten nun aber ein absolut fälschungssicheres System entwickelt. Es arbeitet mit einem öffentlich zugänglichen Schlüssel, der per se für Hacker uninteressant ist. Jedes neue RFID-Etikett verfügt aber über einen geheimen, privaten Schlüssel, mit welchem der Chip die Prüfanfrage des Lesegeräts kodiert.

Der Clou:

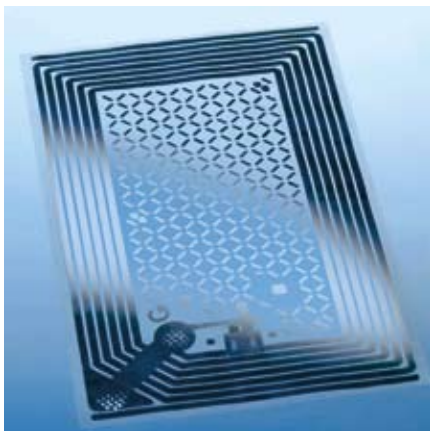
Ein RFID-Tag mit Fingerprint

Damit aber nicht genug: Der IT-Dienstleister und die Innovationsschmiede des Siemens-Konzerns haben zusätzlich einen kryptografischen Algorithmus entwickelt, der mit elliptischen Kurven rechnet. Durch dieses dynamische Verfahren hat der Chip ein zusätzliches Si-



Ein alter RFID-Chip mit Kupferleitbahnen

cherheitsmerkmal, das so eindeutig und authentisch ist, dass man es mit dem Fingerprint einer Person vergleichen kann. Das Lesegerät stellt jedes Mal eine neue Anfrage und der Chip muss ebenfalls neu rechnen und eine andere, aber genau zu der Anfrage passende Antwort geben. Ergo können Kriminelle nur veraltete und damit nutzlose Informationen kopieren. Was die Lesegeräte betrifft, so ist Standardequipment völlig ausreichend. Die Reader laden einmalig ein Zertifikat herunter und sind dann einsatzbereit für den Krypto-Chip. Seit März 2009 wird der neue Chip erstmalig getestet und kann direkt in Produkten oder deren Verpackung angebracht werden. Je nach Stückzahl kann der Preis des Krypto-Chips, der generell unter 50 Cent pro Tag kosten soll, sogar unter 15 Cent sinken.



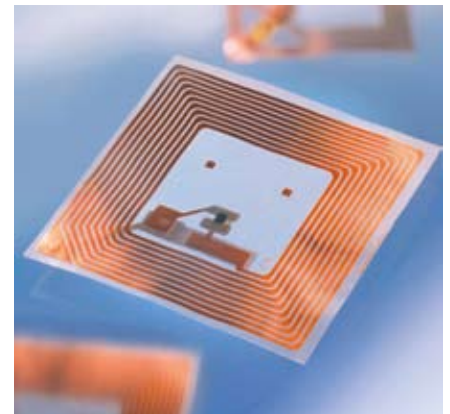
Der neue Krypto-RFID-Chip von Siemens

Umfassendes Portfolio aus einer Hand

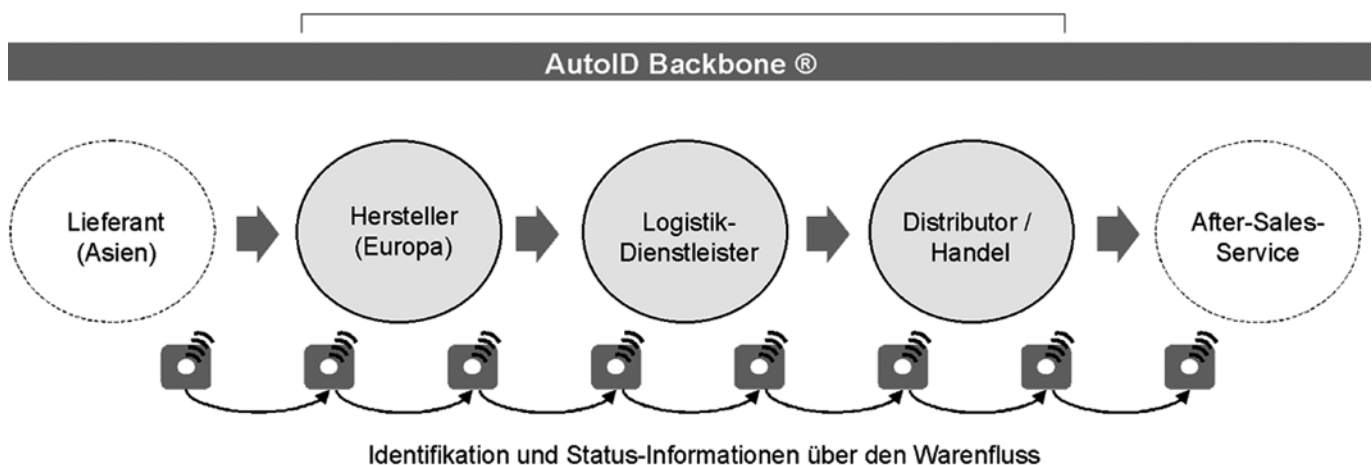
Siemens kennt die strategische Bedeutung von RFID und treibt den Fortschritt auf diesem Gebiet seit über 25 Jahren konsequent voran. Als weltweit führender Anbieter verfügt der Konzern über ein lückenloses Portfolio an Hard- und Software – abgerundet durch Prozessberatung, Systemintegration und Projektmanagement, was die Realisierung von RFID-Komplettlösungen von A bis Z aus einer Hand ermöglicht. In jedem Fall profitieren die Kunden von fundiertem Technologie- und Branchen-Know-how. Siemens ist darüber hinaus Mitglied bei EPCglobal, ETSI und der Future Store Initiative, den führenden Organisationen in der Entwicklung von RFID-Standards.

Quelle: http://www.automation.siemens.com/rfid/_media/e20001-a180-p871.pdf

Die Hauptanwendungsszenarien liegen im Plagiatsschutz für hochwertige Konsumgüter, wie zum Beispiel Bekleidung, Sportgeräte oder Konsumelektronik. Der Krypto-Chip ist aber generell interessant für alle Branchen, die höherwertigere Waren anbieten, deren Echtheit für das Geschäft und das Image entscheidend sind. Verhindert werden kann der Graumarkt damit zwar nicht, aber wesentlich eingedämmt und die Regressansprüche an die Hersteller logischerweise auch. Mit Blick auf die weltweiten Warenströme kann der Zoll ebenfalls profitieren: Wenn Ware importiert und exportiert wird, ist mittels der auf dem Chip gespeicherten und fälschungssicheren Informationen schnell feststellbar, um was es sich wirklich handelt, um somit



Zoll und Steuer korrekt berechnen zu können. In der Textilbranche können die Tags sowohl innerhalb der Kleidung angebracht werden, also zum Beispiel ins Futter eingenäht, oder außerhalb. Wichtig dabei: Der Kunde darf sich nicht

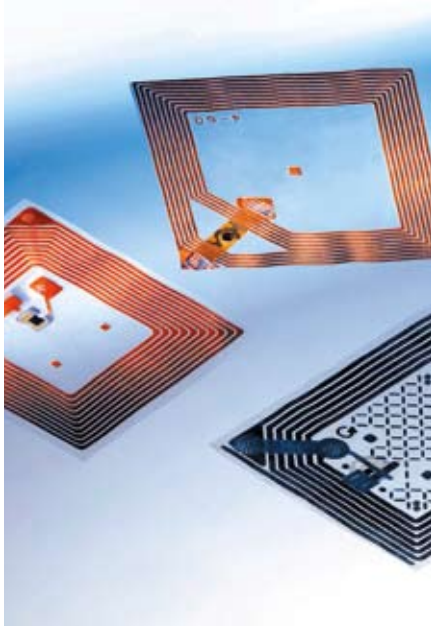


Services für die automatische Identifikation (AutoID) sorgen für die digitale Vernetzung der Partner entlang der gesamten Lieferkette. Sie optimieren Informations- und Warenflüsse. (Quelle: Siemens)

gestört fühlen und die Ware darf nicht beschädigt werden. Da auf dem Chip keine personenbezogenen Daten zu finden sind, ist auch keinerlei Tracking von Personen und ihren Angewohnheiten möglich.

**Sicherheit: Nicht messbar,
aber machbar**

Auch wenn RFID in Logistik und Handel inzwischen etabliert ist, wird dort überwiegend noch mit fälschbaren Tags und nicht mit Sicherheitstranspondern gearbeitet. In vielen Anwendungen ist das nicht kritisch, aber Ausnahmen bestätigen wie immer die Regel. Nachdem die Technik mittlerweile ausgereift ist und Logistik und Handel seit langem erfolgreich und prozessoptimierend mit den Funkchips arbeiten, rücken nun aber immer mehr der Sicherheitsaspekt und damit auch der Verbraucherschutz in den Vordergrund. Entsprechend steigt die Nachfrage nach Anwendungen wie dem Krypto-Chip. Erste Förderprojekte zum Thema Plagiatsschutz zeigen zudem, dass das Thema von Forschung und Wirtschaft ernstgenommen wird. In den Unternehmen hingegen gibt es noch Aufklärungsbedarf.

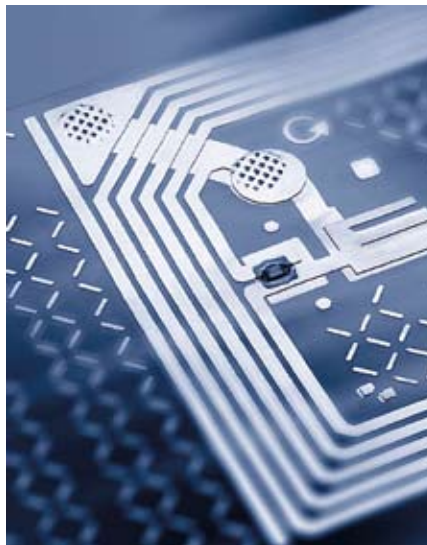


Alte und neue Generation der RFID-Chips im Vergleich

Vorteile aus einer Hand – auf einen Blick

- Über 25 Jahre Erfahrung
- Dutzende erfolgreich implementierte RFID-Projekte
- Erfahrung mit globalen Supply Chains durch eine der weltweit ersten transatlantischen RFID-Implementierungen
- Aktives Mitglied in einem weltweiten Wissensnetzwerk / Zusammenarbeit mit Universitäten, Standardisierungs-Gremien etc.
- Mehrere Technologiezentren und Laboratorien
- Globale Unterstützung für ausgedehnte Supply Chains
- Weltweit präsent mit erfahrenen Mitarbeitern
- Umfassende, langjährige Erfahrung bei der Realisierung von komplexen Projekten
- Engagement in Forschung und Entwicklung (Polymer-Elektronik, RFID-Lösungen)
- zur Fälschungssicherheit, Integration von RFID und Sensorik etc.)

Quelle: http://www.automation.siemens.com/rfid/_media/e20001-a180-p871.pdf



Der neue Krypto-RFID-Chip von Siemens im Detail

Da eine quantitative Bewertung von Sicherheit beinahe unmöglich ist, sollte das große Ganze betrachtet werden: Anwender sollten Sicherheit nicht nur als einen singulären Punkt betrachten, sondern als Ganzes.

Im Handel beispielsweise gilt es, alle Stufen der Wertschöpfungskette zu beachten: den Hersteller, die Logistikkette, den Point of Sale. Wenn man dann die notwendigen Sicherheitsgrade identifiziert und festgelegt hat, beginnt man

mit der Implementierung des Systems. Dabei geht es unter anderem um die Integration des Chips in konkrete, gegen Plagiate zu schützende Produkte, um die erforderliche Infrastruktur ebenso wie um die möglichen Prozesse zur Absicherung der Vertriebswege.

**Kosten-Nutzen-Faktor
überzeugt**

Was die Hardware betrifft, wird derzeit ein RFID-HF-Chip nach ISO-Standard 15693 genutzt, der auf 13,56 MHz funkt. Statt eines programmierbaren Prozessors setzten die Experten eine fest verdrahtete Logik, auch bekannt unter dem Begriff Rechenwerk, in die Tags ein. Das senkte nicht nur den Energieverbrauch, sondern auch den Kostenfaktor – wichtige Eigenschaften, die diese vollautomatische, nicht-proprietäre Technologie mit leicht erweiterbarem Protokoll in kurzer Zeit sicher fest im Markt verankern werden.

Die Vorteile des Krypto-Chips liegen auf der Hand: Neben maximaler Sicherheit bietet er einen attraktiven Preis, der nur rund ein Zehntel dessen beträgt, was

vergleichbare Smart-Card-Technologien für eine sichere Zugangskontrolle kosten. Zudem deckt er die gesamte Wertschöpfungskette vom Hersteller und Lieferanten bis hin zum Kunden ab und ermöglicht eine Echtheitsüberprüfung ohne Datenbankanbindung. Eine Onlineverbindung ist nicht nötig, die Ergebnisse liegen in Zehntelsekunden vor. Andere Schutzmaßnahmen wie etwa Hologramme oder Wasserzeichen können da nicht mithalten. Neben dem privaten Schlüssel, der nicht ausgelesen werden kann, und einem Zertifikat verfügt der Chip zudem über einen Anwenderspeicher von 256 Bit, genug Platz, um zum Beispiel eine weltweit eindeutige Produktnummer nach dem EPCglobal-Standard aufzunehmen.

www.siemens.com/rfid

GCS
CONSULTING

Die GCS Consulting,
Gesellschaft für Consul-
ting und Synergie mbH,

ist eine Unternehmensberatung mit Sitz in München, die ihren Branchenfokus in der Textil-, Bekleidungs- und Schuhindustrie hat. Seit 2004 betreibt die GCS Consulting eine RFID Initiative namens fashion group RFID, in der sich „Early Mover“ aus Modehandel und Bekleidungsindustrie regelmäßig treffen, um Erfahrungen auszutauschen, gemeinsam Hardware einzukaufen und das Thema RFID im deutschen Fashionbereich auf der Basis bestehender Standards nach vorne zu bringen.

www.gcs-consulting.de

www.fashiongroupRFID.com



Helmut Gilbert,
Managing Partner
GCS Consulting



Volker Klaas,
Leiter Global Competence
Center Auto ID/RFID,
Siemens IT Solutions and
Services (Foto: Siemens)

Neue Richtlinien von GS1 EPC global

Ein Etikett optimiert Logistikprozesse

EPC global, die Radiofrequenzidentifikation(RFID)-Initiative von GS1, hat jetzt eine neue Richtlinie veröffentlicht. Sie legt Standards fest, wie die üblichen proprietären Diebstahlsicherungstechniken durch RFID-Technologie in Ein- oder Mehrwegetiketten ersetzt werden können.

Avery Dennison hat diese neuen Richtlinien als Partner von EPCglobal mitentwickelt. Das Unternehmen ist überzeugt, dass die Standards allen Beteiligten entlang der Wertschöpfungskette von der Bekleidungsherstellung bis zum Einzelhandel zugute kommen werden. Durch diese Technik ist es möglich, einerseits die Logistikprozesse zu optimieren und andererseits die Warensicherung in den Läden zu gewährleisten. Die Stärken der EPC/RFID- und der EAS-Technologie (Electronical Article Surveillance = Elektronische Warenüberwachung) sind hier in einem einzelnen Etikett vereint, ein nachträgliches Auszeichnen mit Warensicherungsetiketten entfällt. Das bringt viele Vorteile, erklärt Paul Chamandy, Leiter der Abteilung New Business Development bei Avery Dennison: „Diese Richtlinien zeigen, wie das kombinierte RFID/EAS-System eingesetzt werden kann. In der Praxis eröffnet das eine Vielzahl von Möglichkeiten Kosten einzusparen, den Betrieb effizient zu machen und die Lagerhaltung zu präzisieren.“

Chris Adcock, der Präsident von EPC global Inc., sieht in den Standards ein neues Modell, mit dem die Einzelhändler ihre Diebstahlverluste sichtbar machen und managen können. Avery Dennison beliefert Einzelhandel, Markenbesitzer und Hersteller mit einer kompletten Serie von Tags und Etiketten, die mit der RFID-basierten EAS-Technologie ausgestattet

werden können. Viele große Einzelhändler bauten bereits bei der Einführung eines globalen EAS-Programms mit Quell-Tags und bei der Umsetzung von RFID-Programmen auf Warenebene auf die Erfahrung von Avery Dennison. Im Einzelhandel gibt es bisher verschiedene Standards für Diebstahlsicherungssysteme. Denen ist allen gemeinsam, dass sie dem Händler lediglich sagen, dass ein Diebstahl vorliegt, wenn ein Produkt den Laden verlässt. Sie sagen ihm nicht, was genau gestohlen wurde. Die RFID-basierte Warensicherung liefert darüber hinaus Informationen zum spezifischen Produkt. „Das bringt mehr Transparenz. Die Händler können solche Verluste jetzt schnell und exakt in den Regalen nachfüllen“, meint Chamandy.

Die unterschiedlichen EAS-Technologien haben bisher die Ausstattung mit Quell-Tags zur Warensicherung behindert. Je nach Technologie, die der Händler bei der Diebstahlsicherung nutzte, musste er die Waren nachträglich und aufwändig mit unterschiedlichen Etiketten versehen. „Wir gehen davon aus, dass durch die neuen Richtlinien der Prozess einheitlicher und die Anwendung von RFID-Quell-Tags auf Warenebene vereinfacht wird“, sagt Chamandy.

www.epcglobalinc.org

www.gs1.org

www.eu.averydennison.com