

Corporate Technology

Für die Fachpresse

München, 17. Oktober 2006

Sicherer funken – RFID-Etiketten mit digitalem Echtheitszertifikat

RFID-Etiketten zur berührungslosen Erfassung von Waren erfreuen sich wachsender Beliebtheit. Doch der Schutz der Funkinformation vor Produktpiraten ist nur mit einer aufwändigen lokalen Infrastruktur zu gewährleisten. Siemens-Entwickler haben effiziente Sicherheitsverfahren entwickelt, die sich auf den winzigen RFID-Chips implementieren lassen. Damit kann die Sicherheit dieser Etiketten und der auf ihnen gespeicherten Daten mit wesentlich geringerem Aufwand gewährleistet werden.

Funketiketten – so genannte RFID-Chips (Radio Frequency Identification Devices) – sind auf dem besten Wege, sich in der Logistik und bei der individuellen und fälschungssicheren Markierung von Waren zu etablieren. RFID-Etiketten, so genannte Tags, tragen in ihrem Inneren einen Chip, der Informationen wie Zieladresse oder Haltbarkeitsdatum enthält. Per Funksignal lassen sich diese Informationen abrufen – etwa im Wareneingang einer Firma. Anders als beim Barcode ist dafür keine Sichtverbindung nötig. Die kleinen Datenträger lassen sich sogar durch Verpackungen hindurch auslesen. Doch ohne Schutzmaßnahmen hat die drahtlose Funkverbindung ihre Tücken, und die über die Luft transportierten Daten könnten von Produktpiraten ausspioniert werden. Gelingt es beispielsweise, den Datensatz oder die Identifikationsnummer von hochwertiger Markenkleidung zu kopieren, könnten diese beliebig vervielfältigt und auf unechte Funketiketten geschrieben werden. Günstige Imitate würden sich in der ganzen Lieferkette als wertvolle originale Ware ausweisen. Es gilt also, den RFID-Funkverkehr fälschungssicher zu machen. Heute existierende Verfahren gewährleisten zwar eine ausreichende Datensicherheit, sind jedoch mit einem verhältnismäßig hohen Rechenaufwand verbunden. Weniger rechenintensive

1 / 4

Verfahren wiederum erfordern eine aufwändige Infrastruktur und passten bisher nicht auf die kleinen RFIDs. „Unser Ziel war es, unseren Kunden eine Lösung anzubieten, die sie unabhängig von der Infrastruktur macht, und beispielsweise den permanenten Anschluss an eine Datenbank erübrigt“, so Lechner. „Wir haben nach einer Lösung gesucht, mit der mobil und autark die Echtheit von RFIDs geprüft werden kann.“

Mathematiker aus dem Bereich Corporate Technology (CT) in München haben jetzt eine Methode gefunden, die benötigten Verfahren so weit zu verdichten, dass sie weltweit erstmals auch auf RFIDs ablaufen können. Dadurch wird der Echtheitsnachweis anwenderfreundlich und im großen Stil einsetzbar. Die Forscher aus München setzen dabei auf das so genannte asymmetrische Verschlüsselungsprinzip, das Fachleute von der „symmetrischen Verschlüsselung“ abgrenzen. Bei der herkömmlichen symmetrischen Verschlüsselung arbeitet das Lesegerät, mit dem man den Code scannt, und das Funketikett mit demselben geheimen Schlüssel. Das ist eine sehr komplexe Lösung, weil man im Lesegerät mitunter Hunderte von RFID-Schlüsseln für viele verschiedene Produkte abspeichern muss. Zwar lässt sich ein Lesegerät z.B. via Internet mit einer Datenbank koppeln, die die Schlüssel verwaltet, aber auch das erhöht die Komplexität des gesamten RFID-Systems.

Mit dem asymmetrischen System vermeiden die Forscher aus München einen derartigen Datenwust, denn bei diesem Verfahren benötigt nur der RFID-Code eine Art Sicherheitszertifikat. Dieses Zertifikat kann zwar vom Lesegerät erkannt, aber weder kopiert noch verändert werden. Möglich macht das eine komplexe mathematische Signatur der Etikett-Information. Für gewöhnlich werden für die Generierung dieser Signatur lange Primzahlen miteinander multipliziert, wofür umfangreiche Datenmengen gespeichert werden müssen. Von den Chips auf EC-Karten oder Smart-Cards können diese Datenmengen zwar problemlos verarbeitet werden, die Leistung eines winzigen Funketiketts sprengten sie bislang aber bei weitem. Nicht so bei der neuen Methode. Den Forschern gelang es dank intelligenter Berechnung, die Datenmenge um mehr als die Hälfte zu reduzieren. „Wir stellen die Information nicht mit großen Primzahlen dar, sondern – auch das ist ein weit verbreitetes Verfahren – als Punkte auf einer Kurve“, erklärte Dr. Stephan Lechner, Leiter des Bereichs Sicherheitsforschung bei CT. „Die Reduktion erreichen wir, indem wir einfach Koordinaten weglassen. Wir weben eine Art

mathematisches Netz, das zwar ausgedünnt ist, auf dessen Tragfähigkeit wir uns aber verlassen können.“ Die neue Siemens-Methode arbeitet so platzsparend, dass sich damit erstmals asymmetrische Verfahren auf RFID-Chips unterbringen lassen. Das ist vor allem deshalb bemerkenswert, weil das Thema noch Ende 2004 für so schwierig gehalten wurde, dass es in der internationalen Studie des Bundesamts für Sicherheit in der Informationstechnik keine Berücksichtigung findet.

Künftig könnten mit dem neuen Verfahren RFID-Etiketten für die berührungslose automatische Zugangskontrolle ausgerüstet oder beispielsweise Musik- und Software-CDs mit eingearbeiteten oder aufgeklebten Tags versehen werden. Mit dem neuen Verfahren kann beispielsweise der Zoll die Echtheit der Ware an jeder beliebigen Stelle des Transports mobil überprüfen. Eine weitere Anwendung sind Frachtpapiere. „Es kommt heute durchaus vor, dass ganze Container mit Hilfe gefälschter Frachtpapiere von Lagerplätzen gestohlen werden“, sagte Lechner. „Will später der rechtmäßige Besitzer die Ware abholen, ist sie bereits weg.“ Um derlei Diebstahl zu vermeiden, könnten Frachtpapier und Container über RFID-Etiketten mit asymmetrischer Kryptographie gekoppelt werden. Nur wenn das Frachtpapier das richtige Zertifikat enthält, wird die Ware ausgeliefert. „Bei dem Volumen der anfallenden Frachtpapiere ist eine solche Echtheitskontrolle nur mit einer dezentralen Zertifikatsüberprüfung auf einem mobilen Endgerät praktikabel. Dafür liefern wir jetzt erstmalig die Voraussetzungen.“ Lechner und seine Mitarbeiter passen ihre Methode derzeit an unterschiedliche Anwendungen in den Siemens-Bereichen an. Künftig soll dann die asymmetrische Kryptografie auf RFID-Etiketten auch externen Kunden zur Verfügung stehen.

Passende Pressefotos in druckfähiger Auflösung finden Sie unter
<http://www.siemens.com/ct-bild/ct200610002>



Güteridentifizierung und -verfolgung in der Logistikkette. Dabei werden Daten zwischen dem Objekt und dem RFID-Lesegerät ausgetauscht. Um zu vermeiden, dass die ausgetauschten Daten abgehört und manipuliert werden können, sind effektive Sicherheitsmaßnahmen nötig. Ein weltweit einzigartiges, patentiertes kryptographisches Verfahren von Siemens Corporate Technology bietet genau dies.