

Den Fälschern auf der Spur

RFID als wirksames Mittel gegen Produktpiraten

Der Schaden ist enorm: Produktfälschungen kosten allein der deutschen Wirtschaft jährlich rund 30 Milliarden Euro. Zur Abwehr könnten RFID-Transponder in jedes Produkt eingebracht werden, doch bislang sind die Funkchips leicht zu kopieren. Nicht so mit einer Erfindung von Siemens: Durch kryptografische Algorithmen ist der neue RFID-Crypto-Chip fälschungssicher.

Mit der Globalisierung und der weltweiten Verteilung von Warenströmen haben auch Produktfälscher neue Möglichkeiten gefunden, ihre Erzeugnisse in die Märkte zu schleusen. Von Bekleidung bis zu Uhren, von Elektronikgeräten bis zu Parfüm gibt es kaum einen Konsumartikel, der nicht gefälscht wird. Die Konsequenzen für die Hersteller der Originale sind erheblich: Neben entgangenen Umsätzen können erhebliche Image-Schäden entstehen, wenn das vermeintliche Marken-Schnäppchen nach kurzer Zeit den Geist aufgibt. Bei manchen kopierten Produkten wie Bremsscheiben, Maschinenteilen oder Arzneimitteln geht es aber um weit mehr als nur um Geld: Die schlechte Qualität kann zu Unfällen und anderen, ernsten Gesundheitsrisiken führen.

Durch die Serialisierung der Produkte (Zuordnung einer eindeutigen Identifikationsnummer) soll ein erster Schutz gegen Fälschungen erreicht werden. An jeder Übergabestelle wird diese ID per 2D-Code oder RFID erfasst und in einer zentralen Datenbank abgelegt. Hierdurch soll die Distribution eines Produkts lückenlos nachverfolgt werden können. Doch die eingesetzten Identifikationsmethoden bieten selbst keinen Kopierschutz. Ein handelsüblicher RFID-Transponder besitzt das Sicherheitsniveau einer Postkarte – jeder kann den Chip auslesen und kopieren – und verfügt über kein eigenes Echtheitsmerkmal. Bei einem Vergleich eines echten und eines gefälschten Produkts kann somit nur die Tatsache einer Fälschung festgestellt werden – welches der beiden Produkte das Original ist, bleibt offen.

Siemens Corporate Technology hat deshalb einen fälschungssicheren RFID-Chip entwickelt, der Produktpiraten das Handwerk legen soll. Hierzu wurde ein RFID-Transponder nach ISO 15693 um ein Authentifizierungsverfahren auf Basis der Public-Key-Kryptografie ergänzt. Dabei codiert der Chip eine Prüfanfrage des Lesegerätes mit seinem privaten Schlüssel. Der Empfänger kann die Antwort auf diese Anfrage mit dem dazugehörigen öffentlichen Schlüssel auf seine Richtigkeit überprüfen - innerhalb einer

Zehntelsekunde. Der besondere Vorteil: Hat das Lesegerät den öffentlichen Schlüssel einmal geladen, benötigt es zur eigentlichen Überprüfung keine Online-Verbindung ins Internet. Zudem kann die Überprüfung automatisch erfolgen, zum Beispiel beim Kassiervorgang im Einzelhandel.

Bis heute waren solche Verfahren bei den kleinen RFID-Chips aufgrund mangelnder Rechenleistung und Energieversorgung nicht möglich. Mit optimierten Algorithmen konnten die Siemens-Forscher die notwendige Rechenleistung deutlich reduzieren. Statt eines programmierbaren Prozessors haben sie feste, nicht programmierbare Schaltungselemente eingesetzt. Somit wurden der Energieverbrauch und die für den Kostenfaktor wichtige Größe des Chips erheblich gesenkt. Der Transponder arbeitet auf der weltweit standardisierten Frequenz von 13,56 MHz und ist kompatibel zur Norm ISO 15693. Neben dem privaten Schlüssel, der nicht ausgelesen werden kann, und einem Zertifikat bietet der Chip noch 256 Bit Anwenderspeicher – genug Platz, um zum Beispiel eine weltweit eindeutige Produktnummer nach dem EPCglobal-Standard aufzunehmen.

Zur Authentifizierung werden gängige RFID-Lesegeräte eingesetzt, denn durch das Public-Key-Verfahren sind keine besonderen Sicherheitsmaßnahmen auf Seiten der Leser erforderlich. Auch eine Implementierung auf Handheld-Geräten oder Mobiltelefonen ist denkbar. Die Überprüfung kann zum Beispiel beim Zoll im Rahmen einer Grenzbeschlagnahme, im Handel an der Kasse oder – mit einem RFID-fähigen Mobiltelefon – beim Konsumenten selbst durchgeführt werden.

Für den fälschungssicheren RFID-Chip gibt es breite Anwendungsfelder. Der günstige Transponderpreis, der nur wenig über vergleichbaren Funkchips ohne Kryptografie liegen wird, macht das hohe Sicherheitsniveau für viele Applikationen nutzbar. So können Dokumente aller Art ein neues Sicherheitsmerkmal erhalten, das automatisch überprüft werden kann, zum Beispiel Frachtpapiere oder Ausweise. Auch für anspruchsvolle Zugangskontrollsysteme, die bislang nur über teure Smart Cards realisiert wurden, ist der neue Crypto-Chip geeignet.

Siemens AG
Competence Center RFID
Gleiwitzer Straße 555
90475 Nürnberg

www.siemens.de/rfid
Email: info.rfid@siemens.com