

Vortrag RFID

Sebastian Amend

- RFID steht für „radio-frequency identification“ (Deutsch: „Identifizierung mit Hilfe elektromagnetischer Wellen“)
- automatische Identifizierung und Lokalisierung von Gegenständen und Lebewesen
- Erfassung von Daten wird erleichtert

Ein RFID-System besteht aus:

- Transponder
- Lesegerät (Reader)
- Software (Schnittstelle zum EDV System)

Geschichte:

- 1. Anwendung während des 2. Weltkrieges: zur Erkennung der eigenen Panzer und Flugzeuge.
- Nachfolgesysteme werden noch heute eingesetzt
- Ende der 1960er Jahre SICARID (Siemens Car Identification): eindeutige Identifizierung von Eisenbahnwagen und Autoteilen in der Lackiererei
- 1970er Jahre: elektronische Warensicherungssysteme mit 1 Bit Speicherkapazität. Prüfung, ob Markierung vorhanden, Alarm / kein Alarm
- 1980er Jahre: mehrere US-Staaten und Norwegen setzen RFID Technik für Mautsysteme ein

Funktion

- Reader erzeugt hochfrequentes, elektromagnetisches Feld → Transponder wird dem Feld ausgesetzt
- Stromversorgung des Transponders → siehe Transponderarten
- Mikrochip im RFID-Tag decodiert Signal → Antwort erfolgt entweder durch Feldschwächung oder gegenphasige Reflexion

Transponder

Deutlichstes Unterscheidungsmerkmal der Transponder ist Energieversorgung

Passive Transponder

- versorgen sich aus Funksignalen des Readers
- mittels Induktion wird ein Kondensator aufgeladen, welcher als Energiequelle dient
- Bis Kondensator geladen ist → Latenzzeit
- Nachteile: Geringe Leistung, kurze Reichweite, Latenzzeit
- Anwendung: viele, günstige Transponder werden gebraucht, z.B. Auszeichnung von Produkten

RFID-Transponder mit eigener Energieversorgung:

- höhere Reichweiten u. geringere Latenzen
- einen größeren Funktionsumfang (z.B. Temperaturüberwachung von Kühltransporten)
- Nachteil: deutliche höhere Kosten
- Anwendung: dort, wo zu verfolgende Objekte selbst teuer sind (z.B. wiederverwendbare Container in der Containerlogistik)
- Befinden sich meist im Ruhezustand (sleep modus) bis sie vom Reader getriggert werden → Lebensdauer der Batterie erhöht sich (bis zu Jahre)

Man unterscheidet zwei Arten von Transpondern mit eigener Energieversorgung:

- Aktive RFID-Transponder nutzen Batterie sowohl für Versorgung des Mikrochips als auch zur Erzeugung des Rücksignales. Sehr große Reichweite.
- Semi-aktive (oder semi-passive) Transponder besitzen keinen eigenen Sender, sondern beeinflussen nur das Elektromagnetische Feld → keine so große Reichweite, andere Vorteile bleiben bestehen

RFID versus Barcode

- Barcode und RFID-Chip ähneln sich (vergleichbare Einsatzgebiete)

Unterschiede:

- Barcode muss in die Nähe des Scanners gebracht werden → RFID funktioniert auch über eine gewisse Distanz
- Barcode nur lesbar → RFID-Chip kann gelesen und beschrieben werden
- RFID-Chips sind störungsresistenter als Barcodes (z.B. Verschmutzung)
- RFID-Chip liefert mehr Infos als Barcode (Barcode zeigt nur Art des Produktes, RFID zeigt um welches Produkt es sich genau handelt etc.)

nPA

Einführung wurde am 18. Dezember 2008 vom Deutschen Bundestag beschlossen. FDP (seit 2009 mitregierend) wollte Aussetzung bis 2020, war nicht erfolgreich.

Neuheit ggn. altem Ausweis:

- Scheckkartenformat
- Eingebauter RFID-Chip, der hoheitliche und nicht hoheitliche Funktionen unterstützt.

Hoheitliche Funktionen

- Entspricht in Grunde ePass
- Unterschied: Speicherung der Fingerabdrücke ist freiwillig
- nPA kann also als Passersatz für Reisen innerhalb der EU verwendet werden

Die biometrischen Daten dürfen nur von folgenden Behörden ausgelesen werden:

- Polizeivollzugsbehörden
- Zollverwaltung
- Steuerfahndungsstellen der Länder
- Pass-, Personalausweis- und Meldebehörden

Daten können im Gegensatz zum ePass auch geändert werden

Folgende Daten können die Behörden ändern:

- Ein- und Ausschalten der eID-Funktion
- Wechsel der Wohnadresse und damit ggf. des amtlichen Gemeindeschlüssels (Adresse auf Ausweis muss weiterhin überklebt werden)
- Neusetzen der Geheimnummer

Andere Daten, z.B. neuer Name nach Eheschließung, können nicht geändert werden → neuen Ausweis beantragen

Nicht hoheitliche Funktionen

eID-Funktion

- nPA soll im Internet auch als Identitätsnachweis dienen
- Benutzer kann sich ggnüber Behörden oder privaten Firmen im Internet ausweisen → AusweisApp (entwickelt von Siemens, der Bundesdruckerei und OpenLimit)
- Dienstanbieter müssen sich ggnüber nPA authentifizieren → Zugriff auf bestimmte, freigeschaltete Datenfelder des nPA nach Eingabe des PINs durch Benutzer
- Dienstanbieter muss sich bei zentraler Bundesstelle ein elektronisches Berechtigungszertifikat besorgen → Datenfelder, die ausgelesen werden dürfen, werden festgelegt

Die eID Funktion ist auf jeden Personalausweis standardmäßig eingeschaltet → kann man aber abschalten lassen

- Folgende Daten können durch Eingabe der PIN freigegeben werden:
- Vor- und Familienname, ggf. Ordens- und Künstlername oder Doktorgrad
- „D“ für Bundesrepublik Deutschland
- Angaben zur Über- oder Unterschreitung eines bestimmten Alters (Altersbestätigung)
- Geburtstag und Geburtsort
- Anschrift
- Dokumententyp
- Angabe, ob der eigene Wohnort einem abgefragten Wohnort entspricht (Wohnortbestätigung)

.

Alter- und Wohnortbestätigung

Dienstanbieter können Alter- oder Wohnortbestätigung abfragen, ohne dass die wirklichen Daten übertragen wird, sondern lediglich Bestätigung oder Verneinung (z.B. Online-Wetten: Ist Benutzer über 18?)

Digitale Unterschrift

Damit können digitale Dokumente unterschrieben werden

Benötigt:

- Signatur-PIN (eigene PIN, vgl. PIN für eID)
- Komfortlesegerät

Ein Signaturzertifikat muss auf den RFID-Chip des nPA geladen werden → muss bei speziellen Dienstleistern beantragt werden → funktioniert im Moment noch nicht

Drei Varianten des Kartenlesegerätes (unterschiedliche Sicherheitsstandards)

- Basisversion: PIN-Eingabe über PC-Tastatur
 - o Nachteil: Keylogger können PIN ausspähen
- Standard- und Komfortkartenleser: haben eigenes Tastenfeld

Sicherheit

- Kommunikation erfolgt grundsätzlich verschlüsselt

Sicherheitsprotokolle:

BAC (Basic Access Control)

- Kommt zum Einsatz, wenn nPA als Passersatz verwendet wird
- BAC Protokoll gilt als unsicher
- Verwendet Triple-DES-Algorithmus (112 Bit Verschlüsselung) → allerdings werden nur Geburtsdatum, Ablaufdatum und Dokumentennummer zur Schlüsselerzeugung verwendet
- Um Verschlüsselungsstärke zu erhöhen, werden in Deutschland alphanumerische Dokumentennummern eingesetzt (A, B, D, E, I, O, Q, S, U) → ca. 64 Bit
- Niederlande besonders starke Einschränkungen bei Seriennummer → Verschlüsselungsstärke von nur 35 Bit → Firma Riscure konnte bereits 2006 RFID-Daten innerhalb weniger Stunden entschlüsseln

PACE (Password Authenticated Connection Establishment)

- Findet bei den anderen Funktionen des nPA Verwendung (z.B. eID)
- Wurde vom BSI entwickelt
- Anwender muss eine 6-stellige PIN eingeben → Chip auf nPA generiert Zufallszahl, die mit der PIN verschlüsselt wird → Lesegerät entschlüsselt diese wieder
- Dann wird ein Diffie-Hellman-Schlüsselaustausch durchgeführt → Angreifer hat keine Chance, weil er nicht weiß, ob er Zufallszahl tatsächlich entschlüsselt hat
- Größte Gefahr: Keylogger (v.a. bei Basislesegerät)
- Allerdings nützt PIN allein nicht viel, Angreifer brauchen entweder exakte Kopie oder nPA

Kritik, Gefahren

- Überwachung (Big Brother is watching you)
- Entsorgung → RFID-Tags auf Verpackungen verunreinigen Verpackungsmaterial beim Recycling → sind schwer abzutrennen
- „Verschwendung“ von Edelmetallen für Massenfertigung von RFID-Chips (z.B. für Lebensmittelpackungen)

Quellen:

- <http://de.wikipedia.org>
- <http://www.zdnet.de>
- <http://www.rfid-basis.de>
- <http://www.bm-tricon.com>
- <http://www.rfid-journal.de>