Kryptografie in UHF Tags

Aktueller DIN-Vorschlag zur Standardisierung einer Crypto-Suite

Klaus Finkenzeller, Katharina Schulz, Dr. Walter Hinz

16. Mai 2013

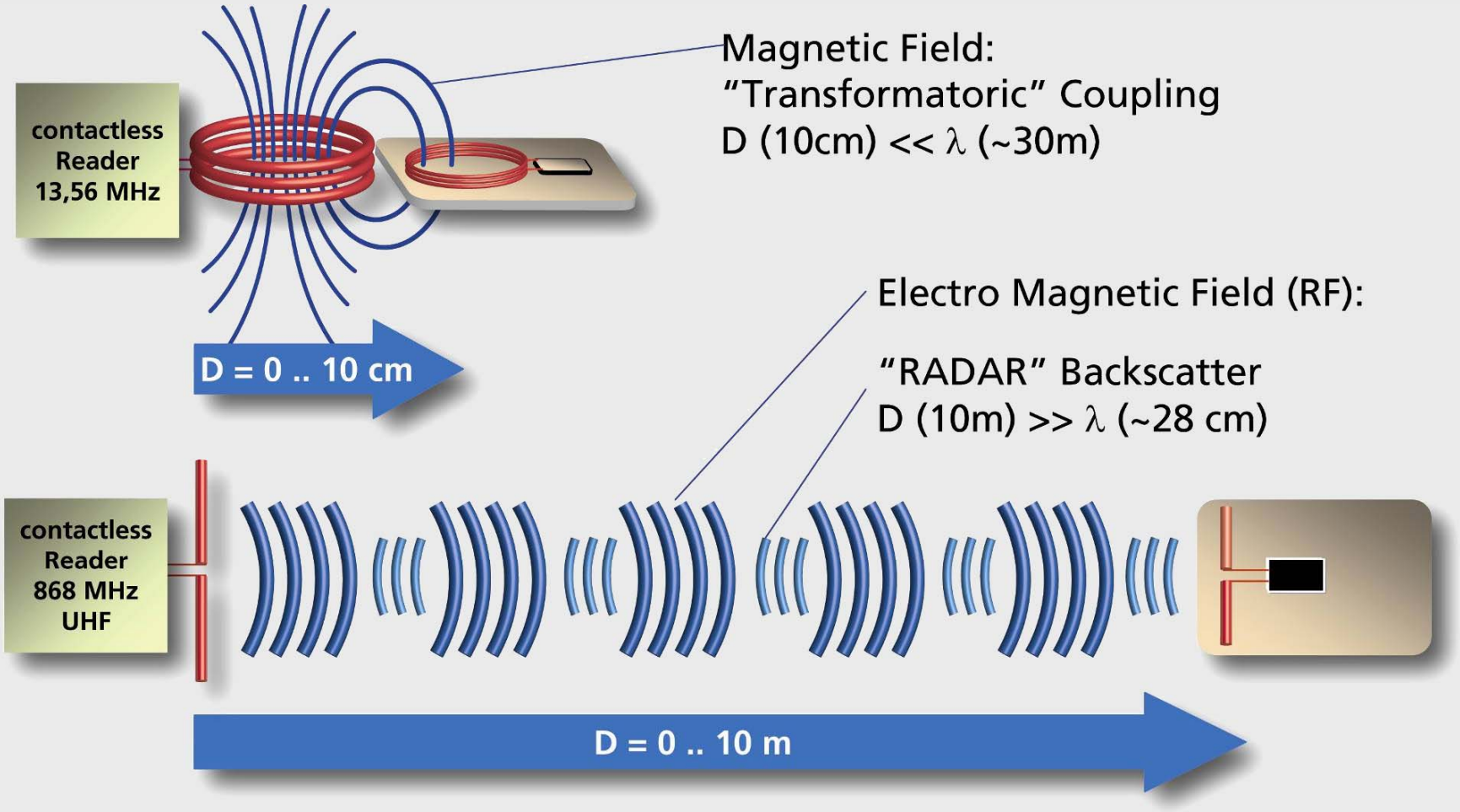
Giesecke & Devrient

Creating Confidence.

Agenda

- UHF RFID - Zum Stand der Technik
- Stand der Standardisierung
- Rabin-Montgomery Kryptosystem
- Prototypische Implementierung
- Zusammenfassung und Ausblick

Induktive und radiative RFID Systeme



Giesecke & Devrient

Secure UHF RFID

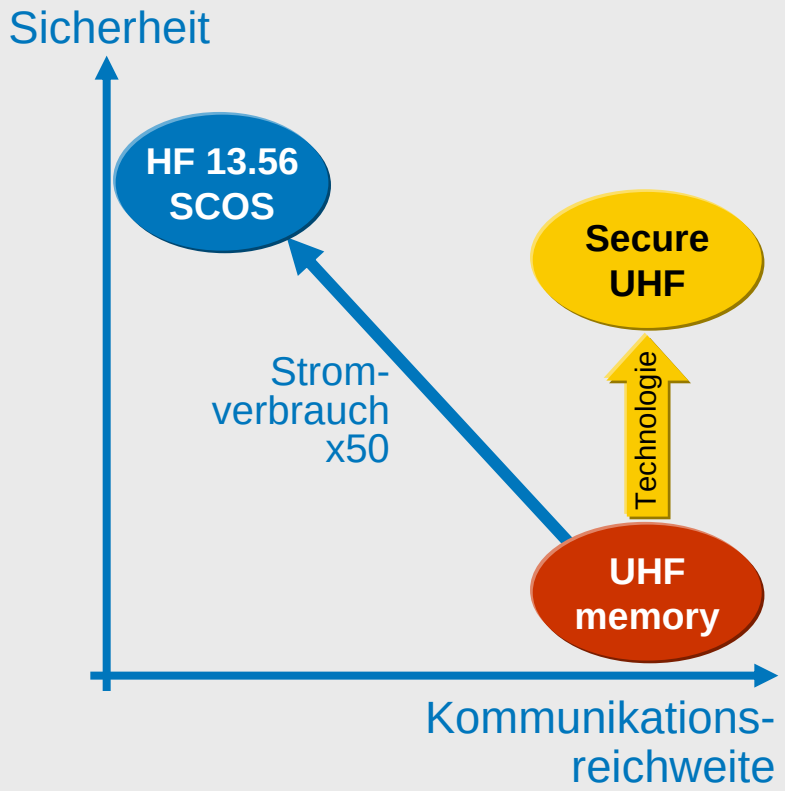
Kryptografische Absicherung für UHF RFID Systeme ermöglicht neue Anwendungen.

Stand heute:

- ISO/IEC 14443: RF 13,56 MHz: Smart Card OS, 10 cm
- ISO/IEC 18000-63: UHF 868 MHz: Unsicherer Speicher, 10 m

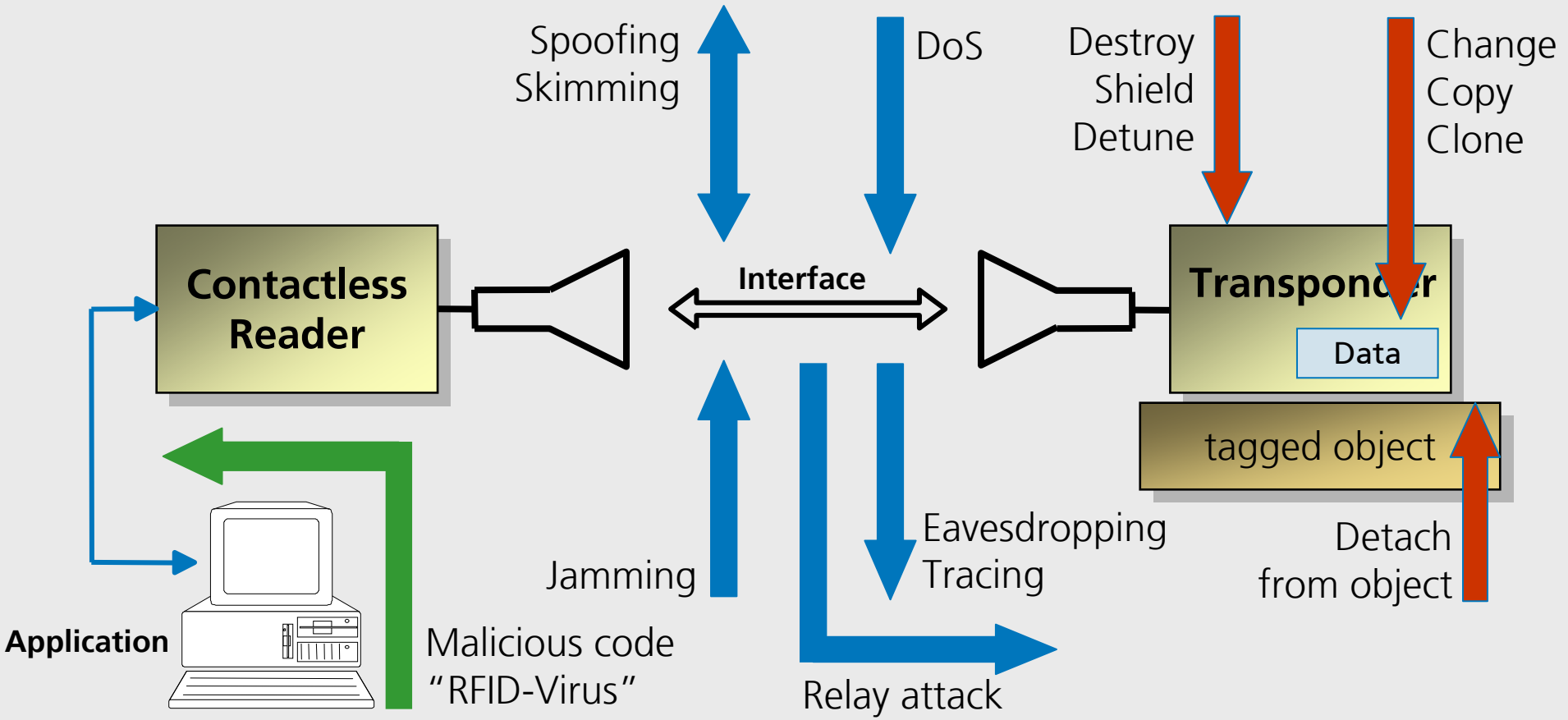
Secure UHF RFID:

- Kryptografische Absicherung bei gleicher Reichweite → Technologiesprung
- µC mit Secure OS → Flexibilität bei der Auswahl der Krypto-Protokolle



Giesecke & Devrient

Mögliche Angriffe auf RFID Systeme



Giesecke & Devrient

Agenda

- UHF RFID - Zum Stand der Technik
- Stand der Standardisierung
- Rabin-Montgomery Kryptosystem
- Prototypische Implementierung
- Zusammenfassung und Ausblick

ISO/IEC 29167 Crypto Suites – Bisherige Beiträge

Norm	Crypto Suite	Projekt-Editor	Status / Ballot *)
ISO/IEC 29167-10	AES128	NL	2nd CD
ISO/IEC 29167-11	PRESENT 80	BE	DIS
ISO/IEC 29167-12	ECC-DH	AT	CD
ISO/IEC 29167-13	GRAIN 128	US	WD
ISO/IEC 29167-14	AES128-OFB	KR	CD
ISO/IEC 29167-15	XOR	CN	WD
ISO/IEC 29167-16	ECDSA-ECDH	CN	2nd CD
ISO/IEC 29167-17	GPS	FR	2nd CD
ISO/IEC 29167-18	Humming Bird 2	US	NP: WD
ISO/IEC 29167-19	RAMON	DE	NP: WD

*) Stand: 22. April 2013

Agenda

- UHF RFID - Stand der Technik
- Stand der Standardisierung
- Rabin-Montgomery Kryptosystem
- Prototypische Implementierung
- Zusammenfassung und Ausblick

Die RAMON Crypto Suite

RAMON basiert auf dem **Rabin**-Kryptosystem, kombiniert mit dem **Montgomery**-Verfahren, und verwendet folgende Schlüssel:


Öffentlicher Verschlüsselungsschlüssel K_E
→ auf dem Transponder gespeichert


Geheimer Entschlüsselungsschlüssel K_D
→ auf Leser-Seite gespeichert


Optionales ECDSA Signaturschlüsselpaar $\{K_S, K_V\}$

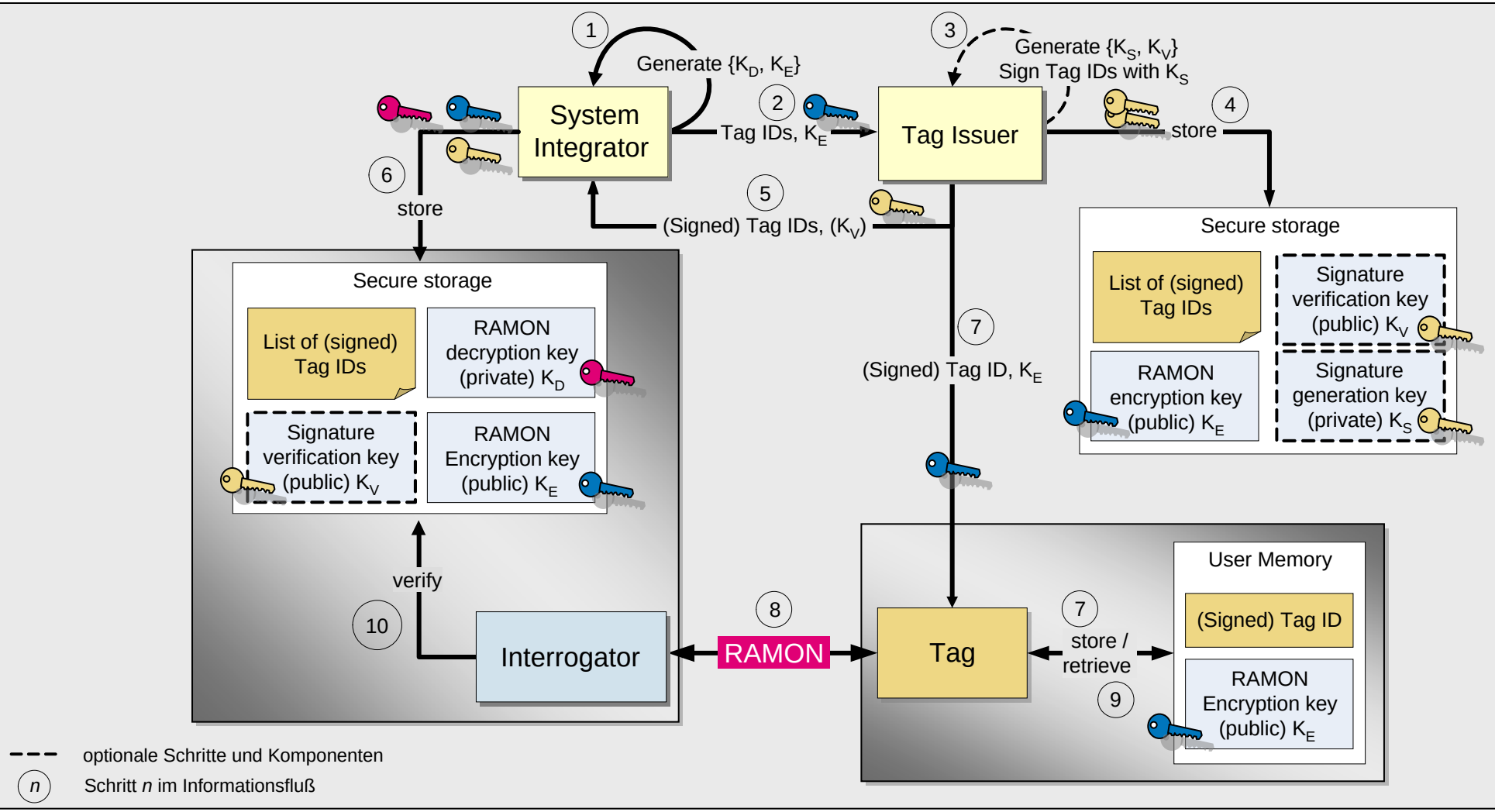

Statische Secure Channel Schlüssel K_{ENC}, K_{MAC}


Secure Channel Sitzungsschlüssel S_{ENC}, S_{MAC}

Die Crypto Suite ermöglicht:

- Sichere Tag-Identifikation durch das Rabin-Montgomery Verfahren
- Randomisierung der Tag-UII (EPC) verhindert weiteres Tracing/Tracking
- AES-basierte gegenseitige Authentisierung und Generierung von Sitzungsschlüsseln für sichere Kommunikation

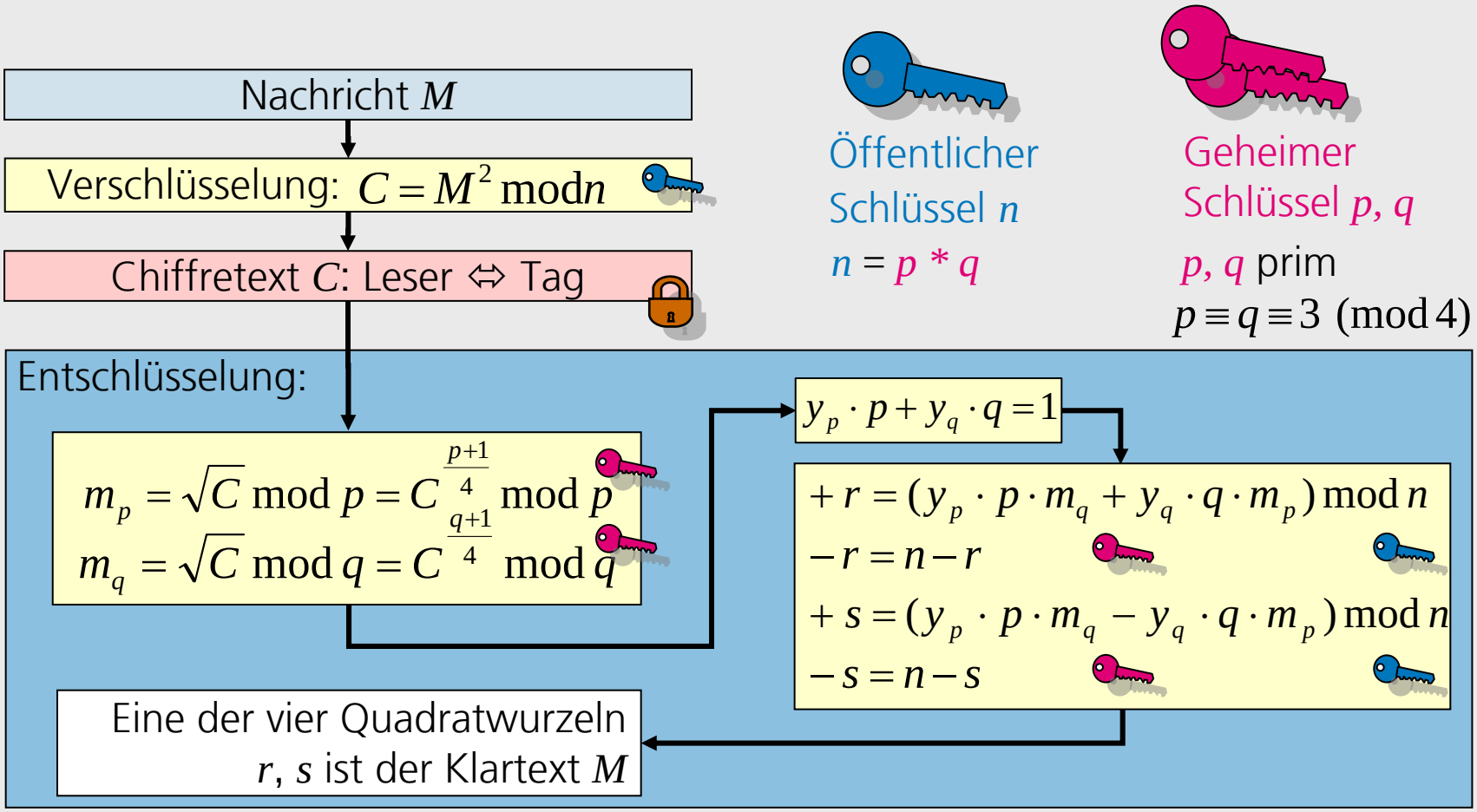
Rollen, Komponenten und Informationsflüsse



Giesecke & Devrient

Das Rabin-Kryptosystem

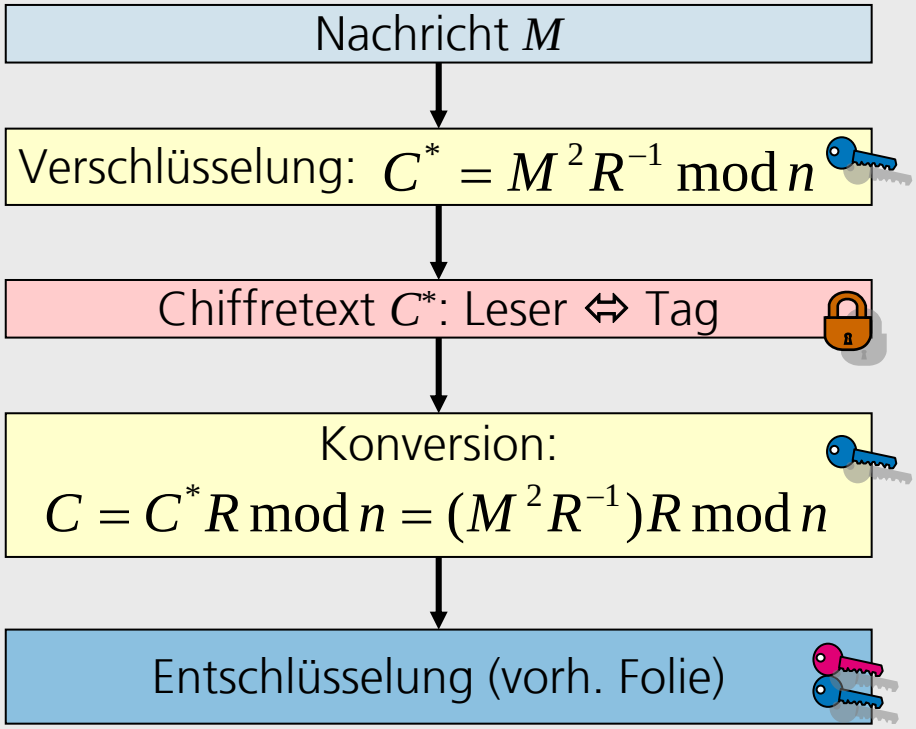
Die Sicherheit des Rabin-Verfahrens beruht auf dem Faktorisierungsproblem.

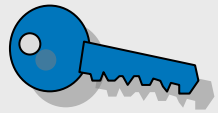


Giesecke & Devrient

Modulare Montgomery-Multiplikation

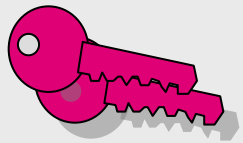
Der Montgomery-Ansatz erlaubt effiziente Durchführung der Verschlüsselung auf dem Transponder.





Öffentlicher Schlüssel n

$n = p * q$



Geheimer Schlüssel p, q

p, q prim

$p \equiv q \equiv 3 \pmod 4$

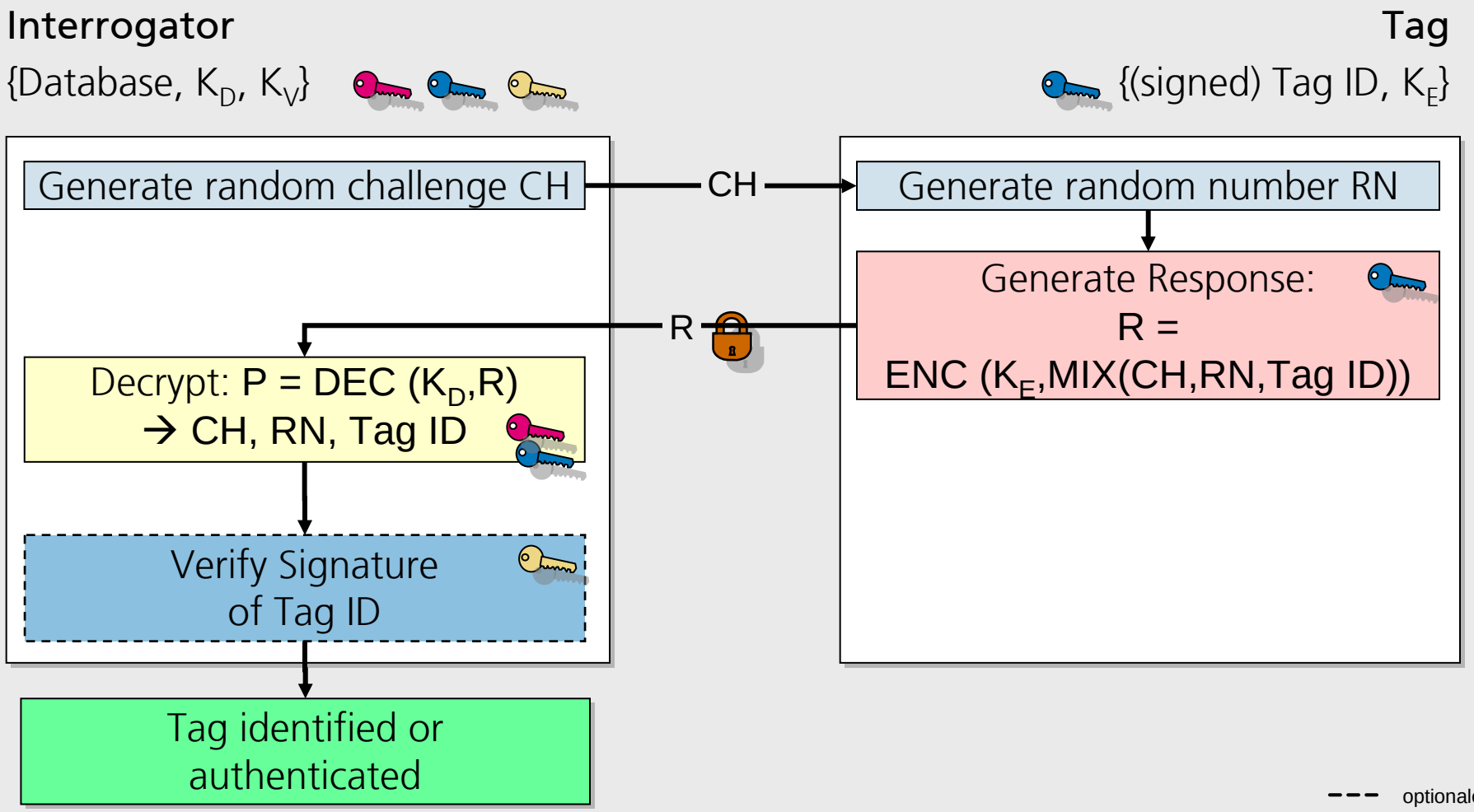
Für Residuum R gilt $R \geq 2^k > n$

R ist eine Zweierpotenz, größer als und teilerfremd zu n.

$n = 1 \bmod 2^{bl \cdot nd}; 1 \leq nd < d; nd \approx d/2$

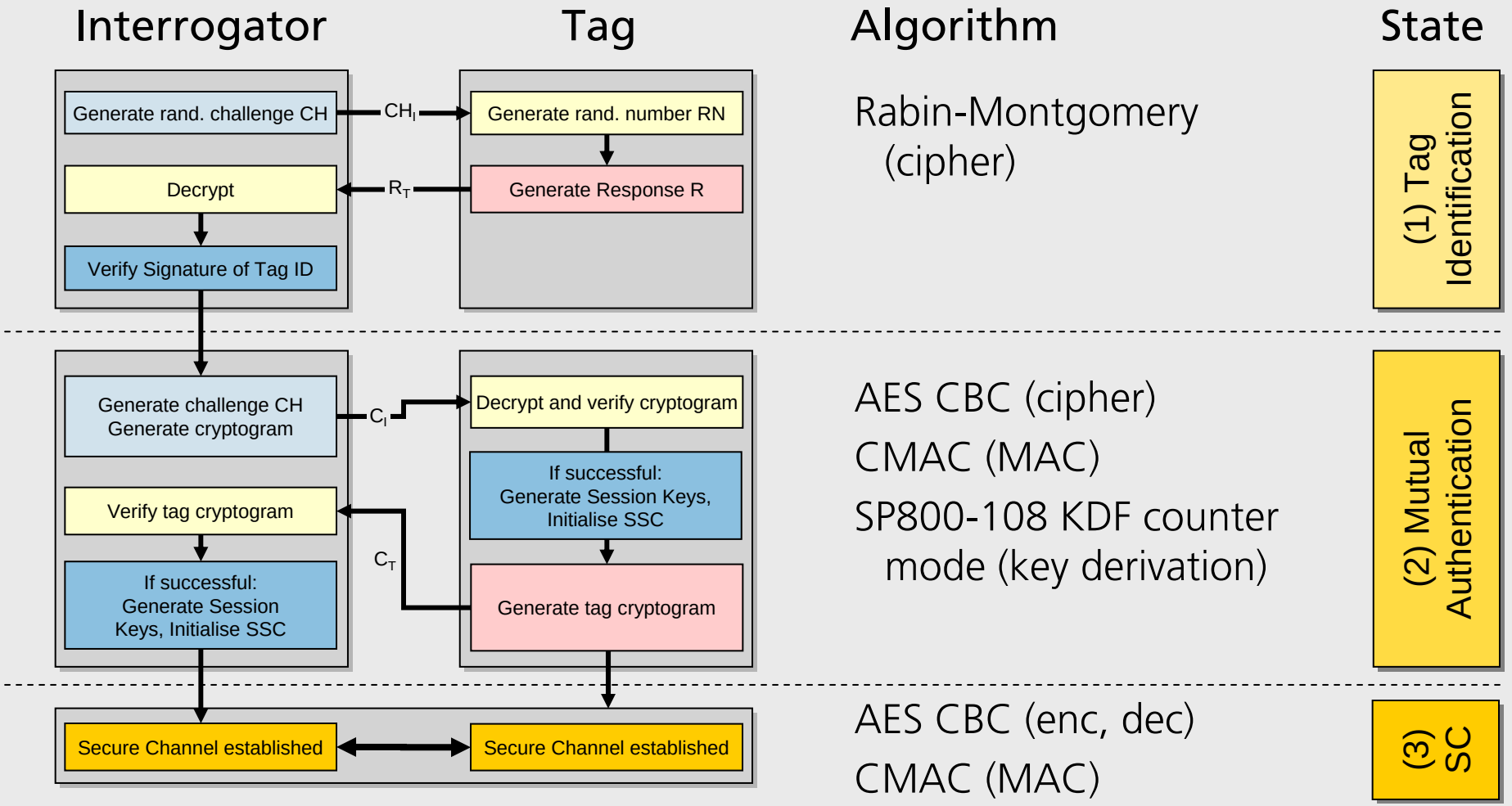
Giesecke & Devrient

RAMON Protokollschritte – Tag-Identifikation



Giesecke & Devrient

Protokollerweiterung um gegenseitige Authentisierung



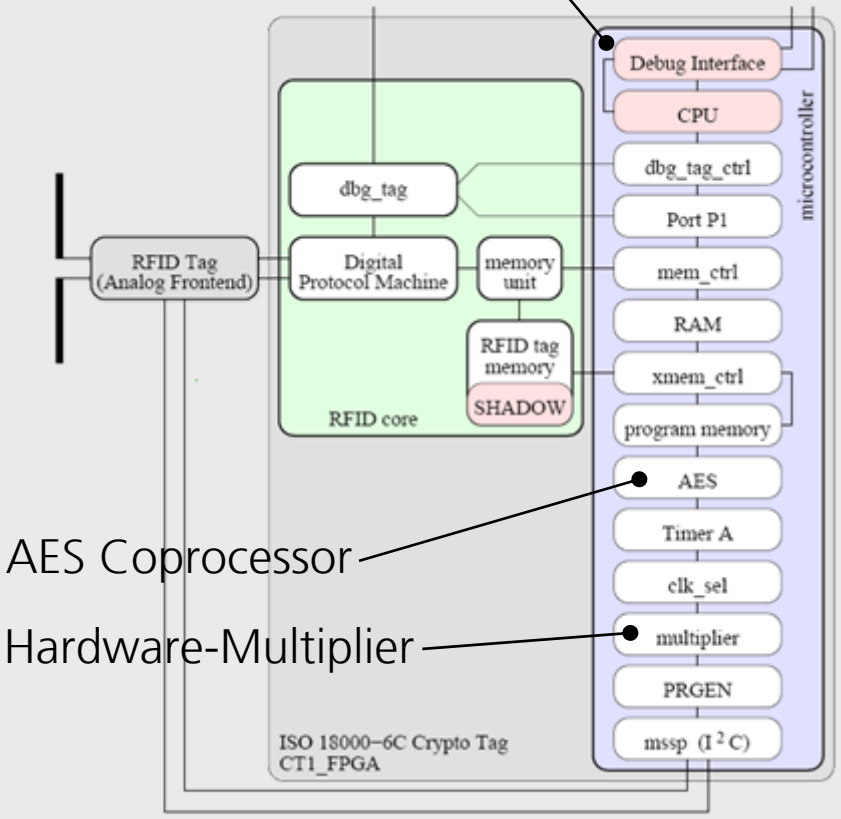
Giesecke & Devrient

Agenda

- UHF RFID - Stand der Technik
- Stand der Standardisierung
- Rabin-Montgomery Kryptosystem
- Prototypische Implementierung
- Zusammenfassung und Ausblick

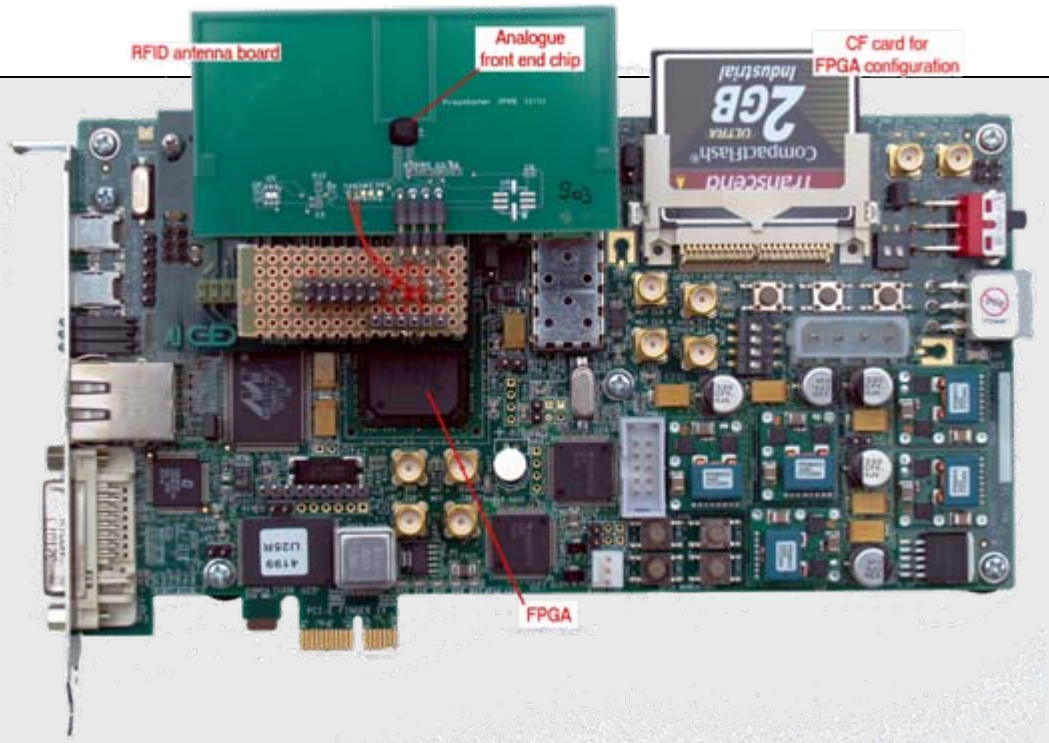
Secure-UHF Demonstrator

Soft-core Microcontroller,
MSP430X-kompatibel



AES Coprocessor

Hardware-Multiplier



- Handelsüblicher RFID-Leser und Tag mit Analog Front End
- FPGA Evaluation Board mit externer Energieversorgung
- Nachimplementierter ISO 18000-63 Zustandsautomat und Tagspeicher

Giesecke & Devrient

Zusammenfassung und Ausblick

- RAMON kombiniert Vorteile des Rabin-Verfahrens mit der Montgomery-Multiplikation
- Datenübertragung und Verschlüsselung werden parallel ausgeführt
- Sichere Tag-Identifikation, Schutz vor Tracking/Tracing
- Handelsübliche RFID-Leser können verwendet werden
- Kombiniert mit einem Verfahren für symmetrische gegenseitige Authentisierung
- Nächste Schritte:
  - Ende 2014 Veröffentlichung des Standards
  - Entwicklung eines RAMON UHF Chips in Zusammenarbeit mit Hardware-Herstellern

Vielen Dank für Ihre Aufmerksamkeit!

Katharina Schulz
Giesecke & Devrient
Mobile Security Secure Devices

Tel: +49 89 4119-1397
Fax: +49 89 4119-2819
E-Mail: Katharina.Schulz@gi-de.com

Giesecke & Devrient

Historie der Standardisierung

- Basisstandard
  - 2000 – 2001 ISO/IEC 18000-6 Type A und Type B
  - 2001 – 2002 EPCglobal Class 1 und Class 0
  - 2003 – 2005 ECPglobal Class 1 Gen 2
  - 2006 – 2007 ISO/IEC 18000-6 Type C ← EPCglobal C1G2 V1.0.9
  - 2007 – 2008 EPCglobal C1G2 V1.2.0 || ISO/IEC 18000-6 Type C:2010
- Sicherheits-Standard
  - 2008 NWIP für Sicherheit in RFID
  - 2009 Gründung WG7 im SC31
  - 2010 EPCglobal nimmt Arbeit an Sicherheitsthemen auf
  - 2011 SC31 nimmt den EPCglobal AI Beitrag in ISO/IEC 18000-63REV1 auf
  - 2011 WG7 bittet um Beiträge zu Crypto Suites

Randomisierung der Tag-UII verhindert Tracing/Tracking

Der EPC geht zurück auf ECPglobal Class 1 Gen2 UHR RFID Standard.
ISO/IEC18000-63 verwendet die Bezeichnung UII (Unique Item Identifier)
Einfaches Auslesen des UII durch *Select*, *ACK* und *Read* Kommandos.

01.000000A89.00016F.0000169DC0

Header	EPC Manager	Object Class	Serial Number
8 bits	28 bits	24 bits	36 bits

Gewöhnlicher 96 Bit EPC

01.000472644.5D19AC23DFDC04CE

Header	EPC Manager	Random Number
8 bits	28 bits	60 bits

Randomisierter 96 Bit EPC