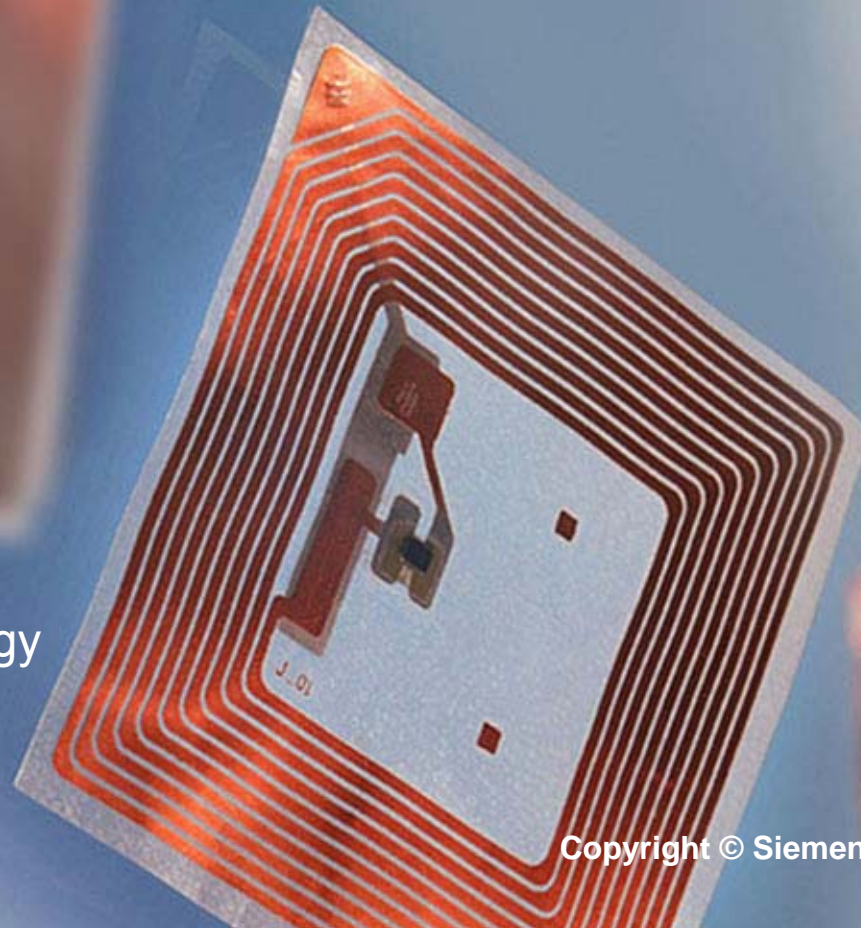


RFID-Technologie + Kryptographie

Dr. Erwin Heß
Siemens AG
Corporate Technology



Inhalt

- Motivation: Weshalb braucht man Kryptographie für RFID-Tags?
- Einschub: Kryptographie
- Sicherheits RFID-Tags: mit symmetrischer Kryptographie
- Sicherheits RFID-Tags: mit asymmetrischer Kryptographie

Weshalb braucht man Kryptographie für RFID-Tags?

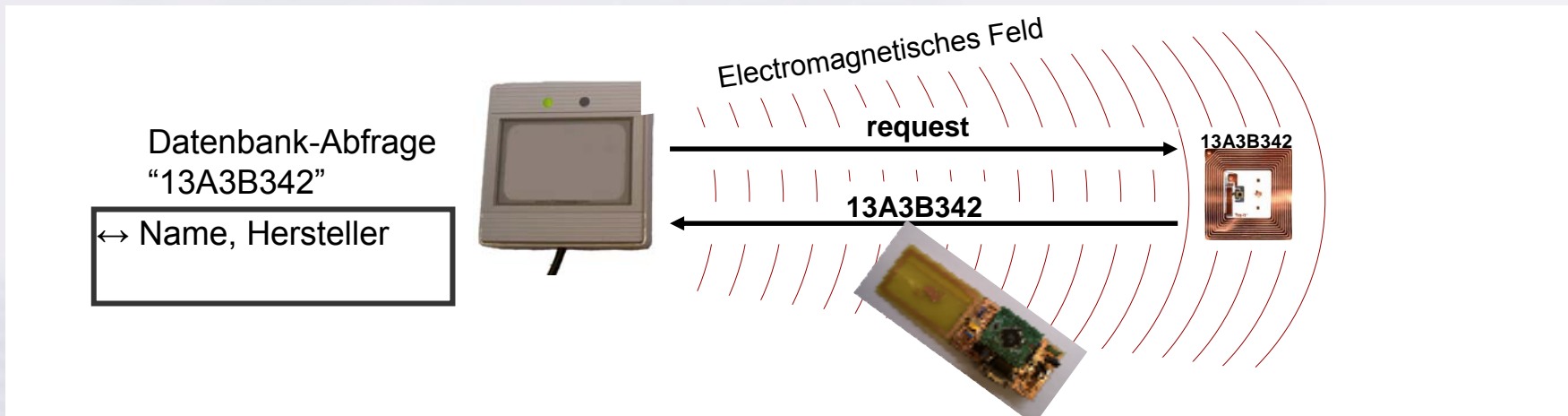
Die Fakten ...

- Alle relevanten Informationen über die Funktionsweise von RFID-Tags sind öffentlich bekannt (Kommunikationsprotokolle, Chip-Layouts verfügbar im Internet, RFID-Handbuch, etc.).
- Entwicklungs-Tools sind öffentlich zugänglich.
- Gerät zum Aufzeichnen/Einspielen der Kommunikation zwischen RFID-Tag und Lesegerät kann sehr leicht gebaut werden:
 - 8-Bit-Atmel-Prozessor
 - ISO 14443 A/B, ISO 15963 (13,56 MHz)
 - Serien-Nr. und Nutzerdaten sind frei programmierbar



Weshalb braucht man Kryptographie für RFID-Tags?

RFID-Tags übertragen ihre Daten üblicherweise im Klartext.



In dieser Situation können die Tag-Daten abgefangen und auf andere RFID-Tags kopiert werden. Der ursprüngliche RFID-Tag ist somit "geklont".



Weshalb braucht man Kryptographie für RFID-Tags?

Fazit

- RFID-Tags können leicht geklont werden, falls sie nicht durch kryptographische Maßnahmen gesichert sind.
- Das Klonen eines RFID-Tags ist kaum schwieriger als das Kopieren eines Barcodes, falls der RFID-Tag seine Daten im Klartext überträgt.
- Erforderlich sind kryptographische Authentikationsverfahren:

Challenge & Response-Protokoll



Inhalt

- Motivation: Weshalb braucht man Kryptographie für RFID-Tags?
- **Einschub: Kryptographie**
- Sicherheits-RFID-Tags: mit symmetrischer Kryptographie
- Sicherheits-RFID-Tags: mit asymmetrischer Kryptographie

Kryptographie - Was kann sie leisten ?

Vertraulichkeit

- Nachrichten werden für nicht autorisierte Personen unverständlich.

Vertrauen

- in die **Integrität** von Nachrichten
 - Ist die empfangene Nachricht wirklich unverändert?
- in die **Authentizität** von Kommunikationspartnern und Nachrichten
 - Kommt die Nachricht wirklich vom angegebenen Absender?
 - Ist der Kommunikationspartner wirklich der, der er vorgibt zu sein?
- in die **Verbindlichkeit** („Non-repudiation“)
 - Absender einer Nachricht kann seine Urheberschaft nicht abstreiten.

Kryptographie - Wie arbeitet sie ?

Die Nachricht m wird einer geeigneten mathematischen Datentransformation $m \rightarrow f(m)$ unterzogen

- Die verwendete Transformation f wird festgelegt durch
 - Kryptoalgorithmus **ALG**
 - Geheiminformation K (= Schlüssel, secret key)

$$f(m) = \mathbf{ALG}_K(m)$$

Maximen der Kryptographie:

- Die Sicherheit der verwendeten Verfahren darf nicht davon abhängen, dass der verwendete Algorithmus **ALG** geheim ist.
- Die Sicherheit darf ausschließlich auf der Geheimhaltung des verwendeten Schlüssels K beruhen.
- Mit geheimen Schlüsseln muss mit **äußerster Vorsicht** umgegangen werden.

Kryptographie - Grundtypen von Algorithmen

Symmetrisch: Kommunikationspartner haben **gemeinsamen Schlüssel K**

- ++ Viele und schnelle Verfahren verfügbar
- Problem der Schlüsselvereinbarung
- Verbindlichkeit nicht voll befriedigend zu gewährleisten

Asymmetrisch: Jeder Kommunikationsteilnehmer hat ein Schlüsselpaar

öffentlicher Schlüssel e

(„public key“)

privater (geheimer) Schlüssel d

(„private key“)

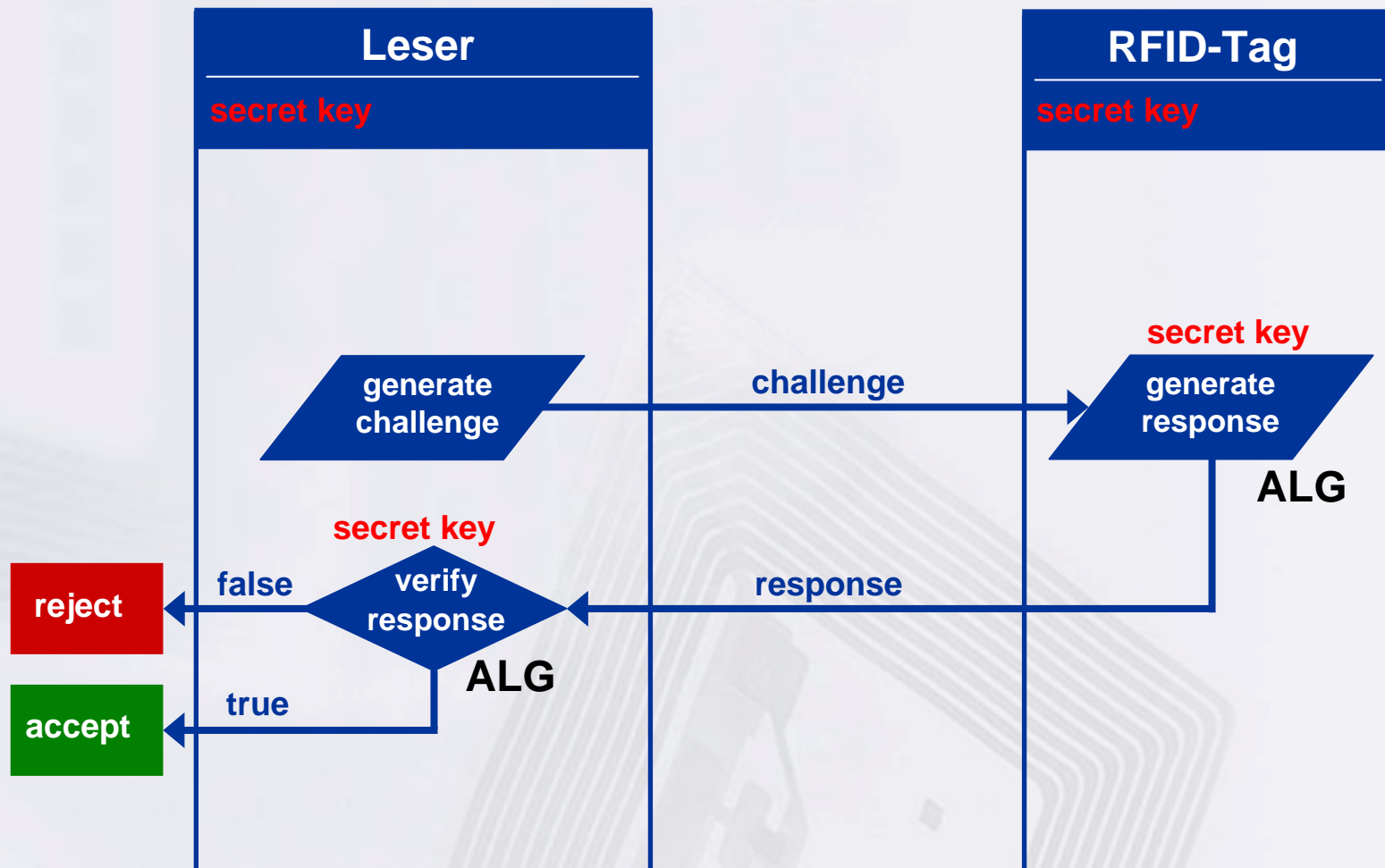
Es muss rechentechnisch unmöglich sein, aus e auf d zu schließen

- ++ Lösung des Problems der Schlüsselvereinbarung
- ++ digitale Signatur (löst das Problems der Verbindlichkeit)
- wenige Verfahren bekannt, aufwändig, langsam

Inhalt

- Motivation: Weshalb braucht man Kryptographie für RFID-Tags?
- Einschub: Kryptographie
- **Sicherheits-RFID-Tags: mit symmetrischer Kryptographie**
- Sicherheits-RFID-Tags: mit asymmetrischer Kryptographie

Verfahrensablauf einer **symmetrischen** kryptographischen Authentikation: Challenge & Response-Protokoll



Symmetrische kryptographische Authentikation

Vorteile:

- Symmetrische Kryptographie ist verfügbar auf Low-Cost-Chips, z. B.:
 - My-d von Infineon
 - MIFARE von NXP
- Hohe Performance ist erreichbar.



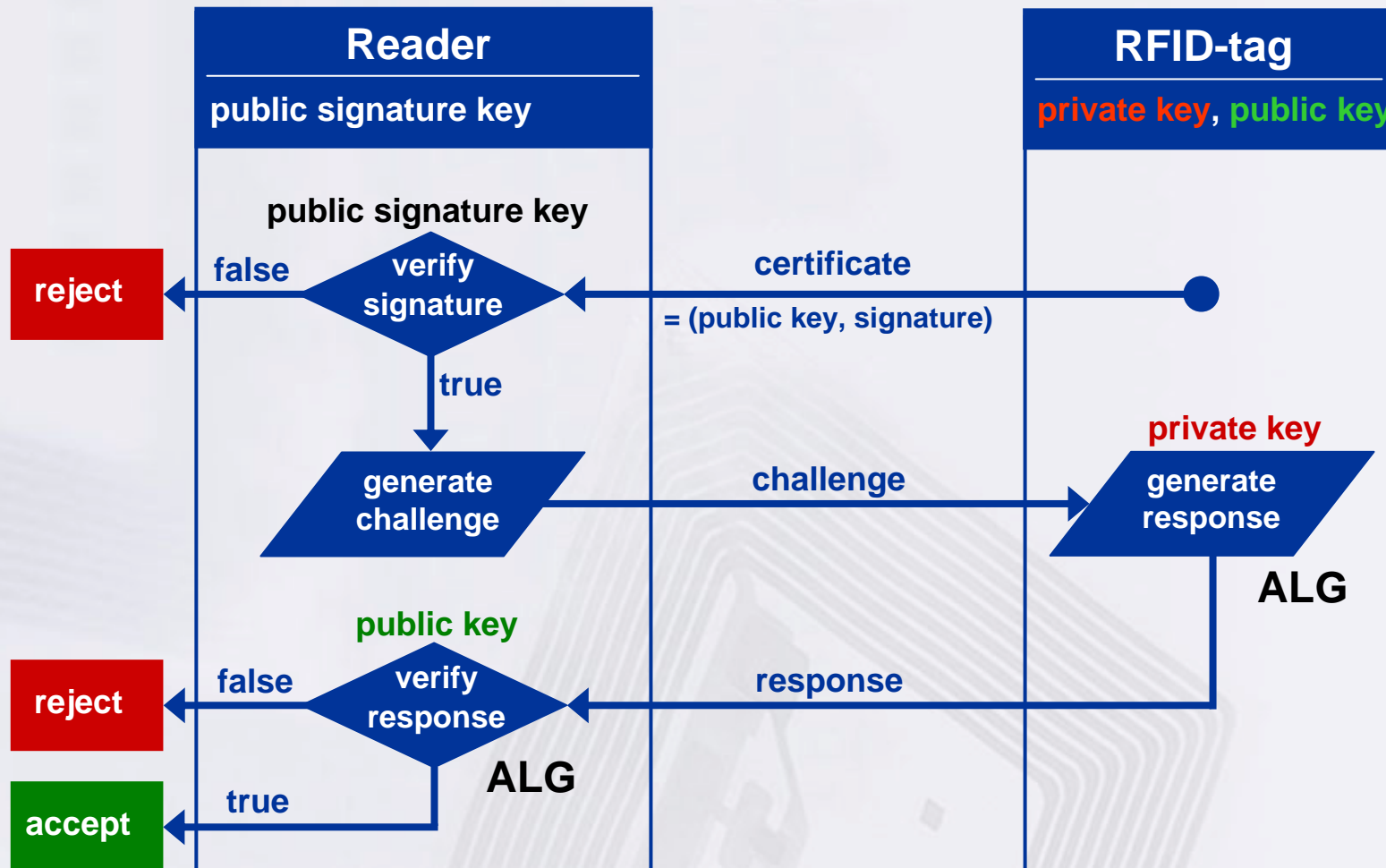
Nachteile:

- Grosses Angriffspotential auf Leserseite
- Alle Leser besitzen systemweiten Geheimschlüssel
- Alternativ: Sichere Verbindung zu Hintergrundsystem
- Leser müssen physikalisch gesichert werden

Inhalt

- Motivation: Weshalb braucht man Kryptographie für RFID-Tags?
- Einschub: Kryptographie
- Sicherheits RFID-Tags: mit symmetrischer Kryptographie
- **Sicherheits RFID-Tags: mit asymmetrischer Kryptographie**

Verfahrensablauf einer **asymmetrischen** kryptographischen Authentikation: Challenge & Response-Protokoll



Asymmetrische kryptographische Authentikation

Vorteile:

- Die Leser müssen keine geheimen Schlüssel enthalten.
- Die Leser müssen nicht physikalisch sicher sein.
- RFID-Authentizität kann offline überprüft werden.
- Sicherheit der Schlüssel gewährleistet durch Trustee-Center-Zertifikat.



Technologische Herausforderung

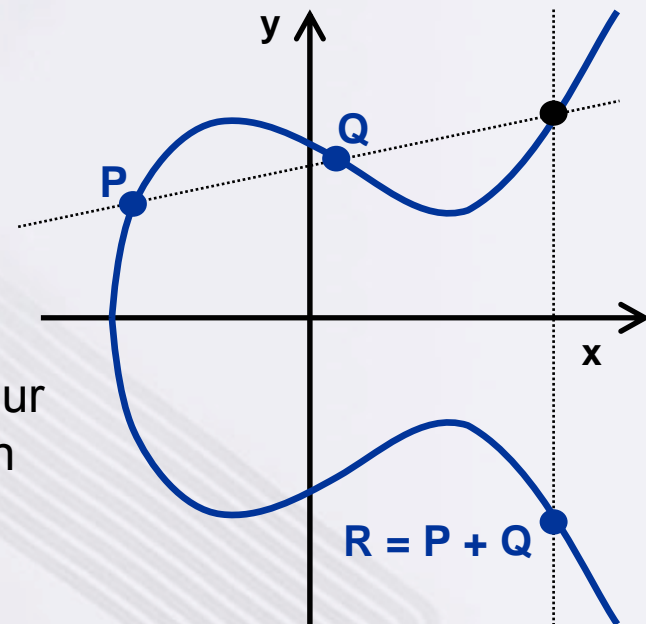
- Längere Parameter als bei der symmetrischen Kryptographie
- Große Chip-Fläche
- Performance schlechter als bei symmetrischen Systemen

Lassen sich diese Probleme unter RFID-Randbedingungen lösen ?

Siemens-Ansatz für asymmetrischen Krypto-RFID

Idee:

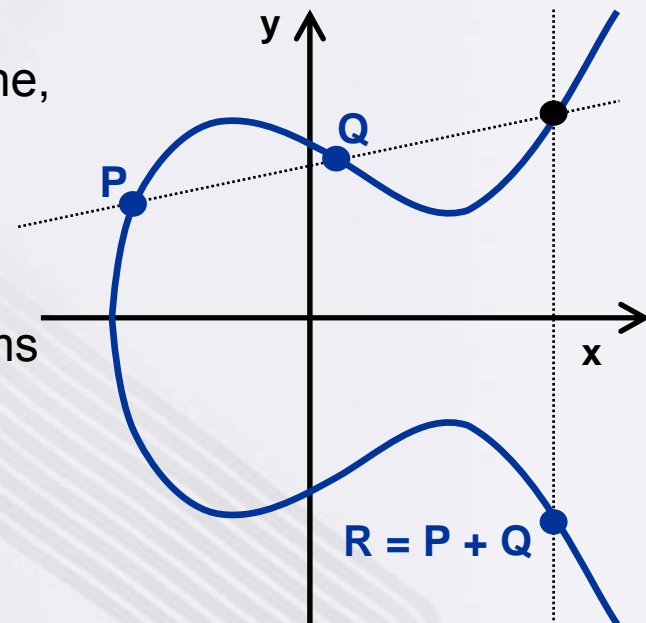
- Verzicht auf Funktionsprinzip „digitale Signatur“
- Asymmetrisches und interaktives Authentikations-verfahren, angelehnt an ElGamal-Verschlüsselung
- Elliptische Kurven über $GF(2^n)$
 - Kern des Rechenwerks besteht fast nur aus Schieberegister und XOR-Gattern
- Protokolloptimierung: Weitgehende Verlagerung der Rechenlast auf Terminalseite
- Verwendung spezieller „gehärteter“ elliptischer Kurven



Siemens-Ansatz für asymmetrischen Krypto-RFID

Ergebnis:

- Sehr einfache und kleine Arithmetik-Einheit
- Ablaufsteuerung über Finite-State-Maschine, kein Prozessor erforderlich
- Chip-Fläche $< 0.2\text{mm}^2$
- Rechenzeit für RFID-Authentikation $< 70\text{ ms}$



Asymmetrischer Krypto-RFID

Status:

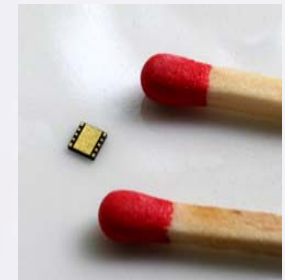
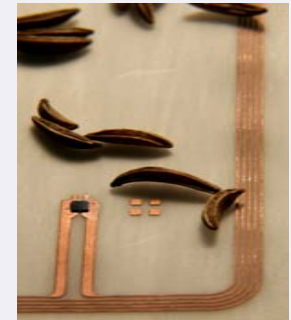
11/2006: Deutscher IT-Sicherheitspreis 2006 für RFID-Konzept

02/2009: Seriennahe Prototypen verfügbar (My-d-ECC)

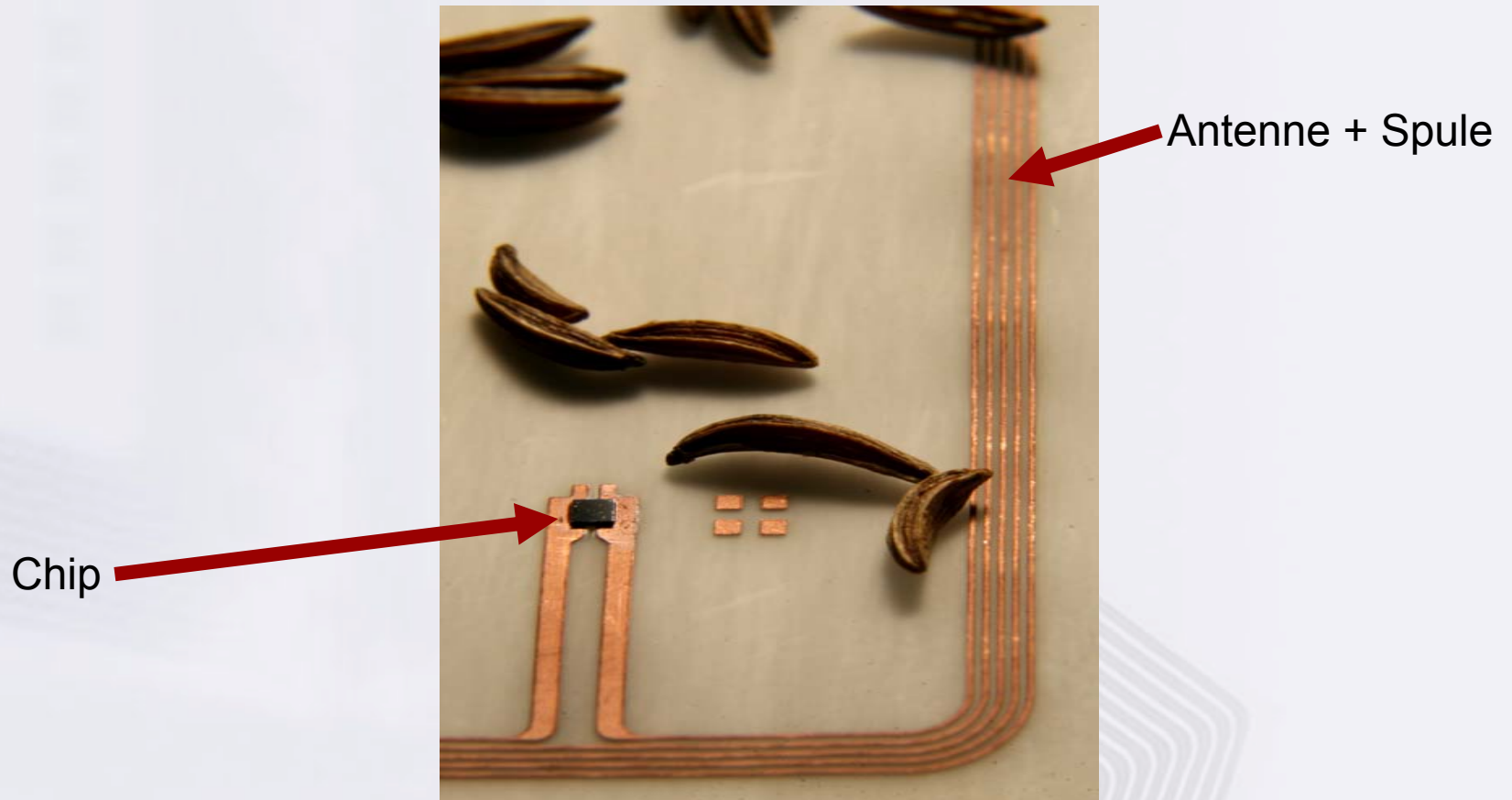
03/2009: Präsentation auf Cebit 2009

05/2009: Präsentation auf EuroID 2009: European EuroID Award 2009 für Siemens als “most innovative company”

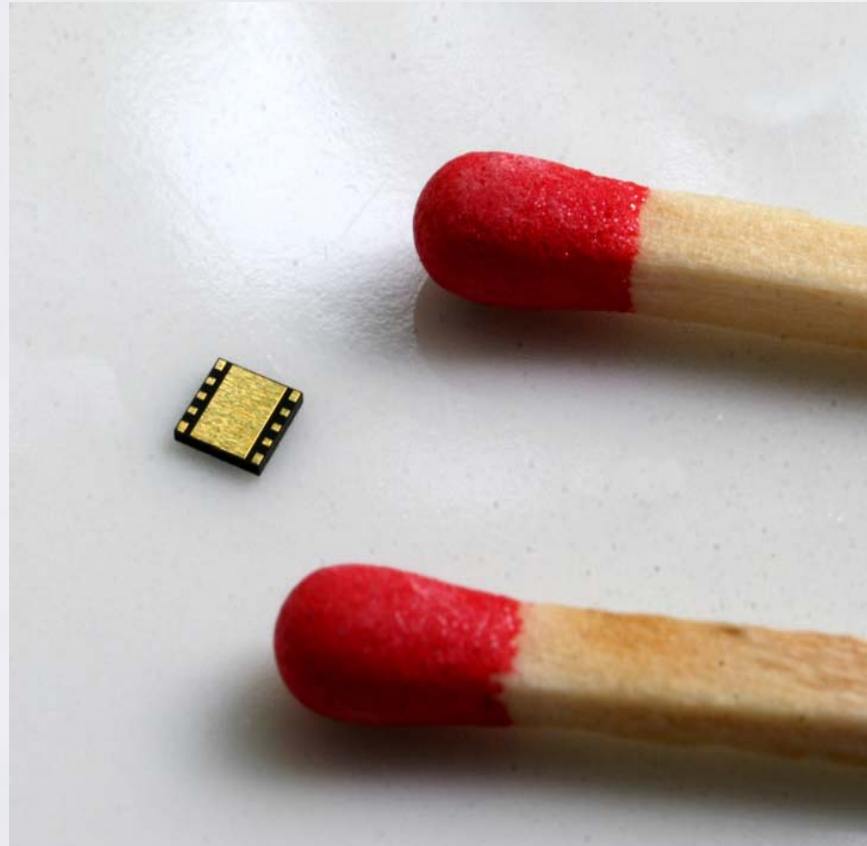
2008: Infineon-Produkt ORIGA. RFID-Derivat mit galvanischem Interface



Der asymmetrische Krypto-RFID My-d-ECC



Der asymmetrische Authentisierungs-IC ORIGA



Ansprechpartner

Dr. Erwin Heß

CT IC 3

Otto-Hahn-Ring 6

81730 München

Telefon: +49 89 636-41040

E-Mail: erwin.hess@siemens.com