Application of Passive Asymmetric RFID Tags in a High-Assurance Avionics Multi-Domain RFID Processing System

Dr. Rainer Falk, Florian Kohlmayer, **Andreas Köpf,** Dr. Michael Braun, Hermann Seuschek *

Dr. Mingyan Li °

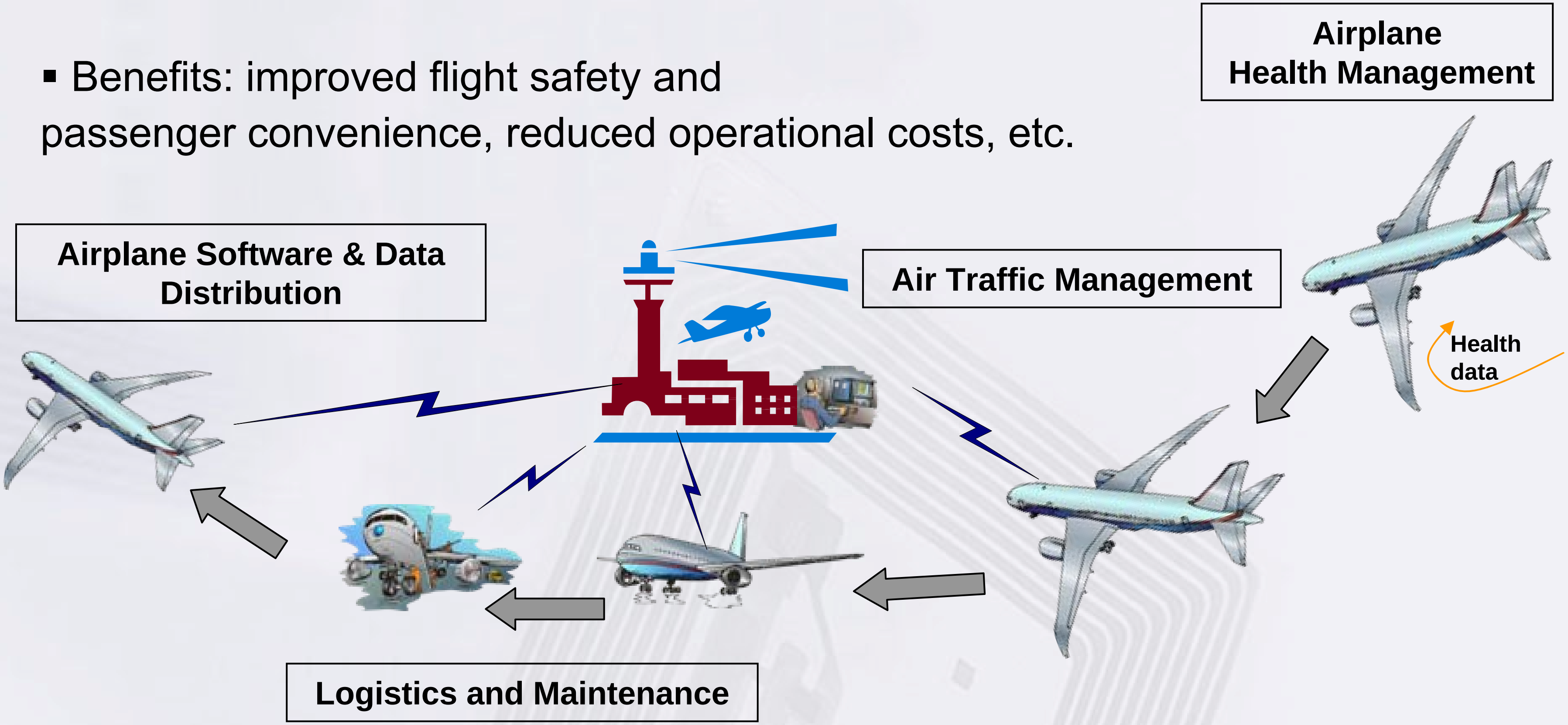
* Siemens AG – Corporate Technology, Germany
° Boeing Phantom Works, U.S.

SIEMENS

RFID Application Scenarios

- eEnabled airplanes have significant networking, processing, & storage capabilities

- Benefits: improved flight safety and passenger convenience, reduced operational costs, etc.



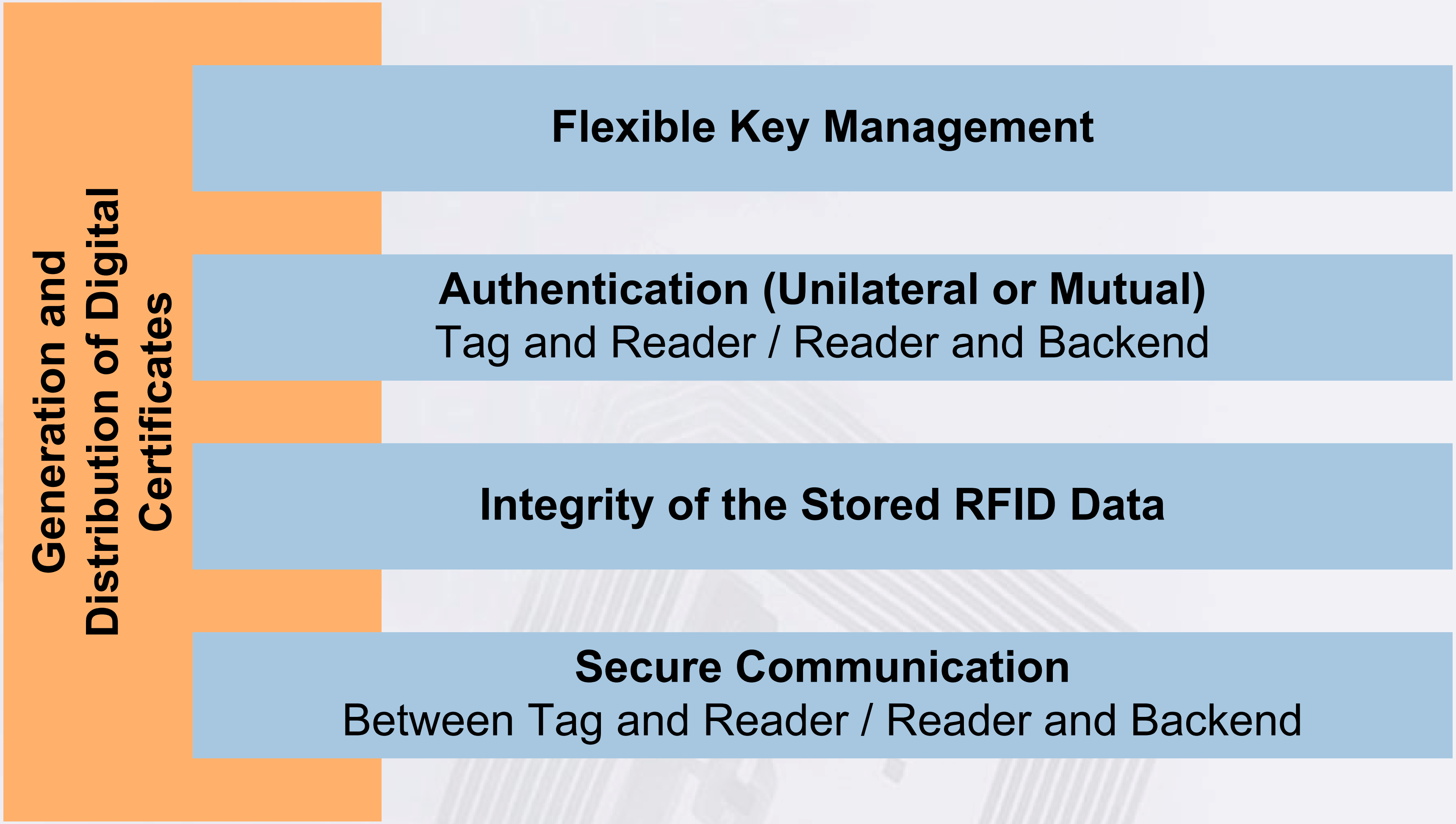
Airplane Health Management

Airplane Software & Data Distribution

Air Traffic Management

Logistics and Maintenance

Motivation for Supporting RFID Systems with PKI



Generation and Distribution of Digital Certificates

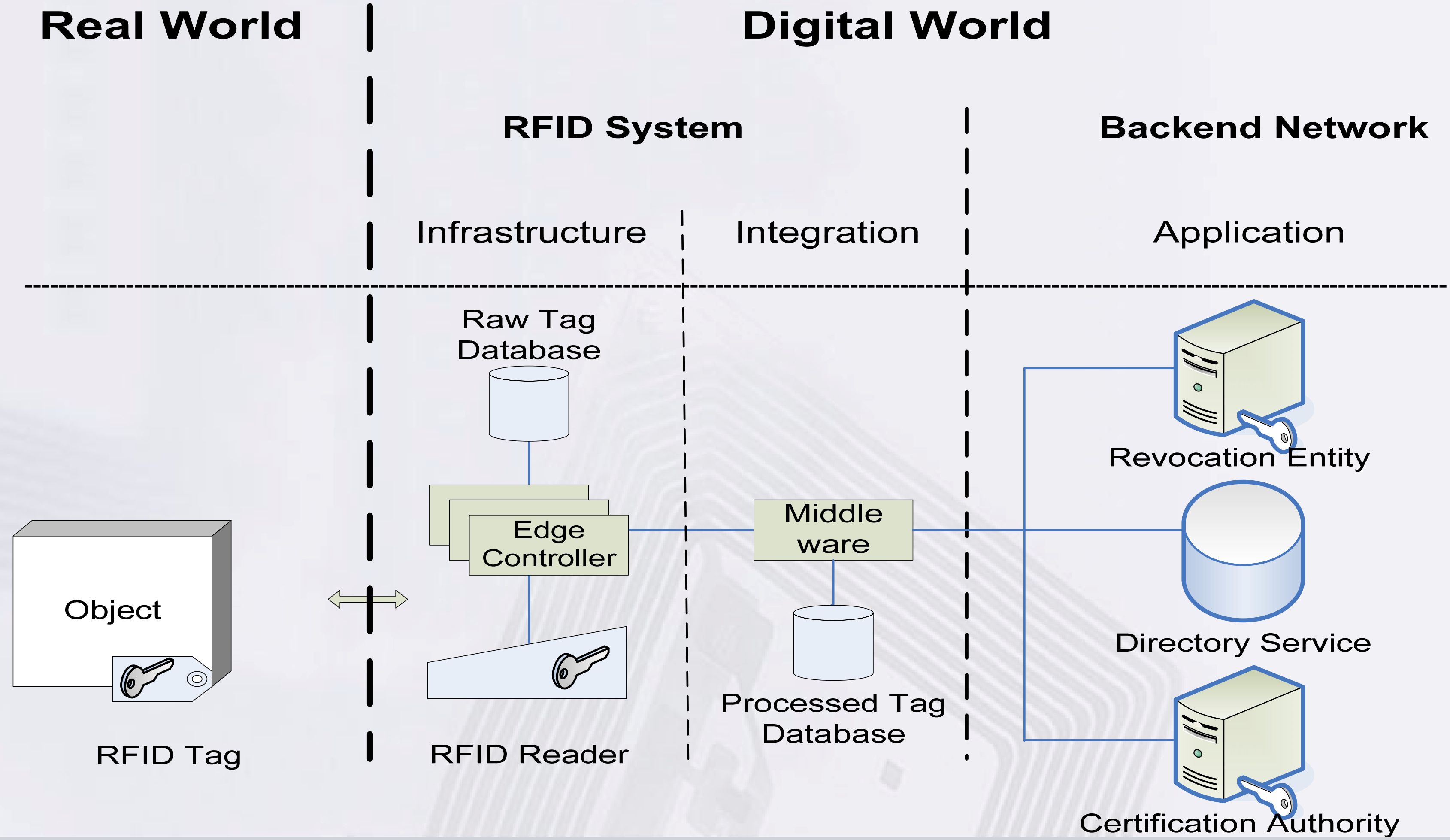
Flexible Key Management

Authentication (Unilateral or Mutual)
Tag and Reader / Reader and Backend

Integrity of the Stored RFID Data

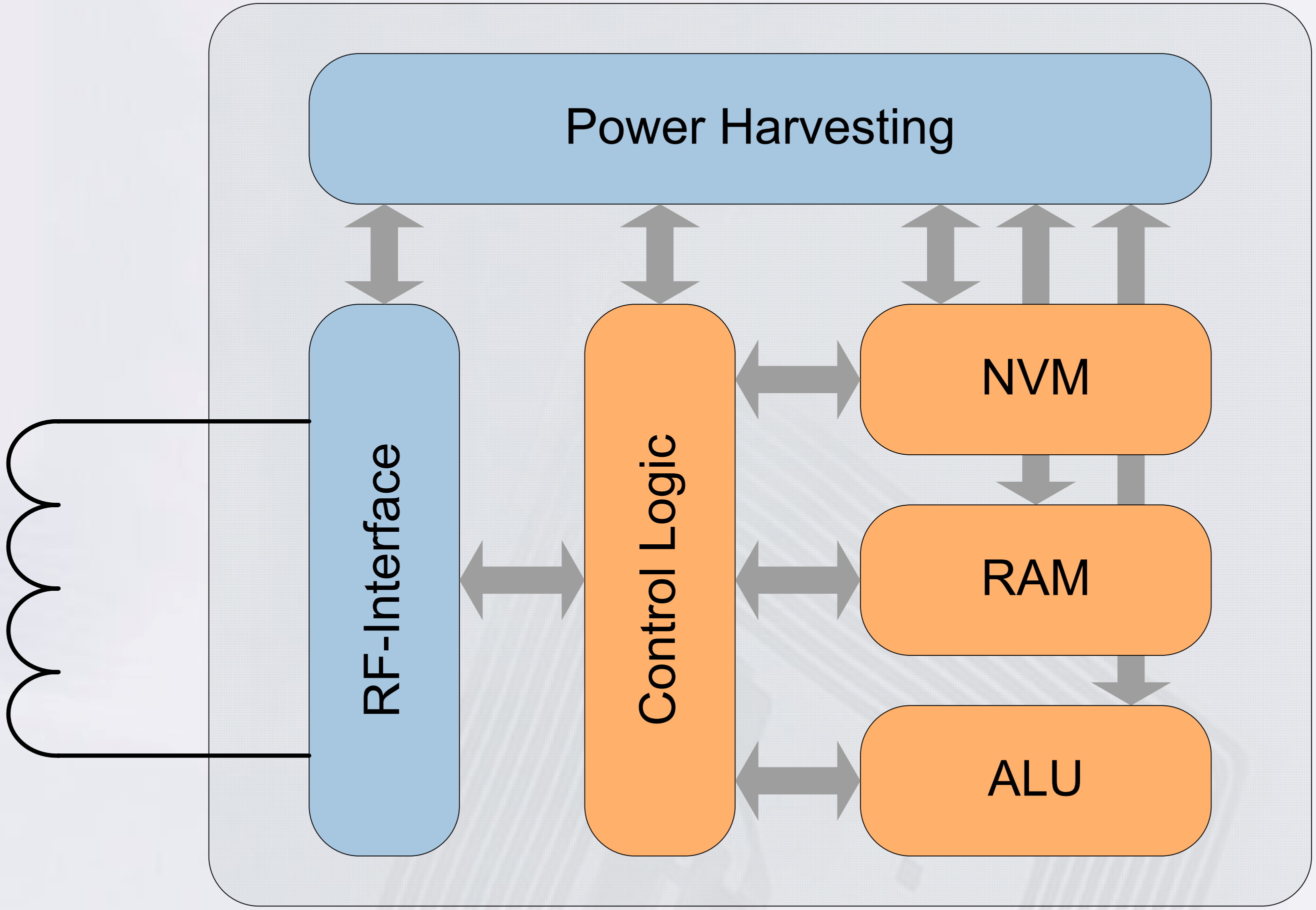
Secure Communication
Between Tag and Reader / Reader and Backend

Basic PKI Architecture for RFID

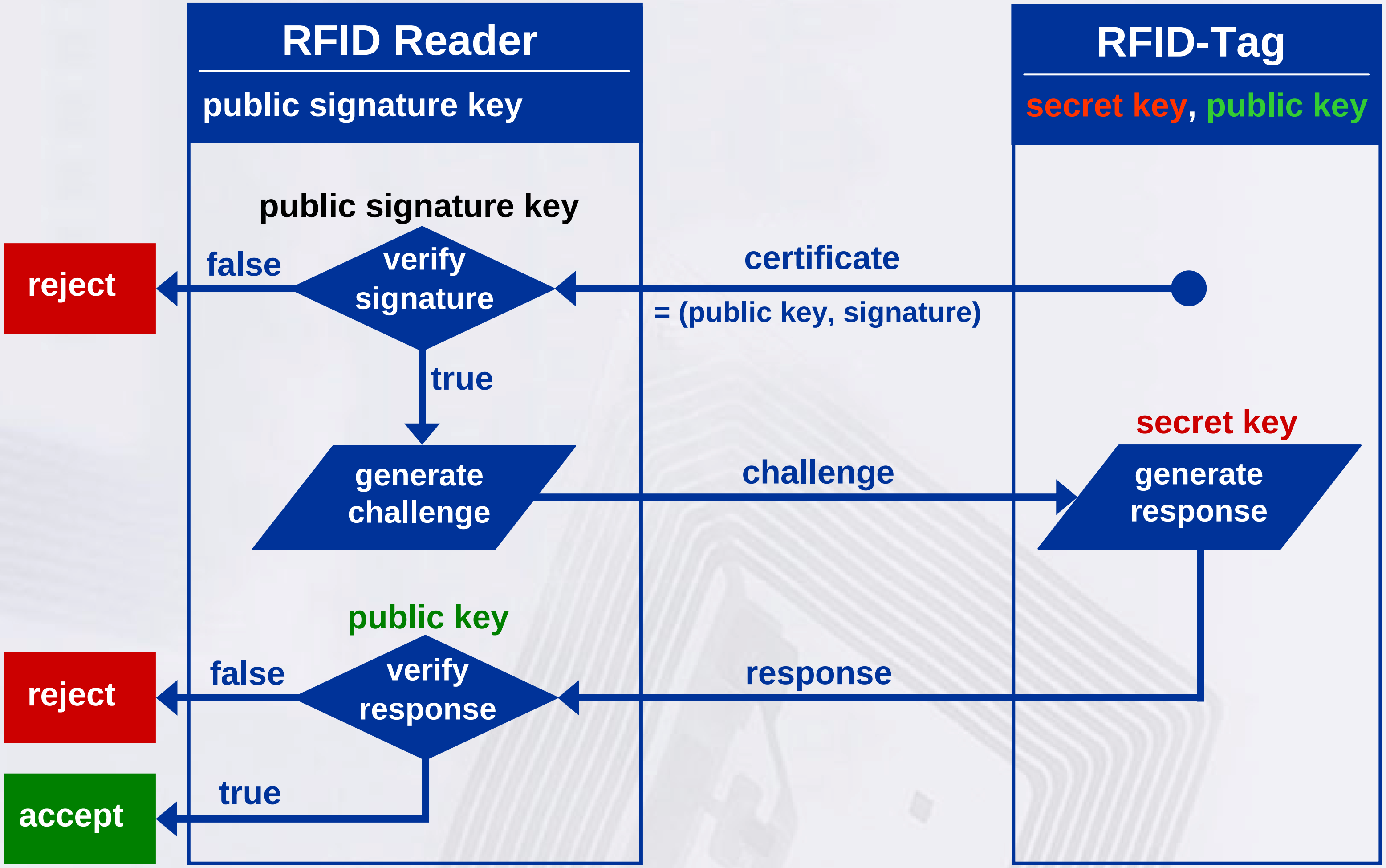


SIEMENS

RFID Tag Architecture



Asymmetric Authentication



Siemens’ novel RFID tag soon available

ISO 15693 / ISO 18000-3 Mode 1 Compliant (HF – 13.56 MHz)

- 64 Bit UID

Asymmetric Challenge Response Authentication

- Based on optimized Elliptic Curve Cryptography (163 bit ECC)
- Awarded in 2006 by German Federal Office for Information Security (BSI)

1152 Bit EEPROM

- 256 Bit user area
- 736 Bit storage for keys and certificate
- 160 Bit service area (UID, Lock Bits, Service Data)

Operating Distance

- Programmable calculation speed → variable operating distance / speed

150 ms Transaction Time in Low Power Mode

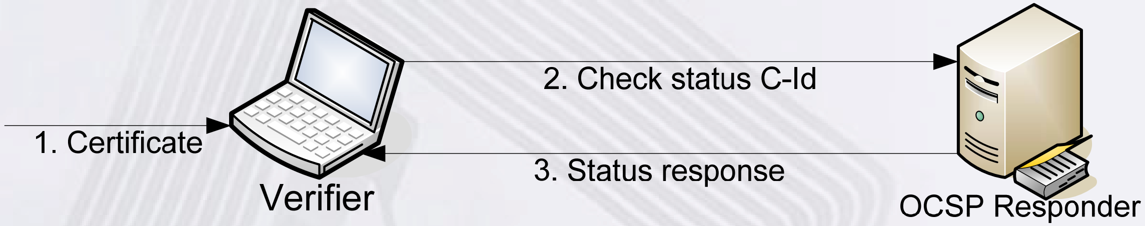
- Data transfer: 045ms @ 26kBit/s
- Calculation: 104ms @ 848kHz clock
  013ms @ 6.8MHz clock

Certificate Revocation Check

Certificate Revocation List (CRL)

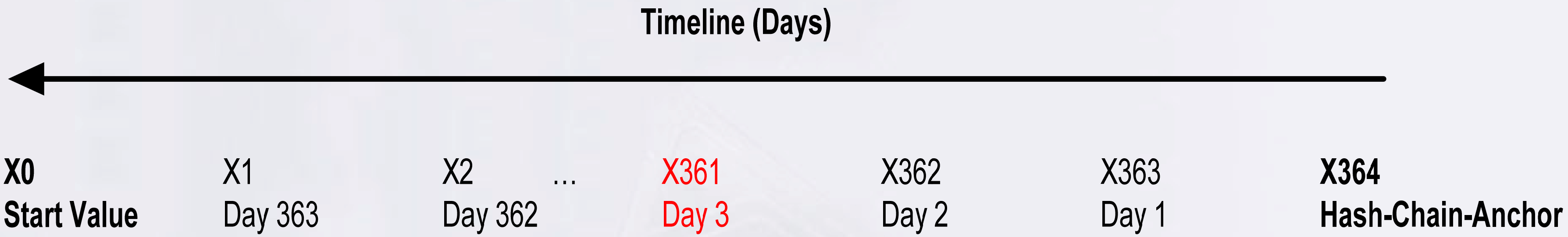
```
CRL
  issuer: Name
  thisUpdate: Time
  nextUpdate: Time
  revokedCertificates
          user Certificate: CertificateSerialNumber
          revocationDate: Time

          user Certificate: CertificateSerialNumber
          revocationDate: Time

          user Certificate: CertificateSerialNumber
          revocationDate: Time
                          ⋮
Signature
```

Online Certificate Status Protocol (OCSP)



Short-lived certificates

Certificate Status Validation Using Hash-Chains (1/2)



Timeline (Days)

X0
Start Value

X1
Day 363

X2
Day 362

...

X361
Day 3

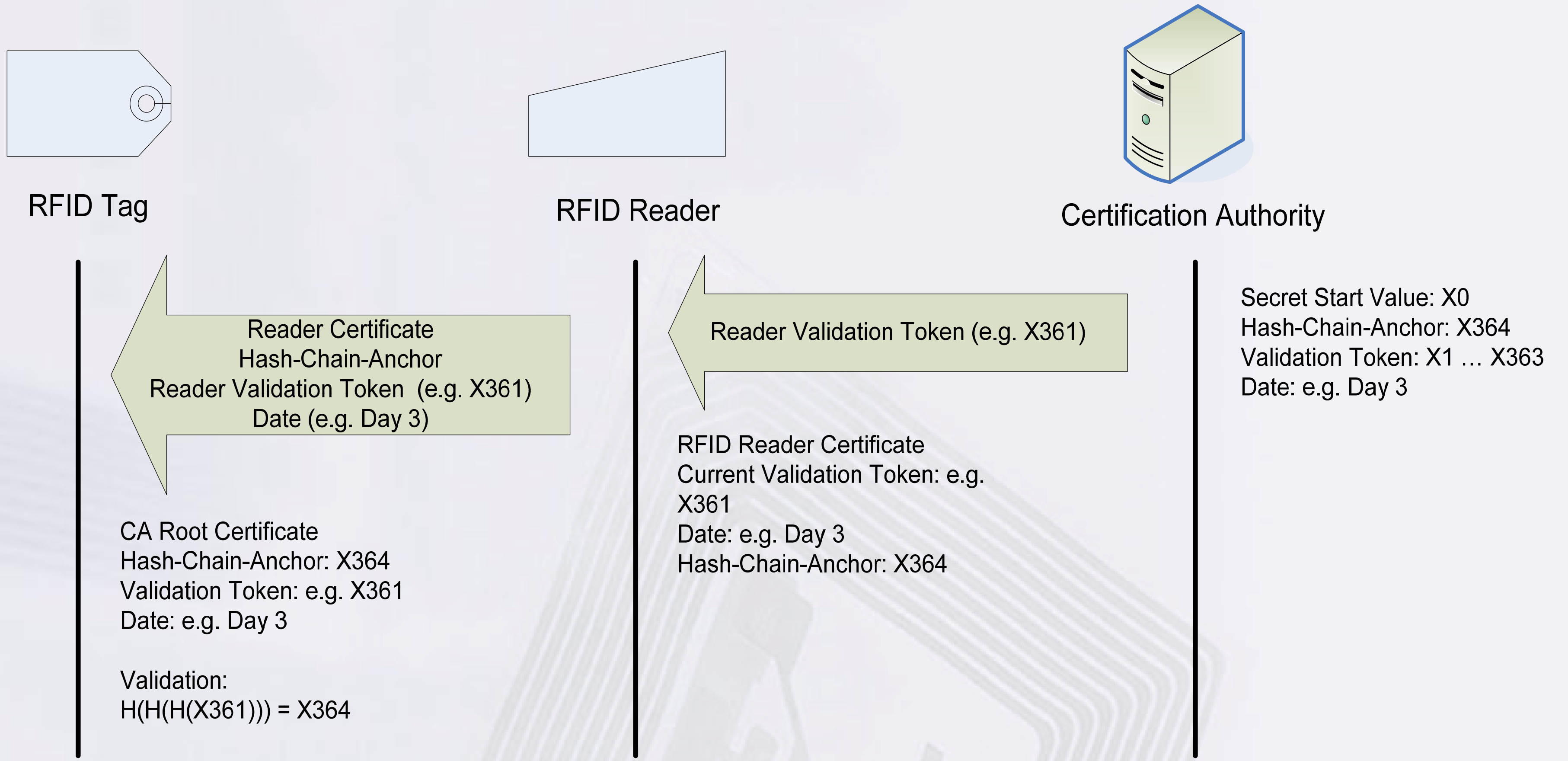
X362
Day 2

X363
Day 1

X364
Hash-Chain-Anchor

X0 is the Secret Start Value
X1 = Hash(X0) X2 = Hash(X1) ... X364 = Hash(X363) are the Validation Tokens
X364 is the Hash-Chain-Anchor signed by the root CA

Certificate Status Validation Using Hash-Chains (2/2)



RFID Tag

RFID Reader

Certification Authority

Reader Certificate
Hash-Chain-Anchor
Reader Validation Token (e.g. X361)
Date (e.g. Day 3)

Reader Validation Token (e.g. X361)

Secret Start Value: X0
Hash-Chain-Anchor: X364
Validation Token: X1 … X363
Date: e.g. Day 3

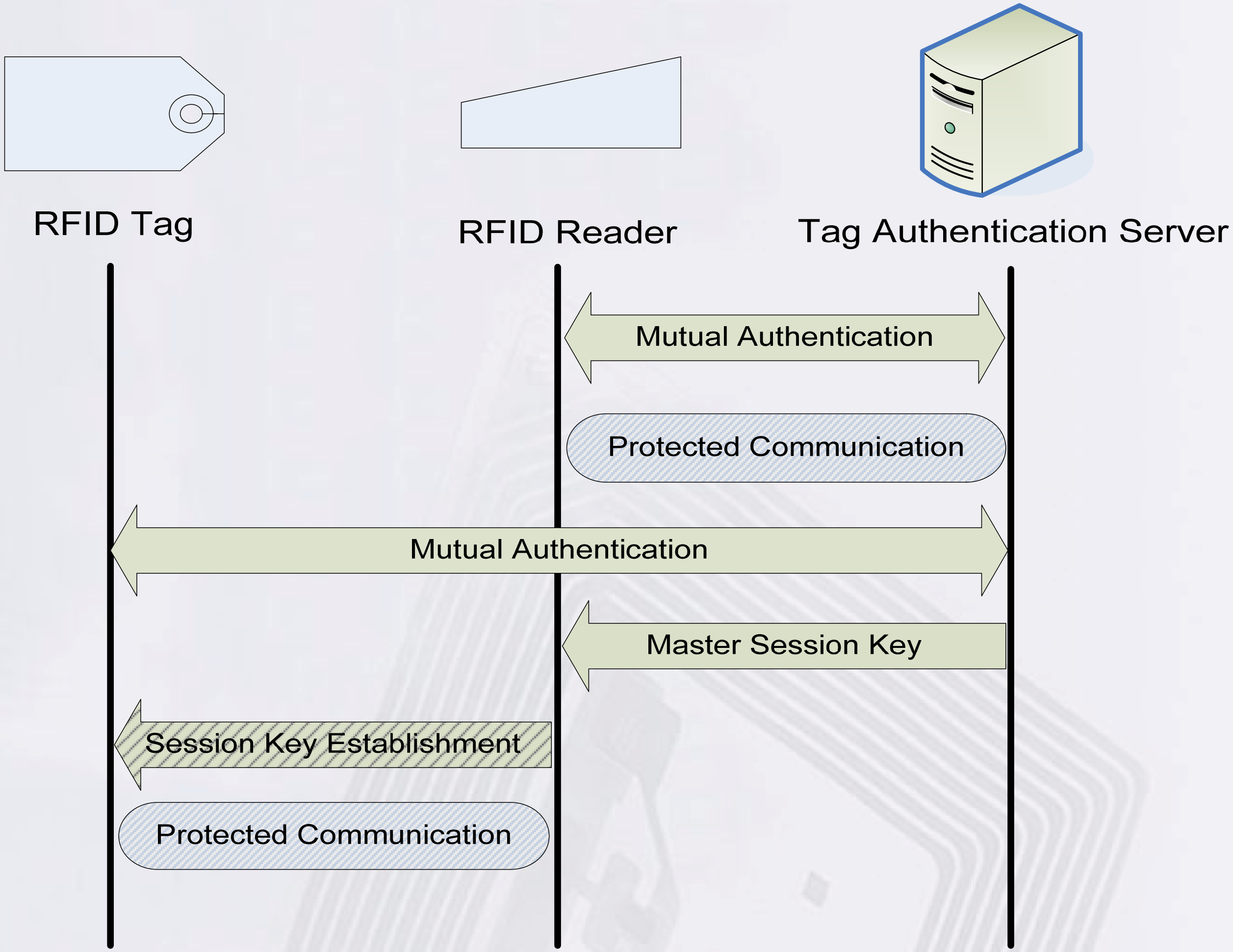
RFID Reader Certificate
Current Validation Token: e.g. X361
Date: e.g. Day 3
Hash-Chain-Anchor: X364

CA Root Certificate
Hash-Chain-Anchor: X364
Validation Token: e.g. X361
Date: e.g. Day 3

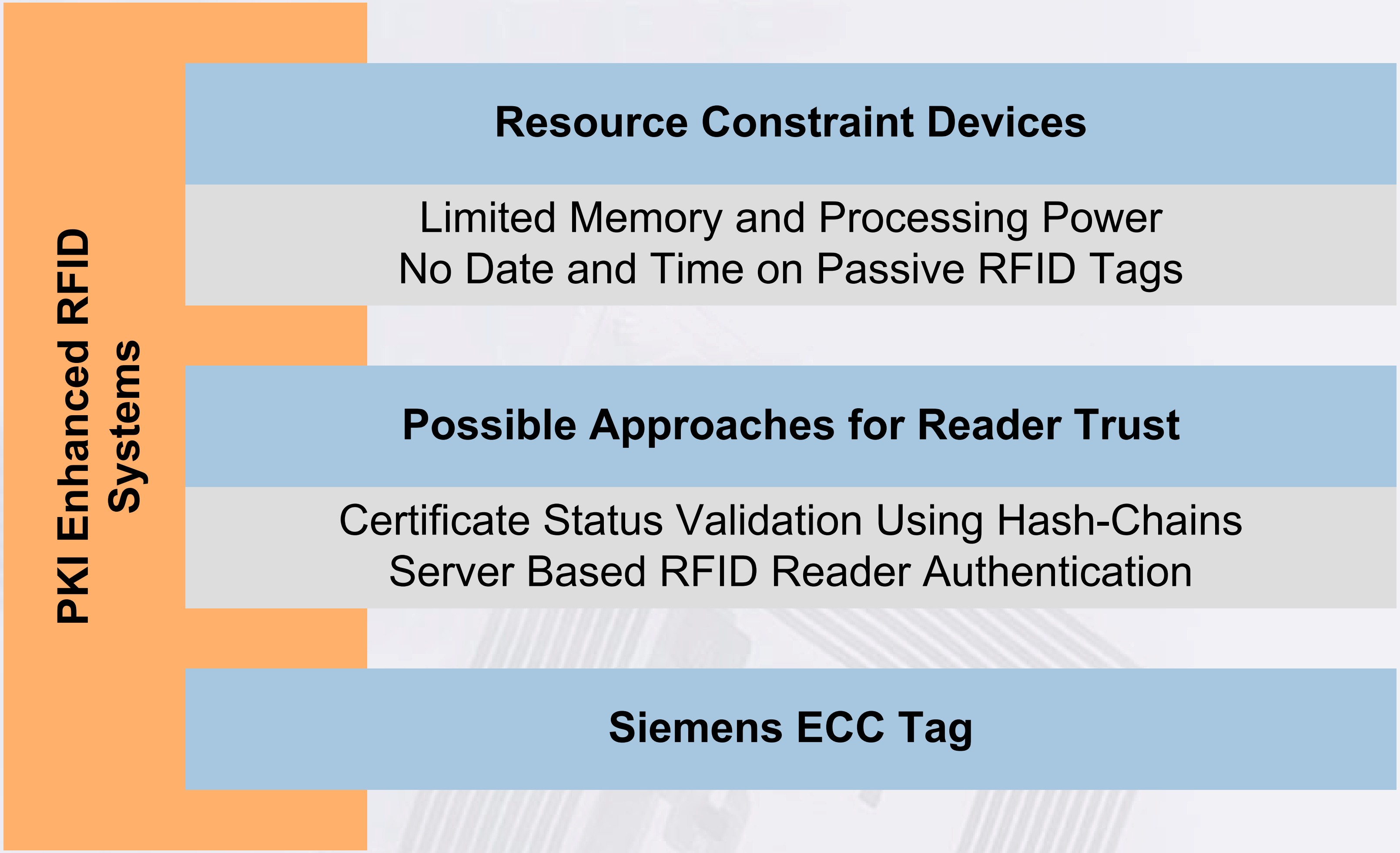
Validation:
H(H(H(X361))) = X364

SIEMENS

Server Based RFID Reader Authentication



Summary & Outlook



PKI Enhanced RFID Systems

Resource Constraint Devices

Limited Memory and Processing Power
No Date and Time on Passive RFID Tags

Possible Approaches for Reader Trust

Certificate Status Validation Using Hash-Chains
Server Based RFID Reader Authentication

Siemens ECC Tag

Andreas Köpf
Siemens AG, CT IC 3
Andreas.Koepf@Siemens.com
+49 89 636 50524