OSS-ASSOCIATION E.V.

(Open Security Standards Association)

Aussicht zukünftige Standards

Stand: Juni 2018

OSS ASSOCIATION

STANDARD KEY MANAGEMENT

OSS
STANDARD KEY MANAGEMENT

ADVANTAGES OF OSS STANDARD KEY MANAGEMENT:

- Invisible keys
- Multiapplication
- Key rolling

OSS ASSOCIATION

Projekt 1: Standard Key Management

- Key Management für RFID smartcards
- Key Management für mobile ID
- OSS SKM für RFID smartcards
- Multi-application smartcard
- Umfang des Projektes
- Ziel von OSS SKM

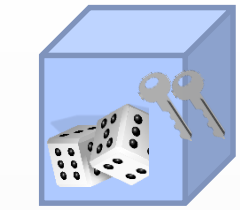
Ziele OSS SKM

- Sicheres Schlüsselhandling
- Sichere Schlüsselfreigabe für Multiapplikationslösungen
- Einzelne Marktteilnehmer können z.B. einen Teil der Lösung aufbauen:

- Tool zur Generierung von Anwendungsschlüsseln und Erstellung von OSS-konformen Schlüsselcontainern
- System mit Online-RFID-Lesegeräten zum Laden von Anwendungsschlüsseln auf Basis eines OSS-konformen Schlüsselbehälters
- Offline-RFID-Lesegeräte, die das Laden von Anwendungsschlüsseln auf Basis eines OSS-konformen Schlüsselbehälters unterstützen.
- RFID-Smartcard-Hersteller unterstützt Schlüsselabruf aus OSS-konformen Schlüsselbehältern

OSS ASSOCIATION

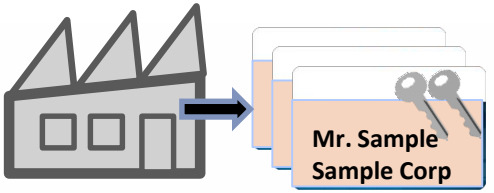
Key Management für RFID smartcards



Key generation

Key distribution

Key storage

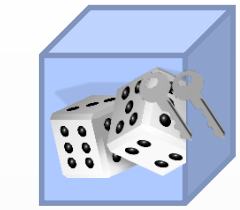


Key usage for RFID
smartcard initialization

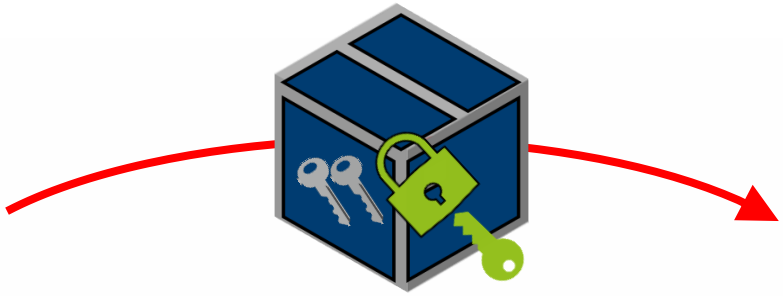
Key configuration
Key rolling

OSS ASSOCIATION

Key Management für mobile ID



Key generation



Key distribution

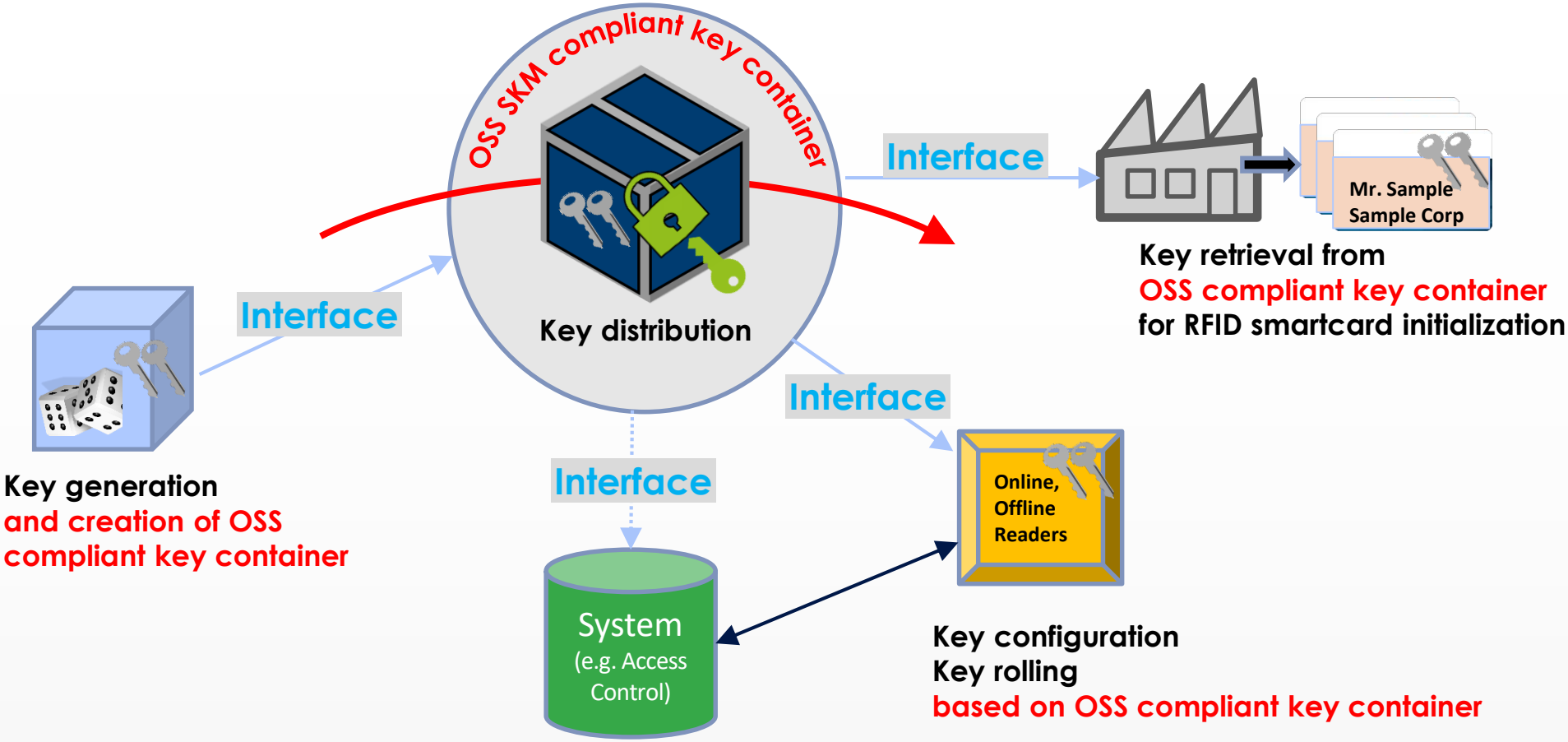
Key usage for mobile credential deployment

Key storage

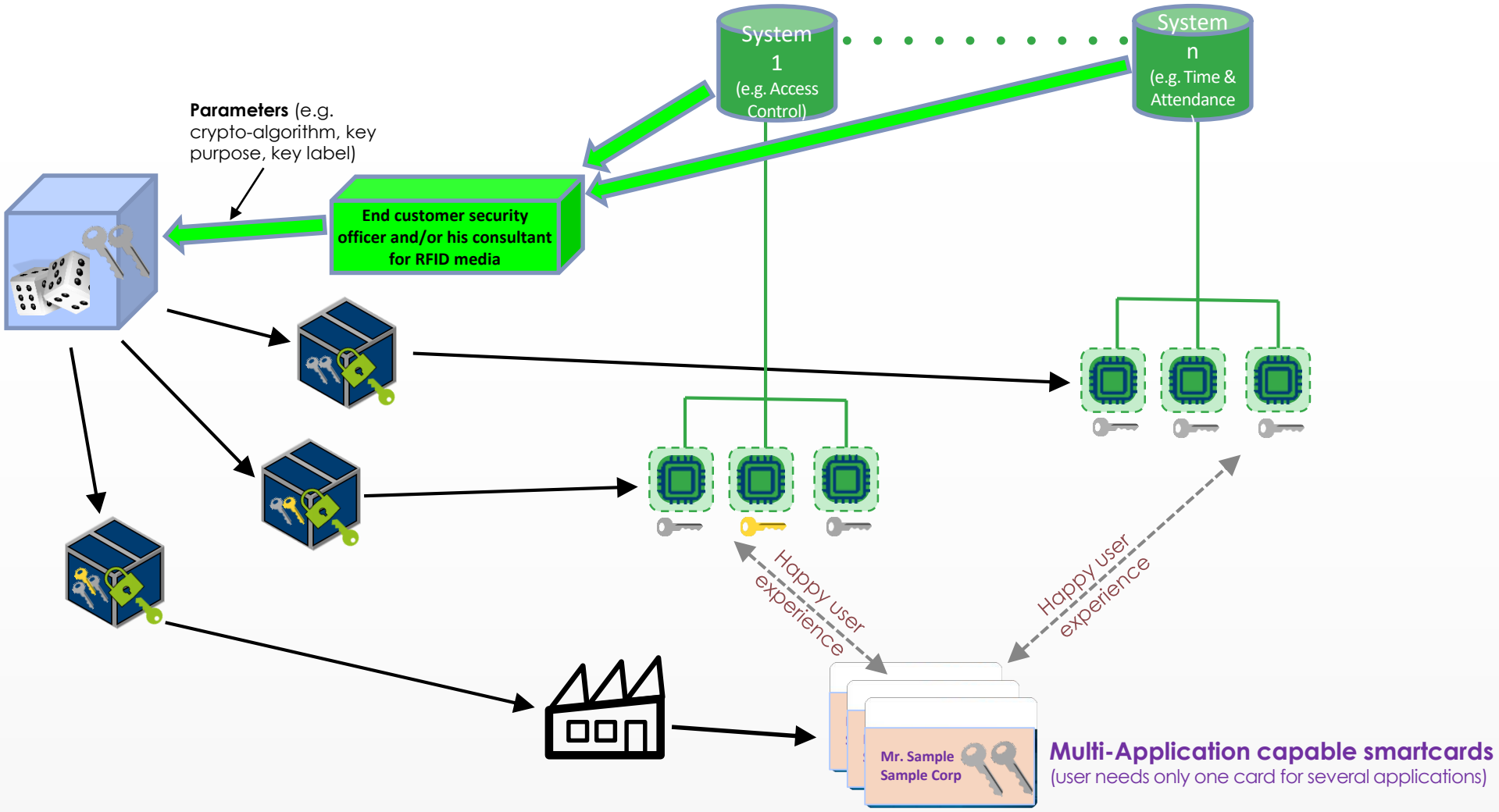
Key configuration
Key rolling

OSS ASSOCIATION

OSS SKM für RFID smartcards



Multi-application RFID smartcard



OSS ASSOCIATION

Umfang SKM

Standardisierung des OSS-Schlüsselcontainers

Aspekte:

- **Zugriffsrechte** auf dem Leser
- **Dateninhalt:** Anwendungsschlüssel mit Schlüsselzweck, Krypto-Algorithmus, Absender, Erstellungsdatum....
- **Datenformat** und -struktur im Container
- **Kryptographischer Schutz** des Containers (symmetrischer oder asymmetrischer Containerschlüssel*)
- Transportmedien (RFID-Smartcard, mobiler Ausweis, Internet)

OSS ASSOCIATION

Wir starten

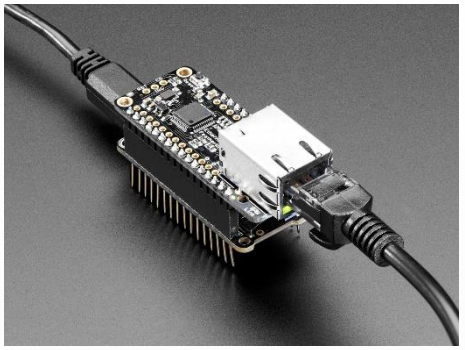
- Jetzt
- Mit Mifare DESfire
- Anschließend Legic
- Dann Mobile

Das alles hängt aber davon ab ob Endkunden Interesse bekunden und anschließend auch kaufen.

OSS ASSOCIATION

OSS Open Door Protocol ODP

- Standard Protokoll für alle Elemente die „Auf, Stopp, Zu“ machen
- Ersetzt den potential freien Kontakt durch LAN
- Ersetzt teure Schnittstellen für Gebäudemanagement Systeme
- Erlaubt Wartungsinformationen



OSS ASSOCIATION

Wir sind offen

- Für Anforderungen der Endkunden an bestehende Standards
- Für Anforderungen an den zukünftigen Standards SKM und ODP

OSS ASSOCIATION

Vielen Dank! / Thank you!

Fragen und Antworten / Questions and answers

OSS ASSOCIATION

Kontakt / Contact

OSS-Association e.V.
In der Aue 41
14480 Potsdam
Deutschland

www.oss-association.com