

MOBILE PHYSICAL ACCESS CONTROL

HOME

TOKENIZATION

DIGITAL KEY

IDaaS

IoT

DIGITALIZATION

SMART WORKSPACE

CONNECTED CAR

INDUSTRIE 4.0

CITY

IDENTITY & ACCESS MANAGEMENT

OSS Mobile Key Concept
Standardization Proposal



OSS - Open Security Standards Association (Germany)

- ▶ **Standard Offline:** standardized way for offline locks of various brands to read and receive access permissions from different card vendors.
- ▶ **OSS SKM 2018:** Secure key management, key authentication for multi-app solutions, tool for OSS compliant key container, etc...
- ▶ **NEW:** For **Standard Offline - Mobile Key** to be defined



- ▶ Concept comparable to “**OSS – Standard Offline for Card**”
- ▶ **Manufacture independency** – Customer can select broad range of products from various vendors to satisfy its needs
- ▶ **Hardware independency** – to support various locks, **Bluetooth LE ICs / NFC ICs**
- ▶ **Easy to implement** – the implementation of the standard should be economically reasonable for product vendor
- ▶ **Cost of the Standard** – Ideally, the standard is **Free of Charge**



5.2 SYSTEM TOPOLOGY

The following chapter provides a brief overview of all of the components involved and describes how they interact with each other.

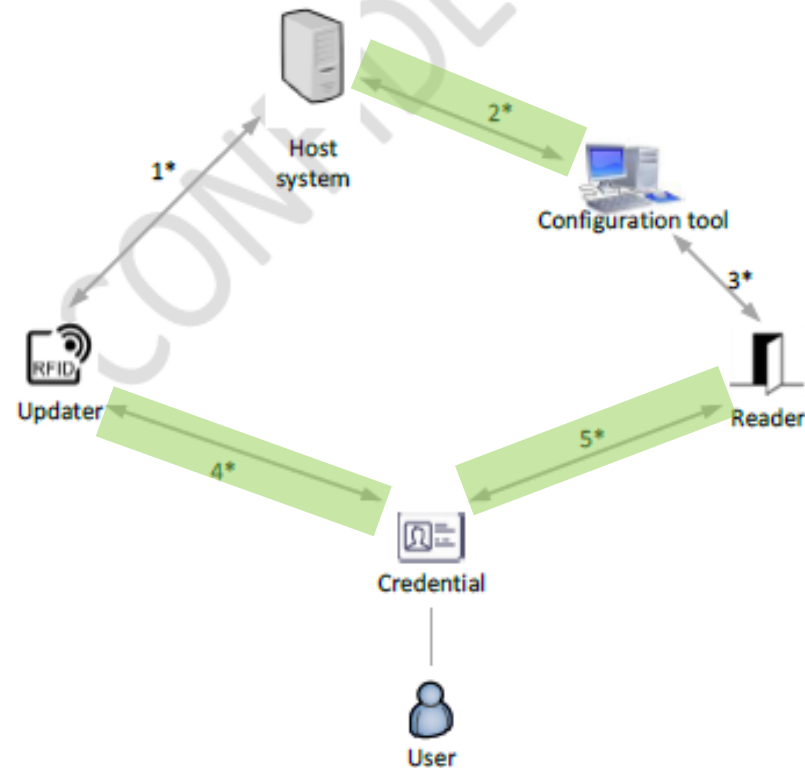


Figure 2 Overview of system topology

5.2 SYSTEM TOPOLOGY

The following chapter provides a brief overview of all of the components involved and describes how they interact with each other.

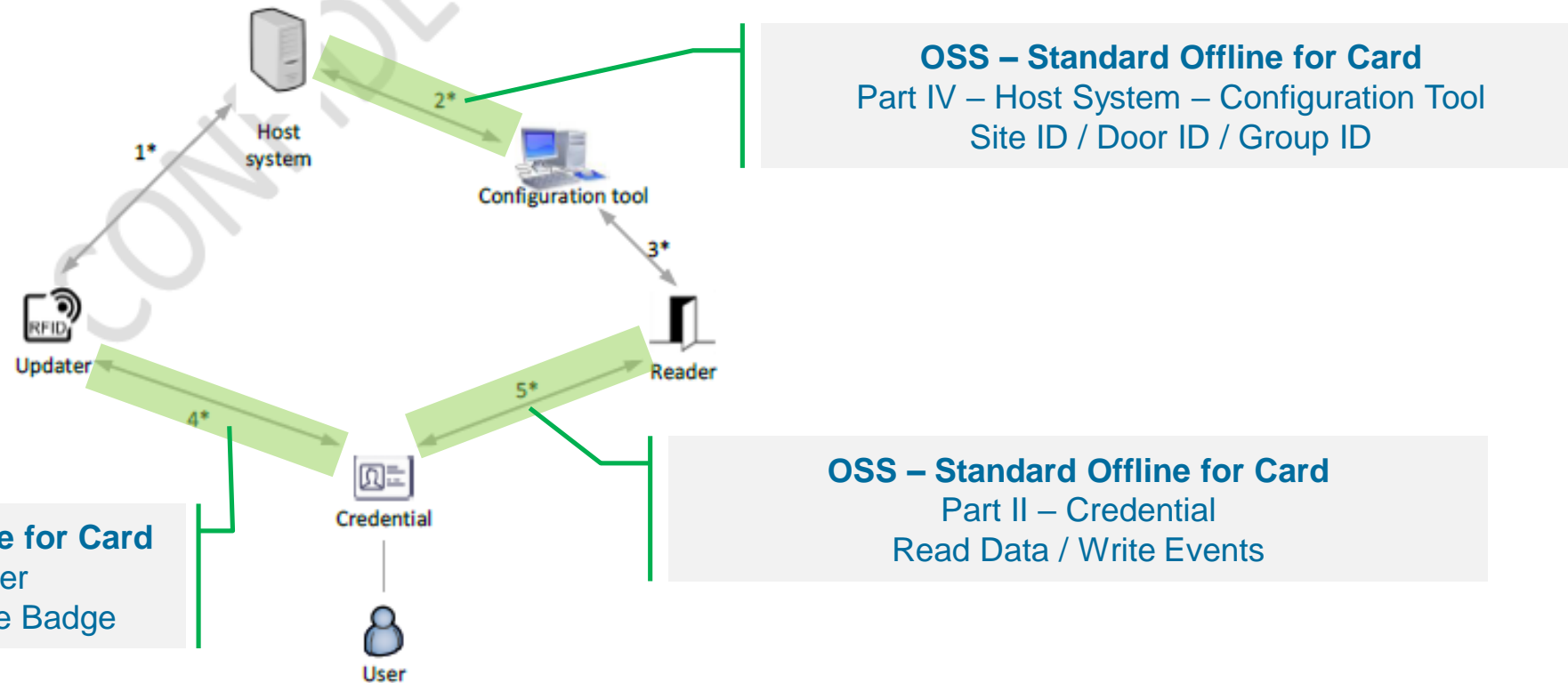
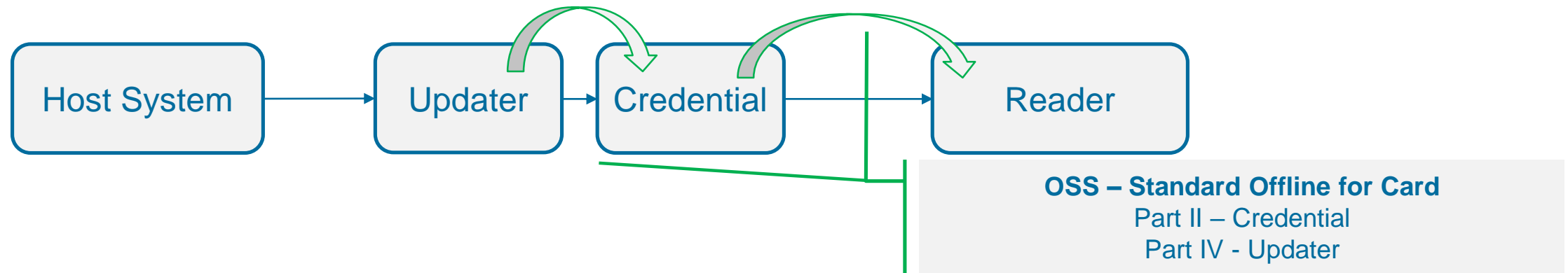
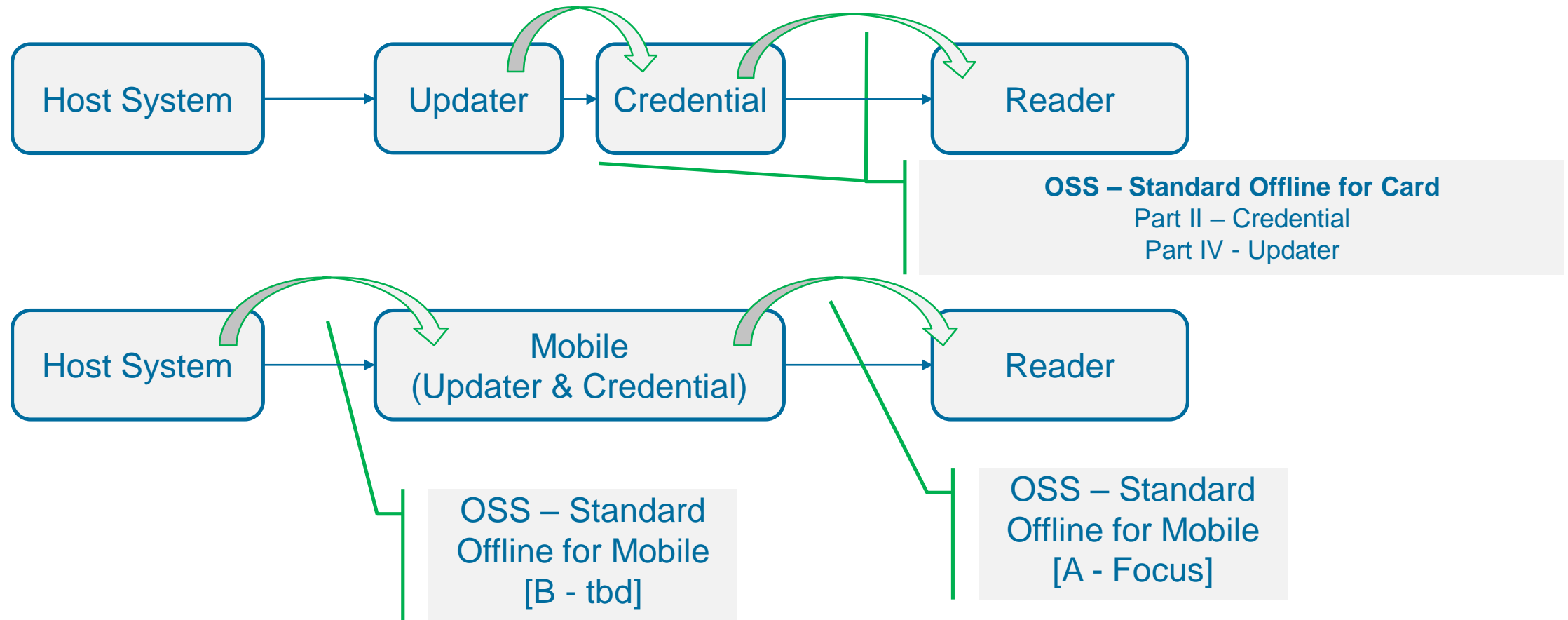


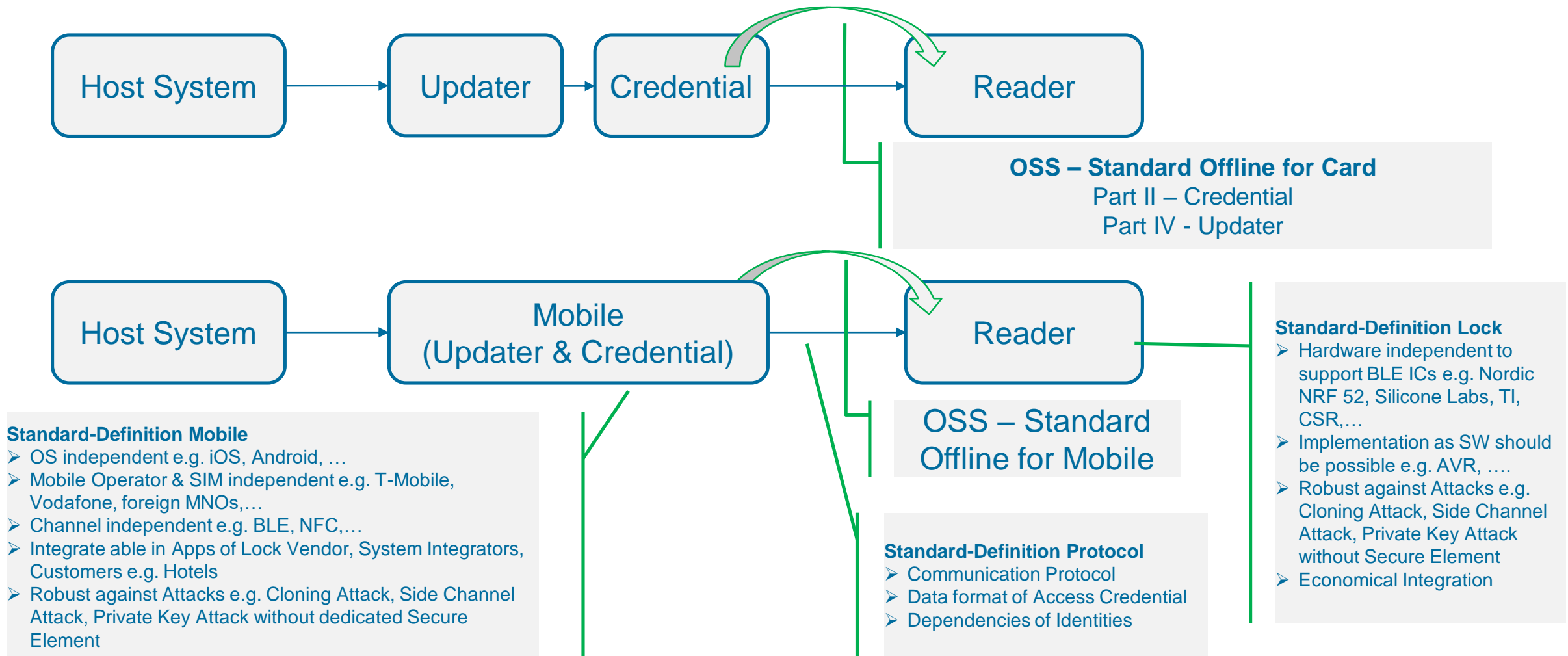
Figure 2 Overview of system topology



Comparison of Interfaces



Requirements of Mobile Key

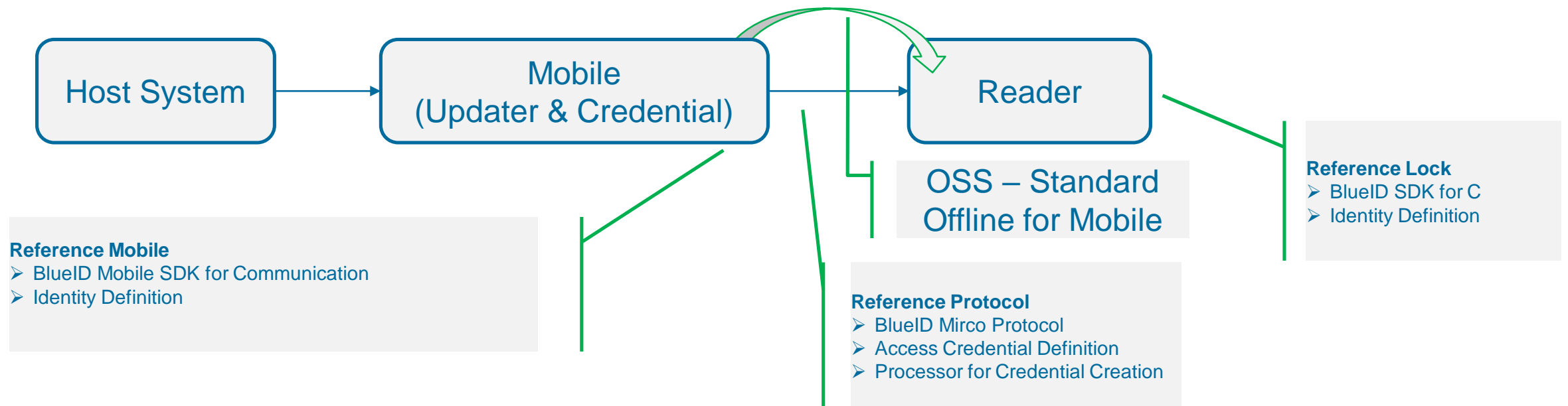


BlueID has a proven and established Mobile Key Implementation

- ▶ Based on state-of-the-art PKI
- ▶ audited extensively by security specialists and it's customer

Mobile Key based on Certificates

- ▶ No hardware dependency → because software
- ▶ No Secure Element required → thanks to PKI
- ▶ Asymmetric crypto Keys → completely Offline



Mobile Key Standard based on Certificates (asymmetric Crypto & PKI)

- ▶ Protocol definition could be based on Micro Protocol
 - ▶ Communication Protocol
 - ▶ Data Format of Access Credential (Certificates/Token)
- ▶ Software Implementation for Lock
 - ▶ Crypto and communication free under OSS
 - ▶ Integration possible in any Chip and as software only
- ▶ Software Implementation for Mobile
 - ▶ Protocol implementation for Communication for iOS & Android free under OSS
- ▶ Standard for Identities
 - ▶ implementation statement for Mobile and Lock Identities

In the interest of the OSS goals,

- BlueID willing to contribute it's Micro Protocol into OSS
- Provide Communication SDKs for the Standard under OSS for free

We're open to further discussions

Thank you for your attention!



...granting access everywhere!

BlueID GmbH

Marcel-Breuer-Strasse 15
D-80807 Munich
Germany

+49 / 89 / 8 09 90 26 – 00
+49 / 89 / 8 09 90 26 – 19

info@blueid.net