HARDWARE SECURITY
W3C COMMUNITY GROUP MEETING

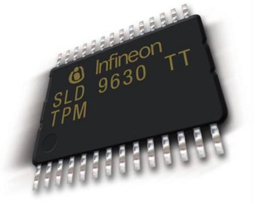
April 2016

LIFE IS FOR SHARING.

W3C HARDWARE SECURITY WG – LONDON APRIL 26/27

DEUTSCHE TELEKOM VIEW OF PROBLEM SPACE

TrustZone®
Security Foundation by ARM®



HARDWARE FEATURES TO SUPPORT

- Embedded Secure Element
  - Found in many handsets (e.g. Apple iPhone)
- Smartcard
  - Via card reader attached to PC
  - Contactless via NFC
  - In the handset as microSD card
- UICC
  - In handset connected via Single Wire Protocol
- TEE
  - Hardware-backed security for ARM and Intel processors
- TPM
  - Security anchor in PCs

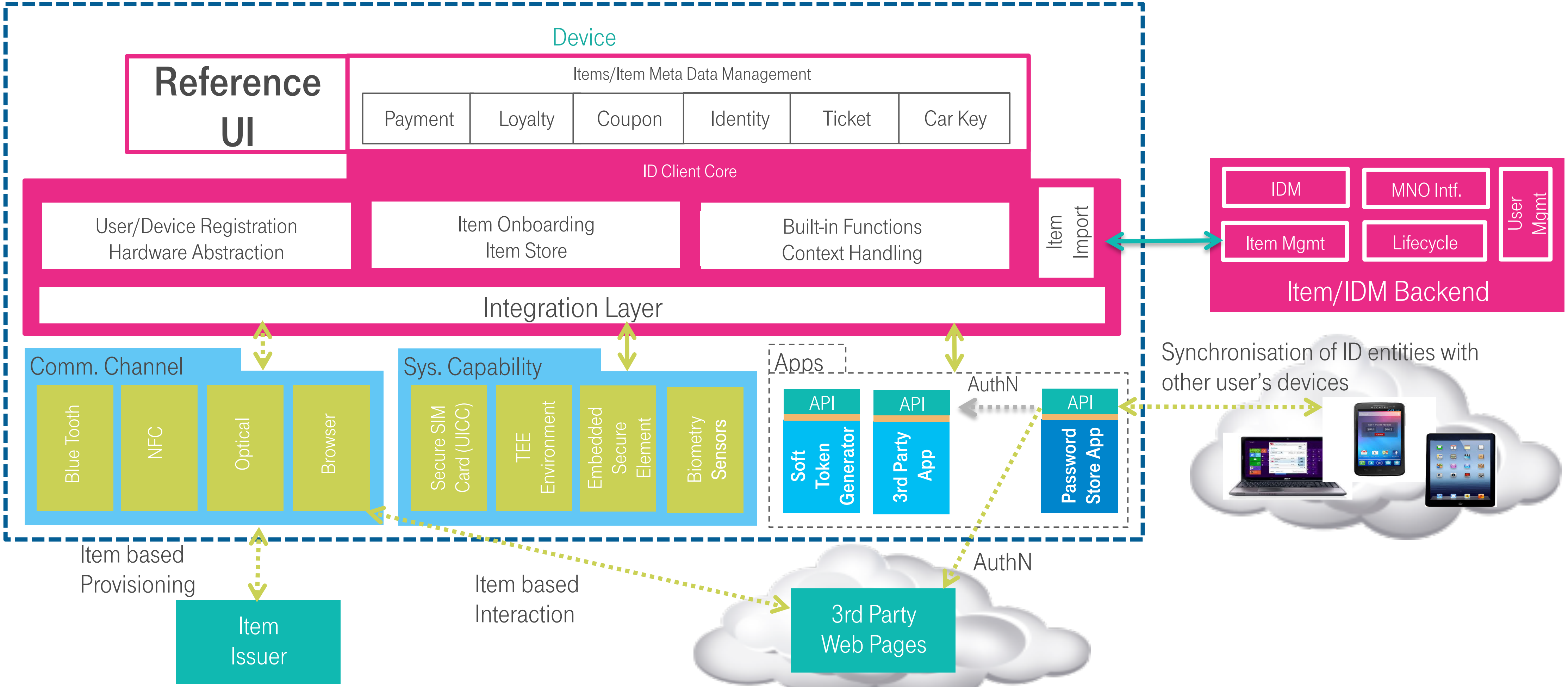
OTP

(((eTicket
Deutschland

USE CASES TO SUPPORT

- Car Key
- One-time password
- Ticketing (e.g. public transport)
- Payment
- Banking (German HBCI)
- Access control
- Authentication, signature, encryption (typical smartcard scenarios) - FIDO

T-LABS ID-CLIENT
OVERALL FUNCTIONAL ARCHITECTURE



Telekom **Innovation Laboratories**

GENERAL CONSIDERATIONS WITH HARDWARE SECURITY

Hardware security is being used billions of times all around the world

- SIM cards
- Payment
- Contactless tickets (some even ‚with contact')
- Door keys (in corporations as well as in e.g. hotels)
- Citizen IDs

Many of which already have – or could have – touchpoints with the Web

- 'Embedded SIMs' allowing to virtualize what used to be a distinct piece of hardware
- Finally getting EMVCo ‚Card present' payment in the web (VISA/ MC seem to be working on using the SE for this…)
- ‚Derived Identity Data' from proprietary citizen IDs

The potential to ‚webinize' the processes for virtualizing, provisioning, purchasing and administrating existing hardware security-based everyday processes is huge