G+D Mobile Security

Java Card Forum Webinar

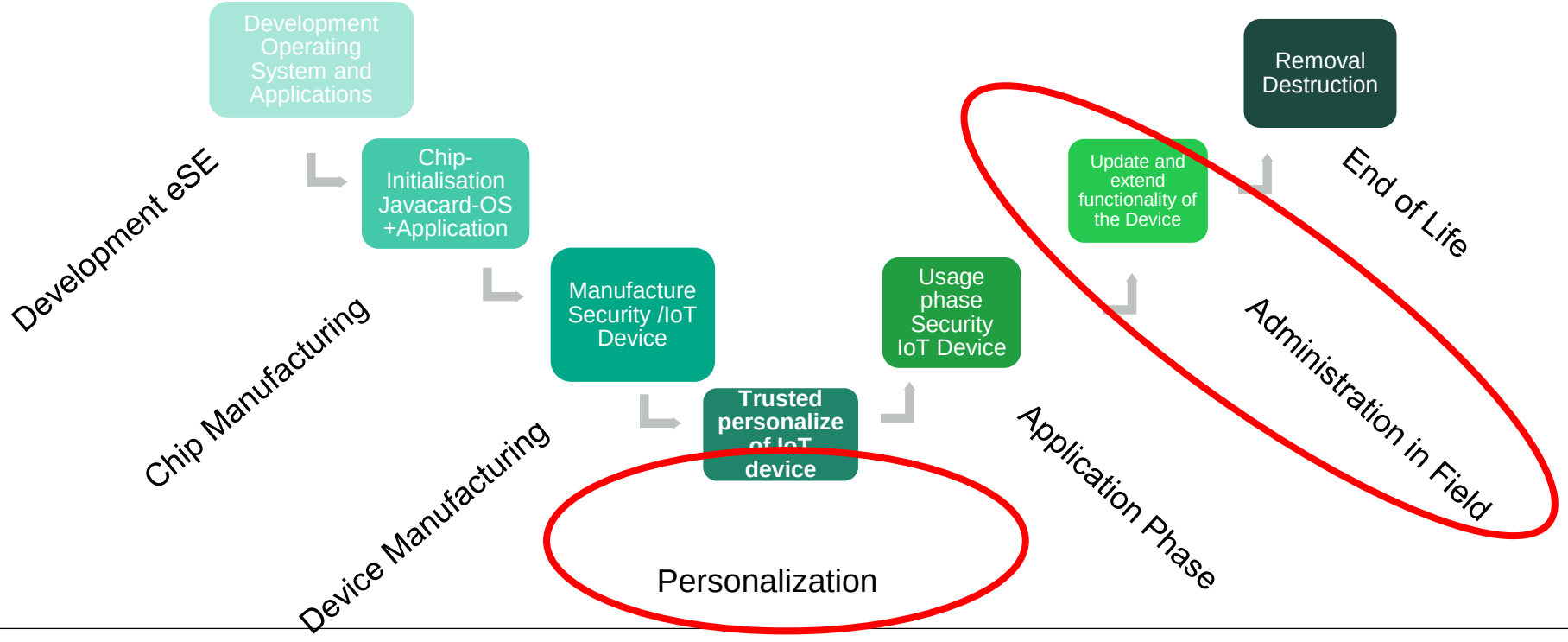
Secure Personalization of Java Card and Applications in the Operational Phase

Dr. Ullrich Martini
Product Management
Giesecke + Devrient Mobile Security GmbH
25th November 2020

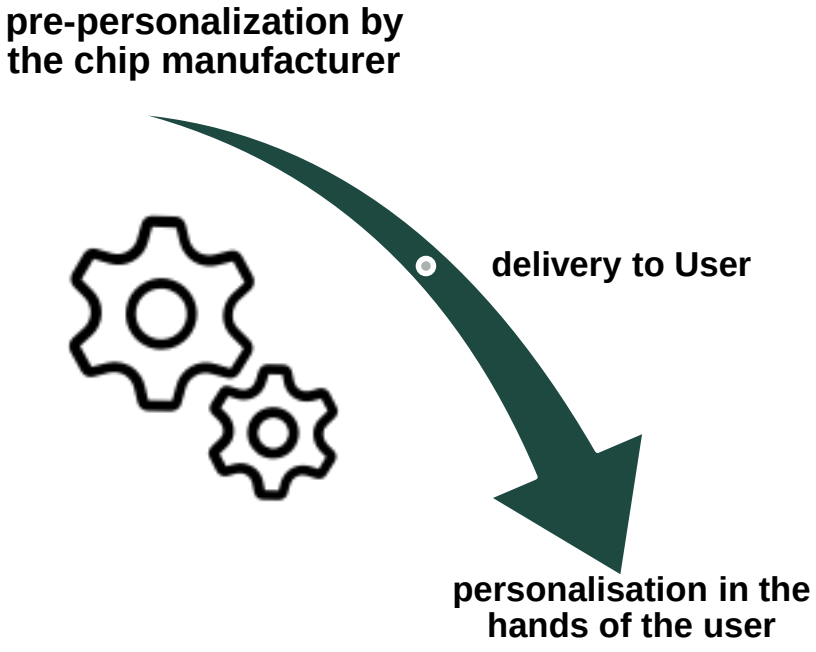
Overview

- Requirements and Problem Statement
- Related Specifications
  - JavaCard
  - GlobalPlatform
- Solution
- Implementation
- Examples

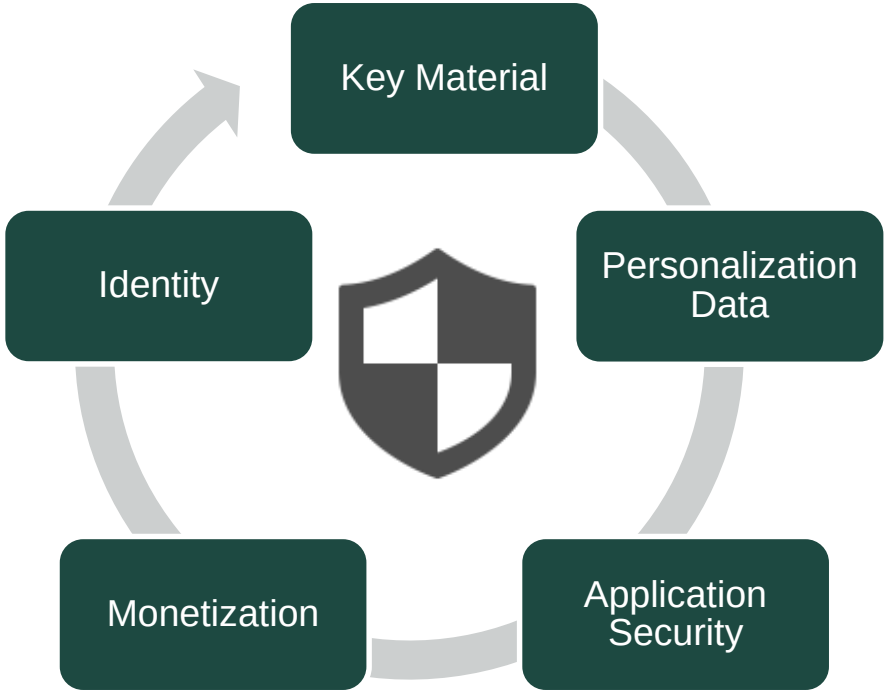
Life Cycle of a Security/IoT Device



Requirements for Flexible Production



Requirements for Secure Personalization



Basic Requirement: Implemented Java Card Features

Cryptography:

- Elliptic Curve Signatue (ECDSA)
- Elliptic Curve Key Agreement (ECKA)
- (Optionally) RSA (variant of key generation)
- AES

Applet-to-Applet Communication:

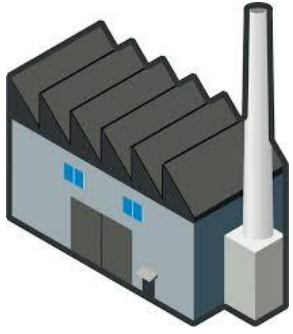
- Communication between Security Domain and CASD

  → CASD will generate a key set for this instance

- Communication between Applet and its (associated) Security Domain

  → Applet will use its associated Security Domain to verify and decrypt personalization commands

Solution for Flexible and Secure Personalization: Overview



GP Specifications offers extensions of Java Cards:
Amendment A: Confidential Card Content Management
Amendment F: Secure Channel Protocol '11'
Amendment I : Secure Element Management Service

In the factory:
Install JavaCard operating system and applet packages
Create Issuer Security Domain
Create Controlling Authority Security Domain (CASD)
Pre-Personalizing

In the field:
Apply Secure Channels
Provide Key Generation
Perform Applet-Loading/-Personalization

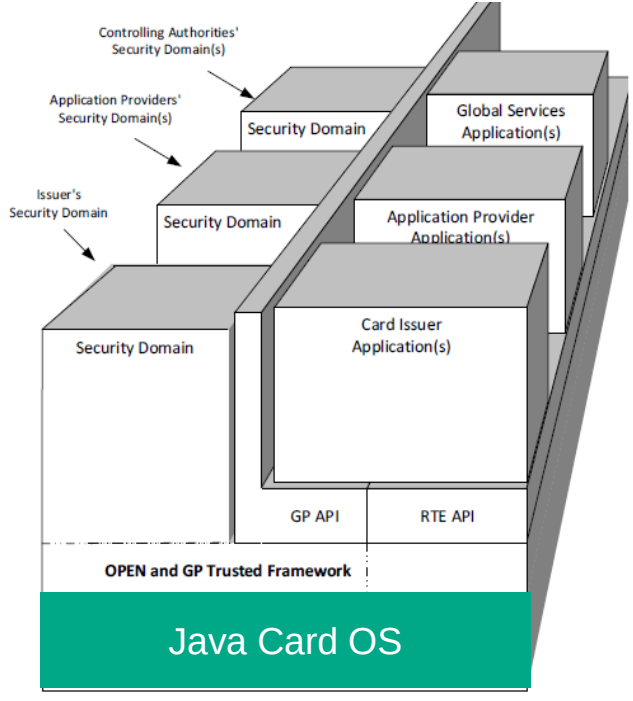
Relevant Entities in the Java Card/GP Architecture

- Java Card OS
- GlobalPlatform Framework
- Security Domains

  →manage keys for their associated application
- Specific Security Domains

  →Issuer Security Domain

  →Controlling Authority Security Domain
- Contactless Registry



What is needed for Secure Personalisation

- Pre-defined Security Domain
- Pre-defined Controlling Authority Security Domain (Amendment A)

  →required for key generation in the field
- Set-Up of a Secure Channel
  - → Secure Channel Protocol 11 (Amendment F)
    - Elliptic curve key agreement
    - Elliptic curve signature
    - establish AES keys for Authentiation / Encryption of Secured Command Sequences (CMAC) acc. Secure Channel Protocol 03
  - → Subsequent commands secured commands using AES/SCP03
- Contactless Registry (for contactless applet registration)

Preparation of Secure Personalisation in field

External Data Generation

Generation of

- Public Key Pair
- Certificates

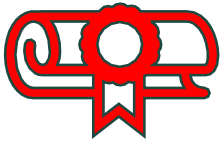
chip individual key material

Pre-Personalisation of ISD/CASD Data in each chip

CA public key

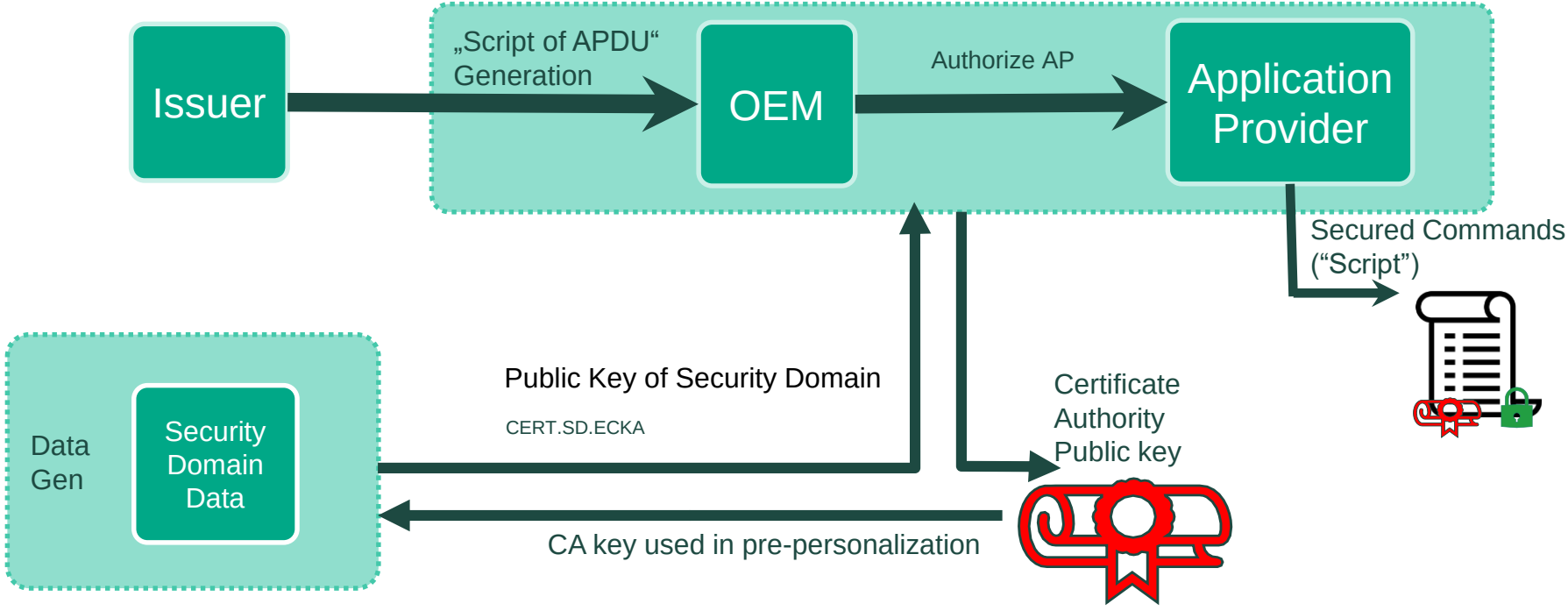
CA hierarchy for Application Providers

Application Provider's certificates

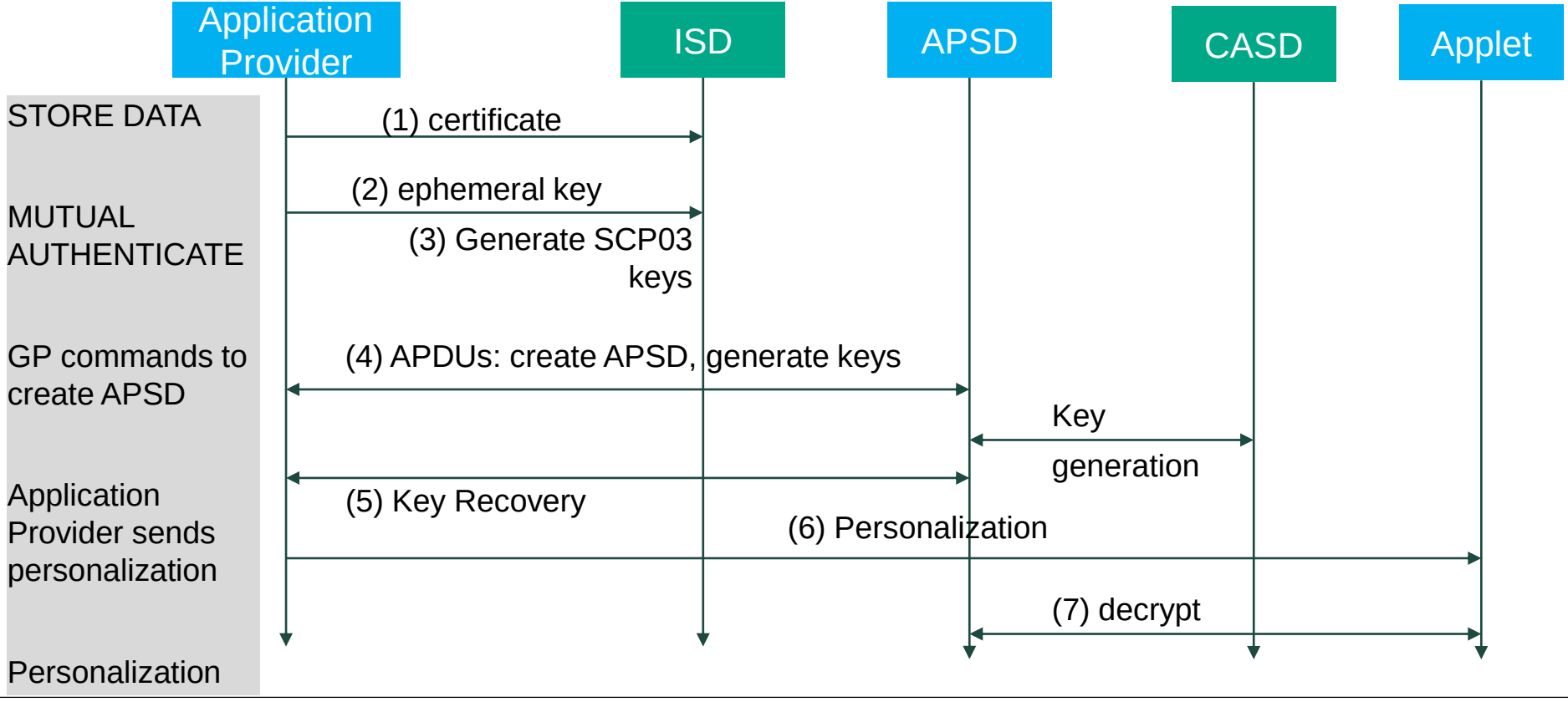


Secure APDU Sequence Generation

Preparation for personalization scripts in Usage Phase



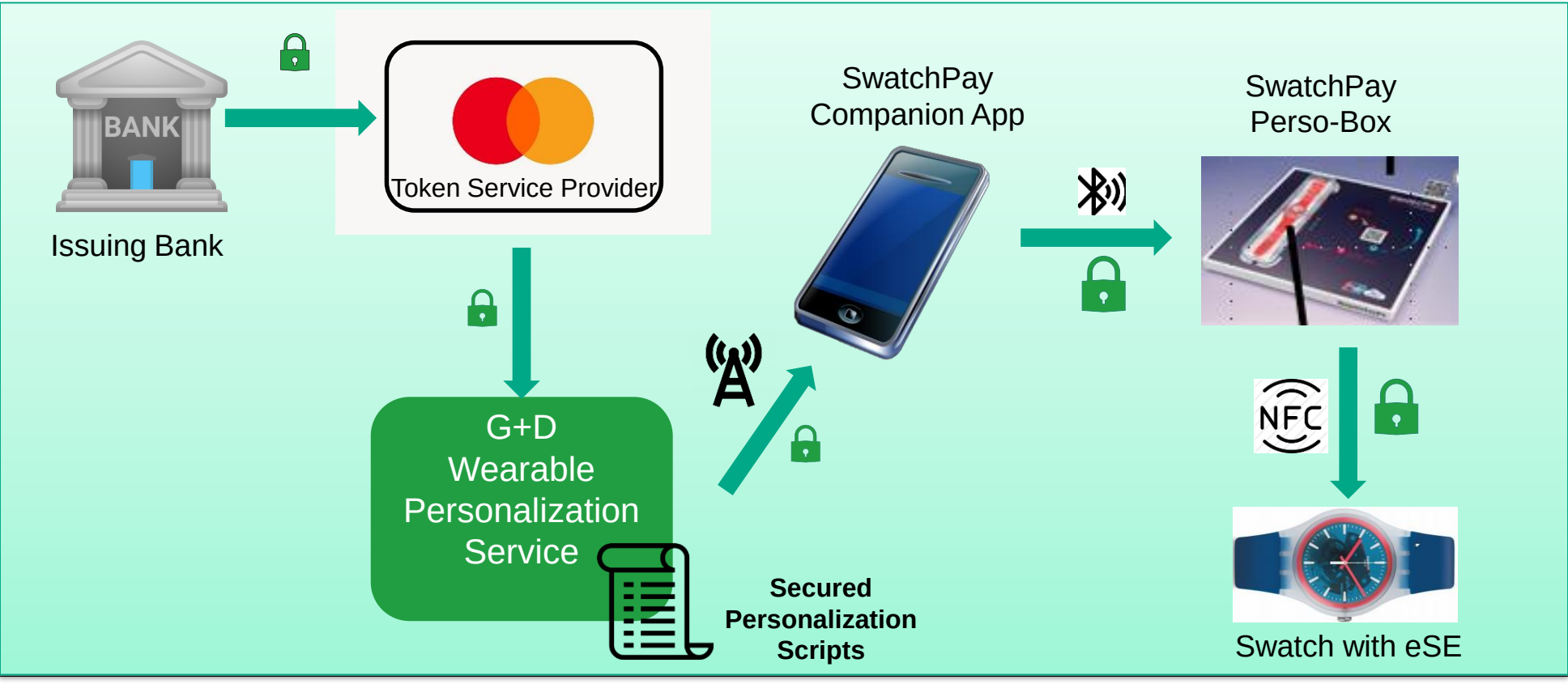
Personalize applet in the field



Details of Secured Comand Sequence APDUs

- First APDU
  - Certificate that identifies the Application Provider
  - Certificate may contain information about allowed commands
- Second APDU
  - Ephemeral key of Application Provider
  - No ephemeral key of Security Domain
  - Key Agreement performed and SCP03 opened
- Following Commands
  - SCP03 security as specified by Global Platform

Personalization in Field: Swatch Pay!



Example 1: Payment Function for Wearable Devices

Users have a companion app for their wearable device

- User Interface
  - Personalization
  - Management
- Distribution of APDU sequences („Scripts“) via Google Firebase
- Connect wearable device to Token Requestor
- Management of tokens
  - Set preferred card directly
  - Suspend, unsuspend, delete, view transactions via the Token Requestor

Wearable can be used like a contactless card in the shop

Example 2: IoT device managed in field

Remote Management for an Excavator Machine

- Machine prepared for remote maintenance
- When setting up a new excavator machine owner will:
  - Update the machine to install owner‘s keys.
  - Initialize a remote maintenance application.
  - Make remote management secure.

Owner now can access remote maintenance

G+D
Mobile Security

Thank you!

Questions

Dr. Ullrich Martini
Ullrich.martini@gi-de.com