GSMA IoT SAFE Applet – only for the eSIM?
Motivation

**Usecase Secure Cloud Authentication**
- Establishing secure connection to AWS, Azure and Co. with TLS

**High Level Overview about the GSMA IoT SAFE specification**
- A common API provided by an Java Card Applet used as a ‘Root of Trust’ by IoT devices

**GSMA IoT SAFE for non-cellular?**
- IoT SAFE was originally intended for eSIM.

**Benefits for IoT SAFE applet with Java Card™ for Infineon**
- Java Card as the basis for Plug and Play Security.

**Infineon findings with a GSMA IoT SAFE applet**
- Performance and Feature proposals
Usecase Secure Cloud Authentication: System Integration Perspective **Without** Hardware Security
Usecase Secure Cloud Authentication: System Integration Perspective with Hardware Security

Secured IoT Device with discrete Secure Element

AWS IoT

AWS IoT Endpoint

Managed MQTT Broker

Authentication & Authorization

Transport Layer Security (TLS)

Network Stack

Device Private Key

Device Certificate

AWS Trust Anchor

Secure FW

Network Stack

Host Library for TLS

I2C Library

MQTT

Application

IoT Device Host
Main drivers why customers decide on discrete SecureElements for Cloud Authentication

Secure Trust Provisioning decoupled from the Main MCU Firmware
› Cloud authentication keys is security sensitive data
› Device OEM treating this very carefully and try to separate this from standard firmware loading for the MCU
› SE components provide a secure storage for this sensitive data
› This sensitive data shall only be handled by highly secure and trusted personalization sites.

Physical Tamper Resistance
› mitigation against strong adversaries, e.g. against cold boot memory attacks or hardware bugs such as Spectre/Meltdown Rowhammer, or Clkscrew
› the main application processor will always have a significantly larger attack surface than dedicated secure hardware

Certification and Regulations
› Some cloud products require a certified Secure Element today e.g. AliCloud
› Preparing long term
› Proofing “state of the art security” by using a certified product

Persistant Storage for flashless SoC
› Application Processors with their extremely small technology nodes today (<10nm) cannot efficiently accommodate NVM anymore
› Monotonic values for countermeasures need to reside in NVM
- Retry counter for the PIN
- Session counter in Secure Protocols Replay Attack Prevention
- Values have to be persistent (atomic and tearing-safe)

Flexible, fast and costefficient personalization options
› Loading of customer specific and chip unique credentials during the wafer test
› Wireless of the inbuild low cost contactless interface on each chip (for some products)
GSMA IoT SAFE
IoT SIM Applet For Secure End-to-End Communication

IoT SAFE:
› Uses the SIM as a mini ‘crypto-safe’ inside the device to securely establish a (D)TLS session with a corresponding application cloud/server
› Is compatible with all SIM form factors (e.g. SIM, eSIM, iSIM)
› Provides a common API for the highly secure SIM to be used as a hardware ‘Root of Trust’ by IoT devices
› Helps solve the challenge of provisioning millions of IoT devices

- Standardized approach for a TLS Root of Trust in form of an Java Card Applet
- Another important step towards real Plug and Play Security
- Eases the integration efforts with middleware ecosystems eg. openSSL
GSMA IoT SAFE
Supporting Documents

Download from [here](#)

Download from [here](#)
Plug and Play Trust Anchor Secure Element

Secured IoT Device with discrete Secure Element

- Java Card™ SE
- IoT SAFE Secure Element
- Java Card™ OS

IoT Device Host
- Application
- MQTT
- GP T1’ I2C
- Host Library for TLS
- Network Stack

» Java Card is the foundations for even further standardized components
» IoT SAFE implements the application for the cloud authentication vertical
» The GlobalPlatform APDU over I2C/SPI T1’ specification defines an common protocol layer
Flying with Security ease – paradigm of flying IoT

Secure enrollment
Sensor fusion
Geo-tagging
Secure GPS
Secure platform
Multiple PKIs
Secure communication
Secure mission profile(s)
Multi layered security
Data analytics
Geo-fencing
Secure beacon
Software signing
Battery authentication
Multiple certification and PKI in action

No-fly zone – e.g. airport

Special permit to enter no-fly zones – e.g. to inspect critical infrastructure
Issuance of certificates and keys to the drone

Permission is granted via personalization of certificates and keys

Permission is managed by PKI system provided by PrimeKey

Certificates are used to authenticate the drone to a Air Traffic Control Center using LTE
Secure Drone Demo
Securing the commercial use of multicopters - whitepaper

PKI in Action
Securing the commercial use of multicopters

Infineon Multicopters and Drones - website
IoT SAFE
One Applet multiple use

› Applet Development
› Verification
› Documentation

External Sourcing because of Java Card API and IoT SAFE

GSMA IoT SAFE Java Card™ Applet

Cellular eSIM portfolio
- Java Card™
- OPTIGA™ Connect IoT

non-cellular SE portfolio
- Java Card™
- OPTIGA™ Connect Consumer
- Java Card™
- OPTIGA™ Trust non-cellular IoT
- Java Card™
- Secora™ Connect for wearables

Copyright © Infineon Technologies AG 2020. All rights reserved.
Findings in our IoT SAFE implementation

**Performance Improvements**
- Extended APDU vs Chaining support
- Combination of commands into oneShot operations

**Feature Improvements**
- Configurable Access Policies
- Creation of generic data objects
- Creation of referenced key object
- More algorithm supported e.g. ED25519 and NIST p384/521

**ALI ID2 support**
- AES encryption schemes(ECB)
Key take-aways / Summary / Conclusion

IoT Cloud Authentication with discrete HW Root of Trust are frequently asked by OEMS

The great idea of IoT SAFE can also be extended to non-cellular products

Real Plug n Play security requires standardization on different level to make the integrations experience best in class
infineon

Part of your life. Part of tomorrow.