Security Conference

UICC, the universal toolbox for securing your services in the 5G ecosystem

Presented by: Denis PRACA – ETSI TC SET CHAIR

THALES

19/10/2023

Overview

- Background
- Closing gaps:
  - Support of multiple logical SE
  - Better integration and improved performances
- Europe and 5G certification
- Next Steps

BACKGROUD

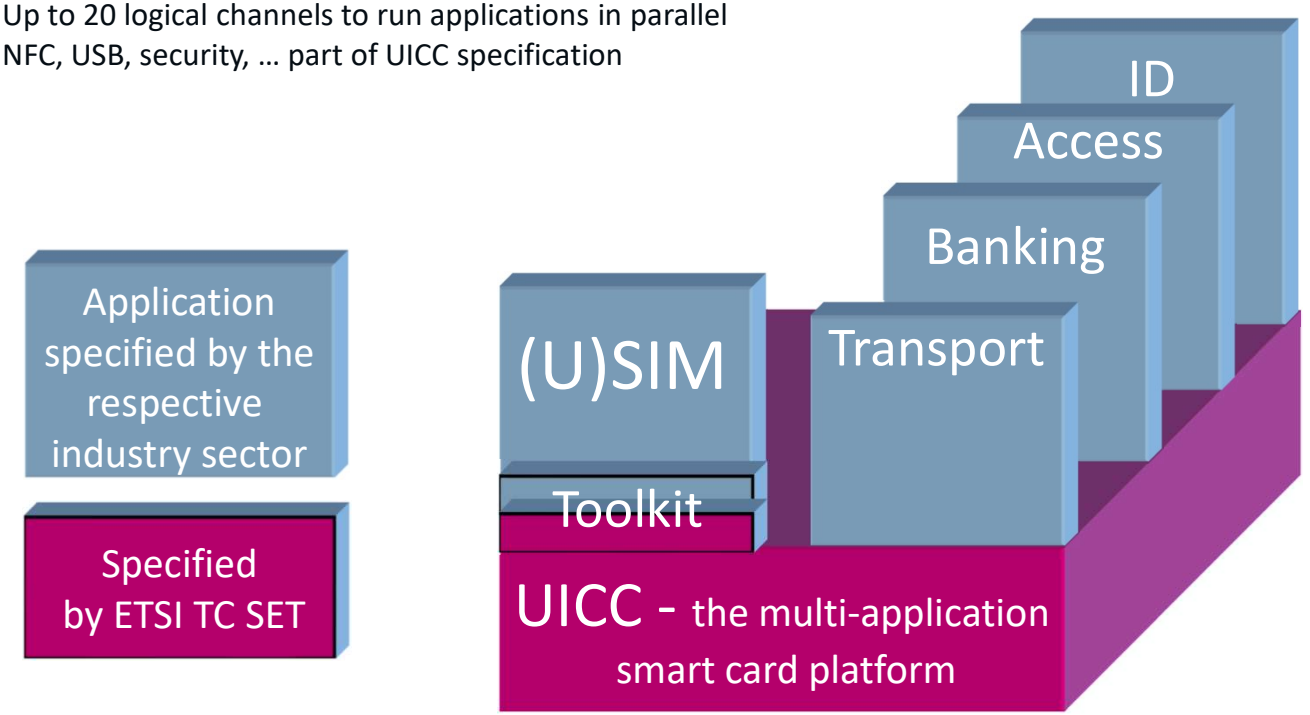
Where we are coming from: ETSI SET is currently defining and maintaining 2 secure platforms: UICC and SSP

ETSI TC SET

Home of the UICC – the most widely deployed Secure Element with more than 5 billion pieces going into the market every year just as SIM cards

The UICC consists of (all) application independent functions and features – the SIM resides as an application on the UICC

- Separation of lower layers and applications
- Up to 20 logical channels to run applications in parallel
- NFC, USB, security, … part of UICC specification



(e)UICC is the base platform for eSIM remote provisioning

The Smart Secure Platform

The new Smart Secure Platform (SSP)

- Started in 2015, delivered in 2019
- Objective: Better integration into the specific use case
- Design: Modular platform offering a core set of features and a number of options
  - Flexible: Options selected at time of implementation, application dependent
  - Choice of interfaces: SPI, I2C, I3C, …
  - Choice of hardware
  - New filesystem and transport/application protocols
  - Support of existing functions: Contactless, Toolkit, APDU, …

How to provide a smoother transition?

- SSP is a nice, modern and powerful platform for hosting secure applications, unfortunately, not yet reaching the field
  - Too late or too much in advance?
  - Too complex?
  - Too costly to invest in?
  - Backward compatibility?
  - Interoperability?
- Could we take benefit of some of the SSP features for the UICCC?
  1. More independence between application issuers
  2. Increased performance
  3. Easier integration in mobile devices
  4. …

CLOSING GAPS

Improve UICC multiapplication support by allowing more independence to application issuers

Problem statement

- Even if applications can be isolated thanks to security domains, they share common resources:
  1. The filesystem
  2. Card Application Toolkit (CAT)
  3. Logical channels
  4. Identifiers
  5. Security context
- Primary request coming from Remote Provisioning (eSIM) specification for the support of multiple enabled Profiles (MultiSIM devices)
  - Different Profiles comes from different MNOs cannot share the same files, CAT, LC…

TC SET answer

- A UICC can be divided in several Logical Secure Elements (LSEs), accessed through different Logical SE Interfaces (LSIs)
  - Every LSE has its own filesystem, security context, up to 20 logical channels,…
  - The LSI is addressed thanks to an extension of T=1 protocol by using the NAD byte or by issuing a MANAGE_LSI(select LSI) command
  - Strict isolation between LSEs is required and may be certified
- An LSE can be:
  1. A logical UICC for use in telecom context (i.e., hosting a Profile remotely provisioned) or hosting different NAAs coming from different providers (i.e., USIM, ISIM, SSIM)
  2. A secure element defined by GlobalPlaform (i.e., SAM)

CLOSING GAPS

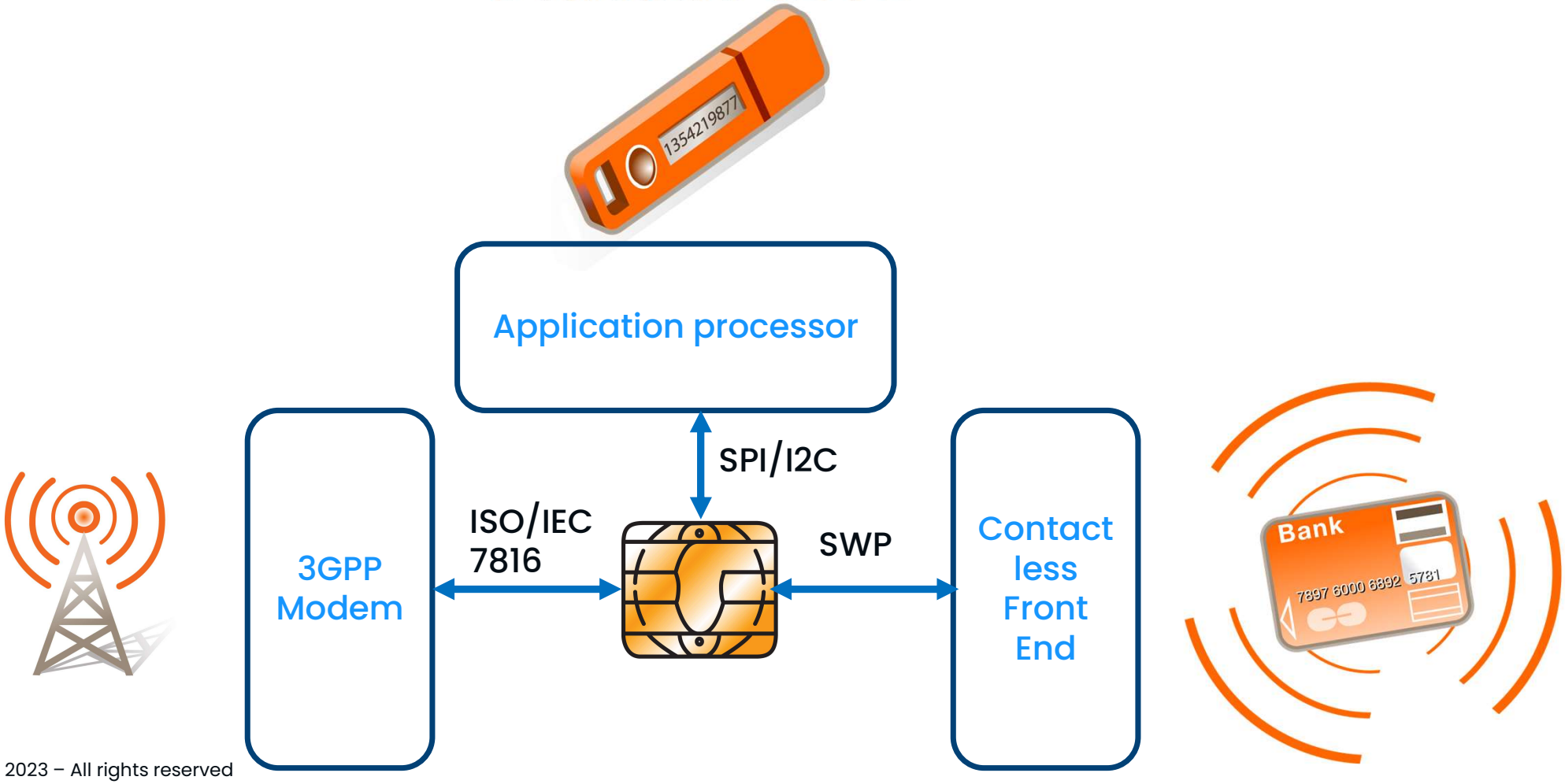
Increase performance and improve UICC integration in mobile devices

Problem statement

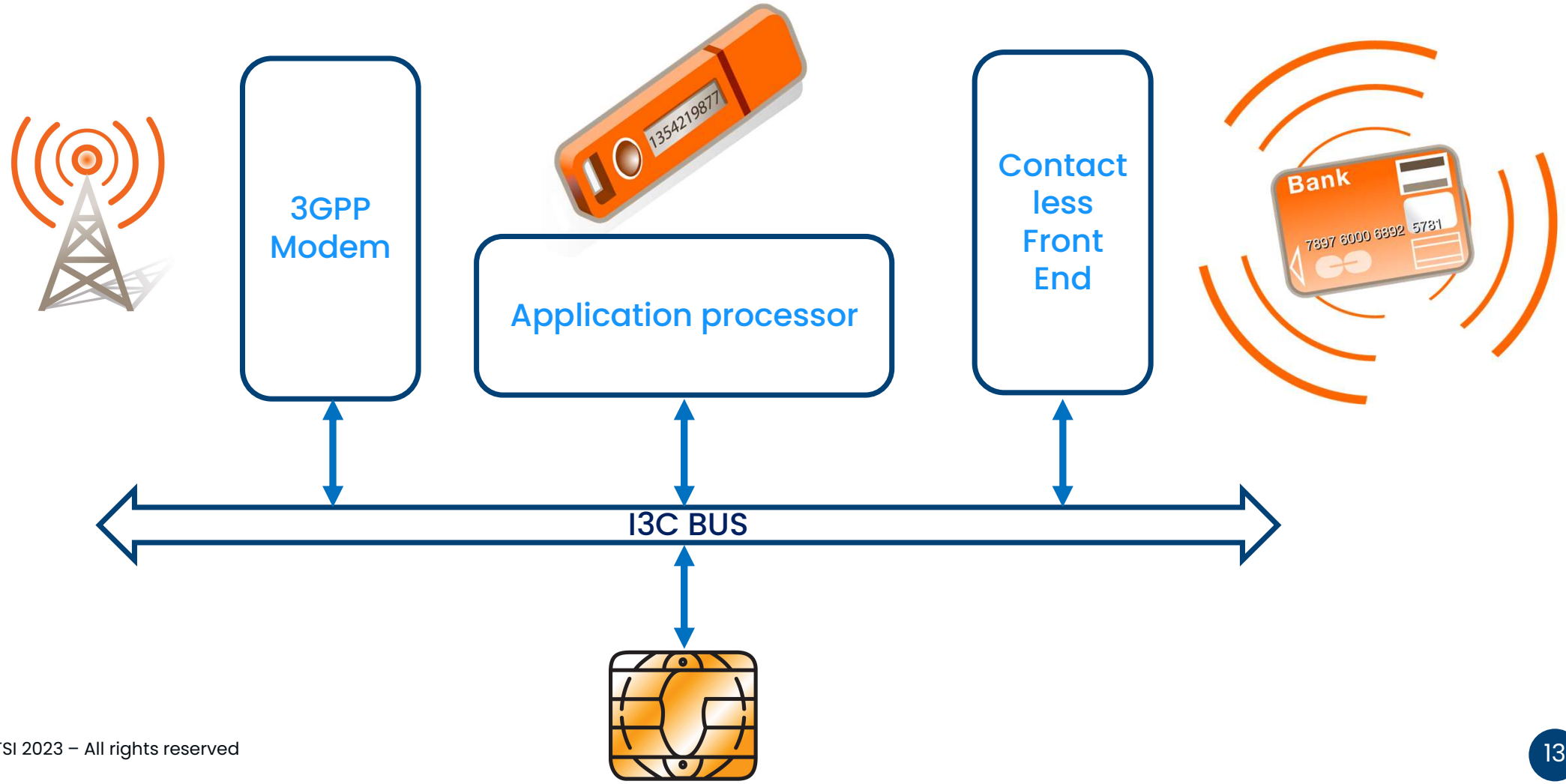
- UICC may combine different applications which require connection to different parts of the mobile device
  1. Connection to the 3GPP modem for network authentication
     - ISO/IEC 7816 physical interface
  2. Connection to a contactless front end for ID, banking, public transport
     - SWP interface
  3. Connection to the application processor for secure token generation, access control, ID
     - Through the 3GPP modem (i.e., OMAPI)
     - Through a dedicated SE interface (e.g., SPI, I2C)

=> More connections, concurrency management, more PCB area

TODAY: up to 3 different interfaces between the UICC and the mobile device



TOMORROW: UICC using MIPI standard



Status

- SET has already defined an I3C interface in TS 103 818
  - In cooperation with MIPI alliance
- This SSP specification will be extended for the UICC in order to support
  - APDU transport with several LSIs
    - Removal of ISO 7816 APDU limitations
  - Contactless
- Multi-controller capability
  - Simultaneous connection to modem, application, CLF…
- Interrupt capability

=> A new small package for embedded UICC supporting I3C is currently under development

EU5G: European certification for 5G elements

eUICC shall be certified according to EU regulations and EU is requesting that eUICC may also be certified to carry European ID (eIDAS)

Technical Proposals

- ID applet should be independent of MNO Profiles
  - Use of different LSE…
  - Rely on GSMA/Globalplatform SAM specifications
- It shall be possible to certify the platform (UICC) independently from the eIDAS applet
  - Certification by composition
  - Rely on CryptographicServiceProvider (CSP) defined by GP
    - CSP holds the keys and crypto services => EAL4+ certified
    - eIDAS applet certified at EAL2 level
- What about provisioning key distribution?

=> On-going activities

What's next in SET?

- Provisioning of LSE on the field?
- Support for Private Network provisioning?
- Creation and configuration LSE supporting of SAM-SD?
  - What will be the PKI model for eIDAS deployment
- PQC…

Thank you for your attention

Follow us on:

Any further questions?

Contact me:

Denis.praca@thalesgroup.com