Date: 13 June 2018 @qualcomm Location: Sophia Antipolis

Qualcomm

Integrating the SIM

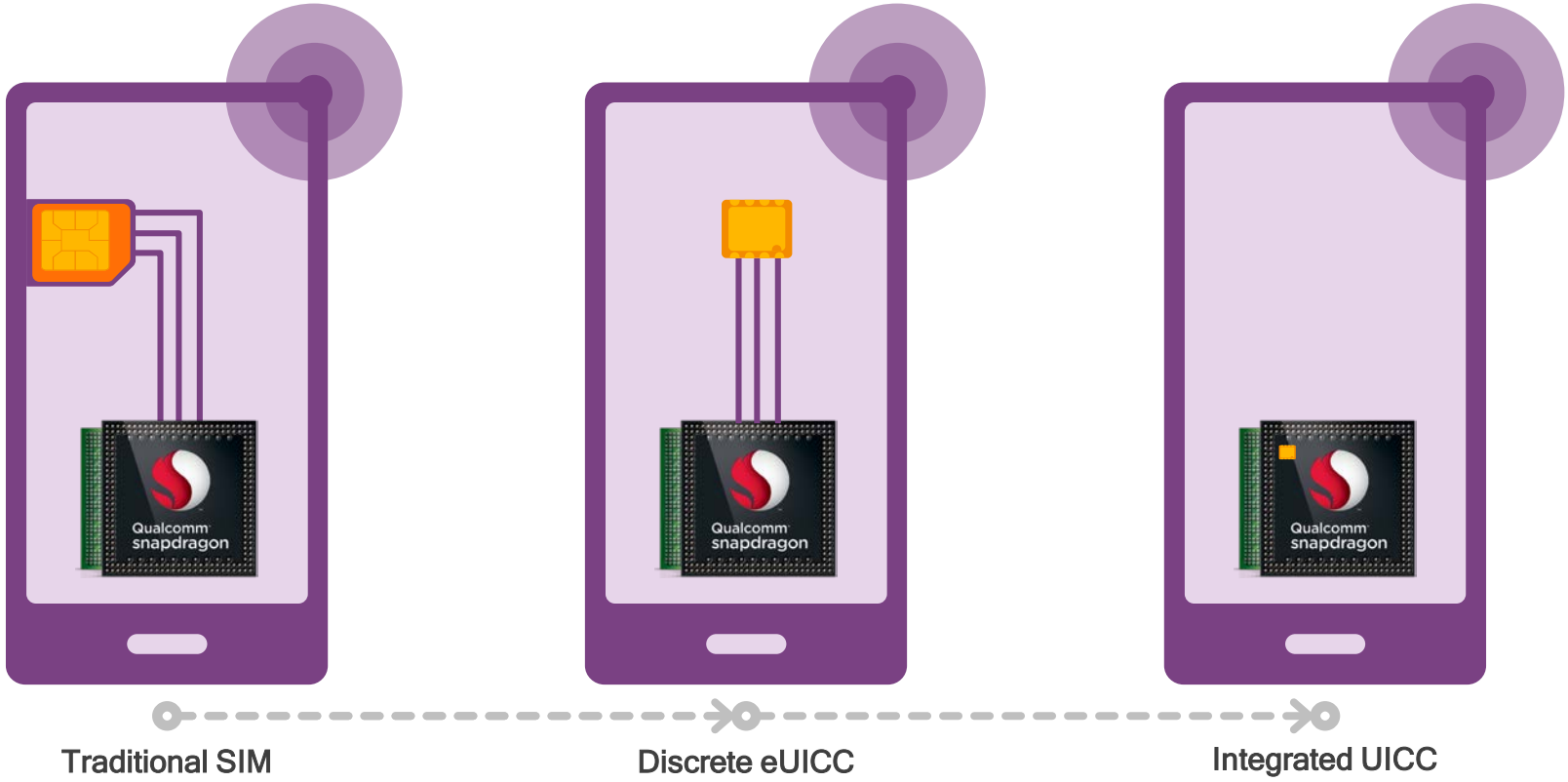
Dr. Adrian Escott

Qualcomm Technologies, Inc.

Agenda

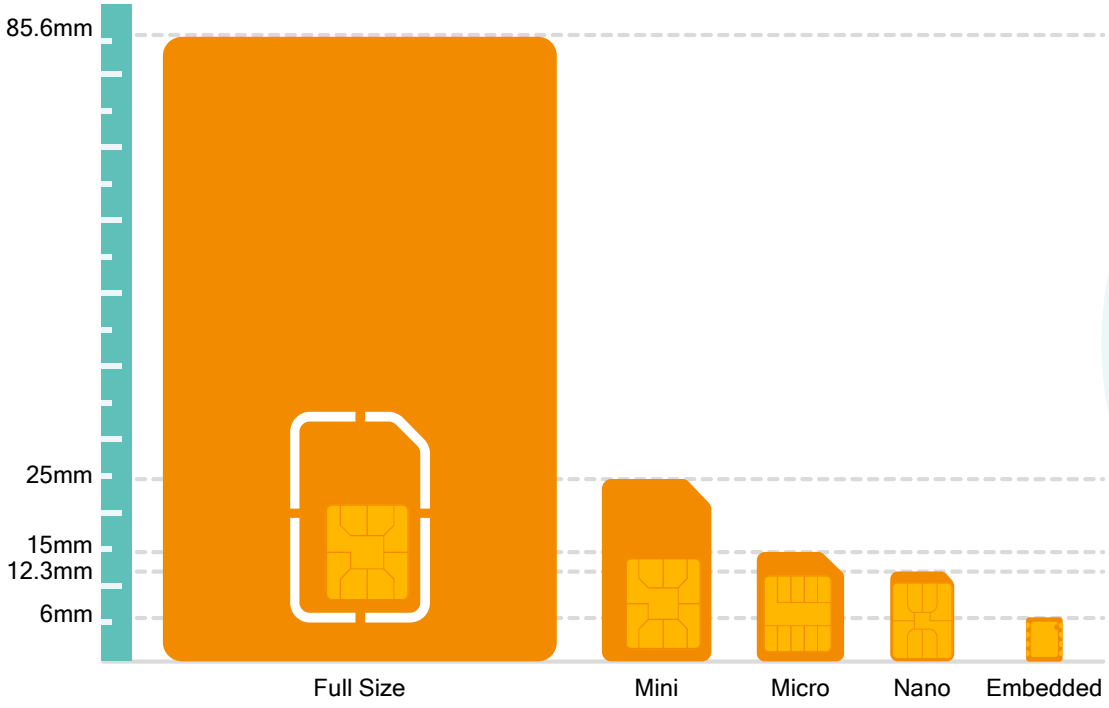
1. Path to iSIM
2. iSIM Size benefit
3. Hardware Architecture
4. Certification and Standardization
5. Beyond the iSIM use case
6. Q&A

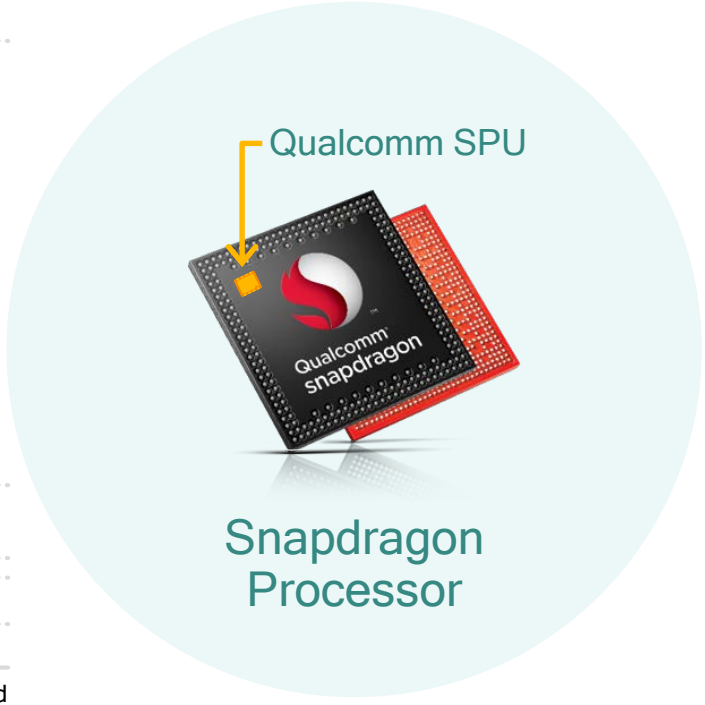
Path to an integrated SIM



Qualcomm Technologies, Inc. (QTI) mobile processor not to scale

Size benefit of integrating the SIM card





Qualcomm SOC not to scale

Size benefit of integrating the SIM card

Traditional SIM cards or eSIMs include NVM, constraining the technology node it can use

Typically 30nm

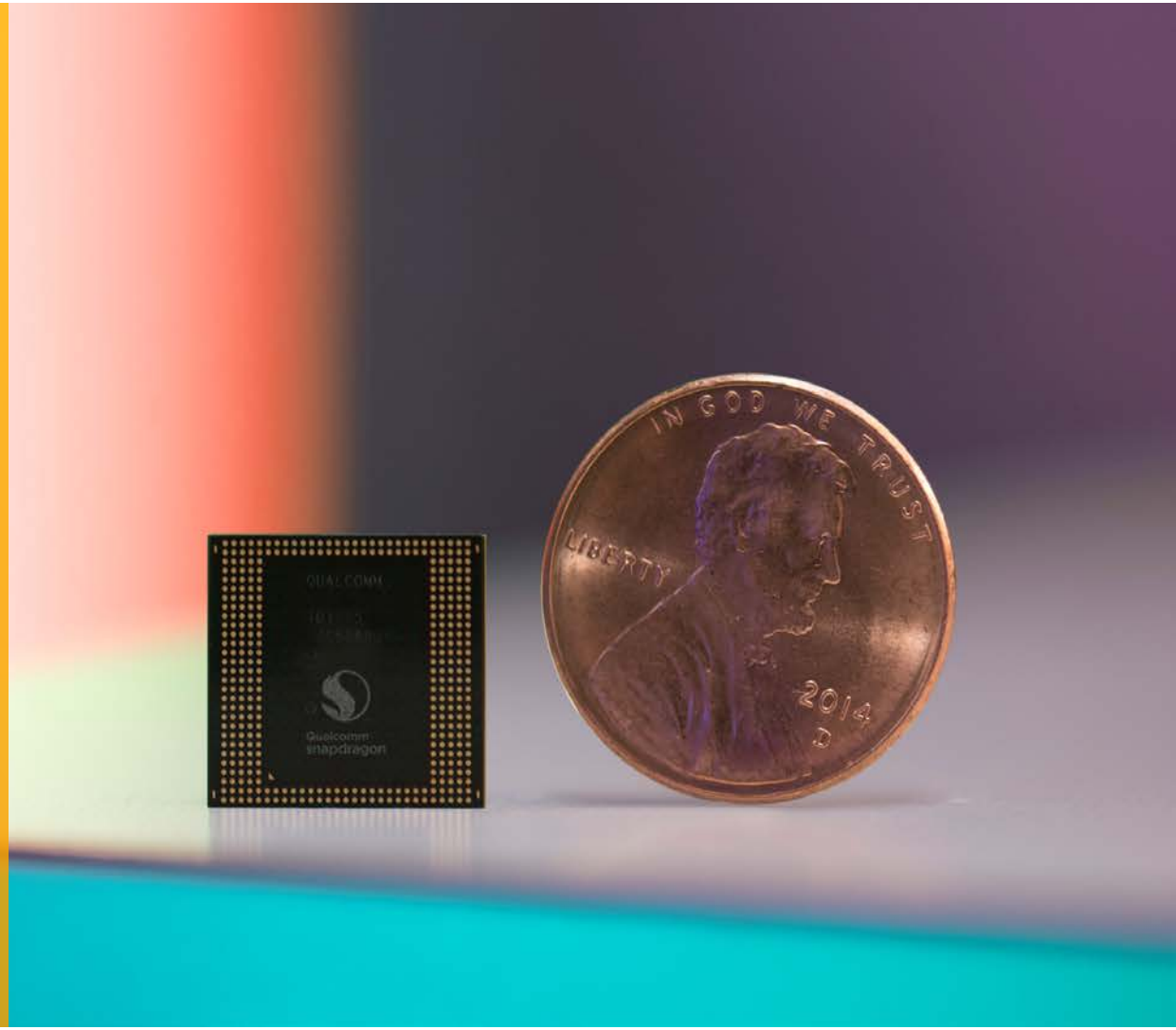
SoC use the latest technology nodes, currently at 10nm and reducing

External NVM is leveraged

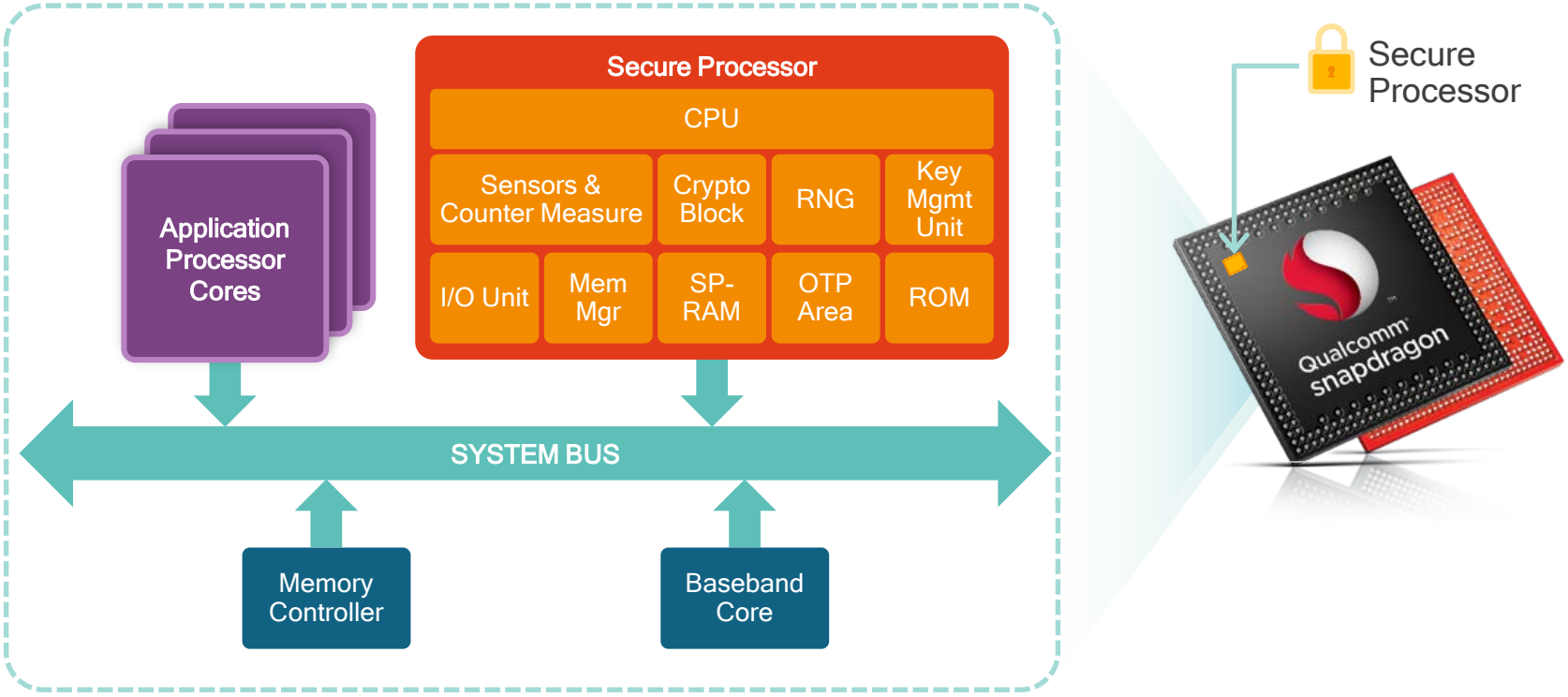
Snapdragon Processor

Qualcomm SOC not to scale

Snapdragon Processor

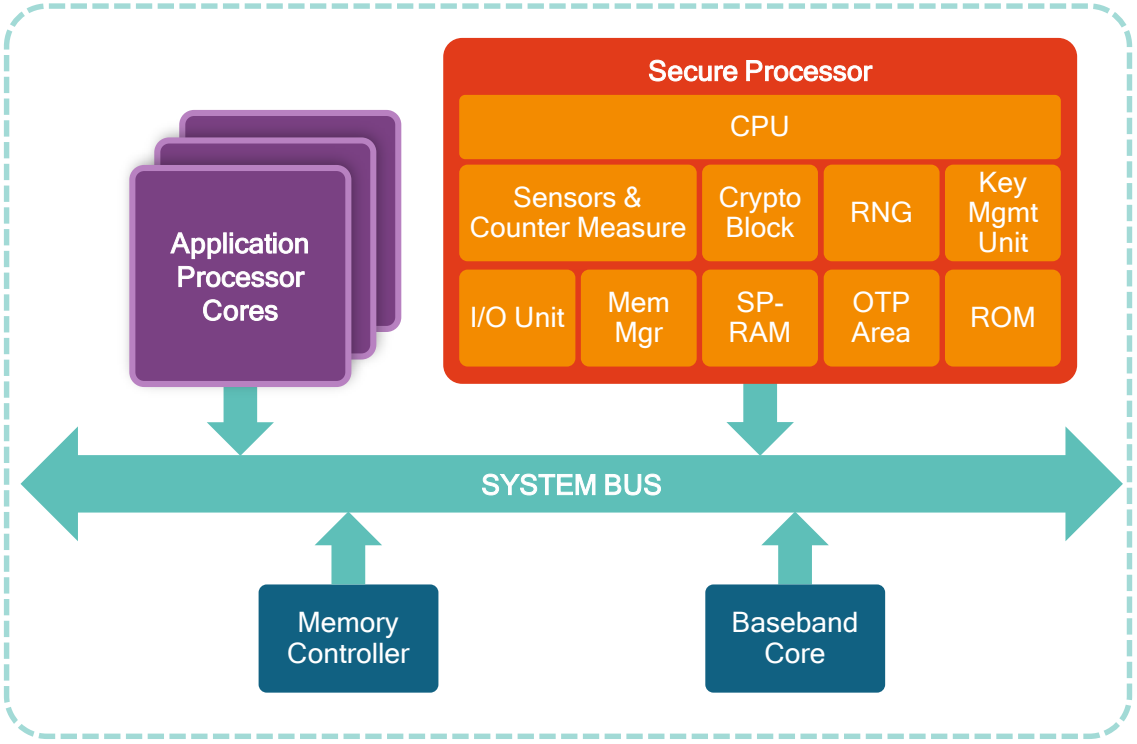


Hardware Architecture



Qualcomm SOC not to scale

Hardware Architecture



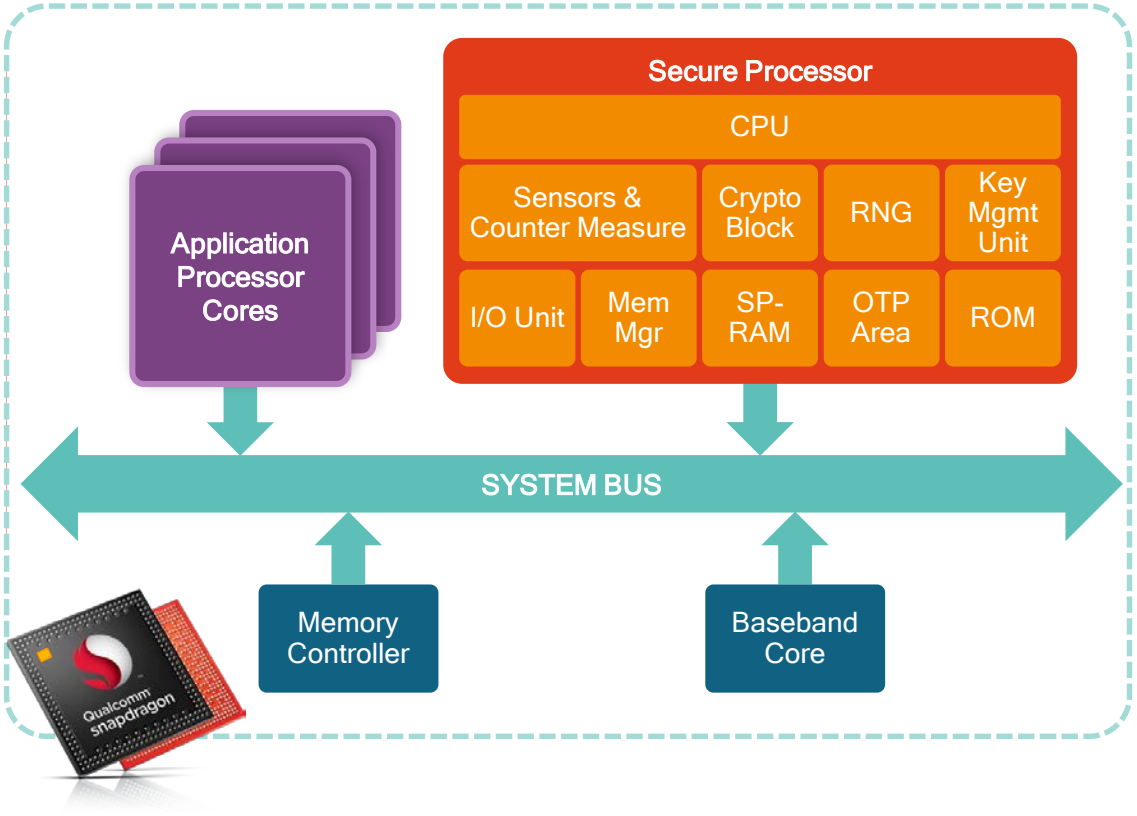
Qualcomm SOC not to scale

The Secure Processor is an isolated core with secure trust boundaries with all other cores

It is not a softSIM or a TEE-based SIM

The Secure Processor is designed to meet the same security criteria as a SIM card: **Common Criteria EAL4+**

Security



Secure Processing Unit

Active and passive security against SCA, FA and invasive attacks

HW accelerated and secure crypto operations (AES, RSA, ECC)

HW Random Number Generator

Random Access Memory (contains the executable code and data)

One Time Programmable (store configuration and per device keys)

Read Only Memory (store the SPU firmware – root of trust)

Security

The **Secure Processing Unit** is equivalent to a discrete smartcard Secure IC except that it does not host Flash memory

Code and Data at rest are stored in the device Flash with a high level of security enforced by SPU:

- **Confidentiality**
  (AES-256 encryption)
- **Authenticity**
  (CMAC-AES-256)
- **Anti-Rollback**
  (version counter handle and stored in SPU)

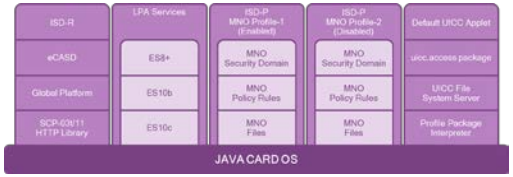
Qualcomm® SPU design is targeting EAL4+ certification according to PP084 (Secure IC Platform)

Certification – example of eSIM

The principles of composite certification can apply as in the case of eSIM

Embedded UICC PP
BSI-CC-PP-0089

A Remote SIM Provisioning PP leverages a JavaCard PP



JavaCard PP
Open Configuration

The JavaCard PP leverages a secure IC PP

Secure IC Platform PP
BSI-CC-PP-0084

The Target of Evaluation is the Secure Processor only

Qualcomm has initiated a certification effort for the Secure Processor with the BSI, targeting EAL4+

11

Standardization efforts & Industry activities

GSMA

Publication of
iUICC POC Group Primary
Platform Requirements

3GPP
A GLOBAL INITIATIVE

Endorsed new ways to store
operator credentials compatible
with integrated SIM

ETSI
World Class Standards

On-going standardization
within ETSI SCP

Beyond the SIM use case – realizing the full potential of a secure processor

Payment

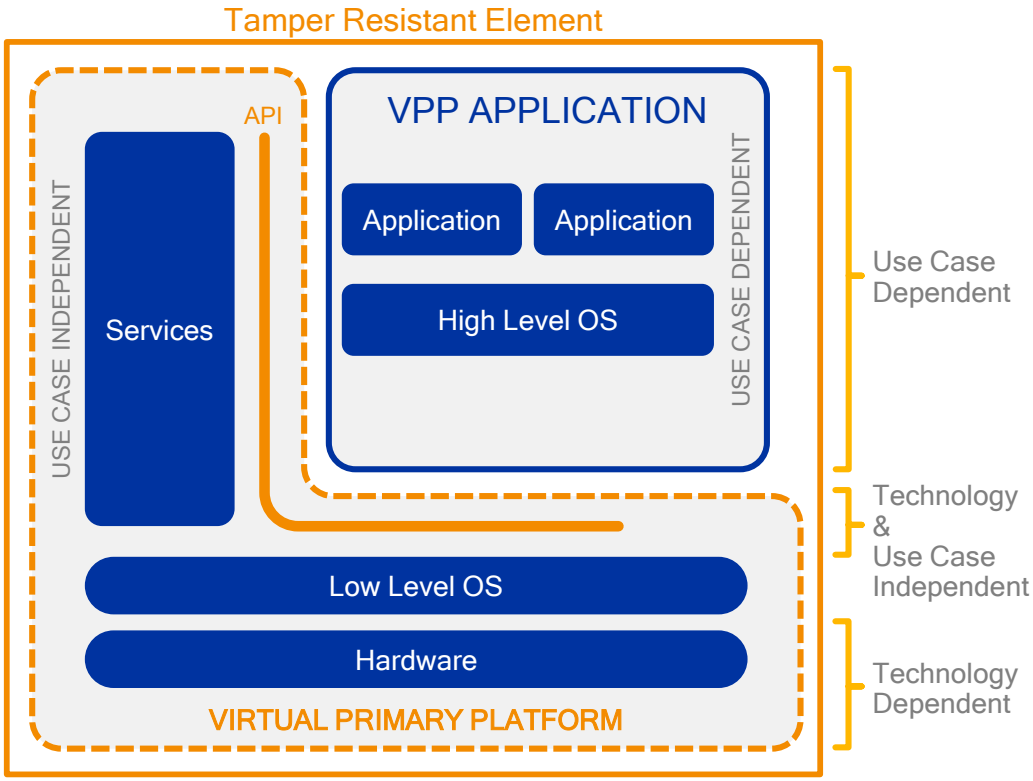
Transit

Secure Identity

Each use case today has his own dedicated solution, with its own ecosystem, standardization and security certification processes.

Enabling multiple use cases

VPP Interfaces Standardized in GlobalPlatform



Qualcomm

Thank you

Follow us on:
For more information, visit us at:
www.qualcomm.com & www.qualcomm.com/blog