JAVA CARD Forum

Webinar series 2021

Secure Element Device Integration

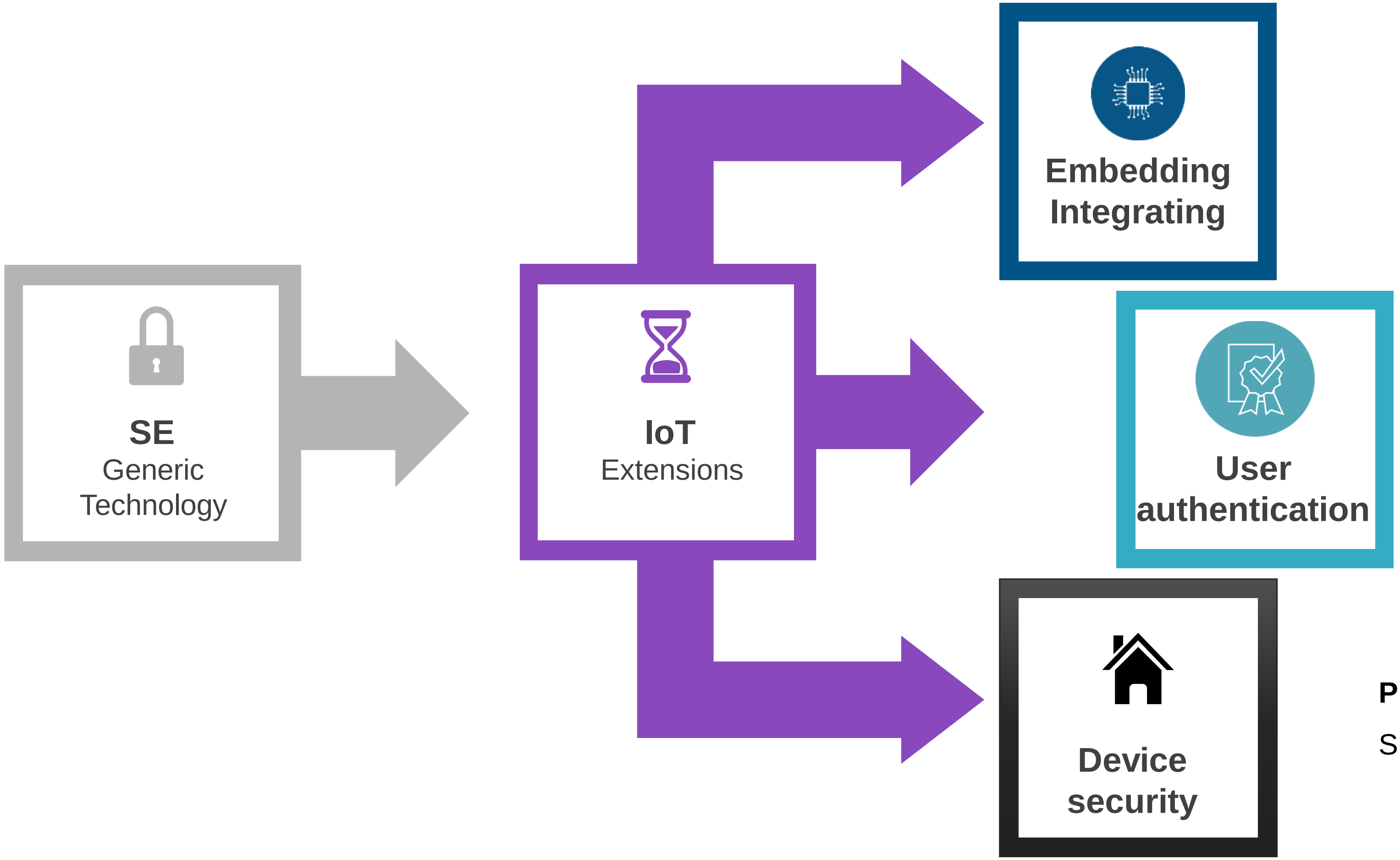
Gil Bernabeu

GlobalPlatform Technical Director

December 2021

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Secure Element (SE) Device Integration: Strategy



Embedded SE (eSE) or integrated SE (iSE)

Extensions are required to connect the SE with the IoT device

User authentication

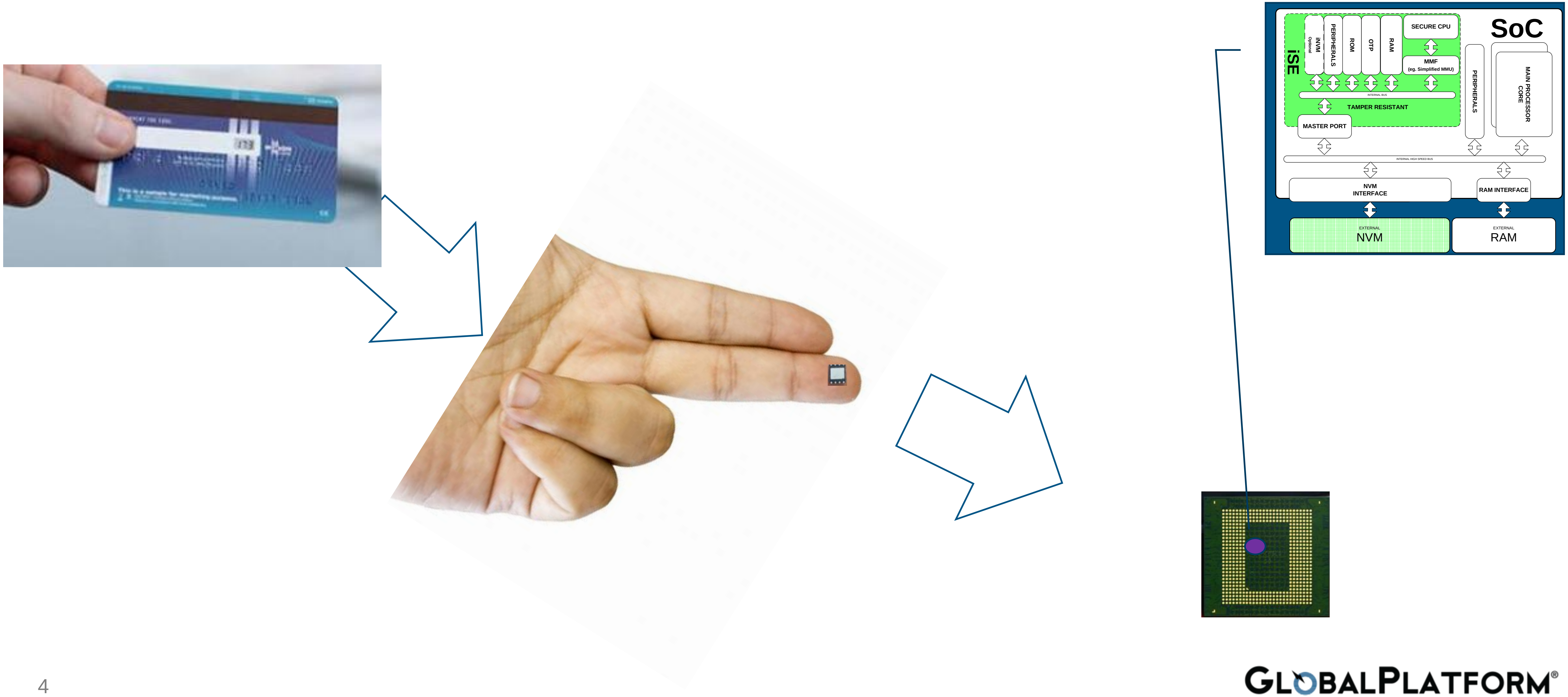
Compliance is key to avoid issues in the field

Provide different levels of security services

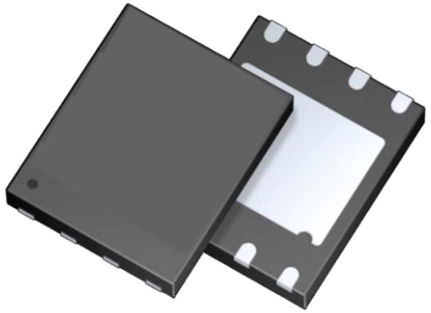
Simplify access to SEs in connected devices

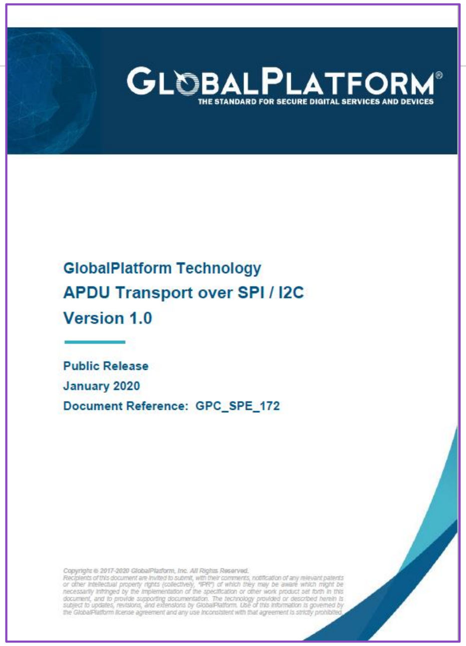
Embedding / Integrating

From Card format to Embedded SE to Integrated SE



Embedded SE





GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
APDU Transport over SPI / I2C
Version 1.0

Public Release
January 2020
Document Reference: GPC_SPE_172

From ISO 7816-3 to I2C and SPI

This specification provides a bridge between APDU command/response standard model of SE and SPI/I2C.

This specification describes how APDUs (as defined in [7816-3]) may be conveyed over these alternative physical interfaces.

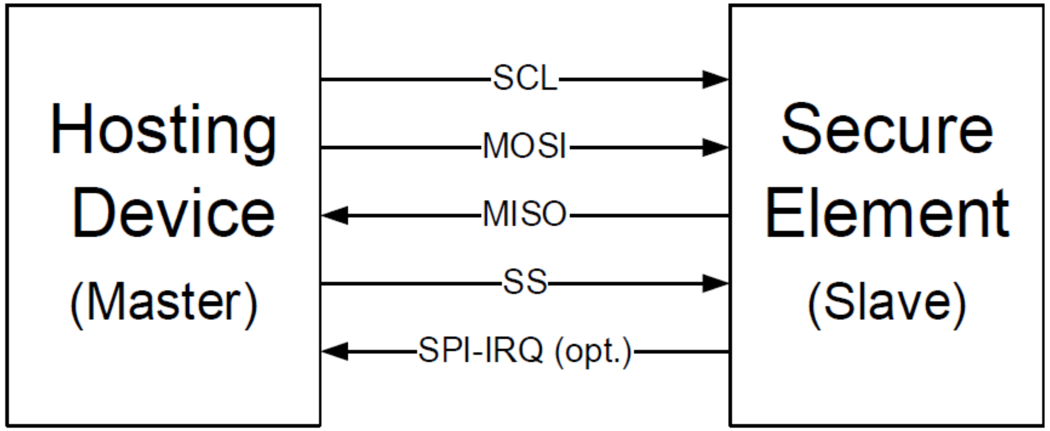
This new protocol allows transferring longer payloads and is meant to adapt to the specific features of the underlying physical interfaces.

As I2C and SPI protocols have high transfer speed and are easy to implement, many devices on IoT only implement I2C or SPI interface without UART interface.

New Link with the Device

SPI

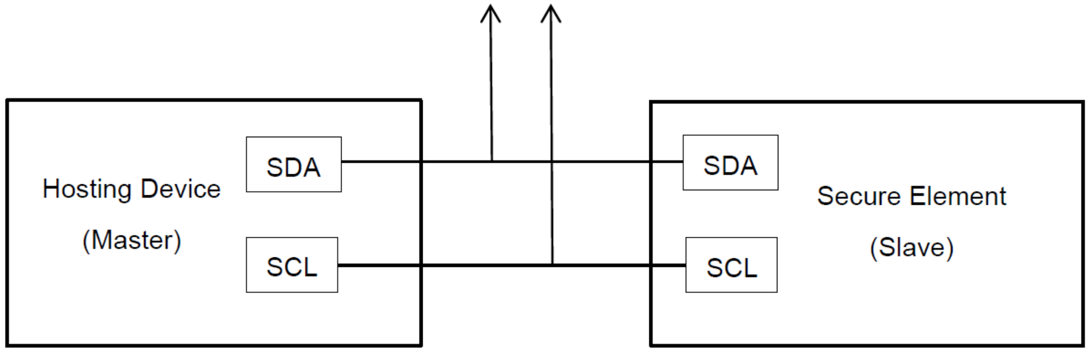
- SCL line: Serial Clock (output from HD)
- MOSI line: Master Out / Slave In (output from HD)
- MISO line: Master In / Slave Out (output from SE)
- SS line: Slave Select (active low, output from HD)



SPI interface is only used for half-duplex communication.

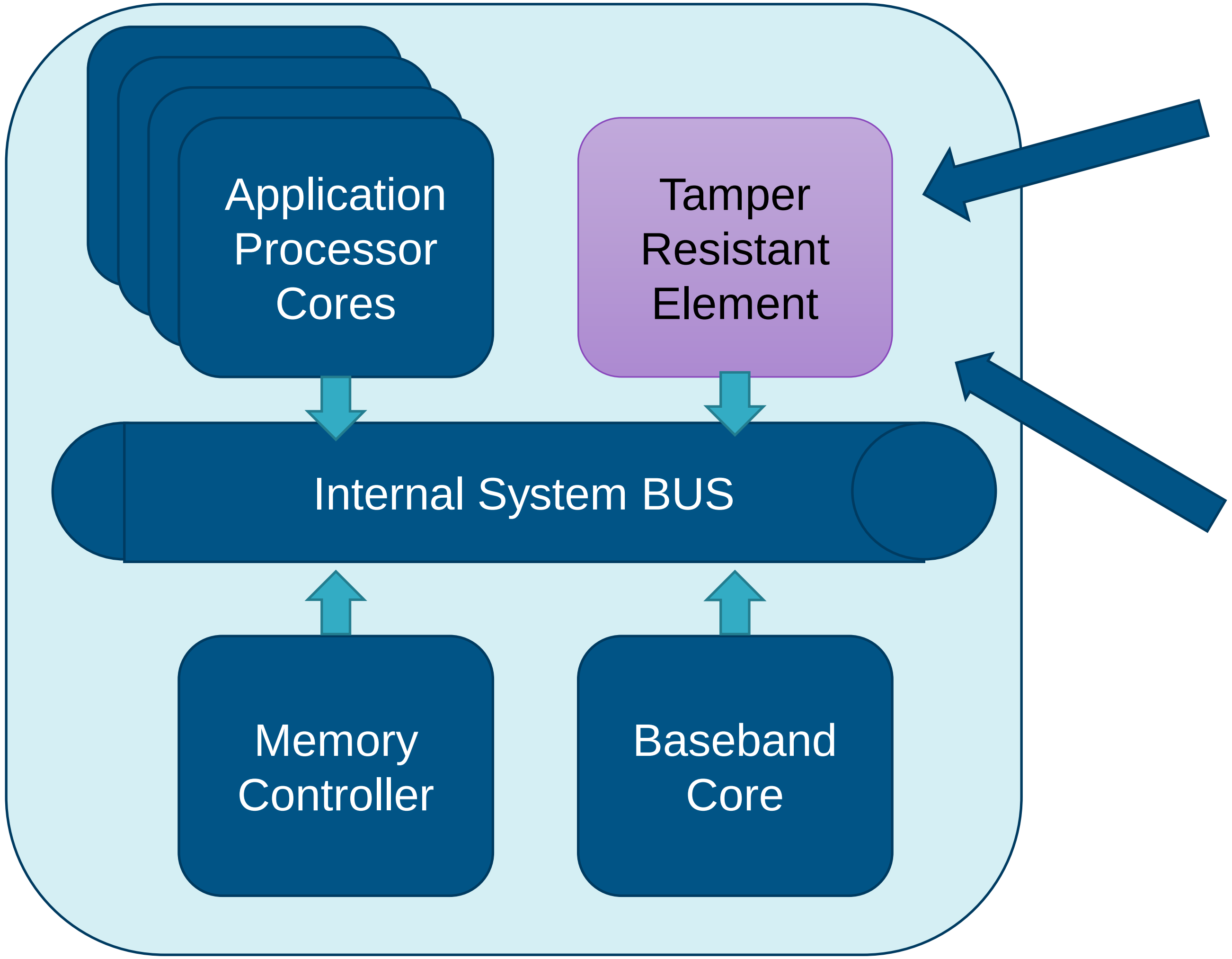
I2C

- Serial Clock Line (SCL)
- Serial Data Line (SDA)



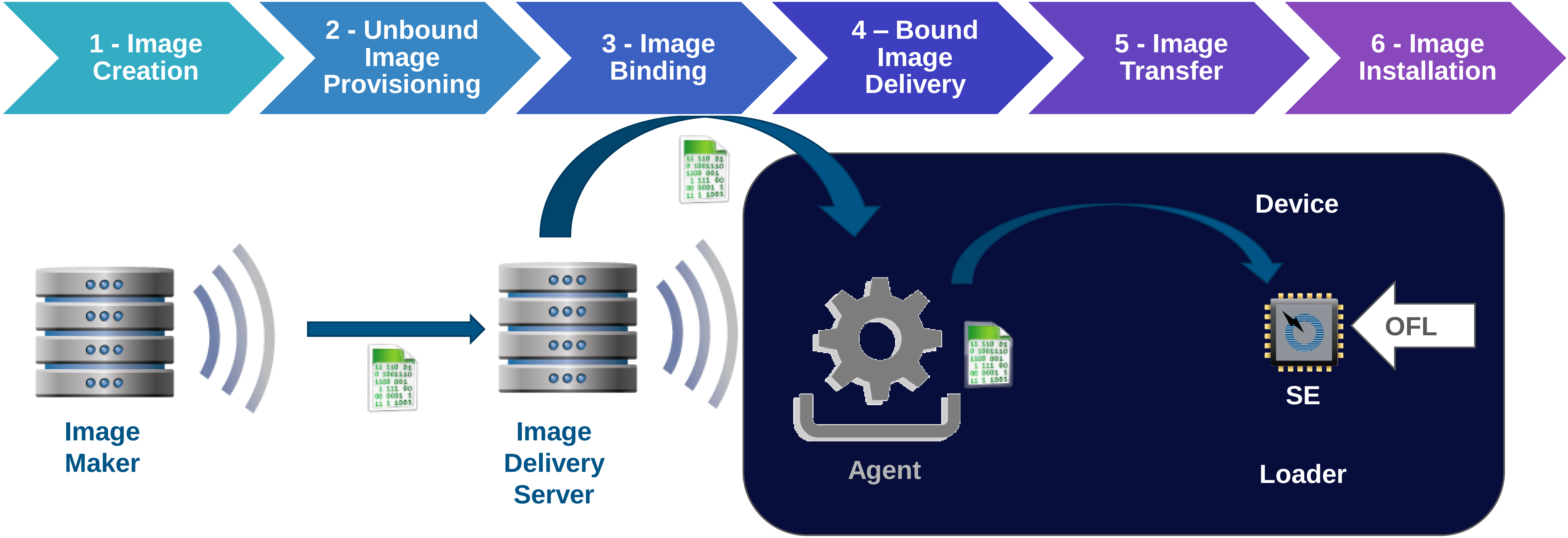
The Hosting Device (HD) acts as master, the Secure Element (SE) acts as the slave

Technologies for Integrated Secure Element



- **Open Firmware Loader** for Tamper Resistant Elements **(OFL)**
  - standardizes how secure element (SE) firmware – combining the secure operating system (OS), applications and data – can be remotely loaded and managed.
- **Virtual Primary Platform (VPP)**
  - defines clear responsibility boundaries between HW and SE firmware, and standardizes the interfaces and the behavior of the Tamper Resistant Element (TRE).

OFL - SE Firmware Management Solution: An Overview



1 - Image Creation

2 - Unbound Image Provisioning

3 - Image Binding

4 – Bound Image Delivery

5 - Image Transfer

6 - Image Installation

Image Maker

Image Delivery Server

Device

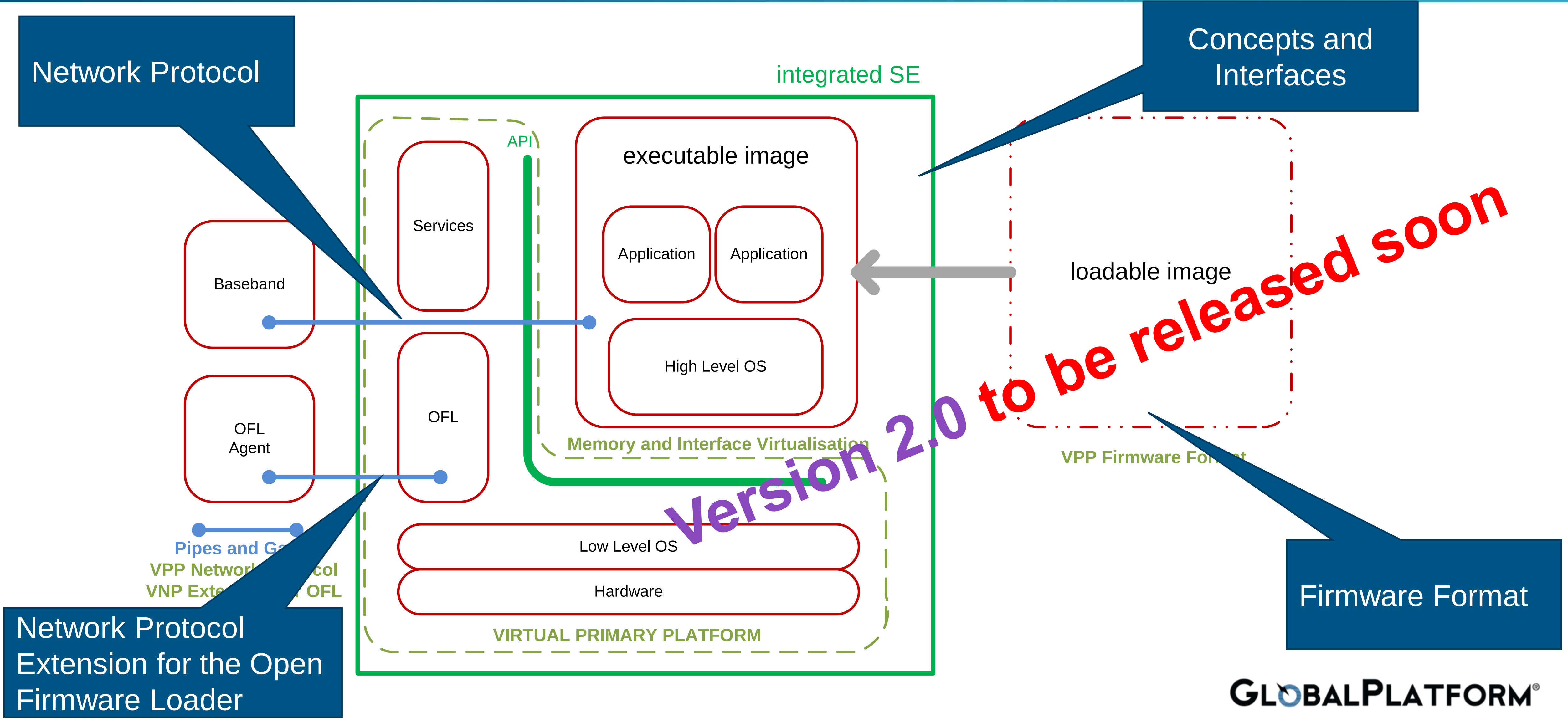
Agent

OFL

SE

Loader

Virtual Primary Platform (VPP) = 4 Documents



Network Protocol

Concepts and Interfaces

Firmware Format

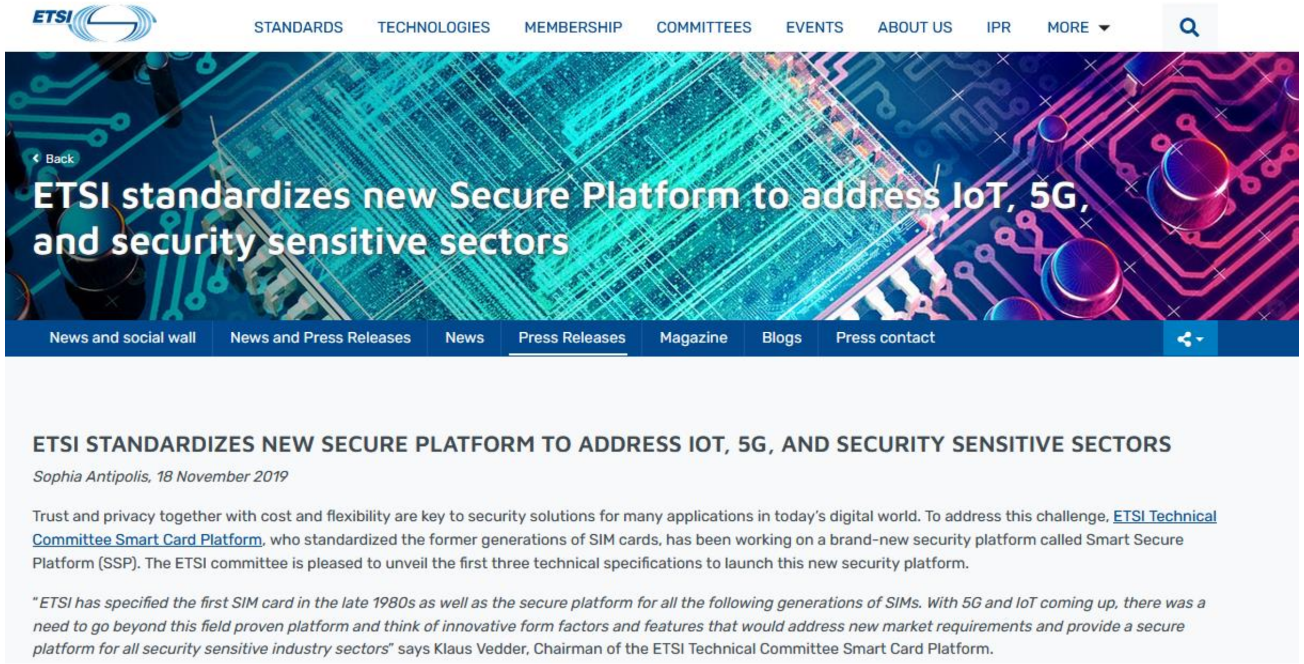
Network Protocol Extension for the Open Firmware Loader

Version 2.0 to be released soon

GLOBALPLATFORM®

Already Integrated in the Next-Gen SIM

GlobalPlatform Open Firmware Loader and Virtual Primary Platform are already referenced in the new ETSI Smart Secure Platform (SSP)



ETSI standardizes new Secure Platform to address IoT, 5G, and security sensitive sectors

ETSI STANDARDIZES NEW SECURE PLATFORM TO ADDRESS IOT, 5G, AND SECURITY SENSITIVE SECTORS

Sophia Antipolis, 18 November 2019

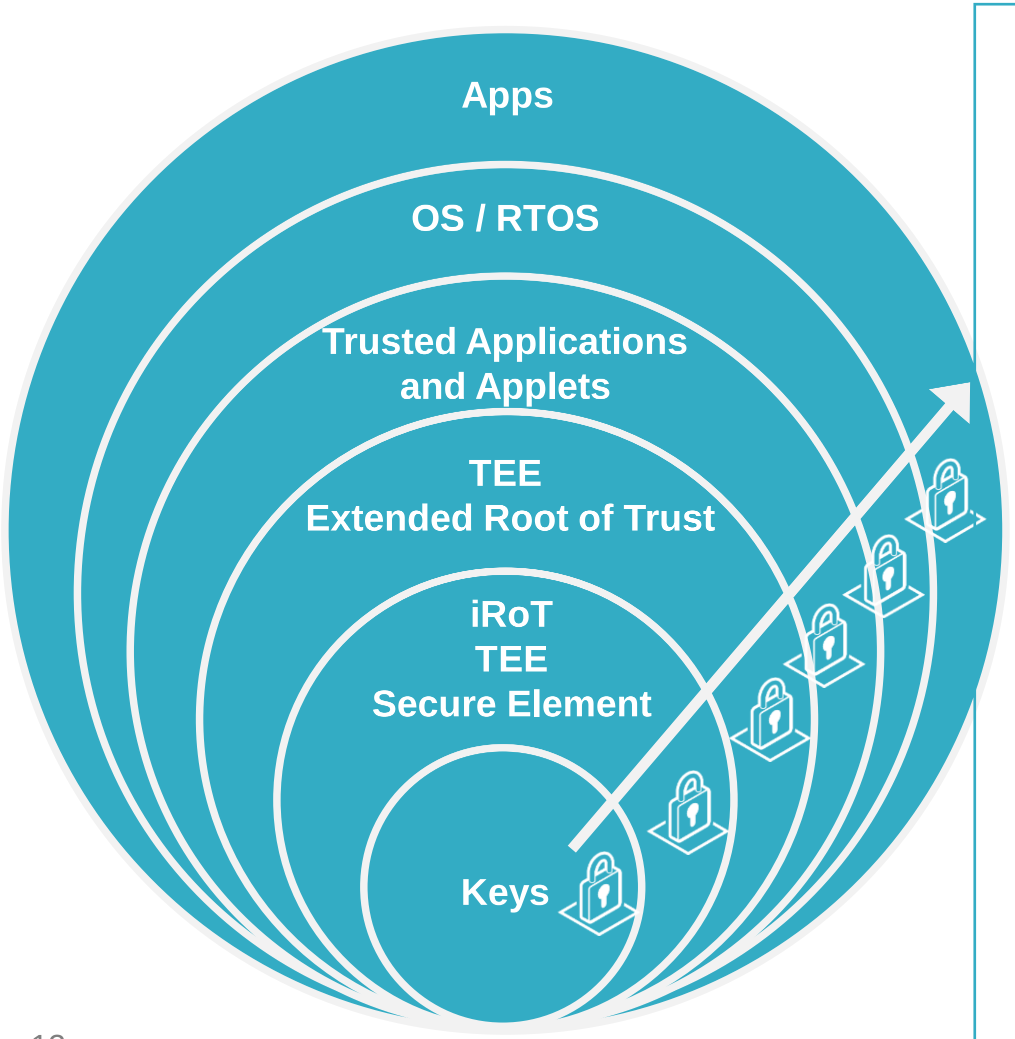
Trust and privacy together with cost and flexibility are key to security solutions for many applications in today's digital world. To address this challenge, ETSI Technical Committee Smart Card Platform, who standardized the former generations of SIM cards, has been working on a brand-new security platform called Smart Secure Platform (SSP). The ETSI committee is pleased to unveil the first three technical specifications to launch this new security platform.

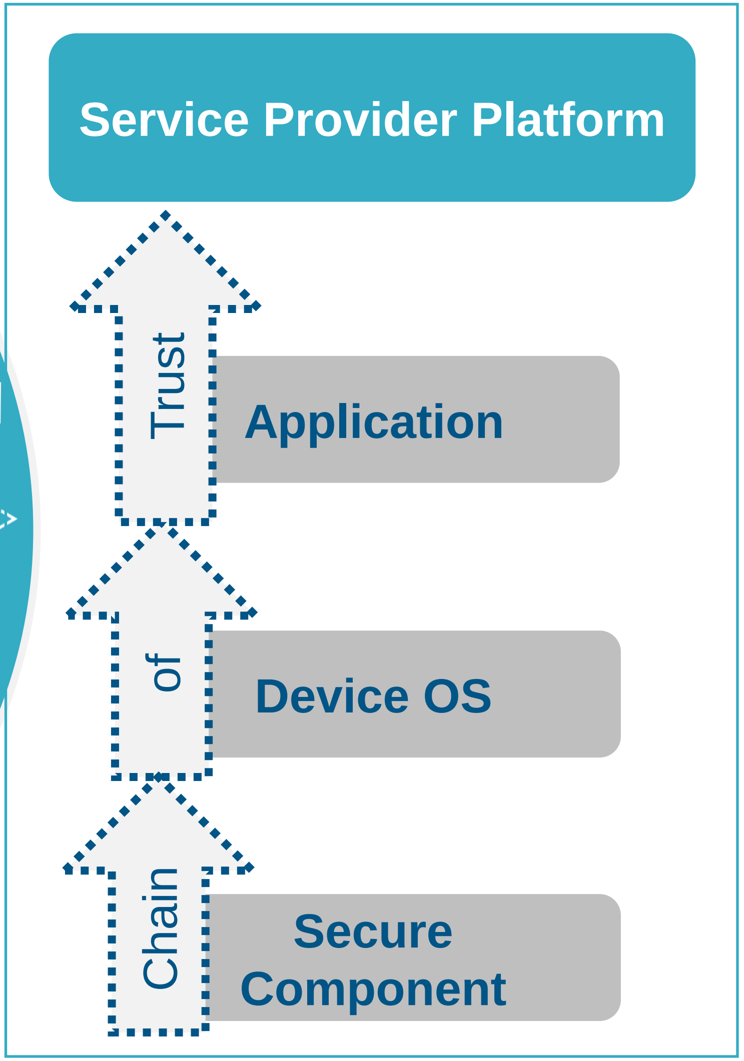
"*ETSI has specified the first SIM card in the late 1980s as well as the secure platform for all the following generations of SIMs. With 5G and IoT coming up, there was a need to go beyond this field proven platform and think of innovative form factors and features that would address new market requirements and provide a secure platform for all security sensitive industry sectors*" says Klaus Vedder, Chairman of the ETSI Technical Committee Smart Card Platform.

The three specifications cover the general technical characteristics of the Smart Secure Platform with ETSI TS 103 666-1, the integration of the Secure Element into a System on Chip (SoC) solution in ETSI TS 103 666-2 and, as the first protocol between the Smart Secure Platform and the outside world, the Serial Peripheral Interface (SPI) which is specified in ETSI TS 103 713.

Device Integration

Device Trust Hierarchy





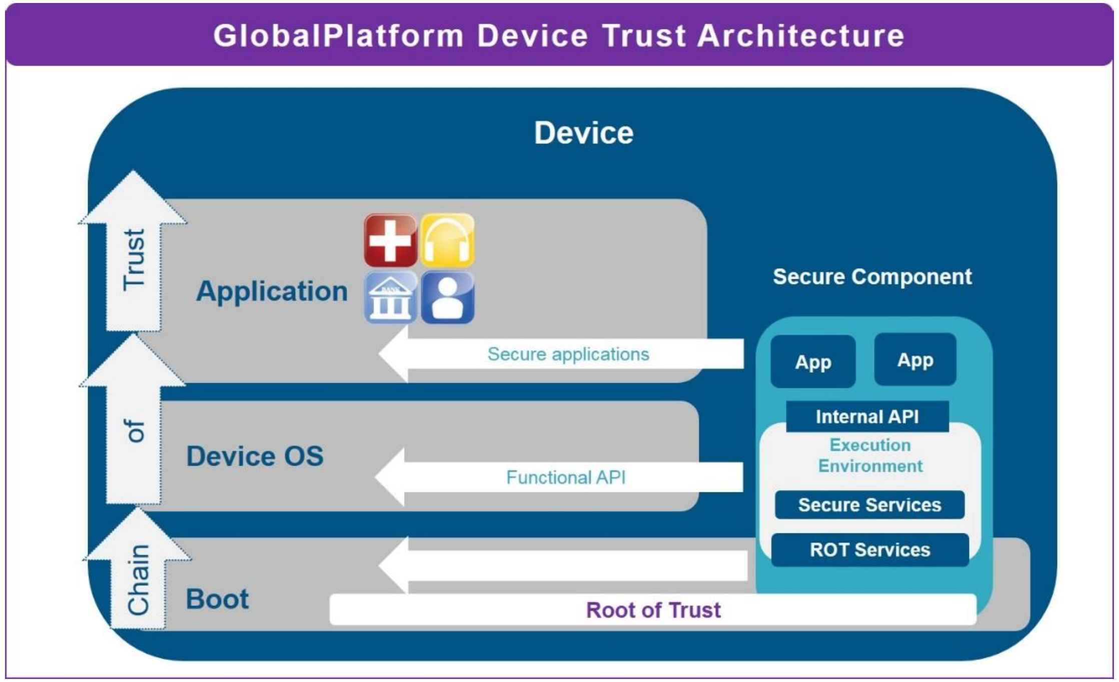
Root of Trust technology within devices enables 'Chains of Trust' to be built. These chains allow device manufacturers and service providers to offer secure digital services while ensuring device integrity and security, alongside end-user privacy.

GlobalPlatform Device Trust Architecture
A Security Framework

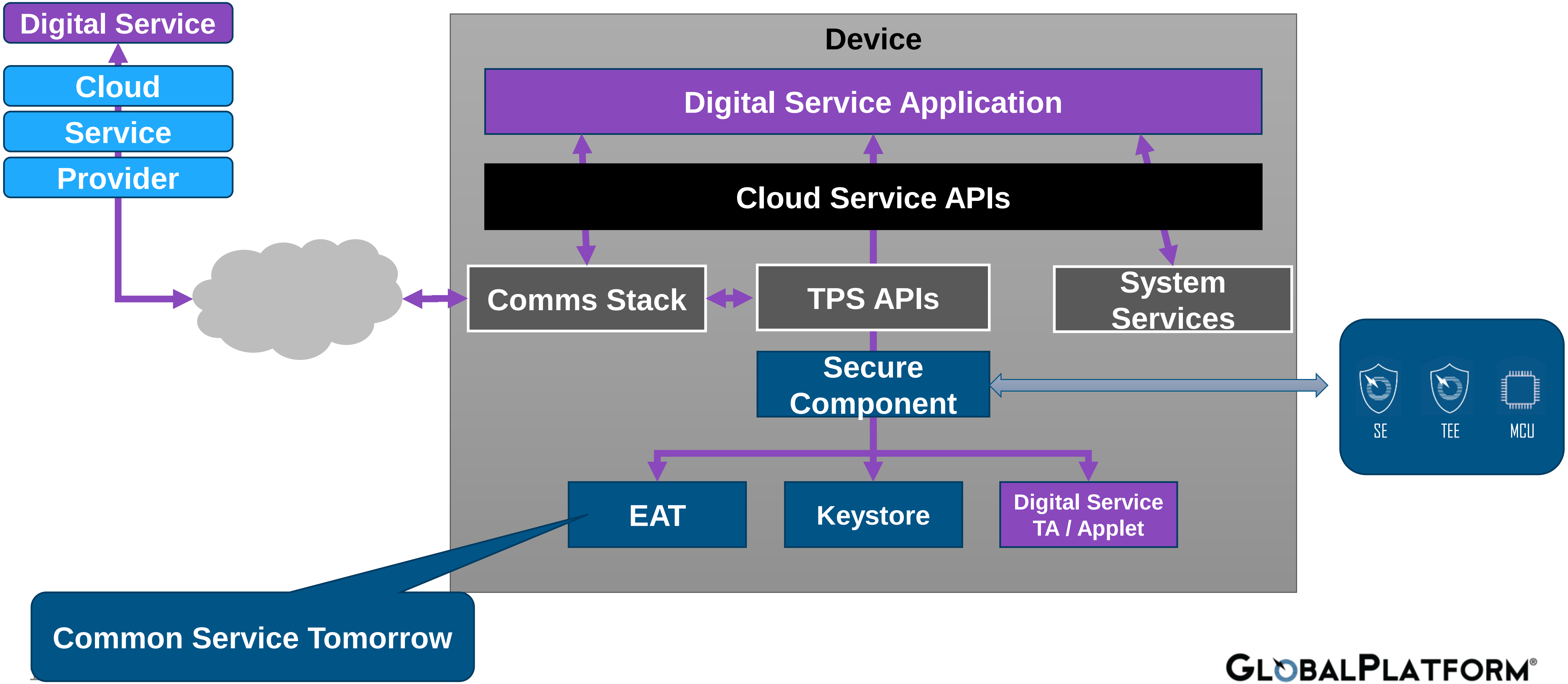
- GlobalPlatform promotes a framework to create trustworthy devices based on secure components.

- It shows how GlobalPlatform's standardized secure component technology can be used to build a Chain of Trust which protects both devices and digital services.

- It does this by offering secure services, originating within the secure component's Root of Trust, which can be used at each level of a Chain of Trust:
  - the boot mechanism
  - the device operating system (OS)
  - the application layer
  - the attestation services



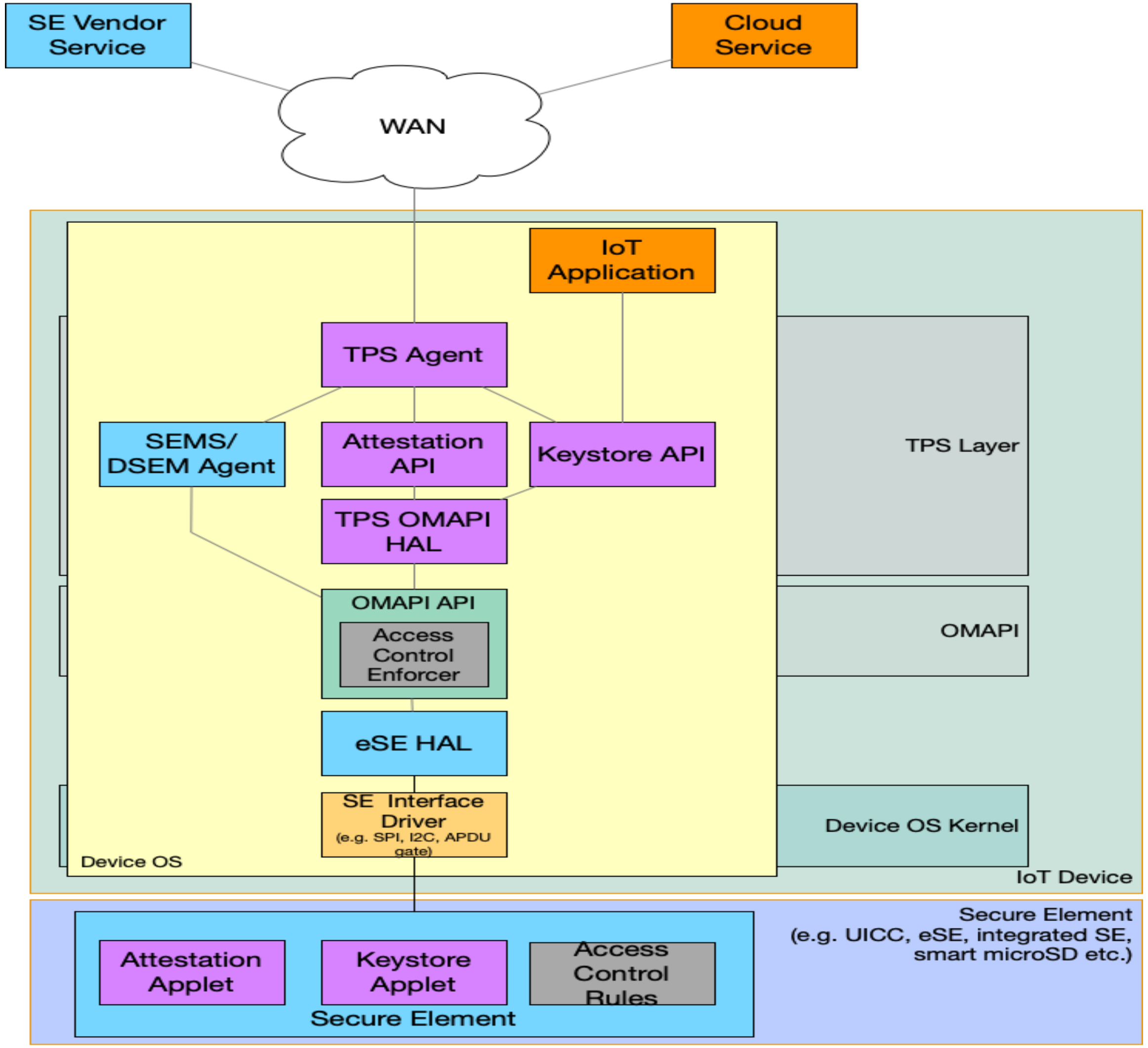
Securing a Digital Service with Trusted Platform Services (TPS)



GLOBALPLATFORM®

TPS Services on Secure Elements

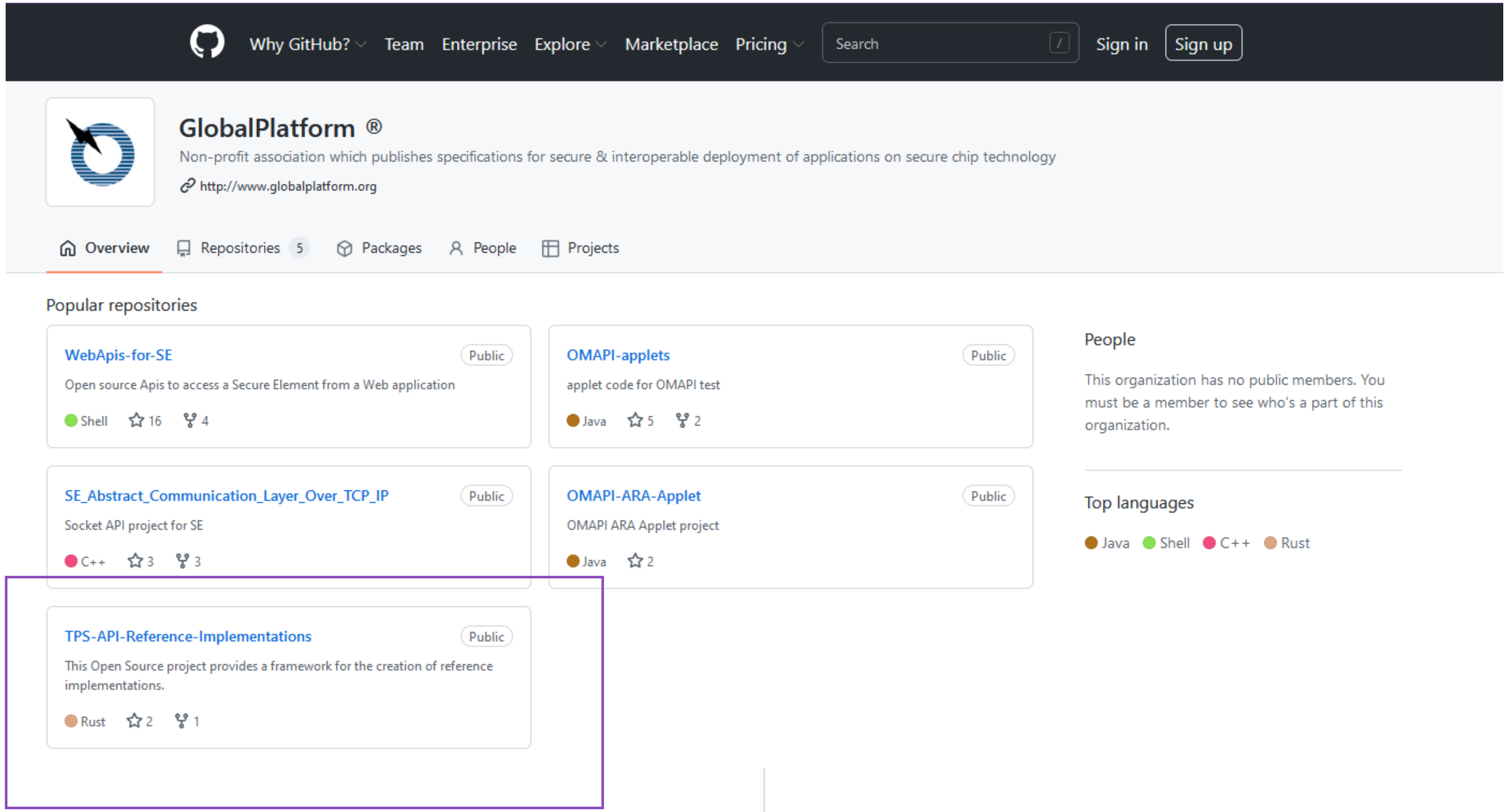
- Secure Element has multiple options for applet distribution / update
  - Pre-installed in SE on delivery
  - “Push” install using one of the SCP from a TSM
  - “Pull” install using SEMS / DSEM supports multiple distribution options (pull from SE vendor, pull from cloud, distribute with app updates…)
- OMAPI API provides standard mechanism for apps to communicate with SE
  - Manages logical connections with multiple clients
  - Provides some isolation so that only authorized device apps can communicate to applets
- GlobalPlatform will define standard interfaces for SE applets implementing TPS services
  - Making solutions vendor agnostic – app developer only needs to know TPS API.



Soon to be Available as Open Source

Starting on GitHub

- https://github.com/GlobalPlatform/
- MIT license
- Based on CBOR, COSE and CDDL



GlobalPlatform ®

Non-profit association which publishes specifications for secure & interoperable deployment of applications on secure chip technology

http://www.globalplatform.org

Popular repositories

WebApis-for-SE (Public)
Open source Apis to access a Secure Element from a Web application
Shell ☆ 16 4

OMAPI-applets (Public)
applet code for OMAPI test
Java ☆ 5 2

SE_Abstract_Communication_Layer_Over_TCP_IP (Public)
Socket API project for SE
C++ ☆ 3 3

OMAPI-ARA-Applet (Public)
OMAPI ARA Applet project
Java ☆ 2

TPS-API-Reference-Implementations (Public)
This Open Source project provides a framework for the creation of reference implementations.
Rust ☆ 2 1

People

This organization has no public members. You must be a member to see who's a part of this organization.

Top languages

● Java ● Shell ● C++ ● Rust

The first uploads are:

rs_minicbor: a no_std implementation of CBOR in safe rust

rs_cddl: an early preview of CDDL tooling. Quite a bit of work needed to get to code generation, but parsing is complete.

Trend One – Embedded Hardware Security

35% of smartphones sold globally in H1 2020 had embedded hardware security.* This is expected to increase to over 50% by 2025.**

NFC eSEs are generally used for payment, couponing, transport, access control, ticketing…

NFC embedded Secure Element shipments are expected to reach [473 million units] among mobile devices by 2024.

[* https://www.counterpointresearch.com/embedded-hardware-security-smartphones-h1-2020/]

** [https://www.counterpointresearch.com/podcast-50-percent-smartphones-embedded-hardware-security-2025/]

Trend Two – Biometric Authentication

In 2019 only 27% of consumers used biometrics to authenticate…

By 2024, Mercator forecasts that 66% of smartphone owners will use biometrics for authentication.

By 2020, 41% of phones were being unlocked with biometrics…

SOURCE: https://www.thefacerecognitioncompany.com/news/the-future-of-face-recognition-technology

What Needs to be Solved - High level

Service provider

- Risk management
- The quality of the authenticator

Device

- More and more devices with different architecture
- Different types of biometrics

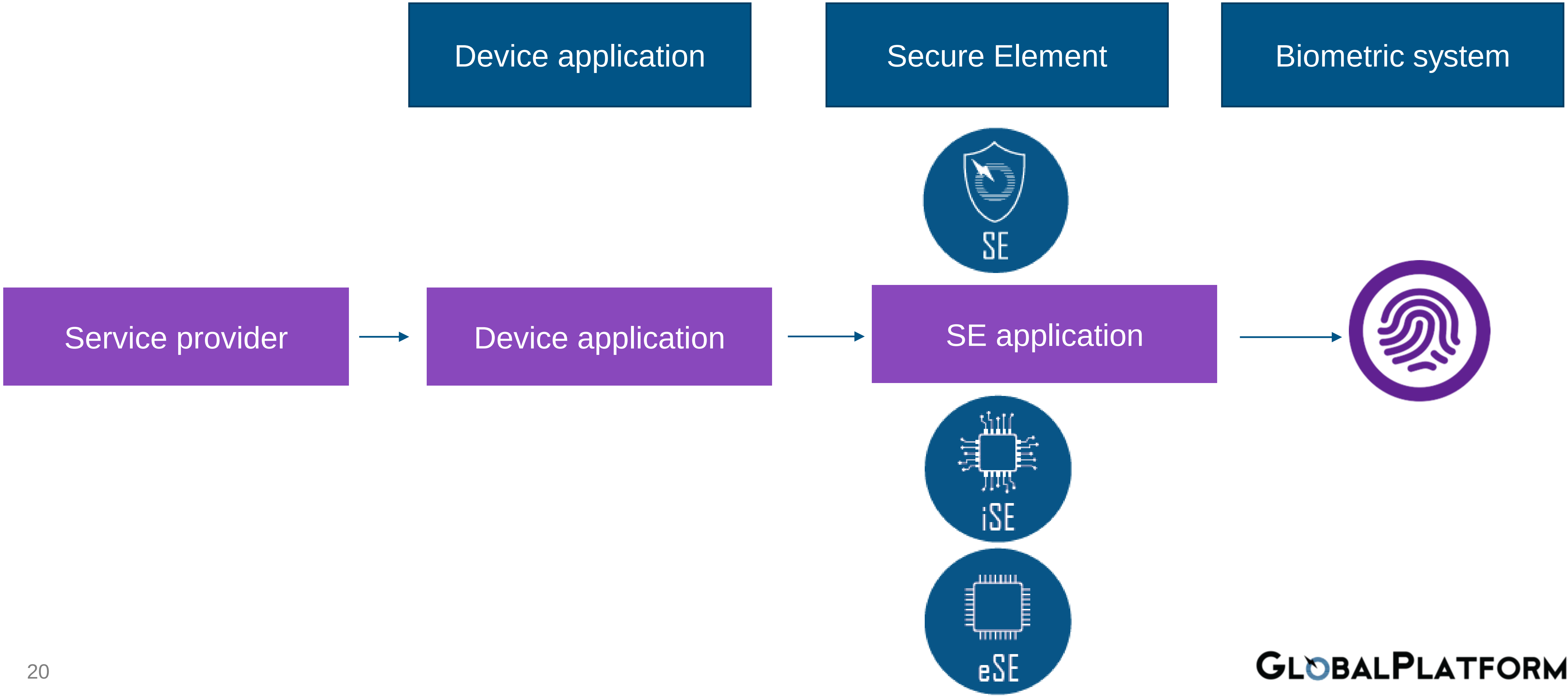
Sensor

- More and more devices with different architecture
- Different types of biometrics

End user

- Frictionless transaction
- Similar experience across-devices

What Needs to be Solved - Technical Level



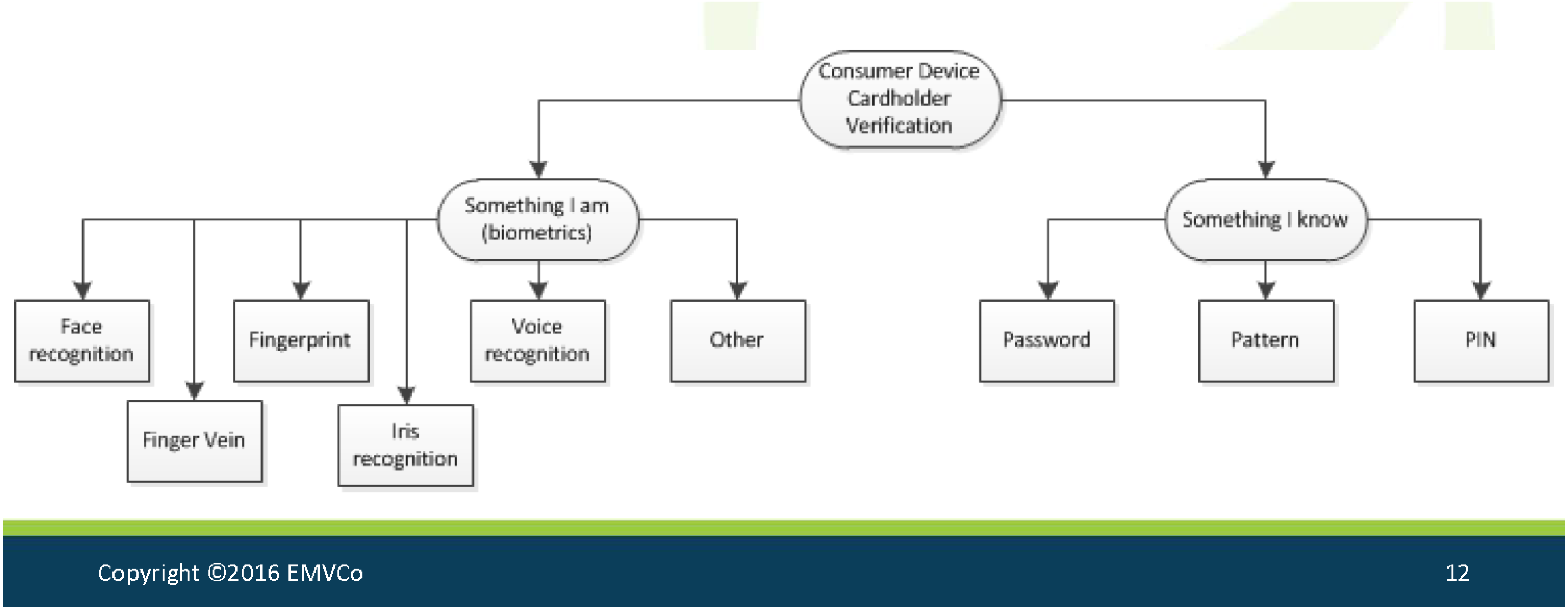
Device application

Secure Element

Biometric system

Service provider → Device application → SE application →

Cardholder Verification
The EMVCo View

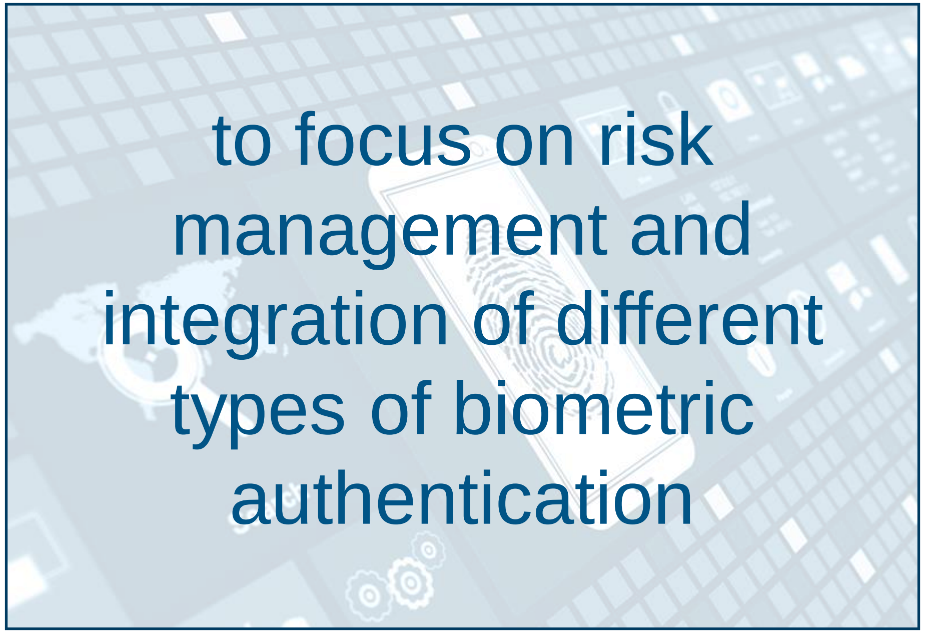


Copyright ©2016 EMVCo 12

CDCVM = Consumer Device Cardholder Verification Method

We Need a Solution That Allows

The service provider



to focus on risk management and integration of different types of biometric authentication

The device manufacturer

to focus on performances and integration of biometric authentication within the Secure Element

GlobalPlatform Broker Interface

- Payment applications located in the embedded SE of the smartphone require biometric Cardholder Verification.

- To simplify applet design, it is useful to centralize the management of Cardholder Verification methods offered by the device and provide a standardized interface to such information.

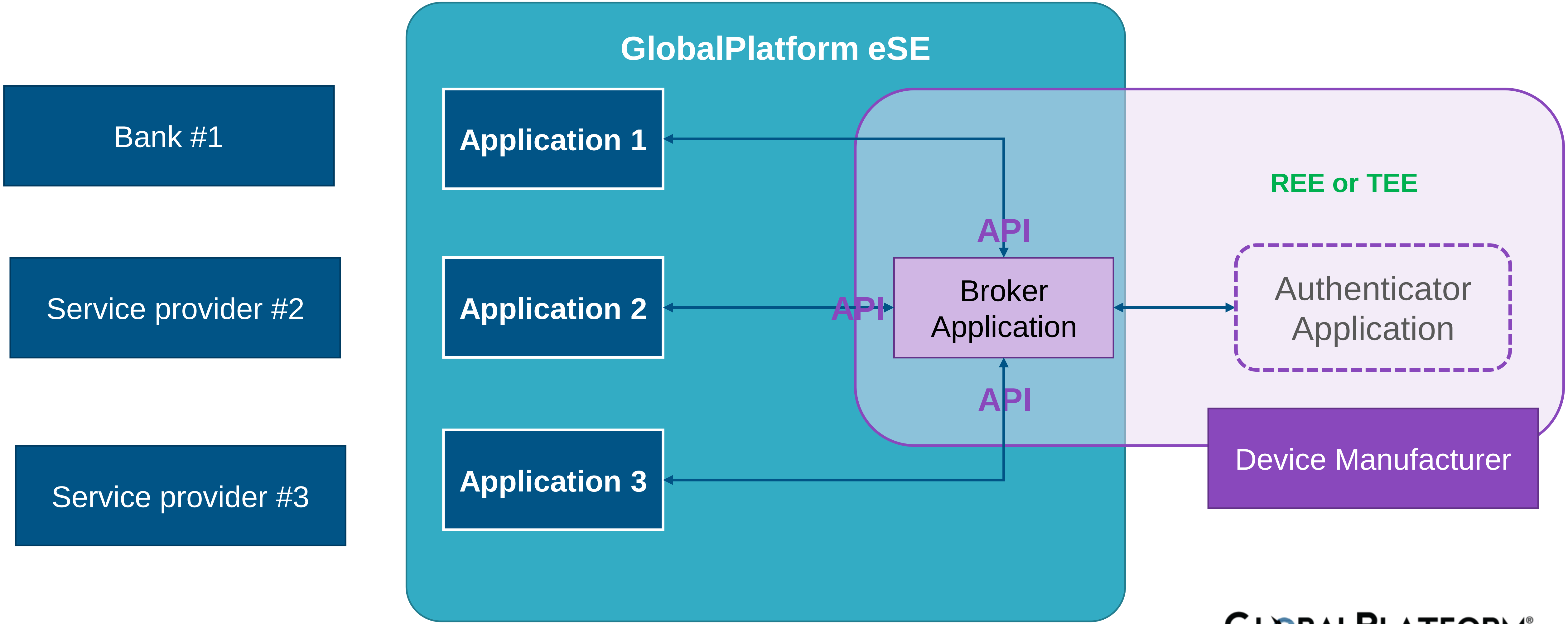
- This central application is the Broker Application, providing a Broker Interface to other applications.

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

GlobalPlatform Technology
Amendment J Broker Interface
Card Specification v2.3 – Amendment J
Version 1.0

Public Release
July 2020
Document Reference: GPC_SPE_157

Broker Application and Broker API



Contact Us

Membership:

membership@globalplatform.org

PR Contact:

globalplatform@iseepr.co.uk
Tel: +44 (0) 113 350 1922

Questions:

secretariat@globalplatform.org

Twitter
@GlobalPlatform_

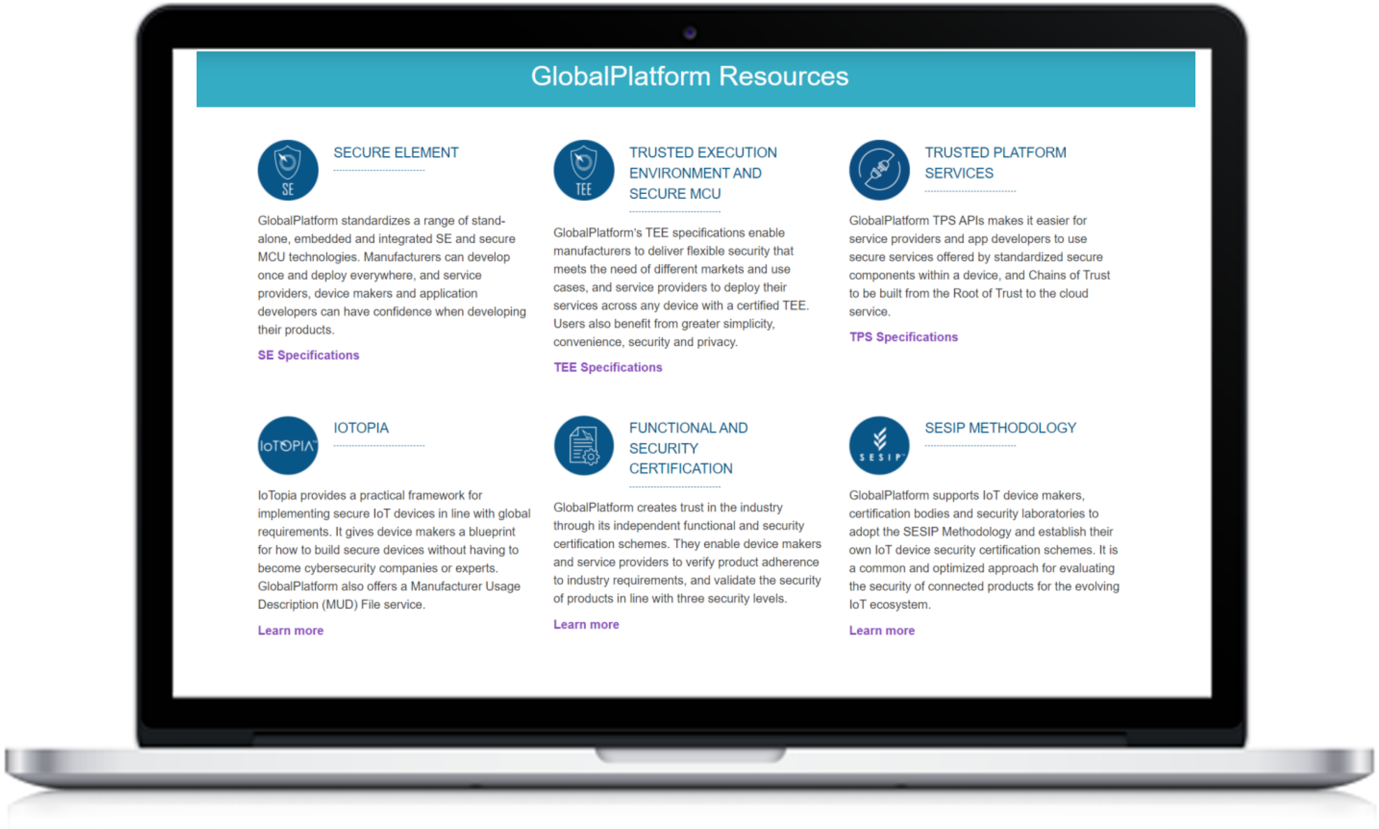
YouTube
GlobalPlatformTV

LinkedIn
GlobalPlatform

WeChat
GlobalPlatform China

YouKu
GlobalPlatform

GitHub
GlobalPlatform.GitHub.com



GlobalPlatform Resources

SECURE ELEMENT

GlobalPlatform standardizes a range of stand-alone, embedded and integrated SE and secure MCU technologies. Manufacturers can develop once and deploy everywhere, and service providers, device makers and application developers can have confidence when developing their products.

SE Specifications

TRUSTED EXECUTION ENVIRONMENT AND SECURE MCU

GlobalPlatform's TEE specifications enable manufacturers to deliver flexible security that meets the need of different markets and use cases, and service providers to deploy their services across any device with a certified TEE. Users also benefit from greater simplicity, convenience, security and privacy.

TEE Specifications

TRUSTED PLATFORM SERVICES

GlobalPlatform TPS APIs makes it easier for service providers and app developers to use secure services offered by standardized secure components within a device, and Chains of Trust to be built from the Root of Trust to the cloud service.

TPS Specifications

IOTOPIA

IoTopia provides a practical framework for implementing secure IoT devices in line with global requirements. It gives device makers a blueprint for how to build secure devices without having to become cybersecurity companies or experts. GlobalPlatform also offers a Manufacturer Usage Description (MUD) File service.

Learn more

FUNCTIONAL AND SECURITY CERTIFICATION

GlobalPlatform creates trust in the industry through its independent functional and security certification schemes. They enable device makers and service providers to verify product adherence to industry requirements, and validate the security of products in line with three security levels.

Learn more

SESIP METHODOLOGY

GlobalPlatform supports IoT device makers, certification bodies and security laboratories to adopt the SESIP Methodology and establish their own IoT device security certification schemes. It is a common and optimized approach for evaluating the security of connected products for the evolving IoT ecosystem.

Learn more

www.globalplatform.org

GLOBALPLATFORM®

Thank you!