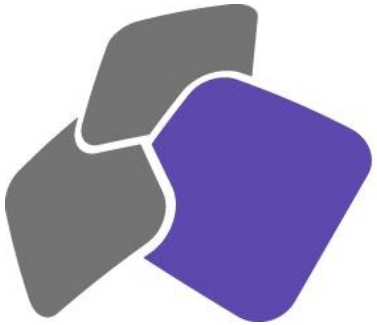


JAVA CARD Forum

Webinar series 2021

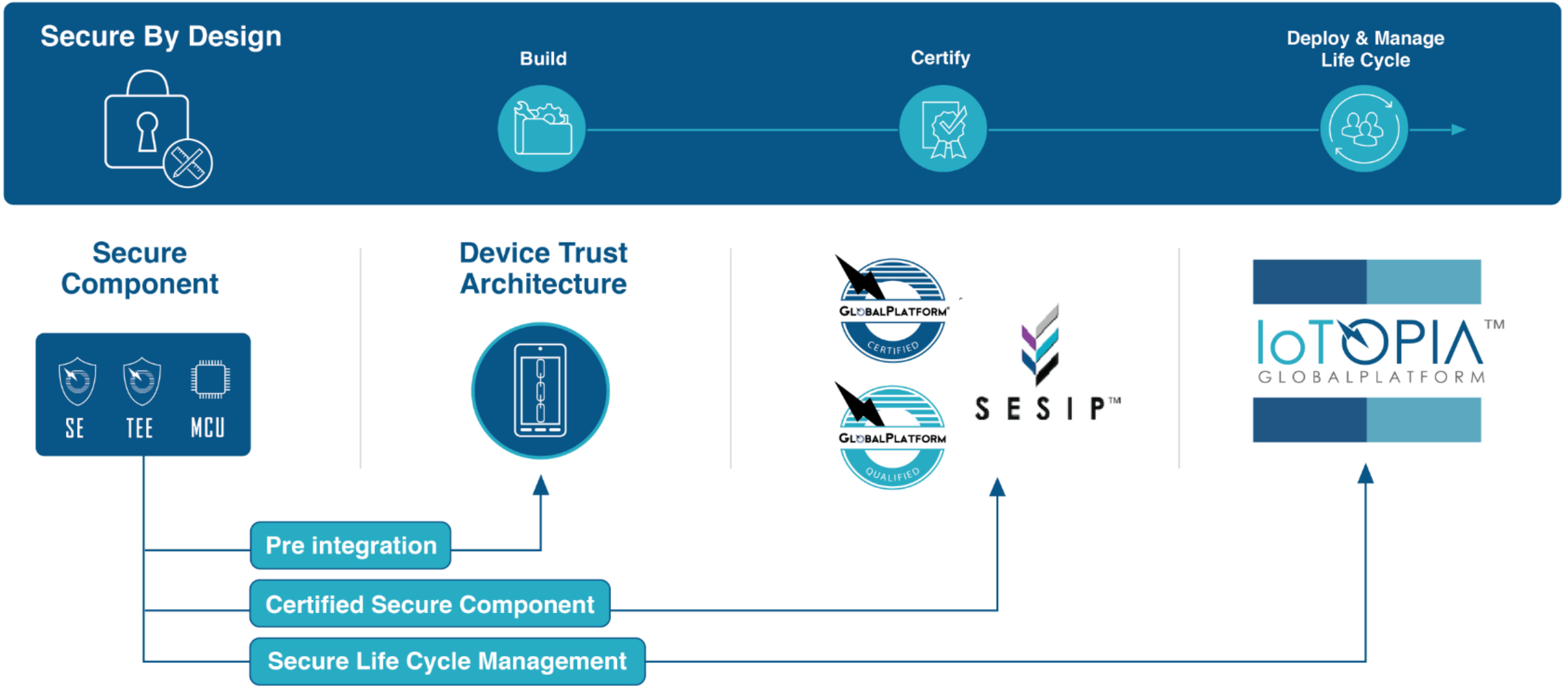
GlobalPlatform Secure Element Protection Profile and FIDO 2.0 Extension

Gil Bernabeu

December 2021

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Helping Device Manufacturers to Reach Market Requirements in Security & Privacy



GLOBALPLATFORM®

The state-of-play Today
Different Uses Cases, Risks, Security Levels & Certification

Payment

EMVCo

Payment Card / SE

ID

CC / FIDO L3+

ID / SE

Industrial

CC (>= EAL4+)

Meter Gateway

IEC 62443 (SL4)

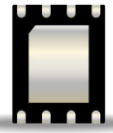
PLC

Consumer

Telco

GSMA

eSIM



PCI

PoS

EMVCo

Mobile

CC / FIDO L3

ID / TEE

CC (EAL3)

Smart Meter

IEC 62443 (SL3)

PLC

IEC 62443 (SL1 / 2)

PLC

RED directive

Child Devices

PLC : Programmable Logic Controller

GlobalPlatform's Answer

Payment ID/telco Industrial Consumer

EMVCo
Payment Card / SE

CC / FIDO L3+ / GSMA
ID / SE

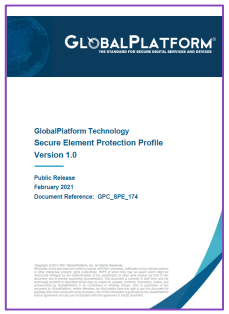
CC (>= EAL4+)
Meter Gateway

IEC 62443 (SL4)
PLC

VAN 5

VAN 4

SE PP



PCI
PoS

CC / FIDO L3
ID / TEE
TEE

CC (EAL3)
Smart Meter

IEC 62443 (SL3)
PLC

IEC 62443 (SL1 / 2)
PLC

VAN 3

TEE PP

MCU PP

RED directive
Child Devices

VAN 2

VAN 1

PLC : Programmable Logic Controller

GLOBALPLATFORM®

GlobalPlatform Secure Element PP

Payment ID/telco Industrial Consumer

EMVCo
Payment Card / SE

CC / FIDO L3+ / GSMA
ID / SE

CC (>= EAL4+)
Meter Gateway

IEC 62443 (SL4)
PLC

VAN 5

VAN 4

PCI
PoS

CC / FIDO L3
ID / TEE
TEE

CC (EAL3)
Smart Meter

IEC 62443 (SL3)
PLC

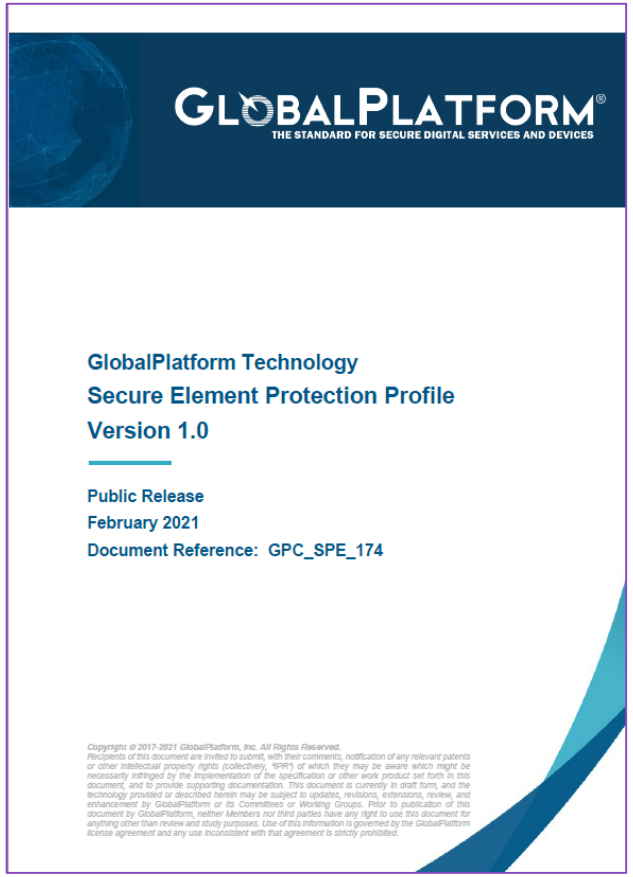
VAN 3

IEC 62443 (SL1 / 2)
PLC

RED directive
Child Devices

VAN 2

VAN 1



https://www.commoncriteriaportal.org/files/ppfiles/CCN-CC-PP-5-2021.pdf

GLOBALPLATFORM®

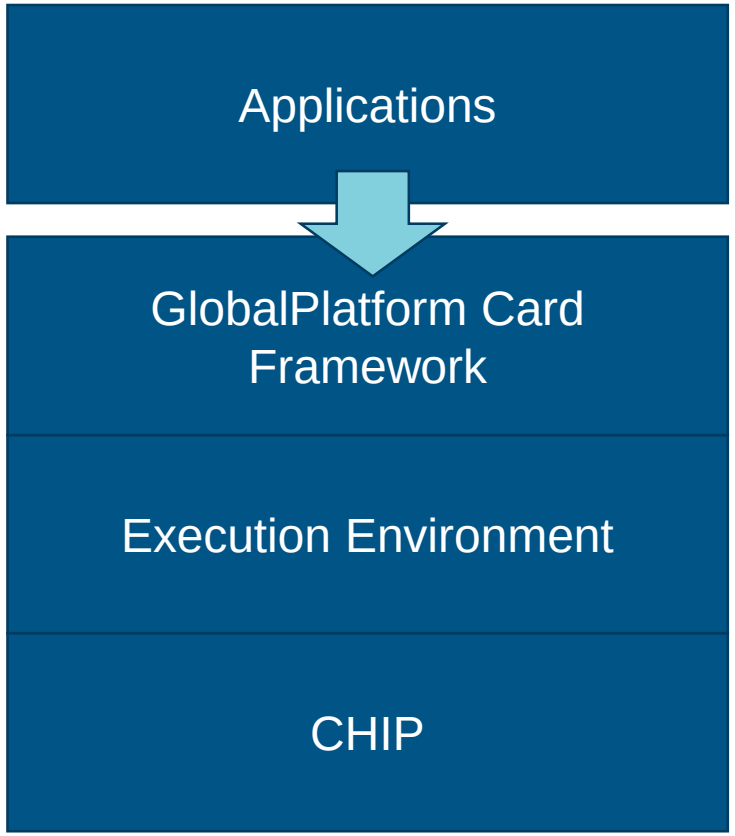
SE PP Defines a Standardized Evaluation for Secure Elements

- SE PP defines a **standardized description for the evaluation** (the assets, the threats, the security objectives and the security requirements) **of all the Card Content Management**
- It will simplify the evaluation work for the vendors and for the labs
- It will simplify the work of the certification authorities
- It improves transparency on the features supported by the products

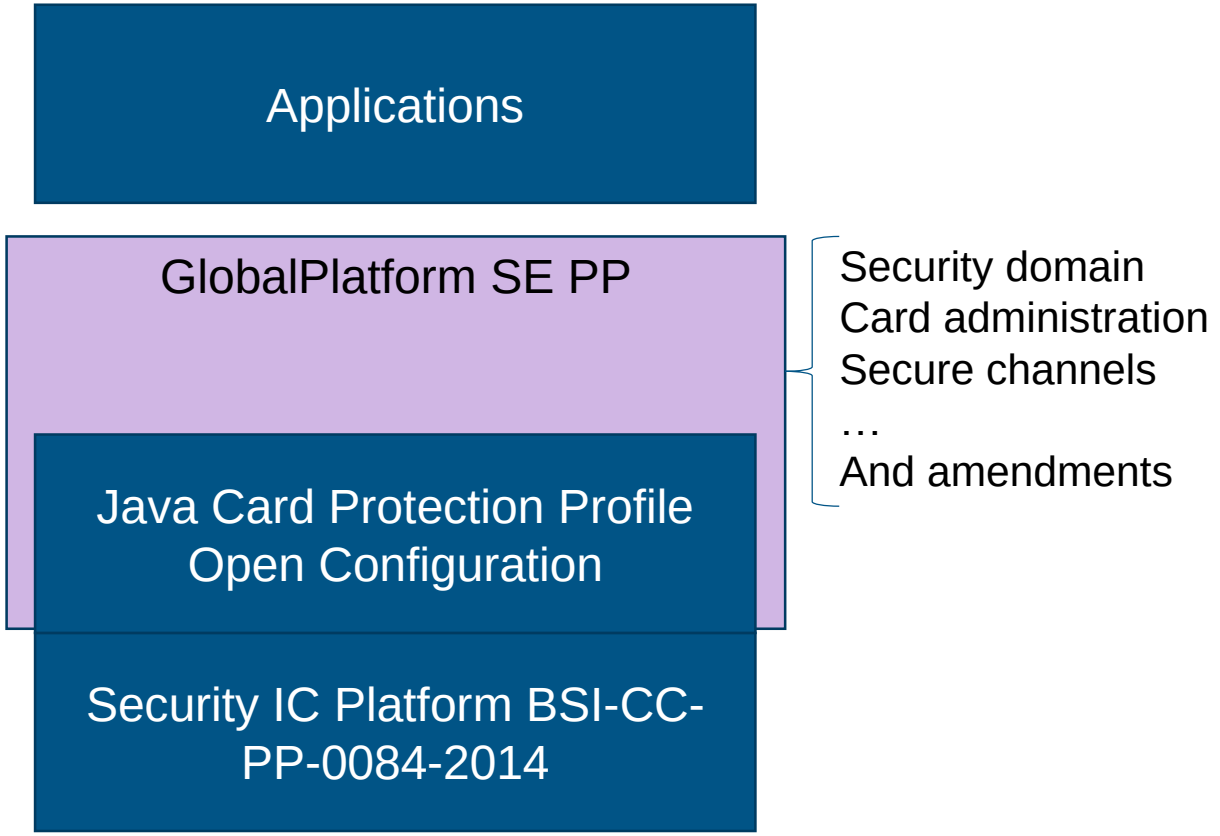
Card Content Management: Mechanisms defined in GlobalPlatform Card Specification to load, install, remove Card Content (the code of the applications, the application data , and the data to manage the SE itself example memory usage) in a dynamic multi-application multi-actor environment.

Secure Element Protection Profile

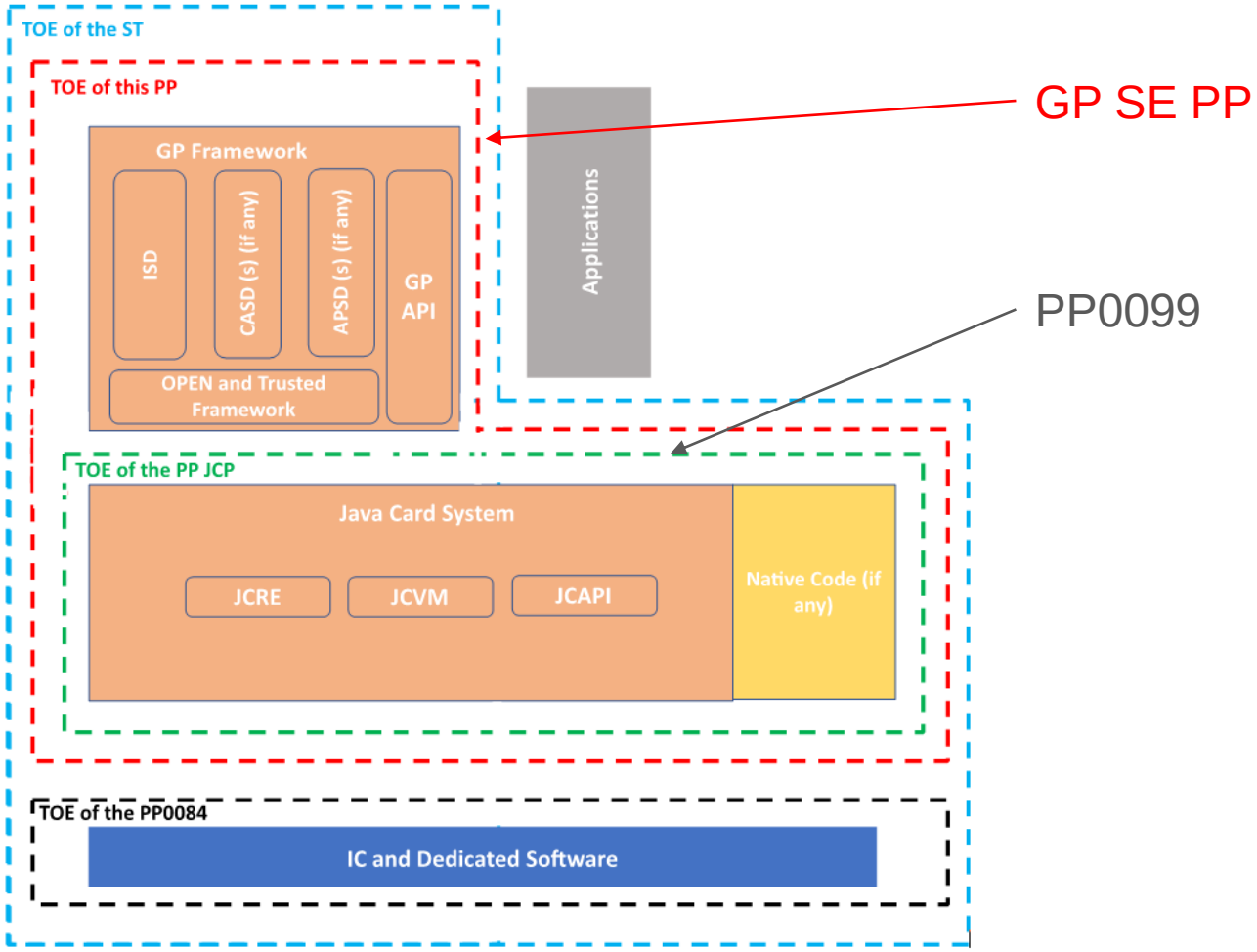
Applicative Stack



Secure Element Protection Profile



GP SE PP TOE components



The protection profile is built to optimize the writing of the product Security Target of the final product :

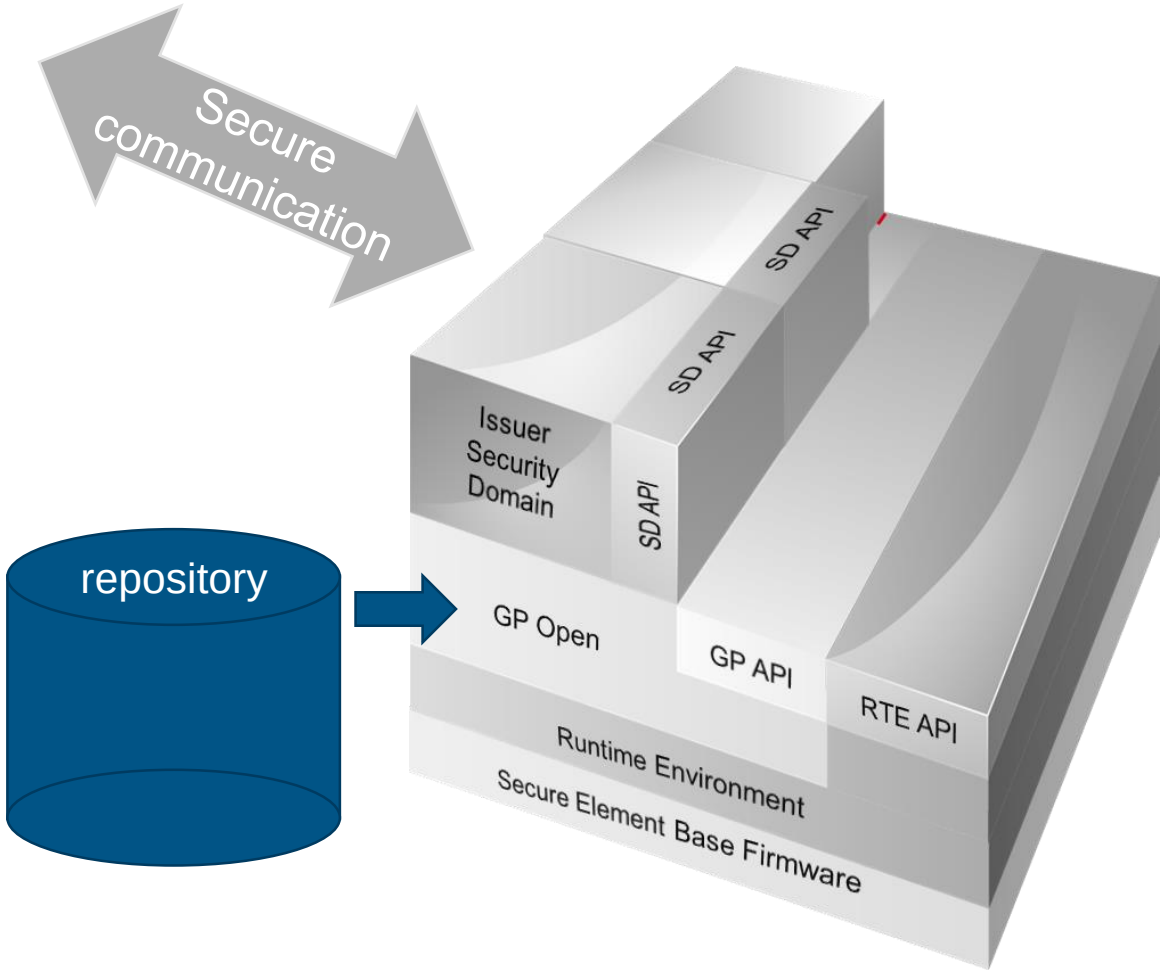
All GlobalPlatform features are defined

Just pick and choose of features is needed

GlobalPlatform SE PP - Modular Structure (1/4)

The **core** PP defines the security problem, objectives, and requirements for SEs by extending the Java Card PP [PP0099]. This includes:

- Card and application life cycle management
- Privileges Management
- Trusted Framework
- Secure communication covering all Secure Channel Protocols (SCPs).

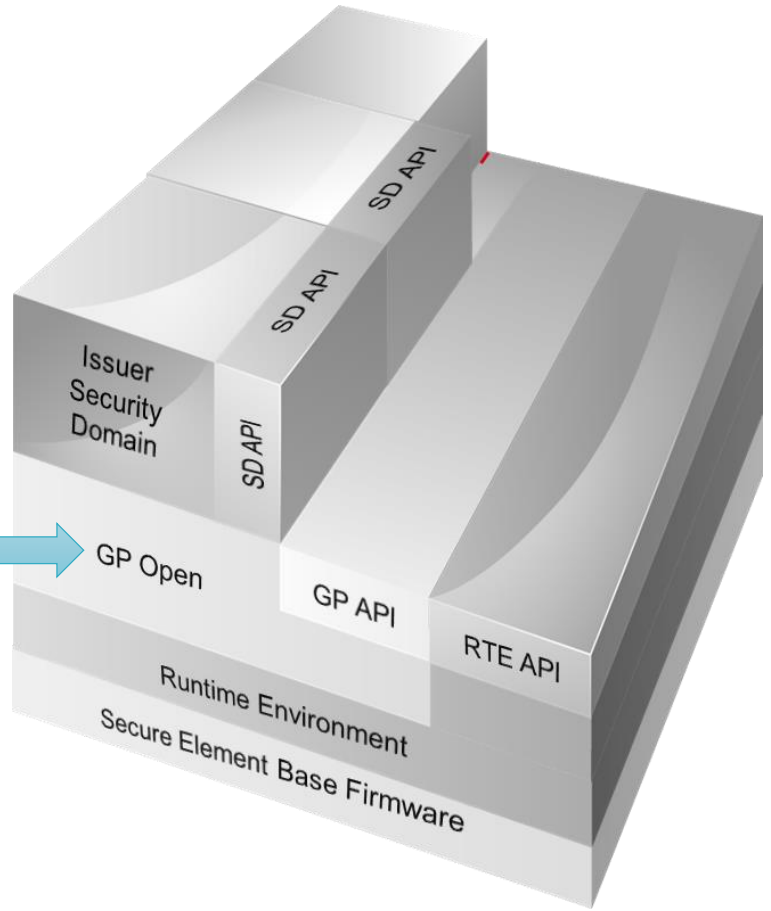


GlobalPlatform SE PP - Modular Structure (2/4)

The six **functional packages** address privileges assigned to the Security Domains (SDs) or Applications in the card to permit changes to the card content:

- Ciphered Load File Data Block
- Global Services
- Cardholder Verification Method (CVM)
- Delegated Management
- DAP Verification
- Mandated DAP Verification

GP Open additional secure services :
Global Services,
CVM,
DAP,
CLFDB

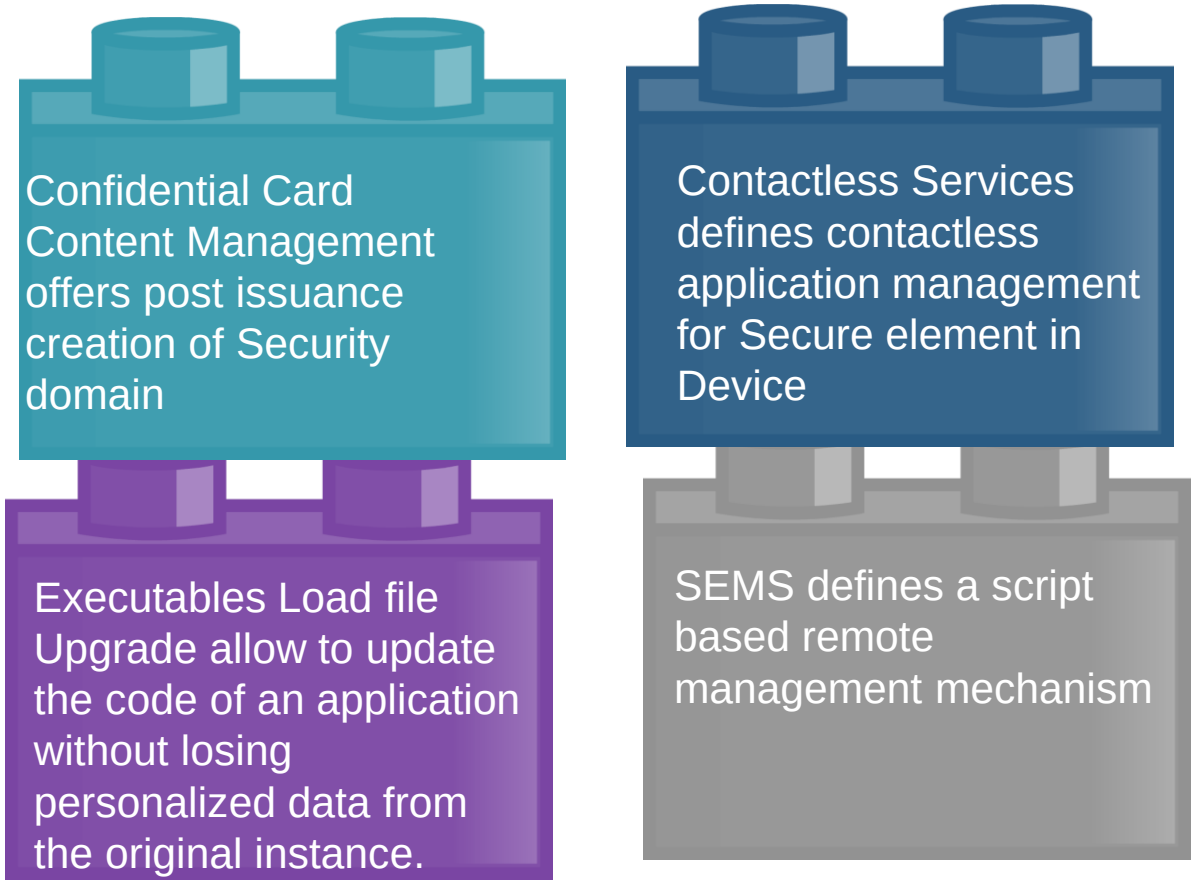


GLOBALPLATFORM®

GlobalPlatform SE PP - Modular Structure (3/4)

Additionally, **four PP Modules** are defined to cover:

- Confidential Card Content Management [Amd A]
- Contactless Services [Amd C]
- Executable Load File Upgrade [Amd H]
- Secure Element Management Service [Amd I]

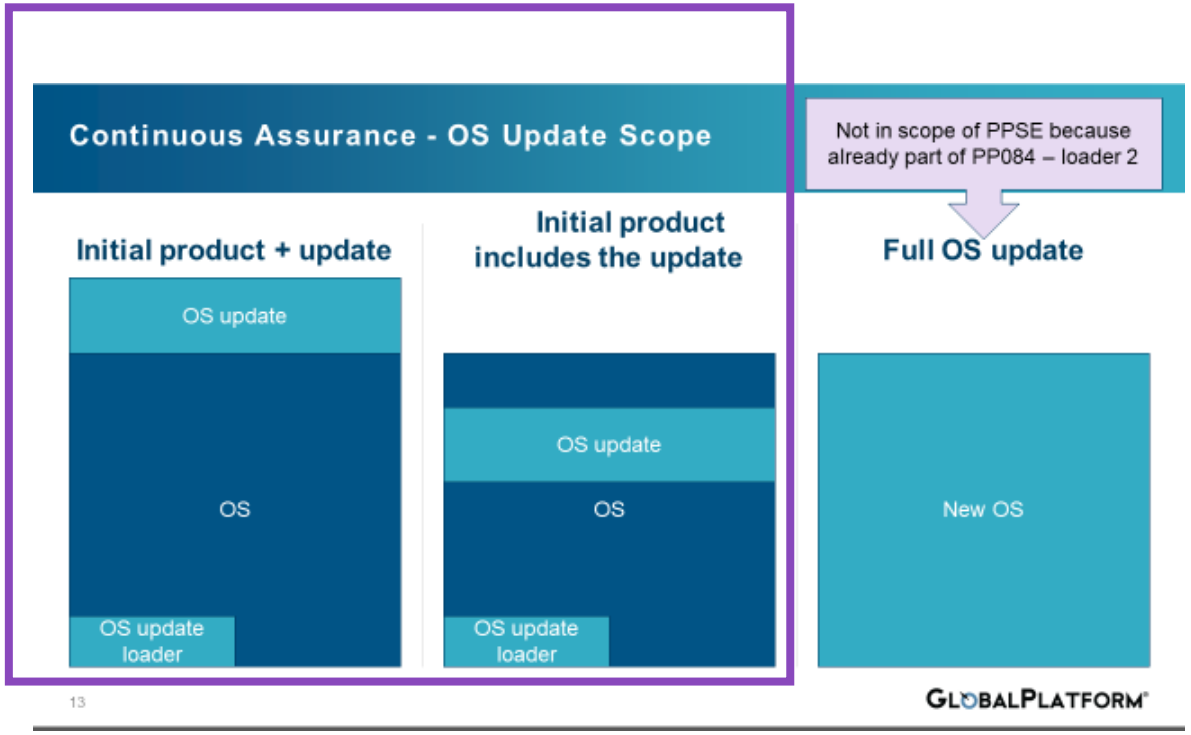


GLOBALPLATFORM®

GlobalPlatform SE PP - Modular Structure (3/4)

An additional fifth Module to address

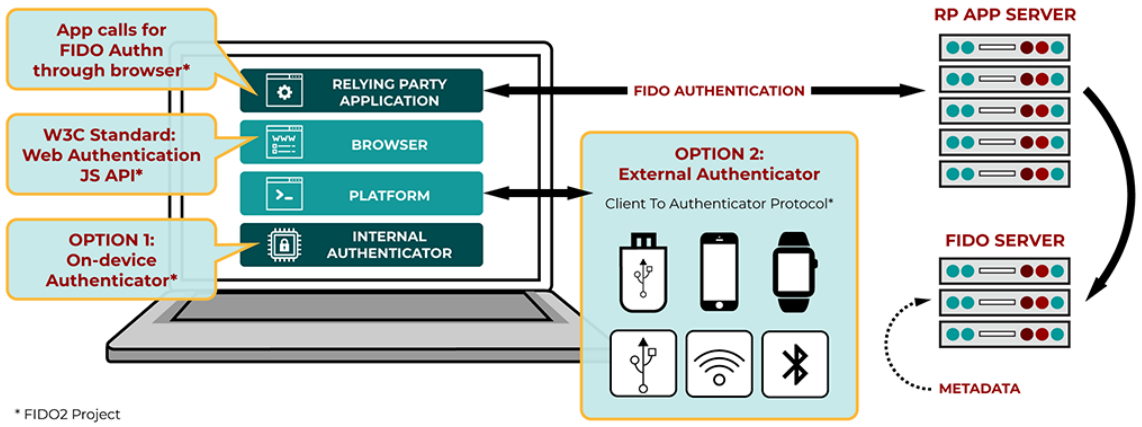
- The post-issuance OS update capability
- Support for EU-CSA OS Update mandate and EU-CC



GLOBALPLATFORM®

Extension to support FIDO 2.0

FIDO 2.0 is here



FIDO 2.0

- The FIDO2 Specification distinguishes between:
  - Roaming authenticators, which are implemented externally, support the CTAP protocol and can communicate based on different technologies (e.g. USB, Bluetooth, or NFC);
  - Platform authenticators, which are embedded inside a device such as a laptop and cannot be disconnected from the device, e.g. a laptop with a Touch Bar supporting Touch ID fingerprint recognition.

CTAP 2.1: Client to Authenticator Protocol (CTAP) Proposed Standard, June 2021

FIDO 2.0 on SE PP

Scope

- This document focuses specifically on external, off-device roaming authenticators that verify user presence and that rely on the GlobalPlatform SE on top of which a FIDO2 Authenticator Application (FIDO2 AA) is running

- Answer both to GlobalPlatform SE PP requirements and FIDO Level 3+ requirements

- A FIDO2 SE Authenticator is a composed IT product with a platform architecture providing a secure execution environment and security services for the FIDO2 Authenticator Application running on top of it.

- The TOE comprises:
  - All hardware, firmware and software relied upon to provide the FIDO2 SE Authenticator security functionality.
- The TOE does not comprise:
  - The FIDO Client application;
  - The Relying Party;
  - The FIDO Server.

takeway

It offers a simple framework for:

- Security laboratories to evaluate the security of SE-based products, and validate conformance with security, regulatory and data protection mandates, such as the European Cybersecurity Act.
- Silicon and SE vendors to demonstrate their products are secure for use across devices and verticals including payment and identity cards, ePassports, smartphones and IoT devices.
- Device manufacturers to determine the trustworthiness of components, and select a solution with the required features to protect apps and digital services on their devices.

Secure Element PP address the need for consistent and verifiable security across SE products.

Contact Us

Membership:
membership@globalplatform.org

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

Questions:
secretariat@globalplatform.org

Twitter
@GlobalPlatform_

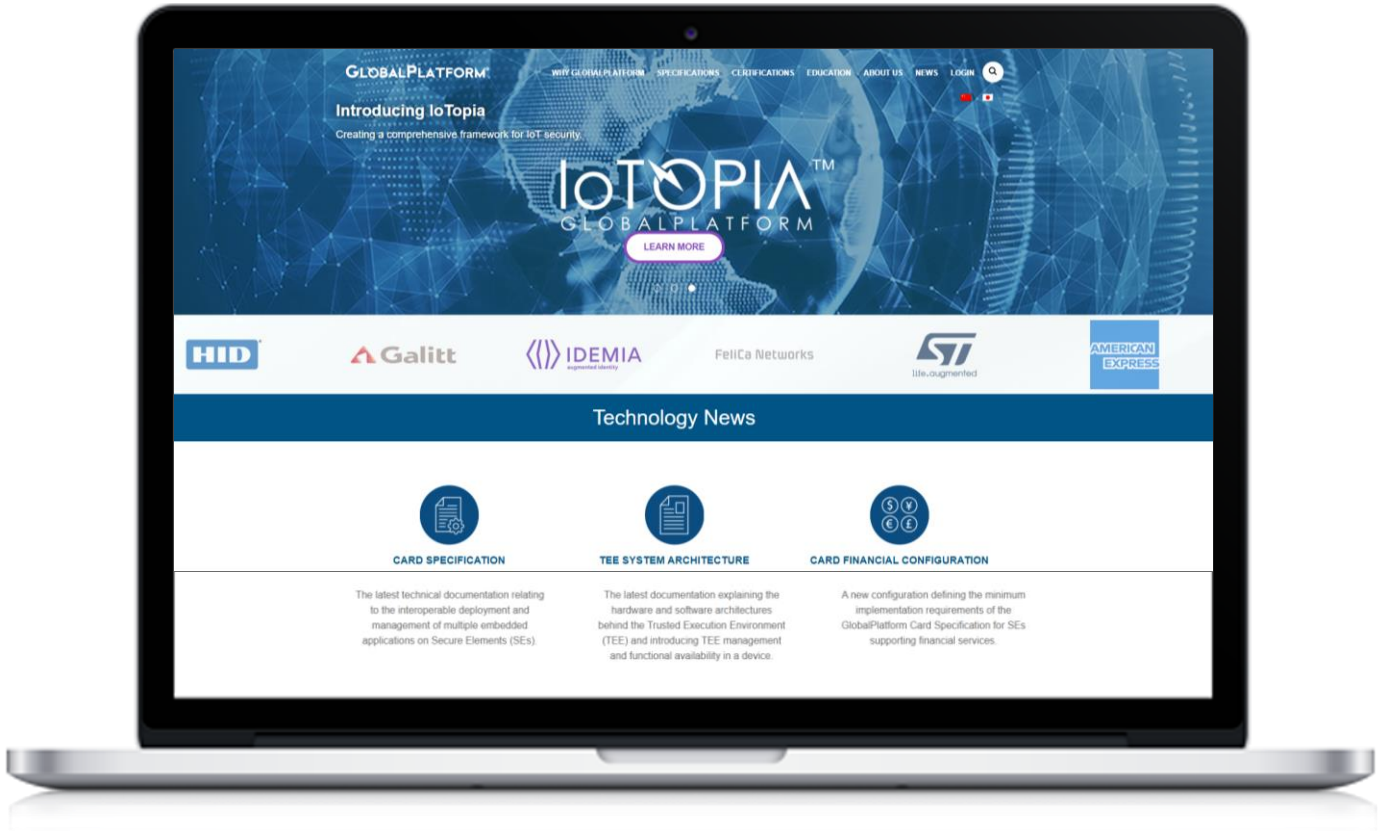
YouTube
GlobalPlatformTV

LinkedIn
GlobalPlatform

WeChat
GlobalPlatform China

YouKu
GlobalPlatform

GitHub
GlobalPlatform.GitHub.com



www.globalplatform.org

GLOBALPLATFORM®