GlobalPlatform Root of Trust

Olivier Van Nieuwenhuyze

STMicroelectronics, GP RoT sub-Task Force chair

Cybersecurity Innovation Forum, September 10th, 2015

Washington

@GlobalPlatform_ www.linkedin.com/company/globalplatform GlobalPlatformTV

Welcome

Agenda

- GlobalPlatform
- Root of Trust vision
  - Root of Trust
    - Primary Root of Trust
    - Secondary Root of Trust
  - Security services
  - Chain of Trust
- Mapping with the GP technology

About GlobalPlatform

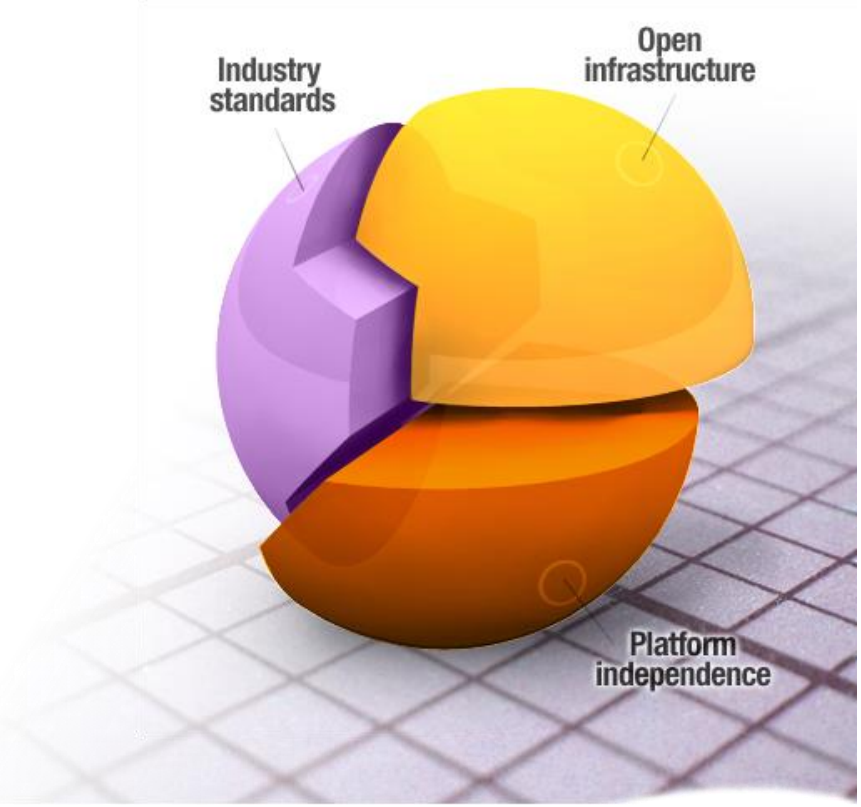
GlobalPlatform Mission

- GlobalPlatform works across industries to identify, develop and publish specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology
- GlobalPlatform Specifications enable trusted end-to-end solutions which serve multiple actors and support several business models

GlobalPlatform Vision

- Member-driven organization to define technology standards for cards, devices and systems and create foundation for future growth.
- License royalty-free card, device, and systems specifications.
- Compliance Program tools to verify card, device, systems compliance to GlobalPlatform technology.
- Foster adoption of secure chip technology standards and implementations across industries.

GlobalPlatform At-a-Glance



What is the output of GlobalPlatform?

- Specifications – technical industry guidelines
- Configurations – applying the guidelines to different market sectors
- Security Certifications – streamlining security requirements & testing
- Industry Compliance Program – confirming a product's functionality aligns to GlobalPlatform technology
- Educating the Industry – white papers & technical documents
- Workshops – specification training & educational

GlobalPlatform Members

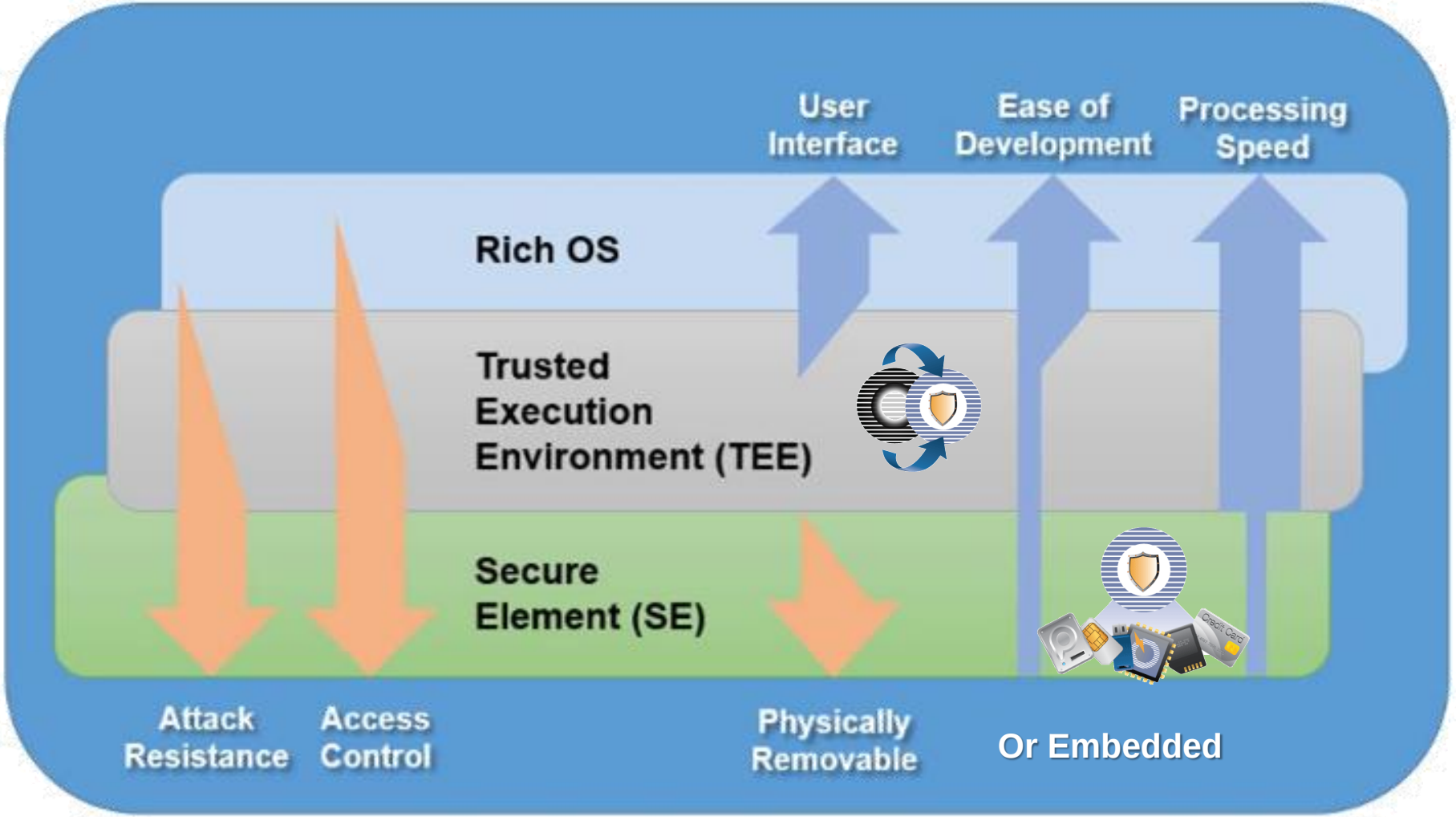
GLOBALPLATFORM®

Our Collaborative Industry Partners

Secure Content Storage Association

2 Types of Secure Components

GLOBALPLATFORM®

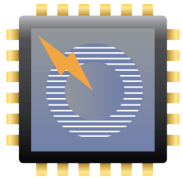


Definition – Secure Element (SE)

- An SE is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities.
- There are three different form factors of SE: Universal Integrated Circuit Card (UICC), embedded SE and smart microSD. Both the UICC and smart microSD are removable. Each form factor links to a different business implementation and satisfies a different market need.

UICC

Embedded SE

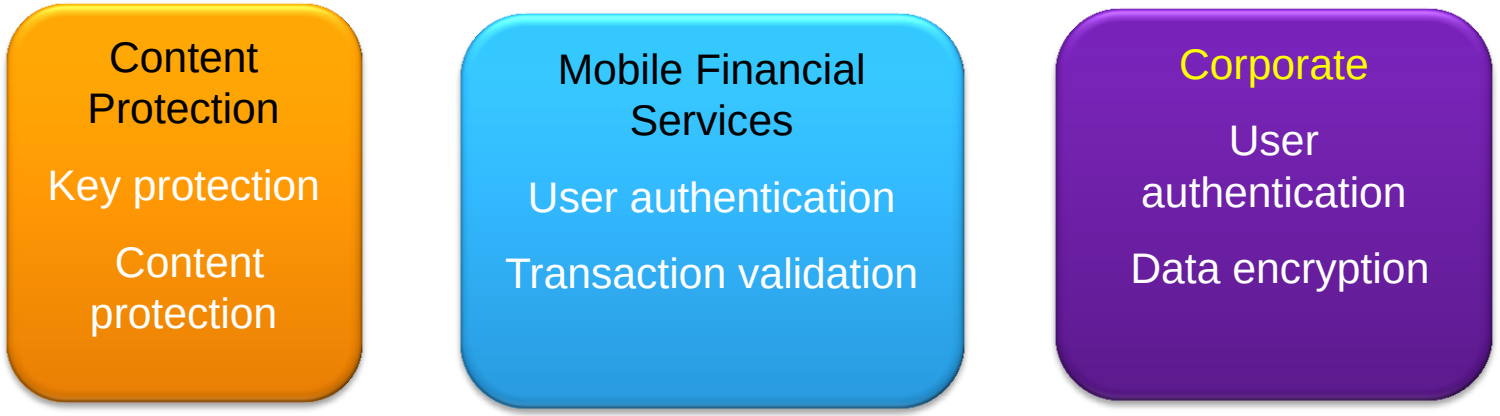


Smart microSD

Definition – Trusted Execution Environment (TEE)

GLOBALPLATFORM®

- The TEE is a secure area that resides in the main processor of the mobile handset and guarantees that data is stored, processed and protected in a trusted environment. It assists in the control of access rights and houses sensitive applications, which need to be isolated from the rich operating system (OS).



Why GP is positioning in the RoT ?

- The GP specifications require the presence of the basis information to use the technology
  - Key set and data associated
- Define the requirements to load securely the basis information
  - Already done as common practice but not specified in GlobalPlatform
- Clarify the role of all actors and relationship between all of them

Disclaimer

- GlobalPlaform is defining the “RoT Definitions and requirements” document

- This document is under review process internally in GlobalPlatform

Root of Trust

Market Status

- Increasing number of connected devices
  - Mobile phone
  - Car connected
  - Home connected
- Higher security needs
  - Privacy
  - Authentication
- Complexity of the solutions
  - Multi-actors
- Examples of security holes
  - Hacker used MMS to install a spyware on a Mobile
  - Hacker was able to kill a jeep on the highway

Terminology

- Platform
  - One computing engine
  - Executable code (providing set of functionalities)
  - I.e. :
    - Secure Element
    - TEE with display, …
- Device
  - End-user product
  - Composed of at least one platform
  - I.e. :
    - UICC
    - Mobile with several platforms (TEE with display, µSD, …)

What is a Root of Trust ? 1/2

- Specificities
  - Composed of computing engine, code and data all co-located on the same platform
  - Provide at least one security service

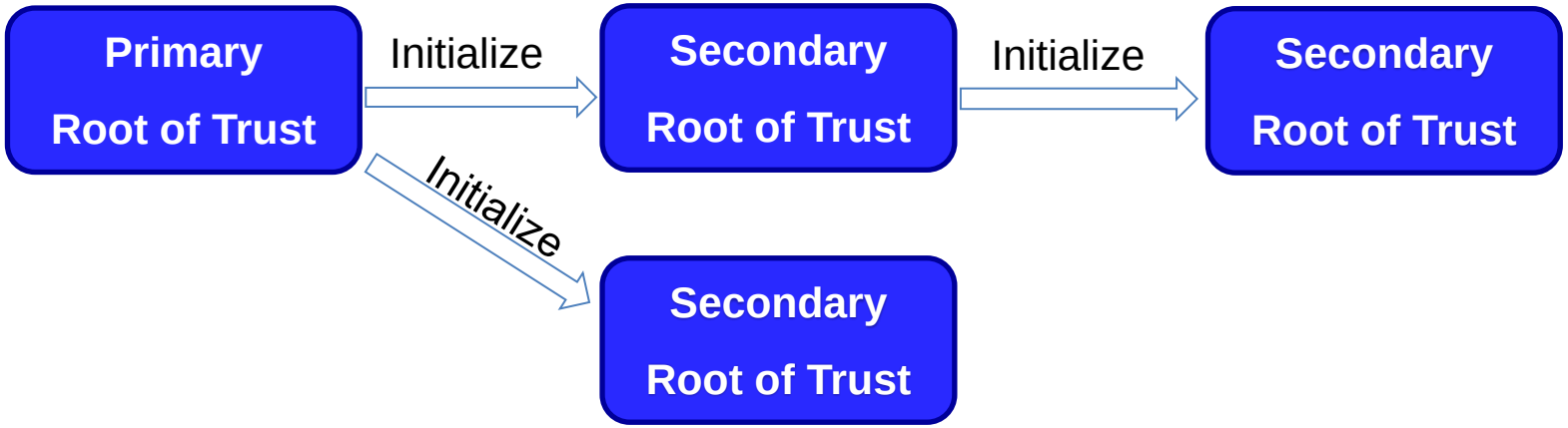
- Properties
  - Immutability
    - Or Mutability under authorization
  - Unique identifiable Ownership
  - Ownership optionally transferable

- Suitable for certification

What is a Root of Trust ? 2/2

- Primary Root of Trust

- Secondary Root of Trust
  - Parent Root of Trust may be unable to access to shielded location to preserve reportable verification
  - Some vendors may provide additional security services
  - When the blocks are coming from different vendors
    - Differentiate the code of the two blocks



Primary Root of Trust (pRoT)

- Specificities
  - Composed of computing engine, code and data all co-located on the same platform
  - Provide at least one security service

- Properties
  - Immutability
    - Or Mutability under authorization
  - Unique identifiable Ownership
  - Ownership optionally transferable
  - Created and provisioned during the manufacturing process
  - Code which executes first upon the initialization in the platform

- Suitable for certification

Secondary Root of Trust (sRoT)

- Specificities
  - Composed of computing engine, code and data all co-located on the same platform
  - Provide at least one security service

- Properties
  - Immutability
    - Or Mutability under authorization
  - Unique identifiable Ownership
  - Ownership optionally transferable
  - A parent RoT must verify the integrity of the code and data of a sRoT before its first execution of the sRoT
  - A parent must not preserve the reportable verification of the code and data of the sRoT

- Suitable for certification

Security Services List

- Authentication
- Confidentiality
- Identification (of a Root of Trust)
- Integrity
- Measurement
- Authorization
- Reporting
- Update
- Verification

Security Services

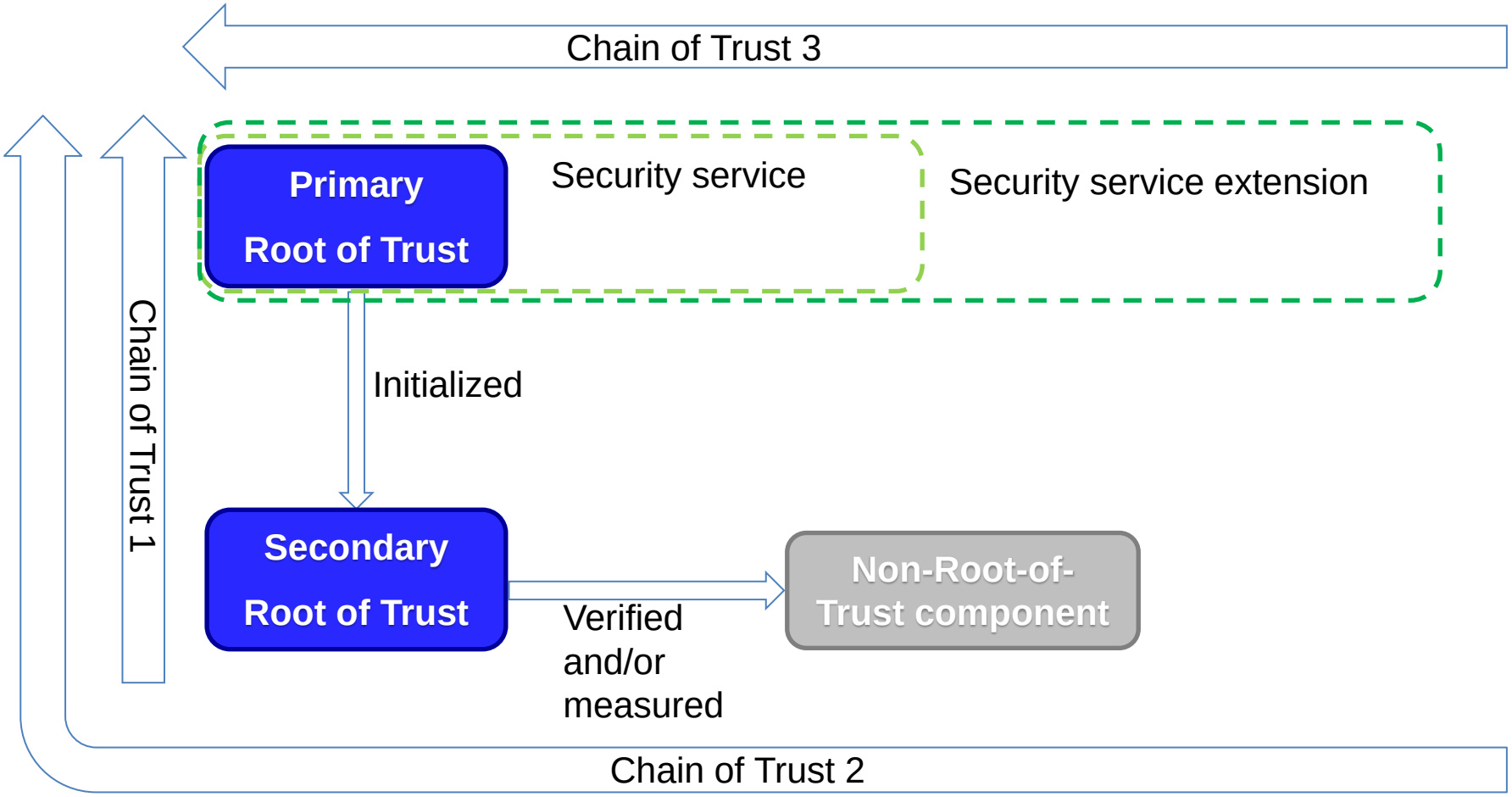
- In a Root of Trust
  - At least one security service shall be implemented
  - Other security services are optional

Security Services

- Most of them rely on shielded locations to protect the “sensitive data”
  - tamper-resistant or tamper-evident locations

- Provide interface to restricted access and/or enforce internal policy access to the content
  - Unauthorized access / use
  - Restricted access
  - Non-Disclosure

Three types of Chain of Trust 1/2



Chain of Trust 2/2

- The primary RoT and its secondary RoT of a chain may be on different components

- Multiple Chains of Trust
  - Several Chains of Trust may exist in the same device
    - i.e.: Two independent Chains of Trust in a Mobile:

      GlobalPlatform TEE

      UICC
  - No implicit interaction

Mapping with GlobalPlatform technology

GlobalPlatform Technology

- Security Domain (SD)
  - Load and install new application
  - Provide secure messaging service to the application to securely load its key and data
  - Manage the application without interaction of the other Security Domain (i.e.: Initial Security Domain)

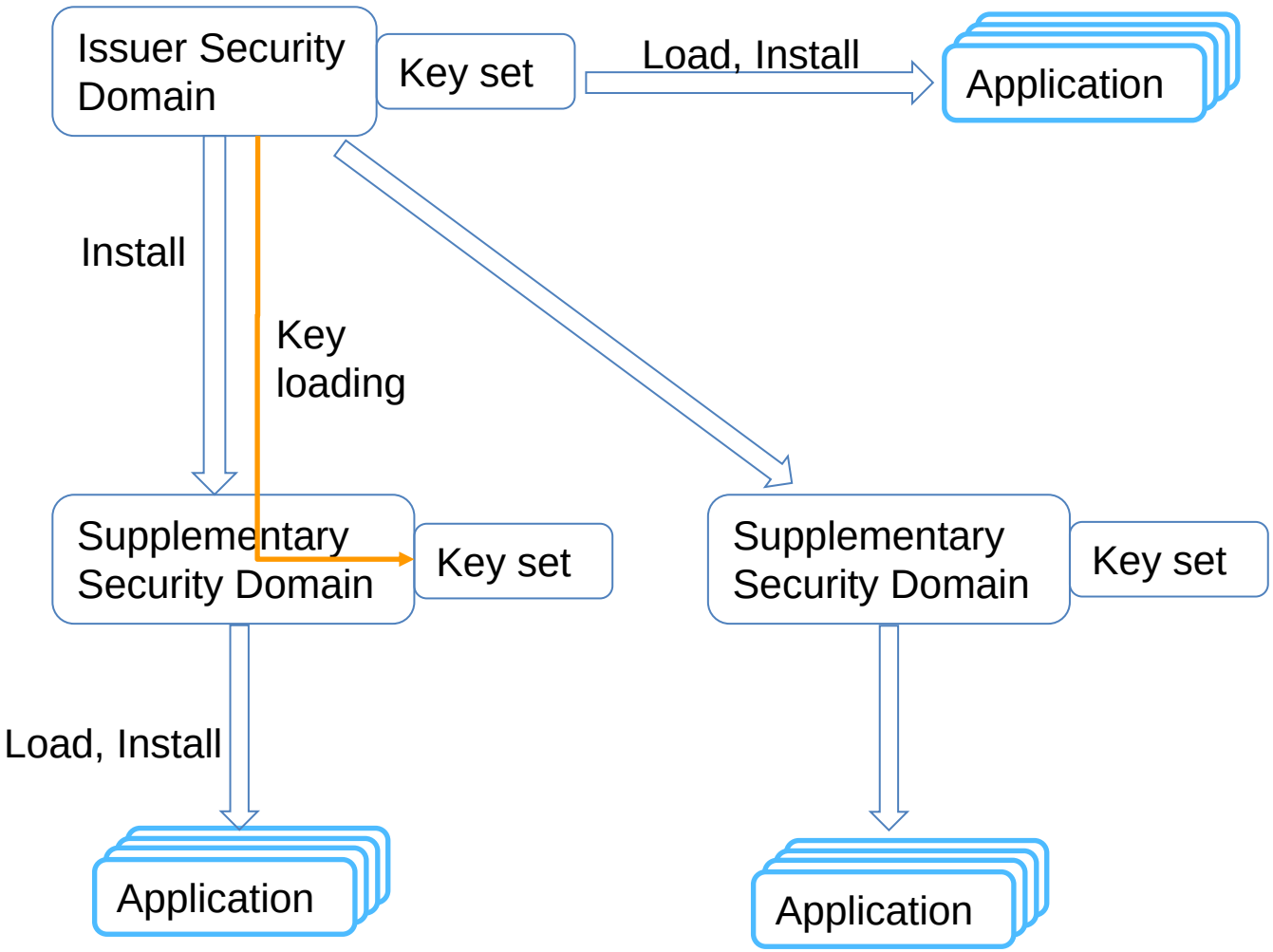
- Initial SD, provisioned during the manufacturing process
  - Data and Key Set

- Initial SD may authorize to install new SD
  - New SD is managed by the another owner
  - Loading Keys and Data through Secure Channel
  - New SD becomes autonomous (extradition in GP terminology)

GP RoT Requirements

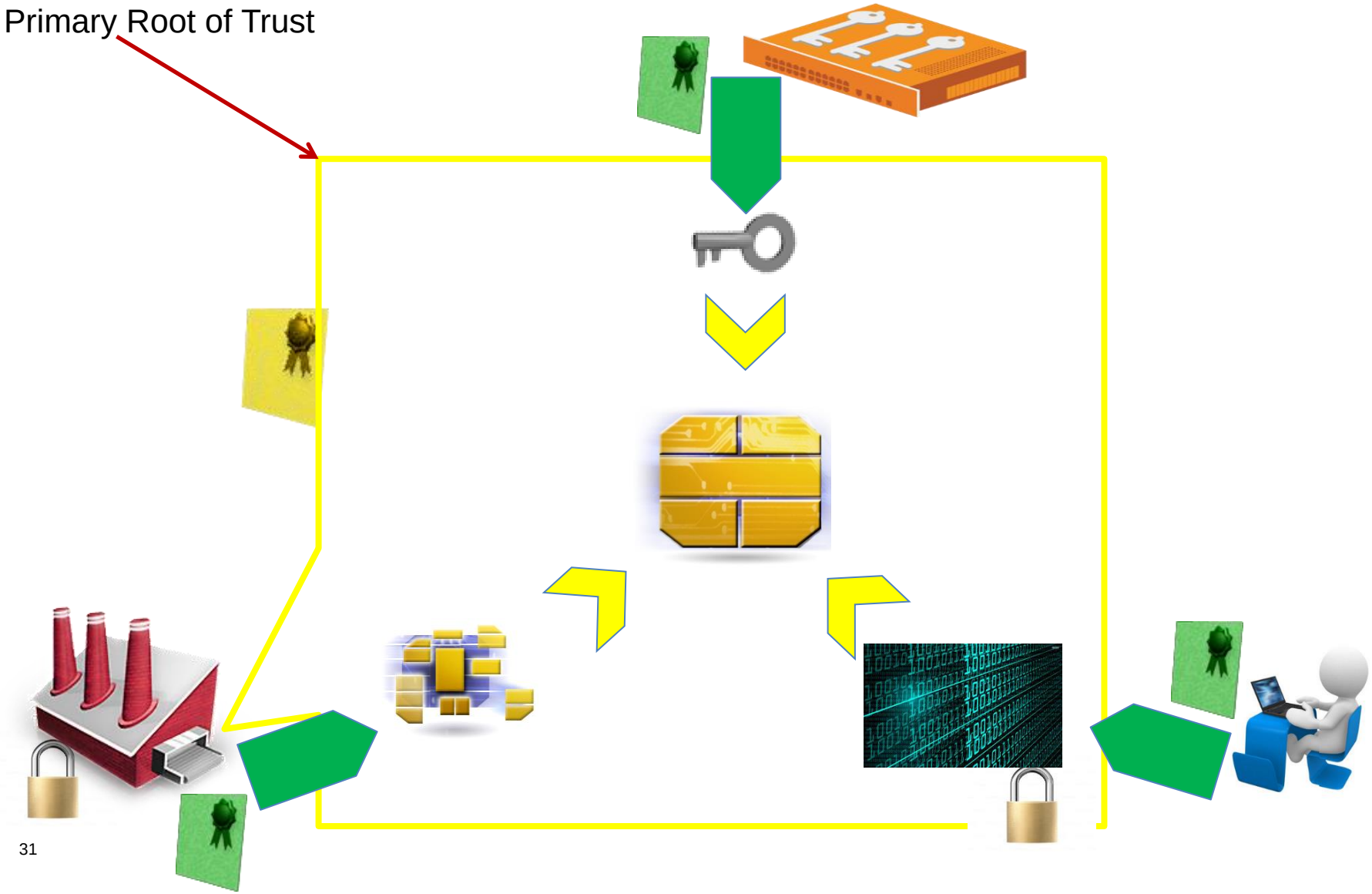
- Manufacturing process
  - Protected environment
- Manufacturing process certification
  - Certify the process
- Device certification
  - Reach the tamper resistant level required to protect the Root of Trust
- Multi-tenant
  - The sensitive information for a supplementary SD for a service extension may be loaded during the manufacturing process
- GP Chain of Trust
  - Provided by the service extension, of the SSD that extends the Confidentiality Service
- GP Identification
  - Identification of all actors of the Chain of Trust
- GP RoT verification
  - Protection if the data for the RoT is missing

Secure Element

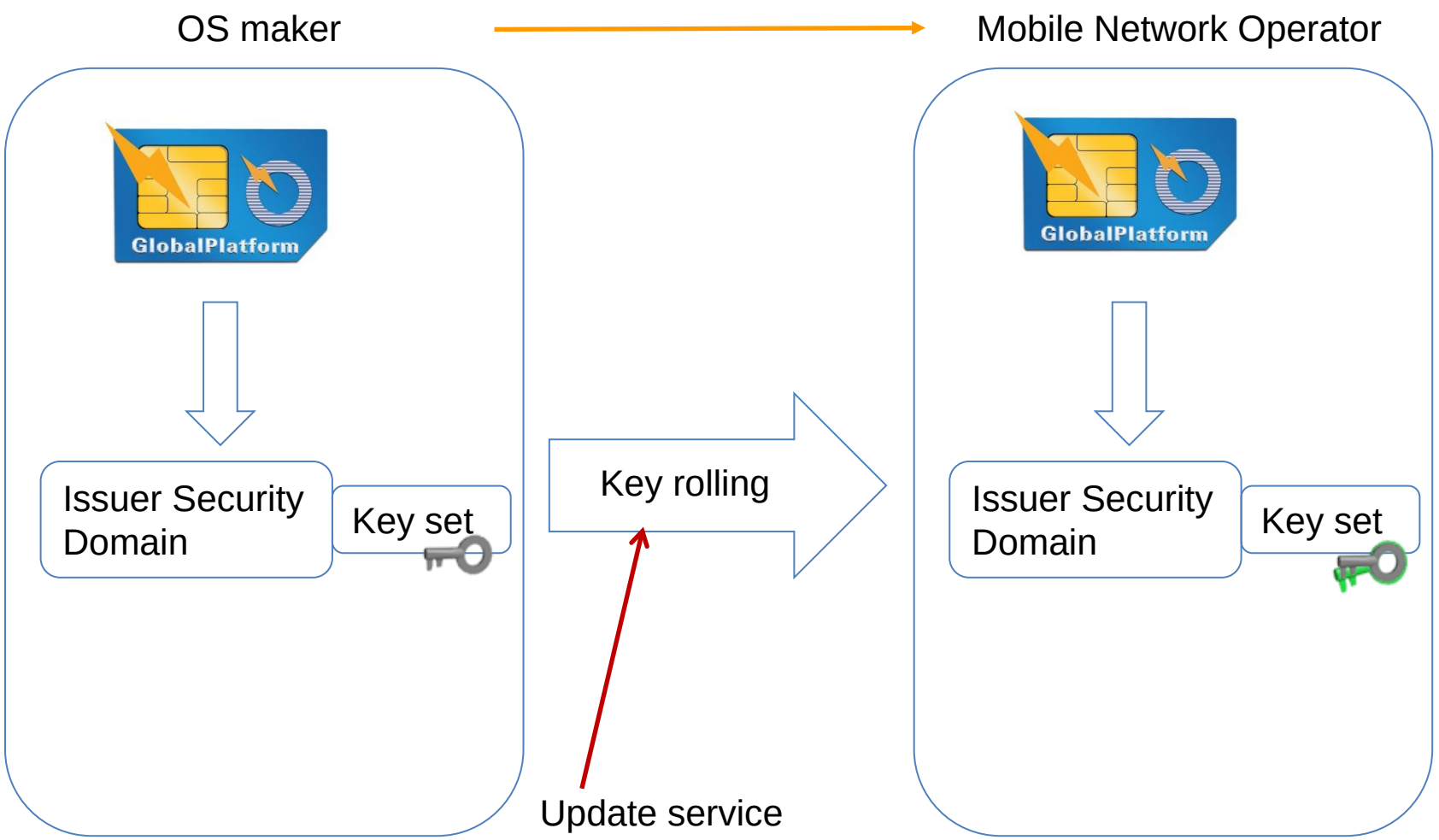


Secure Element Use Case 1/4

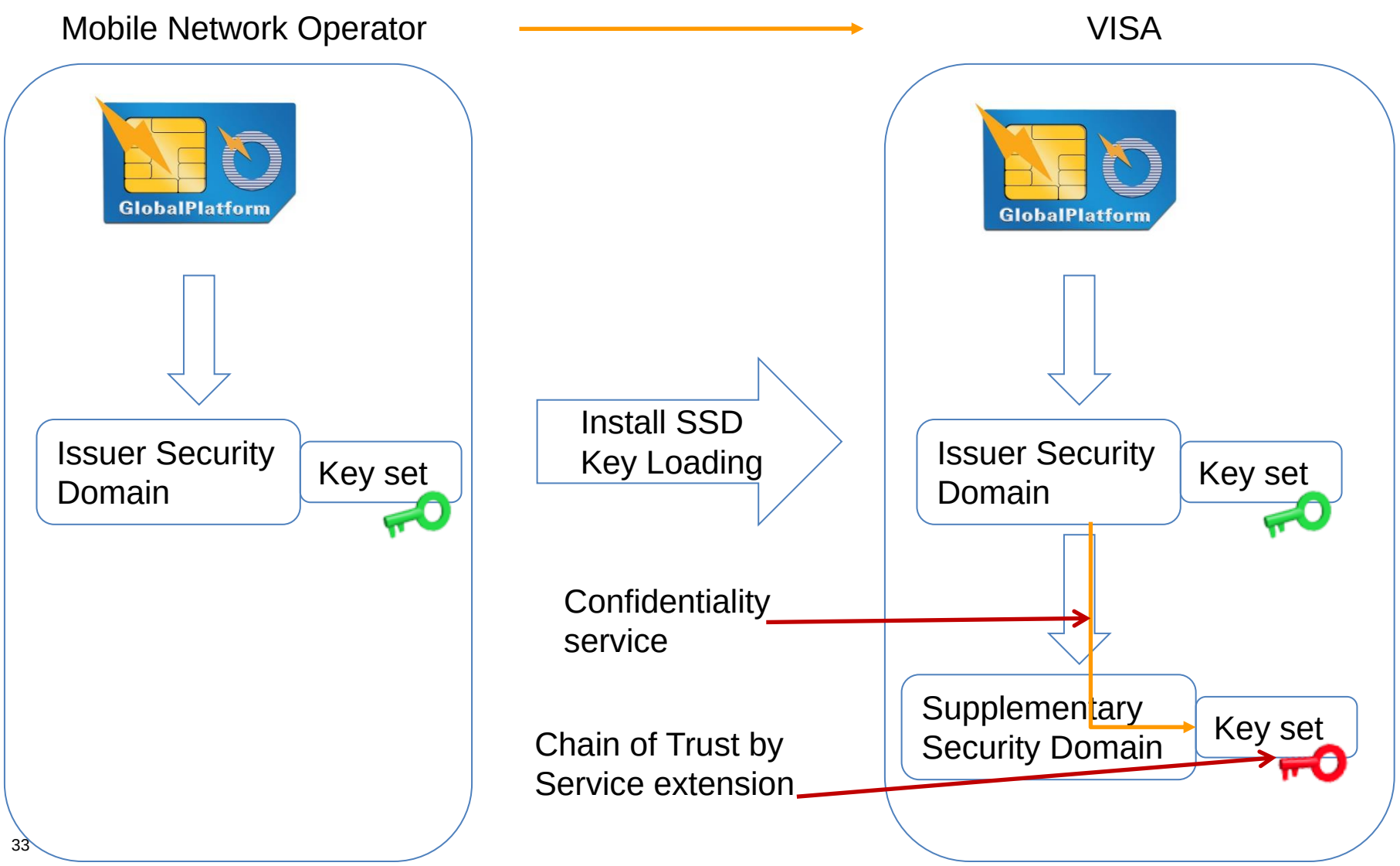
GLOBALPLATFORM®



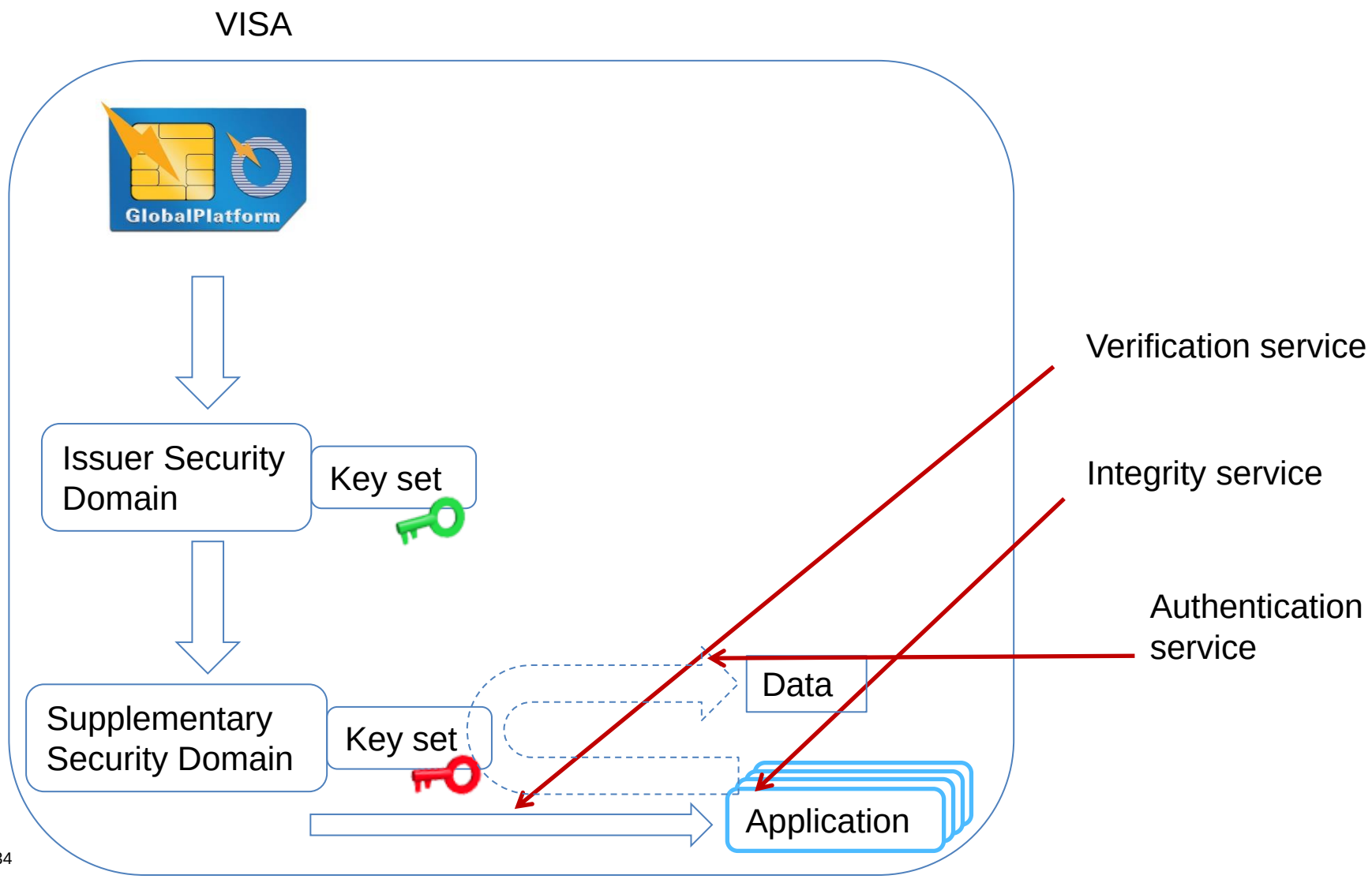
Secure Element Use Case 2/4



Secure Element Use Case 3/4



Secure Element UICC Use Case 4/4



TEE: Adding Mechanism vs SE

- TEE uses same mechanism of Security Domain hierarchy
- Difference with UICC
  - TEE provides services to the Mobile
  - TEE Software needs to be instantiated
- In booting implementation, the Secure Boot shall initialize the TEE software
  - The Secure Boot is the primary Root of Trust of the platform
  - The TEE Software is the secondary Root of Trust of the platform

Next steps

- Finalize our GP review
  - The interaction between two separate Chains of Trust needs to be clarified
  - Clarify some specific topics of the TEE mapping with the Root of Trust
- Include the requirements into our specifications

Thank you!

Backup slides

GlobalPlatform Technologies

- Management of applications
  - Loads, delete applet
  - Install, delete application(s)

- Allowing multiple actors to manage their own applications independently on the same secure component

- Define Secure Channel Protocol to manage securely the applications
  - Signature, authentication, cipher/decipher

Security Services

- Authentication service
  - Shielded location for storing credentials to be used in authentication protocol
  - Interface that maintains integrity of the contents of the shielded locations and restricts them for authorized access and uses in authentication protocols and protects against unauthorized use and disclosure

- Confidentiality service
  - Shielded locations for storing secret
  - Interface that enforces internal access control policies regarding the use and management of the contents of the shielded locations
  - The value are secret, the interface must protect content from unauthorized use and disclosure

Security Services

- Identification service
  - Shielded location for storing a secret value
    - a secret key (symmetric or private key) to establish the identity of the Root of Trust
  - Identity service for proof of possessing and signature generation
  - Protect the content against unauthorized use and disclosure
  - Different that the owner of the Root of Trust

- Integrity service
  - Shielded location for storing and protecting the integrity of non-secret but critical security parameters and platforms characteristics
  - Enforce internal policy regarding access and use of the shielded locations
  - Protect the shielded locations from unauthorized modifications

Security Services

GLOBALPLATFORM®

- Measurement Service
  - Reliably create platform characteristics
  - Typically does not contain a shielded location for the measurement
- Authorization Service
  - Reliably assess authorization tokens and determine whether or not they satisfy policies for access control
  - Provide same services as Root of Trust for Authentication, Integrity or both (in which case(s) it must also satisfy the requirements of these security services)
- Reporting Service
  - Reliably report platform characteristics authenticated by the platform's identity in a non-reputable way
  - Subset of service authentication, confidentiality, identification, integrity and measurement (in which case(s) it must also satisfy the requirements of these security services)

Security Services

- Update service
  - Verify the integrity and authenticity of signed updated and upon successful verifications, authorize the initiation of the update process
  - It may contain the RoT services as Authentication, Authorization, Confidentiality, Integrity and Measurement (in which case(s) it must also satisfy the requirements of these security services)

- Verification service
  - Verify the authenticity of digital signatures and verify the integrity of the objects protected by the signatures
  - It may contain the RoT services as Authentication, Confidentiality, Integrity and Measurement (in which case(s) it must also satisfy the requirements of these security services)

Secure Element mapping with RoT

- Primary Root of Trust is
  - System code and Secure Element hardware protection
  - OPEN
  - Runtime environment
  - ISD + Secure Channel Protocol + Related Data (Data + Key Set)

Secure Element mapping with RoT

- Authentication Service
  - Keeps integrity, non-disclosure, protects against attack and restrict access to
    - Key Set (S-MAC key) used for authentication
    - CVM (PIN)

- Confidentiality Service
  - Provides isolation of application in the runtime environment (i.e.: Firewall between application)
  - Keeps integrity, non-disclosure, protects against attack and restrict access to
    - Key Set (S-ENC) used to cipher/decipher

- Identification Service
  - Keeps integrity, non-disclosure, protects against attack and restrict access to
    - Key Set (S-MAC key) used to provide a signature on an unique identification number

Secure Element mapping with RoT

- Authorization Service
  - Provide a shielded location to store the right of the applications. These right are verified when some application try to access to:
    - Secure Messaging Protocol of the SD
    - Card locking and termination
    - …
  - Verified the right between two applications when one application access to a second application (Shareable interface in the runtime environment)

- Reporting Service
  - Keeps integrity, non-disclosure, protects against attack and restrict access to
    - Key Set (S-MAC key) used to provide a signature on a specific data

Secure Element mapping with RoT

- Update Service
  - Mechanism to update the contents of the shielded location where the Key Set is stored. This mechanism is endorsed by authentication. It is used to transfer the ownership
- Verification Service
  - Mechanism to verify the integrity and authenticity of
    - Loading of applet code
    - Installing application
    - Writing key set
  - Runtime mechanism that verify continuously that the code is executing correctly and verify the integrity of the parameters, data and keys.

Context Setting: Device Technologies

GLOBALPLATFORM®

	Rich OS Environment	Trusted Execution Environment (TEE)	Secure Element (SE) (when present)
Functionality	★★★	★★	★
Performance	★★★	★★	★
Memory Size Access	★★★	★★	★
Peripherals Access (display, touchscreen, video decoder/renderer, …)	★★★	★★	N/A
Attack Resistance	★	★★ (designed for SW-based attacks resistance)	★★★ (tamper-resistant)

Card architecture