

GlobalPlatform's Secure Components and the Root of Trust

Olivier Van Nieuwenhuyze

STMicroelectronics, GlobalPlatform Security Task Force chair

International Cryptographic Module Conference, 19 May 2016 Ottawa, Ontario

GP Confidential © 2016







Welcome

Agenda

- Introduction to GlobalPlatform
- GlobalPlatform's vision for the Root of Trust (RoT)
 - Root of Trust types
 - Security services
 - Chain of Trust
- Example of a RoT with GlobalPlatform Secure Components





GlobalPlatform

GlobalPlatform's 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

GLOBAL PLATE

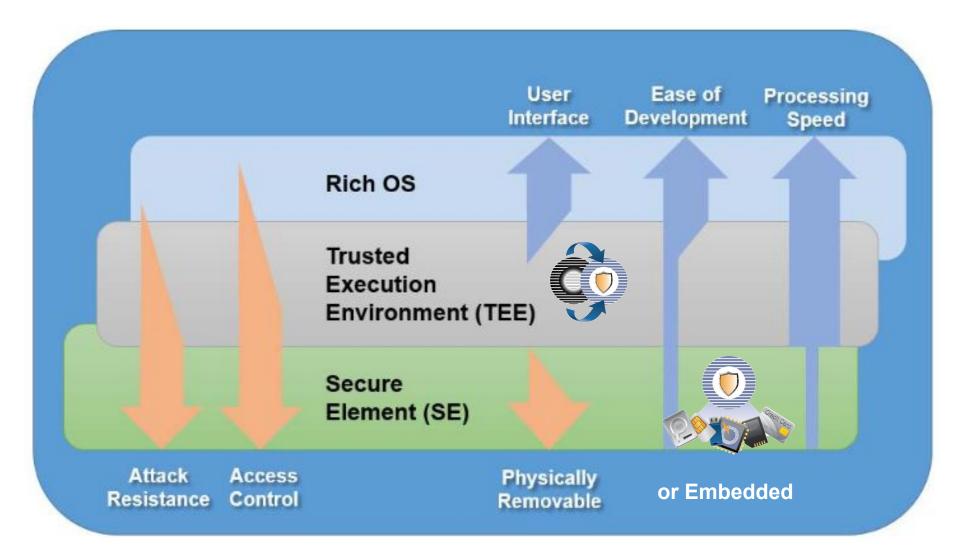
GlobalPlatform's vision

- Member-driven organization to define technology standards for cards, devices and systems and create a 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

LOBALPLATFORM

9010

There are two types of secure component







GlobalPlatform's Vision for the Root of Trust

RoT and Chain of Trust

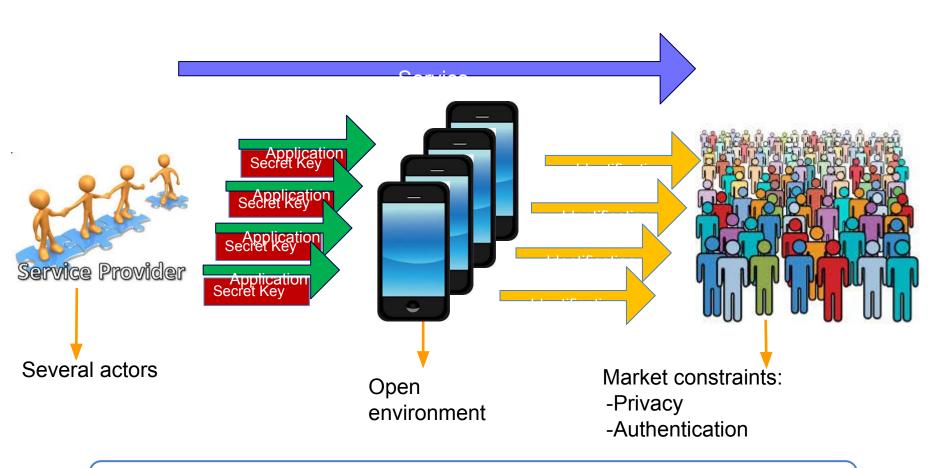
- Trust is the basis of our human relationships
 - You don't trust everybody
 - But you trust someone (or an entity) because you built a common history with them (or it)



- The Electronic component (hw device) has no history for you, this is an open gate for hackers
- GlobalPlatform creates a history of your electronic component
 - Details can be found in the GP Root of Trust Definitions and Requirements document

Service provider and service deployment

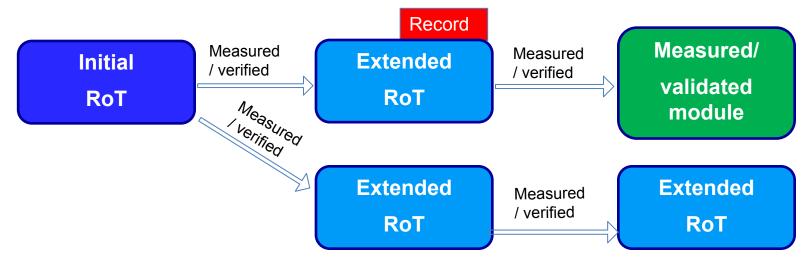
GLOBALPLATFORM®



The GlobalPlatform Chain of Trust facilitates the service deployment and guarantees the application execution environment

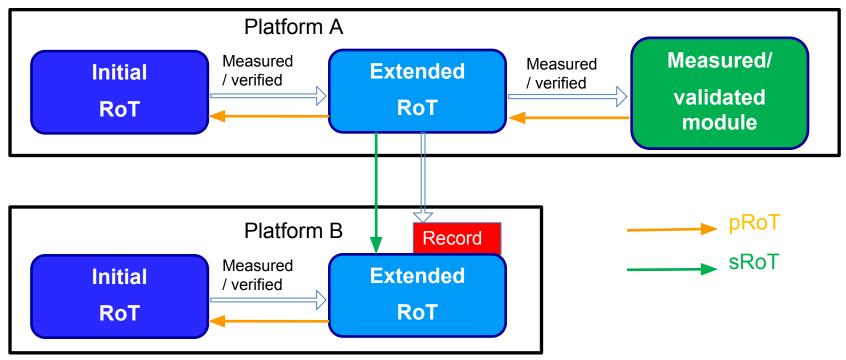
RoT types

- Initial RoT
 - Unique on a platform
 - The first code executed on the platform
 - Created and provisioned during the manufacturing process
- Extended RoT
 - Verified/measured by its Parent RoT without providing a reportable verification
- Measured/validated module
 - Verified/measured by its Parent RoT that preserves a reportable verification



RoT types cont.

- Primary Root of Trust (pRoT)
 - Combination of Initial RoT and 0 or more Extended RoT which are executed on the same platform
- Secondary Root of Trust (sRoT)
 - A RoT providing security services used by another platform



Security services list

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

Security services

- A RoT
 - Implements at least one security service
 - Other security services are optional
- A validated/measured module
 - May offer additional security services than its parents
 - May extend a parent security service
- Most of the security services rely on shielded locations to protect the "sensitive data"
 - Thanks to tamper-resistant or tamper-evident locations
- Provides interface to restricted access and/or enforces internal policy access to the content
 - Unauthorized access/use
 - Restricted access
 - Non-disclosure

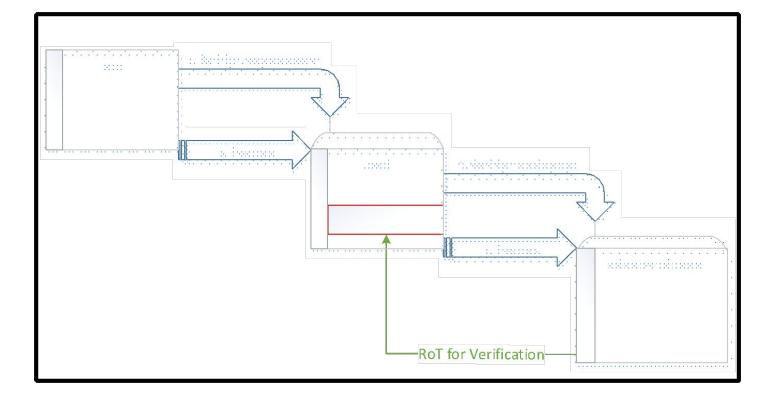
Chain of Trust

- Implicit Chain of Trust
 - Sequence of code modules, which is a RoT, performs the verification and authorization on the next code module (without leaving a reportable record behind)

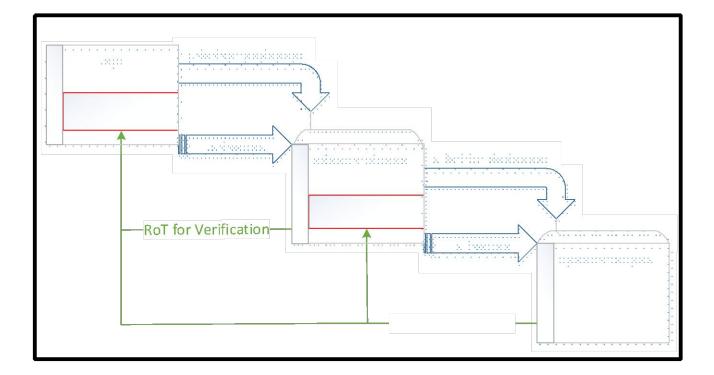


- Explicit Chain of Trust
 - Extends a service from a RoT
 - Between two Chains of Trust
 - Or module to other module(s)
 - Reusing a security service code execution with data/keys from another actor than the ones from the owner of the security service

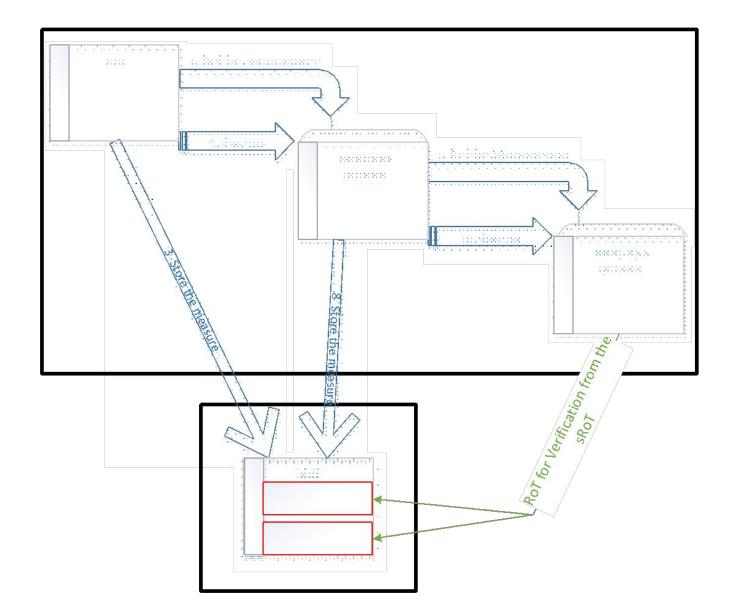
Implicit Chain of Trust



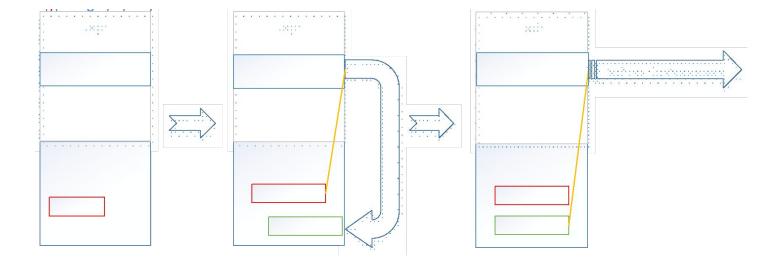
Explicit Chain of Trust



Explicit Chain of Trust cont.



Explicit Chain of Trust cont.



GLOBALPLATFORM®

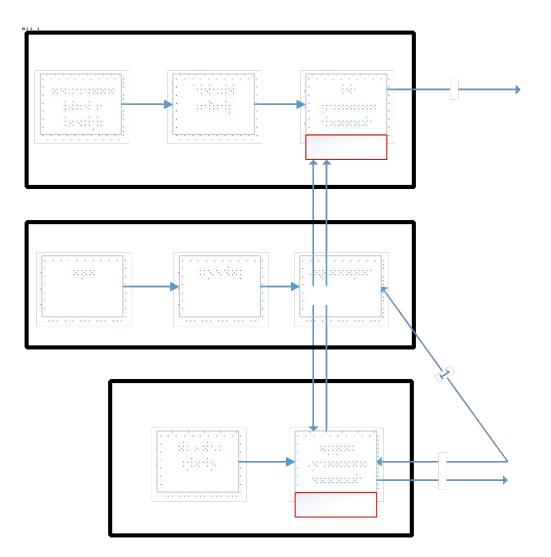


Example of a RoT with GlobalPlatform Secure Components

Example of GlobalPlatform implementation



Example of GlobalPlatform implementation cont.



GlobalPlatform technology provides...

• A Standardized

- Trusted execution environment (TEE) allowing a trusted application to provide the TUI
- Secure element (SE) environment allowing it to execute an applet and to securely store its sensitive information
- Mechanism to manage and deploy the secure application service on secure components issued in the field
- A mechanism to pair and to open a secure channel between the SE and the TEE

GlobalPlatform members



More @ www.globalplatform.org

GLOBALPLATFO	RM [®] Home Memt	berLogin Become a Member Store Search Contact Us
specifications compliance certificati	ion membership about us media & resour	rce center training 中文内容 jobs
	The Standard for Ma on Secure Chip Tech	
Download the Latest Specs Card Device Systems Specs under public review 	Become a Member > Influence specifications development > Enhance your global industry positioning > Build industry relationships Join Now >	Made Simple Guides GlobalPlatform has launched a series of guides that aim to explain in simple terms the technology developments that it is working on and how these will benefit the industry. Read More >
Technical Priorities	GlobalPlatform News	Recent Updates/Latest Content
Identity Task Force	> 09 Mar 16 - Executive Director Newsletter	The call for papers for the 2016 TEE Conference is now
Internet-Of-Things Task Force	> 01 Mar 16 - Shenzhen Excelsecu Data	open! Submit your speaker proposal now to discuss
> Japan Task Force	Technology Co., Ltd. Joins GlobalPlatform	payments, IoT, premium content protection, certification
> Mobile Task Force	> 18 Feb 16 - GlobalPlatform Qualifies Laboratories	and more. Also, here's highlights from the 2015 event:
> Premium Content Task Force	& Tools for GSMA eUICC Testing	
Security Task Force	> 10 Feb 16 - TA Technology (Shanghai) Co., Ltd.	Trusted Execution Environment: Device
Card Committee	Becomes GlobalPlatform Member	
> Device Committee	> More news	The second literation
Systems Committee		
Enter Email Address	Global Events & Discounts	
I want to receive specification updates		





Thank you!





Back-up slides

What is a RoT?

GLOBALPLATFORM®

- Specificities
 - Composed of computing engine, code and data all co-located on the same platform
 - Provides at least one security service
 - As small as possible to limit the attack surface
- Properties
 - Immutability
 - Or mutability under authorization
 - Unique identifiable ownership
 - Ownership optionally transferable
- Suitable for certification

Additional requirements for a GlobalPlatform RoT:

- Manufacturing process SHALL be protected and certified
- When a platform is starting, it SHALL verify the integrity and presence of key and data sets
 - If the verification fails the RoT SHALL forbid any interaction with any (communication) interface
- All service providers using the security services of an actor SHALL be identified
- Each RoT SHALL have a unique RoT Identification number