GLOBALPLATFORM®

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Deploying and Protecting Digital Services with Chains of Trust

How to achieve security, privacy and integrity with GlobalPlatform secure components

May 2018

 |

TABLE OF CONTENTS

Introduction 3

What is a Root of Trust 6

How is a Chain of Trust Built? 7

RoT & Chain of Trust – The Foundation of Secure Components 9

GlobalPlatform Secure Components 10

Secure Element (SE) 11

Trusted Execution Environment (TEE) 12

The Value of Secure Components 13

Future Vision 14

About GlobalPlatform 15

INTRODUCTION

As the number and variety of devices capable of accessing digital services increases, so too does the attack surface.

The world around us is becoming increasingly connected. As consumer and industrial demand continues to drive growth in digital services, an increasing number and choice of devices including connected cars, set top boxes, smart cards, smartphones, tablets, wearables, and other Internet-of-Things (IoT) devices are accessing digital services.

But as connectivity increases, so does the attack surface available to attackers.

- 83% increase in smart phone infections in the second half of 2016[1]
- 9 of the 10 countries with the largest number of rooted devices are in the top 25 countries where devices are attacked most often.[2]
- Mobile IoT devices were compromised by the Mirai botnet and participated in the massive Mirai DDoS attacks in September and October 2016

With so many devices, digital services, stakeholders and other variables creating a dynamic landscape, a very real security challenge exists: ensuring that devices which enable digital service delivery can protect digital data and assets against threats and attacks, while also protecting the network infrastructure against unauthorized access.

"The security of IoT devices has become a major concern. The Mirai botnet attacks demonstrated how thousands of unsecured IoT devices could easily be hijacked to launch crippling DDoS attacks. As the number and types of IoT devices continue to proliferate, the risks will only increase."

- Kevin McNamee, Head of the Nokia Threat Intelligence Lab

It is not possible to effectively secure devices if they have not been designed with security at the core.

[1] https://pages.nokia.com/8859.Threat.Intelligence.Report.html [2] https://www.kaspersky.com/blog/android-root-faq/17135/

INSECURE DEVICES CAN BECOME A PLATFORM FOR ATTACKS

If security is not foundational, seemingly innocuous devices like lamps, refrigerators and cameras can become the platform for attacks. It is important to remember that effective security needs to be built into the device, it cannot be added afterwards. Think of a sandcastle, once built it will crumble once the tide comes in. If you add cement to the sand before you build the castle, though, it can better resist the elements.

The largest DDoS attack ever seen – 1Tbps – originated from an IoT botnet which compromised CCTV cameras[3]

When devices and services are hacked, or used to launch attacks, the risk is not only that data and infrastructures are compromised; brands can suffer irreparable damage too.

Managing risk, therefore, should be front of mind for service providers and device manufacturers to:

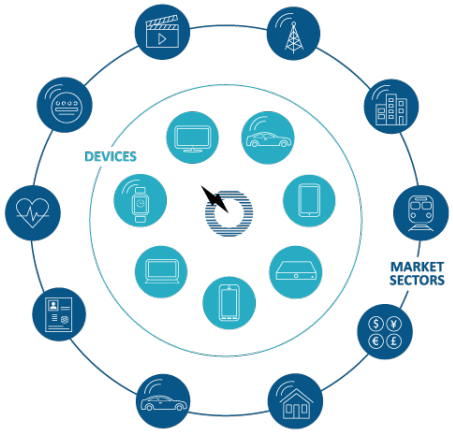
- Prevent devices from being used as a platform for attacks
- Ensure brand integrity
- Ensure data privacy
- Build trust
- Safeguard the usability of devices

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.

[3] http://bit.ly/2cWMESx

GLOBALPLATFORM SUPPORTS THE RIGHT DEVICE SECURITY CHOICES

This document defines the terms Root of Trust (RoT) and Chains of Trust. It goes on to explain how device manufacturers can create a secure RoT with GlobalPlatform technology, which is proven to meet the requirements of service providers and can be utilized by them to serve multiple markets and use cases. This, in turn, enables digital services to be bound to a physical on-device 'trust anchor'. The presence of this trust anchor makes it cheaper to protect applications than on an insecure device.



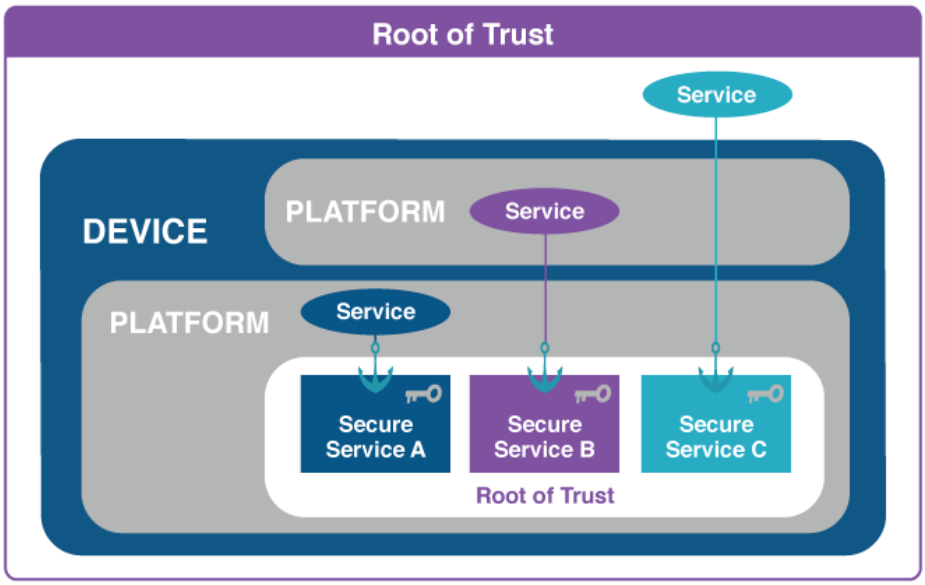
GlobalPlatform and its members have been working with device manufacturers and service providers for two decades, to standardize key requirements of successful secure digital service deployments. GlobalPlatform's resulting specifications deliver sustainable business models and empower both stakeholders to ensure that devices are protected against threats and attacks to enable the delivery of secure digital services.

Let's take a closer look at Root of Trust and Chain of Trust.

WHAT IS A ROOT OF TRUST?

RoT is a well-known term in the trusted computing space and an important security concept which has been widely deployed in devices for many years. Since connectivity today has evolved beyond computers and laptops however, it is necessary for the RoT concept to be extended to a much wider range of connected devices.

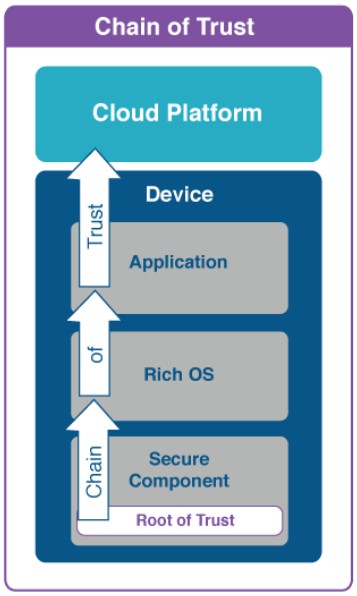
A RoT is a small computing engine – comprising code, data and keys – that offers secure services to, and is always trusted by, a platform. Secure devices can then be built using one or more platforms. It is the first code that is executed on a platform and offers secure services to other code (like the operating system and applications) hosted in a device. Limiting the size of the RoT reduces the attack surface, and certifying it enhances trust, both improving security.



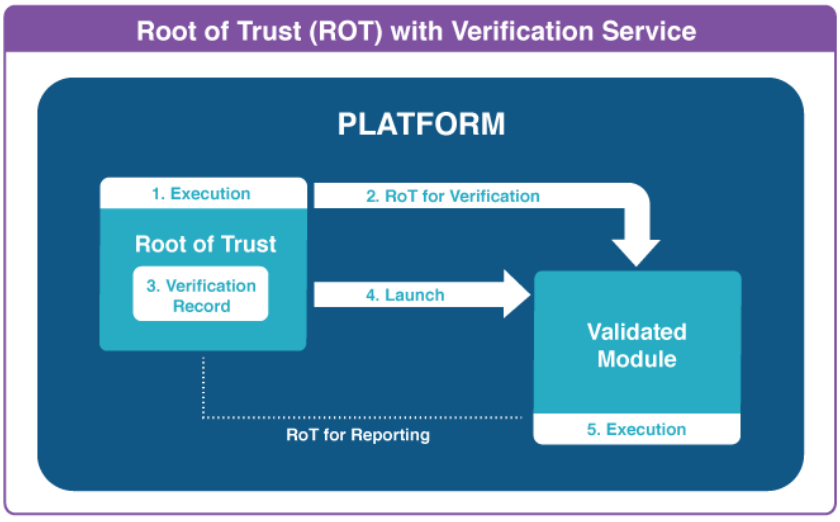
While the concept of RoT is important, its value lies in its ability to establish Chains of Trust to securely connect digital services with secure components and/or the device RoT.

How is a Chain of Trust Built?

Chains of Trust start with a RoT and each node in the chain is validated by the previous node. Service providers are using RoT secure services to attach their on-device applications, and therefore their services, into a Chain of Trust. As with a boat's anchor, the quality of the RoT determines the strength of a Chain of Trust.



The following diagram describes the creation of a link in a Chain of Trust, based on the verification services.



1. **Execution** – a new module needs to be executed
2. **RoT for Verification** – the verification service generates proof that the module is authentic
3. **Verification Record** – the RoT stores a record of this verification
4. **Launch** – the RoT transfers the execution to the validated module
5. **Execution** – the validated module begins execution

This process is repeated if the Chain of Trust needs to be extended using verification services.

When service providers want to enable and update digital services, they need to create an end-to-end secure communication with the end-point platform or device. The reliability of this secure communication is based on the secure services and the RoT available in the end-points. With consumer devices, the end-point will be used to authenticate the end user and store private data. IoT devices generate data that needs to be authenticated by the device and protected ahead of management in the IoT network's cloud server. Both use cases require a security in the end-point to enable this secure link and perform authentication.

The Chain of Trust security concept is already well known for the protection of the device operating system. GlobalPlatform's secure architecture extends this concept to help service providers to protect their digital services with the Chain of Trust.

If foundational security is important to your devices and services, GlobalPlatform secure components enable RoT and deliver additional, unique security, privacy and functionality benefits.

RoT & Chain of Trust – The Foundation of Secure Components

GlobalPlatform's widely adopted specifications enable device manufacturers to embed a standardized and certified security hardware/firmware combination, known as a secure component. GlobalPlatform specifies two types of secure component: a Secure Element and a Trusted Execution Environment. Both of these secure component form factors have the concept of RoT at their core. As such, GlobalPlatform Specifications define how device manufacturers can create a secure RoT which meets the needs of service providers for an accessible, on-device physical 'trust anchor' to protect digital services from fraud and attack.

The organization's Root of Trust Definitions and Requirements document explains how GlobalPlatform-compliant secure components enhance on-device security with additional security services beyond RoT.

GLOBALPLATFORM SECURE COMPONENTS

When secure chip technology is underpinned by a Root of Trust, the resulting platform combined with application management functionalities is called a secure component.

Secure components bring a range of benefits. They provide the isolated and controlled environment required for secure services (such as authentication, confidentiality, identification, attestation, and digital signatures) to be stored, executed and remotely managed. These are all essential for the deployment of value added services.

Root of Trust
+ Hardware Isolation
+ Application Management
SECURE COMPONENT

At present, there are two widely recognized secure components in use around the world – Secure Elements and Trusted Execution Environments – and GlobalPlatform Specifications define the standard for both.

Secure Element

Trusted Execution Environment

When a device features more than one GlobalPlatform secure component, service providers can develop even safer services by combining the security services offered by multiple RoTs. GlobalPlatform also recognizes the need to support the full lifecycle of components and devices as the ownership of devices often needs to be changed due to sale or refurbishment, for example. GlobalPlatform therefore supports the process to securely transfer the ownership of a secure component in a multi-stakeholder environment. This is required when a Secure Element manufacturer passes administration ownership of the component to a device manufacturer or car manufacturer, for example. These additional features offer additional value, beyond RoT, to device manufacturers and service providers.

Let's take a closer look at GlobalPlatform secure components.

SECURE ELEMENT (SE)

More than 22 billion GlobalPlatform certified SEs are already live in the market.

A secure component which comprises autonomous, tamper-resistant hardware within which secure applications and their confidential cryptographic data (e.g. key management) are stored and executed.

Different form factors are available to satisfy different business models and market needs. For example, removable SEs like SIM cards and USB tokens offer flexibility as they can be added to devices once they are in the field. Separately, embedded SEs are soldered into the device, giving manufacturers greater control.

Use Cases:

- Secure storage
- Secure authentication
- Identification
- PIN management
- Signatures

Key Markets:

- Telecoms
- IoT / M2M security
- Financial services
- Enterprise
- Government

Secure Elements offer the highest levels of hardware security but have limited storage and processing power.

TRUSTED EXECUTION ENVIRONMENT (TEE)

More than 1 billion TEE-enabled processors are shipped per quarter.

The TEE is a secure area of the main processor of a connected device that ensures sensitive data is stored, processed and protected in an isolated, trusted environment. The TEE's ability to offer isolated safe execution of authorized security software, known as 'trusted applications', enables it to provide end-point security by enforcing protection, confidentiality, integrity and data access rights.

The TEE offers a level of protection against software attacks, generated in the Rich OS environment. It assists in the control of access rights and houses sensitive applications, which need to be isolated from the Rich OS.

Use Cases:

- Secure storage & processing
- Secure authentication & biometrics
- Secure data entry
- Secured display

Key Markets:

- IoT / M2M security
- Financial services
- Premium content protection
- Enterprise
- Government
- Social media

Let's look at the value GlobalPlatform-certified secure components offer to manufacturers and service providers.

THE VALUE OF SECURE COMPONENTS

Secure components bring value to billions of devices around the world:

- More than 22 billion GlobalPlatform Secure Elements are deployed globally
- 191 secure component products qualified by GlobalPlatform
- GlobalPlatform estimates there were 5 billion TEE-enabled processors worldwide within devices at the end of 2017

Services implemented on GlobalPlatform-certified secure components benefit from:

- **Unique device identity –** RoT is the DNA of secure components, meaning each GlobalPlatform SE or TEE is produced in a controlled environment. This ensures the unicity of its identity and protects the primary credential, safeguarding devices against cloning.
- **Integrity** – Thanks to the RoT at their core, secure components enable secure boot, asset protection and certificate generation, all of which contribute to ensuring the integrity of devices and services.
- **Proven secure storage and protection of digital services** – Any connected device can become a service platform and secure components are already proven to be robust and interoperable across sectors including payment, automotive, IoT, premium content, enterprise and government.
- **Authentication –** Authentication mechanisms and associated credential (ranging from simple to complex ones requiring end-user interaction) between cloud and device or between cloud services and end user can be protected by secure components.
- **Secure and isolated** – The separate execution environment provided by a secure component allows services to be deployed, and trusted apps to run, safely. Only GlobalPlatform enables the isolation of applications with different security requirements running on the same secure component.
- **Remote management –** New applications, updates and upgrades can be remotely loaded into the isolated areas offered by secure components, once a device is already in the field. This ensures device longevity and flexibility for secure services.
- **Combining secure components** – Uniquely, where two GlobalPlatform secure components exist on a device, one can offer security services to the other, enabled by the Chain of Trust.

GlobalPlatform secure components protect a device and its services with a RoT and Chains of Trust. They offer multiple security benefits to device manufacturers and service providers, which are not provided by other security technologies.

FUTURE VISION

Foundational security built in at the core of devices is the only way to effectively protect devices and is less expensive than trying to secure services on insecure devices or dealing with the impact of hacked devices and services.

With hacking, malware and attacks growing in parallel with the increasing connectivity of objects, device manufacturers around the world are already integrating GlobalPlatform-certified secure components to enable RoT and Chain of Trust security for the benefit of their devices and third party services. There is widespread understanding that RoT provides the essential foundation on which to build Chains of Trust and secure services. The additional security functionality offered by GlobalPlatform-certified secure components delivers a proven, seamless and cost-effective way to protect digital services across multiple use cases and vertical markets.

Technologies and requirements are changing rapidly. GlobalPlatform's legacy of successful technical specification development is thanks to two decades of energetic and effective industry collaboration. Members influence the organization's output through participation in technical committees, working groups and strategic task forces. GlobalPlatform technology is developed in collaboration with numerous standards bodies and regional organizations across the world, to ensure continual relevance and timeliness, relative to multiple services, sectors and business models.

GlobalPlatform specifications are today highly regarded as the international standard for enabling digital services and devices to be trusted and securely managed throughout their lifecycle.

ABOUT GLOBALPLATFORM

GlobalPlatform is a non-profit industry association driven by over 100 member companies. Members share a common goal to develop GlobalPlatform's specifications, which are today highly regarded as the international standard for enabling digital services and devices to be trusted and securely managed throughout their lifecycle.

GlobalPlatform protects digital services by standardizing and certifying a security hardware/firmware combination, known as a secure component, which acts as an on-device trust anchor. This facilitates collaboration between service providers and device manufacturers, empowering them to ensure the right level of security within all devices to protect against threats.

GlobalPlatform specifications also standardize the secure management of digital services and devices once deployed in the field. Altogether, GlobalPlatform enables convenient and secure digital service delivery to end users, while supporting privacy, regardless of market sector or device type. Devices secured by GlobalPlatform include connected cars, set top boxes, smart cards, smartphones, tablets, wearables, and other Internet-of-Things (IoT) devices.

The technology's widespread global adoption delivers cost and time-to-market efficiencies to all. Market sectors adopting GlobalPlatform technology include automotive, healthcare, government and enterprise ID, payments, premium content, smart cities, smart home, telecoms, transportation, and utilities.

GlobalPlatform's legacy of successful technical specification development is thanks to two decades of energetic and effective industry collaboration. Members influence the organization's output through participation in technical committees, working groups and strategic task forces. GlobalPlatform technology is developed in collaboration with numerous standards bodies and regional organizations across the world, to ensure continual relevance and timeliness.