GLOBALPLATFORM®

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

An Introduction to GlobalPlatform's Device Trust Architecture

July 2019

 |

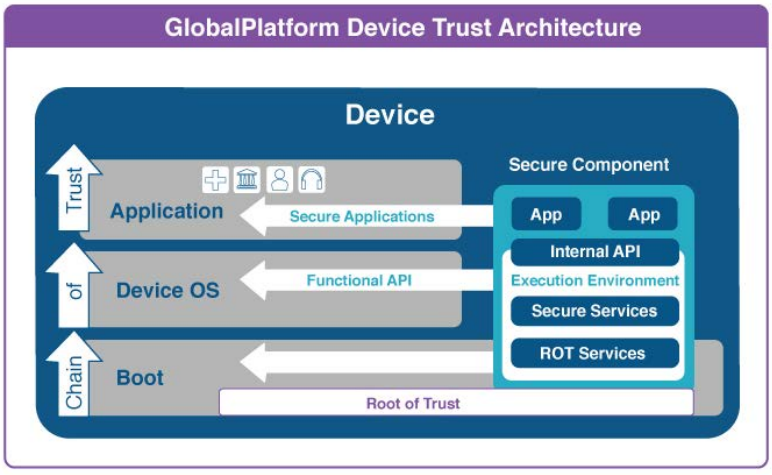
WHY HAS GLOBALPLATFORM CREATED THE DEVICE TRUST ARCHITECTURE?

The connected device landscape is expanding rapidly. New devices and device types – operating at the network edge and in the fog – are being connected to a range of different cloud platforms, new device operating systems are being created and digital services are being developed. Yet not all devices are secure enough to protect against threats and attacks. Considering the sensitive nature of data being gathered and exchanged between many connected devices, the lack of standardized security poses a significant risk across the complete ecosystem.

For digital services to be a success:

- **Service providers** need to trust that the devices which are responsible for gathering and sending back service-related data are fully protected and updatable against future attack threats. It is therefore important to provide assurances that data is generated by a trusted device.
- **Device makers** need to support a range of device OS, securely connect to multiple cloud platform providers and offer a proven level of security services to service providers.
- **Cloud platform providers** need to securely enroll many device types, running a wide range of different secure services. End to end data integrity, from verifiable devices, is fundamental to their business model; big data is useless if you cannot trust the source of that data.

Collaboration between these key stakeholders on securing digital services is a priority; without it, the IoT ecosystem will not realize its full potential and 'big brand' IoT data breaches could become the norm.



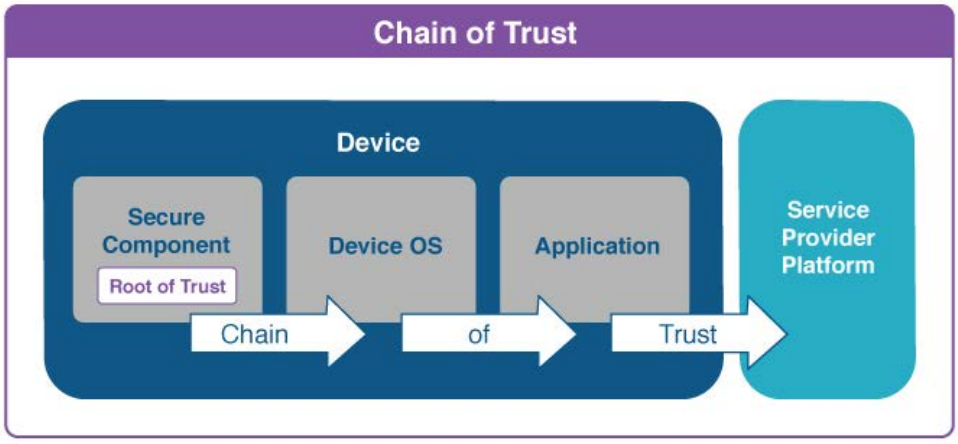
The GlobalPlatform Device Trust Architecture framework enables seamless interaction between stakeholders when deploying secure digital services, regardless of market or device type. The Chain of Trust that it delivers, alongside accompanying attestation capabilities, is key to enabling edge and fog computing to be realized on a mass market scale. In edge computing deployments, the integrity of data and protection of the data source (i.e. end-point device) against attacks is vital to service precision. This is equally applicable to fog computing deployments, where gateway devices play a critical role in the secure transmission of management data from a cloud server to the edge device and vice versa.

DEVICE TRUST ARCHITECTURE: THE TECHNOLOGY

The Device Trust Architecture is a security framework which shows how GlobalPlatform's standardized secure component technology can be used to build an attestable Chain of Trust to protect devices and digital services sitting at and connected to all layers of the Internet of Things (IoT) architecture: in the cloud, the fog and at the network edge. It does this by offering secure services, implemented within a secure component and which can be used at each level of a Chain of Trust: from the boot mechanism, to the device Operating System (OS) and up to the application layer.

A device OS is typically the main OS of the device that runs applications and / or services. In the case of smartphones, it can be an OS such as Android. On other Internet of Things (IoT) devices, examples may include a Linux-based OS or a real-time operating system (RTOS).

In this context, the secure component provides:



- **(Chain of Trust: Step 1) Root of Trust services to the device boot mechanism,** including device identification and attestation services. Since the boot is assisted by the Root of Trust from the secure component, the integrity of the device boot chain process is assured and protection offered against various attacks and infections from malware.

- **(Chain of Trust: Step 2) Secure services to protect the device OS.** A connection between the device OS and the secure component enables the device OS to access highly secure services within the secure component. These can be used to protect the assets of the OS, such as its certificates

and update processes. Application assets, such as data and keys, and end-user authentication also need to be protected. Thanks to the secure component, they too can access the most advanced level of security services.

- **(Chain of Trust: Step 3) Dedicated security services for device applications.** To offer most value-added services (VAS), device applications require more advanced security services that are optimized (in terms of security, performance etc.) and tailored for that particular application (e.g. providing specific algorithms). Dedicated security services can be loaded as needed into a secure component and made accessible to the device applications which require them.

An application hosted in the connected device needs to connect with the Chain of Trust. It is here that the attestation mechanism is applied. Attestation is the process by which an application locally, or a server remotely, requests a status from a trusted anchor within the device. The authenticity of the response provided is then verified (usually through approval by a third party). There are many status examples which may be sought from a device, including device identity and GPS position. When a standardized GlobalPlatform secure component offers the attestation services, multiple claims can be asked and verified about the device user, application, status of applications or OS integrity.

WHY IS A CHAIN OF TRUST NECESSARY?

For Device Manufacturers

In the past decade, many global industries seeking new routes to market have capitalized on the digitalization of services. As consumer and industrial demand continues to drive growth in digital services, an increasing number and choice of devices provide access to digital services. Many of these devices sit at the 'edge' of the connected network i.e. in the hands of end users or collating / delivering data and services in machine to machine use cases. These devices, such as connected cars, set top boxes, smartphones, tablets, wearables, and other IoT devices, are connected to a server in the cloud (for example belonging to a service provider or device manufacturer) which acts as one end point of a two-way management data flow. The edge device is the other end point. This connection can happen either directly (i.e. cloud server to edge device), or indirectly via a gateway, which sits between the cloud server and edge device, in an area known in computing terms as the 'fog'. Fog devices can support an edge device with redistributed computing power, storage, control and networking, at a position closer to the network edge than the cloud server. This can have multiple benefits in terms of latency and optimized usage of processing power for example. Fog devices can also be end points in their own right, connected only to a cloud-based server.

This dynamic landscape creates a very real security challenge. Device manufacturers in the cloud, fog or network edge, must demonstrate that they can offer trusted, secure services which allow their devices to be used confidently by service providers to, for example, run secure applications, manage data securely and deliver digital services to end users.

An established Chain of Trust provides consistency of secure service delivery within a device. It allows device manufacturers to:

- Ensure their devices can be securely enrolled to IoT cloud platforms;
- Provide assurances that their devices can securely support different device OS;
- Enable end to end data privacy / secure communications;

- Manage secure remote updates for device services;
- Protect critical edge calculations;
- Provide device attestation services.

For Digital Service Providers

Digital service providers need to be confident that they can connect their business activities and back end systems with end-point devices which are attestable and therefore trusted. This reassures them that they are interacting with, and serving, the right customers. While the trusted end-point is vital to their service delivery, so too is a secure communication channel between the service provider's server and the end user device. A secure channel enables service providers to confidently use the secure services on the device, such as those which allow them to:

- Enable or update digital services;
- Enroll end users / devices to the service provider platform;
- Authenticate end users;
- Store private data;
- Authenticate data generated by the device, through attestation services if required;
- Protect data generated by the device ahead of data transmission / exchange in the cloud.

For Cloud Platform Providers

In today's connected device ecosystem, the cloud platform provider has become firmly established as an actor which provides a platform that enables end-users and suppliers to interact and / or conduct transactions. There are different examples of this new ecosystem player: for example, app stores (e.g. the App Store, Play Store) for smartphone and tablet applications; online market places for consumers (e.g. Amazon, Alibaba); and IoT cloud platform providers (e.g. Azure, Google, Artik, etc.) for enterprise and M2M applications.

All cloud platform providers need to remotely and securely enroll and manage connected devices; this enables the cloud provider to offer new services and send regular updates. Secure end user and device authentication is also commonly required, to ensure that the provider is interacting with the intended devices and audience. The key requirements of cloud platform providers are:

- **Enrollment.** Complexities arise with device enrollment when the cloud platform provider needs to enroll a variety of devices from heterogeneous domains (e.g. healthcare, energy, home automation etc.) and from different manufacturers. Reliable device enrollment is critical for IoT cloud platform providers across M2M and enterprise use cases. The Chain of Trust established by the GlobalPlatform Device Trust Architecture supports device identification and offers a solution for the secure storage of identity credentials allocated by cloud platform providers.

- **Remote management.** Cloud platform providers must always be able to remotely manage devices. To do this, the devices need to be trusted end-points and they need a secure channel which allows them to engage with the right devices and be sure that their update processes are not compromised.

- **Authentication.** End user and device authentication is required across both consumer and M2M use cases, to allow the correct access to platform services and to ensure non-repudiation. The cloud platform provider needs to use the secure services available on the device for this purpose.

THE ROLE OF GLOBALPLATFORM

GlobalPlatform is a non-profit industry association driven by approximately 90 member companies. Members share a common goal to develop GlobalPlatform 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.

A core focus of GlobalPlatform's work is the standardization and interoperability of application management within secure components, specifically Secure Element (SE) and Trusted Execution Environment (TEE) technology.

To advance the concept of the Device Trust Architecture framework, GlobalPlatform has created a Trusted Platform Services (TPS) Committee, which creates open specifications that:

- Provide mechanisms enabling access to secure services offered by secure components, both from within a device and from platforms external to it.
- Assure the trustworthiness of a secure component within a device enabling a secure service, thanks to a chain of trust, which originates from the RoT and extends to the application or the cloud service.

One of the committee's current priorities is to develop APIs for attestation of device state and services.

THE GLOBALPLATFORM CERTIFICATION (FUNCTIONAL AND SECURITY) SCHEME

GlobalPlatform's work to develop and maintain a certification scheme promotes a collaborative and open ecosystem where digital services and devices can be trusted. Certifying secure components within devices is essential in facilitating collaboration and trust between service providers and device manufacturers.

The certification scheme allows stakeholders to verify product adherence to the association's specifications and configurations.

- **Device manufacturers** that use GlobalPlatform certified secure components can proactively market their products as meeting the needs of digital service providers. They can effectively illustrate that their digital service management capabilities are interoperable and meet industry defined security requirements.

- **Service providers** recognize this level of assurance, which enables them to select a product which matches their security and privacy needs.

GlobalPlatform security certification confirms conformance of Trusted Execution Environment (TEE) products to the Common Criteria recognized GlobalPlatform Protection Profile, through independent security evaluation. It ensures that secure components meet the security levels defined by some industries, enabling service providers to comply with industry requirements and manage risk effectively.

GlobalPlatform functional certification evaluates the functional behavior of a Secure Element (SE) or TEE product against the requirements outlined by GlobalPlatform configurations and associated specifications to achieve market interoperability. Independent testing of this nature provides confirmation that the digital service will perform as intended in the field.

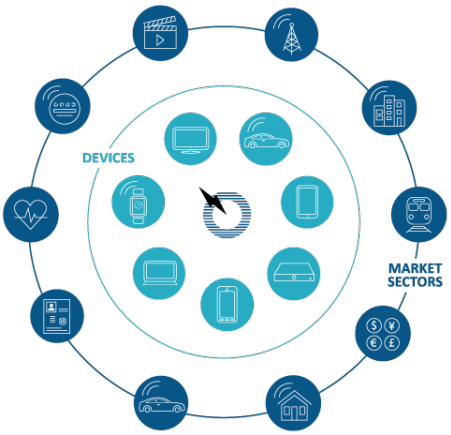
View more information on the GlobalPlatform certification scheme.

To learn more about GlobalPlatform's Device Trust Architecture, educational resources and events, please visit www.globalplatform.org.

ABOUT GLOBALPLATFORM

GlobalPlatform is a non-profit industry association driven by over 85 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.