IoT Device Manufacturers:
Leveraging Standards-based Security to Gain Advantage in a Crowded Marketplace

GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Contents:

Navigating digital security in a connected world: the 21st century frontier

The global connected device landscape is expanding rapidly. Many sectors are capitalizing on the digitalization of services. As a result, our automobiles, homes, cities and industries are increasingly indistinguishable from the internet of things (IoT).

New devices and device types are being connected to a range of different cloud platforms. New device operating systems are being created. New digital services are being developed.

Our world is transforming. Growth in many sectors relies on IoT device manufacturers providing trusted, secure services which allow their devices to be used confidently by service providers and end users. Knowingly or not, IoT device manufacturers have a significant responsibility for securing this ecosystem.

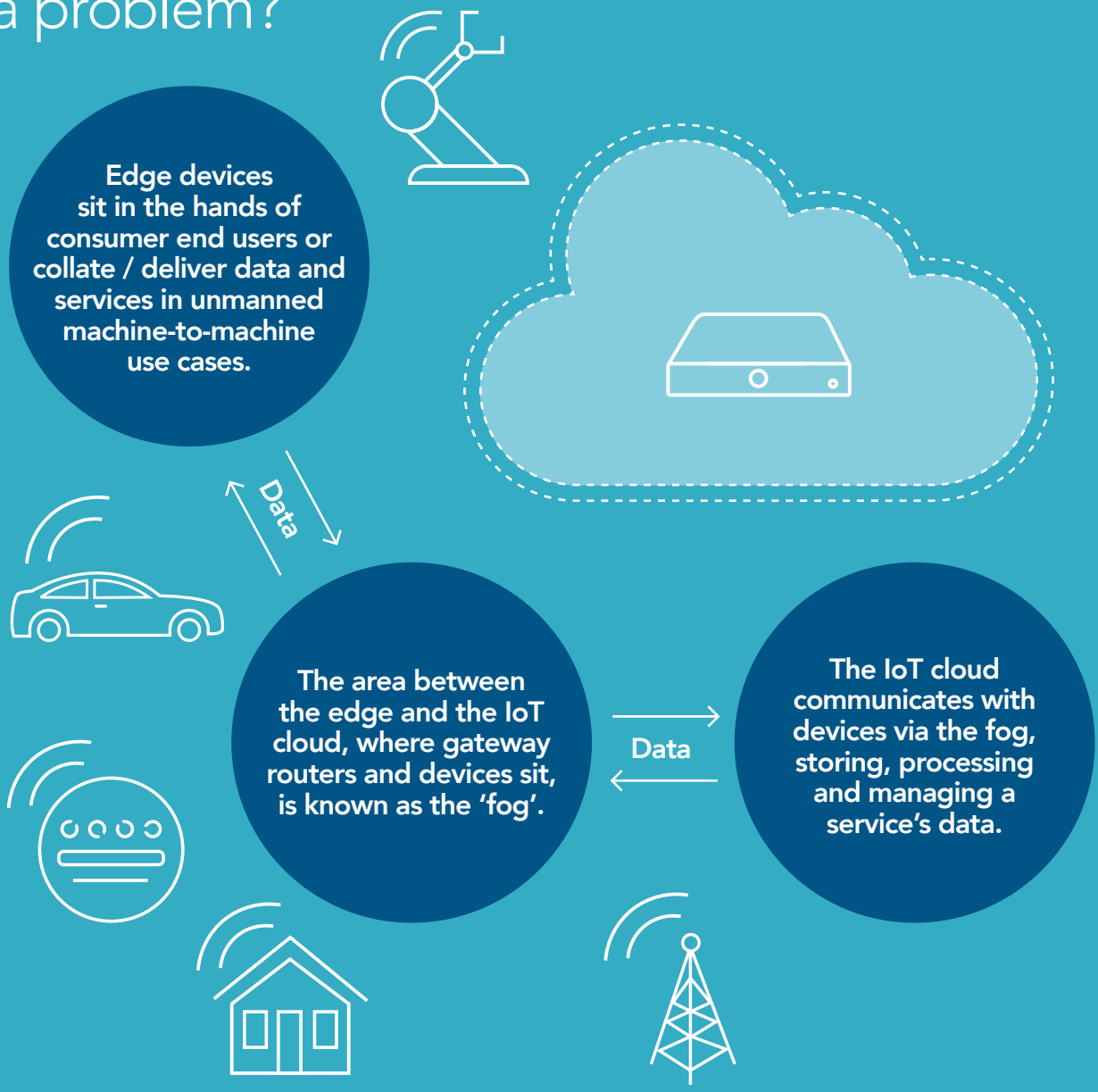
Yet the rapid pace of innovation has its drawbacks. Many connected devices providing access to digital services – from payment-enabled fridges and wearables through to machinery used in manufacturing – have little or no in-built security. This leaves them unprotected against threats and attacks. At the same time, many new IoT device manufacturers, particularly those whose products have traditionally been used without connectivity (e.g. fridges, doorbells, food processors, vending machines) have little or no cybersecurity expertise. When the lack of education among connected service end users on the security risks and precautions is also factored in, the challenge for the industry is plain to see: too many devices are easy to attack, resulting in end users, service providers and device manufacturers being extremely vulnerable. This is evidenced by the 'big brand' IoT data breaches and product launch failures which continue to create headlines around the world on an all-too-frequent basis.

Why are insecure devices a problem?

Many connected devices sit at the 'edge' of the connected network - i.e. in the hands of consumer end users or collating / delivering data and services in unmanned machine-to-machine use cases (where there is no consumer end user). These devices are connected to a server in the cloud that belongs, for example, to a service provider or device manufacturer. This server acts as one end point of a two-way management data flow, where the edge device is the other end point.

The connection between cloud-based server and edge device can happen either directly or indirectly, via a gateway router or device which sits between the cloud server and edge device, in an area called the fog.

This dynamic, crowded landscape creates a very real security challenge. Any device vulnerability within this ecosystem can pose a significant risk to end users, service providers and device manufacturers on multiple levels: privacy breaches, data theft / tampering, unauthorized network access, reputational damage and legal implications, threats to critical infrastructure… the list goes on.



Why secure devices make good business sense for device manufacturers…

By maximizing the appeal and relevance of connected devices to end users, service providers and cloud platform providers, IoT device manufacturers can optimize their market share and credibility. Accordingly, IoT devices should be flexible enough to accommodate the requirements of these different stakeholders who collectively enable digital services to be brought to market. Device flexibility should consider compatibility with different device operating systems (OSs), the varying security requirements of service providers, and the capability to securely connect to multiple cloud platform providers.

For digital services to be a success, trust must be fundamental

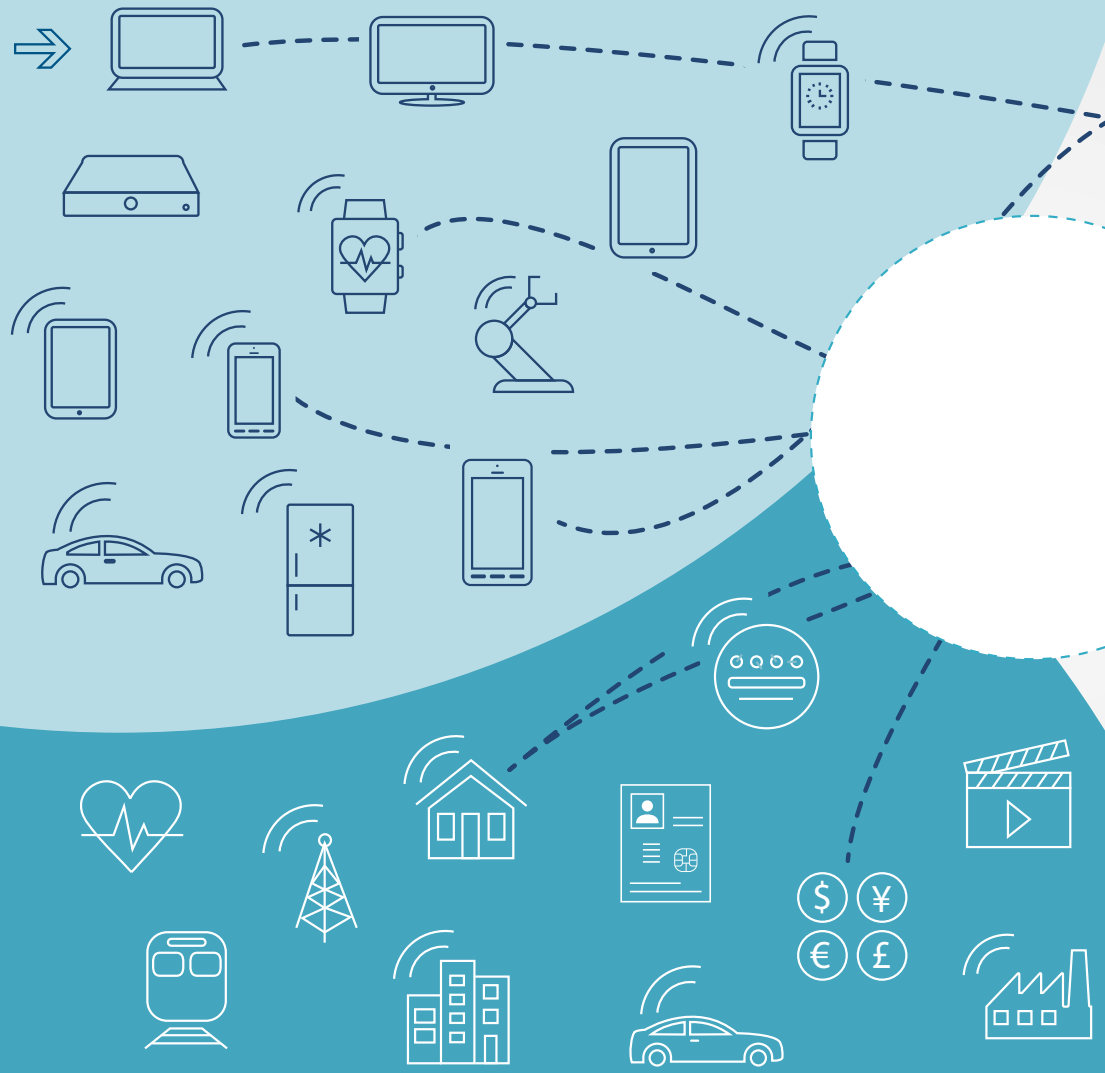
A device OS is typically the main OS of the device that runs applications and/or services. In the case of smartphones, it can be an OS such as Android. On other IoT devices it may be a Linux-based OS or a real-time operating system (RTOS).

Service providers need reassurance that they are engaging with a genuine, authorized end user through a trusted device. Device manufacturers must therefore enable devices authorized to access a service to be identified and authenticated. This allows service providers to confidently anchor their services on a trusted device. Service providers must also be assured that these devices, which gather and send back service-related data, are fully protected and updatable against future attack threats. This delivers confidence that the right customers / devices are receiving the intended service, and, crucially, mitigates the risk of potential reputational damage for the service provider, associated loss of revenues and worst-case scenarios in critical applications.

Equally, device manufacturers need to enable IoT cloud platforms to securely enroll many device types, which may run a wide range of secure services, to their platforms. IoT cloud actors also need to be sure that they are engaging with intended devices and audiences. As such, device identification and verification and end-to-end data integrity are fundamental to their business model - big data is useless if you cannot trust the sources of that data. This is a business-critical consideration.

Device manufacturers (in the cloud, fog or edge) must demonstrate that their devices can be trusted (through authentication) to run applications with varying security requirements, manage data securely and deliver digital services to intended end users on behalf of service providers. This will create confidence and stimulate further growth across the IoT landscape.

Collaboration between device manufacturers, service providers and IoT cloud actors on standardizing securing digital services is a priority. Without it, complexity will rule, and the IoT ecosystem will not realize its full potential.



thingworx
CISCO
aws
Samsung ARTIK Cloud
Alibaba Cloud
ORACLE
PREDIX
Google Cloud
Watson IoT
ThingSpeak
Bosch IoT Suite
Baidu Cloud
Azure
Kaa IoT

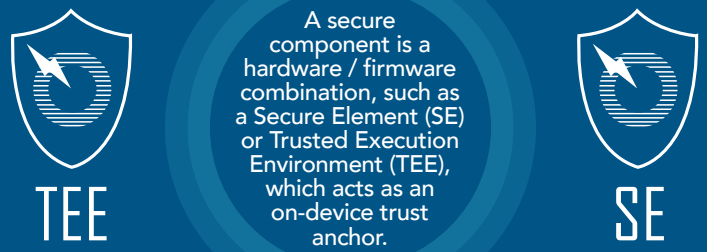
What can device manufacturers do to protect themselves and their customers?

Simple. They can implement standardized, foundational security.

It is only possible to effectively protect devices if they have been designed with security at the core. That's why the Device Trust Architecture (DTA) framework was developed by GlobalPlatform: to give device manufacturers a flexible approach to interact seamlessly with other stakeholders when deploying secure digital services, regardless of security requirements, market or device type.

The DTA framework enables IoT device manufacturers to create trustworthy devices that are flexible enough to accommodate the functional and security needs of different stakeholders within the digital services value chain.

It demonstrates how standardized secure component technology (see definition below) can be used by IoT device manufacturers to protect digital services and devices across all layers of the internet of things – from a tablet, TV or piece of manufacturing equipment at the edge, through a fog server, all the way up to a cloud server.



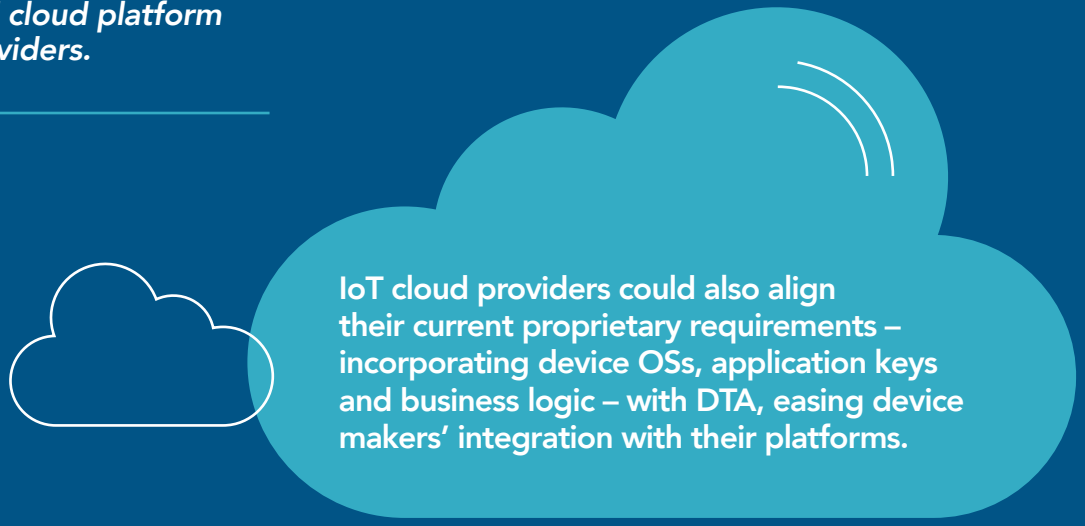
Q. Why is the use of standardized secure components important?

A. Only device manufacturers using standardized SEs and TEEs can proactively market their products as meeting the needs of digital service providers, because only they can effectively illustrate that their digital service management capabilities are flexible enough to meet any industry defined security requirements. Standardized secure components are proven, already deployed at scale internationally, and their specifications are maintained in line with evolving security requirements of different industries and regions. Additionally, standardized secure component technology's widespread global adoption delivers cost and time-to-market efficiencies to all.

Device Trust Architecture explained

DTA is a technical framework that shows device manufacturers how to use standardized secure component technology to meet the varying functional and security requirements of service providers and cloud platform providers.

DTA allows service and cloud platform providers to understand how trust has been created within devices and between authorized devices and remote servers / platforms. It does this by providing a traceable path – also known as a Chain of Trust – from a trust anchor within a device's secure component through to a cloud-based server. This Chain of Trust enables device attestation (see definition below) by the service provider or cloud actor. This gives them confidence that the right end user and device is accessing its services.



IoT cloud providers could also align their current proprietary requirements – incorporating device OSs, application keys and business logic – with DTA, easing device makers' integration with their platforms.

Q. What is attestation, and why is it important?

A. Device 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 can then be 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 location, from active applications in the device. This is important because service providers need reassurance that they are engaging with a genuine, authorized end user through a trusted device.

All stakeholders in the IoT value chain can build secure Chains of Trust when devices are built using the DTA framework.

Learn more about Chains of Trust in *Deploying and Protecting Digital Services with Chains of Trust.*

Closing the loop

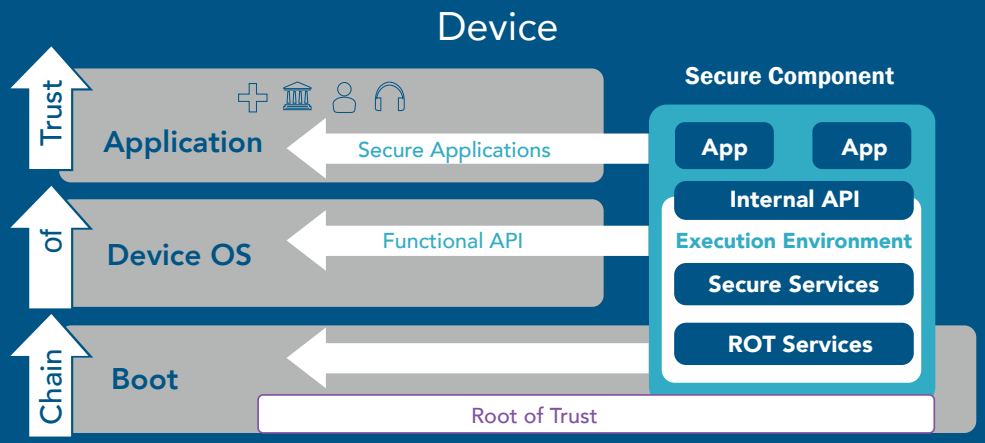
If an IoT device is built using the DTA framework and certified secure components, service providers have the means to create Chains of Trust and IoT cloud actors can use the DTA secure services library to build their own, interoperable security 'recipe'.

Furthermore, device manufacturers using DTA can guarantee consistency of secure service delivery to service providers and IoT cloud actors.

Device Trust Architecture provides the flexibility and security to:

- Ensure that devices can be securely enrolled to multiple IoT cloud platforms;
- Ensure that devices can securely support different device OSs;
- Enable end to end data privacy / secure communications;
- Manage secure remote updates for device services;
- Protect critical edge calculations;
- Provide device attestation services.

GlobalPlatform Device Trust Architecture



This optimizes an IoT device manufacturer's investment and increases profitability by enabling them to address the widest market possible – while protecting them from the reputational damage and financial losses associated with inadequate security.

Ready to delve deeper? Download our *technical introduction to Device Trust Architecture*

The role of GlobalPlatform

GlobalPlatform is a non-profit industry association driven by its 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.

The GlobalPlatform Certification (Functional and Security) Program

GlobalPlatform's work to develop and maintain a certification program 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 program 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.

View more information on GlobalPlatform's certification program.