Introducing IoTOPIA™

GLOBALPLATFORM

A practical implementation guide to secure IoT devices across all markets and in line with global requirements

October 2019

GLOBALPLATFORM®

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Contents:

IOT SECURITY – THE STATE OF PLAY

This eBook offers an introduction to IoTopia, a practical implementation guide to secure IoT devices across all markets and in line with global requirements. Before exploring IoTopia in detail, it is first important to understand the market context of this framework in addition to the legacy of work and expertise within GlobalPlatform that is now being brought to bear for the benefit of the internet of things (IoT) ecosystem.

We are creating a wide variety of devices that connect the world around us, creating the IoT. Many sectors are seeking to capitalize on the digitalization of services and, as a result, there is an explosion in the number of devices being connected to networks.

Various vertical markets are leading this charge – from consumer right through to industrial use cases – and industry projections forecast an even faster adoption of IoT in the coming years.

The total installed base of Internet of Things (IoT) connected devices is projected to amount to

75.44 bn

worldwide by 2025, a fivefold increase in ten years. *(Statista)*

IOT SECURITY – THE STATE OF PLAY cont...

However, serious security concerns need to be addressed to realize the full potential of IoT.

Many of today's connected objects – from sensors and actuators to automobiles and industrial machinery – do more than simply provide information at your fingertips. They can make use of sensitive data, gather information and even impact the physical world, in many cases in critical ways. In light of this, there is a need for ubiquitous and standardized end-point / network security, regardless of the use case, to prevent devices from becoming an entry point into a network or a platform for 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 processor, vending machines) have little or no cyber security expertise. When the lack of understanding among connected service end users on the security risks and precautions is also factored in, the challenge for the industry is plain to see: the attack surface is huge, 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 disappointments which continue to create headlines around the world on an all-too-frequent basis.

Think back to the 2016 Mirai botnet distributed denial-of-service (DDoS) attacks that caused major internet problems worldwide. The botnet was executed using a network that including baby monitors and printers. Reports tracked Mirai at just over 1tbps and there is an upward trend in attack size, with the largest currently on record coming in at 1.7tbps in 2018. But the threat is not just about attacks, hacks also need to be considered and seemingly innocuous devices can offer opportunities.

One great example comes from 2017, where hackers stole 10gb of high-roller data from a Las Vegas casino by attacking a fish tank's connected temperature sensor. Clearly, the theft of personal and corporate data is an issue that needs to be met head on. Every hack and attack can lead to brand damage, loss of customers and sanctions. With the average cost of a data breach in 2019 coming in at €3.9m, the impact on businesses can be catastrophic.

There were 105m cyberattacks on IoT devices in H1 2019.
Seven times higher than H1 2018.

Source: Kaspersky https://www.techradar.com/news/smart-home-devices-are-being-hit-with-more-cyberattacks-than-ever

GLOBALPLATFORM'S EXPERTISE

GlobalPlatform is a non-profit industry association driven by its member companies. Over the last 20 years our members have shared 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 like Secure Elements (SE) and Trusted Execution Environments (TEE).

Standardizing SE

In 1999, payment and ID enabled smart cards were evolving in an unstructured manner – with costly proprietary implementations restricting technical advances and interoperability. GlobalPlatform connected these communities to standardize the development, deployment and in-field management of multiple applications on SEs – including SIMs and embedded SEs – regardless of form factor or device.

This provided significant benefits, offering trust and security, and enabling manufacturers to develop once and deploy across multiple markets. This reduced time to market, and development costs for members and non-members alike. End users now enjoy pioneering, trusted and privacy-assured digital services.

Standardizing TEE

Our proven approach was then embraced by the ever-expanding device market, to standardize the TEE. Facing fragmentation, app developers, device manufacturers and TEE providers endured high development costs and uncertainty over functionality and security, limiting adoption.

Working with all stakeholders, our membership again created a platform for innovation, providing the framework for the TEE to thrive.

GLOBALPLATFORM'S EXPERTISE cont...

Applying This Legacy to IoT

Demand for our member's expertise has never been greater. As the IoT expands, GlobalPlatform has expanded its focus to device security, in addition to secure components. The organization is using its experience to standardize the design, certification, deployment and management of IoT devices. This work will enable the IoT ecosystem to evolve with trust and security at its core and assure that users can effectively manage risk.

The GlobalPlatform Certification (Functional and Security) Program

In addition to its collaborative standardization work, GlobalPlatform develops and maintains a certification program to promote a collaborative and open ecosystem where digital services and devices can be trusted. Certifying secure components within devices, and soon devices themselves, 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.

GlobalPlatform has a long history of successful component and device standardization, which is essential to IoT security. The problem of security is just too big for any one company to solve alone. The GlobalPlatform membership is perfectly placed to go beyond simply defining best practice and help the market to implement security.

INTRODUCING IOTOPIA

Building on GlobalPlatform's existing work to secure the IoT, IoTopia proposes a common framework for standardizing the design, certification, deployment and management of IoT devices. IoTopia device security will be testable and meet vertical market requirements by building upon the following four foundational pillars: secure by design; device intent; autonomous, scalable and secure onboarding; and device life-cycle management.

It is a detailed but executable framework that is standards-based, industry-wide and able to evolve as security capabilities and requirements change. IoTopia also enables device makers to build in line with a consolidated set of parameters by mapping to the leading global guidelines and regulations, and support tiers of security as well as certification in desired verticals.

IoTopia will:

- Deliver a common, cross industry IoT security framework with set baseline references and standards-based approaches across the four pillars.
- Drive industry support, adoption and continued development of the IoTopia pillars.
- Engage & represent the entire IoT ecosystem: chip vendors, device manufacturers, thing makers, IoT platform providers, system integrators, service providers, certification labs, network vendors, end users, government bodies and policy makers.
- Give device makers a blueprint for how to build secure devices without having to become cybersecurity companies or experts.
- Ensure that compliance with the baseline requires low to no additional costs for device makers.

GlobalPlatform invites and welcomes contributions from chip vendors, device manufacturers, thing makers, IoT platform providers, system integrators, service providers, certification labs, network vendors, end users, government bodies and policy makers

THE FOUR PILLARS OF IOTOPIA

IoTopia is built upon four foundational pillars. Each pillar represents a fundamental element in the secure design, development, deployment, certification and management of secure IoT devices and services.

1

Secure by Design

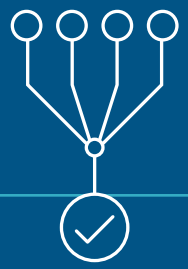
Specific, detailed capabilities and features that go beyond best practice and define how secure components and APIs can be used with existing secure by design standards. GlobalPlatform is working in collaboration with existing certification labs to focus on driving industry adoption.

2

Device Intent

What is this thing? Who is responsible for it? How do I protect it and my business? Is it behaving as it should? IoTopia leverages IETF's manufacturer usage descriptions (MUD) and uniform resource identifier (URI) to effectively manage device permissions and access on networks.

3



Autonomous, Scalable, Secure Onboarding for IoT Devices

IoTopia will offer an open, standards-based secure onboarding process to streamline network administration. This standards-based secure on-boarding process will help solve problems for network administrators, streamlining the process of onboarding the many and varying types of things that need to connect to their networks.

4

Device Lifecycle Management

Software, firmware and hardware patching and updates, update tracking, end-of-life support/service, etc. to effectively manage devices throughout their entire lifecycle, including updates and maintenance to services, in line with international regulations. This will help device manufacturers, device owners, network vendors and IT staff to implement product end-of-life.

LEADING THE WAY

IoTopia's goal is to give the ecosystem the standards-based approach to IoT security implementation that it badly needs.

To lead this work, GlobalPlatform has created an IoTopia technical committee which is open to Full and Participating GlobalPlatform members. Key industry stakeholders and beneficiaries will include chip vendors, device manufacturers, thing makers, IoT platform providers, system integrators, service providers, certification labs, network vendors, end users, government bodies and policy makers.

GlobalPlatform is working to represent and support the entire IoT ecosystem and therefore invites and welcomes contributions to this work.

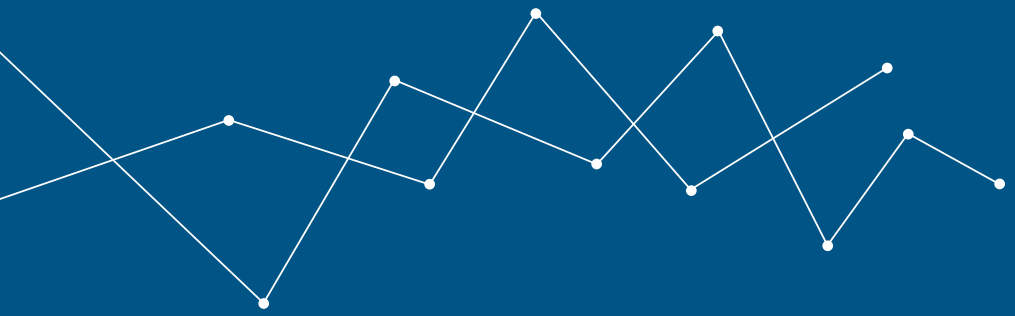
Get involved!

ABOUT US

View more information visit globalplatform.org

GlobalPlatform is a non-profit industry association driven by approximately 90 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 adequate 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 smartphones, tablets, set top boxes, wearables, connected cars, other internet of things (IoT) devices and smart cards.

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

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.