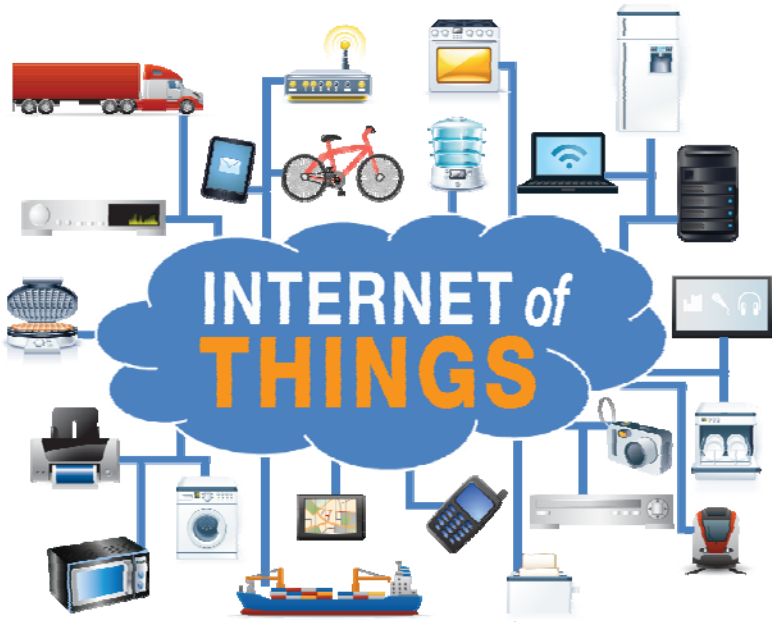
GLOBALPLATFORM®

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

Leveraging GlobalPlatform to Improve Security and Privacy in the Internet-of-Things

Whitepaper
May 2014



secretariat@globalplatform.org | www.globalplatform.org |

Table of Contents

About GlobalPlatform

GlobalPlatform is a cross industry, not-for-profit association that identifies, develops and publishes specifications to facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. Its proven technical specifications are regarded as *the* international industry standard for building a trusted end-to-end solution which serves multiple actors and supports several business models.

The freely available specifications provide the foundation for market convergence and innovative new cross-sector partnerships. The technology has been adopted globally across finance, mobile/telecom, government, healthcare, retail and transit sectors. GlobalPlatform also supports an open compliance program ecosystem to ensure the long-term interoperability of secure chip technology.

As a member-driven association with cross-market representation from all world continents, GlobalPlatform membership is open to any organization operating within this landscape. Its 100+ members contribute to technical committees and market-led task forces.
www.globalplatform.org

PUBLICATION ACKNOWLEDGEMENTS

GlobalPlatform wishes to thank all members of the Internet of Things Task Force, which helped to shape the vision for GlobalPlatform's Internet-of-Things whitepaper. Special thanks go out to the following GlobalPlatform members and their respective organizations:

Full Members:

Göran Selander – Ericsson
Francois Ennesser – Gemalto
Frank Goschenhofer – Giesecke & Devrient
Markus Streets – Good Technologies
Sebastian Hans – Oracle
Jouni Korhonen – Broadcom
John McDonald – American Express

GlobalPlatform Team Members:

Alliances Management – Operations Secretariat
Gil Bernabeu – GlobalPlatform Technical Director
Kevin Gillick – Executive Director of GlobalPlatform

INTENDED AUDIENCE

This document is intended for professionals interested in the way that industries such as health care, automotive, and energy are increasingly making use of embedded technologies that allow for new forms of secure communication and data transmission. The intended reader includes product managers, business development personnel, or system integrators who have an interest in understanding the potential use cases—and related security concerns—that result from these connected devices.

While this is not a technical document, it is expected that the reader has a general familiarity with the specifications developed by GlobalPlatform.

EXECUTIVE SUMMARY

The *Internet-of-Things* (IoT)—often also called *Machine to Machine* (M2M) communications—refers to the increasing trend for devices to be connected to the Internet. It is noteworthy that though such devices are proliferating, this market is still in its infancy.

Today's automobiles, medical devices, home technologies, and other devices contain sensors capable of gathering information and actuators capable of impacting the physical world. Embedding computing devices into such products may change the way that those products are manufactured and managed, as well as the services that are offered to consumers. These Internet-connected devices enable entirely new services to be offered to the consumer.

As the number of devices proliferates, entirely new categories of services will be possible. Yet, the proliferation of such devices and services creates a new set of privacy and security concerns: just as consumers will want to ensure that their personal and usage data are not misused, any number of stakeholders—including Device Manufacturers, Service Providers, Service Subscribers, Network Providers, and others—will want to ensure that their data are protected and that services are securely delivered.

For the Internet-of-Things to be successful, GlobalPlatform believes that a number of principles are important. First, IoT Devices must support a multi-actor environment that allows for different security and access settings for each stakeholder. Second, each Service Provider should be able to remotely manage its own security parameters or appoint an authorized party to act on its behalf. Next, it must be possible to add services or Service Providers to a device after it is deployed in the field; similarly, a Service Subscriber must be able to change Service Providers. And, critically, all security measures must be sufficiently robust and flexible to support a device's deployed lifetime, which in some instances may exceed twenty years.

GlobalPlatform specifications offer several features that, if properly leveraged, address the privacy and security concerns in the IoT market:

- The Secure Element (SE), a separate chip hardened against physical and logical attacks, enables secure hosting of applications for various stakeholders.
- The Security Domain (SD) stores cryptographic content for a stakeholder on the Secure Element and provides mechanisms to manage such content and establish secure communications with external entities.
- The Trusted Service Manager (TSM) is a third party broker that establishes business agreements and technical relationships between different stakeholders in a service delivery.
- The Controlling Authority (CA) allows for confidential post-issuance introduction of new stakeholders onto a Secure Element.
- The Trusted Execution Environment (TEE) is a secure area residing on a mobile device that ensures that sensitive data is safely stored, processed, and protected in a trusted environment on that device.

In addition, there are several security features, such as key derivation, transport mechanisms, and communication protocols that function in the background to protect the stakeholders and enable the introduction of additional services.

This whitepaper seeks to educate the market on ways that these security features, which already exist today in GlobalPlatform specifications, can enhance security and privacy for the Internet-of-Things. GlobalPlatform welcomes feedback on this whitepaper and is interested in collaborating with others to further enhance GlobalPlatform technology for the Internet-of-Things.

INTRODUCTION: HOW TECHNOLOGY & CONNECTIVITY ARE REVOLUTIONIZING COMMERCE

At the beginning of the 2013 U.S. holiday shopping season, Amazon CEO Jeff Bezos generated skepticism—and criticism—by suggesting that future deliveries could come via unmanned drones. Opponents expressed concerns about battery life, accuracy, safety, and privacy. However, one need not look to the distant future to see how technology is revolutionizing commerce. Today, in industry after industry, unattended computing devices are being introduced in a wide range of environments. As these embedded devices proliferate, there is an increasing awareness about the need to manage them in a secure manner.

Consider just a few examples where connected computing devices are changing the very nature of their respective industries:

- **Automotive** – Today's automobiles contain an abundance of connected embedded computers that host diagnostic information about a car's performance, service, and usage.[1] This information needs to be protected and securely managed by different stakeholders (including car manufacturers, service garages, car owners, and more).

- **Healthcare** – Medical devices routinely transmit data wirelessly. In many instances today, a patient's medical records can be automatically updated by monitoring devices—and those records subsequently shared with another physician.[2]

- **Utilities** – Utilities routinely transmit residential or commercial usage information and dynamically update pricing parameters. New smart metering devices can host services from multiple service providers and even the end user.[3]

These examples illustrate the way in which devices are no longer static in nature, but rather, require management and maintenance after initial deployment. They show how additional usage information can be gathered to inform the service provider, customer, or other party. And, they make possible an entirely new set of services that rely on information transfer between connected devices, customer, service provider, and other stakeholders.

This trend will only continue, and there will be countless profit opportunities for companies that leverage these embedded devices to deliver new and exciting services in established industries. However, along with opportunity comes challenges, the most obvious being the security of the services and of users' information. The benefits of change will thus be balanced by the concern for security and privacy, and thus, there is a need for technologies that enable new services without sacrificing the security that is demanded.

---

[1] An entire book could be written on the evolution of electronics and computing in automobiles, but suffice it to say that the proliferation has mostly happened in the past fifty years. Volkswagen is typically credited with the first onboard computer (1969), but onboard diagnostics did not become commonplace until the 1980s. Since that time, systems have become increasingly sophisticated and complex. For reference, see http://en.wikipedia.org/wiki/On-board_diagnostics. Accessed 6 November 2013.

[2] Remote patient monitoring is an especially vibrant topic within the medical industry today. Businesses are navigating the regulatory, security, and financial requirements to develop technologies that allow for remote patient monitoring. See, for reference, "Remote Patient Monitoring," Information Week. Accessed 6 November 2013. http://www.informationweek.com/healthcare/mobile-wireless/remote-patient-monitoring-9-promising-te/240159160.

[3] Countless examples of "Smart Meter" deployments exist around the world. See, for example, http://en.wikipedia.org/wiki/Smart_meter. Accessed 6 November 2013.

SECTION 1: DEFINING THE "INTERNET-OF-THINGS"

The *Internet-of-Things*[4] (IoT) refers to "uniquely identifiable objects and their virtual representations in an Internet-like structure."[5] The "things" in the IoT are tangible assets that communicate with other entities. These so-called *IoT Devices*[6] interact with each other to perform measurements (sensors) or to make an impact (actuators) in the physical world. A key feature of IoT Devices is that there need not be any human actor involved in the communication between devices. For certain use cases, there is a need for a gateway or proxy to perform services for a set of IoT Devices. This includes connecting IoT Devices to the Internet or performing security services on their behalf. We call these *IoT Gateways*.

Market intelligence company IDC has predicted that, in 2014, "we will see new partnerships among IT vendors, service providers, and semiconductor vendors that will address this market." IDC estimates that, by 2020, the world will have *thirty billion* IoT Devices.[7]

While the introduction referenced this trend in the automotive, healthcare, and utility industries, there are abundant examples, including (but not limited to) the following:

- Asset and cargo tracking systems
- Building and home automation systems that measure and control indoor environments
- Control and monitoring systems in utility networks (gas, water, electricity, etc.)
- Smart meters that measure utility consumption
- Industrial metering appliances that measure physical and chemical quantities
- Medical sensors for remote diagnostics
- Onboard diagnostic systems in automobiles
- Vending machines and point-of-sale terminals
- Weather and traffic monitoring
- Vehicle-to-vehicle communication and vehicle-to-smart city communication

Thus, the things in the IoT require connected sensor and actuator devices. These devices, in turn, use various networking technologies to communicate with one another. The devices and services built around them provide knowledge and control of physical assets, and this in turn opens up an entirely new set of potential services desirable to multiple parties involved in the ecosystem.

The quality and dependability of the service, however, depend heavily on the security and assurance that these devices provide. One approach to fulfill these objectives is to employ devices that support a secure environment for the execution of applications, storage, and use of cryptographic keys. GlobalPlatform provides several options—such as the Secure Element (SE) and Trusted Execution Environment (TEE)—for achieving a secure execution environment. Devices with such a secure execution environment and that are connected to the Internet are the main focus of this whitepaper.

1.1 Generic Features of IoT Devices

[4] *Machine to Machine* (M2M) is a similar term, which refers to wireless and wired devices that communicate with one another. For the purposes of this paper, *Internet-of-Things* and *Machine to Machine* are interchangeable terms.
[5] Source: http://en.wikipedia.org/wiki/Internet_of_Things. Accessed 6 November 2013.
[6] IoT Devices are also known as M2M Devices, where M2M stands for *Machine to Machine*.
[7] "IDC: Top 10 Technology Predictions for 2014." *Forbes*. http://www.forbes.com/sites/gilpress/2013/12/03/idc-top-10-technology-predictions-for-2014/. Accessed 9 December 2013.

Although the scope of possible services in the IoT field is vast and the variety of devices is large, there are common generic characteristics that apply to many IoT deployments:

- Constrained Computing Power & Resources
- Long Service Lifetime
- Unattended Operation
- Ubiquitous Installations

Devices may fall into different classes:

- Devices that measure physical properties (sensors)
- Devices that influence or modify their environment (actuators)
- Devices (such as computing infrastructures) that process data from sensors (such as translation, conversion, correlation, analysis, or aggregation of information) for further usage (processors)
- Devices that do two or more of the above tasks

These characteristics open up an exciting set of prospective use cases, but they also create challenges. Device manufacturers and service providers must adapt to—and will be impacted by—the increased level of communication and data transfer inherent to these devices. From the consumer's perspective, the communication with these devices should be transparent.

1.2 Roles in the IoT

Historically, devices were manufactured and distributed to service providers, who in turn deployed the devices to the consumer. There was very little interaction between these parties, and the devices and services were static in nature. Namely, there were no post-deployment software updates or service modifications. The devices had little or no communication links with other systems, backend systems, or other devices.

In the IoT, however, there is a much wider range of actors, and a considerable amount of interplay between them. Each of the following will be discussed later in the document, but introducing them here helps to underscore the complexity of an IoT deployment and the associated security and other concerns:

IoT Service Provider (SP) – This is the party responsible for providing a generic IoT Service infrastructure on which IoT applications rely. Such a service may include, for example, cloud-based data storage and analysis capabilities acting on the IoT sensor data. An IoT Device may be subscribed to one or multiple IoT Service Providers.

IoT Application Provider (AP) – This is the party providing specific IoT applications, such as a device tracking application or a traffic management application for automobiles. There may be multiple IoT Applications, each with a different AP, on a single device.

IoT Service Subscriber (SS) – This is the entity that has a contract with an IoT Service Provider for an IoT Service. This could be the consumer, or it could be a manufacturer of a machine that is, for example, using an IoT Device to obtain usage information or maintain the machine.

Network Provider (NP) – This party—typically a Mobile Network Operator (MNO) or Internet Service Provider (ISP)—provides Wide Area Network (WAN) access to the IoT Device. In other words, the NP enables communication.

Network Subscriber (NS) – This is the party that has a contract with the IoT Network Provider for WAN access for the IoT Device. This could be the consumer, or it could be an SP.

Device Manufacturer (DM) – This is the manufacturer of the IoT Device. The Device Manufacturer is responsible for integrating the Secure Element (SE) and/or the Trusted Execution Environment (TEE) into the device.

In addition to these roles, there are others (to be introduced later) that are necessitated by security, privacy, and other concerns. What is critical to understand is that, in the IoT, since there are potentially many roles and stakeholders that could interact years after initial deployment, there is a need to ensure that relevant information and other assets are protected and can be managed throughout the lifetime of the device.

1.3 Security and Privacy

The demand for security and privacy is dependent on market, regulatory, and user expectations. IoT Devices are used in the context of critical infrastructure or potentially dangerous systems, such as transportation systems, water pumps, electric substations, and medical devices. Additional risks come from the fact that the technology is interacting with the physical world around us (potentially impacting our safety), and thus unattended devices such as electricity meters potentially expose private data about our life and environment without our awareness.

ABI Research suggests that the entire trend toward IoT Devices and services "risks being thwarted by the growing security concerns." To avoid this, the authors suggest that, "Significant efforts need to be invested into M2M application security in order for the M2M market to fully evolve. Whether this is through open source initiatives or standards development, the demand for increased M2M application security will have to be answered, and sooner rather than later."[8]

IoT Devices and IoT Gateways need to implement security measures to meet the requirements and counter the specific threats of the service they are enabling or delivering. Consider the following issues:

- Unattended devices may require an environment for secure storage and execution to perform sensitive operations;
- For devices with long lifetimes it is important to select cryptographic algorithms and key sizes accordingly to anticipate the predicted increase in computing power over the device's lifetime; and
- Given advances in cryptoanalysis, it is desirable to include mechanisms to replace keys and algorithms if necessary, which calls for security mechanisms to remotely manage sensitive data and code (device firmware).

1.4 Connectivity and Communication

Long product lifecycles and battery powered devices require communication protocols designed to reduce power consumption during transmission, and those communication protocols need to be secured, which further impacts the power consumption of the device. For certain devices, wireless communication is the most significant energy cost of the device. Thus, the IoT communication infrastructure needs to be able to manage access to devices that are sleeping

[8] "M2M Dream Challenged by Alarming Security Concerns." *ABI Research.* https://www.abiresearch.com/press/m2m-dream-challenged-by-alarming-security-concerns. Accessed 9 December 2013.

most of the time and therefore not reachable until they are scheduled to wake up or receive a wake-up trigger.

This is especially important for devices that are deployed in diverse environments where no specific communication security can be assumed. In these instances, the device and application need to provide appropriate security regardless of which communication technology is available—Powerline communication, fixed line telecommunications, or cellular or satellite communications. Other standardization organizations, such as Internet Engineering Task Force (IETF) and Open Mobile Alliance (OMA), are in the process of defining protocols that support communication and management in constrained environments.

1.5 Provisioning and Management

For a service to remain operational throughout long lifetimes, it must be possible to efficiently patch, update, reconfigure, change data, or update software on the IoT Device.

Since most IoT Devices cannot be efficiently managed onsite, there is a need for robust mechanisms for remote management. These mechanisms must adhere to the security properties discussed in Section 1.3.

In order to manage the device remotely and securely, there must be some cryptographic keys in place. The process of equipping a device within a network for a new service is known as *provisioning*.

In this system there are multiple actors—such as device manufacturers, network operator(s), service provider(s), and application providers. These stakeholders are all involved in the provisioning of IoT Devices and services, and need to be represented on the device by their corresponding credentials.

SECTION 2: SERVICE DELIVERY REQUIREMENTS

The previous sections illustrated how IoT services require the capability to handle (among other things) large quantities of devices, constrained devices, long deployment lifetimes, and post-deployment management.

But, the need also extends to service providers, manufacturers, and other actors in the IoT service delivery process. Two service providers with proprietary information on the same device will insist that this data not be shared with a competitor. Device Manufacturers may or may not be allowed access to customer or service provider information. And, there are additional actors whose rights must be established, monitored, and reviewed.

What is critical to understand, however, is that *no two IoT services will be identical*. For this reason, the technologies implemented to enable new service delivery and ensure security must be flexible enough to accommodate different business models and different requirements for sharing information. IoT security models must thus be able to accommodate a wide range of deployments.

With this in mind, GlobalPlatform believes that the following principles are important when developing the technologies of IoT Devices and associated service delivery:

- IoT Devices (or IoT Gateways) must support a multi-actor environment that allows for different security and access settings for each actor. The ability to give each actor exclusive access to a particular, and secured, domain on the Device ensures that confidential data can remain so.

- Each Service Provider should be able to remotely manage its own security parameters or appoint authorized parties to manage these parameters on its behalf. This requires built-in functionality in the IoT Device/Gateway, and it will provide each SP the necessary confidence that its information will be kept independent of other Service Providers.[9]
- Since Service Providers may not be defined at the time a Device is manufactured, installing a new Service Provider must be possible during initial deployment—or, even after the Device has been deployed in the field.
- A Service Subscriber should be able to change Service Providers, provided this is supported by the contract.[10]
- IoT Devices and Gateways must allow for the involvement of third parties, which consumers, Service Providers, manufacturers, or other actors may wish to leverage in a deployment and service delivery process. As an example, a manufacturer need not be required to become an expert in service delivery, but rather, should be able to outsource long-term device and security management to a third party that specializes in provisioning services.
- All cryptographic algorithms, protocols and key sizes must be sufficiently secure over the anticipated lifetime of an IoT Device.[11] Note that when devices are physically accessible to potential attackers, which is the case of most unattended objects, hardware protection is required to protect credentials and their manipulations in the device.

SECTION 3: THE SECURE ELEMENT & OTHER GLOBALPLATFORM ASSETS

GlobalPlatform has produced several specifications that, while not produced with IoT specifically in mind, have concepts that are relevant to IoT deployments. The purpose in this section is to understand these definitions as they exist today—and to extrapolate to potential future uses for IoT deployments. Sections 3.1 – 3.4 describe features specified by GlobalPlatform while Sections 3.5 – 3.9 discuss applications of GlobalPlatform features.

3.1 The Secure Element

GlobalPlatform defines a Secure Element (SE), which is a removable or non-removable semiconductor device. These are often used in the form factor of a SIM/UICC card, a generic smart card, or a solderable secure device. The very nature of an SE enables it to securely host applications and their sensitive data on behalf of the relevant stakeholders (e.g. Service Providers and Application Providers).

Conceptually, the SE adheres to the outlined principles necessary to make IoT deployments successful. It is designed to allow different actors to participate, to protect stakeholder data and ensure that it is shared only with trusted parties, to allow for remote and post-issuance secure management (including subscription assets), and to allow for third party participation.

The Secure Element can be managed directly, but it can also be managed with the help of a third party, such as the Trusted Service Manager (TSM). This, as explained in the next section,

[9] Note that in this way there is no need for a single party to have all information related to the service, which would have privacy implications.
[10] Consider, for example, that the European Union Universal Service Directive requires subscription data (identity and keys) in devices to be exchangeable in the field when a Subscriber changes Provider.
[11] Information about minimum requirements on cryptographic mechanisms and key sizes is available in documents like NIST SP 800-131A and SP 800-57. SP 800-57 part 1, table 4 provides information for the time period until 2030.

would be desirable in the event that several IoT Service Providers want to make remote updates to their content and applications.

With the introduction of the SE, two new roles emerge:

Secure Element Supplier (SES) – This party provides the SE Issuer, Trusted Service Manager, or other party with the necessary initial credentials for managing the SE.

Secure Element Issuer (SEI) – This party has the ultimate responsibility for the SE and therefore retains far-reaching privileges. The SE Issuer has the keys to the Issuer Security Domain (ISD), through which it enacts its privileges on the SE.

3.2 The Security Domain

The GlobalPlatform Card Specification defines the concept of the Security Domain (SD), which represents a stakeholder on the SE. It stores credentials for the stakeholder and provides mechanisms to securely manage both the SE content and the SE, including management of these credentials and establishment of secure channels to allow for secure data transfer.

The Security Domain is an application on the SE with special privileges to manage the card content; in a traditional "smart card" (e.g. SIM card or credit card) deployment, only the card issuer would have a Security Domain on the card. However, there are mechanisms in place to allow for more than one actor to have a Security Domain. This would allow for multiple stakeholders in an IoT context to have their own secure applications and associated data stored on the same device while ensuring that, because each is operating within a Security Domain, the applications and data being transferred are kept confidential. Each owner of a Security Domain can provide its own cryptographic services within the Security Domain.

Security Domains can be established in hierarchies, with different privileges. Because creating a thriving IoT business ecosystem requires multiple stakeholders to be present on the SE and to act independently, leveraging Security Domains to enable different stakeholders to assume relevant roles with associated privileges is a natural extension of their current use.

3.3 Trusted Service Manager & Controlling Authority

Central to the GlobalPlatform messaging specification is the concept of a Trusted Service Manager[12] (TSM), which is a trusted broker that establishes business agreements and technical relationships between different actors in a service delivery environment. The TSM performs Card Content Management operations on the SE, which include loading application code, installing, and deleting applications; it also installs and deletes Security Domains and more on behalf of another party. Currently a TSM often operates in the mobile communications market to establish relationship between, for example, mobile network operators, mobile phone manufacturers, service providers such as payment institutions, or other actors on a mobile phone.

In an IoT context, the TSM could help to establish relationships between the IoT Device Manufacturer, IoT Service and Application Providers, the consumer, and other actors.

GlobalPlatform has also defined the concept of a Controlling Authority[13] (CA), which allows for confidential post-issuance introduction of new actors onto a Secure Element. The CA supports creation of confidential keys for newly created Security Domains on behalf of another party. This flexibility allows for new Service Providers or others to be introduced without having to rely on untrusted entities such as an SE owner or another party for service confidentiality.

[12] See the GlobalPlatform System Messaging Specification for Management of Mobile-NFC Services.
[13] See the GlobalPlatform Card Confidential Card Content Management Card Specification v2.2 – Amendment A.

3.4 The Trusted Execution Environment

The Trusted Execution Environment (TEE) is, in a sense, a complement to the SE. It is a secure area that resides in the main processor of a smart phone (or any communicating device) and ensures that sensitive data is stored, processed and protected in a trusted environment. The TEE's ability to offer safe execution of authorized software, known as trusted applications, enables it to provide end-to-end security by enforcing protection, confidentiality, integrity, and data access rights.

3.5 Provisioning of Credentials

For IoT Devices to access an IoT service infrastructure, a cryptographic key must first be established between the device and the infrastructure. IoT applications often need to provision their own application credentials into communicating devices.

Provisioning is common in certain markets, such as secure payment or mobile telephony. However, IoT Devices may be unique to a particular market or application, and there may not be a pre-existing trust relationship between the device manufacturers and IoT Service or Application Providers. GlobalPlatform enables trusted SE issuers to pre-provision credentials into IoT Devices while preserving confidentiality for various stakeholders.

Important to note is that the IoT includes applications for which pre-provisioning of cryptographic keys at manufacturing may be impossible because it is not known which service or network provider will be involved or where the device will be deployed. Furthermore, a large number of today's M2M applications, such as energy or transportation, have costly infrastructures that require long equipment lifetime and development lifecycles that are not aligned with the quick pace of telecommunications or information technology. Accordingly, it is important to be able to remotely update and add new security credentials during the device deployment phase. GlobalPlatform's flexible security model and secure remote administration capabilities provide an important avenue to do just that.

3.6 Key Derivation

To enable secure communication between an IoT Device and another entity, cryptographic keys for authentication and protection of the communication channel need to be established. To handle issues related to frequent use of a long-lifetime master key and to mitigate risks of device compromise, security best practices call for confining a "master key" or "base key" to a secure storage, such as the SE, and using the SE to derive a short lifetime "session key" that is made available to the device by the SE. The communication channel can thus be protected using the session key. This enables the master key to be well protected at all times from all actors.

Because a GlobalPlatform-enabled SE can support multiple Security Domains for different service providers, each can contain its master keys, sensitive data, and key derivation algorithms, and each Security Domain can be securely separated from others on the SE.

This fits nicely with the need in an IoT deployment for multiple actors to be able to secure their data and exchange it as needed with other entities. For example, consider an application in the device running an IoT-related service that needs to establish an application-specific security context to securely communicate with a network node. The application could be installed on the SE (on which the master key is securely stored), and a session key is derived for this particular IoT service.

3.7 Transport Mechanism

GlobalPlatform's specifications also address integration into remote management architecture. GlobalPlatform has always followed a basic design principle of being independent from the underlying network architecture, defining management commands, and keeping the security

for these commands independent from the actual transport protocol. Today GlobalPlatform supports the management of Secure Elements utilizing both IP and cellular networks.

3.8 Communication Protocol

In order to remotely manage the IoT service-related data and applications on the SE, appropriate secure communication protocols need to be in place.

GlobalPlatform has developed two different specifications, "Amendment B" and "Network Framework," to provide a mechanism to remotely manage Secure Elements over an IP network. Both are based on the basic client-server architecture inherent to the HTTP protocol and implement a RESTful[14] API for the management of SEs.

3.9 Compliance Testing and Security Evaluation

In GlobalPlatform's current multi-actor/multi-application environments, compliance testing plays an important role. GlobalPlatform offers compliance programs that certify compliance of Secure Elements, devices, and server products to a well-defined set of GlobalPlatform specifications for certain market segments (such as Finance and for contactless UICCs).

Compliance testing will be even more important in the IoT environment, where service or application providers cannot be assumed to have a business relationship with manufacturers of IoT Devices and associated Secure Elements. Processes similar to those currently followed by GlobalPlatform will need to be established for the IoT market to ensure compliance and security.

SECTION 4: USE CASES

The introduction to this whitepaper briefly alluded to three use cases—automotive, healthcare, and utilities—that are continually evolving as a result of increased device connectivity. Section 1.2 described some of the actors that are typically understood to exist in these sorts of deployments. And, Section 3.2 introduced the TSM and CA, two important actors in a GlobalPlatform environment.

The simplified use cases discussed at the outset can be made more comprehensive by the introduction of IoT concepts. And, introducing GlobalPlatform concepts and assets into the management of IoT Devices requires further explanation. Accordingly, this section re-examines these three use cases in an IoT context and with the introduction of GlobalPlatform-defined roles.

In the sections below, we examine theoretical IoT deployment examples using the terminology and abbreviations defined throughout this document. Depending on the use case, an actor may assume one or several roles; to avoid confusion, the role name is indicated within parenthesis. In instances where more than one party plays the same role, these are differentiated by the addition of a hyphen and number (i.e. "SP-1" to denote the first of multiple Service Providers).

4.1 Utilities

Consider a scenario in which a smart meter manufacturer (DM) sells smart meters with an integrated SE that it acquired from an SE Supplier. A local energy provider (SEI and SP) purchases and installs the smart meter in a house. An associated energy distribution network provider or grid operator company (AP) asks its Trusted Service Manager to install an application that measures and manages line quality aspects on the device. This information obviously needs to be protected from being intercepted during transmission, so there is a need to install cryptographic keys during deployment. Another AP (such as a local energy provider)

[14] REST = Representational State Transfer; see http://en.wikipedia.org/wiki/Representational_state_transfer.

will typically be the entity that bills the consumer for energy usage and will load its own application on the meter to monitor energy usage. This possibly involves real-time demand-response incentives.

In some countries, the house owner or tenant (SS) may select an energy supplier (SP-1) other than the grid company, a process known as "unbundling." Different energy suppliers may charge different rates, depending on time of day, overall energy consumption, and more. These suppliers may require different types of information in order to calculate their rate. Additionally, different energy distribution network operators may monitor different parameters to optimize their grid management.

Now consider what happens when the homeowner changes his/her energy supplier. The new supplier (SP-2) must contact the TSM associated with the utility grid company (SEI) to replace the old supplier's rate information in the smart meter; this includes the secret keys used for protecting the records that are sent back. These keys may need to be kept confidential since the utility grid company may be a competing energy supplier. It is at this stage where the Security Domain of the CA, and optionally the CA itself, is involved.

In this example, both the utility grid company and the energy supplier are dependent on network connectivity for their services, but the Network Provider role may be played by any number of different parties. One natural scenario calls for the grid company itself to become the NP by using Power-Line Communications for backhaul. In this instance, the energy supplier (SP-2) may be the Network Subscriber, thus paying the grid company for its connectivity costs. Alternatively, if the smart meter supports cellular connectivity, an MNO may assume the role as NP. The grid operator would in this case be a natural NS and simply charge the energy supplier for its connectivity costs.

Finally, consider that the homeowner (SS) may also have its own application running in the device to measure raw energy consumption. In this instance, the homeowner would be another AP.

4.2 Automotive

The automotive market has long been moving towards software-based control. This trend is accelerating with more systems giving greater authority to computer-controlled systems. Automotive systems are also rapidly becoming more connected, both to each other and to the outside world. Taken together these trends are increasing the exposure and potential consequences of cyber-based attacks. Automotive systems highlight another problem: modern cars can have multiple embedded computing devices that are connected by several networks within the same car; they can also have their own network connectivity for maintenance, diagnosis, and software updates.

Consider a car manufacturer (DM, SEI) that procures batches of SEs from an SES. The manufacturer subsequently integrates the SE into an On-Board Unit (OBU) on the Controller Area Network bus (CAN bus) in the car.

The OBU may support selective access to different services, such as remote car diagnostics, positioning, roadwork information, emergency calls, etc. The car manufacturer could thus, through various applications in the OBU, offer aftermarket services, potentially in collaboration with various partner APs.

To explore this scenario, consider a car owner (SS) that signs up with a service garage (AP-1) for monitoring car diagnostics. An entirely different AP (AP-2) may be in charge of tracking the car in the case of theft, for example. An insurance company may be a third AP (AP-3), offering the car owner a reduced premium in exchange for monitoring certain driving parameters. The car owner may not want the data provided to a given AP to be available to others; s/he may also not want the car manufacturer to have any of the information.

In this situation, each AP would ask the TSM previously selected by the car manufacturer (SEI) to install its application in the OBU. The SEI and car owner in turn authorize the action, with the Security Domain of the CA, and optionally the CA, assisting in setting up confidential keys.

Similar to the homeowner described in the previous section, the car owner may have his/her own interface for various services based on data accessible over the CAN. For example, the car owner could set allowed areas, as well as allowable speeds and alarms for violating the rules (for example, when someone else borrows the car).

In this setup the car manufacturer is a natural candidate to serve as the NS. The car manufacturer can use itemized billing provided by the MNO to charge its partners for their share of the connectivity cost. The MNO may also act as an SP.

4.3 Healthcare

As a third use case, consider a healthcare industry example where a sensor gateway manufacturer (DM) manufactures a Gateway with an integrated SE. A healthcare system provider (SEI) procures medical sensors and Gateways and packages these into Remote Patient Monitoring (RPM) kits.

As part of this configuration, the medical sensors may be "paired" with the Gateway of the RPM kit, which means that connectivity and security parameters are established between the sensor and the Gateway. These RPM kits are in turn offered for sale or lease to healthcare providers (APs). The doctor or other medical personnel at the healthcare provider gives RPM kits to patients and instructs them on how to take measurements of their medical status at home.

As part of integrating the new equipment, the healthcare provider will need to contact the TSM selected by the SEI to install a new Security Domain on the Gateway on behalf of the healthcare provider. The Security Domain of the CA, and optionally the CA, assists in establishing the healthcare provider's secret keys in the Security Domain. Using the secure channel, the healthcare provider can provision other necessary parameters, such as the IP address and the public key of the server that receives patient data.

Given that there is cellular access in the patient's home, the MNO is a natural candidate to serve as the NP. The healthcare provider is taking on the cost of connectivity and is thus a natural candidate to be the NS. Either party can act as an SP, or this role may be delegated to a third party.

Note that in this use case the patient serves as the service subscriber (SS). The patient cannot change the service provider on the RPM device because the equipment is owned or leased by the service provider. Nonetheless, it must be possible to replace the service provider's unique data (such as keys) in the event that the device is leased to another service provider.

It should also be noted that the situation would be different if the patient were to have his/her own device (for example, in the case that a patient owns his/her blood pressure reading device).

CONCLUSION & NEXT STEPS

Despite the millions of connected sensor and actuator devices worldwide, the *Internet-of-Things* is in its infancy. As with many maturing markets, the IoT is dominated by proprietary solutions as different service providers and manufacturers attempt to resolve industry issues and enable broader service delivery.

As devices and services proliferate, there are increasing privacy and security concerns: personal privacy must be respected, vehicles must remain safe and not endanger the general public, and critical infrastructure (such as water and energy systems) must not be hacked. Because IoT Devices and services impact others—and potentially society as a whole—these security concerns are paramount.

Open standards are necessary to take the IoT to the next level. Only open standards can ensure interoperability between the potentially billions of devices that will be connected moving forward. Equally important, however, is that open standards are necessary to ensure the security and safety of devices, services, and the public at large.

GlobalPlatform's role in the IoT standardization landscape should be to provide technical specifications that improve the interoperability and security of these connected devices. This begins with the Secure Element or Trusted Execution Environment and extends to include the Trusted Service Manager, Controlling Authority, and other roles of a multi-stakeholder ecosystem. GlobalPlatform continues to evaluate its existing specifications and engage industry participants to ensure that the needs of the IoT market are met. GlobalPlatform is soliciting industry feedback on how it can best contribute to the IoT market. All feedback is welcome, and all comments or questions may be submitted to secretariat@globalplatform.org.

APPENDIX

Definitions

Term	Definition
Controlling Authority	Party supporting establishment of confidential keys for Security Domains on behalf of another party
Device Manufacturer	Manufacturer of the IoT Device.
IoT Service Provider	Party responsible for IoT Service
IoT Service Subscriber	Party having a contract with an IoT Service Provider about an IoT Service.
Network Provider	Party providing WAN access to the IoT Device/Gateway.
Network Subscriber	Party having a contract with the Network Provider on WAN access for the IoT Device/Gateway.
Secure Element	As defined by GlobalPlatform, a removable or non-removable, temper-resistant semiconductor device.
Security Domain	A concept defined by GlobalPlatform that represents a stakeholder on the SE. It stores credentials for the stakeholder and provides mechanisms to setup secure channels and to manage credentials.
SE Issuer	Issuer of Secure Element
SE Supplier	Supplier of a GlobalPlatform compliant Secure Element.
Trusted Execution Environment	A secure area that resides in the main processor of a mobile device and ensures that sensitive data is stored, processed and protected in a trusted environment.
Trusted Service Manager	Party performing Card Content Management operations on the SE on behalf of other party

Abbreviations

Abbreviation	Meaning
AP	Application Provider
CA	Controlling Authority
CAN	Controller Area Network
DM	Device Manufacturer
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISD	Issuer Security Domain
ISP	Internet Service Provider
M2M	Machine-to-Machine
MNO	Mobile Network Operator
NP	Network Provider
NS	Network Subscriber
OBU	On-Board Unit
OMA	Open Mobile Alliance
RESTful	Representational State Transfer
RPM	Remote Patient Monitoring
SE	Secure Element
SEI	Secure Element Issuer

Abbreviation	Meaning
SES	Secure Element Supplier
SIM	Subscriber Identification Module
SP	IoT Service Provider
SS	IoT Service Subscriber
TSM	Trusted Service Manager
UICC	Universal Integrated Circuit Card
WAN	Wide Area Network