W3C Workshop Synopsis

Speaker name: Gil Bernabeu, Technical Director, GlobalPlatform

Title: Accessing GlobalPlatform Secure Component from a Web Application

Paper:
Delegates attending this presentation will receive:

- An introduction to GlobalPlatform's view on mobile security
- Insight into how a secure component can form a root of trust for applications and rich operating systems
- An explanation of two secure components defined by GlobalPlatform – SE and TEE – and why they are important
- An analysis of the future industry requirements

Mobile service providers are encountering two complementary trends:

1. Consumers' desire for fast access to new and evolving services
2. Product and software innovation cycles that struggle to keep up with this consumer demand.

Often lost in the race to deploy new mobile services is the importance of security. As service providers jockey to deploy and revise services at an ever-faster rate, less emphasis has been placed on security, authentication and end-user identity protection.

Prior to the explosion of mobile devices and services, security and user authentication were governed by hardware-based secure components. It was generally accepted that an end-to-end secure infrastructure was critical. The quick pace of innovation, however, has caused the market's focus to shift from security toward new methods of provisioning products and services to mobile devices, including leveraging a particular device's built-in features or providing a direct-to-consumer solution.

As the association which standardizes the management of applications on secure chip technology, GlobalPlatform believes that it is possible, through secure chip technology, to maintain enhanced levels of security and authentication without stifling innovation and quick product iteration cycles.

Rapidly evolving mobile services are a natural response to consumer and market demand. Consumers want to select any mobile device, change mobile devices, add or delete applications, and change service providers – all while expecting that their information and identities are secure. A host of ecosystem actors – device manufacturers, service providers, network providers, vendors, and more – are scrambling to deliver on these consumer preferences.

Many mobile services such as games, reading, or social applications, have relatively low security risks. Other services such as electronic payment, money transfer, entrance to a secure facility (access control), or digital signature (authentication), to name a few have much higher security requirements. Nonetheless, consumers still expect rapid service evolution and iteration, so any successful approach to security must not slow down this process.

In mobile service delivery, authentication typically occurs on the consumer's mobile device but by definition, the service provider does not control device security. Accordingly, the service provider benefits if there is some mechanism that allows it to establish secure communication channels; this can be accomplished if the device is equipped with a secure component.

GlobalPlatform defines two secure components:

1. **Secure element (SE).** An SE is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and

cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities.

2. **Trusted execution environment (TEE).** The TEE is a secure area that resides in the main processor of a connected 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 security software, known as 'trusted applications', enables it to provide end-to-end security by enforcing protection, confidentiality, integrity and data access rights.

The TEE provides hardware-based isolation from the rich operating system (OS). It runs on the main device chipset and relies on hardware roots of trust (crypto keys and secure boot). A root of trust is a set of functions in the trusted computing module that is always trusted by the computer's OS.

GlobalPlatform recognizes the importance of the TEE for the future of managing applications on secure chip technology. Bridging the gap between the rich OS and SE is essential for the future security of trusted applications on mobile devices. When combined with an SE, the TEE offers an unparalleled combination of security and service flexibility.

In addition to protecting service providers and consumers from external hackers, a secure component prevents competing service providers, or even the consumer, from accessing sensitive service provider information. This is accomplished by allowing each service provider to load secret keys into the SE to protect its own applications. Each service provider may then load secured code that performs the sensitive parts of a transaction (such as end-user authentication, transaction authentication, or signature). When a transaction is executed in such a manner, the service provider has confidence that the transaction has been performed using secured code in a secure platform.

The TEE defines a standardized isolation environment for systems on chip (SoC) in which sensitive code, data and resources are processed away from the main operating environment, software and memory on the device. This isolation is enforced by hardware architecture and the boot sequence uses a hardware root of trust in the SoC package making it highly robust against software and probing attacks. In addition, code running in the TEE and using protected resources (known as 'trusted applications') is cryptographically verified prior to execution, leading to high integrity assurance.

As it provides an isolated runtime environment entirely inside the SoC (processor chip), the TEE enables advanced device or peripheral security use cases such as securing the user interface, or controlling access to an NFC chip. As such, the TEE can be used as a distinct security co-processor or to provide a trusted 'bridge' between the user and other security technologies such as secured UI or
OS user permissions on one side, and SE access control on the other.

The main operating system and rich applications then run as normal on the device, accessing the functionality of the trusted applications via a standardized 'Client API'. Trusted applications are written to an 'internal API' which ensures portable trustworthy access to secure resources, cryptographic operations and secure storage regardless of the underlying SoC hardware.

GlobalPlatform has now undertaken this work to standardize both the TEE and SE and both secure components are now ready to be deployed in the secure chip market. GlobalPlatform is constantly monitoring the evolving industry to ensure its specifications meet the requirements of key stakeholders both today and in the future.