

**Workshop Agenda**

**Thursday, 20 September 2018**

**9:00 AM to 5:00 PM**

**Registration and Welcome coffee/tea (8:30 – 9:00AM)**

**Early morning session (9:00 – 10:30AM)**

***GlobalPlatform Organizational Structure***

This brief presentation will offer insight into the market-based rationale behind recent organizational changes that had an impact on the SE, TEE and TPS Committees.

***Rising to the IoT Security Challenge: The Trusted Platform Services (TPS) Vision***

This session will show delegates how GlobalPlatform technologies make it easier for their services to take advantage of the security offered by secure components (while being component agnostic!). Specifically, this session will look at:

* For TEE, the Trusted Management Framework (TMF) and Open Transport Protocol (OTrP) Specifications
* For SE, the Secure Element Management Service (SEMS), DSEM, Open Mobile API (OMAPI), Secure Element Access Control (SEAC) and Device Access Control (DAC) Specifications.

***What is a Root of Trust (RoT) and why I need one?***

This session will explore the value of the RoT and its role in providing shielded storage for confidential device information such as keys and passwords, making it hard for attackers. The session will also explain how a Chain of Trust is established to provide security from the RoT to the service provider.

**Morning break (10:30 – 10:45AM)**

**Late morning session (10:45 to 12:30PM)**

***Making Secure Cryptography Easier: a Keystore for IoT***

This session will outline the core use cases for cryptography (encryption, decryption, hashing and signing) and the properties that can be used to guarantee confidentiality, integrity and authenticity. The presenters will wrap up by exploring the future importance of keystores and GlobalPlatform’s specific goals for an IoT keystore.

***EAT: A Framework for Entity Attestation***

Entity attestation provides ‘fresh’ and ‘verifiable’ information to other entities about a device so that these entities can tell the good devices from the bad (devices that have been cloned, tampered with, rooted or emulated, for example.) This session will see the experts dig into the use cases and potential service models for entity attestation.

***Onboarding and Updating Secure Components***

The ability to update and personalize secure components is fundamental for digital services and devices. Our speakers will explore the software architecture needed to support secure component updates, and explain how this might differ depending on the use case.

***How Companies Can Contribute to the Success of the TPS Vision***

A call-to-action for delegates! Learn how your company can further the work of the TPS Committee and its various working groups.

**Lunch break (12:30 to 1:30PM)**

**Early afternoon session (1:30 to 3:00PM)**

***How to Secure User Interactions***

For most digital services, users need to be securely authenticated. In many cases, users need to specifically approve sensitive transactions (such as payments and money transfers or agreement digital signatures) or view information displayed on their screens (like a one-time password (OTP)) and this information must be protected. This session will demonstrate how the latest GlobalPlatform TEE Trusted User Interface (TUI) and biometry APIs enable such trusted interactions.

***Endorsing Integrated Secure Element (iSE)***

Chipsets are offering new tamper-resistant secure processors, and GlobalPlatform has started to integrate this new host for SE technology.

This session will explore the Open Firmware Loader (OFL) and the Virtual Primary Platform (VPP) and how these specifications are used by ETSI in the Smart Secure Platform (SSP) to provide a standardized environment for designing secure operating systems targeting iSEs and a standardized loading and switching mechanism for such OSs.

**Afternoon break (3:00 – 3:15PM)**

**Late afternoon session (3:15 to 4:45PM)**

***How to Align with App Store Deployment***

Service providers are strongly invested in deploying their services through the app stores so GlobalPlatform has standardized a new technology to deploy SE applications within this infrastructure, facilitating the offline loading of applications.

This topic will address Secure Element Management Service (SEMS) and Secure Channel Protocol (SCP)11c and how they allow SE applications to be handled in an app store manner, with no Trusted Service Manager (TSM) or secure online sessions required.

***How to Simplify SE Connectivity to Devices***

Embedded SEs can use new interfaces in devices to connect with other applications or services, and to simplify the testing of the embedded SE. GlobalPlatform is standardizing the new physical layers to transport SE commands.

In this session we introduce Secure Peripheral Interface and Inter-Integrated Circuit (SPI+I2C) and GlobalPlatform’s cooperation with the Internet of Things Connectivity Alliance (ICA).

***How to Reduce Smartphone OS Customization for Mobile Network Operators (MNOs)***

With Device API Access Control, Rich OS providers are able to offer an internal API to access MNO applications that are signed and authorized by the smartphone, thanks to the authorization stored inside the UICC.

This session will present the Device API Access Control Specification, recently published by GlobalPlatform.

**Wrap-up and adjourn (4:45 – 5:00PM)**