Trusted Execution Environment (TEE)
Characteristics and Use Cases

Kevin Gillick
Executive Director
MobileCON 2013
18 October 2013
San Jose, California, USA
GlobalPlatform Overview
GlobalPlatform is the standard for managing applications on secure chip technology

Across several market sectors and in converging sectors
GlobalPlatform At-a-Glance

What is the output of GlobalPlatform?

- Specifications – technical industry guidelines
- Configurations – applying the guidelines to different market sectors
- Security certifications – streamlining security requirements & testing
- Industry compliance program – confirming a product’s functionality aligns to GlobalPlatform technology
- Educating the industry – white papers & technical documents
- Workshops – specification training & educational
GlobalPlatform’s Mission

• GlobalPlatform works across industries to identify, develop and publish specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology.

• GlobalPlatform Specifications enable trusted end-to-end solutions which serve multiple actors and support several business models.
GlobalPlatform Vision

- Member-driven organization which defines technology standards for cards, devices and systems and creates foundation for future growth.

- License _royalty-free_ card, device and systems specifications.

- Compliance program tools to verify card, device and system compliance to GlobalPlatform technology.

- Foster adoption of secure chip technology standards and implementations across industries.
High Rate of Adoption

- In 2006 there were over 100 million GlobalPlatform cards in use worldwide.

- In 2012, more than 2 billion GlobalPlatform cards have been produced.

- More than 100 publicized implementations across financial, ID / security, government, mobile telecom and healthcare markets.
We have now released documents that:

- Enable application providers to confidentially and independently manage applications while using a third party communication network.
- Provide increased security for devices which run multiple applications including mobile and/or remote devices.
- Manage the secure delivery over-the-air of new services.
- Outline the behavior of each and every actor involved in a mobile implementation, how they should be represented, and a summary of their role/responsibility in a variety of business models.
- Define the communication between applications running in a rich operating environment and the applications residing in the trusted execution environment (TEE) of a mobile device.
- Define a single administration protocol to perform remote management of applications residing on any type of secure element (SE) in a mobile device.

And soon….

- A framework for setting up and managing a privacy environment.
The Trusted Execution Environment (TEE)
What is a Trusted Execution Environment (TEE)?

- TEE provides \textit{hardware-based isolation} from rich operating systems (OS) such as Android, Windows Phone and Symbian.
- TEE runs on the \textit{main device chipset}.
- TEE has \textit{privileged access} to device resources (user interface, crypto accelerators, secure elements...).
Security vs. Functionality

- Security
  - SE
  - TEE
  - Rich OS

- Functionality
  - Rich OS
  - TEE
  - SE
Almost all recent mobile devices support TEE technology and the primary commercial usage today is DRM.
Overall objective: promote TEE ecosystem
- Have interoperable TEEs across silicon vendors and devices
- Have one single set of APIs for service providers whatever the silicon vendors and devices
- Have standardized way to administrate the TEE

Technology agnostic

Resistant to
- any software attack (remote and local)
- basic hardware attacks (local)
  - debug interface, firmware tampering, …

TEE programming environment
- Native-based (C-based)
- Isolation between Trusted Applications
Growing TEE Momentum

More and more TEE followers within GlobalPlatform

<table>
<thead>
<tr>
<th>SoC and hardware IP vendors</th>
<th>Service providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMD</td>
<td>American Express</td>
</tr>
<tr>
<td>ARM</td>
<td>Discretix</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Elliptic</td>
</tr>
<tr>
<td>Inside Secure</td>
<td>Good</td>
</tr>
<tr>
<td>NXP</td>
<td>Inside Secure</td>
</tr>
<tr>
<td>NVIDIA</td>
<td>Proxama</td>
</tr>
<tr>
<td>Qualcomm</td>
<td>Visa</td>
</tr>
<tr>
<td>Renesas</td>
<td>wave</td>
</tr>
<tr>
<td>Samsung</td>
<td></td>
</tr>
<tr>
<td>ST Ericsson</td>
<td></td>
</tr>
<tr>
<td>Texas Instruments</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TEE OS vendors</th>
<th>Device vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>LG</td>
</tr>
<tr>
<td>SOLACIA</td>
<td>BlackBerry</td>
</tr>
<tr>
<td>Trustonic</td>
<td>Samsung</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test and security labs</th>
<th>Trusted service managers</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIME</td>
<td>Gemalto</td>
</tr>
<tr>
<td>Galitt</td>
<td>Giesecke &amp; Devrient</td>
</tr>
<tr>
<td>Trusted Labs</td>
<td>Oberthur Technologies</td>
</tr>
</tbody>
</table>

Mobile network operators

- at&t
- Sprint
- Verizon Wireless
- France Telecom
TEE Educational Materials Available

Video interviews with industry experts:

- What is the TEE?
- Use cases driving TEE adoption
- What is the role of GlobalPlatform?
- How the TEE enables the development of secure applications
- How secure applications benefit from the underlying secure platform

White paper:

The GlobalPlatform Value Proposition for the Trusted Execution Environment
White paper:

*TPM Mobile with TEE for Comprehensive Mobile Device Security*

- Whitepaper introduces how GlobalPlatform TEE and TCG’s Mobile Trusted Module (TPM MOBILE) can work together in mobile devices to provide security and enhanced services to users.
- The TPM MOBILE standard continues to be developed in line with mobile device security technologies, such as the GlobalPlatform TEE, in order to create something which is not just secure in principle, but secure and usable in real devices.
First Annual TEE Seminar

The Trusted Execution Environment (TEE):
Next Generation Mobile Security for Today and Tomorrow
Santa Clara, California

GlobalPlatform Presents
THE TRUSTED EXECUTION ENVIRONMENT (TEE): NEXT GENERATION MOBILE SECURITY FOR TODAY AND TOMORROW

GlobalPlatform Presents the Trusted Execution Environment (TEE): Next Generation Mobile Security for Today and Tomorrow Conference is the market's only comprehensive event focused on the advancing TEE landscape. The one-day industry gathering provides delegates with an insight into the vast opportunities presented by this technology for the deployment of trusted applications in open environments. Read More
Thank You!