GlobalPlatform Technology for Mobile Contactless Services
Mobile Security and Interoperability

Kevin Gillick, Executive Director,
GlobalPlatform
CTST, New Orleans
7 May, 2009
Discussion Topics

- GlobalPlatform overview
- GlobalPlatform technology for mobile services
GlobalPlatform Overview
How We Started

- Originated as Open Platform architecture and specifications in collaboration with government, financial and telecommunications sectors.

- A cross industry consortium (GlobalPlatform) was formed to shape and commercialize the specifications.
GlobalPlatform delivers the complete set of specifications for an end to end smart card infrastructure
Collaborative Industry Partners

- ACT Canada
- AEPM
- AICF
- APSCA
- CEN TC224
- ETSI
- Eurosmart
- EMVCo
- Global Collaboration Forum
- GSM Association
- INCITS
- ISCAN
- ISO/WG4
- Java Card Forum
- Liberty Alliance
- Mobey Forum
- NICSS
- NIST
- OMA
- OMTP
- SCA
GlobalPlatform Key Strategies

- To maintain the *stability* of the specifications in order to foster implementation, changing the specifications only to meet market needs, rather than for technical elegance.

- To preserve *backward compatibility* when updating the specifications to ensure optimum performance and investment protection.

- To support application *portability*, infrastructure standardization and common interfaces to encourage specification adoption and deployment.

- To provide a *security* architecture with a range of security options to meet market needs.
As of October 2008 …

- Over 305 million GlobalPlatform cards deployed worldwide across the mobile telecom, financial, ID/security, transit and healthcare markets.

- More than 90 known implementations deployed in the marketplace based on GlobalPlatform technology.

- Estimated 2 billion GSM cards use GlobalPlatform for over-the-air (OTA) application downloads.

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>55 million</td>
</tr>
<tr>
<td>2004</td>
<td>85 million</td>
</tr>
<tr>
<td>2005</td>
<td>175 million</td>
</tr>
<tr>
<td>2006</td>
<td>265 million</td>
</tr>
<tr>
<td>2007</td>
<td>305 million</td>
</tr>
<tr>
<td>2008</td>
<td>305 million+</td>
</tr>
</tbody>
</table>
GlobalPlatform Technology for Mobile Services
GlobalPlatform is a foundation of the contactless technology eco-system

- Endorsed by:

  - STLPAN
  - MobeY Forum
  - EMVCo
  - GSMA
  - Ulysse
Secure Element in Mobile

• Service providers may want to store:
  – An application to perform secure execution
  – Keys to perform cryptographic calculation i.e. authentication or signature

• While managing:
  – End user authentication
  – Contactless transactions
  – Update of application data

• A GlobalPlatform Secure Element (SE) provides a standard and secure environment to manage multiple applications in a multiple actors environment

3 types of Secure Elements are envisioned:

Secure Memory Card

Published in November 2008

To be published 2009-2010
Standards and Connectivity

Handset application

J2ME-JSR 177
JSR 257

ISO 14433

apdu ISO 7816

GP

SEs

SE application

SWP 102 613
HCl 102 622

OTA 102 225

ISO 7816

Contactless Reader
To facilitate discussions between stakeholders, a UICC Configuration was published in Q3/08, containing:

- Set of features from the GlobalPlatform Card Specification v2.2
- Definition of the different business models supported
- Guideline for Confidential Card Content (C3) Management (Amendment A)

The MNO chooses the business model(s) and features supported by the UICC and makes them available to its partners via personalization:

- The application provider’s security domain personalization defines the services and privileges available
The UICC is one of the secure element solutions for application providers (APs):
- Standardized, portable and transferable
- Huge deployment
- High end product answers to the security requirements of many markets
  - i.e. TV, banks, transportation
- OTA back-end capacities available worldwide 24/7

A GlobalPlatform UICC provides a standard solution for issuers and stakeholders:
- Supports rental models for issuers i.e. many business models between stakeholders (mobile network operators (MNO), service providers, and also trusted service managers)
- Confidential loading and perso for the service provider with C3 mgt
- Compliancy with other businesses i.e. banks, transportation
Rental Models (MNO Centric)

- The card issuer (CI) provides the service provider (SP) with a security domain (SD)
  - The SP can place secret data in its applications (keys etc.) that the CI is unable to see

- The CI either loads applications itself (using Confidential Mgt), or allows the SP to load applications
  - The CI vets each application before loading
  - CI creates a load token for each application (with delegated management)
  - CI imposes quota on each application
Rental Models (Wholesale)

- The card issuer (CI) rents out blocks of card memory to a service provider or trusted service manager (TSM) or a ‘few’ TSMs:
  - The TSM re-rents the space to ‘many’ end service providers
Different Ecosystems in One Secure Element

- MNO
- Rental Model
- Bank
- Wholesale Model
- Loyalty
- Transit
- TSM
- TV
Service Provider View

- The security domain (SD) represents a private zone inside the card:
  - Same as in a standard GlobalPlatform card

- The application provider (AP) buys a standard set of options attached to the SD:
  - Autonomy of loading (yes/no)
  - Keys
  - Connectivity – contact, contactless, OTA …
• Published in 2008

• Compliance program on-going
  – Publication expected in Q4/09

• Compliance program and certified test tool program started
  – First certified tool expected in Q4/09 / beginning of 2010
  – Create a new eco system with test tool suppliers

• Smart card management systems
  – White paper on-going

• Certification initiative
  – New certification scheme with other industry forum
End User Role in Service Usage

- Contactless services request a migration

From multiple cards... ...to contactless services in one handset
Application Selection – GlobalPlatform’s Scope

End User shall be able to:
• Order the list of services based on user friendly service management
• Deactivate some services

Application provider shall be able to:
• Provide technical meta data (contactless protocol and protocol environment)
• Provide end user selection meta data (logo, family…)

Current reader infrastructure (mainly mono application) shall be able to:
• Select the right service

Sample UI:
- Oyster Activated
- Calypso Deactivated
- Visa Issuer A Activated
- Visa Issuer B Deactivated
- MC Issuer C Activated
Grouping of Applications

Sample UI

- Oyster: Activated
- Calypso: Deactivated
- Visa Issuer A: Activated
- Visa Issuer B: Deactivated
- MC Issuer C: Activated

Group Calypso:
- Calypso: AID 1, Visible, Deactivated
- Air France: AID 2, Invisible, Deactivated
- SNCF: AID 3, Invisible, Deactivated

Group Visa Issuer A:
- Domestic: AID 4, Visible, Activated
- International: AID 5, Invisible, Activated
GlobalPlatform White Paper

• Purpose:
  – To state the value proposition for GlobalPlatform Systems Messaging Specifications for roles in the mobile eco-system
  – To validate the value proposition through detailed specification examination

• Context:
  – Paper will be technically informative and educational
  – Intended audience is the program/project manager, consultant or implementer, application developer or solution architect. Any individual who plays a role in the eco-system

www.globalplatform.org/mediawhitepaper
Thank You!