Model-Based Testing for a WW Compliance Program

Gil Bernabeu
GlobalPlatform Technical Director

Nicolas Lavabre
Senior Consultant
2 speakers for you today!

Gil Bernabeu

Nicolas Lavabre
GlobalPlatform Positioning

GlobalPlatform is the standard for managing applications on secure chip technology

Across several market sectors and in converging sectors
Introducing GlobalPlatform standards...

- Since 1999, With GlobalPlatform standards:
  - Create once based on -
    - Stable and interoperable Application Programming Interfaces (APIs)
    - Stable security requirement
  - Deploy ‘everywhere’
Foundation of the Mobile Contactless Technology Eco-system

• GlobalPlatform is form factor agnostic
• Configurations today support:
  • UICC
  • Embedded SE
  • Smart micro SD

NFC And Contactless-Mobile Projects

Secure Element (SE) OBJECT

220 projects selected

Click on the map or project list for more details

http://nftimes.com/nfc-projects
Interoperability means compliance
GlobalPlatform Card Framework Overview

GlobalPlatform Specification

Commands
APDU (ISO 7816)
First tentative

- Deployment of GlobalPlatform technologies are impossible without strong interoperability
- A first program (classical) has been created in 2001
  - Select one Test tool vendors
  - Create a Test plan
  - Validate the Test plan
  - Use the test tool
- Results
  - Few interest from the eco systems to validate the test plan
    - “Took years”
  - Each Product vendor are using a in-house test environment or specific contract with another test tools provider
    - The selected test tool becomes the worse of the planet
- At the end of the day, the ROI was very low
  - No update of the test plan (as no one wants to validate 500 pages)
  - No good business for the Test tool vendor
First contact with Modeling

- As WW standardization organization, we are always looking for way to optimize the time of expert and the quality of deliverables
  - New tools
  - New process

- Thanks to the EVEREST project (INRIA) a formal model of the card specification has been produced (2004)
  - The objective was to help certification of produce in EAL 7 level that requires end 2 end traceability

- But developed in B language
  - Has generated more discussion about B grammatical issue in B than adoption by the community
  - Model for specification and model for test are not equal

- Formal model available at www.globalplatform.com
  - [here](http://www.globalplatform.com)
Second program in 2006

New objectives
- Provides test suite (means scripts) for integration to the Product vendors in-house systems
- Open to any Test Tools suppliers
- Let the market decide the best tools
- Validate the Test Plan in real
- Supports product variants

New environment
- Acceleration of deployment
- Start of the Mobile Wave deployment
- Strong pressure on adding additional feature

Document based?
UML Modeling based?
Compliance secretariat

Card Spec WG
Spec Configuration

Card Compliance WG
Coverage Test Suite

Test Suite
Test Suite Development

Test Fest

GlobalPlatform Members
Test Tools
Test Labs
Product vendor

Authorized organization

Evolution request

Publication of Qualified Test Tools
- Qualified Test Tools

Publication of Qualified Test Lab
- Qualified Test Labs

Publication of Test Claims
- Qualify Cards
- Self-Tested Cards

Test Report

Qualified?

Qualified?

Good claim?
Test Suite Process, Actors & Deliverables
From Specifications to Test Plan deliverable

GlobalPlatform Card Specification Working Group

GP specification

Test Designer

Test Objective Charter (excel)

Test Design

Reference implementation

Option 1
Option 2
Option 3

UML Model

Option 1
Option 2
Option 3

Smartesting Certifylt

GlobalPlatform Card Compliance Working Group
From Specifications to Test Plan deliverable

GlobalPlatform Card Specification Working Group

GlobalPlatform Card Compliance Working Group

Options (xml)
Initial States spec (doc)
Test Plan (html)
Test Objective Charter (excel)
Abstract Tests (xml)
Adaptation Layer spec (pdf)

Reference implementation
Smartesting Certifylt

Test Designer

UML Model
Tests

Option 1
Option 2
Option 3
From Specifications to Test Plan deliverable

GlobalPlatform Card Specification Working Group

GP specification

Test Designer

Test Objective Charter (excel)

Options (xml)

Initial States spec (doc)

Test Plan (html)

Abstract Tests (xml)

Adaptation Layer spec (pdf)

Reference implementation

UML Model

Tests

Smartesting CertifyIt

Test plan deliverable

GlobalPlatform Card Compliance Working Group

Test Design

Options

Option 1

Option 2

Option 3

Test Plan (html)

Test Plan deliverable
<table>
<thead>
<tr>
<th>Requirement name</th>
<th>Requirement text from spec</th>
<th>Requirement references</th>
</tr>
</thead>
</table>
| SCPI_ADMIN_MESSAGE_SENT | When receiving the HTTP POST request from the Security Domain, the Remote Administration Server shall send an HTTP response which encapsulates a remote APDU format string dedicated to the Security Domain. This dedicated Security Domain is defined as follows:  
   • If no "X-Admin-Targeted-Application" header is present in the HTTP POST response, then the targeted Security Domain is the one which provides the PSK/TL5 security of the communication channel.  
   • If a "X-Admin-Targeted-Application" header is present in the HTTP POST response, the header value is used as the target agent. | Amendment B v.1.1.1,<br>§5.3.3.3<br>scp81_serverSendAPDU <br>check the commands behave according to the targeted SSD |  |
| SCPI_SESSION_CLOSED | * The Remote Administration Server shall send the next remote APDU format string to the Security Domain (over the PSK/TL5 channel), or send a final response requesting the end of the remote administration session in the POST response.  
   If the Security Domain receives a final response from the Remote Administration Server, it shall close the PSK/TL5 channel, and then close the underlying communication channel. | Amendment B v.1.1.1,<br>§5.3.3<br>scp81_closeSession |  |
| OPEN_SECURE_SESSION_ERROR | When the targeted Security Domain is the one unwrapping the remote APDU command string, then the remote APDU command string is trusted and processed. Any attempt to initiate a Secure Channel session (according to another Secure Channel Protocol) within the remote APDU command string shall be | Amendment B v.1.1.1,<br>§5.3.3.2<br>sm_initialize update <br>SM |  |

On what is performed the requirement check

Sub-cases (aims)
Description of all the options possible for a given product
1. Table of content

2. Commands specification
   2.1. Operation Core_DELETE
   2.2. Operation Core_INSTALL_FOR_EXTRADITION
   2.3. Operation Core_INSTALL_FOR_LOAD
   2.4. Operation Core_INSTALL_FOR_MAKE_SELECTABLE

2. Commands specification
   2.1. Operation Core_DELETE()

2.1.1. Description
This operation describes the APDU command DELETE_KEY (dedicated for application) over the interface $IN_interface$
- CLA
  - If $IN_icNumber$ = 0, 1, 2 or 3 then
    - b8 = 1
    - ...

Implementation document describing all the system’s functions used
Test plan assets – Test Plan

7. SetUp
- IN_cardState: SECURED

7.1. checkApduStatusWord
- OUT_StatusWord: SUCCESS

8. nominal_APDU_select
- IN_idNumber: lc_00
- IN_appAid: aid_ISD
- IN_P1: BY_NAME
- IN_P2: FIRST_OR_ONLY_OCCURRENCE
- IN_claSmLevel: sm_no_sm

8.1. checkApduStatusWord
- OUT_StatusWord: SUCCESS

9. nominal_openSecureSession
- IN_idNumber: lc_00
- IN_securityLevel: sm_CMAC
- IN_kvn: KVN_00h

9.1. checkApduStatusWord
- OUT_StatusWord: SUCCESS

Commands are identical in html and xml.
Html is readable, contains a requirement summary and a test overview.
Test plan deliverable
From Specifications to Test Plan deliverable

GlobalPlatform Card Specification Working Group

Initial States spec (doc)

Test Designer

Test Objective Charter (excel)

Options (xml)

Abstract Tests (xml)

Test Plan (html)

Adaptation Layer spec (pdf)

Reference implementation

UML Model

Tests

Option 1
Option 2
Option 3

Option 1
Option 2
Option 3

Smartesting Certifylt

Test plan deliverable

GlobalPlatform Card Compliance Working Group
Specifications and test suites road map

- Test suites available for
  - UICC Configuration v1.0.1
  - Contactless Extension for UICC v1.0
  - Mapping Guidelines of 2.1.1 v1.0.1 (Banking)
  - Basic Financial Configuration (Banking)
  - SWP/HCI test suites from ETSI
  - ID Configuration v1.0

- 2013-2014 Forecast
  - Amendment B (SCP81)
  - Common Implementation Requirements
  - Embedded SE – micro SD (eSE)
  - Secure Element Access Control (applet)
Test suite creation process – old way of work

- UICC
- Banking 1
- Banking 2
- ID
- eSE

Common model

- Test base 1
- Test base 2
- Test base 3
New way of work - Reusability addressed

- UICC
- Banking 1
- Banking 2
- ID
- eSE

Common model - UICC model - Banking model

ID model - eSE model
New way of work - Reusability addressed

- UICC
- Banking 1
- Banking 2
- ID
- eSE

Common model
UICC model
Banking model
ID model
eSE model

Common test base

- UICC specific
- Banking 1 specific
- Banking 2 specific
- ID specific
- eSE specific
Reusability addressed

Common model
Contactless specific model
http/TLS specific model

Ground for other test suites

Contactless
http/TLS
Reusability summary - modelization

• Globally
  – Common behavior is embedded into an operation that can be called by other operations for different usages
  – Documentation can be customized for EACH development
  – Expected results (smart card answers) can be customized for EACH development

• Locally: Through code including switches

<common part>
IF ‘configuration X’ applies THEN
  The expected behaviors and results for X are applicable

• Through inheritance mechanism
  • An Initial State inherits the shared objects and its own objects
  • An Initial State may inherit from another Initial State, and adding its own objects

• Test content
Work setup
<table>
<thead>
<tr>
<th><strong>Work environment</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main model</strong></td>
</tr>
<tr>
<td><strong>Initial States model</strong></td>
</tr>
<tr>
<td><strong>UICC dedicated model</strong></td>
</tr>
<tr>
<td><strong>Banking dedicated model</strong></td>
</tr>
<tr>
<td><strong>UICC test package 1</strong></td>
</tr>
<tr>
<td><strong>UICC test package n</strong></td>
</tr>
<tr>
<td><strong>Banking test package 1</strong></td>
</tr>
<tr>
<td><strong>Banking test package n</strong></td>
</tr>
</tbody>
</table>

- Original model
- Default values for instances, all projects
- Model covering the spec 1 requirements
- Model covering the spec 2 requirements
- UICC test package on topic 1
- UICC test package on topic n
- Banking test package on topic 1
- Banking test package on topic n
Collaborative work

- Main model
- Initial States model
- UICC dedicated model
- Banking dedicated model
- UICC test package 1
- UICC test package n
- Banking test package 1
- Banking test package n
Quality
Development steps

Monitoring the progression is key for quality deliverables
Ensuring non regression

Setup of a complete non-regression framework

→ Ensures non regression on existing test suites
→ Ensures quality of new developments
Modelization benefits
Modelization benefits

- Modeling allows to:
  - Propagate changes very quickly
  - Check the changes both in tests and in Adaptation Layer
  - Be very reactive in proposing test plan updates

- On the Adaptation Layer → updates easy to spot
- On tests → enables to rerun only the ones updated
Modelization benefits

• Reusability
  – Model is 80% reused between each specification
  – 80% of tests are reused across test suites
    • Easier maintenance over time

• Quality
  – Non-regression ensures global quality
  – Sequential approach development
As Take away
Some drawbacks

• Moving from document to HTML document is not immediate

• First complete cycle took more than expected
  – New eco system to synchronize
  – First scope was (too) complex (UICC with 3rd party applications)
    • We found lot of inconsistency in the GP specifications but also inconsistency between GlobalPlatform and ETSI
    • Different LSs and update of specifications were requested
    • Good result for the quality but impacts the schedule
But all objectives achieved

• Strong and vibrant eco systems has been created around the Test suite
  – Product vendors
  – Test Tools vendors
  – Laboratories

• Program endorsed by EMVCO (WW banking standard)
  – Means mandatory for an Multi-application product that needs a Visa, MasterCard, Amex, JCB, China Union Pay or Discover certification

• Collaboration with ETSI and GCF about contactless

• Discussion with GSMA and enhancement for the UICC scope

• Replication done on TEE technology

• Less than 15 months between the release of the specifications and the first product Qualified by a Laboratory
  – Currently 2 products qualified
More information

GlobalPlatform
The Standard for Managing Applications on Secure Chip Technology

Gil Bernabeu
Technical Director
gil.bernabeu@globalplatform.org
phone: +33 4 42 36 66 62
mobile: +33 6 07 98 79 69
www.globalplatform.org
544 Hillside Road
Redwood City, CA 94062 USA

Smart Consulting
EXPERTS IN SMART CARD ENVIRONMENT

Nicolas LAVABRE
Consultant Senior

Smart Consulting
2, rue Louis Vignol
13600 La Ciotat - France
www.smart-consulting.com
Mobile: +33 (0)6 71 88 24 00
Fax: +33 (0)9 55 25 99 45
nicolas.lavabre@smart-consulting.com