Model-Based Testing for a WW Compliance Program

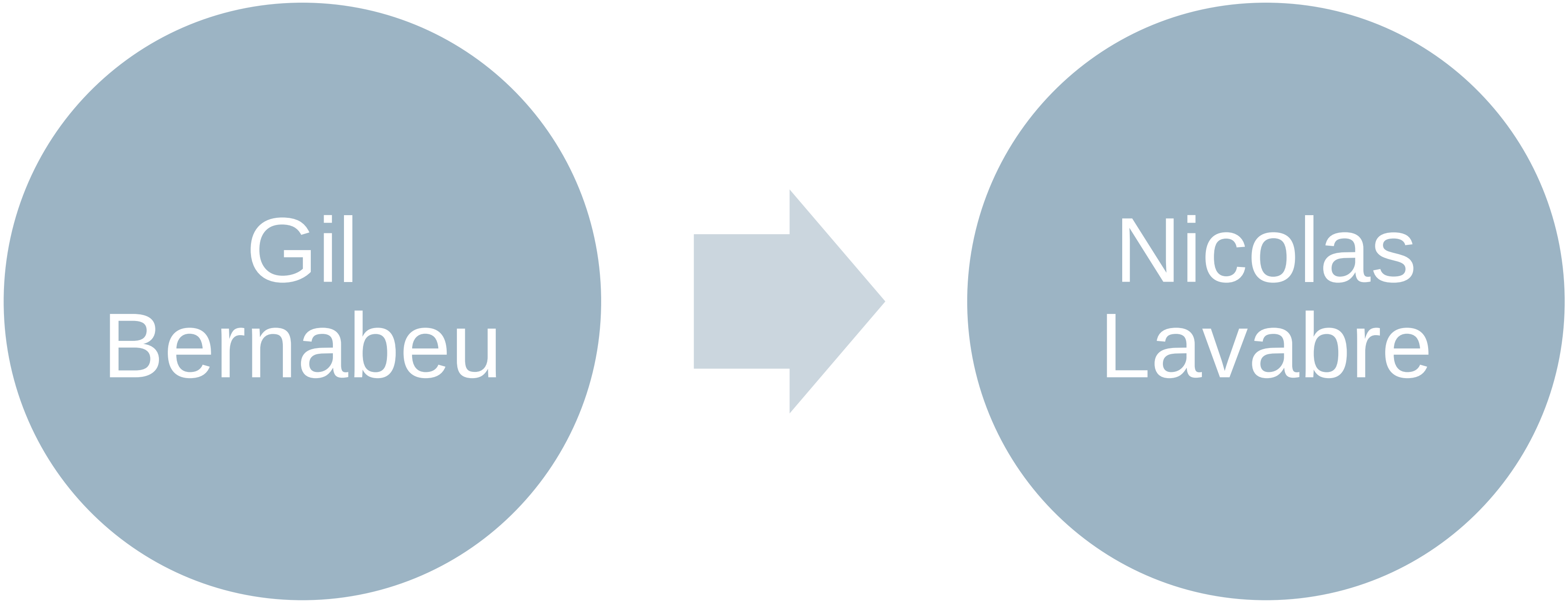
Gil Bernabeu
GlobalPlatform Technical Director

Nicolas Lavabre
Senior Consultant

@GlobalPlatform_

www.linkedin.com/company/globalplatform

2 speakers for you today !

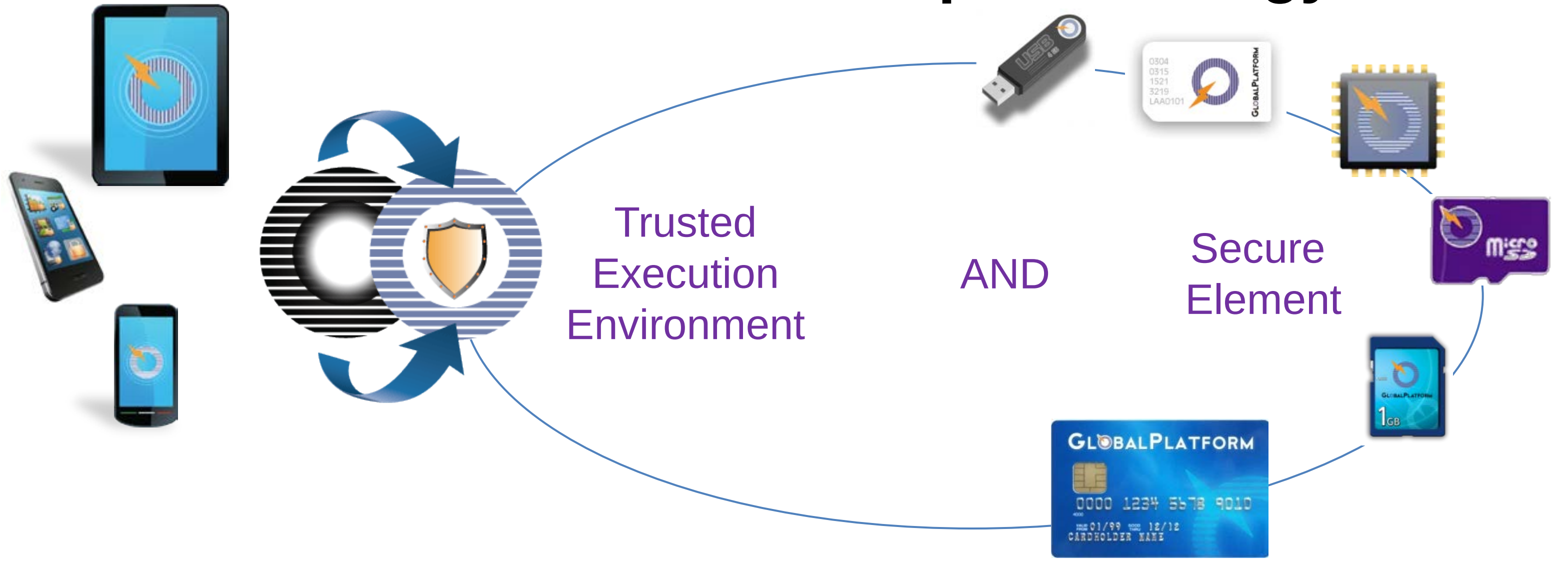


Gil Bernabeu

Nicolas Lavabre

GlobalPlatform Positioning

GlobalPlatform is *the* standard for managing applications on secure chip technology

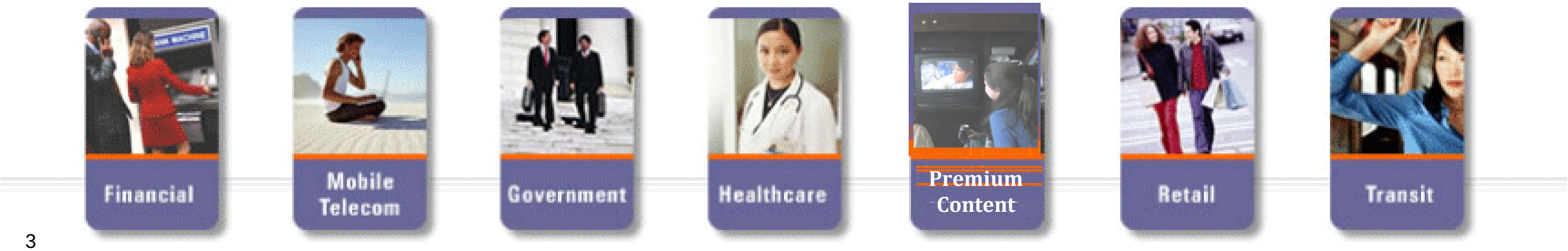


Trusted Execution Environment

AND

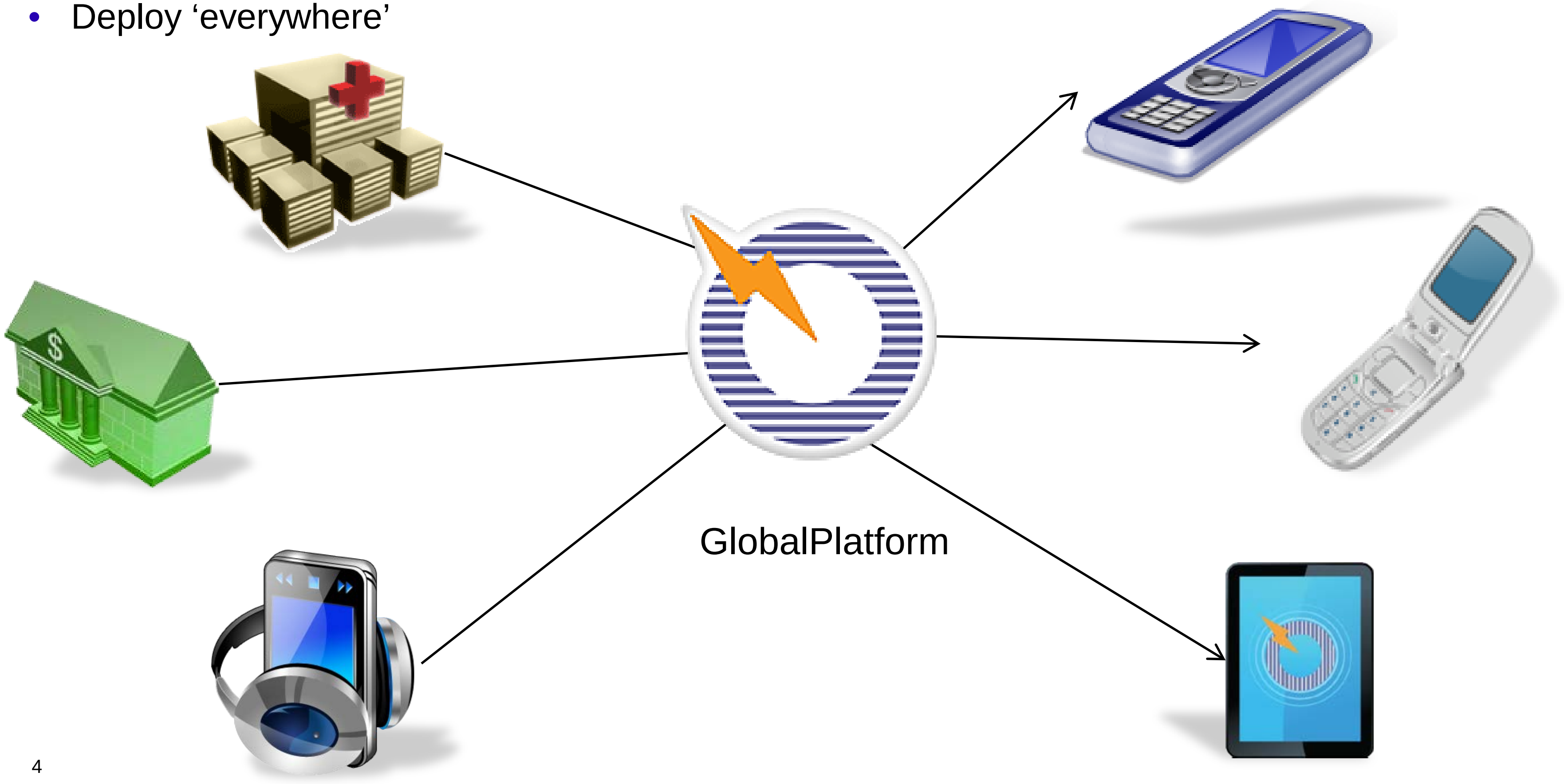
Secure Element

Across several market sectors and in converging sectors

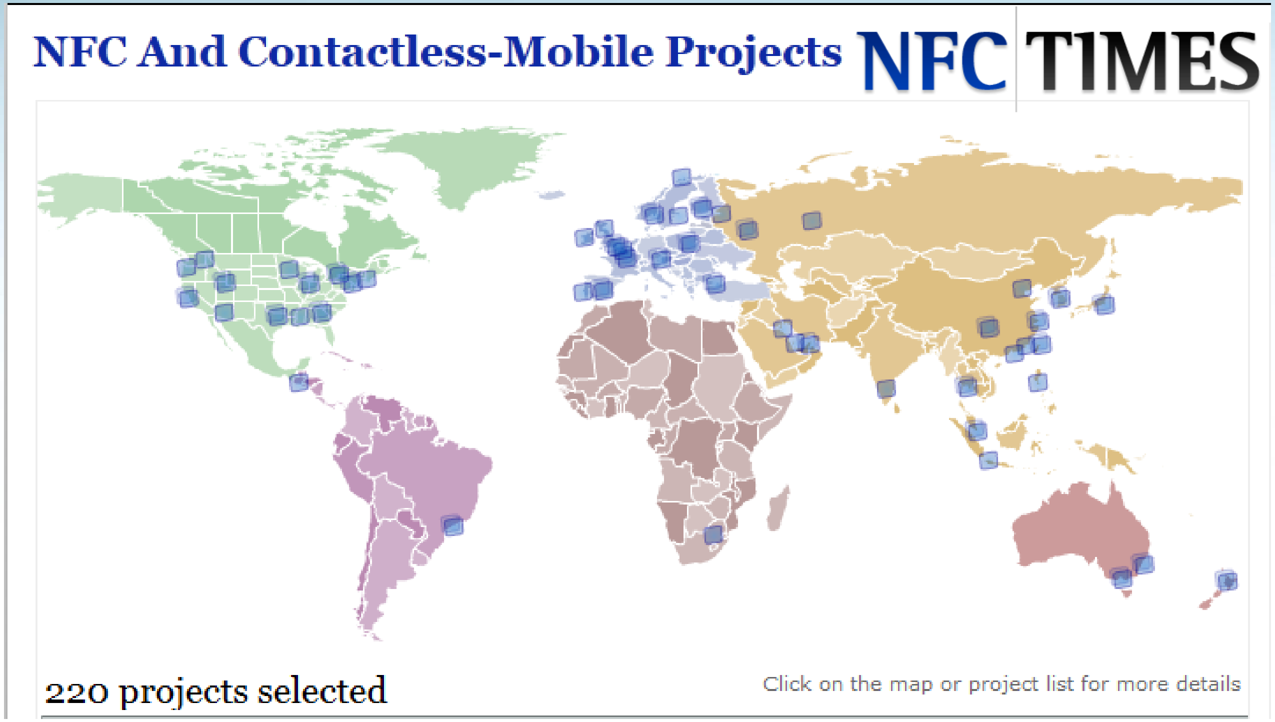


Introducing GlobalPlatform standards...

- 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



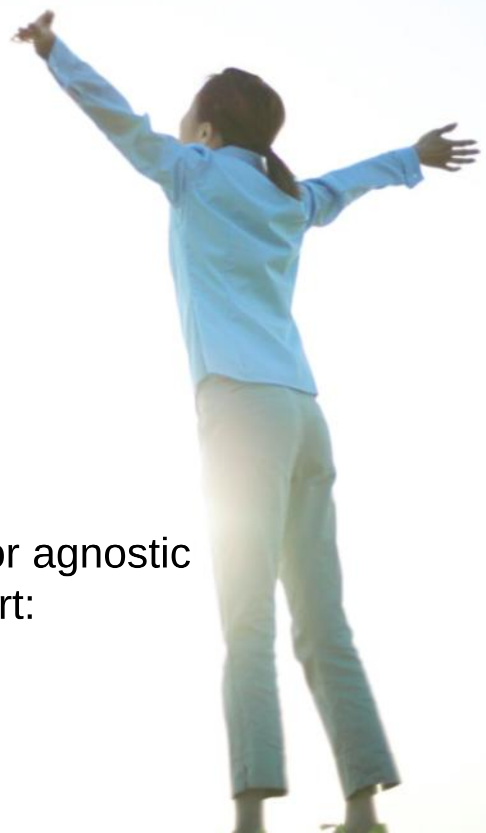
NFC And Contactless-Mobile Projects NFC TIMES

220 projects selected

Click on the map or project list for more details

http://nfctimes.com/nfc-projects

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



GlobalPlatform Members

GLOBALPLATFORM™

AMD
AMERICAN EXPRESS
ARM
athena Smartcard
at&t
BlackBerry
BROADCOM

COMPRION
Clear2Pay
DISCOVER
ERICSSON
FeliCa Networks
Galitt

gemalto security to be free
Giesecke & Devrient
Good
HID
infineon
FIME
inside SECURE
MasterCard Worldwide

NAGRA KUDELSKI
NTT
NVIDIA
NXP founded by Philips
OBERTHUR TECHNOLOGIES
ORACLE
orange

QUALCOMM
RENESAS Everywhere you imagine.
ROGERS
SAFRAN Morpho
SAMSUNG
SOLACIA

Sprint
ST
Trusted Labs
TRUSTONIC
UL
verizon wireless
VISA

Applus
BARNES INTERNATIONAL
CETECOM
DNP
FINGERPRINTS
LG
TÜV SÜD Japan
iCTK

secunet IT security beyond expectations
SK C&C
TELUS
TEXAS INSTRUMENTS
TOSHIBA
VALID

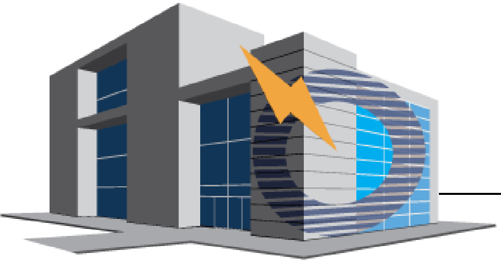
ABnote
aconite
BARCLAYS
北京华大智宝电子系统有限公司 BEIJING HUADAZHIBAO ELECTRONIC SYSTEM CO., LTD.
BellID
i-FREE
CB
CESG
UnionPay 银联 中国银联 China UnionPay
CROCUS Technology Blossoming future
CRYPTOMATHIC www.cryptomathic.com

Datang Microelectronics
DatacardGroup
Discretix trust • embedded
东信和平 EASTCOMPEACE
Elliptic
EQUENS
FEITIAN WE BUILD SECURITY
財金資訊股份有限公司 FINANCIAL INFORMATION SERVICE CO., LTD.
恒宝股份 HENGBAO CO., LTD.
HITACHI Inspire the Next

HUAWEI
intercede
irdeto
isis
JCB Good times start here.
kona i
LG CNS
MARVELL
monetech
movie labs
NEXTENDIS
Plastic Card

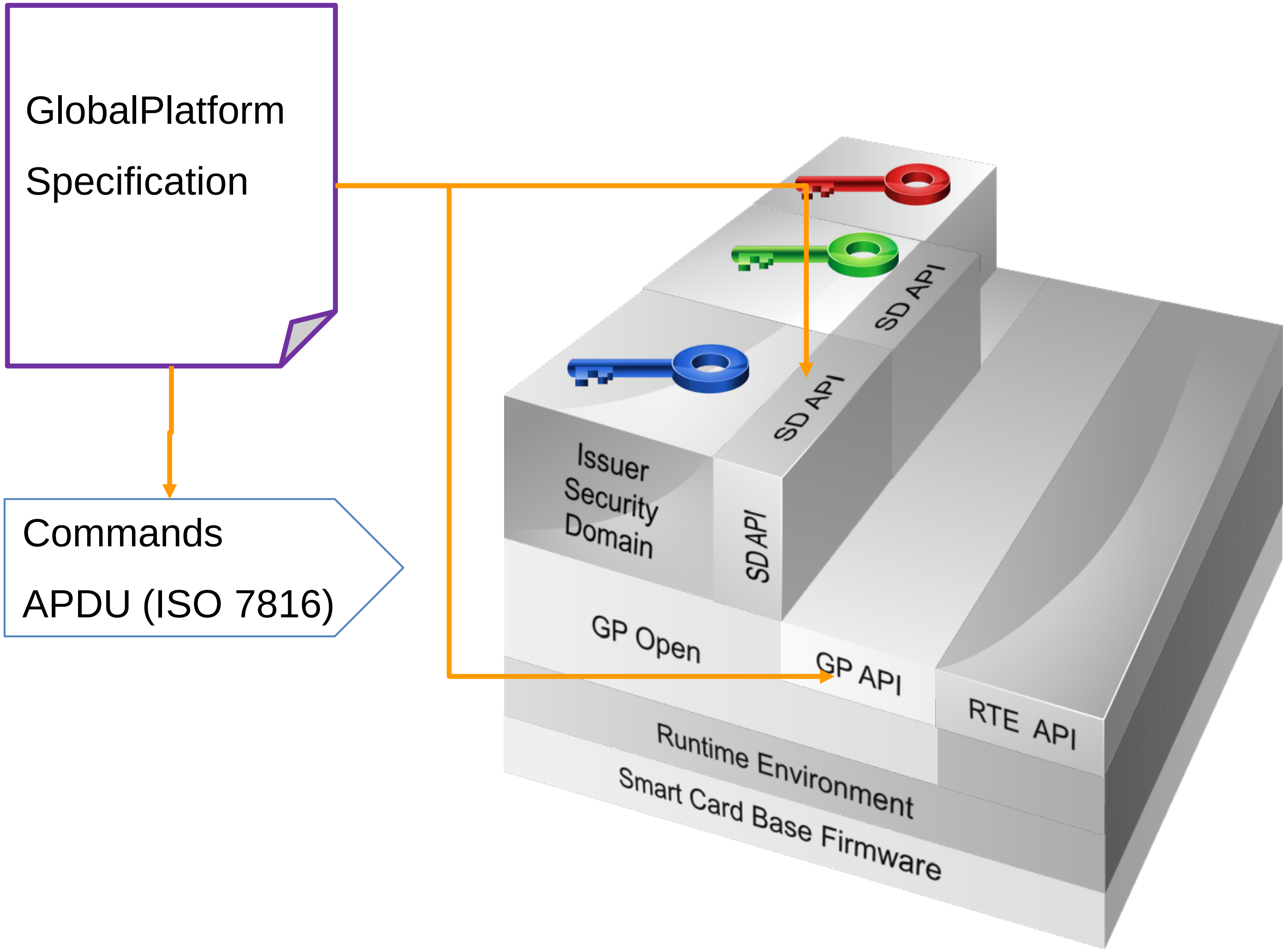
Posteitaliane
Proxama
Real Casa de la Moneda Fábrica Nacional de Moneda y Timbre
Redsys
SafePay systems
SAMSUNG
SAMSUNG SDS
sequent
上海柯斯 SHANGHAI COS
上海华虹集成电路有限责任公司 Shanghai Huahong Integrated Circuit Co., Ltd.
上海复旦微电子集团股份有限公司 Shanghai Fudan Microelectronics Group Company Limited

Secure Platforms Technology SP-Tek
THALES
THATER & SCHWIER CONSULTING
TIANYU
TOPPAN
TOPPAN FORMS
UBIVELOX
validity
Vellhi
Watchdata
wave
XROMB



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

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

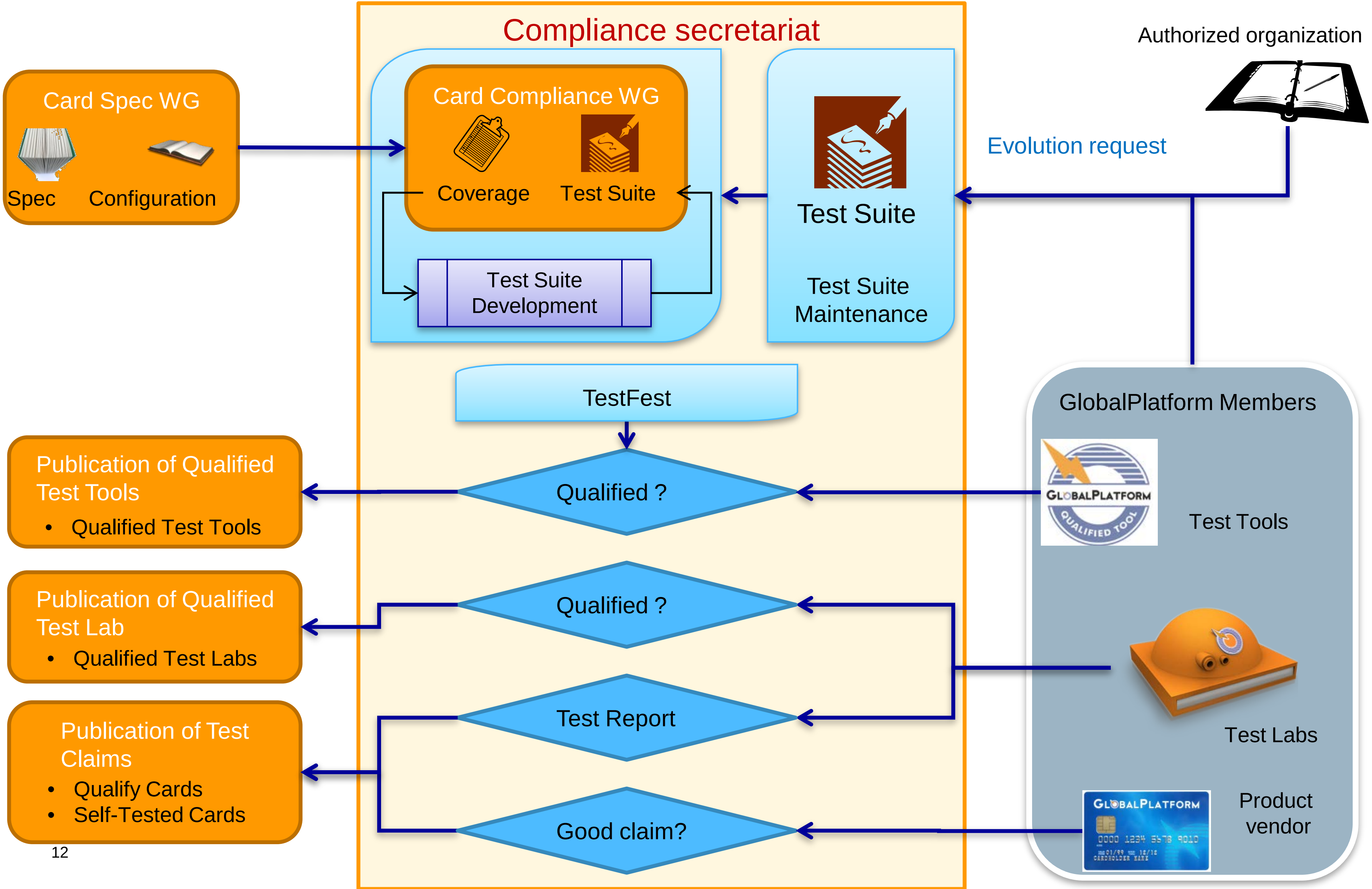
New environment

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

~~Document based ?~~

UML Modeling based ?

Global Overview



Compliance secretariat

Card Spec WG

Spec

Configuration

Card Compliance WG

Coverage

Test Suite

Test Suite Development

Test Suite

Test Suite Maintenance

Authorized organization

Evolution request

TestFest

Qualified ?

Qualified ?

Test Report

Good claim?

GlobalPlatform Members

Test Tools

Test Labs

Product vendor

Publication of Qualified Test Tools

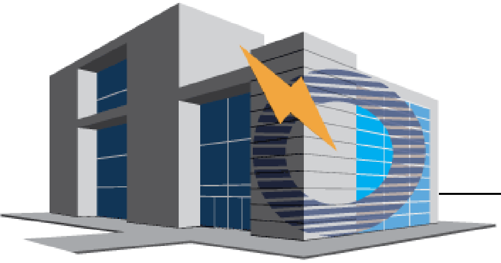
- Qualified Test Tools

Publication of Qualified Test Lab

- Qualified Test Labs

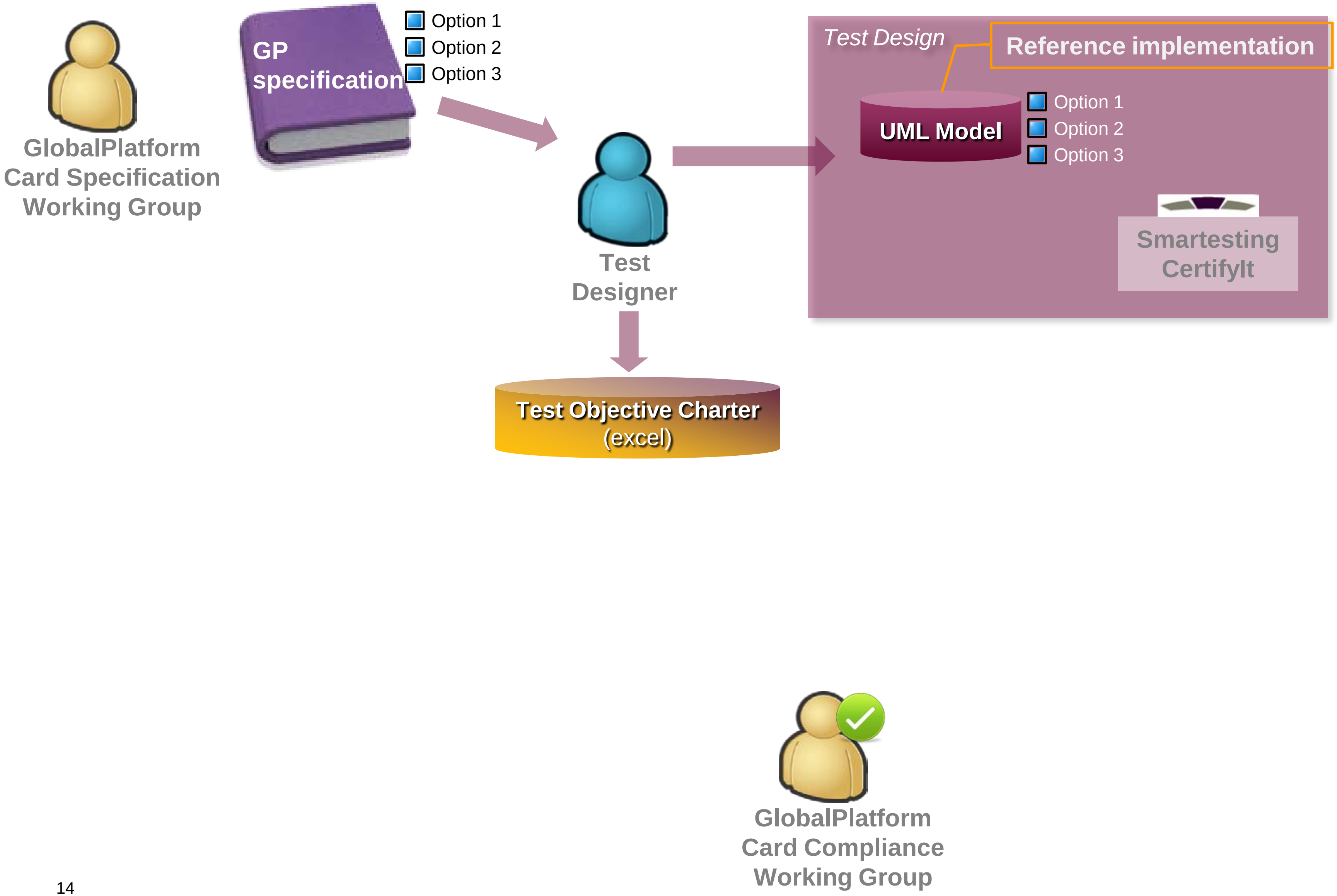
Publication of Test Claims

- Qualify Cards
- Self-Tested Cards



Test Suite Process, Actors & Deliverables

From Specifications to Test Plan deliverable



GlobalPlatform Card Specification Working Group

GP specification

□ Option 1
□ Option 2
□ Option 3

Test Designer

Test Design

Reference implementation

UML Model

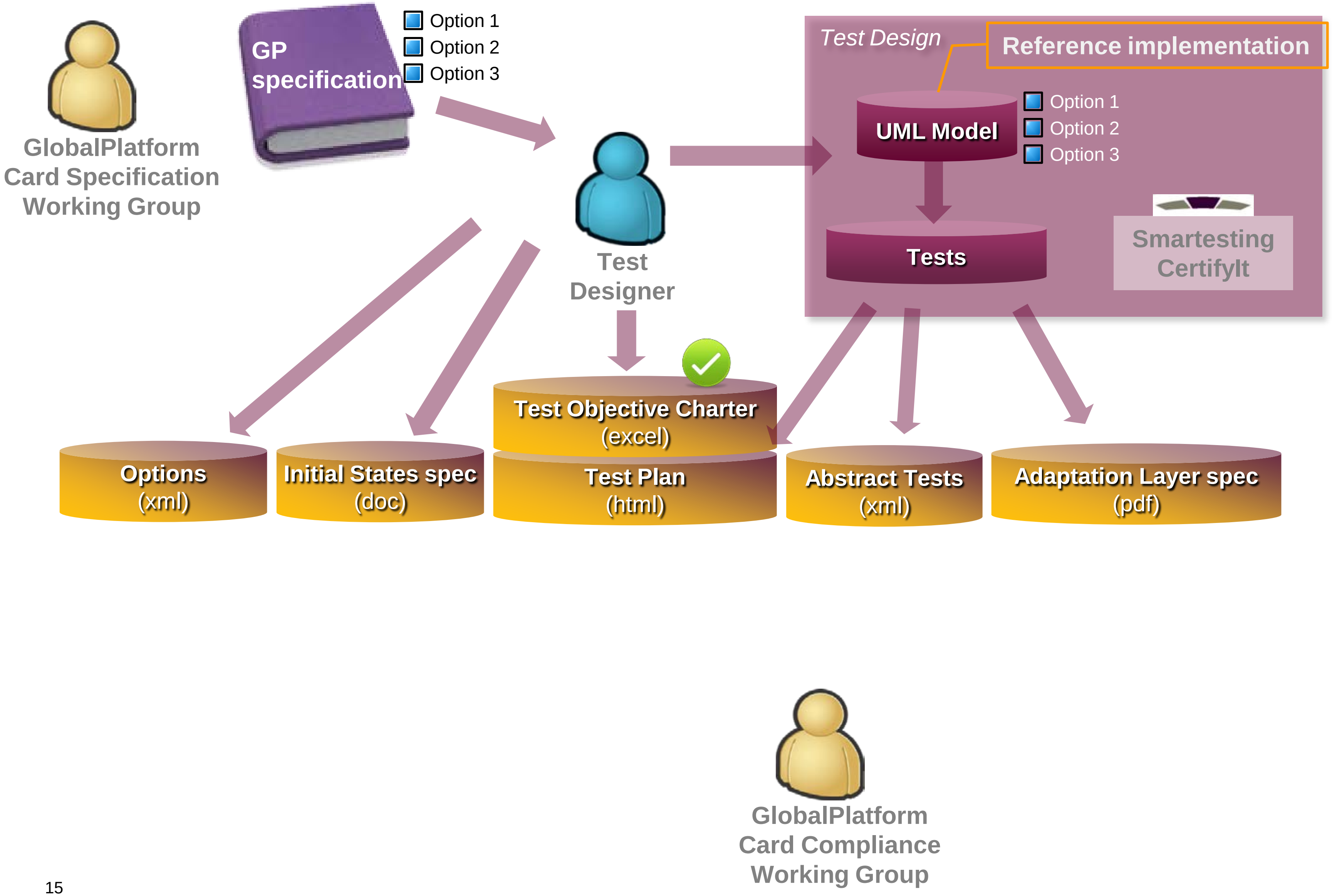
□ Option 1
□ Option 2
□ Option 3

Smartesting CertifyIt

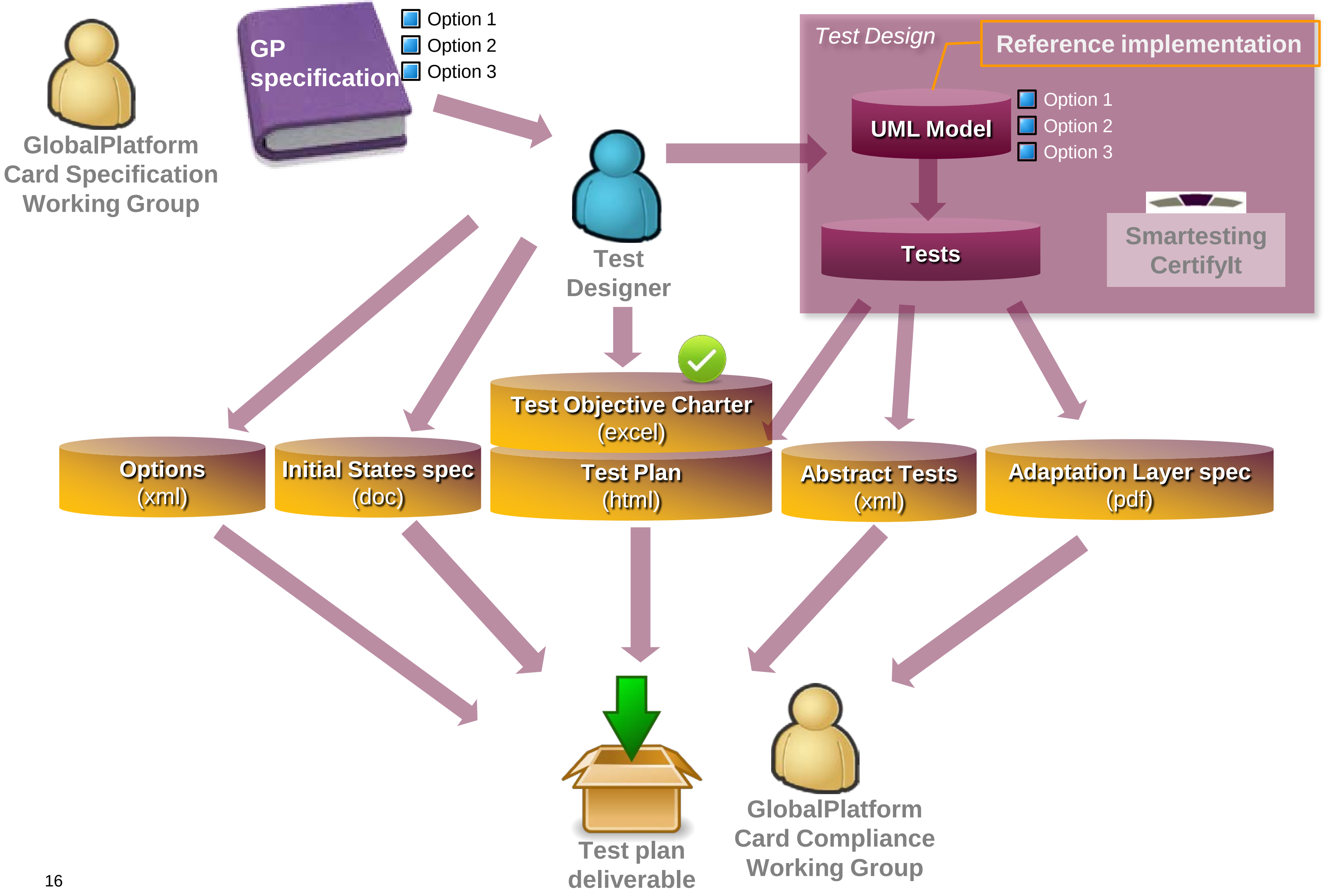
Test Objective Charter (excel)

GlobalPlatform Card Compliance Working Group

From Specifications to Test Plan deliverable



From Specifications to Test Plan deliverable

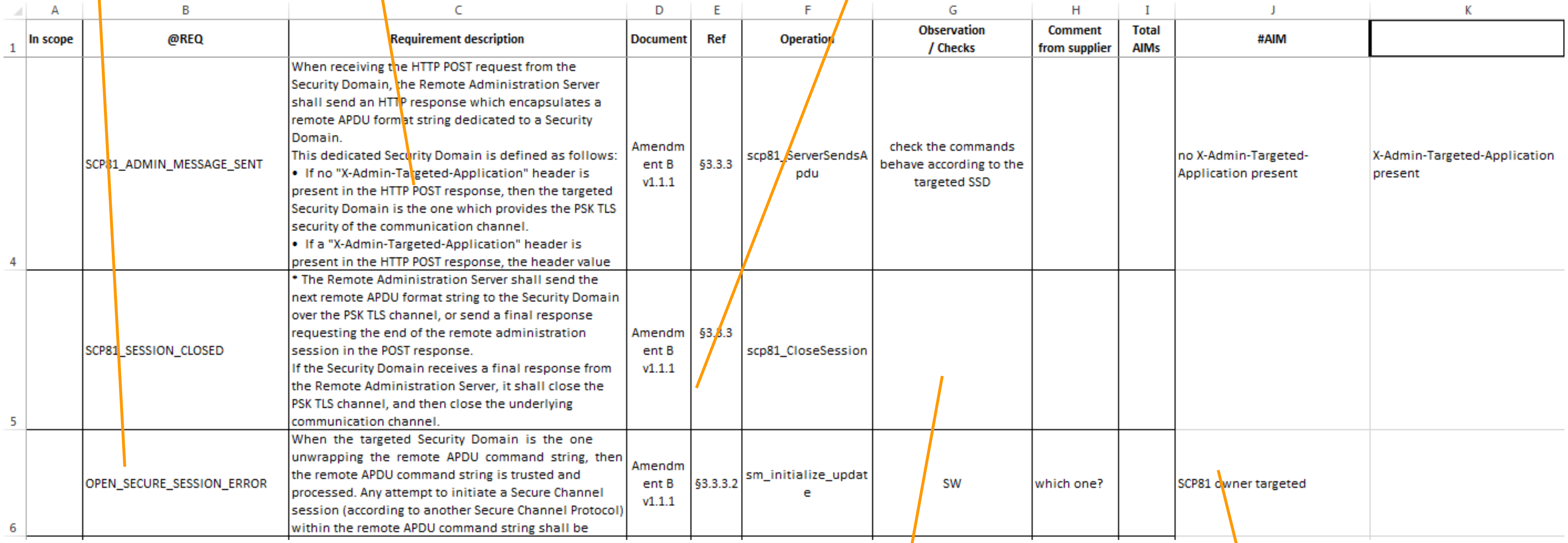


Test plan assets – Test Objective Charter

Requirement name

Requirement text from spec

Requirement references



	A	B	C	D	E	F	G	H	I	J	K
1	In scope	@REQ	Requirement description	Document	Ref	Operation	Observation / Checks	Comment from supplier	Total AIMs	#AIM	
4		SCP81_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 a 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 TLS security of the communication channel. • If a "X-Admin-Targeted-Application" header is present in the HTTP POST response, the header value	Amendment B v1.1.1	§3.3.3	scp81_ServerSendsApdu	check the commands behave according to the targeted SSD			no X-Admin-Targeted-Application present	X-Admin-Targeted-Application present
5		SCP81_SESSION_CLOSED	• The Remote Administration Server shall send the next remote APDU format string to the Security Domain over the PSK TLS 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 TLS channel, and then close the underlying communication channel.	Amendment B v1.1.1	§3.3.3	scp81_CloseSession					
6		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 v1.1.1	§3.3.3.2	sm_initialize_update	SW	which one?		SCP81 owner targeted	

On what is performed the requirement check

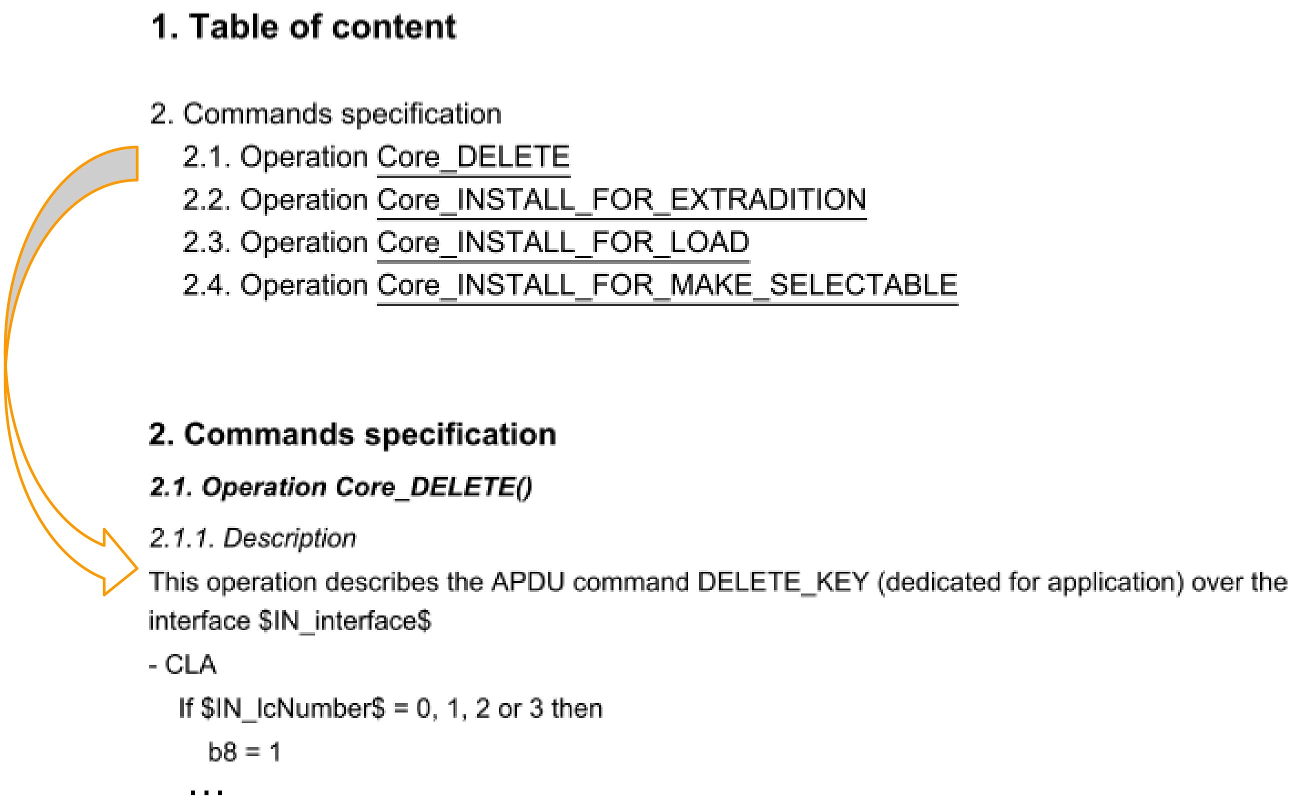
Sub-cases (aims)

Test plan assets - Options

```xml
<?xml version="1.0" encoding="UTF-8"?>
<cardConfiguration name="ID Configuration 1.0" date="2013-06-11" version="1.3">
  <!-- General configuration, shall not be changed -->
  <option name="conf_ProfileUICC" support="True" />
  <option name="conf_implementationSupportsSCP02" support="True" />
  <option name="conf_ISD_Configured_With_SCP02" support="True" />
  <option name="conf_implementationSupportsSCP81" support="True" />
  <option name="conf_implementationSupportSupplementarySD" support="True" />
  <!-- To be configured -->
  <option name="conf_ApduInstForInstallAndInstForMakeSelectableSupportForSdWithAuthorizedManagement" support="False" />
  <option name="conf_algo_AES_Supported" support="False" />
  <option name="conf_implementationSupportsSCP03" support="False" />
  <option name="conf_ApduInitializeUpdateSupportForOtherSD" support="False" />
  <option name="conf_ApduPutKeySupportForOtherSd" support="False" />
  <option name="conf_ApduGetStatusSupportForOtherSd" support="False" />
</cardConfiguration>
```

Description of all the options possible for a given product

Test plan assets – Adaptation Layer



1. Table of content

2. Commands specification

2.1. Operation Core_DELETE()

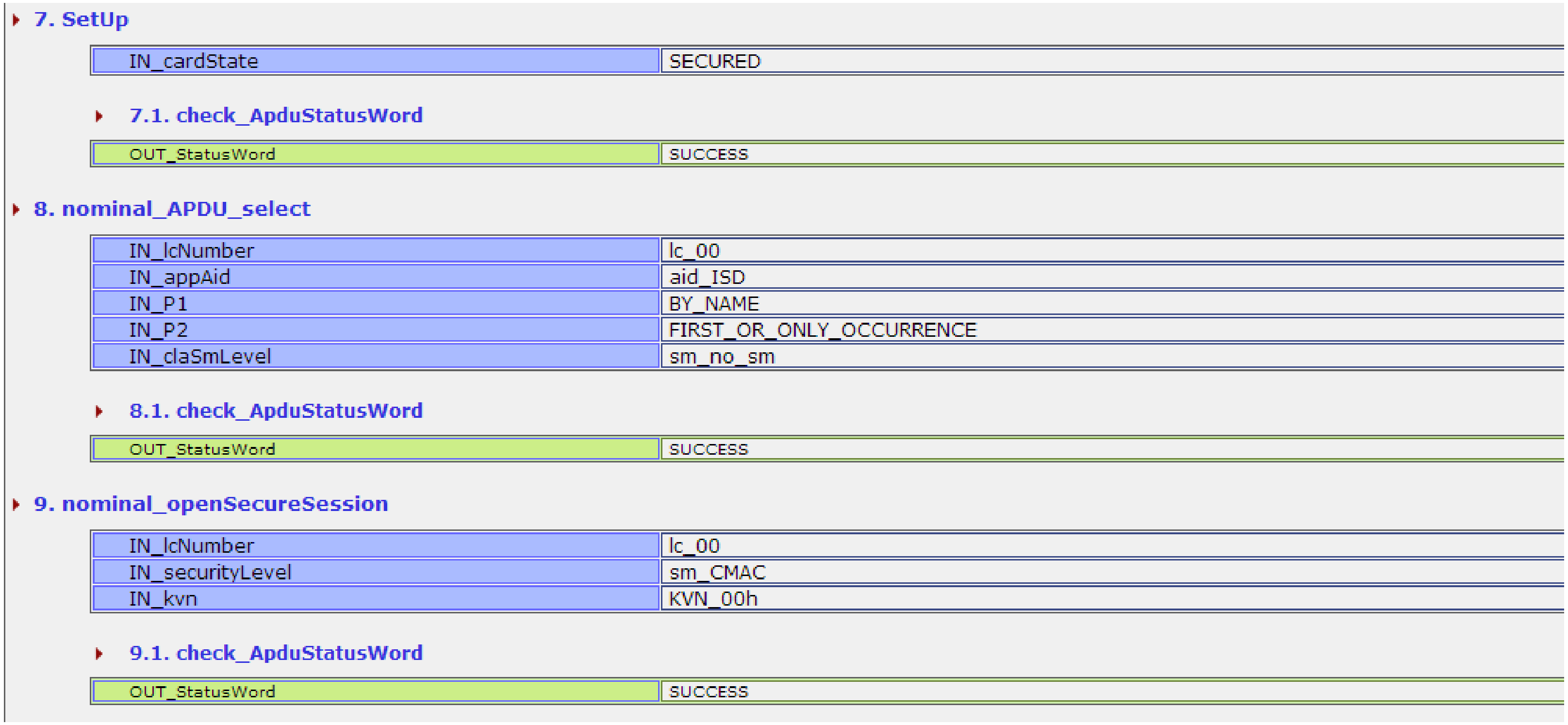
2.1.1. Description

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. check_ApduStatusWord

OUT_StatusWord	SUCCESS

8. nominal_APDU_select

IN_lcNumber	lc_00
IN_appAid	aid_ISD
IN_P1	BY_NAME
IN_P2	FIRST_OR_ONLY_OCCURRENCE
IN_claSmLevel	sm_no_sm

8.1. check_ApduStatusWord

OUT_StatusWord	SUCCESS

9. nominal_openSecureSession

IN_lcNumber	lc_00
IN_securityLevel	sm_CMAC
IN_kvn	KVN_00h

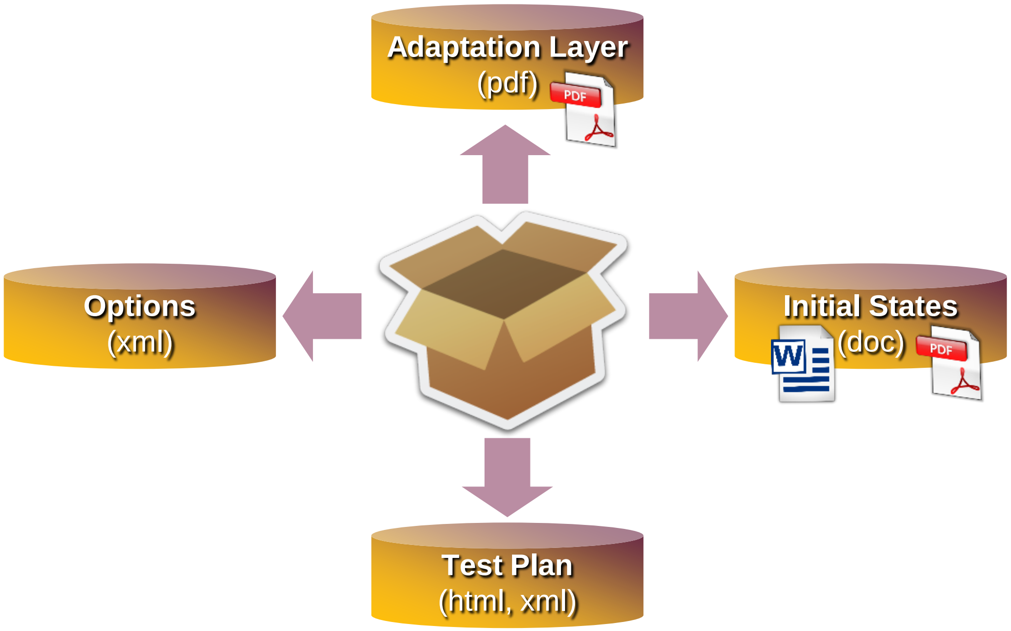
9.1. check_ApduStatusWord

OUT_StatusWord	SUCCESS

Commands are identical in html and xml.

Html is readable, contains a requirement summary and a test overview.

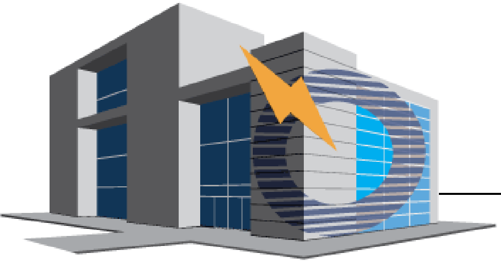
Test plan deliverable



GlobalPlatform
Card Compliance
Working Group

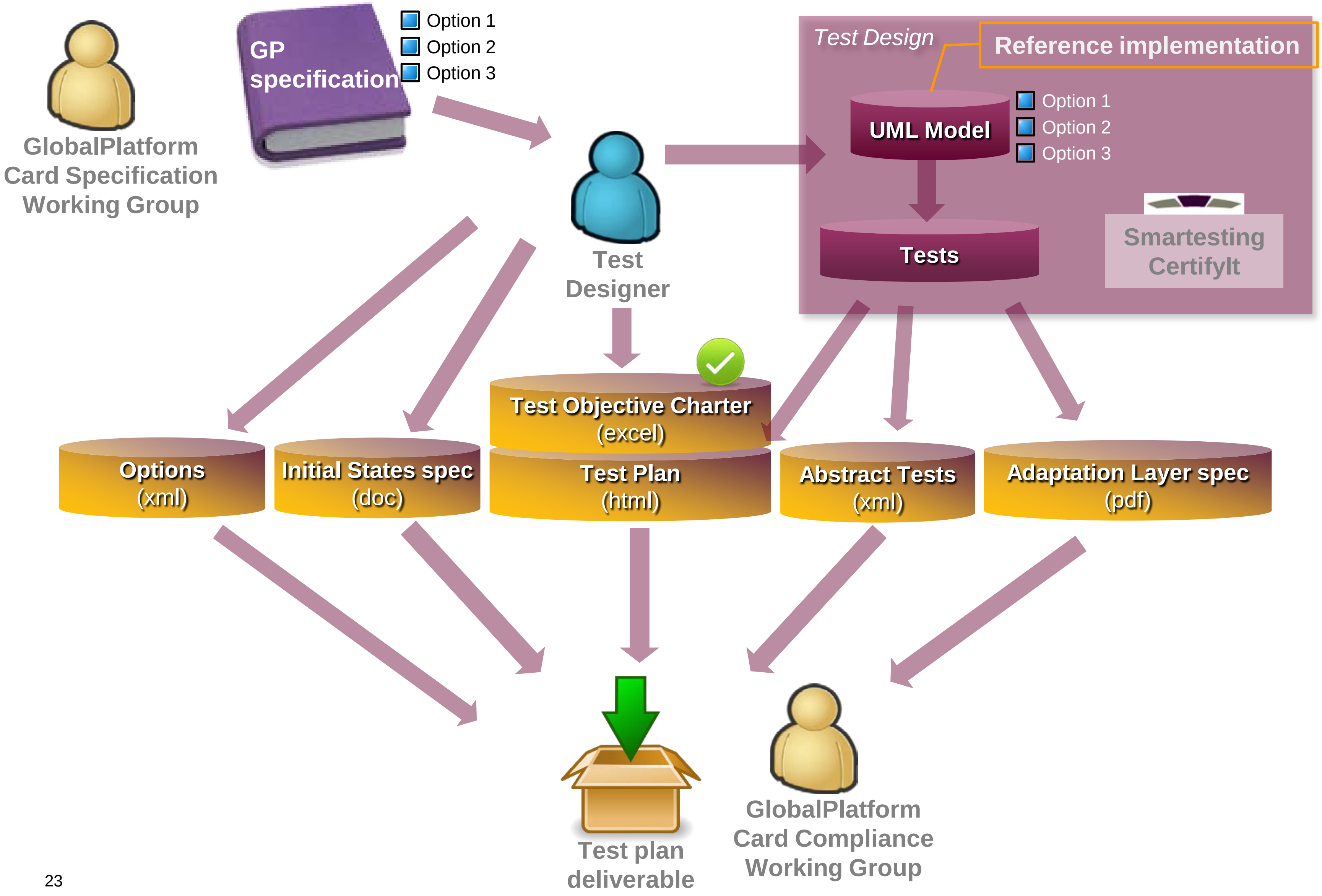
Test tools

Product vendors

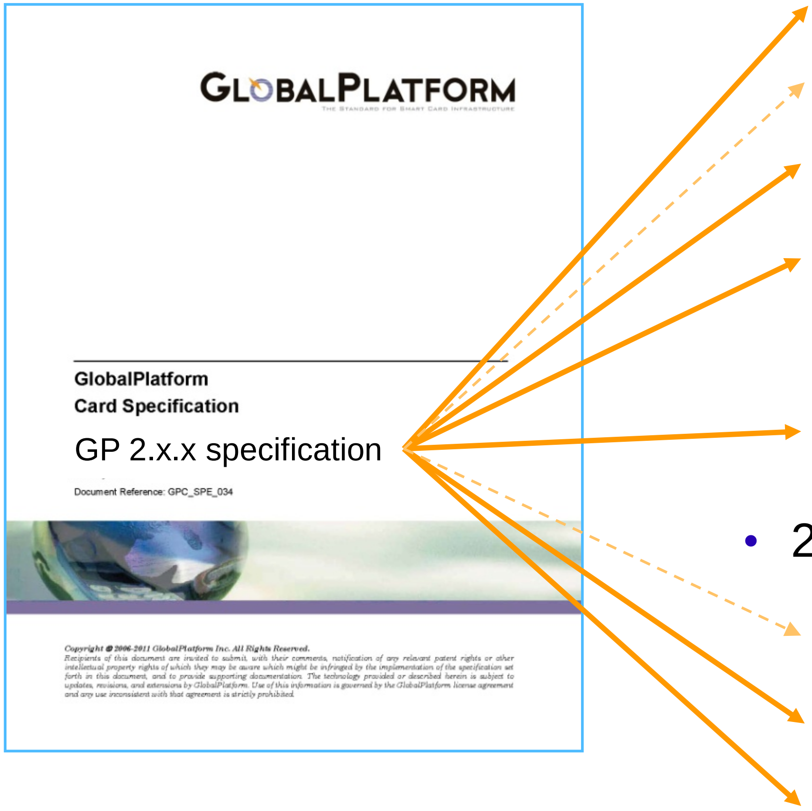


Reusability

From Specifications to Test Plan deliverable



Specifications and test suites road map



GLOBALPLATFORM
THE STANDARD FOR SMART CARD INFRASTRUCTURE

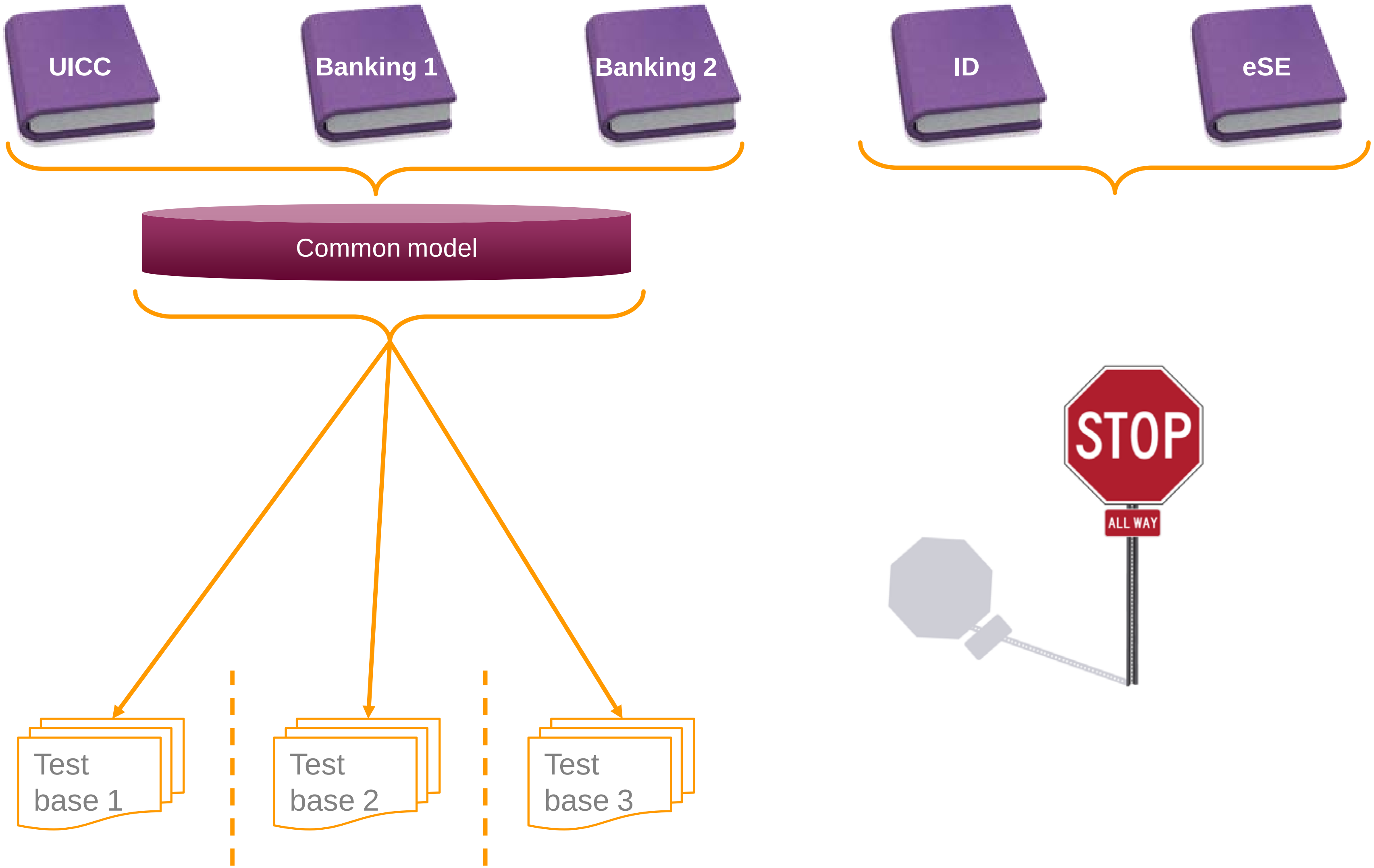
GlobalPlatform
Card Specification

GP 2.x.x specification

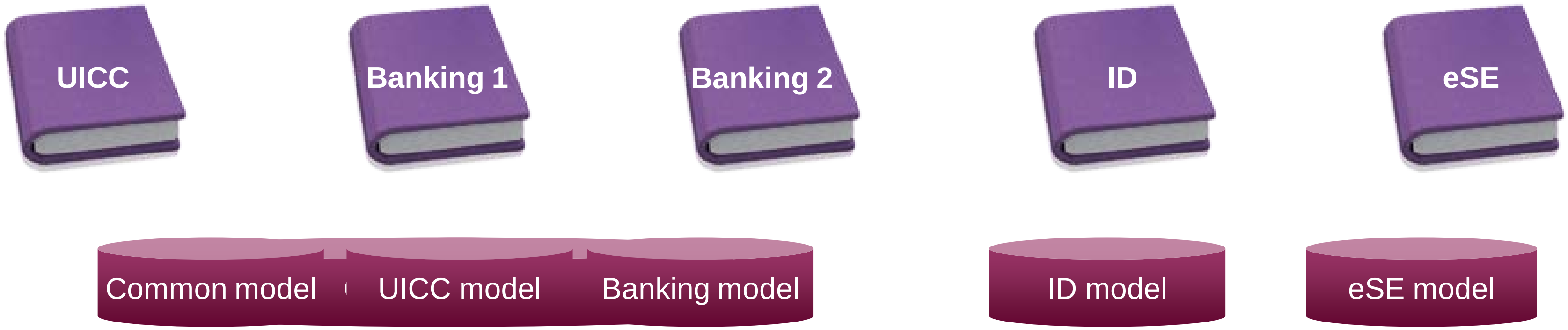
Document Reference: GPC_SPE_034

- 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



New way of work - Reusability addressed



UICC

Banking 1

Banking 2

ID

eSE

Common model

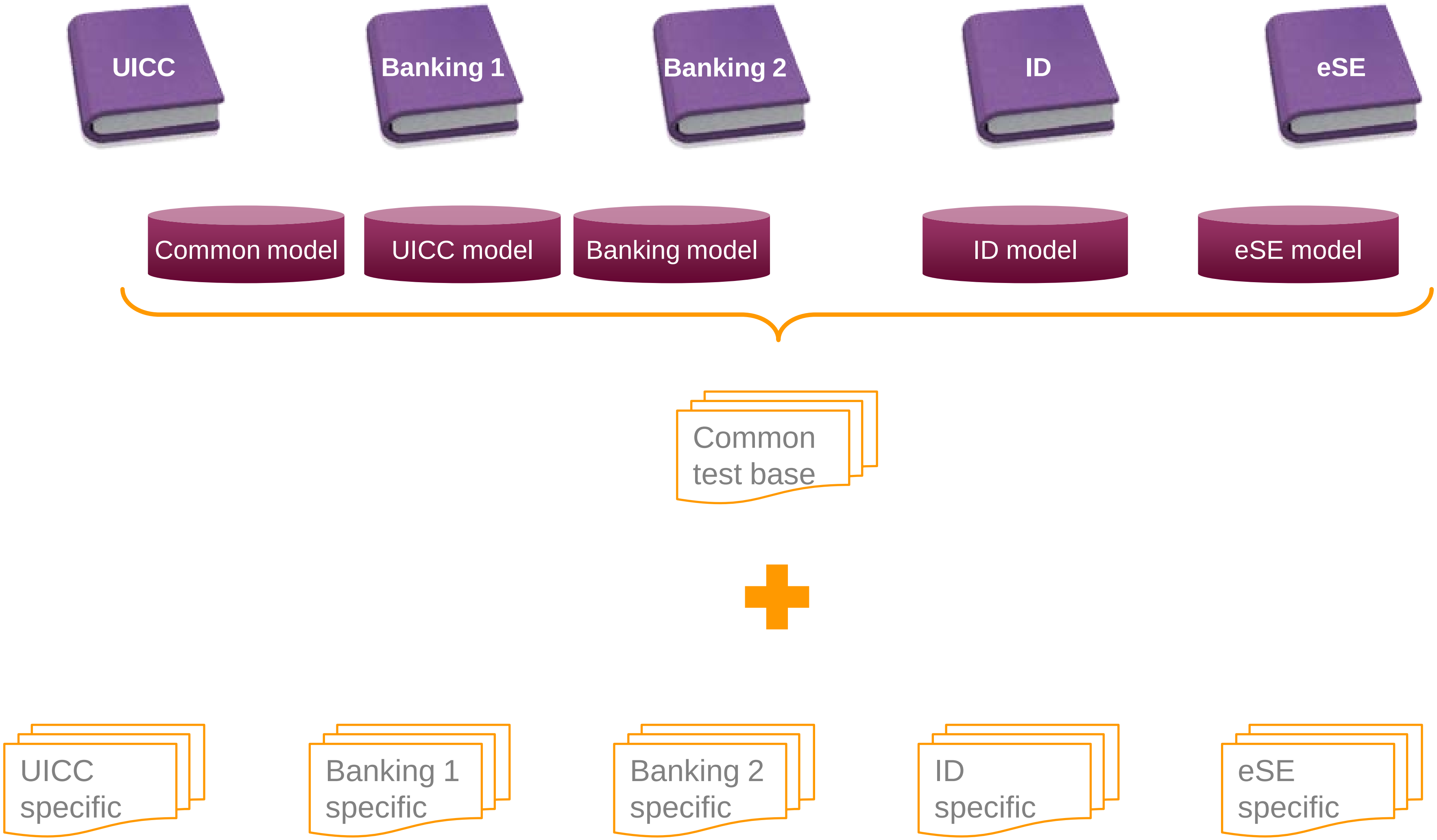
UICC model

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

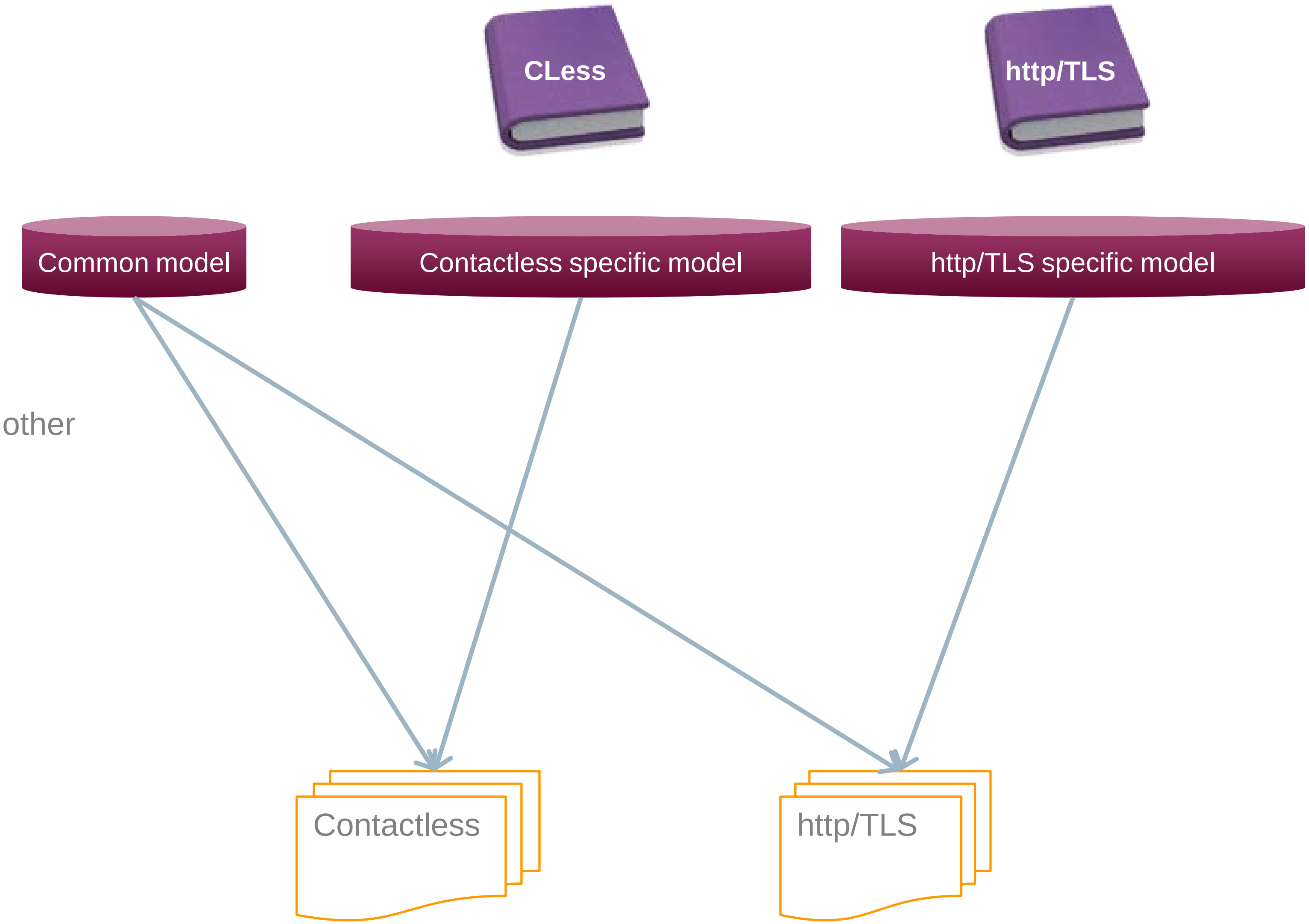
Banking 1 specific

Banking 2 specific

ID specific

eSE specific

Reusability addressed



Ground for other test suites

Reusability summary - modelization

Model behavior

- 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

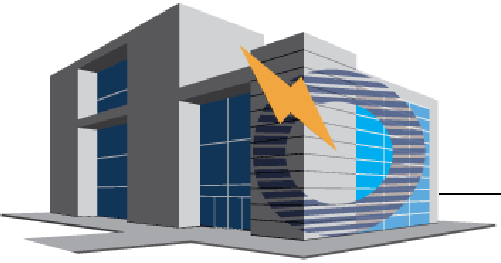
```
<common part>
IF ‘configuration X’ applies THEN
            The expected behaviors and results for X are applicable
```

Initial states

- 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

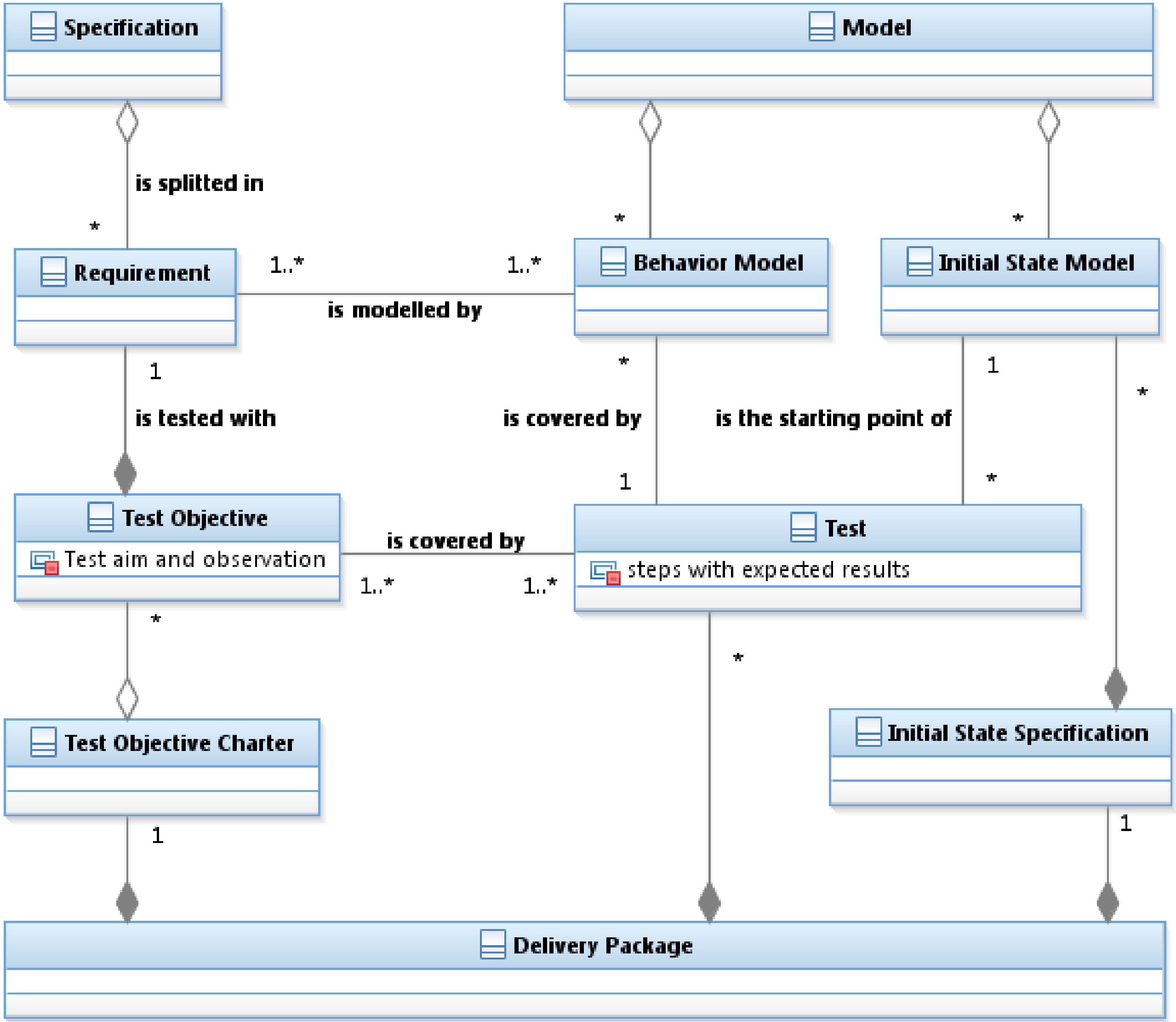
Common test base

- Test content



Work setup

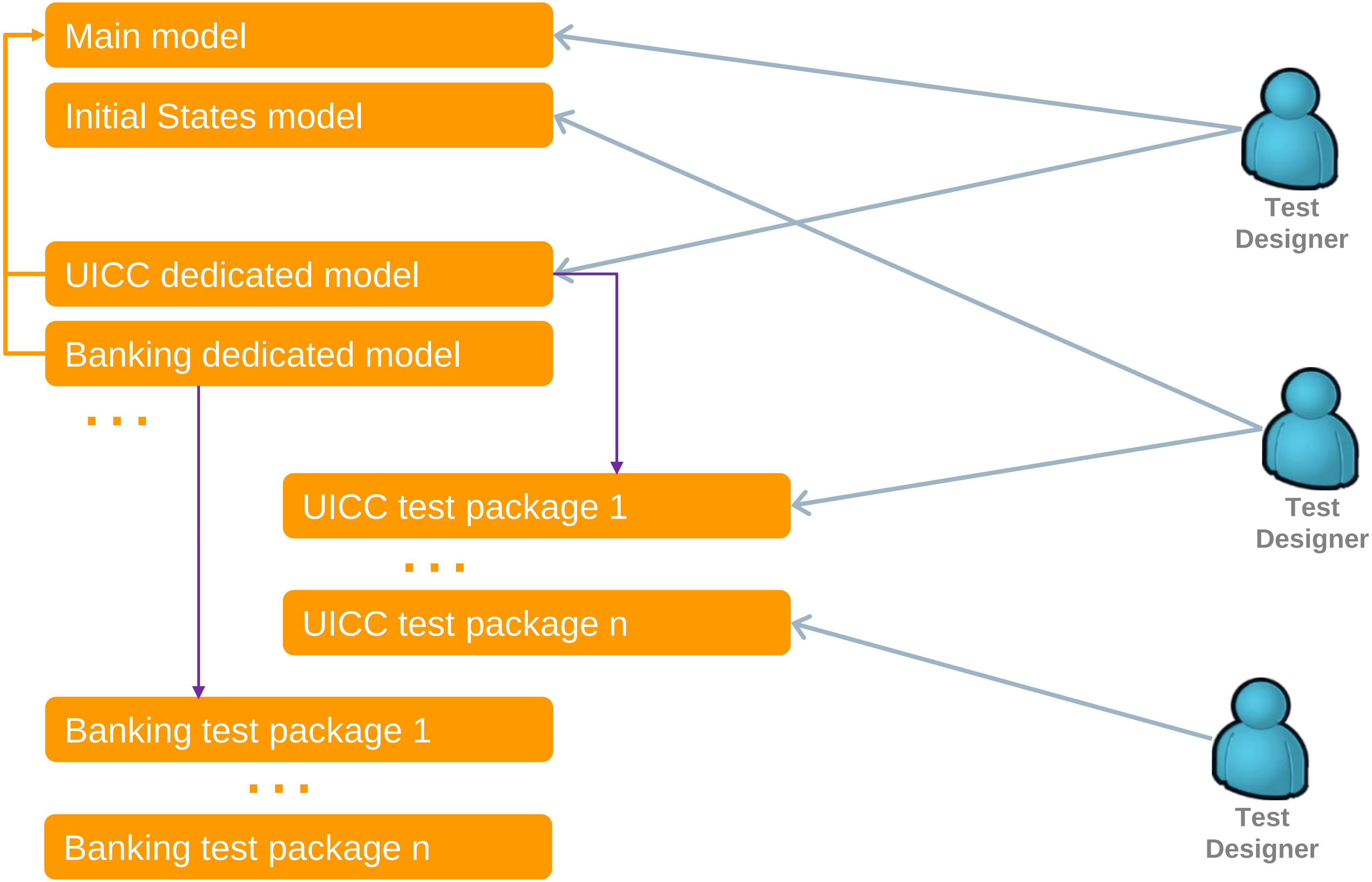
Concepts

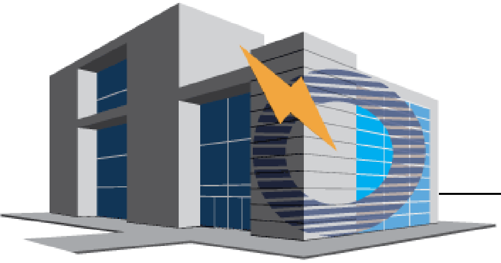

Specification
Model
is splitted in
*
*
*
Requirement
1..*
1..*
Behavior Model
Initial State Model
is modelled by
1
*
1
*
is tested with
is covered by
is the starting point of
1
*
Test Objective
Test aim and observation
is covered by
Test
steps with expected results
1..*
1..*
*
*
Test Objective Charter
Initial State Specification
1
1
Delivery Package

Work environment

Main model	• Original model
Initial States model	• Default values for instances, all projects
UICC dedicated model	• Model covering the spec 1 requirements
Banking dedicated model	• Model covering the spec 2 requirements
. . .	
UICC test package 1	• UICC test package on topic 1
. . .	
UICC test package n	• UICC test package on topic n
Banking test package 1	• Banking test package on topic 1
. . .	
Banking test package n	• Banking test package on topic n

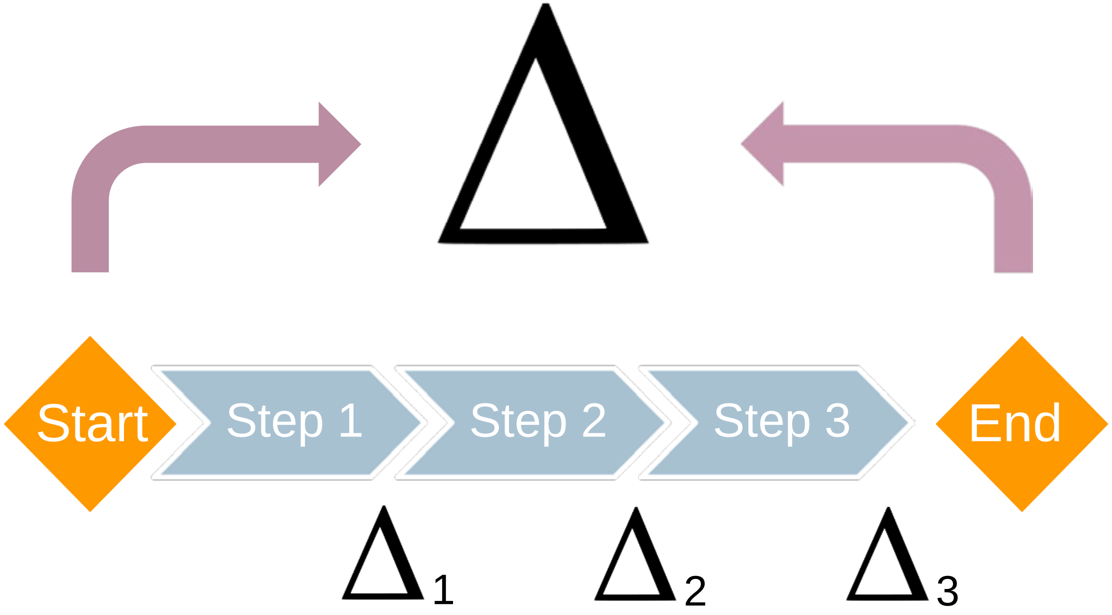
Collaborative work





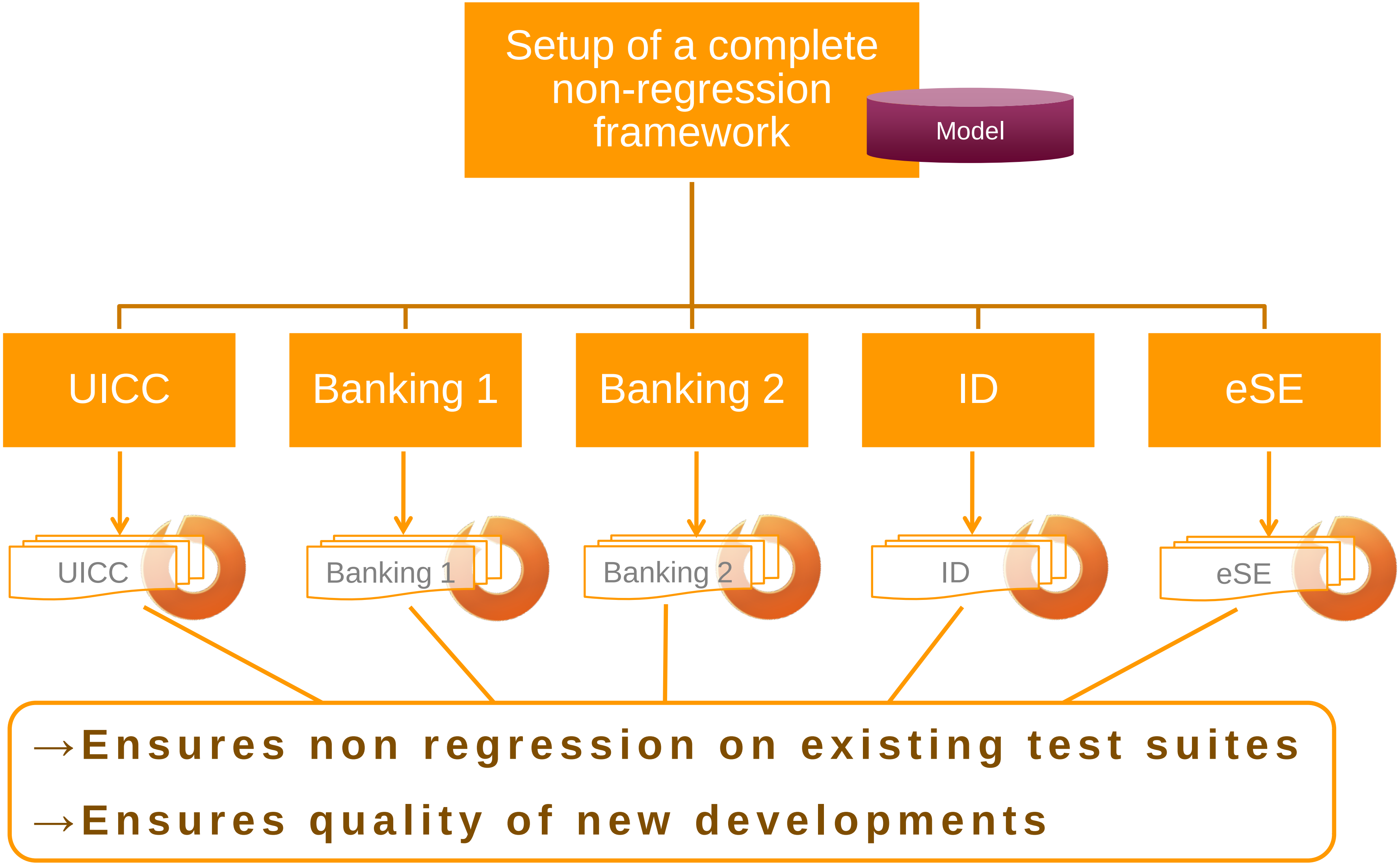
Quality

Development steps



Monitoring the progression is key for quality deliverables

Ensuring non regression



Setup of a complete non-regression framework

UICC

Banking 1

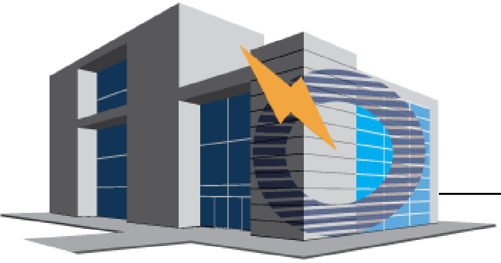
Banking 2

ID

eSE

→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

Before TestFests

During TestFests

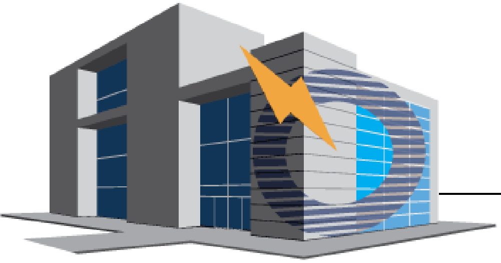
Δ

- 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

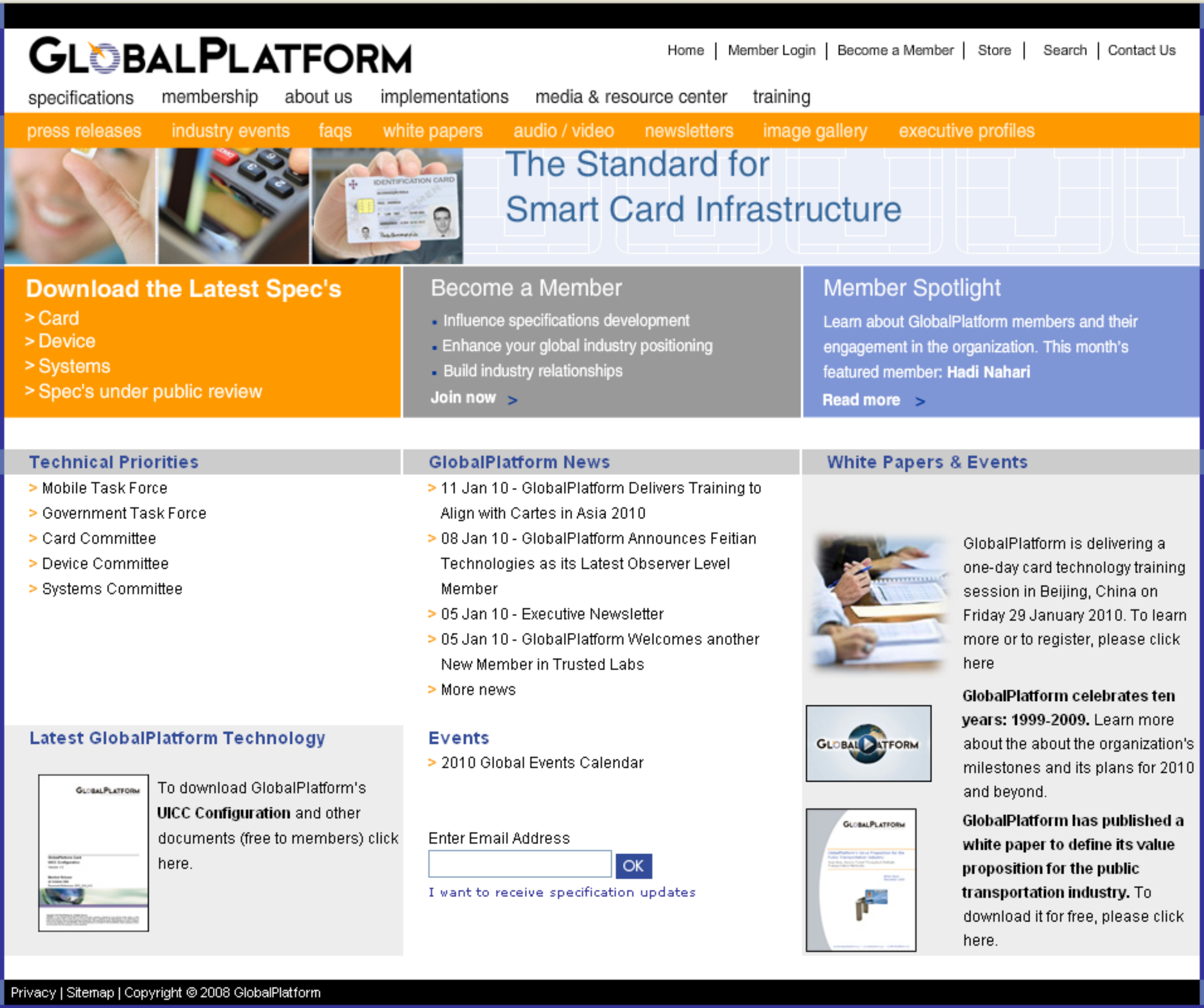
- Moving from document to HTML document is not immediate

- 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

Visit us @ www.globalplatform.org



Home | Member Login | Become a Member | Store | Search | Contact Us

specifications membership about us implementations media & resource center training

press releases industry events faqs white papers audio / video newsletters image gallery executive profiles

The Standard for Smart Card Infrastructure

Download the Latest Spec's

> Card
> Device
> Systems
> Spec's under public review

Become a Member

- Influence specifications development
- Enhance your global industry positioning
- Build industry relationships

Join now >

Member Spotlight

Learn about GlobalPlatform members and their engagement in the organization. This month's featured member: **Hadi Nahari**

Read more >

Technical Priorities

> Mobile Task Force
> Government Task Force
> Card Committee
> Device Committee
> Systems Committee

GlobalPlatform News

> 11 Jan 10 - GlobalPlatform Delivers Training to Align with Cartes in Asia 2010
> 08 Jan 10 - GlobalPlatform Announces Feitian Technologies as its Latest Observer Level Member
> 05 Jan 10 - Executive Newsletter
> 05 Jan 10 - GlobalPlatform Welcomes another New Member in Trusted Labs
> More news

White Papers & Events

GlobalPlatform is delivering a one-day card technology training session in Beijing, China on Friday 29 January 2010. To learn more or to register, please click here

GlobalPlatform celebrates ten years: 1999-2009. Learn more about the about the organization's milestones and its plans for 2010 and beyond.

GlobalPlatform has published a white paper to define its value proposition for the public transportation industry. To download it for free, please click here.

Latest GlobalPlatform Technology

To download GlobalPlatform's **UICC Configuration** and other documents (free to members) click here.

Events

> 2010 Global Events Calendar

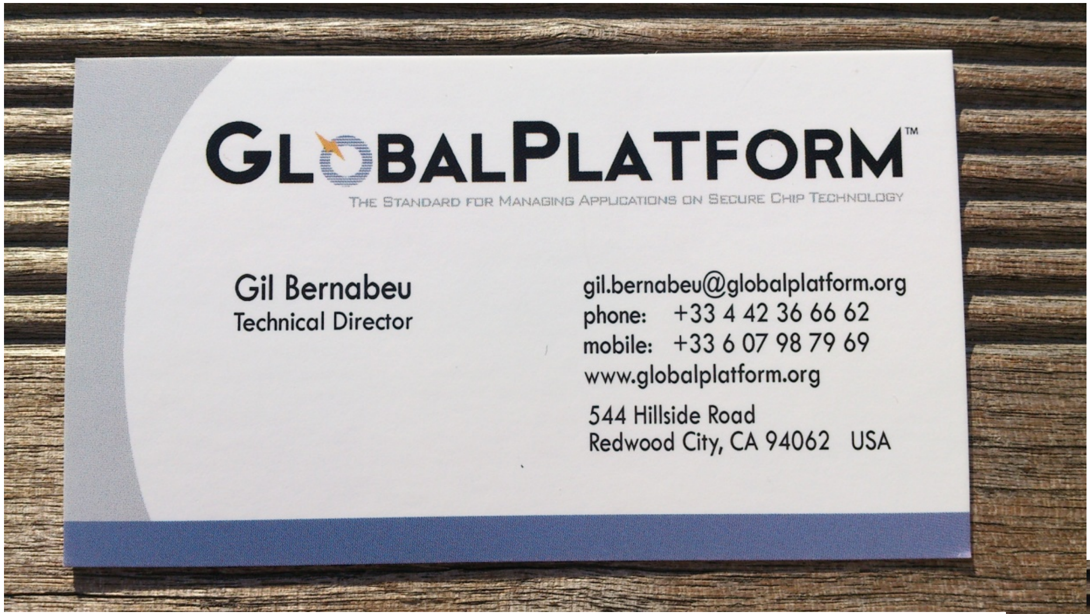
Enter Email Address

OK

I want to receive specification updates

Privacy | Sitemap | Copyright © 2008 GlobalPlatform

More information



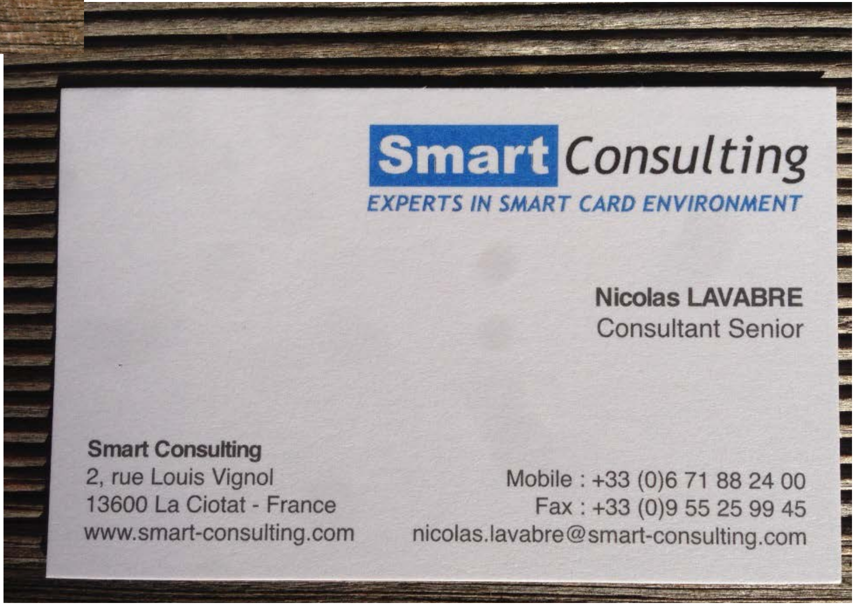
GLOBALPLATFORM™

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