GLOBALPLATFORM™

GlobalPlatform Roadmap and its applicability to PIV

Jerôme Becquart
GlobalPlatform Government Task Force leader

@GlobalPlatform_

www.linkedin.com/company/globalplatform

GlobalPlatform 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 to define technology standards for cards, devices and systems and create foundation for future growth.
- License royalty-free card, device, and systems specifications.
- Compliance Program tools to verify card, device, systems compliance to GlobalPlatform technology.
- Foster adoption of secure chip technology standards and implementations across industries.

GlobalPlatform Members

AMD · AMERICAN EXPRESS · ARM · athena Smartcard · at&t · BlackBerry

COMPRION · Clear2Pay · ERICSSON · FeliCa Networks · FIME · Galitt

gemalto security to be free · Giesecke & Devrient · Good · HID · infineon · 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 · TL Trusted Labs · TRUSTONIC · UL · verizon wireless · VISA

Applus · BARNES INTERNATIONAL · DNP · TÜV SÜD Japan · iCTK

secunet IT security beyond expectations · SK C&C · TELUS · Texas Instruments · FINGERPRINTS · TOSHIBA · VALID

ABnote · aconite · BARCLAYS · Bell ID® · i-FREE · BROADCOM. · CB · CESG · consult hyperion securing tomorrow's transactions · UnionPay 银联 中国银联 China UnionPay · CROCUS Technology Blossoming future · CRYPTOMAThIC www.cryptomathic.com

Datang Microelectronics · Department of Defense United States of America · DatacardGroup · DISCOVER · Discretix trust • embedded · DYNAMICS · 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.

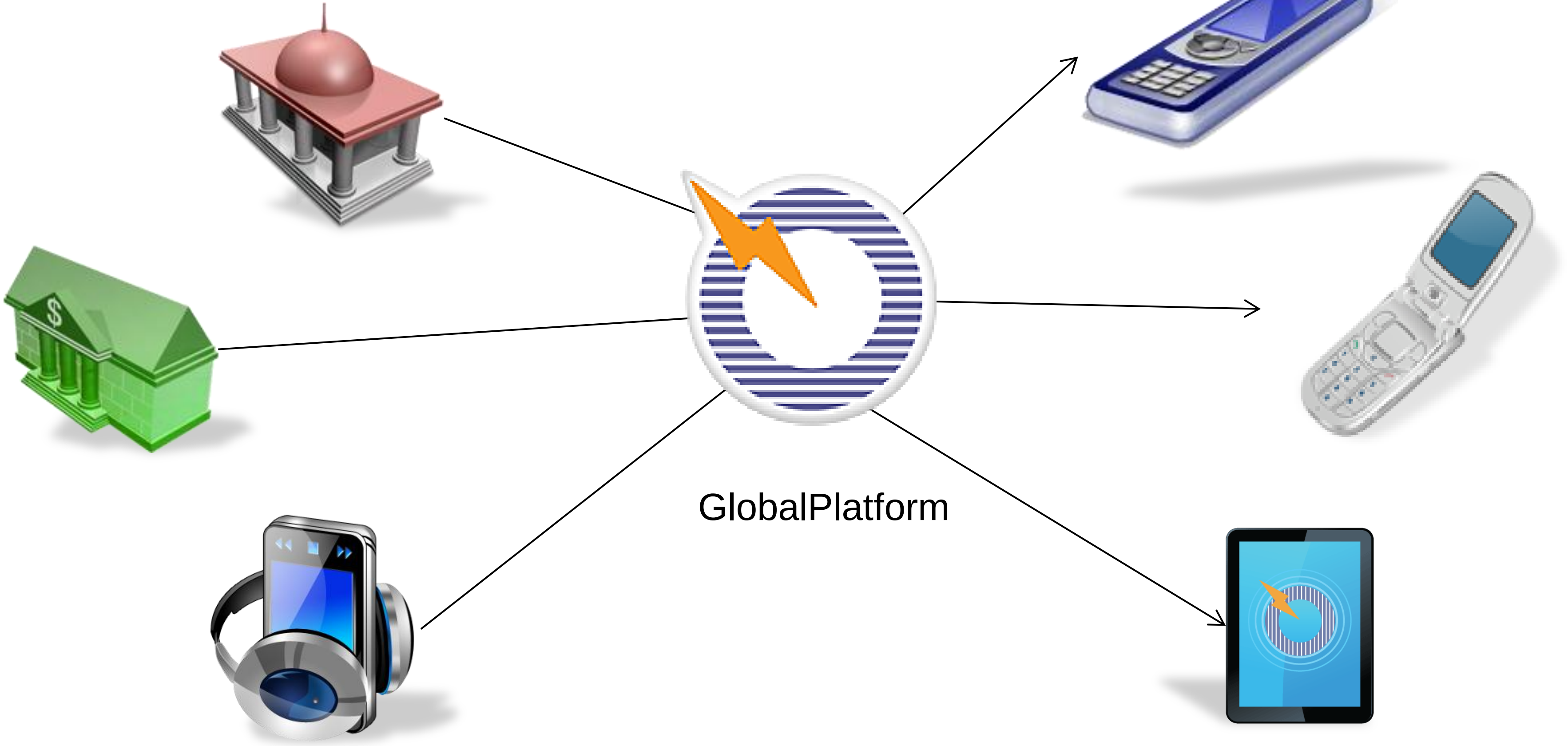
恒宝股份 HENGBAO CO.,LTD. · HITACHI Inspire the Next · HUAWEI · intercede™ · ISIS™ · JCB Good times start here. · kona i · LG · LG CNS · MARVELL · monetech · NEC · NEXTENDIS · Plastic Card

Posteitaliane · Proxama · Real Casa de la Moneda Fábrica Nacional de Moneda y Timbre · Redsýs · 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 · Watchdata · wave · XROMB

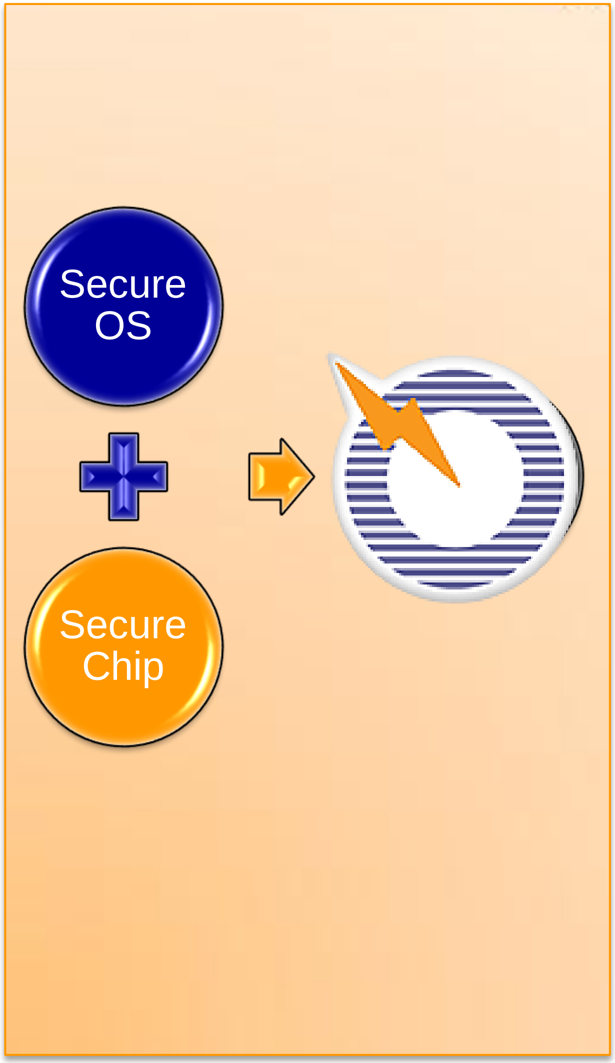
Introducing GlobalPlatform Standards...

- Create once based on -
  - Stable and interoperable Application Programming Interfaces (APIs)
  - Stable security requirement
- Deploy ‘everywhere’

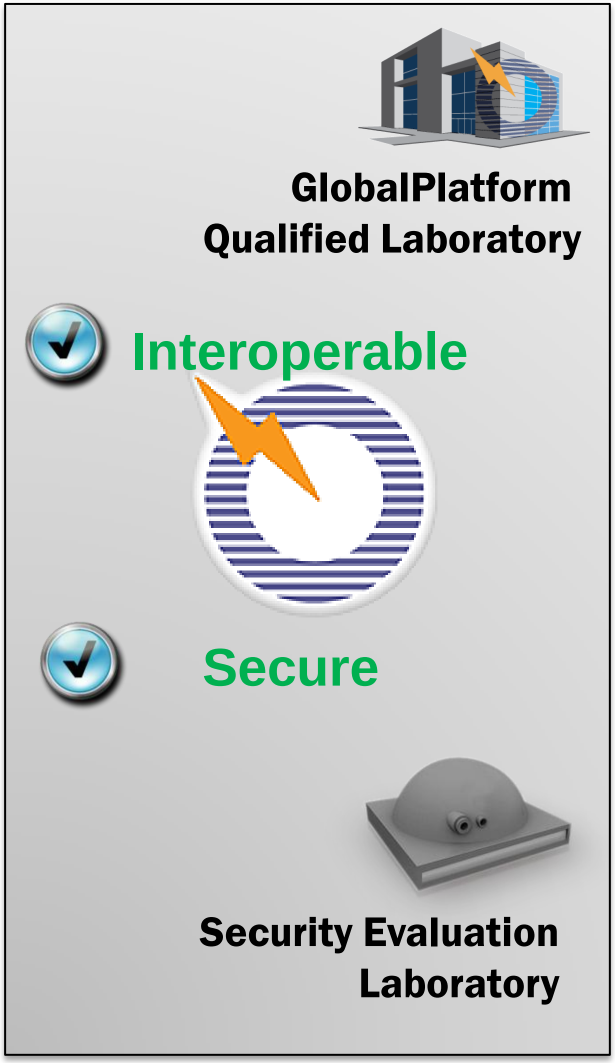


Our vision for security

Secure Chip technology



3rd party qualification and certification

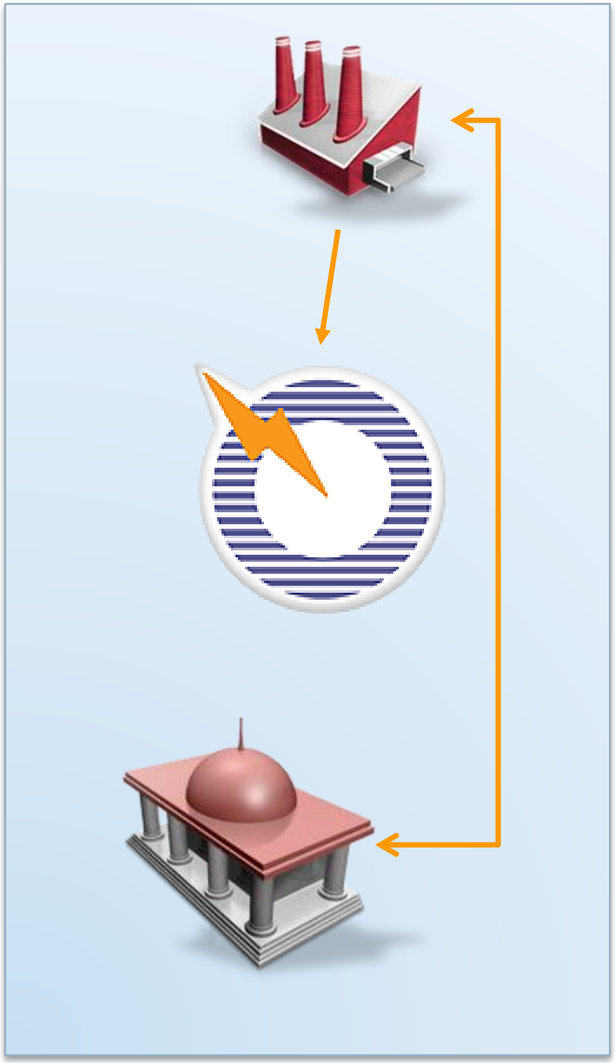

GlobalPlatform Qualified Laboratory

Interoperable

Secure

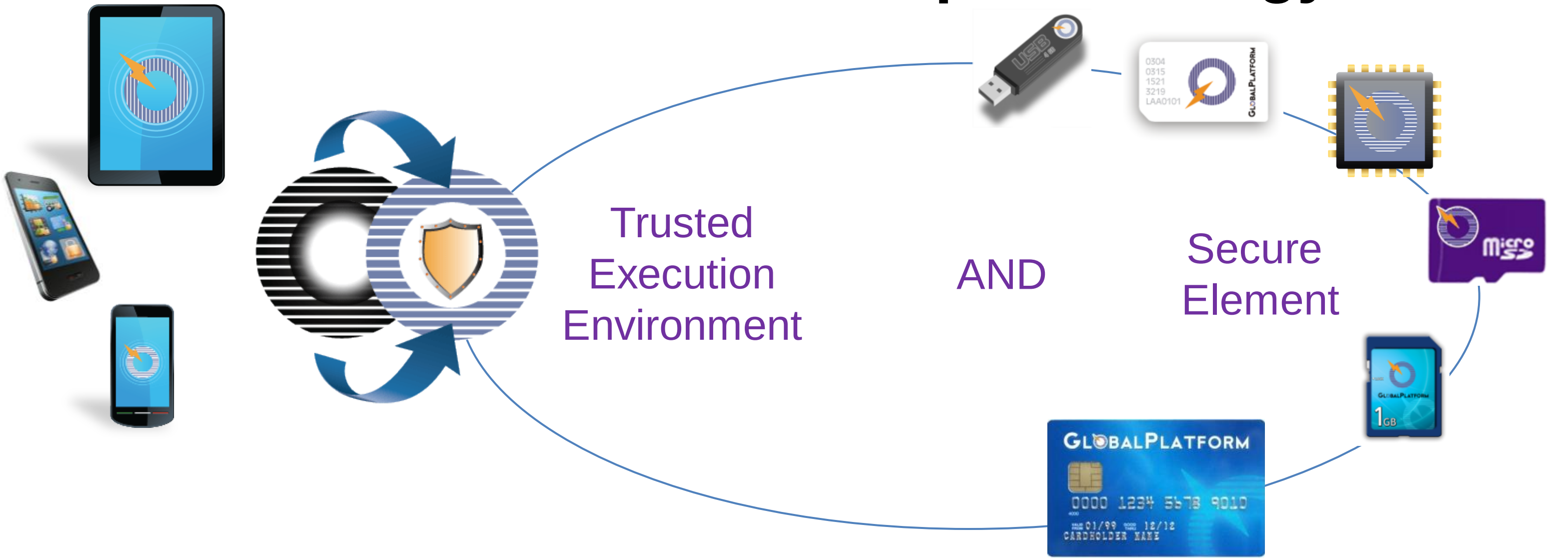
Security Evaluation Laboratory

Secure Key Management



GlobalPlatform Positioning

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



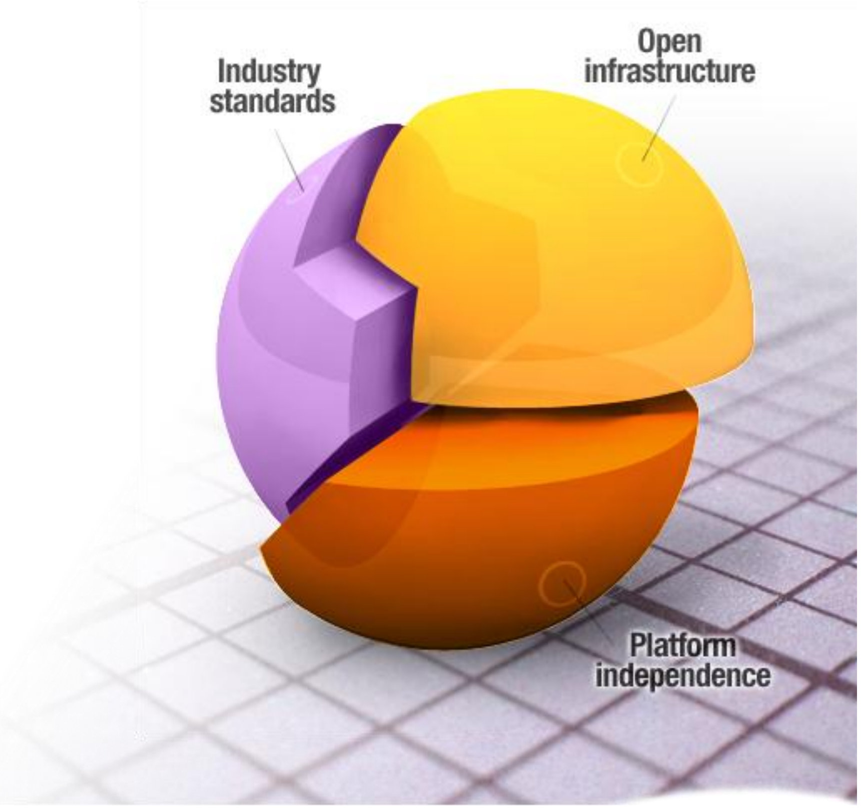
Trusted Execution Environment

AND

Secure Element

Across several market sectors and in converging sectors

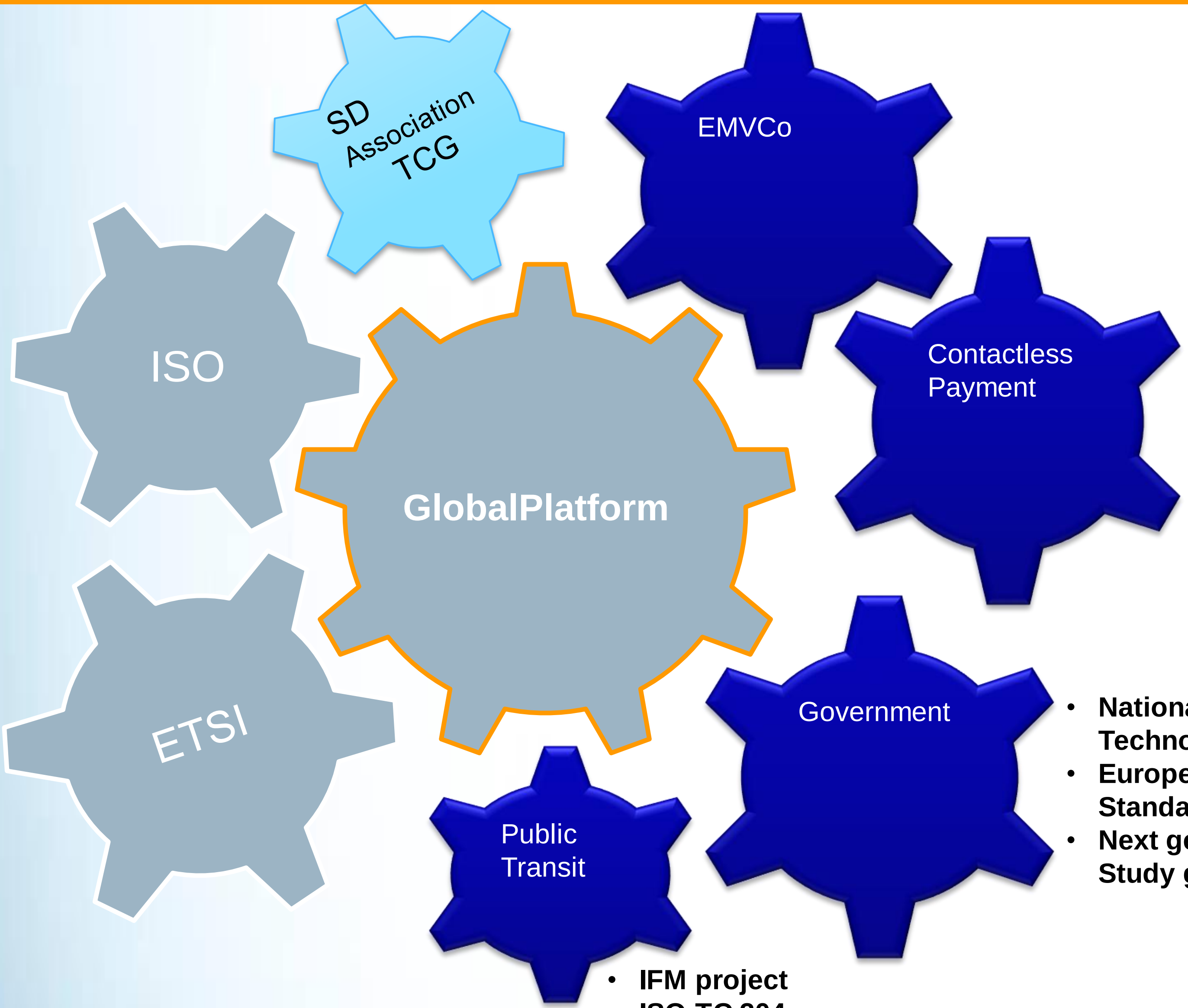
GlobalPlatform At-a-Glance



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

Result of Collaboration



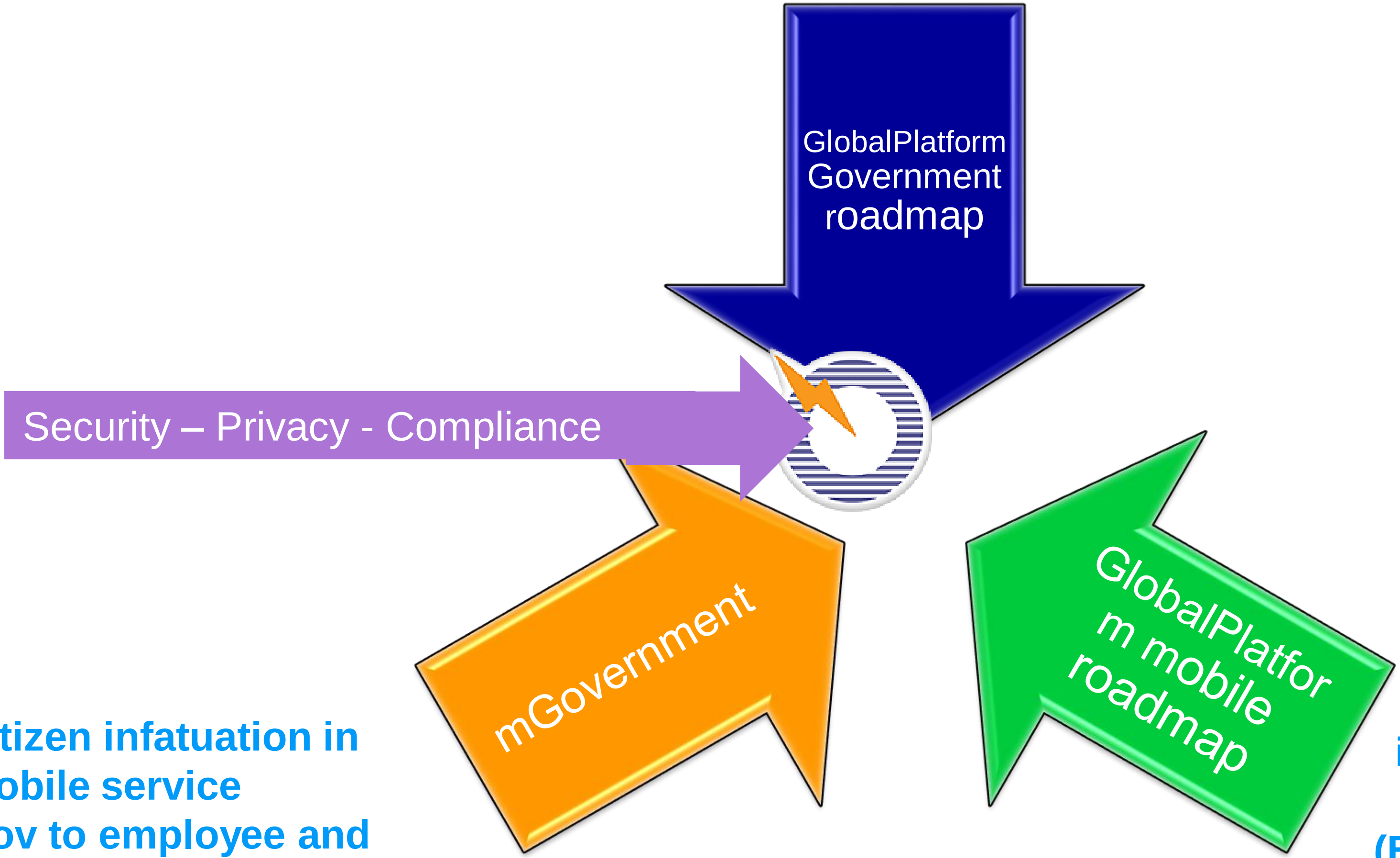
- GSMA Pay-Buy Mobile
- Mobey Forum
- Payez Mobile
- European Payments Council (EPC)
- StolPan
- SIMAlliance

- National Institute of Standards and Technology (NIST)
- European Committee for Standardization (CEN)
- Next generation Ic Card System Study group (NICSS)

- IFM project
- ISO TC 204

GlobalPlatform at the center of Convergence

Government mandates on Security and Privacy


GlobalPlatform Government roadmap
Security – Privacy - Compliance
mGovernment
GlobalPlatform mobile roadmap

Citizen infatuation in mobile service
Gov to employee and BYOD requirements

Other markets interests in mobile services
(Banks, MNO, Over-The-Top)

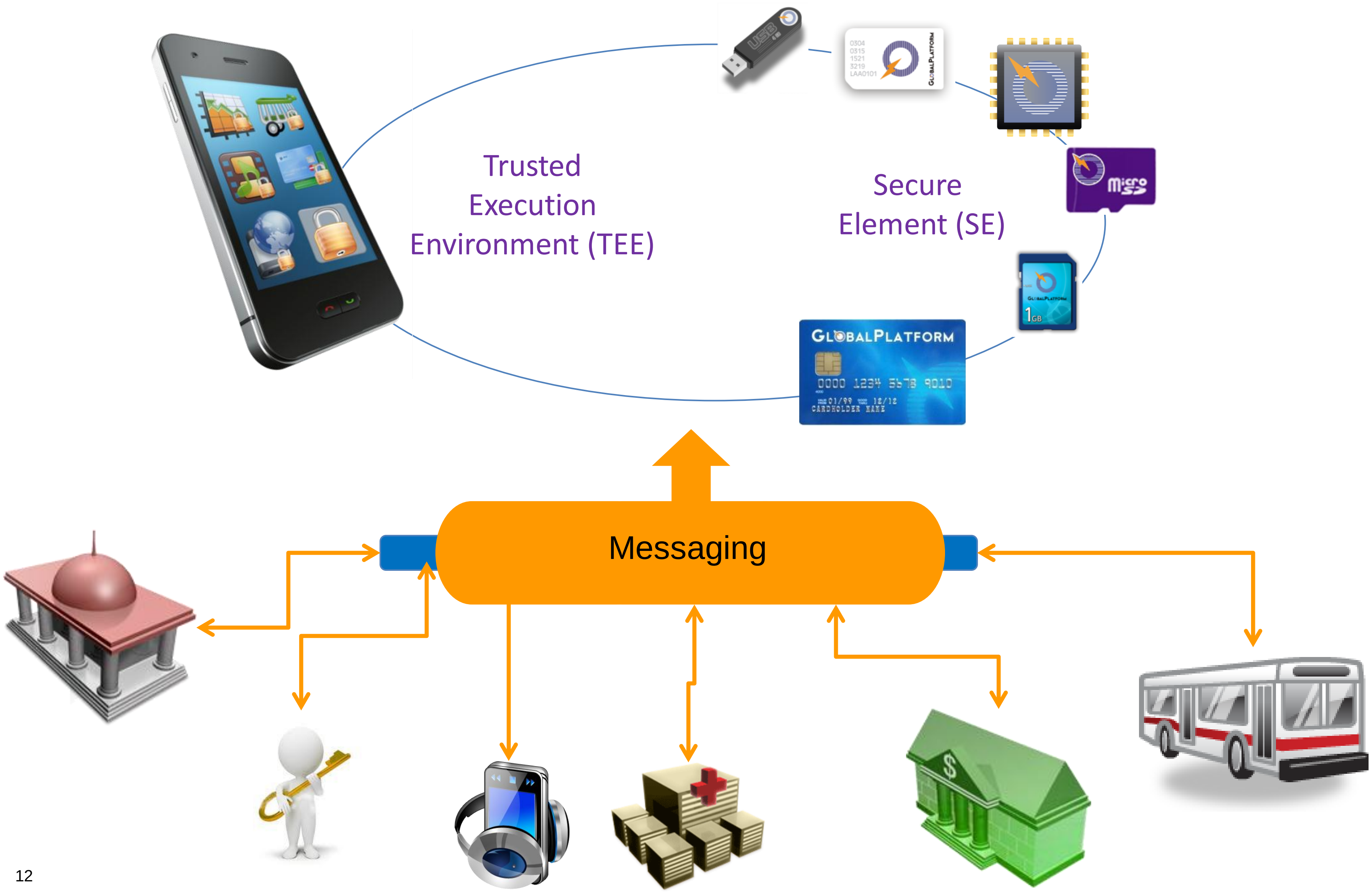
Strong Rate of Growth

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

- In 2012, more than 2 billions of GlobalPlatform cards have been produced

- More than 100 publicized implementations across financial, ID/Security, government, mobile telecom, and healthcare markets.

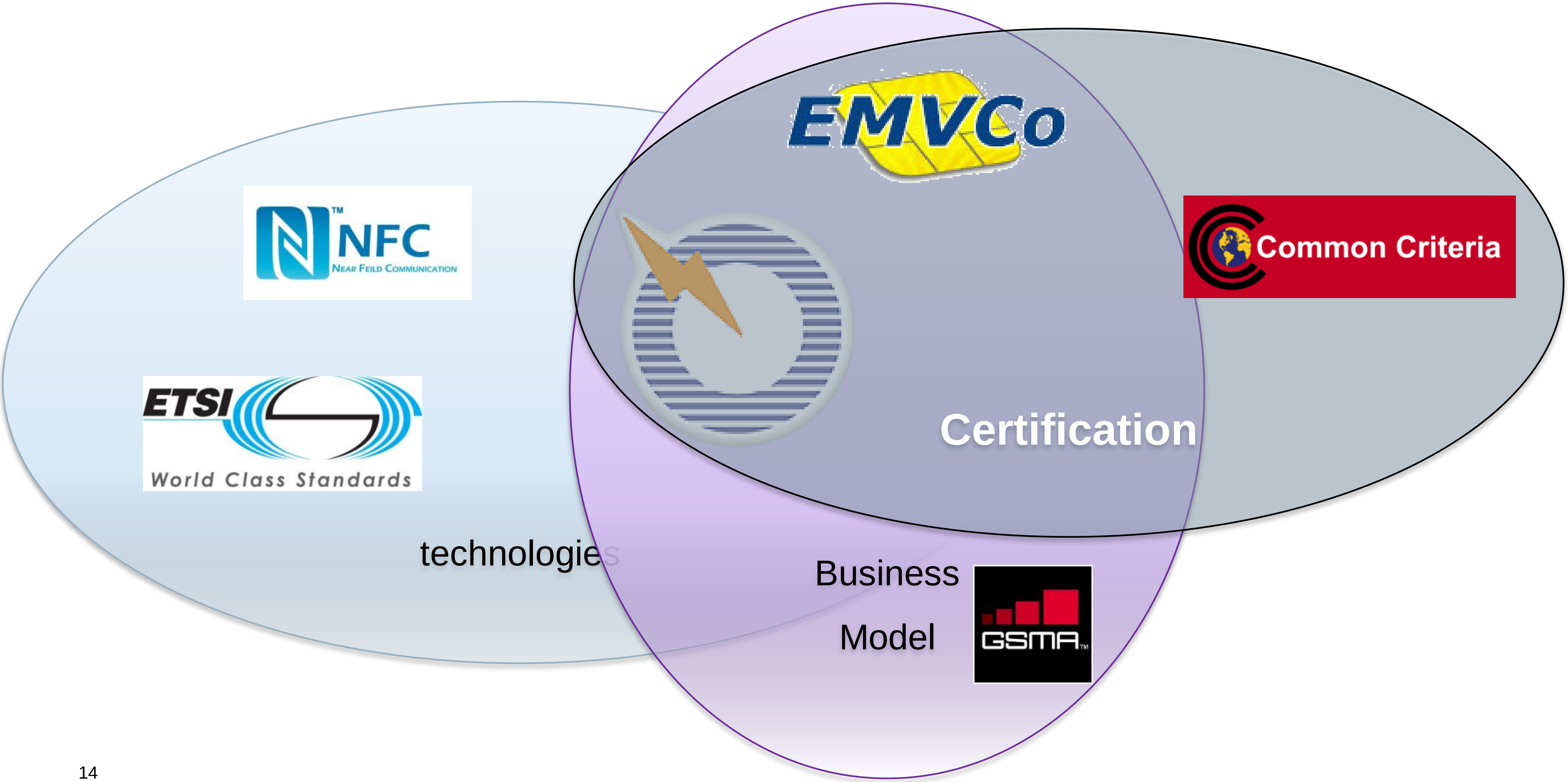
3 Technologies available



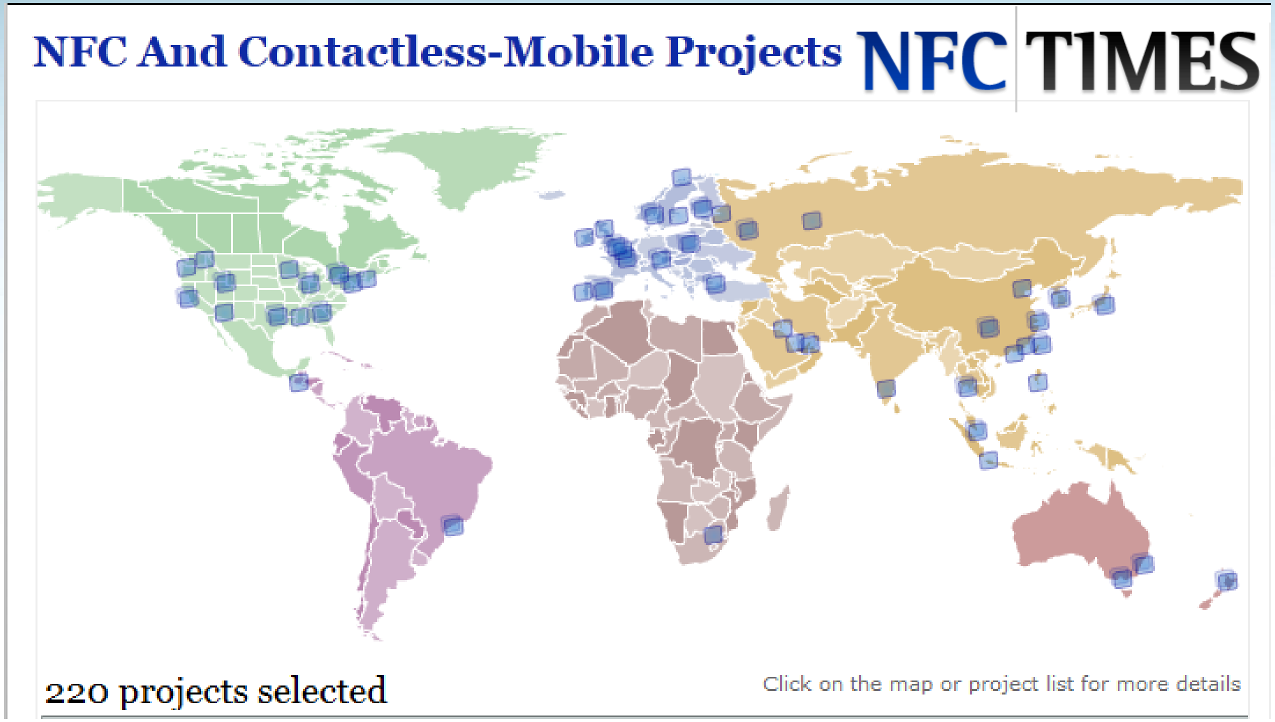
Card and Secure element technology

Multiple services from Different actors : a reality now with NFC deployment

- Based on GlobalPlatform technology a complete framework has been created to allow a banking application to be loaded in a UICC /SIM card



Foundation of the Mobile Contactless Technology Eco-system



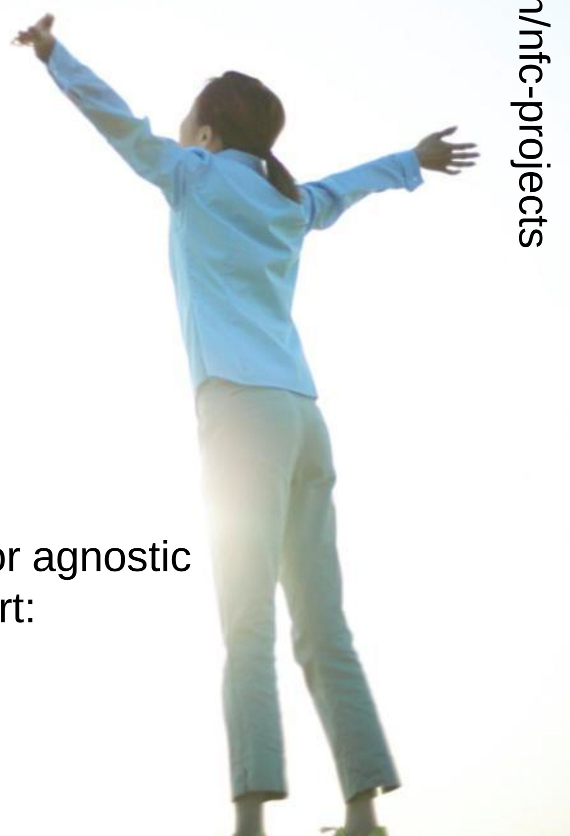
NFC And Contactless-Mobile Projects NFC TIMES

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



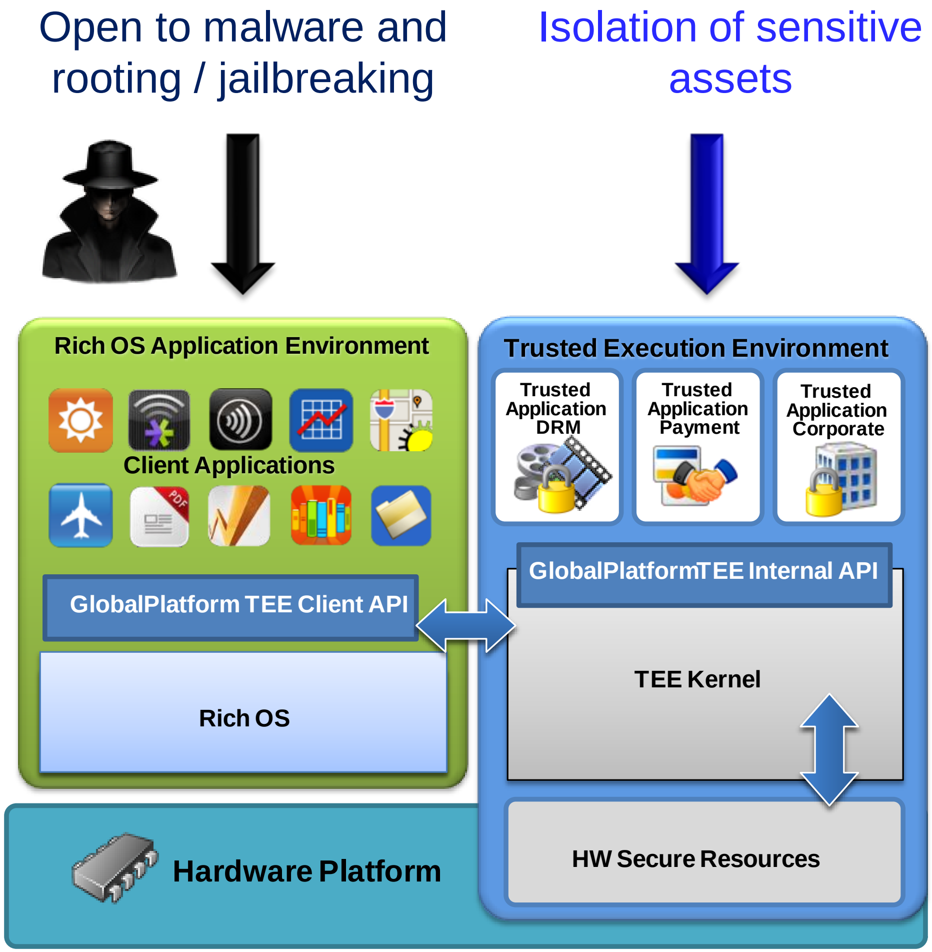
Why this impressive success ?

- Pilots show the attractiveness of a multi application device to the end-user
  - Smartphone: always there, always on,
- GlobalPlatform technology is neutral regarding to the business model used in project (eg multiple form factors, multiple business, …)
- Strong knowledge in GlobalPlatform about “eco systems” since 1999
  - Learned the hard way
  - Each parties (with their differences) are respected
- The same “object” supports different model
  - Investment from different actors in different models are shared
  - → eSE deployment helps UICC deployment and motivate SD deployment

At the end it’s about enabling application & services
Whatever the business environment
Supported by multiple players WW

TEE technology

What is a Trusted Execution Environment (TEE)?


Open to malware and rooting / jailbreaking
Isolation of sensitive assets
Rich OS Application Environment
Client Applications
GlobalPlatform TEE Client API
Rich OS
Trusted Execution Environment
Trusted Application DRM
Trusted Application Payment
Trusted Application Corporate
GlobalPlatformTEE Internal API
TEE Kernel
HW Secure Resources
Hardware Platform

- TEE provides **hardware-based isolation** from rich operating systems (OS) such as Android
- TEE runs on the **main device chipset and relies on hardware roots of trust (crypto keys and secure boot)**
- TEE has **privileged access** to platform and device resources **(user interface, memory controller, video / audio HW, crypto accelerators, biometry, …)**
- Technology already **massively deployed**
- **Premium content protection** is currently a major use case

Unique Feature: Trusted User Interface

Message to be signed

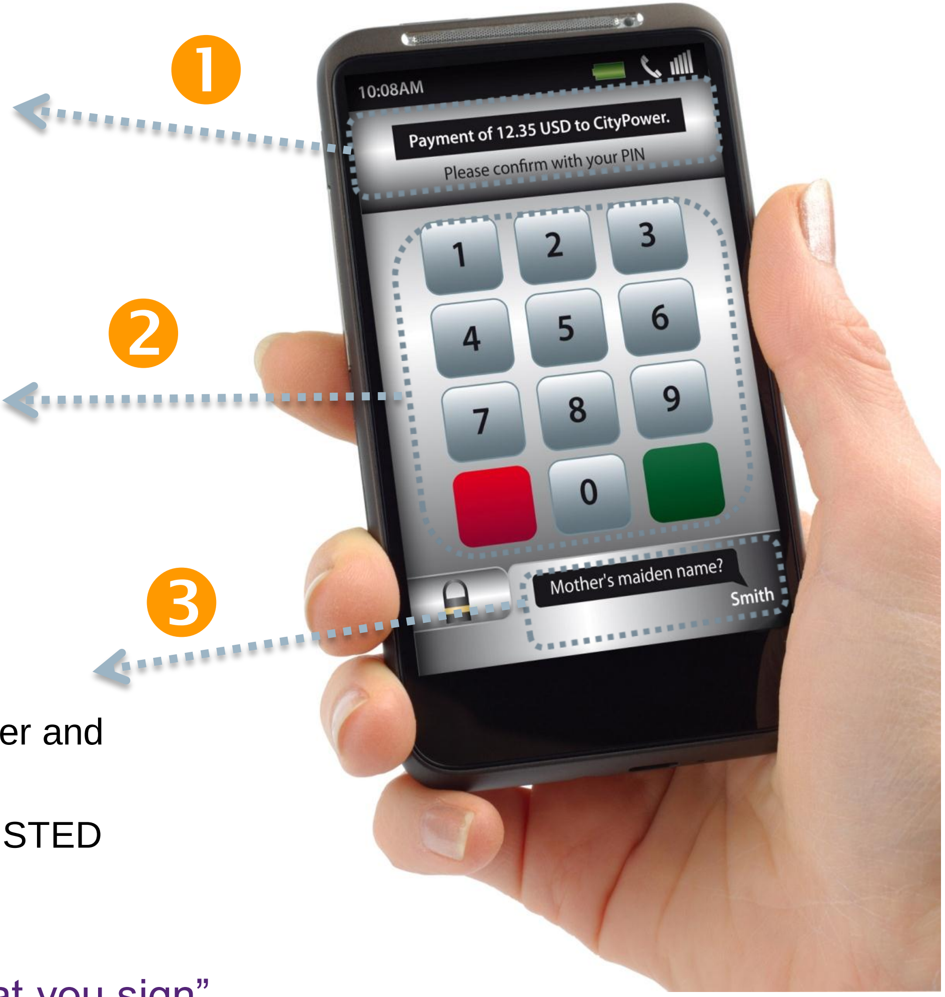
- Transaction summary displayed by TEE
- Rich OS environment cannot tamper with the message
- The user signs exactly what s/he is seeing

Explicit Validation Means

- PIN / password entry → Rich OS environment cannot have access to entered credential

Security Indicator

- Text or image
- “Sign-in Seal concept”
- Information securely configured by the user and securely controlled by TEE
- Proove to the user that the screen is TRUSTED by seeing this known information

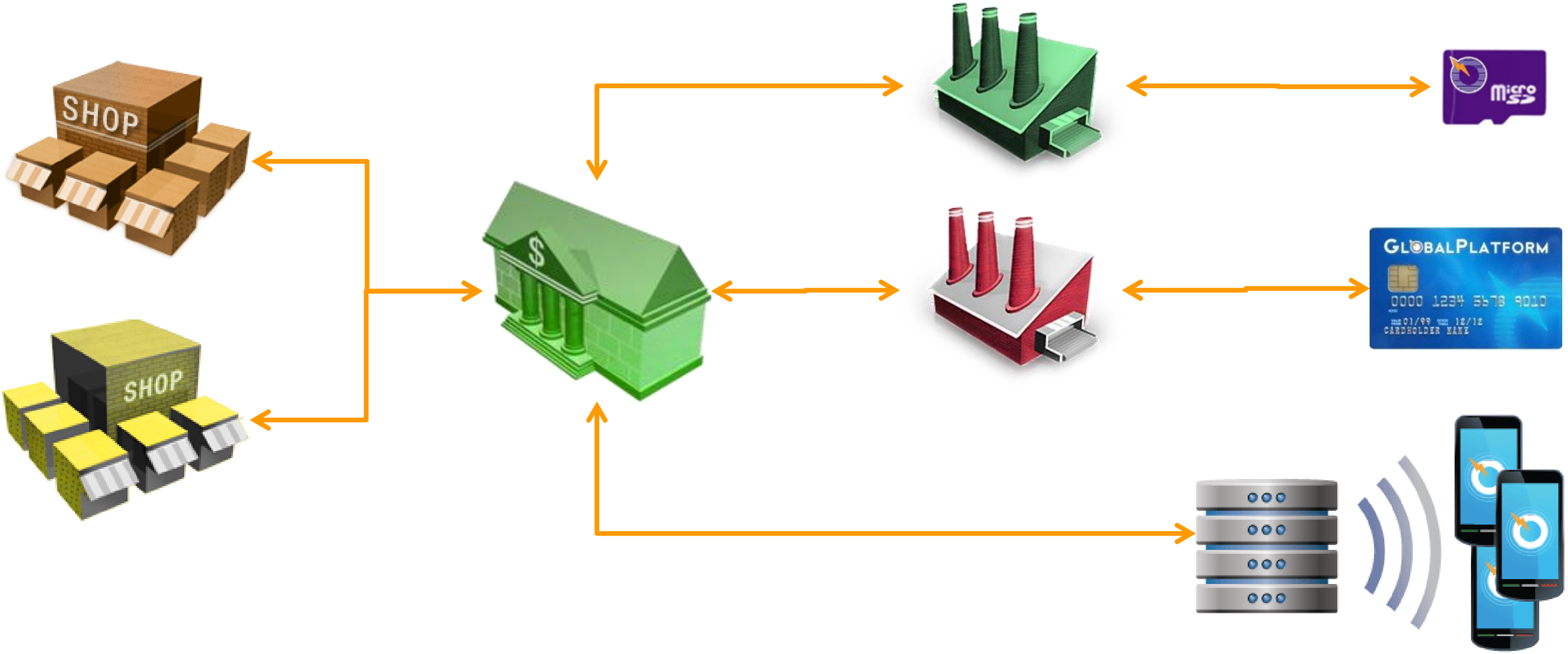

1
2
3
10:08AM
Payment of 12.35 USD to CityPower.
Please confirm with your PIN
1
2
3
4
5
6
7
8
9
0
Mother's maiden name?
Smith

→ Tools to build “what you see is what you sign”, anti-phishing and non repudiation

Messaging technology

Messaging Technology is Answering Business Challenges

- Deployment of value added services requires end-to-end systems connectivity to provide the right information for the right token

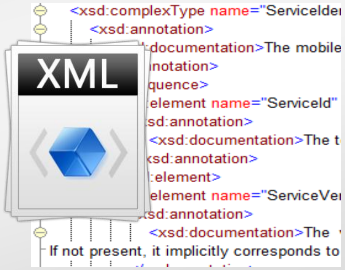


- Diversification, Flexibility
- Evolution, Adaptation to Market Needs
- Centralized to Decentralized

GlobalPlatform Messaging, as a Framework

↳ Language

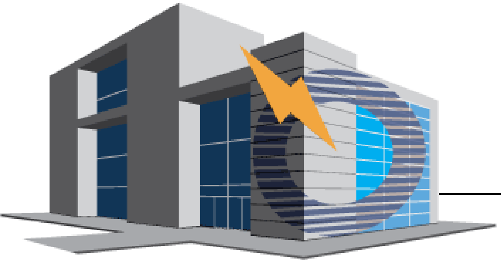
- **Message format**
  - XML-based
  - Programming language agnostic



```
<xsd:complexType name="ServiceIder
  <xsd:annotation>
      :documentation>The mobile
      nnotation>
      quence>
      element name="ServiceId"
      sd:annotation>
        <xsd:documentation>The t
      xsd:annotation>
      :element>
      element name="ServiceVer
      sd:annotation>
        <xsd:documentation>The
If not present, it implicitly corresponds to
```

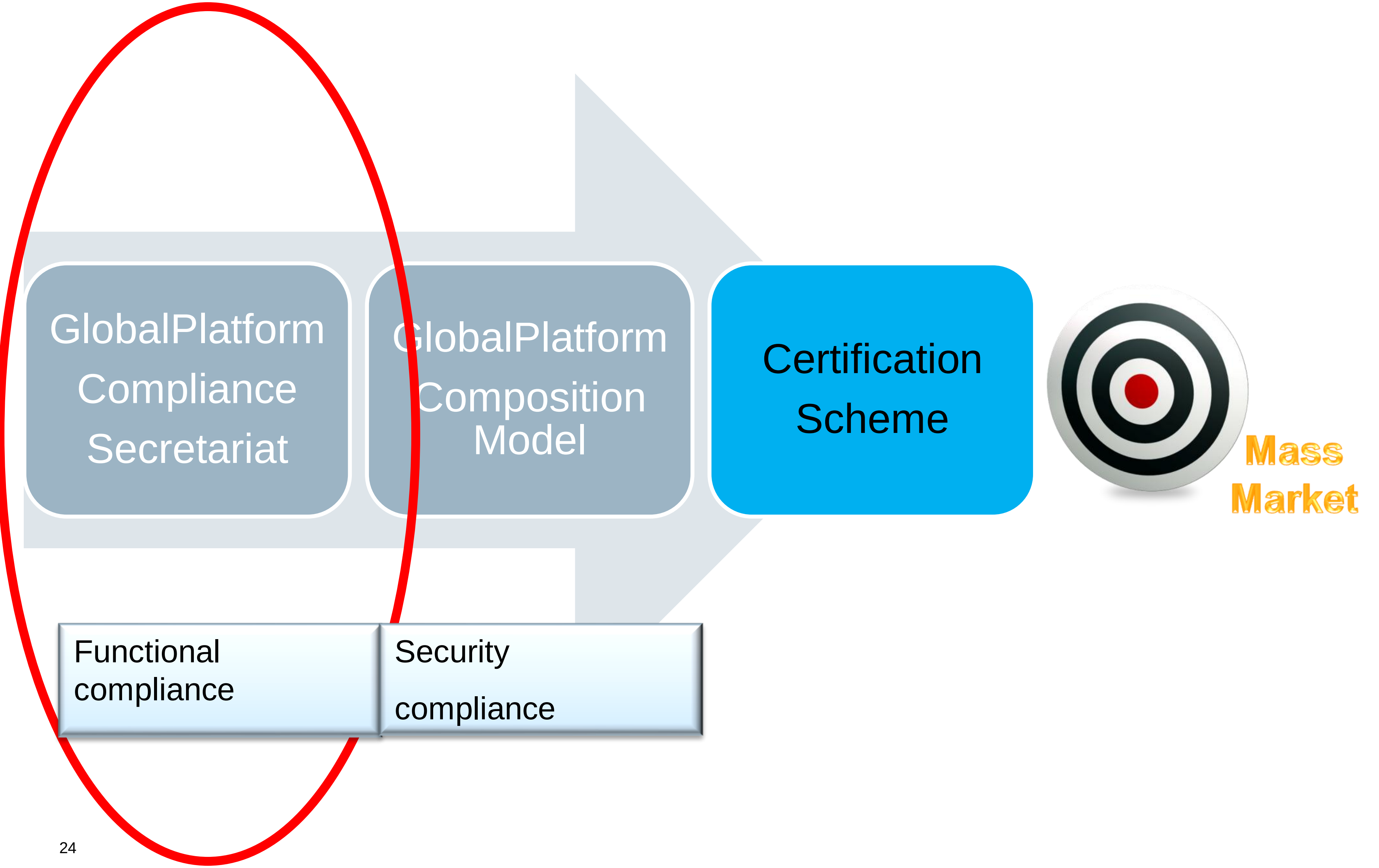
- **SOA architecture**
  - Web Services (WSDL)
  - Portable
  - Interoperable

- **Security**
  - WS-Security standards
  - Authentication, encryption…



Compliance

Positioning the Compliance Secretariat in a Certification Scheme



GlobalPlatform Compliance Secretariat

GlobalPlatform Composition Model

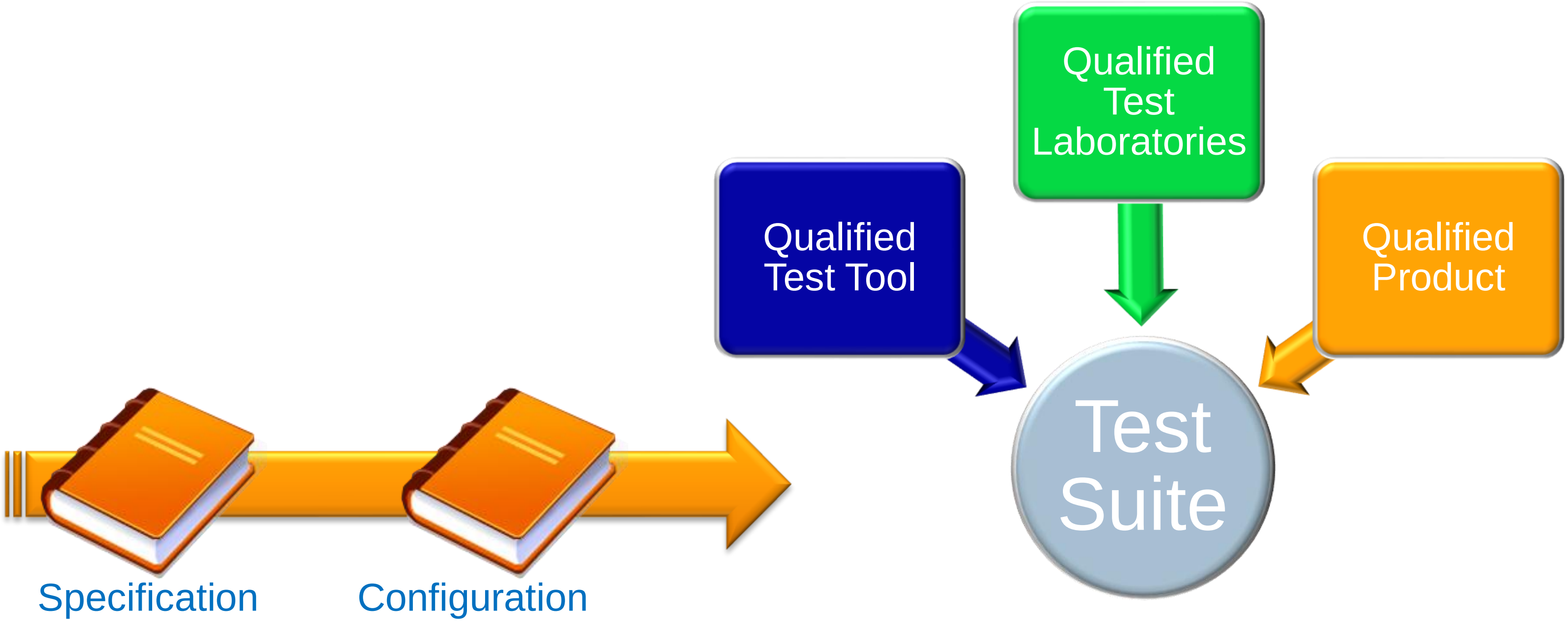
Certification Scheme

Functional compliance

Security compliance

Compliance program

- GlobalPlatform compliance program provides common core interoperable solutions
- An eco-system built around:

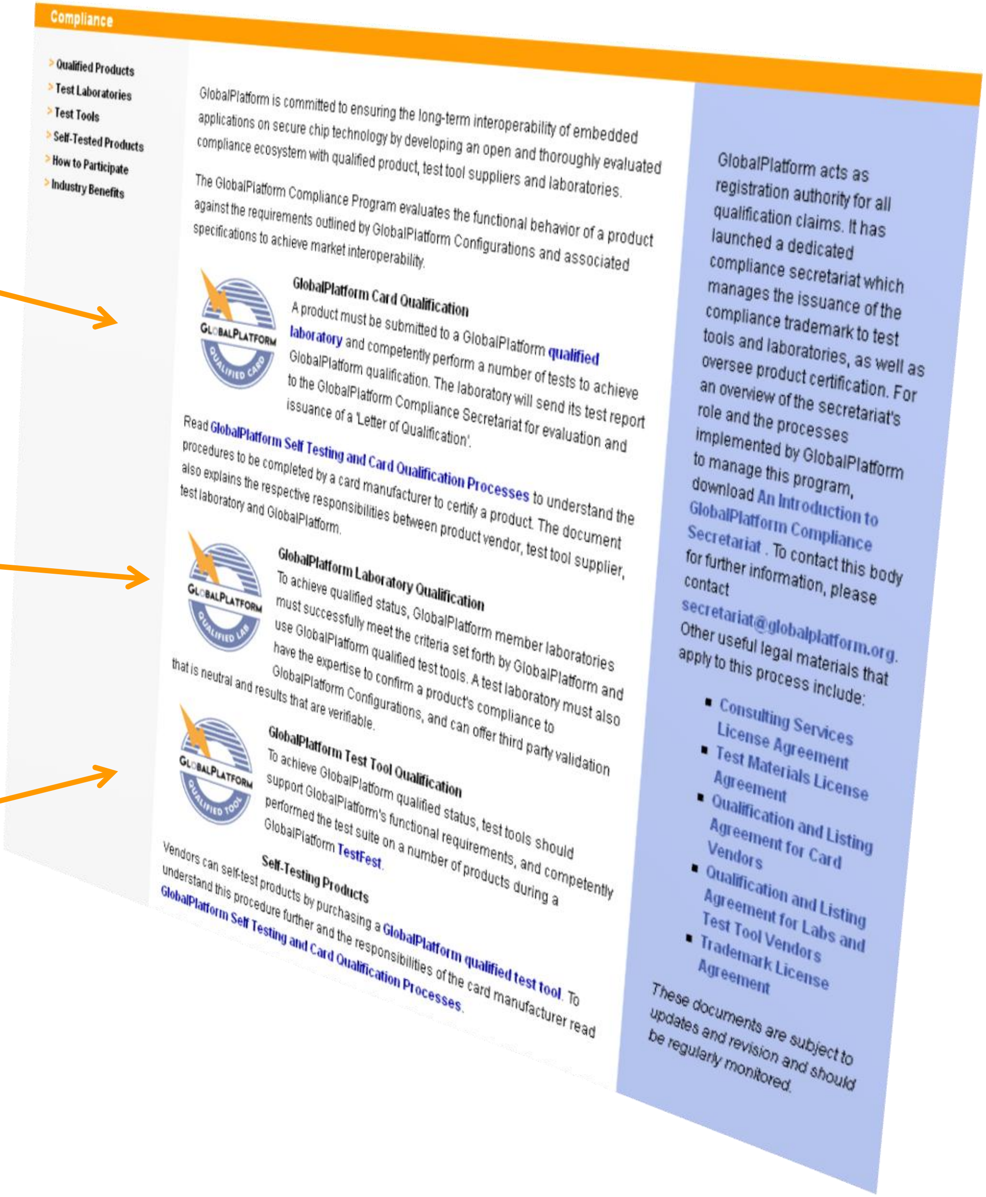


Compliance Results

Test Tools

Test Labs

Qualified Products
Cards, SEs, and TEE



Compliance

- Qualified Products
- Test Laboratories
- Test Tools
- Self-Tested Products
- How to Participate
- Industry Benefits

GlobalPlatform is committed to ensuring the long-term interoperability of embedded applications on secure chip technology by developing an open and thoroughly evaluated compliance ecosystem with qualified product, test tool suppliers and laboratories.

The GlobalPlatform Compliance Program evaluates the functional behavior of a product against the requirements outlined by GlobalPlatform Configurations and associated specifications to achieve market interoperability.

GlobalPlatform Card Qualification

A product must be submitted to a GlobalPlatform qualified laboratory and competently perform a number of tests to achieve GlobalPlatform qualification. The laboratory will send its test report to the GlobalPlatform Compliance Secretariat for evaluation and issuance of a 'Letter of Qualification'.

Read GlobalPlatform Self Testing and Card Qualification Processes to understand the procedures to be completed by a card manufacturer to certify a product. The document also explains the respective responsibilities between product vendor, test tool supplier, test laboratory and GlobalPlatform.

GlobalPlatform Laboratory Qualification

To achieve qualified status, GlobalPlatform member laboratories must successfully meet the criteria set forth by GlobalPlatform and use GlobalPlatform qualified test tools. A test laboratory must also have the expertise to confirm a product's compliance to GlobalPlatform Configurations, and can offer third party validation that is neutral and results that are verifiable.

GlobalPlatform Test Tool Qualification

To achieve GlobalPlatform qualified status, test tools should support GlobalPlatform's functional requirements, and competently performed the test suite on a number of products during a GlobalPlatform TestFest.

Self-Testing Products

Vendors can self-test products by purchasing a GlobalPlatform qualified test tool. To understand this procedure further and the responsibilities of the card manufacturer read GlobalPlatform Self Testing and Card Qualification Processes.

GlobalPlatform acts as registration authority for all qualification claims. It has launched a dedicated compliance secretariat which manages the issuance of the compliance trademark to test tools and laboratories, as well as oversee product certification. For an overview of the secretariat's role and the processes implemented by GlobalPlatform to manage this program, download An Introduction to GlobalPlatform Compliance Secretariat . To contact this body for further information, please contact secretariat@globalplatform.org.

Other useful legal materials that apply to this process include:

- Consulting Services License Agreement
- Test Materials License Agreement
- Qualification and Listing Agreement for Card Vendors
- Qualification and Listing Agreement for Labs and Test Tool Vendors
- Trademark License Agreement

These documents are subject to updates and revision and should be regularly monitored.

Security Compliance: Card certification

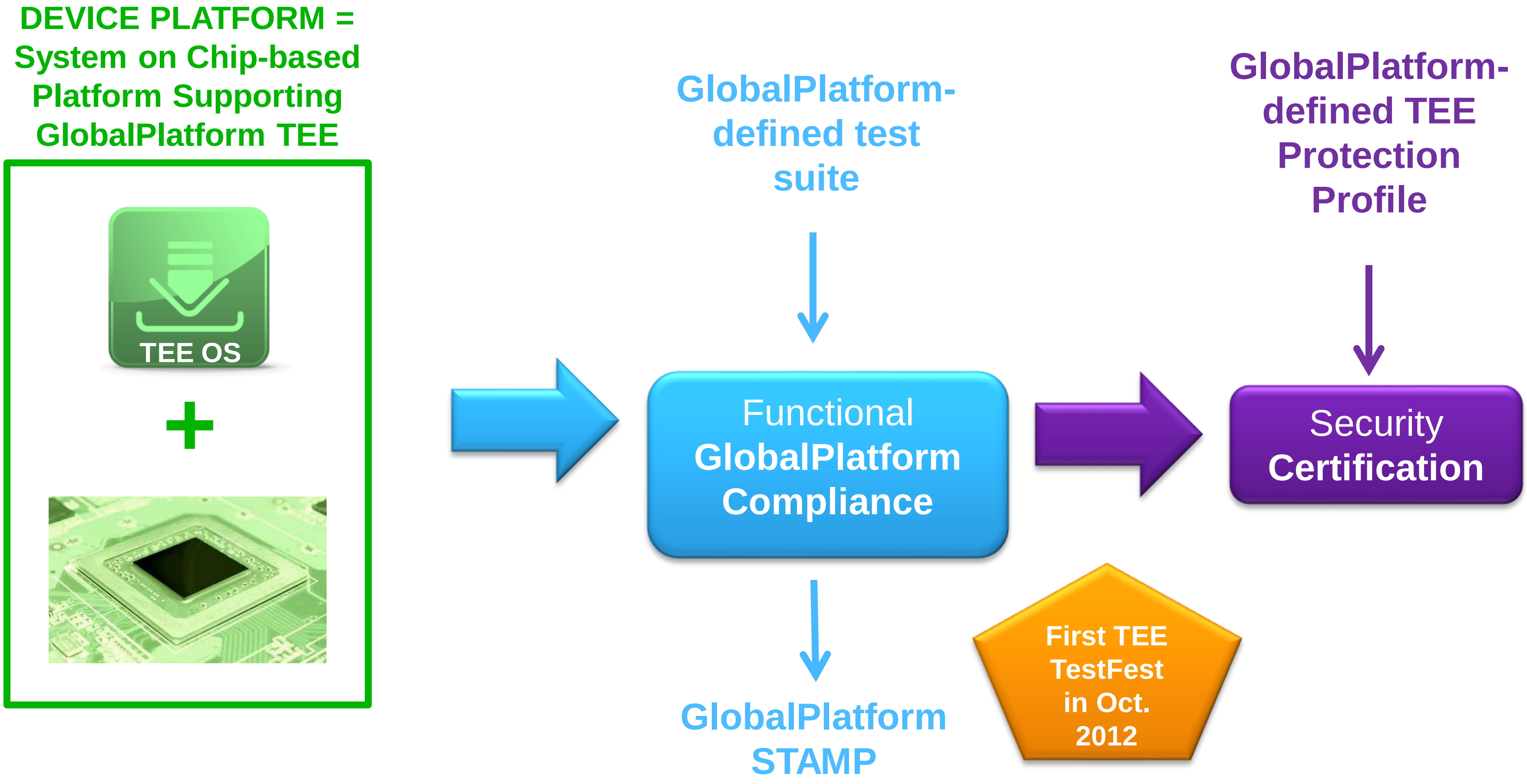
- The industry is continually looking at ways to reduce product time to market while simultaneously advancing the security of a NFC mobile product. As SEs in mobile devices begin to host multiple applications, it is important that all applications perform as intended and do not interfere with the other services being delivered.
- The composition model is a common, cross-industry certification model for SEs with post-issuance capabilities.
  - Today's fully endorsed by EMVCo and Common Criteria

The GlobalPlatform Composition Model specifies how:

1) Existing security evaluation results from EMVCo and Common Criteria can be re-used.

2) Security evaluation work can be limited to only test the impact of a new application and SE combination.

GlobalPlatform TEE Compliance & Security Certification



DEVICE PLATFORM = System on Chip-based Platform Supporting GlobalPlatform TEE

TEE OS

+

GlobalPlatform-defined test suite

Functional GlobalPlatform Compliance

GlobalPlatform STAMP

First TEE TestFest in Oct. 2012

GlobalPlatform-defined TEE Protection Profile

Security Certification

- Current and first-phase focus = DEVICE PLATFORM
- Final product (final smartphone, tablet…): light delta compliance and / or security certification will be defined in a second phase

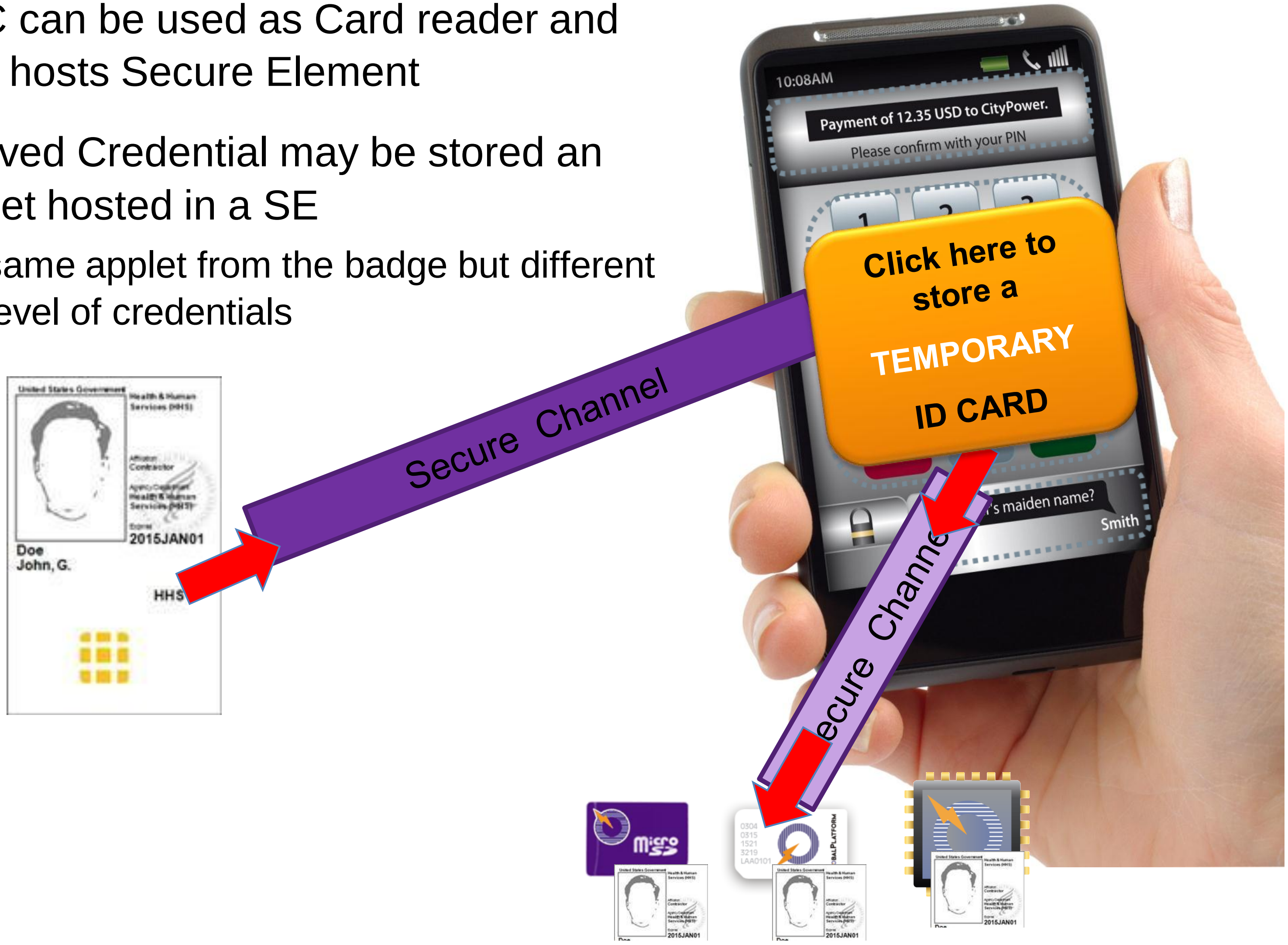
TEE Security Certification Principles

- **Enabling independent entities to validate TEE security level to prove a first level of security of TEE**
- Does not go up to SE / smart card level of security
- Need to prove
  - Isolation of TEE vs rich OS environment
  - Isolation of trusted applications (TAs) between each other
  - TAs are not tampering with the TEE OS
- Main attack vectors
  - Software attacks coming from
    - Rich OS (malware, rooted device, …)
    - Rogue / badly written TAs
  - Few ‘easy’ hardware attacks such as
    - Debug/Jtag interface
    - Firmware replacement
- Not reinventing the wheel
- Use international scheme (e.g. not a country-specific scheme)
- Be lightweight to fulfill time-to-market requirements of mobile industry

GP Technology applied to PIV & Derived Credentials

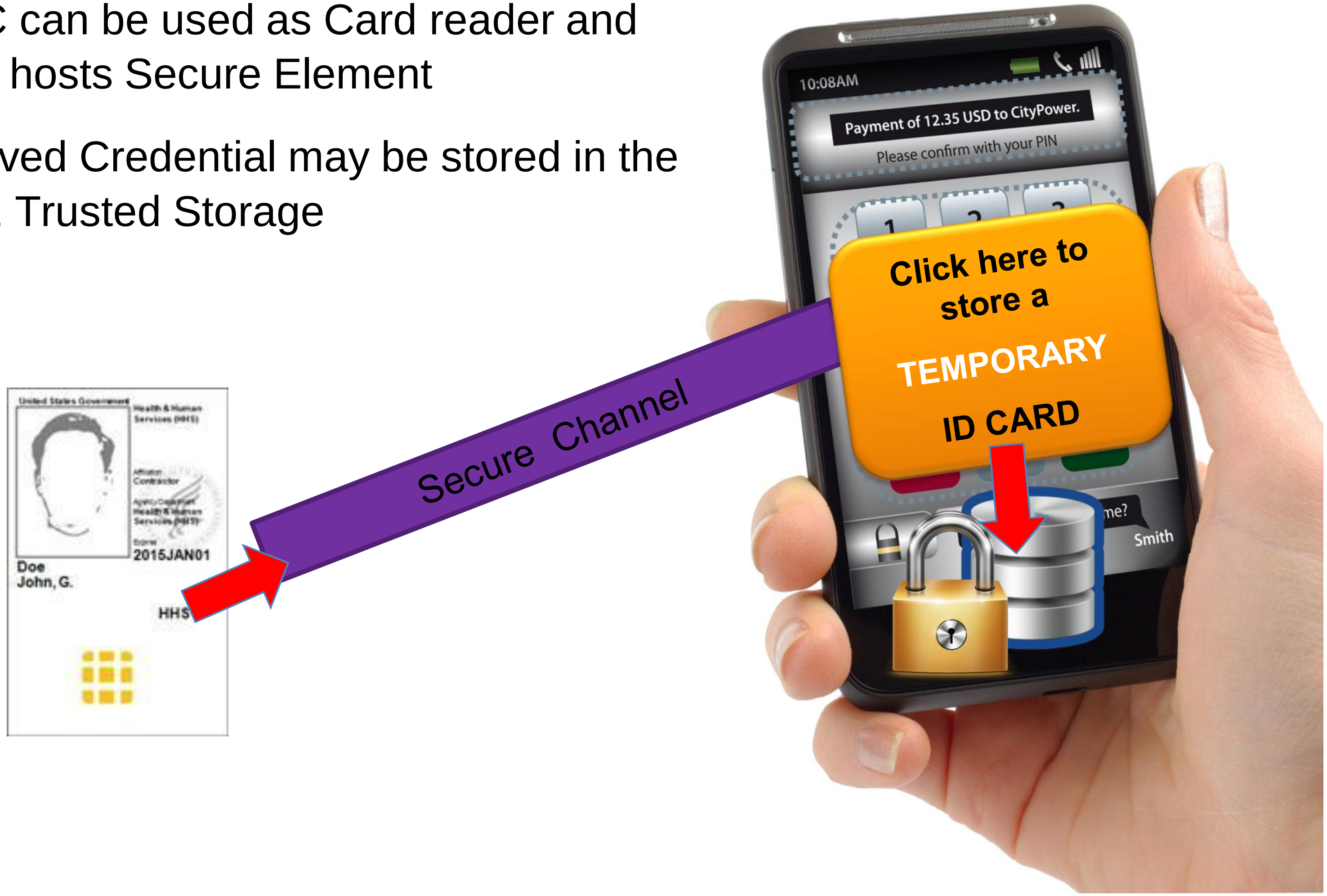
Derived credential

- NFC can be used as Card reader and also hosts Secure Element
- Derived Credential may be stored an applet hosted in a SE
  - same applet from the badge but different level of credentials



Derived credential

- NFC can be used as Card reader and also hosts Secure Element
- Derived Credential may be stored in the TEE Trusted Storage



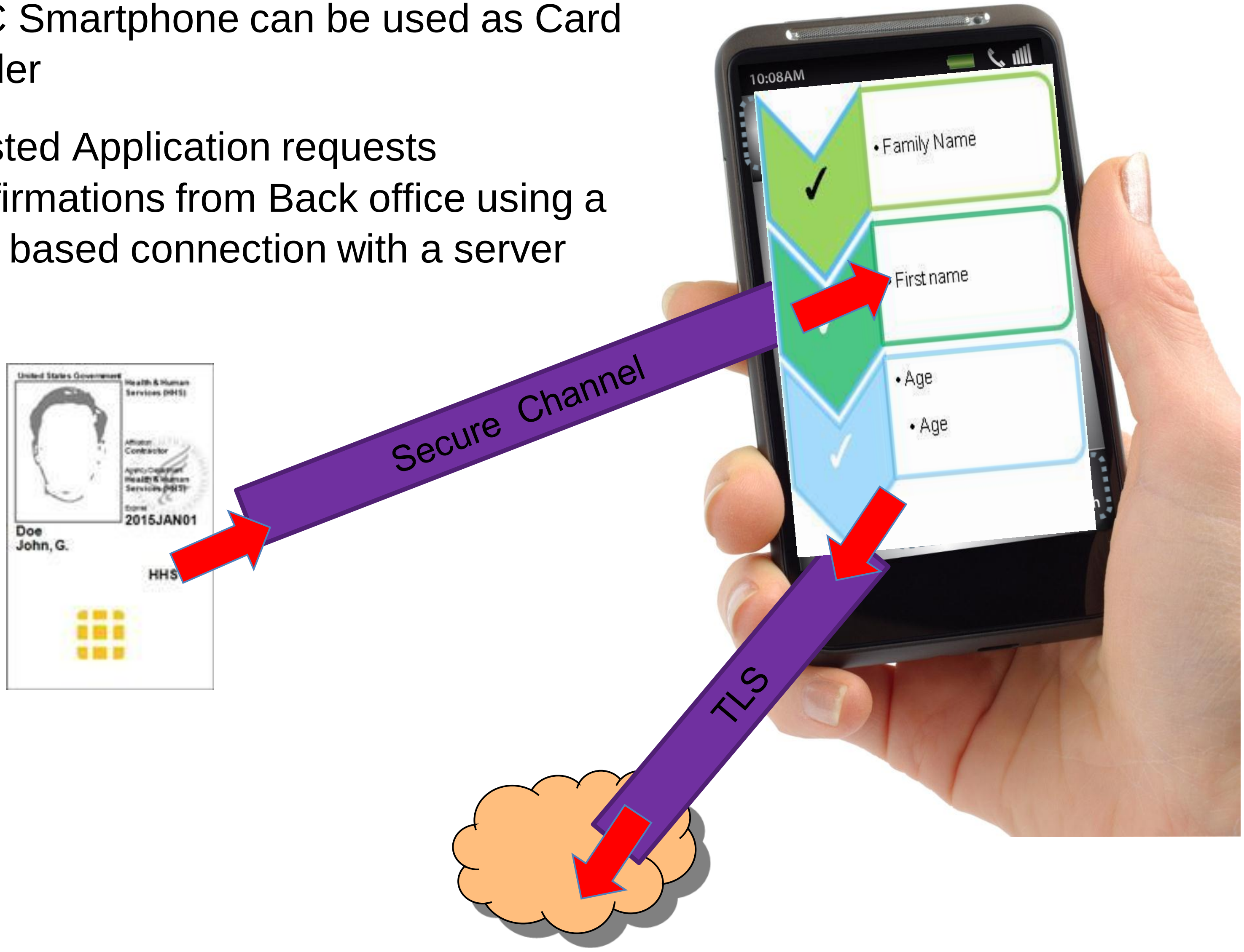
SmartPhone as a reader (1/2)

- NFC Smartphone can be used as Card reader
- Trusted Application opens a secure channel to retrieved data if authorized

10:08AM
Payment of 12.35 USD to CityPower.
United States Government
Health & Human Services (HHS)
Contractor
Health & Human Services (HHS)
2015JAN01
Doe
John, G.
HHS
Smith

SmartPhone as a reader (2/2)

- NFC Smartphone can be used as Card reader
- Trusted Application requests confirmations from Back office using a TLS based connection with a server



Authentication on Mobile Devices
The NFC Option

United States Government

Affiliation
Uniformed Service
Agency/Department
Department of
Homeland Security
Issued
2010SEP24
Issued
2015SEP24

Hall
Lawrence, K

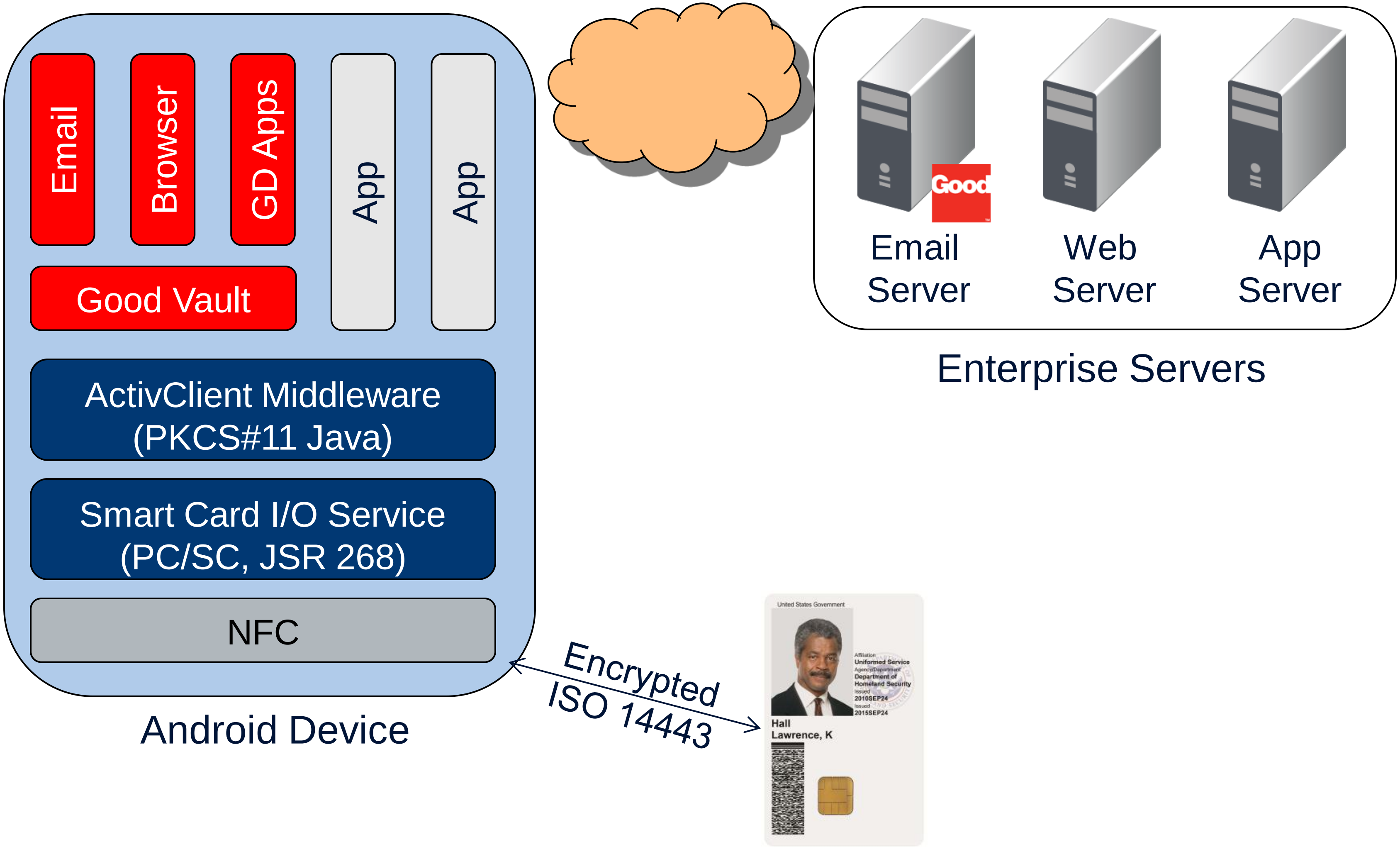
- Just place the card on the back of the phone!
- Leverage the user’s dual-interface card
- No reader required, with differences based on mobile device
- No new derived credential to procure and manage
- Works with majority of devices
  - Nine out of the top 10 smartphone manufacturers have released NFC-enabled handsets.
- Good user experience for infrequent operations (e.g. authentication)
  - A bit clumsy for recurring operations (e.g. signature / decryption)

The Mobile-enabled CAC Next Generation

- Enable CAC user credentials for contactless mode
- Provide CAC middleware for mobile OS
- Secure the contactless communication
  - ANSI 504 OPACITY protocol (FIPS 140-2 approved)
  - Updates to Card applet + Middleware
- Provide middleware-enabled mobile apps
  - GOOD TECHNOLOGY: encrypted GOOD DYNAMICS containerization, S/MIME secure email, secure browser, secure apps

Designing the solution

Architecture



Email

Browser

GD Apps

App

App

Good Vault

ActivClient Middleware
(PKCS#11 Java)

Smart Card I/O Service
(PC/SC, JSR 268)

NFC

Android Device

Encrypted
ISO 14443

Email
Server

Web
Server

App
Server

Enterprise Servers

Project Milestones
The Mobile-enabled CAC Next Generation

- Q4 2012: Prototype
  - Enabling contactless access on CAC applets
  - CAC Middleware for Android, alpha version
  - Prototype Email app (DMDC developed)
  - Lesson learned: dependencies on card / device models and configuration ✓

- Summer 2013: Proof of Concept
  - Enabling secure contactless access on CAC applets with OPACITY
  - CAC Middleware for Android with OPACITY
  - Professional App: Good for Enterprise, Good Vault
  - Non production credentials; 20 to 30 users

- 2014: Pilot
  - Targeting FIPS 201-2 Compliance
  - Production credentials

TakeAway Messages

- Reduce time to market for new services in new form factor for US Government employees → improved productivity, reduce cost

- Global Platform Government Task Force taking into account US Government requirement in order to address the needs for the future

– Composition Model to integrate FIPS 201-2 requirement ?

– Protection profile alignment with NIST

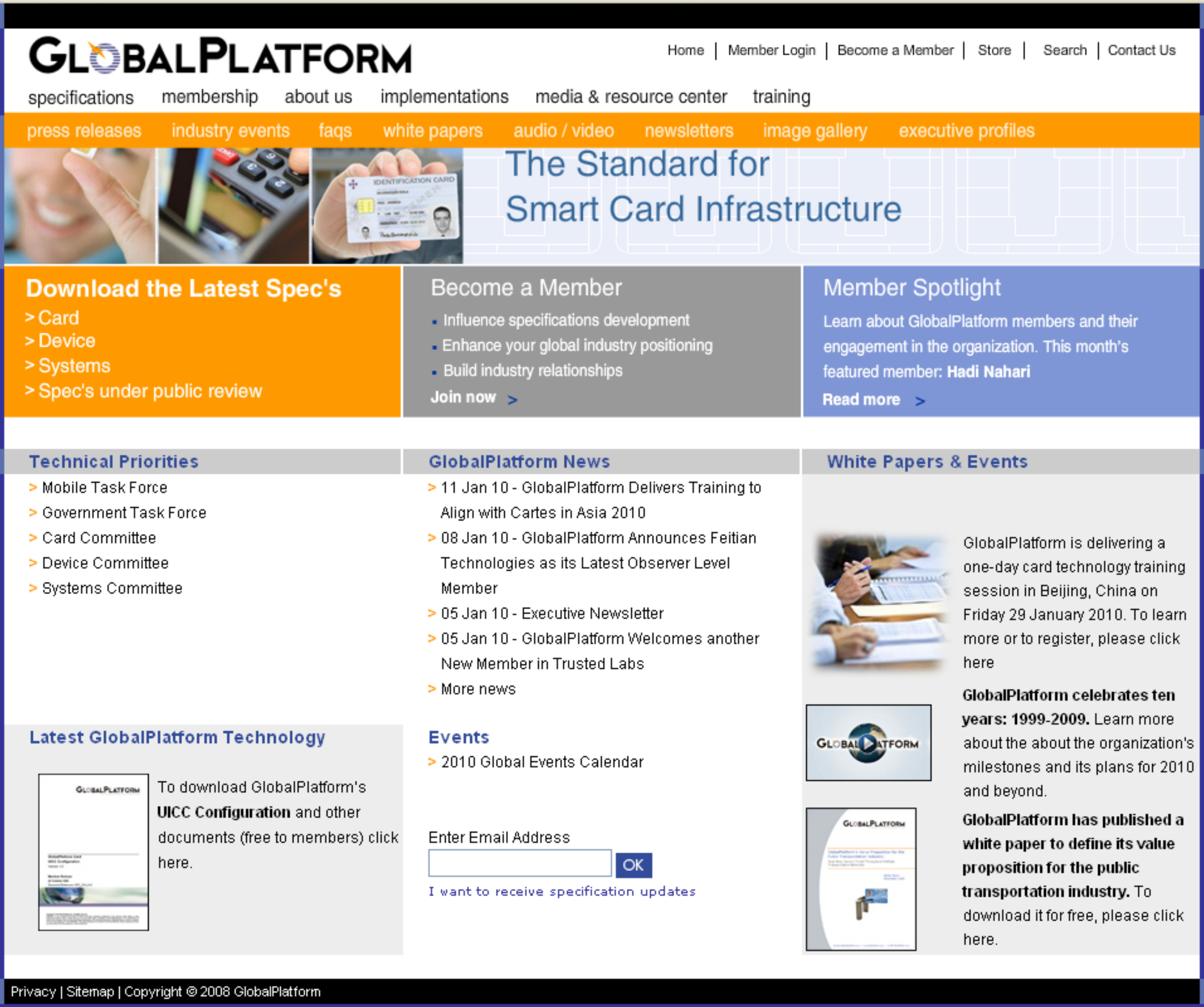
– Secure Element Configuration ?

– Extend UICC configuration to cover needs from US Government

- Next open session on October 16th at the SmartCard Alliance event, open to GP members and US federal employees

Interested ? Contact me at jbecquart@ActivIdentity.com

Visit us @ www.globalplatform.org



GLOBALPLATFORM

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