RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Integrating any Smartphone into your Mobile ID Strategy

SESSION ID: STU-W04A

Kevin Gillick

Executive Director
GlobalPlatform

Setting Context

Setting Context: Increasing Trust

- Devices include open environments with many applications being downloaded
- More and more services are accessible with more and more value
- At the same time, users and services providers are looking for trust and convenience
- Mobile is now becoming the first entry point to digital life (more mobile than PCs)
- Hacking activity is also now focusing more and more on mobile and other devices
- Security technology must answer to increasing needs and hopefully be ahead of malicious activities
- Continuous investment and innovation is also key in security
- Ensuring a ‘trust path’ for service delivery is a critical component for any Mobile ID strategy

Setting Context: Threats are Real

In one year, Android malware up 580%, 23 of the top 500 apps on Google Play deemed 'high risk'

How to hack a cell phone into a spy device (YouTube)

How to hack a cell phone to have free internet

How to hack a cell phone to have free phone calls?
Control a cell phone remotely and make 'free' calls with the Bluetooth Hack (You Tube)

Data hacking – somebody viewing or stealing information stored on your phone e.g. phone numbers, bank account details and emails.

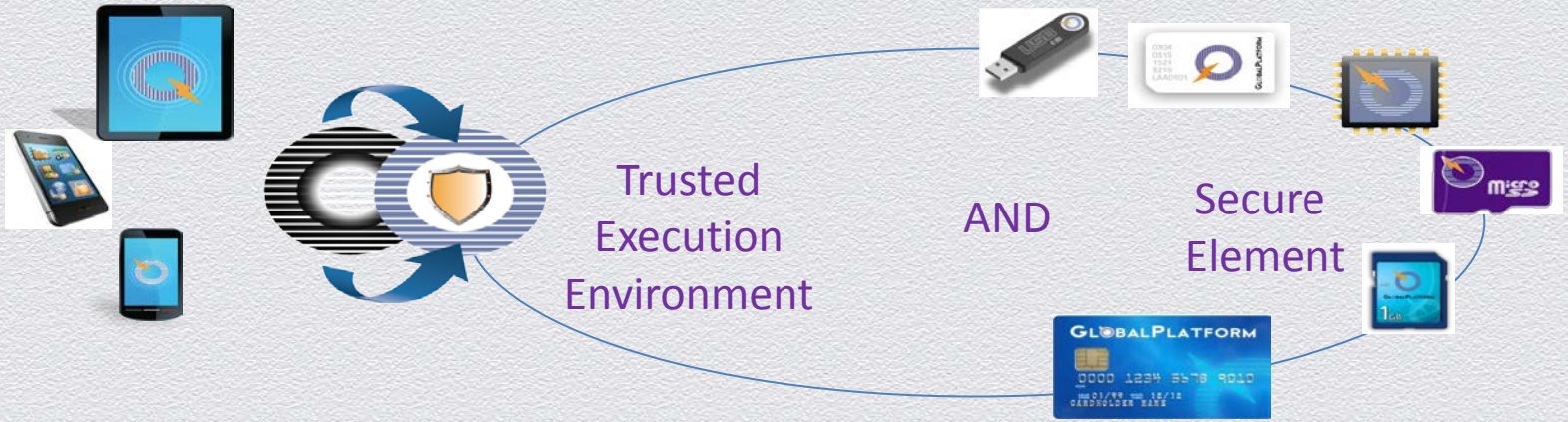
Context Setting: Device Technologies

	Rich OS Environment	Trusted Execution Environment (TEE)	Secure Element (SE) (when present)
Functionality	★★★	★★	★
Performance	★★★	★★	★
Memory Size Access	★★★	★★	★
Peripherals Access (display, touchscreen, video decoder/renderer, …)	★★★	★★	N/A
Attack Resistance	★	★★ (designed for SW-based attacks resistance)	★★★ (tamper-resistant)

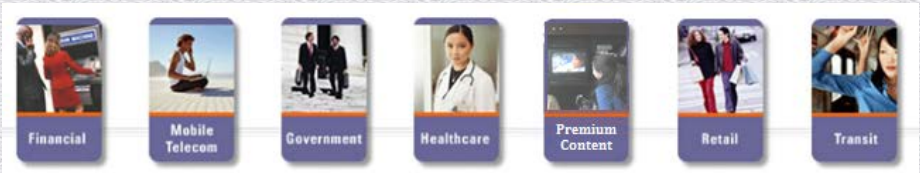
GlobalPlatform Positioning

GlobalPlatform Positioning

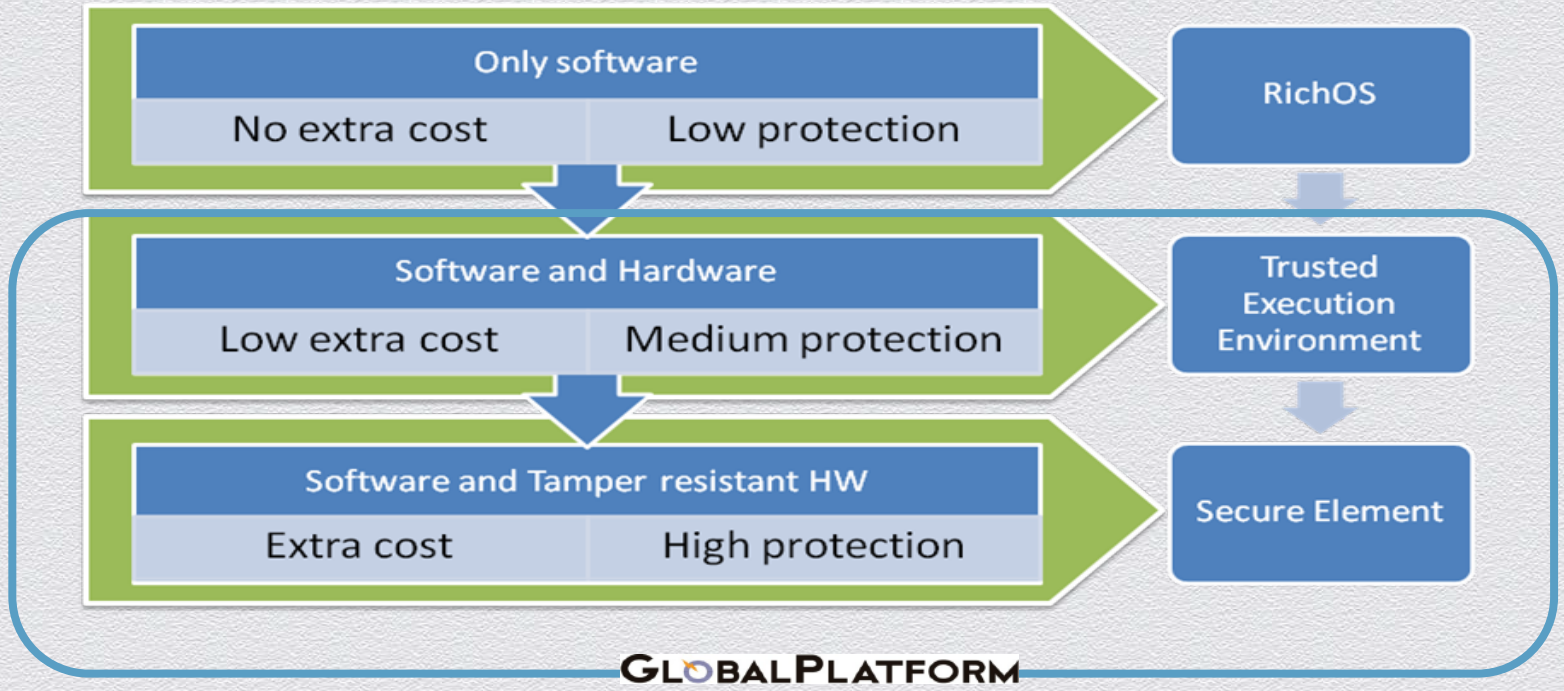
GlobalPlatform is *the* standard for managing applications on secure chip technology



Across several market sectors and in converging sectors



Three Mobile Environments



Standardizing the Secure Element

Definition – Secure Element (SE)

- An SE is a tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities.
- There are three different form factors of SE: Universal Integrated Circuit Card (UICC), embedded SE and smart microSD. Both the UICC and smart microSD are removable. Each form factor links to a different business implementation and satisfies a different market need.

UICC

Embedded SE

Smart microSD

SE

- GlobalPlatform is form factor agnostic
- Configurations today support:
  - UICC
  - Embedded SE
  - Smart microSD
- Endorsed by

Qualified Product Available Today

gemalto security to be free

Giesecke & Devrient

kona i

OBERTHUR TECHNOLOGIES

SK C&C

SOLACIA

UBIVELOX

GLOBALPLATFORM™
THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

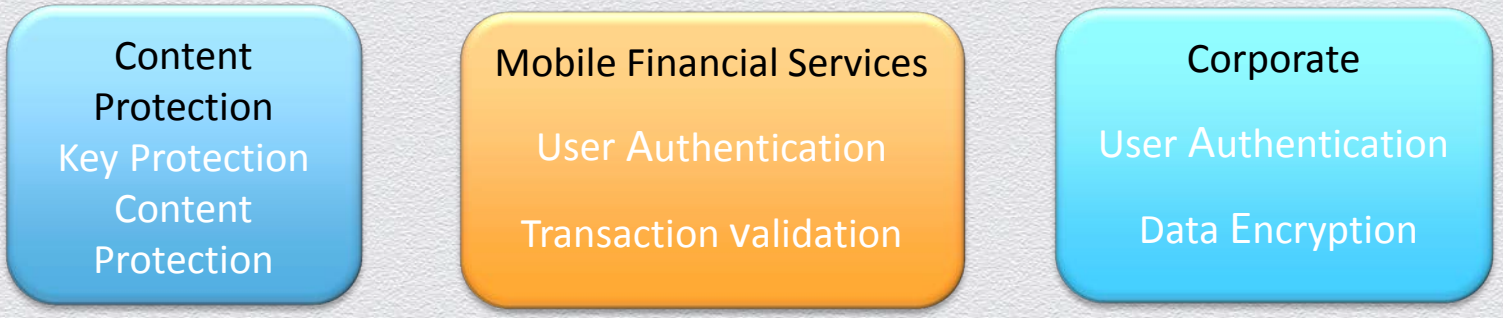
#RSAC

RSACONFERENCE2014

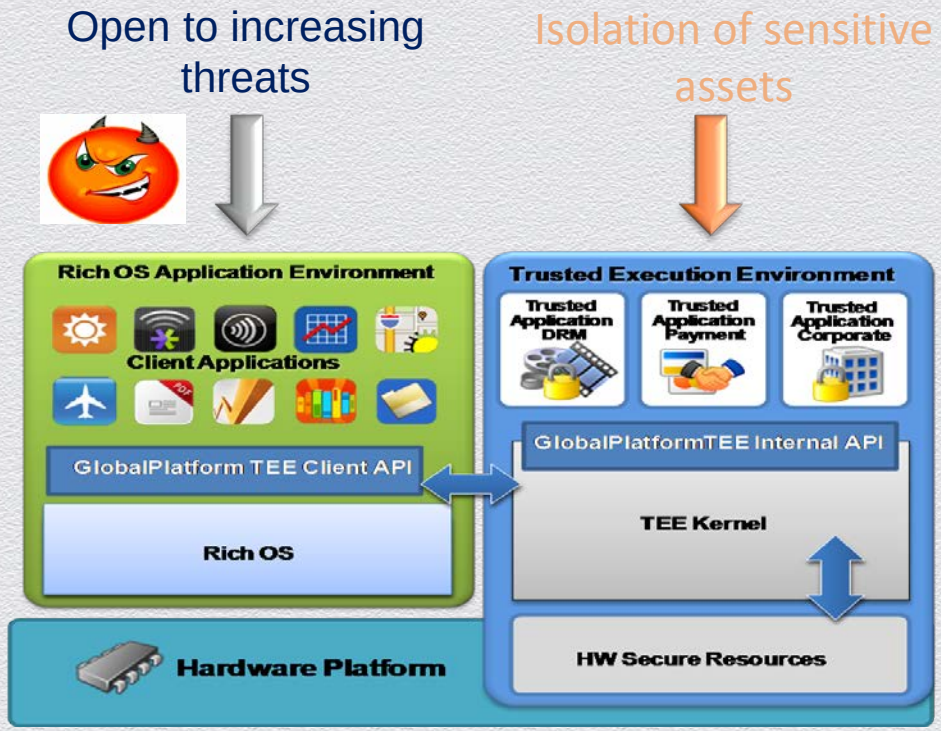
Standardizing the Trusted Execution Environment

Definition – Trusted Execution Environment (TEE)

- The TEE is a secure area that resides in the main processor of the mobile handset and guarantees that data is stored, processed and protected in a trusted environment. It assists in the control of access rights and houses sensitive applications, which need to be isolated from the rich operating system (OS).



The TEE



- TEE provides **hardware-based isolation** from rich OS such as Android
- TEE runs on the **main device chipset**
- TEE has **privileged access** to platform and device resources **(user interface, display controller, memory controller, hardware decoder/renderer, crypto accelerators, SEs…)**
- **Technology already massively deployed**

TEE: The Security Tool Box for Services

GLOBALPLATFORM
THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

Hardware-based TEE Functions

- Code and data isolation
- Secure cryptography
- Secure storage
- Secure clock
- Trusted user interface
- Secure Element interface
- *Administration scheme*
- *Network interface*
- *Biometry*

Value for Secure App Providers includes

- Device authentication
- User authentication
- Protection of any sensitive SW engine
- Digital signature and encryption
- Secure mass storage
- Secure communication to server and/or SE
- Secure functionality to be managed over-the-air

C-Language based environment

Growing TEE Momentum

More and more TEE followers within GlobalPlatform

SoC and hardware IP vendors

AMD, ARM, Broadcom, Discretix, Inside Secure, Marvell, NXP, NVIDIA, Qualcomm, Renesas, Samsung, ST Ericsson, ST, Texas Instruments

Service providers

American Express, Discretix, Elliptic, Good, Inside Secure, MasterCard Worldwide, Proxama, VISA, wave

TEE OS vendors

Oracle, Solacia, Trustonic

Device vendors

LG, BlackBerry, Samsung

Mobile network operators

at&t, orange, Sprint, verizon wireless

Test and security labs

FIME, Galitt, Trusted Labs

Trusted service managers

gemalto, Giesecke & Devrient, Oberthur Technologies

GlobalPlatform™
The Standard for Managing Applications on Secure Chip Technology

#RSAC
RSAConference2014

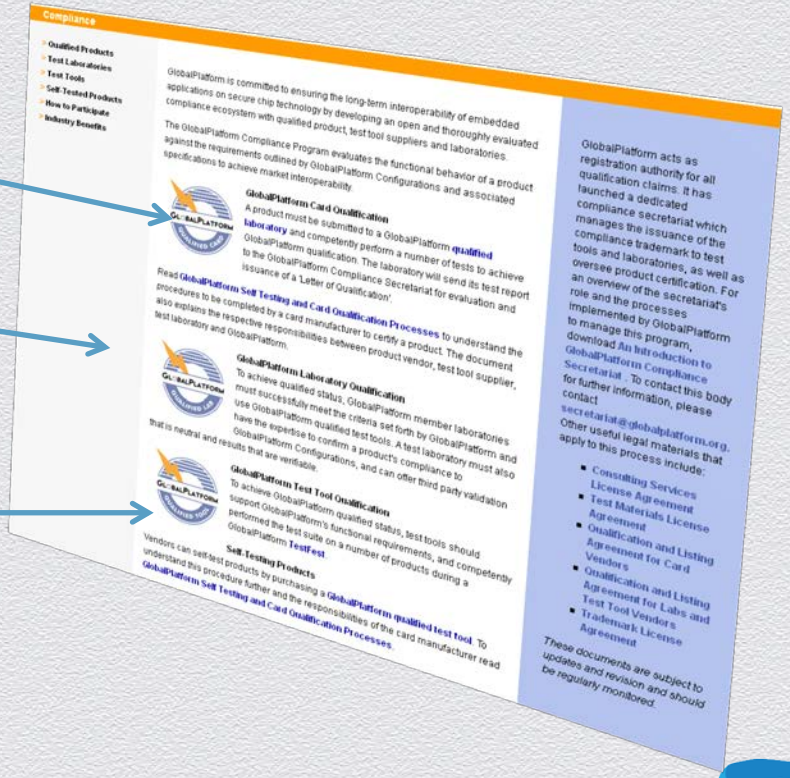
Complying with the Standards

GlobalPlatform Compliance Program

36 Test Tools from
5 Member Companies

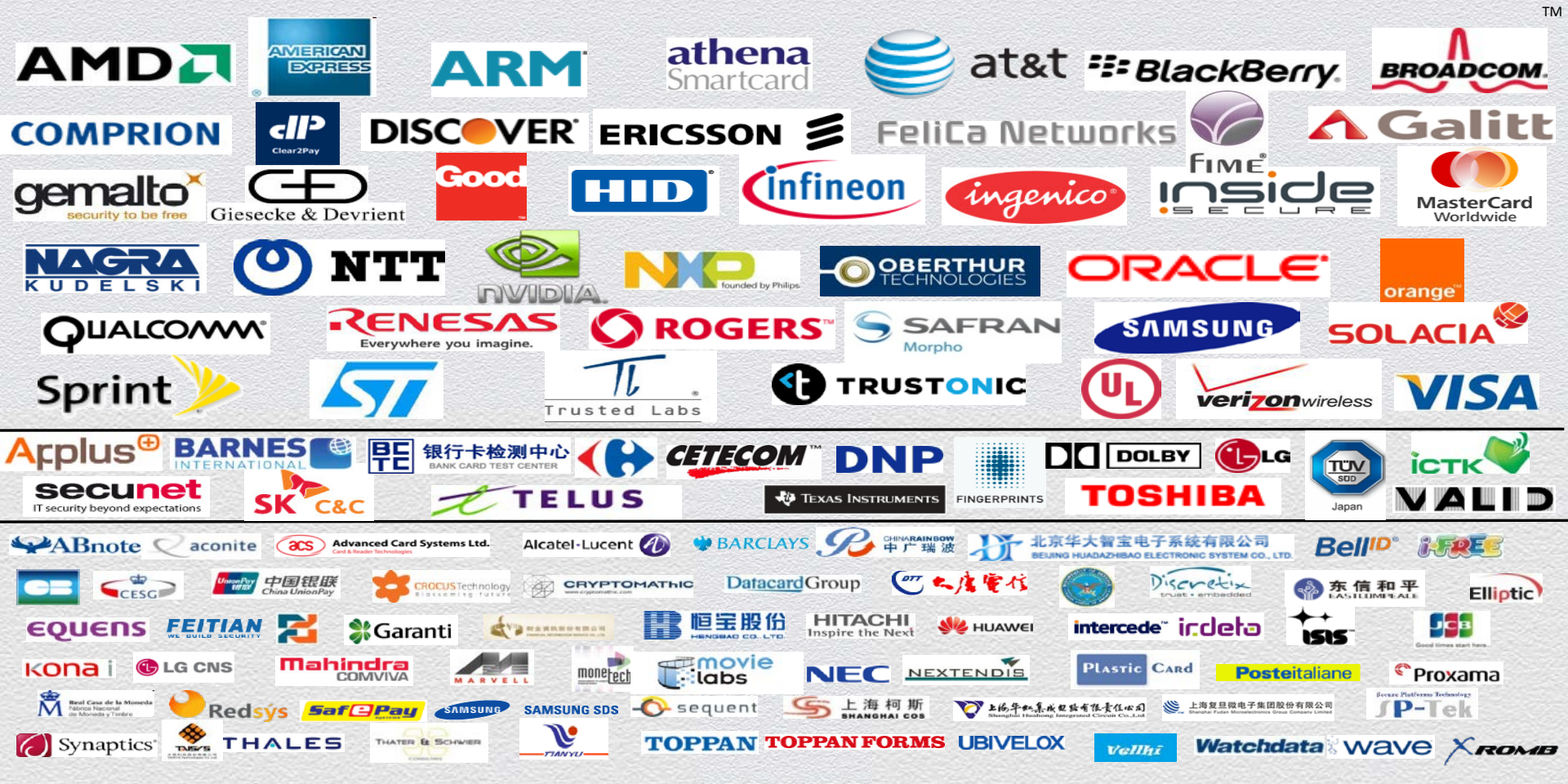
7 Qualified Test Labs
Operated by
5 Member Companies

64 Qualified Products
Card and TEE from
13 Different Companies

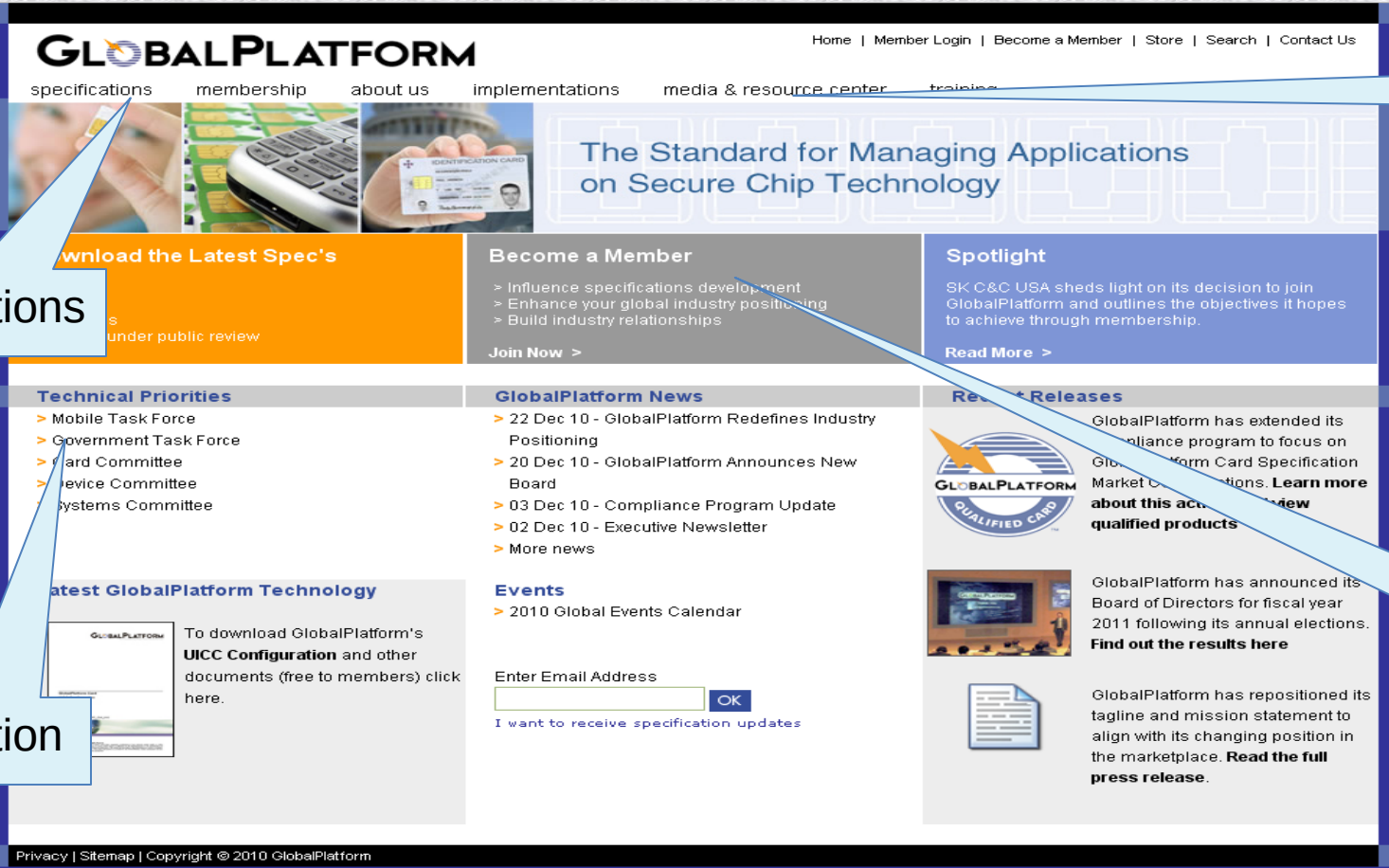


Resources

GlobalPlatform Members



Visit us @ www.globalplatform.org



Specifications

White Papers

Organization

Become a Member

Thank you!