GLOBALPLATFORM®



GlobalPlatform – Mobile ID and Derived Credentials

Alexander Summerer
G&D
Chair, GlobalPlatform SE Access Control WG

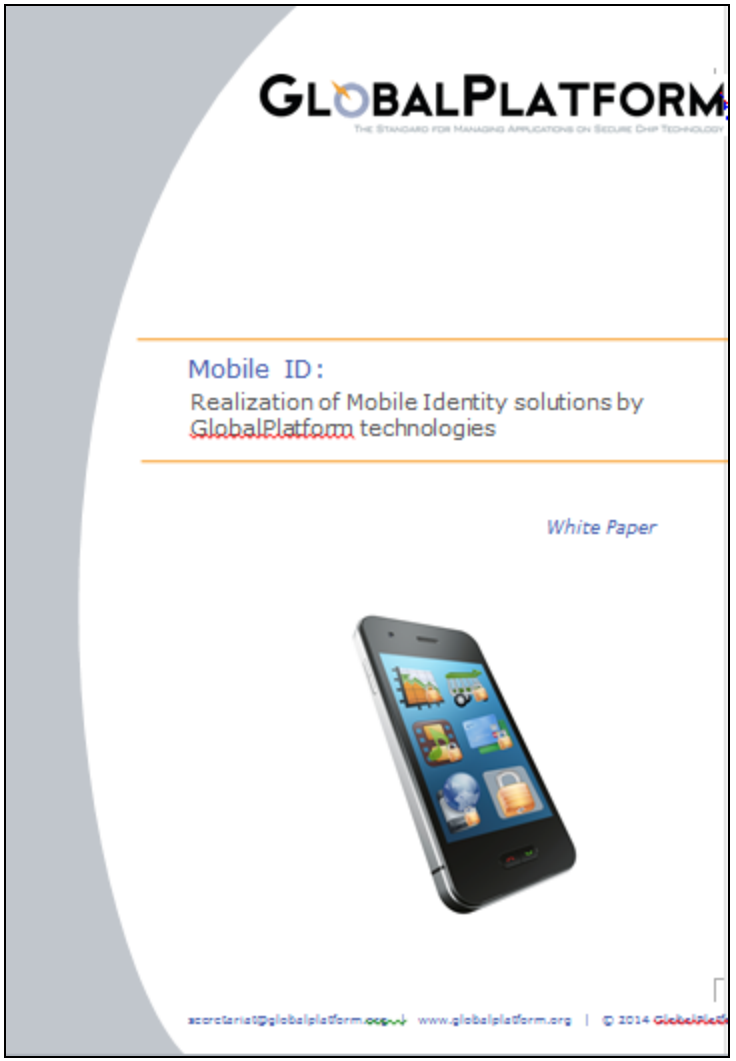
THE THIRD
International Cryptographic Module Conference ICMC15

November 4-6 ▪ Hilton Washington, D.C. ▪ Rockville, Maryland

@GlobalPlatform_ www.linkedin.com/company/globalplatform YouTube GlobalPlatformTV

GlobalPlatform Mobile ID Whitepaper

- ✓ Vision and market potentials
- ✓ Key use cases
- ✓ Technical approaches
- ✓ GlobalPlatform technologies
- ✓ Implementation scenarios

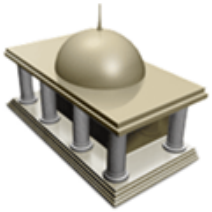


Publication expected in mid-November 2015

Vision and Market Potentials

GLOBALPLATFORM®

- **Government-2-Government:**
  - e.g. access to agency resources as agency employee or agency contractor



- **Government-2-Citizen:**
  - e.g. authentication to eGovernment Online Services as citizen, digital voting, social benefit

- **Enterprise:**
  - e.g. access to enterprise resources as employee

- **eHealth:**
  - e.g. authentication to healthcare services as patient, physician, hospital employees
- **Financial:**
  - e.g. signatures of payment transactions as bank customer

- **Commercial:**
  - e.g. age verification in online shops
  - e.g. driver's license checks for car rental
  - e.g. ID verification for airline and hotel check-in

Mobile ID for Different Kinds of ID Cards

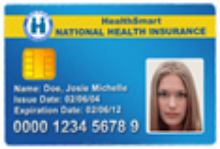
GLOBALPLATFORM®

Bank card

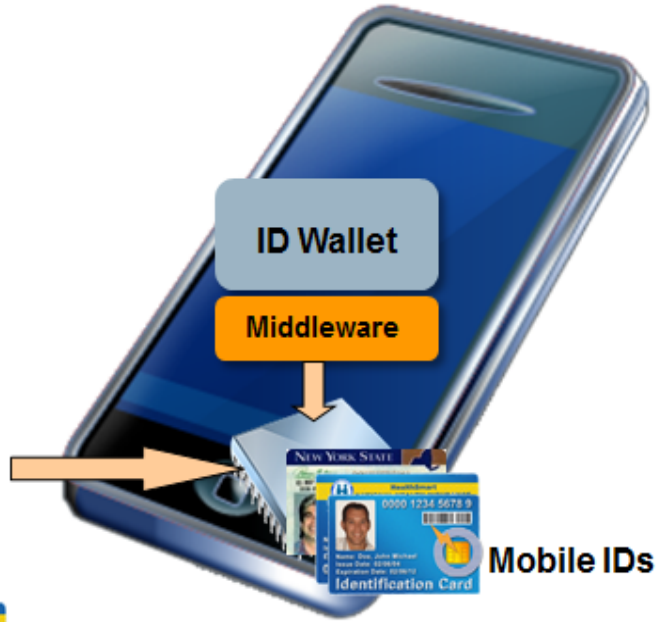
Driver's License card

National ID card

Health card



Company card



Mobile IDs

Generated Mobile ID Credentials

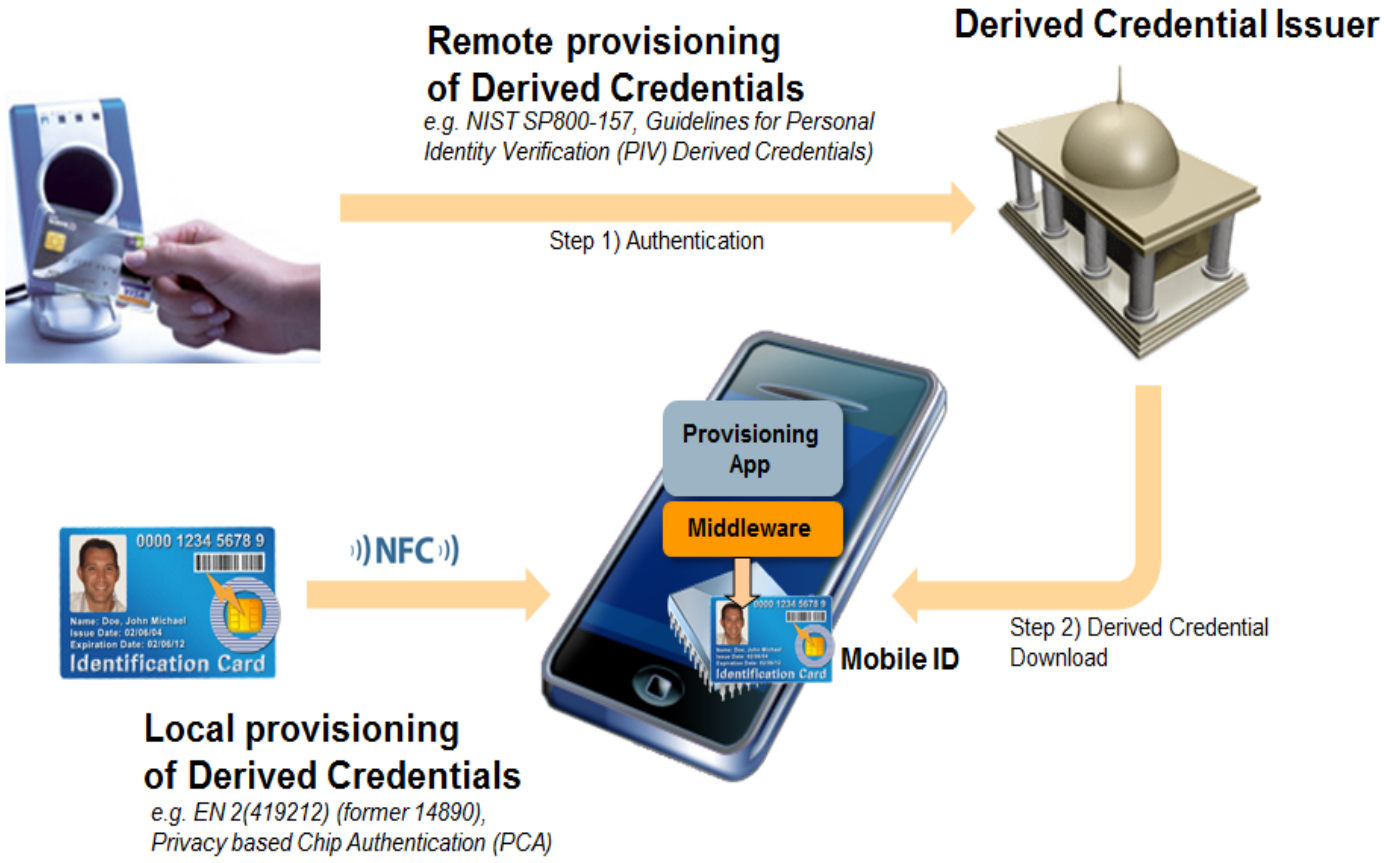
GLOBALPLATFORM®

- Mobile ID credentials generated:
  Option 1: by the issuer and downloaded to the Mobile Device
  Option 2: on the Mobile Device and signed by the issuer

Derived Mobile ID Credentials

GLOBALPLATFORM®

- Mobile ID is derived:
  Option 1: by the issuer and downloaded to the Mobile Device
  Option 2: by the Mobile Device



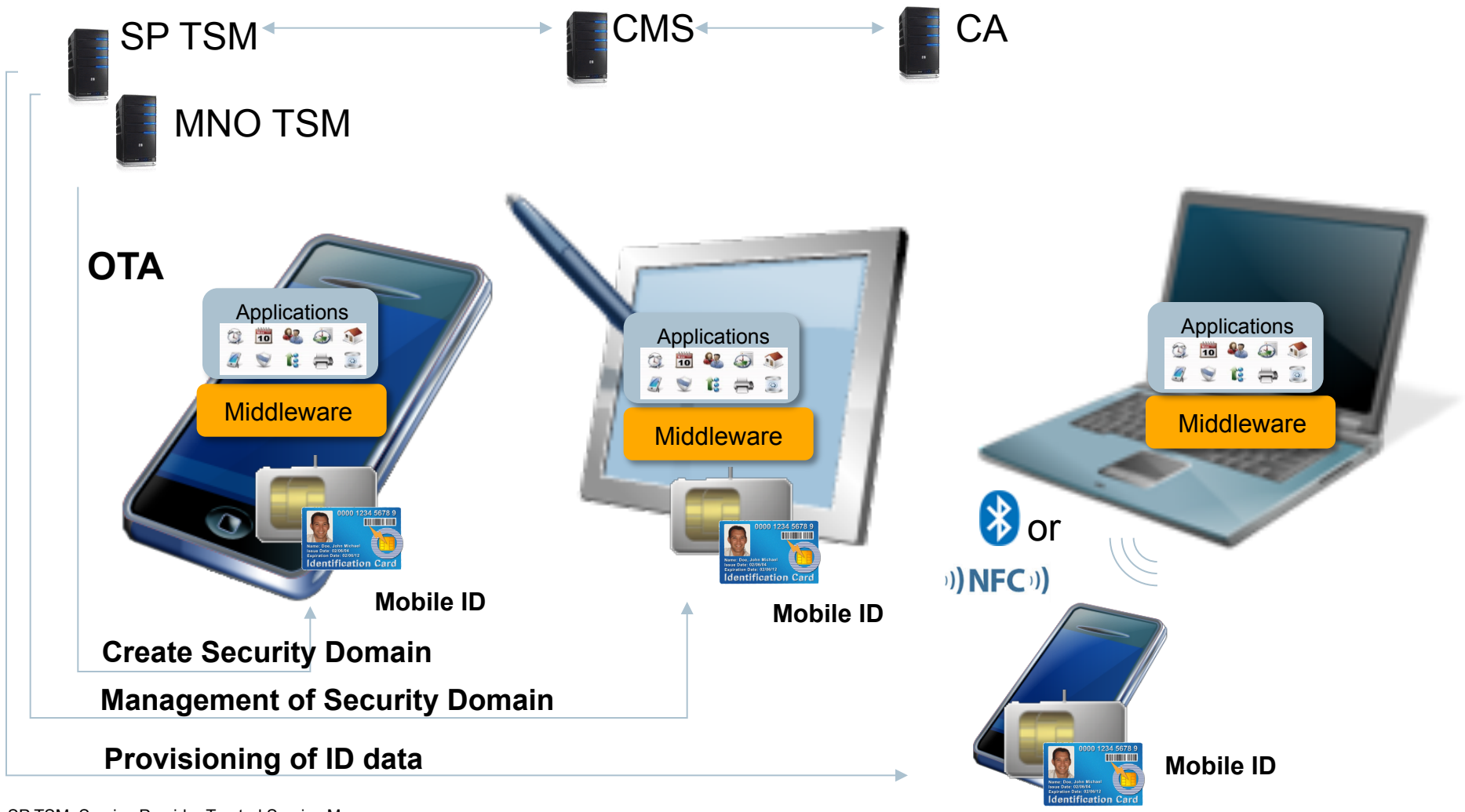
Benefits of Derived Credentials

GLOBALPLATFORM®

- Issuing Mobile ID credentials is simplified since the issuer can rely on the ID card credentials for the user validation which already exist on the ID card.
- Management of Mobile ID credentials is simplified because it is unnecessary to define a dedicated credential life cycle.
- The damage caused by security breaches may be limited since a Derived ID credential may have limited permissions and expiration dates.
- Several IDs may be derived and used individually for different purposes on different mobile devices.

Management of Mobile IDs in UICC

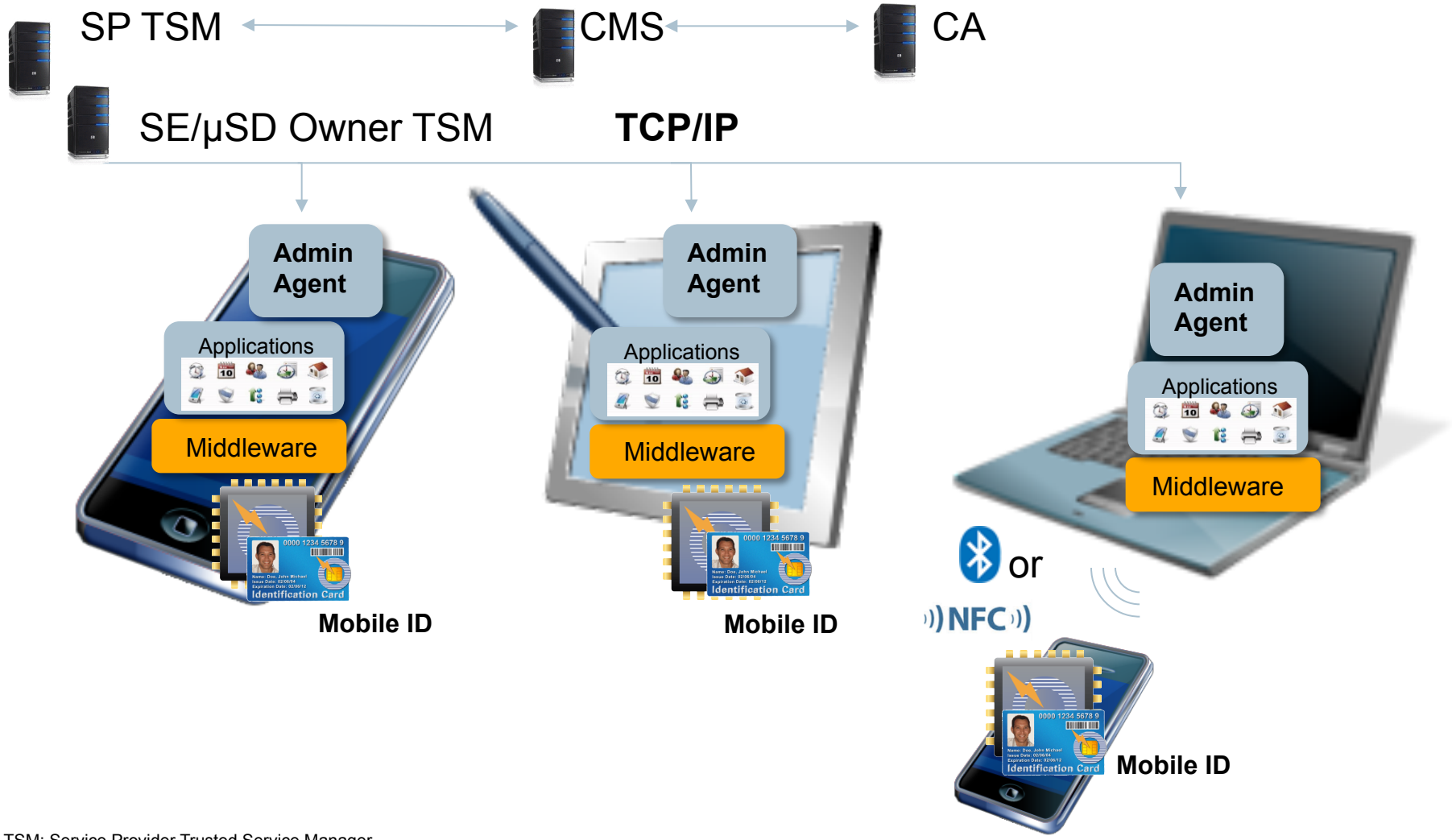
GLOBALPLATFORM®



SP TSM: Service Provider Trusted Service Manager
MNO TSM: Mobile Network Operator Trusted Service Manager
CMS: Credential Management System
CA: Certificate Authority
OTA: Over-The-Air

Management of Mobile IDs in eSE/µSD

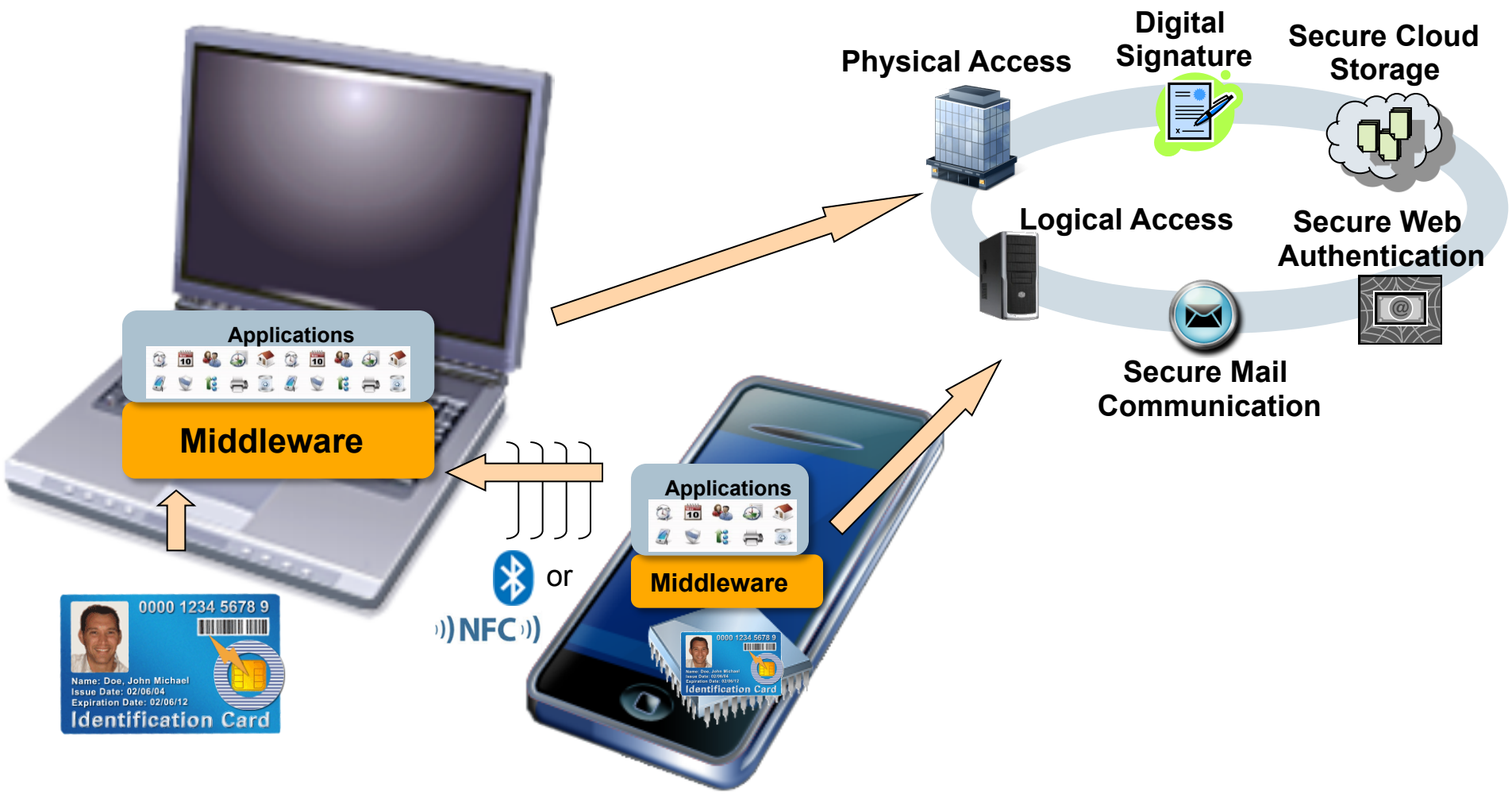
GLOBALPLATFORM®



SP TSM: Service Provider Trusted Service Manager
SE/µSD Owner TSM: Secure Element/microSD Owner Trusted Service Manager
CMS: Credential Management System
CA: Certificate Authority
TCP/IP: Transmission Control Protocol / Internet Protocol

Mobile ID Application – Use Cases

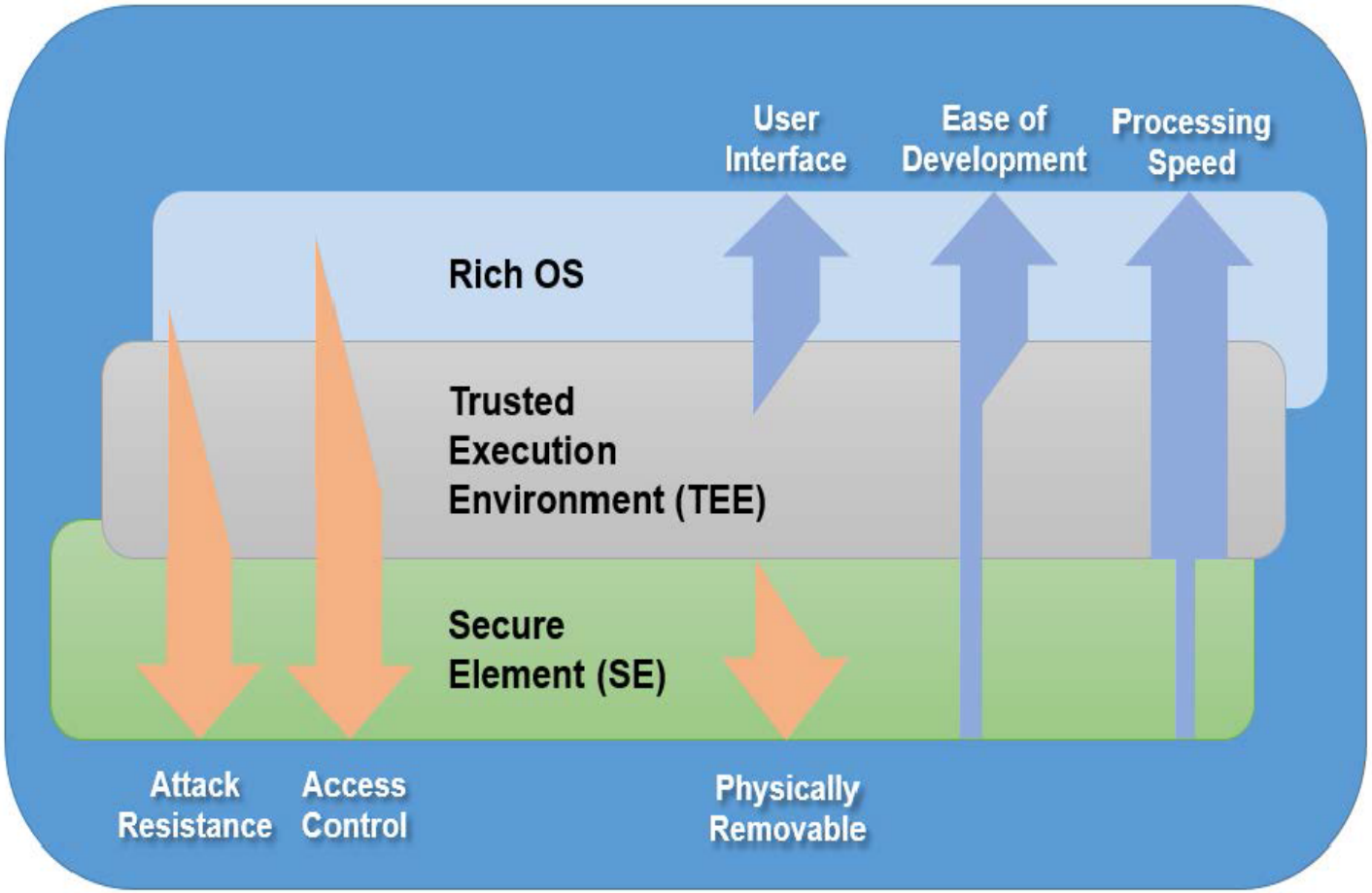
GLOBALPLATFORM®



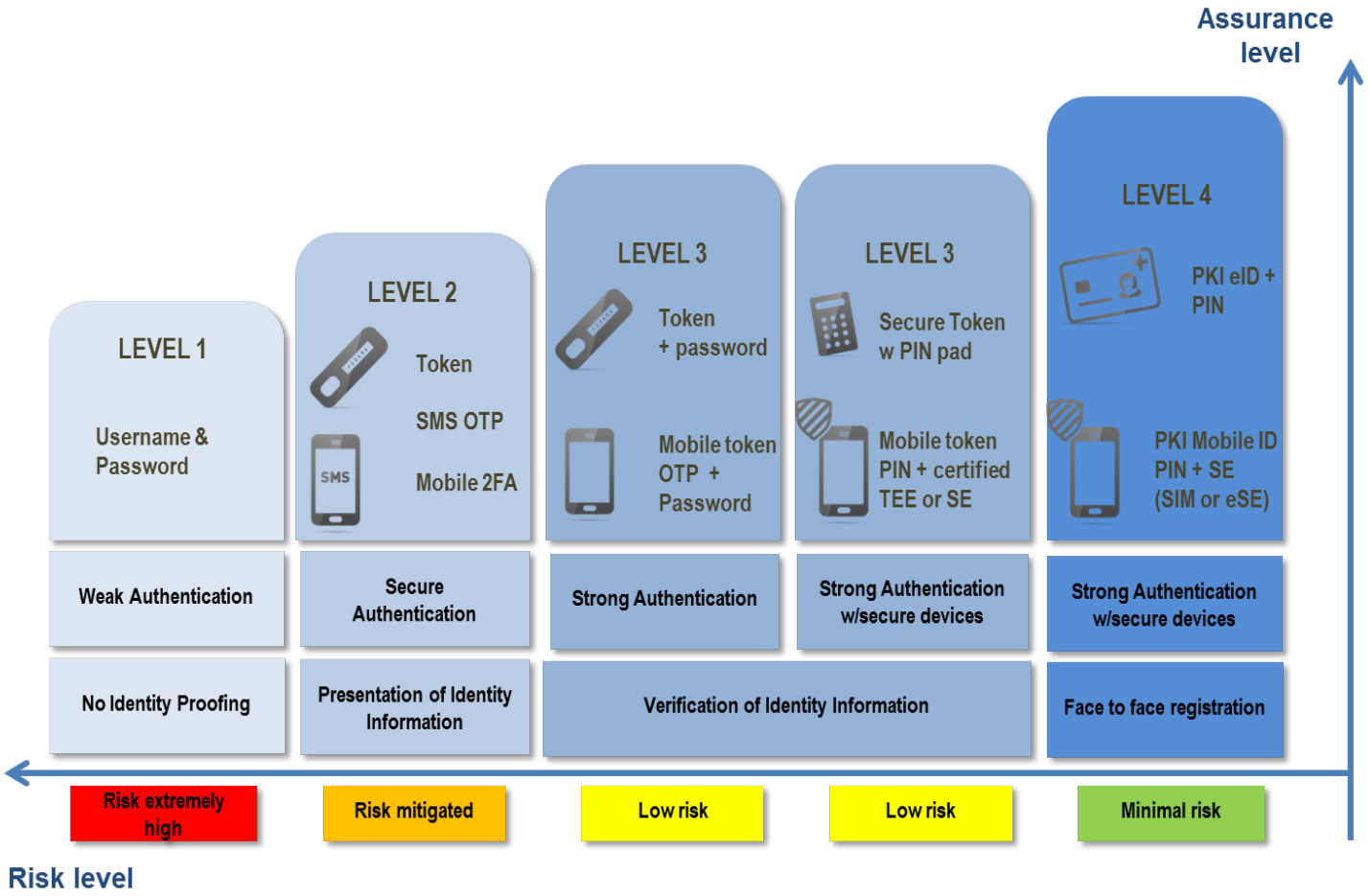
3 different categories for Authentication to:
1) another local application
2) another Mobile Device or Terminal
3) a remote server or cloud service

Processing of Services in the REE, TEE and SE

GLOBALPLATFORM®



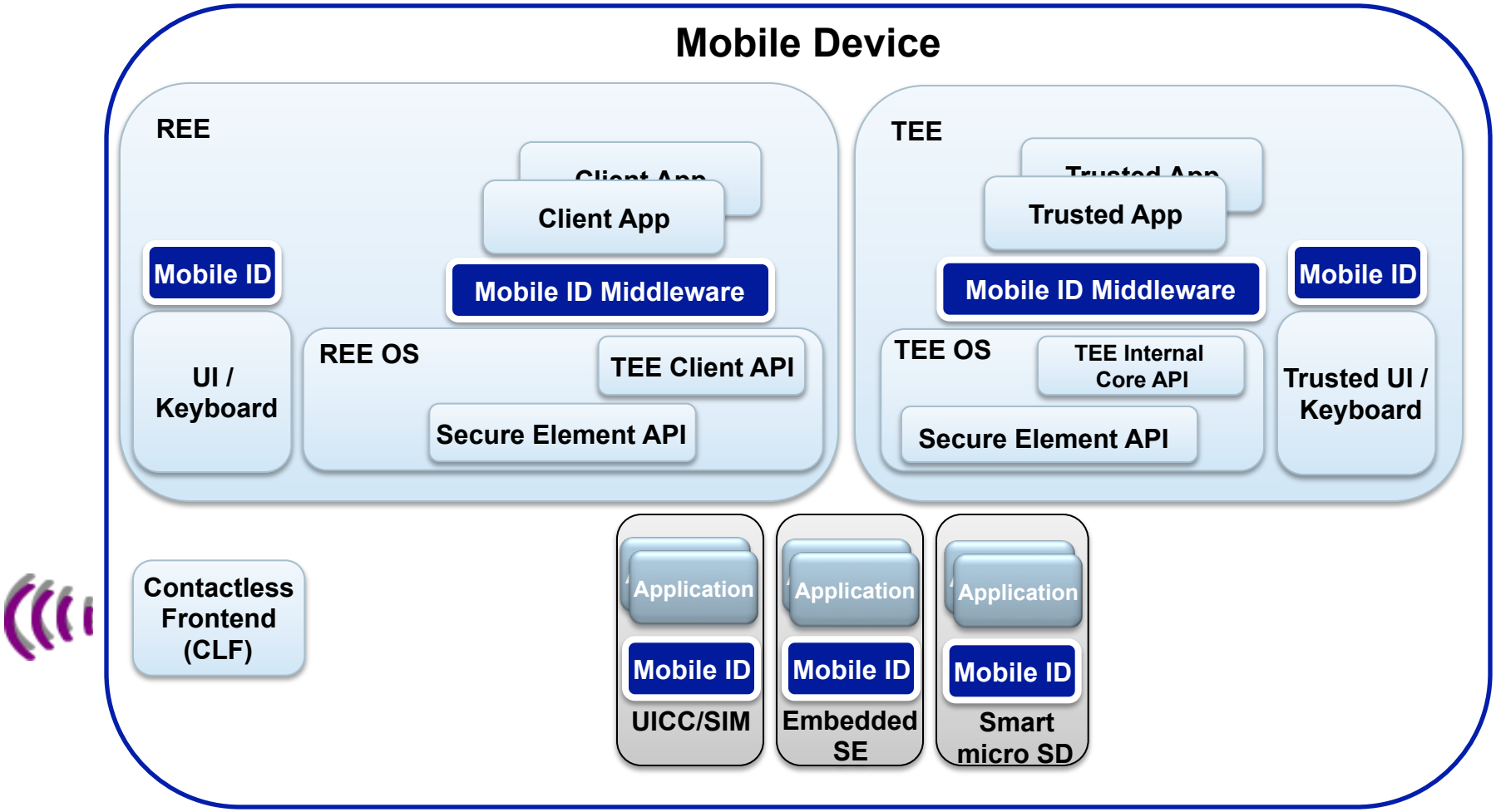
Assurance Level



Mapping between (ISO) Assurance Levels and Authentication Methods
Source: 'Eurosmart position paper – Server Signing within the eIDAS Regulation'

TEE, SE, REE and Mobile ID

GLOBALPLATFORM®



Mobile ID Implementation Scenarios (REE)

GLOBALPLATFORM®

Viability	**This solution can be deployed on all devices.**
Security	Security relies on Rich OS security. Might be secured by e.g. white box cryptography.
Deployment Considerations	Service contracts for deploying applications not needed.
Usability	Mobile ID only usable if phone is powered. Might require further user interactions (such as unlock the screen) especially after the reboot.
Security Considerations	Generally vulnerable to replication attacks. Very high Risk that Mobile ID application is getting compromised if device is rooted.

Mobile ID Implementation Scenarios (REE+SE)

GLOBALPLATFORM®

Viability	**Deployable on devices which support SE access.**
Security	Tamper resistant environment, prevents even physical attacks. End-2-End secured channels. Non-reputation. Multitenant by GP Security Domains. The user verification is implemented in the REE.
Usability	Mobile ID accessible even if device is powered-off or locked (i.e. via NFC interface). Mobile ID transferable with removable SEs (µSD, UICC).
Deployment considerations	Installation contract with the Secure Element issuer or a deployment on an own Secure Element.
Security Considerations	Tamper resistant protection for the Mobile ID credentials User verification happens in an external environment which is not under control of the SE. Certifiable environments under stringent security schemes which are sometimes required for applications on ID cards.

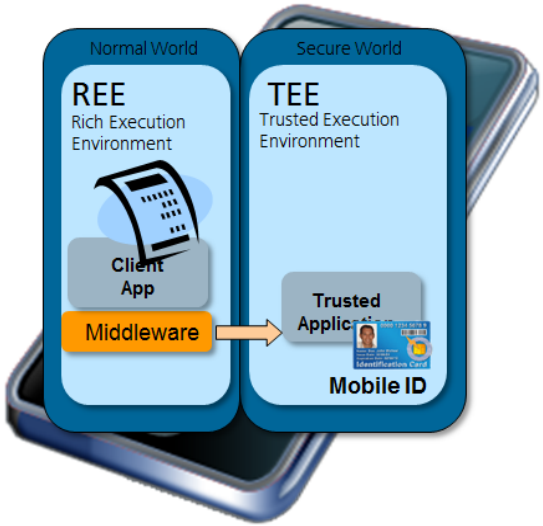
REE+SE

Mobile ID Implementation Scenarios (REE+TEE)

GLOBALPLATFORM®

Viability	Deployable on devices which support TEE.
Security	Mobile IDs are stored and used in TEE that prevents a large number of software attacks.
Usability	Mobile ID can only be used if the phone is powered In some cases it might require further user interactions (such as unlock the screen) especially after the reboot.
Deployment considerations	Requires an installation contract with the TEE owner or TEE trusted service manager.
Security Consideration	Since the TEE is a certifiable environment this solution allows the implementation of Mobile ID applications where all critical components, from processing environment and storage can be certified.

REE+TEE



Mobile ID Implementation Scenarios (REE+TEE)

GLOBALPLATFORM®

Viability	**Deployable on devices which support TEE with TUI support.**
Security	Storage and usage of Mobile ID credentials are performed in the TEE that prevents a large number of software attacks. The user verification can be protected from software attacks by using TUI.
Usability	Mobile ID can only be used if the phone is powered. In some cases it might require further user interactions (such as unlock the screen) especially after the reboot.
Deployment considerations	Requires an installation contract with the TEE owner or TEE trusted service manager.
Security Consideration	Since the TEE is a certifiable environment this solution allows the implementation of Mobile ID applications where all critical components, from user interface, processing environment and storage can be certified.

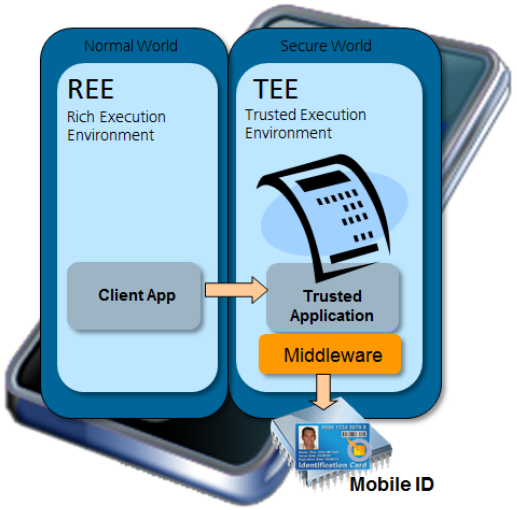
REE+TEE (with TUI)

Mobile ID Implementation Scenarios (REE+TEE+SE)

GLOBALPLATFORM®

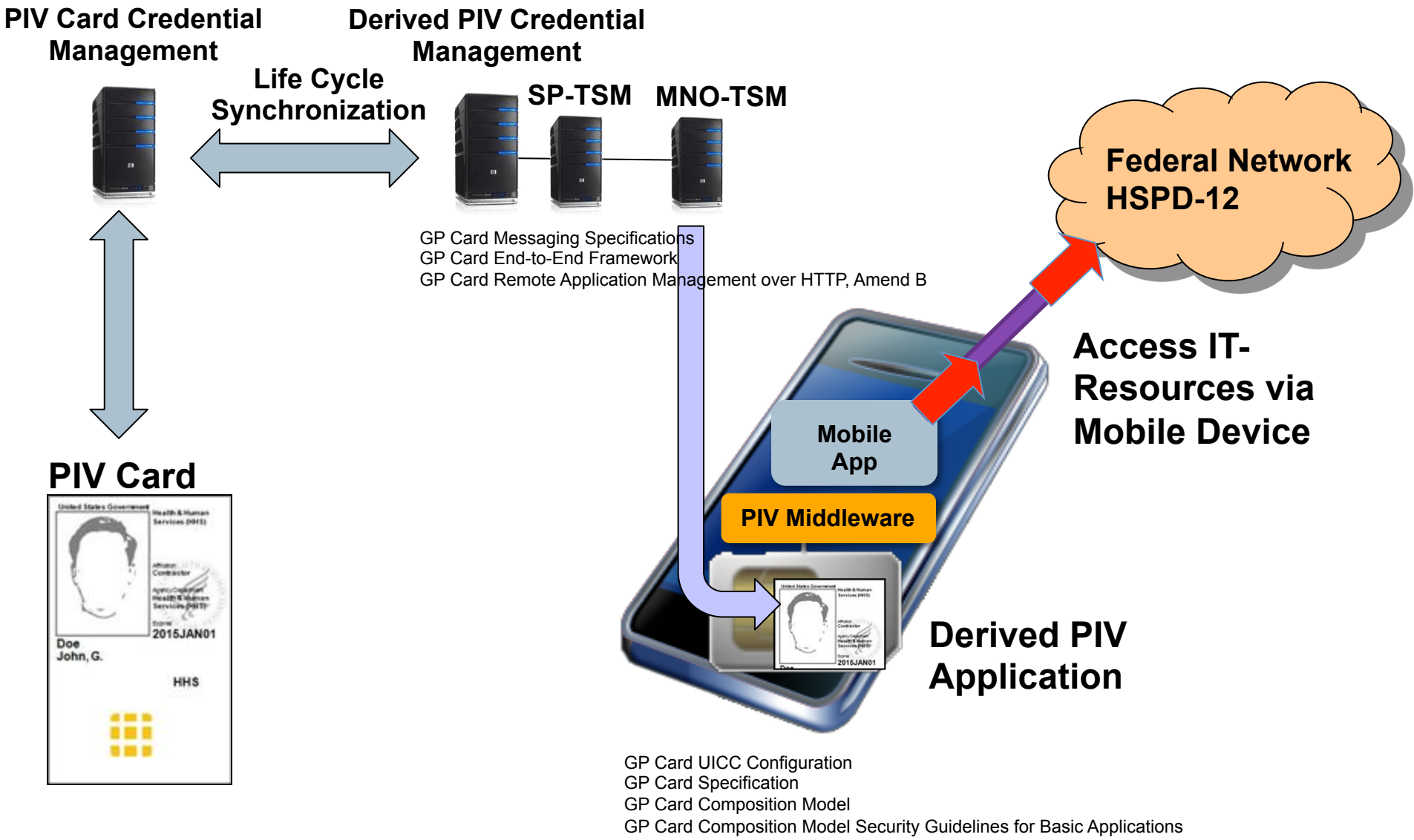
Viability	**Deployable on devices which support TEE with TUI and SE access.**
Security	Mobile ID in a tamper resistant environment prevents even physical attacks. User verification with TEE prevents a large number of software attacks. Secure Channel Protocol SCP11 to secure TEE-2-SE communication.
Usability	Mobile ID accessible even if Device powered-off (i.e. via NFC interface). Mobile ID transferable with removable SE, e.g. UICC or µSD.
Deployment considerations	Implies service contracts for the installation in two environments. Deployed applications in the TEE and SE need to be managed and synchronized.
Security Consideration	This solution provides the highest level of security All critical components, from user interface, processing environment and storage can be certified.

REE+TEE+SE



Mobile ID Example: Derived PIV Credentials (SP800-157) for UICCs

GLOBALPLATFORM®



Conclusion

GLOBALPLATFORM®

- GlobalPlatform is widely adopted by many sectors / industries so there is no need to reinvent the infrastructure. It is deployed in mobile devices today and is stable and secure.

- Mobile ID is increasingly important for a wide range of applications, including government-to-citizen, government-to-government, and public sector applications in finance, healthcare, and others.

- Mobile ID has a diverse number of use cases around the deployment and use of various IDs, and each ID implementation has varying levels of potential technical implementations and security requirements. This involves the SEs, TSMs, Card Specifications and GlobalPlatform's TEE.

- GlobalPlatform provides frameworks, configurations, profiles, protocols, interfaces and standards, which assure interoperability, consistency and enables implementation of end-to-end solutions in a secure and certified way.

Thank you!