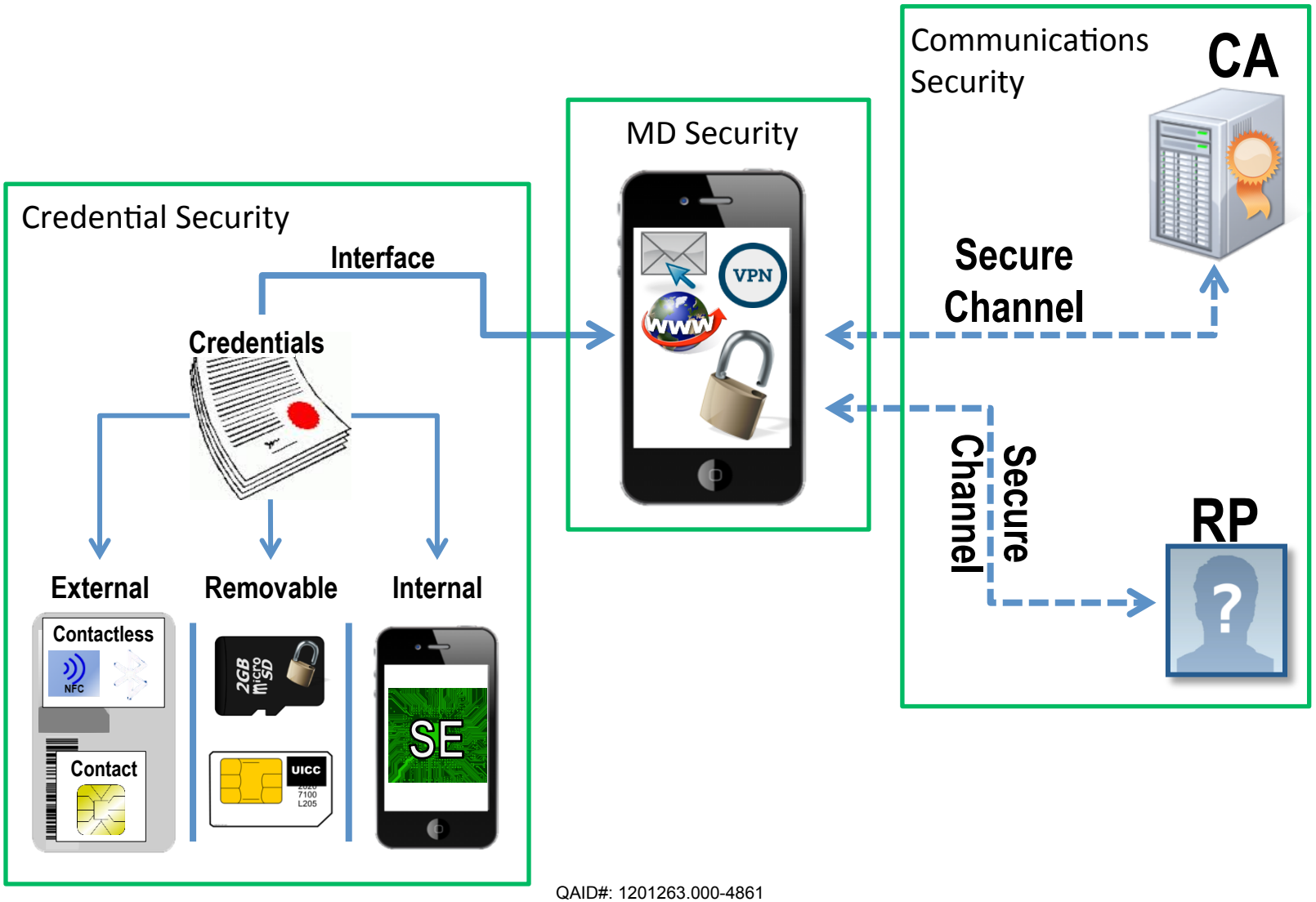



Identity Management in the Mobile Environment

Framework for Mobile Identity Approval Procedures

QAID#: 1201263.000-4861

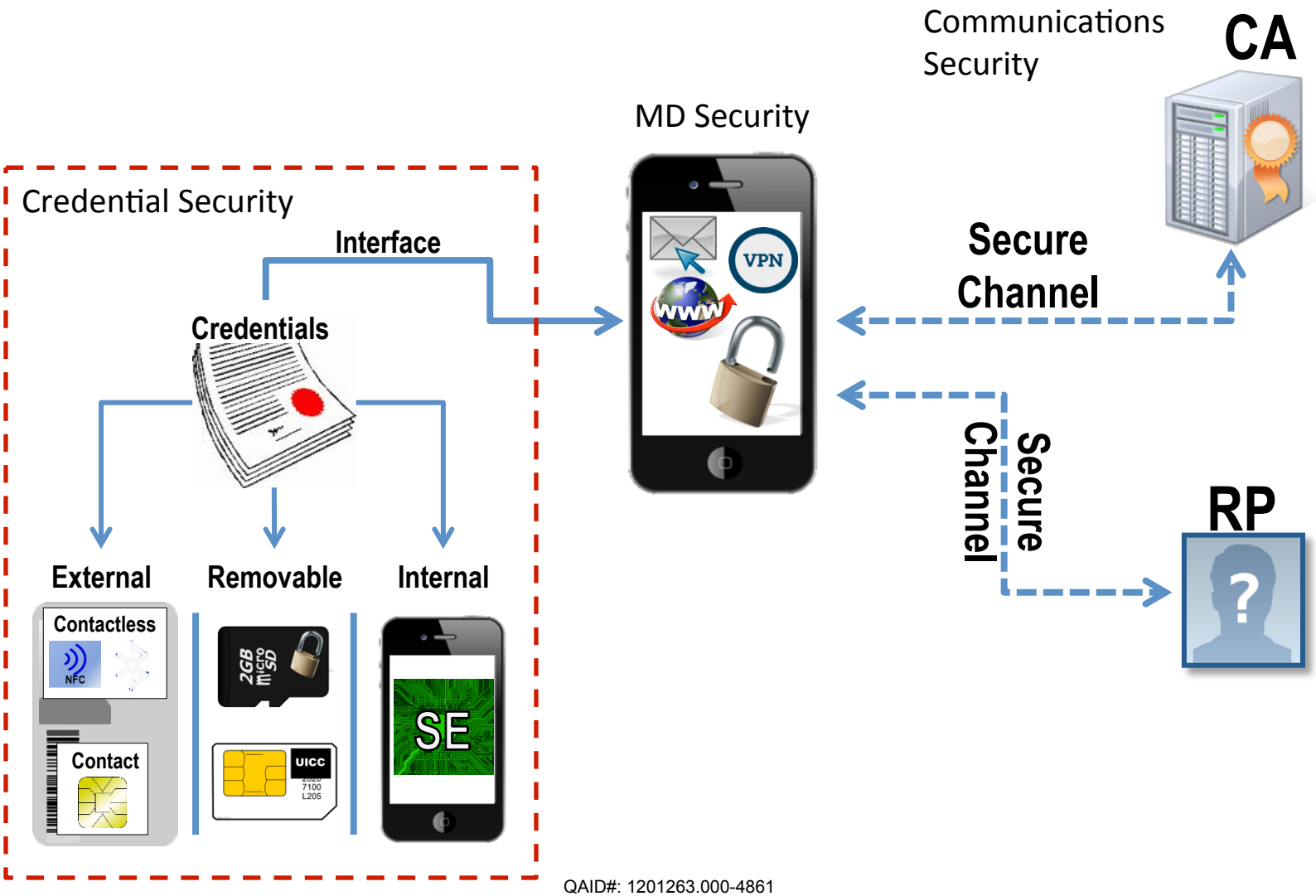
The Big Picture





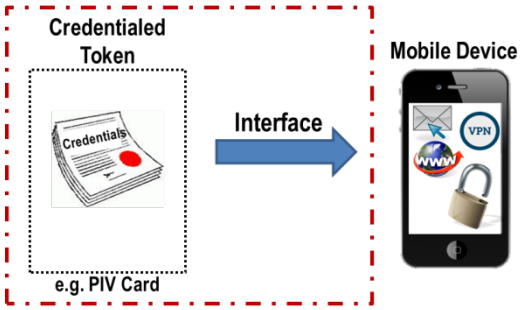

Security of Using a Local Credential with the Mobile Device

Using a Local Credential with a MD



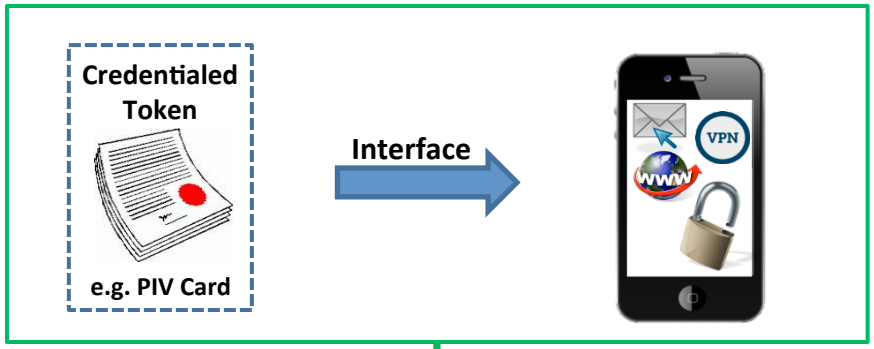
Analysis of Credential-to-MD Transfer

1. Identify potential implementation permutations
2. Break down each permutation into elements (SE, PIV, Token, etc.)
3. Qualify each permutation and its elements to:
    - Is it **PHYSICALLY DURABLE?**
    - Will it be **COMPATIBLE?**
    - Is it **SECURE?**



- **PHYSICAL DURABILITY**
    - Ex: PIV flex test, torsion test, abrasion test, etc. (Usually will be outside this project scope. A report certifying this characteristic will be required)
- **INTERFACE COMPATIBILITY**
    - Internal consistency & compatibility of the hardware & software used in each permutation
    - Handling of multiple credentials or java applets on a SE
- **SECURE**
    - FIPS/Common criteria, cryptographic, PKI, RSA/DSA encryption, etc.
    - Interface security of SE to other components

Credentialed Token Implementation Methods



External

Contactless

NFC

Contact

Removable

UICC/µSD

2GB micro SD

UICC 7100 L205

Internal

MNO UICC / SE-TEE

SE Hardwired

External Credential Implementation

Contact

Interface

Thursby PKard®Reader

Durable? Compatible? Secure?

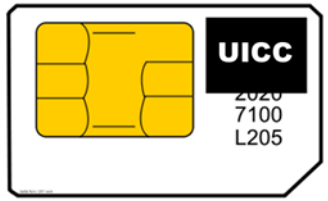
Contactless

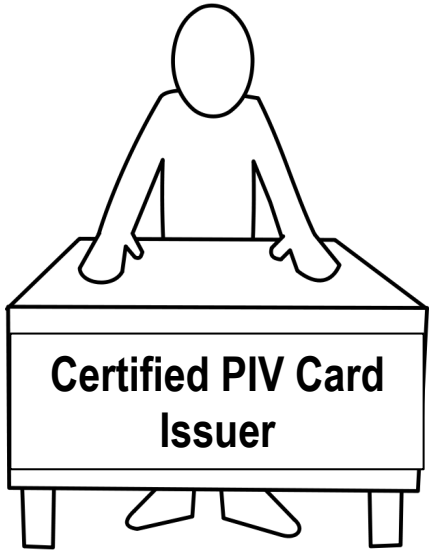
BaiMobile™

Interface

Removable Credential Implementation

- Credential using a UICC/µSD
- Must assess: 1) Durability; 2) Compatibility; and 3) Security

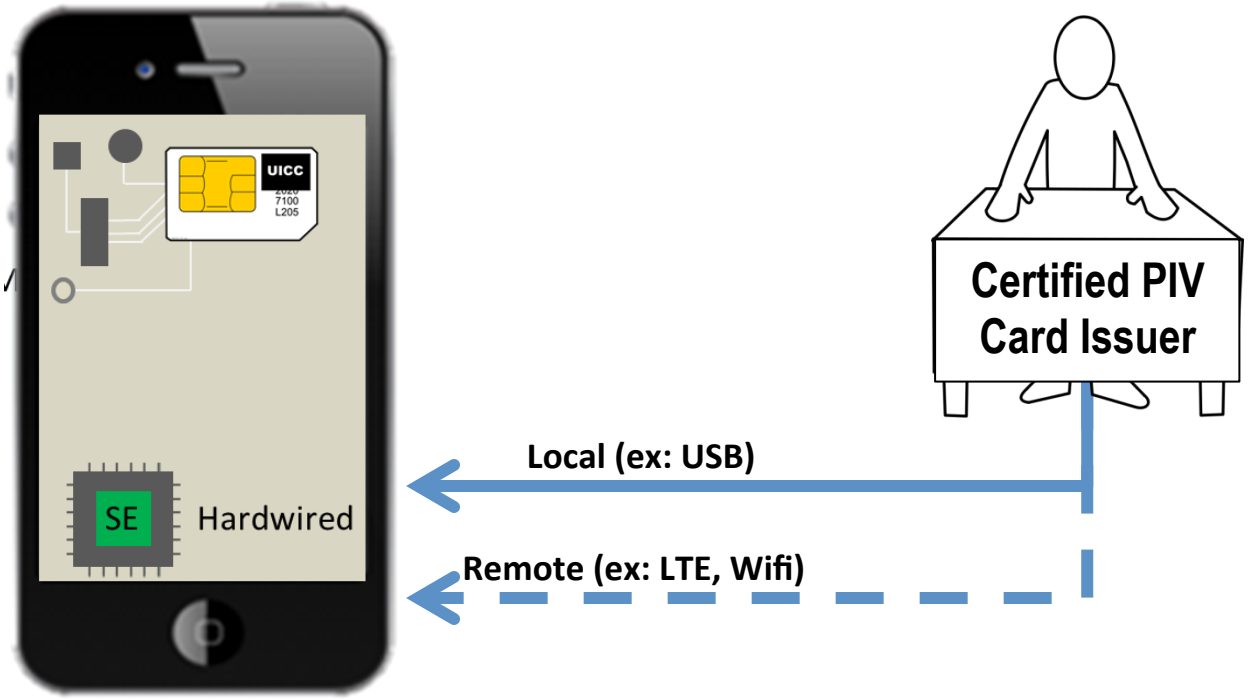




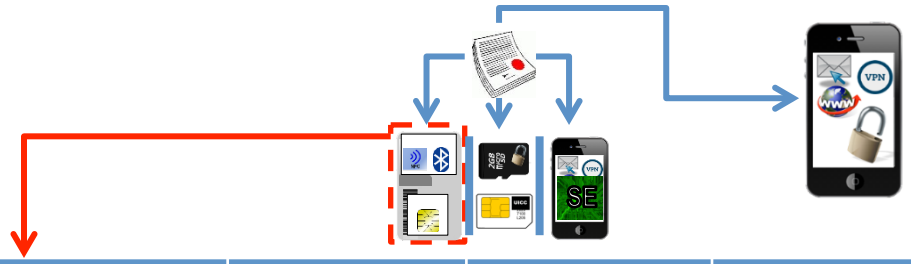
Additional consideration: UICC bound to *one* device only?

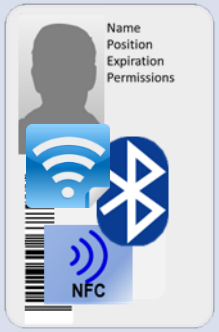
Internal Credential Implementation

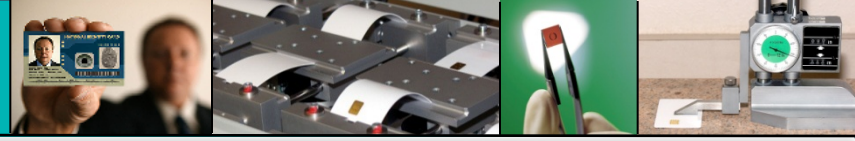
- Credential using an internal token
  - May be provided/managed by MNO
  - UICC
  - Permanently embedded module
- Must assess: 1) Durability; 2) Compatibility; and 3) Security



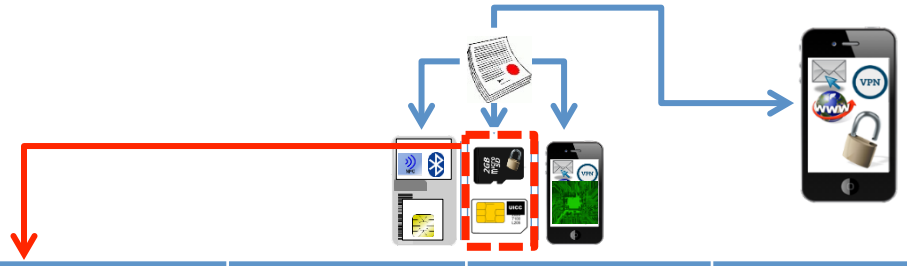
External Credential



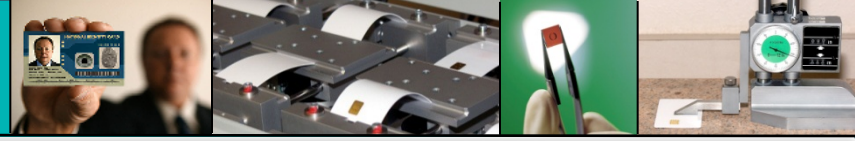
		Standards	Interoperability	Security	Questions	Additional
 Contact		• FIPS 201 • SP800-73 • SP800-76 • SP800-78 • SP800-79	If follows the standards, will it be compatible?	• LOA		• Physical prop's (10373, 7816) • Integrated Circuit prop's
	Interface 	w.r.t. Mobile Security • ?				
 Contactless		• FIPS 201 • SP800-73 • SP800-76 • SP800-78 • SP800-79	If follows the standards, will it be compatible?	• LOA		
		• 14443 • FIPS-201 • FIPS-140				



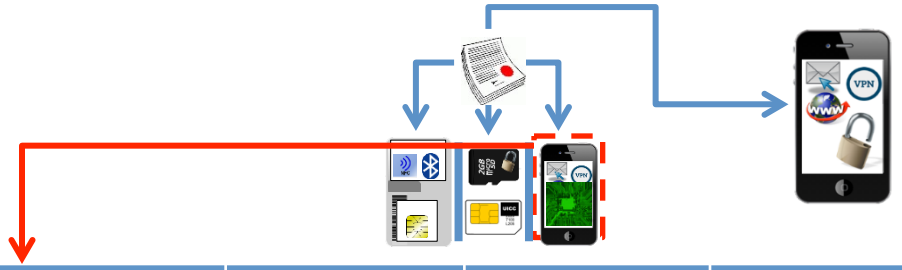
Removable

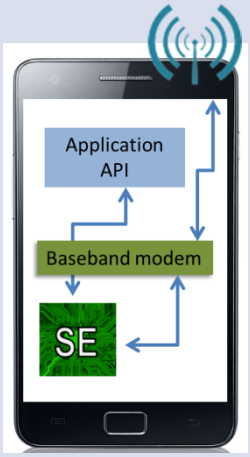
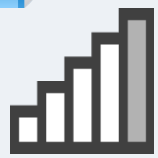


PERMUTATIONS		Standards	Interoperability	Security	Questions	Additional
 UICC		• FIPS 201	If follows the standards, will it be compatible?	• LOA • Common Criteria		• Physical prop's (10373, 7816) • Integrated Circuit prop's
		W.R.T. Mobile Security • ?				
 µSD		• FIPS 201	If follows the standards, will it be compatible?	• LOA		
		• FIPS-201				

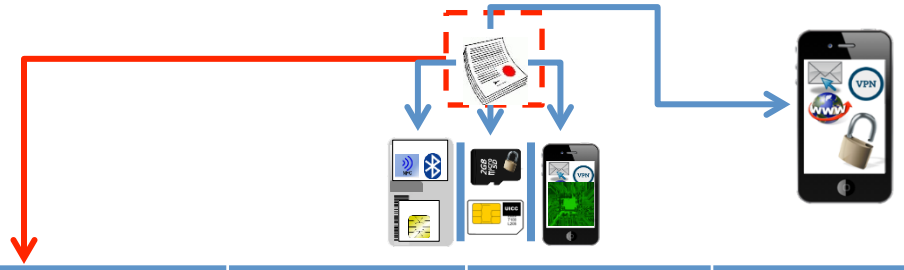


Internal

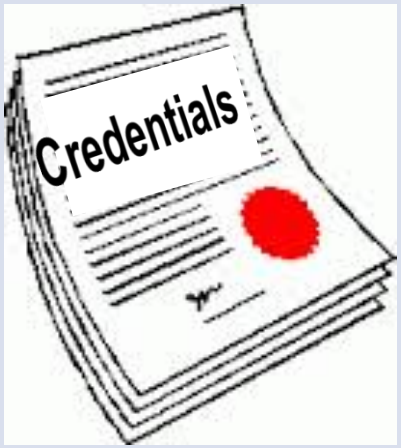


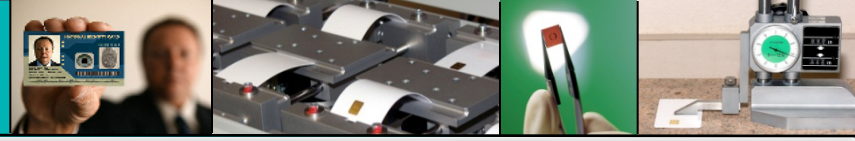
PERMUTATIONS	Standards	Interoperability	Security	Questions	Additional
  **MNO UICC**	• FIPS 201 • FIPS 186 • Cert. Hierarchy Verification	If follows the standards, will it be compatible?	• LOA		
  	W.R.T. Mobile Security • ?				

Credential + Mobile Security

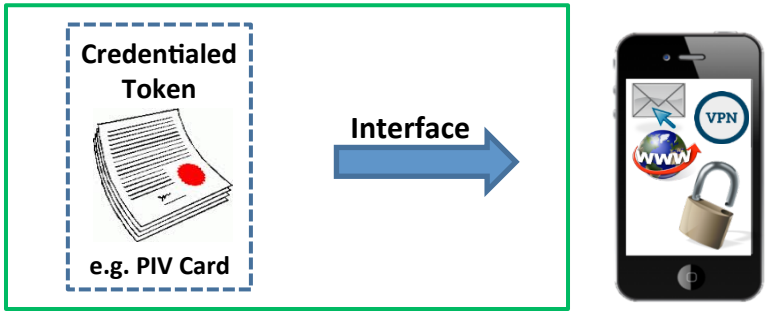


Even the credential! Leave no stone unturned

	Standards	Interoperability	Security	Questions	Additional
	• FIPS 201 • CRL • Certificate hierarchy verification • X.509	If follows the standards, will it be compatible?	• LOA		• Physical prop's (10373, 7816) • Integrated Circuit prop's



Credential Transfer Summary



- Physical durability
- Compatibility
- Security

Credentialed Token

Location	Examples
External	CAC,PIV
Removable	UICC, µSD
Internal	Embedded SE, Virtual SE

Interface

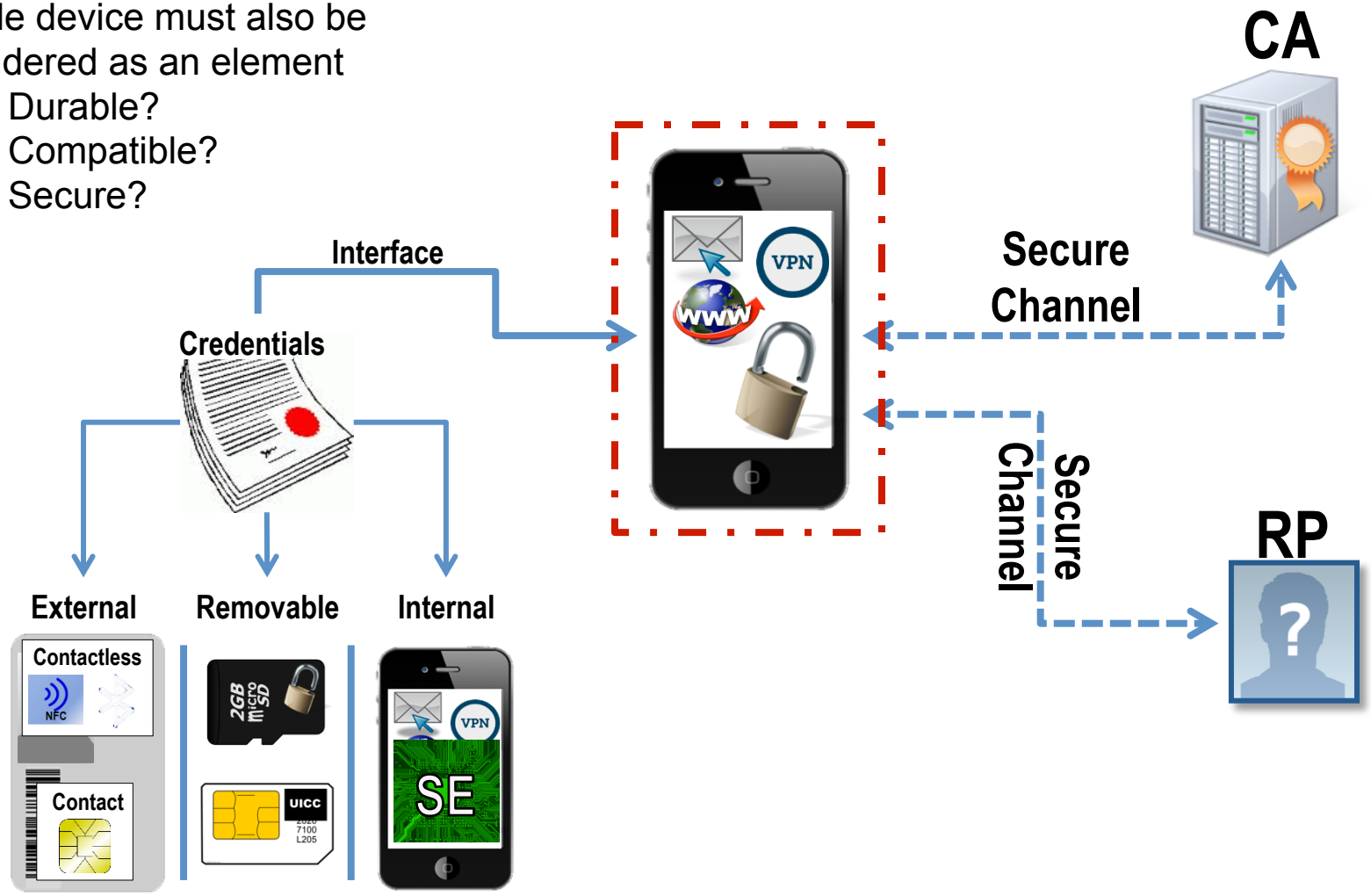
Type	Examples
Contact	CAC sled
Contactless	NFC, Bluetooth, LTE
Interface Policy	Insert-remove, tap, maintained proximity

Security of the Mobile Device

Security of Mobile Device

Mobile device must also be considered as an element

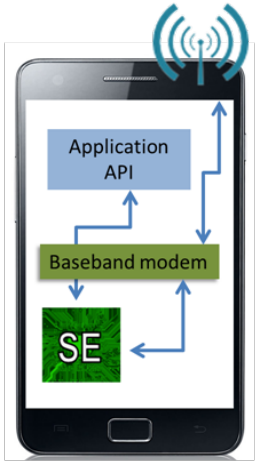
- Durable?
- Compatible?
- Secure?



Summary of Mobile Device Secure Application Considerations

- Each ***element*** within the device and the ***interface*** between them must be tested as durable, compatible, and secure
- Some existing standards
  - Global Platform
    - Trusted User Interface (TUI)
    - Trusted Execution Environment (TEE)
    - SE API specification
    - SE Access control
    - SE Remote application management
  - Common Criteria
  - FIPS 140/201
  - Application security testing (App-vetting)
    - ISO/IEC 7064, 9796, 9797, 14888 , 27001

Trusted User Interface



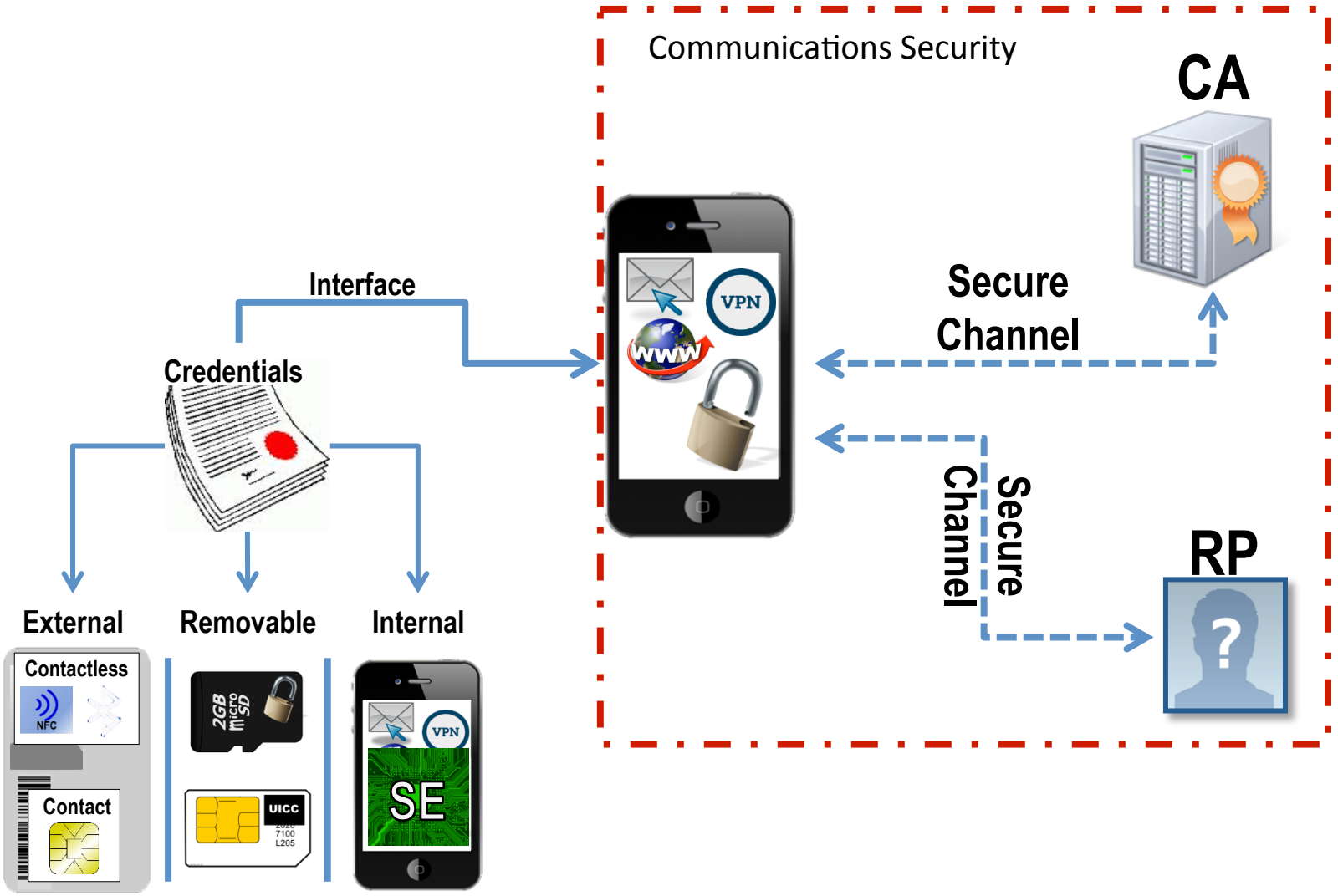
Trusted Execution Environment

Secure Element/ Cryptography




Security of Communications: Encryption and Authentication

Security of Communications






Messaging Options for Secure Communications

- Level of security desired vs. performance
  - **Encryption strategy** (symmetric vs. PKI)
  - **Communication security** (insecure vs. secure (TLS))
  - **Digest usage**
- Higher security ≈ lower performance
- Select from security options below to obtain required/desired level of security

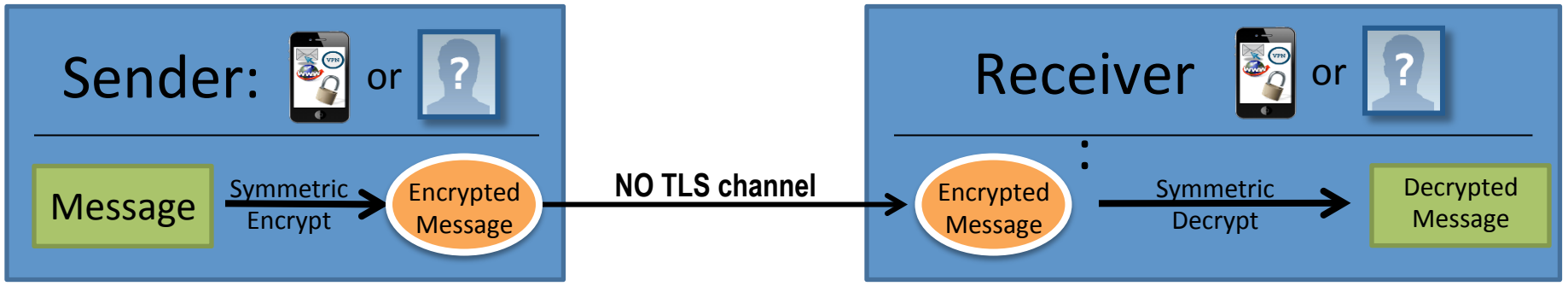
Secure Options Menu

- **Encrypted message**
  - Symmetric (shared (public) key)
  - Asymmetric (PKI)
- **Over-the-Air (OTA) communications**
  - Insecure
  - Secure – Trusted Layer Security (TLS)
- **Digest architecture**
  - Encryption optional

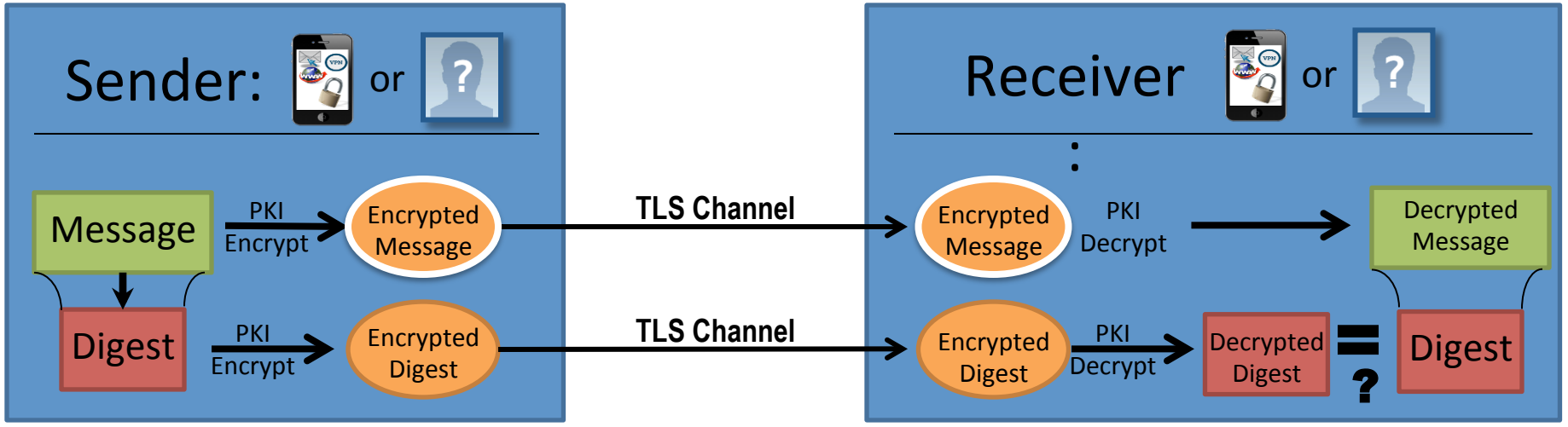
Considerations

- Policy/Externally driven requirements
- Security level
- Reliability
- Availability
- Bandwidth required
- Power required
- Integrity/Confidentiality

Architecture for *Weak* Security



Architecture for *Extreme security*; includes all elements






Additional Considerations

- The following are present in all architectures and their security/compatibility must be considered:

Certificate Authority

- X.509 compliant
- Cert revocation list
- Cert hierarchy verification
- PKCS# CSR, SCEP
- Trusted list of CA's

Over-the-Air Communication

- Insecure
- TLS
- PKCS#

Relying Party

- One-way vs. Two-way trust
- Federation membership




Summary of Communications Security

- Security required/desired vs. performance drives the architecture
  - Encryption strategy
  - Communication security
  - Digest usage
- Performance consideration examples:
  - Bandwidth required
  - Power required
  - Speed of transaction
  - Security level
  - Integrity
  - Confidentiality
  - Reliability
  - Availability
- Testing required to:
  - Identify security gaps
  - Ensure architectures are followed, even as apps are updated
  - Interfacing with the Certificate Authority and Relying Party is flawless

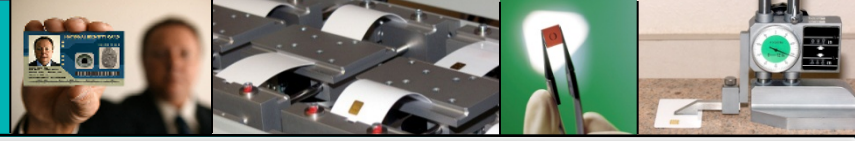
Derived Credentials

Deriving and Derived Credentials

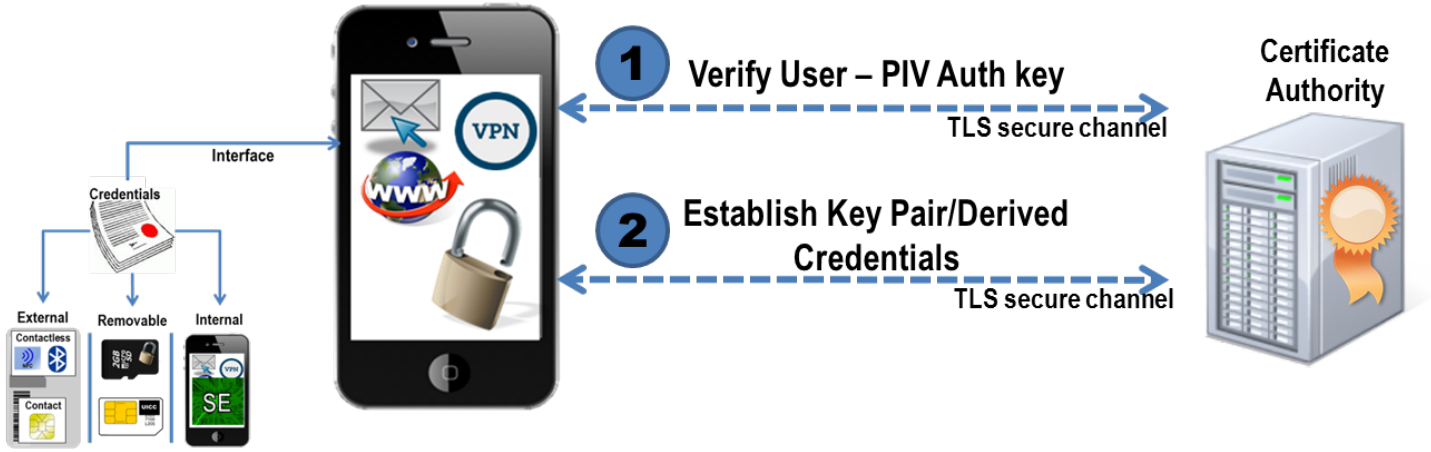
- The derived credential option requires consideration of both the issuance of the credential to the MD, as well as its maintenance and termination.

- Deriving procedure:
  - Driven by NIST SP800-157 and enterprise policy
  - Options exist in SP800-157

- Derived credentials:
  - Also covered in SP800-157
    - Maintenance and termination
    - Relation to original credential



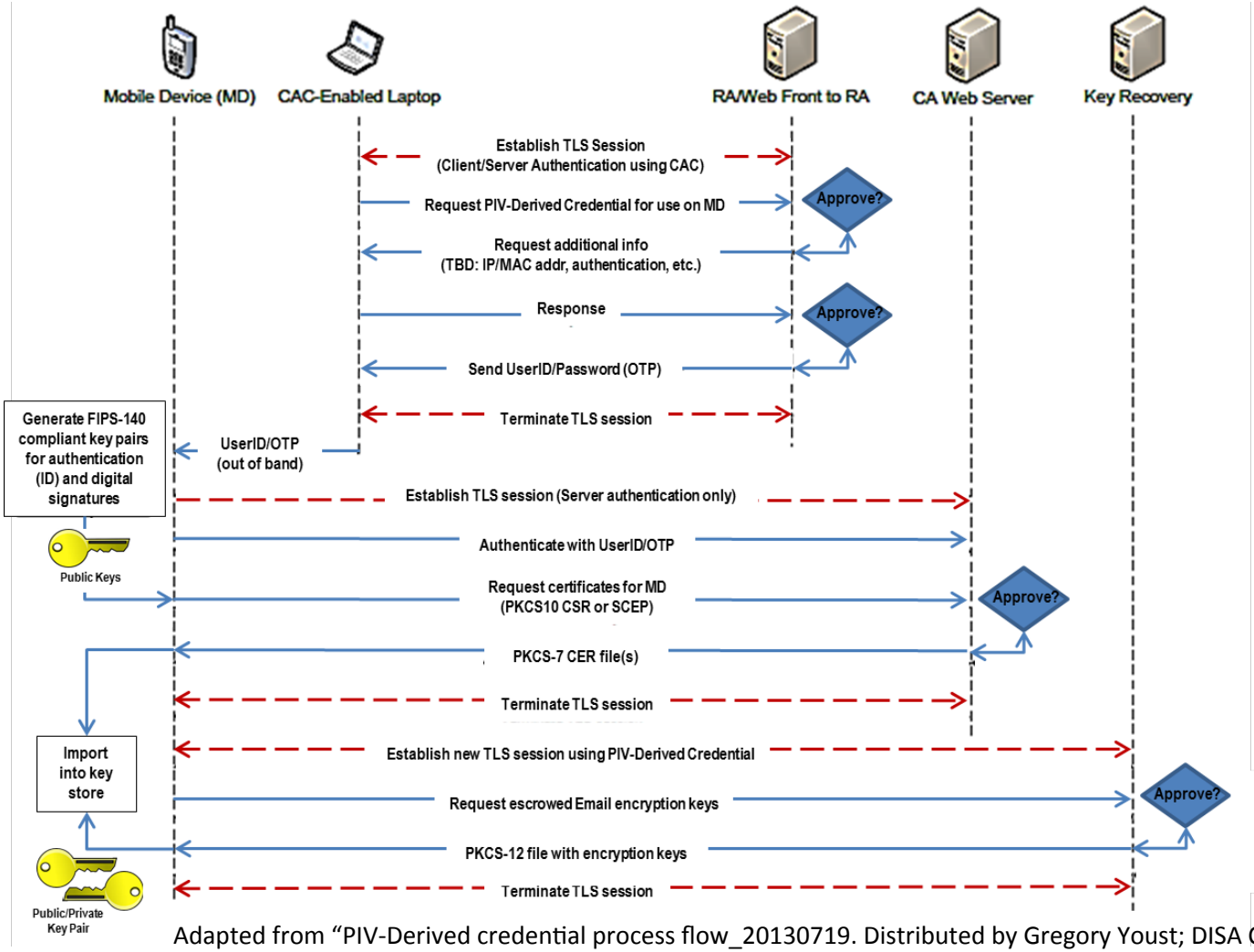
Deriving (Issuance)



- SP800-157 dictates issuance and relationship between PIV credential and MD derived credential
- LOA-3 remote issuance requires TLS communications
- LOA-4 cannot be issued remotely; biometric authentication required.
- MD integrity verification (jailbroken, rooted, etc.)
    - Commercial products available such as Fixmo Sentinel IS
- Testing required to verify conformance to standards/special publications

Special Issuance Situations

EX: What if transferring credential from CAC to MD is unavailable/restricted?



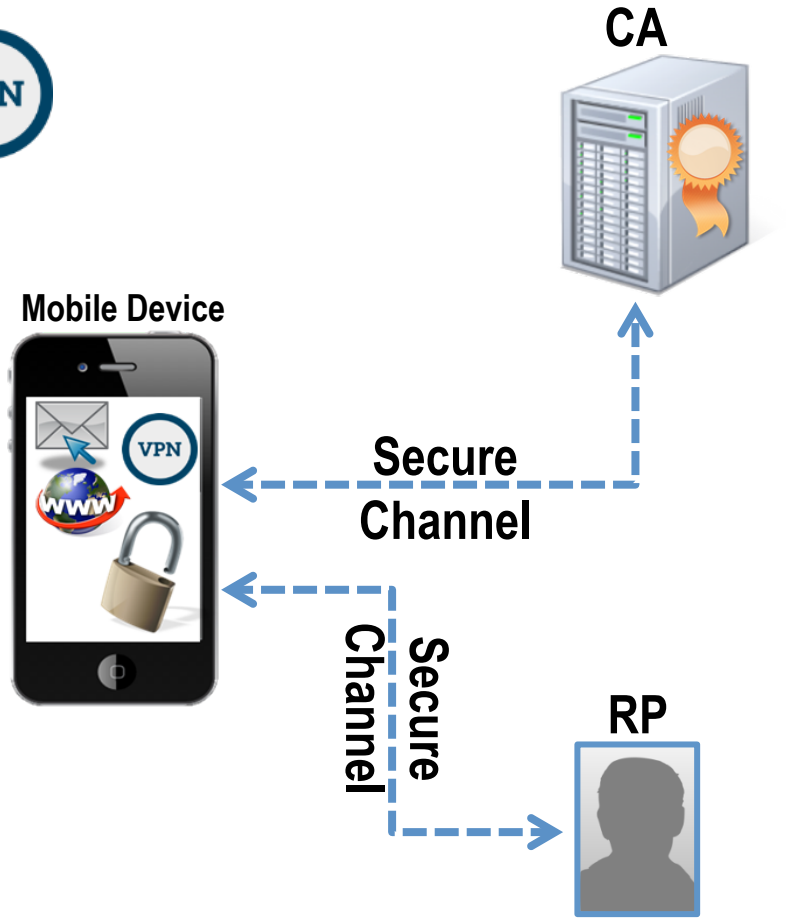
PROCESS:

1. CAC-enabled laptop vouches for MD
2. Laptop receives and forwards OTP to MD out-of-band
3. MD registers with CA using OTP
4. MD uses newly-acquired ID-cert to obtain Email-cert

Adapted from "PIV-Derived credential process flow_20130719. Distributed by Gregory Youst; DISA CTO

Use and Maintenance of Derived Credential

- Use-case drives level of encryption/security used
- Policy for each use case
- Testing required to verify established security and that security is maintained during updates






Derived Credentials Summary

- SP800-157 specifies secure policy, software, and hardware requirements for derived credentials
- Secure issuance must also be strongly considered
- Testing is required for standards/policy conformance
- Gaps in the standard can exist, which must be explored
- Additional standards and testing may be required

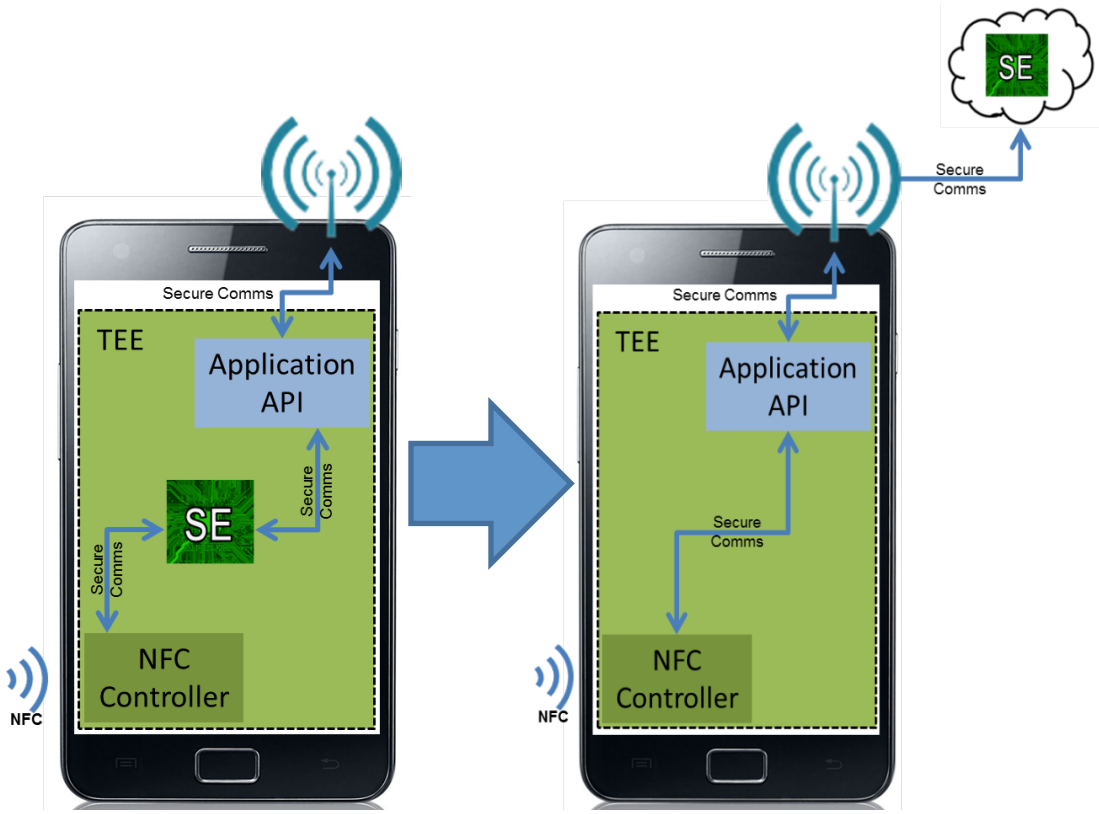
Commercial Efforts Toward Mobile Authentication

Host Card Emulation (HCE)

- Recently adopted by Visa/ Mastercard for NFC-payments
- **The secure element is moved out of the phone and onto the cloud**
- Requires over-the-air communication

Relevance for FICAM

- User authenticates to server, instead of locally to mobile device
- Requires transmitting PIN/ Biometric to the SE for authentication
- Questions exist for how to protect this transmission – with no local SE, Private Key Encryption is not possible
- LOA considerations will guide the feasibility and inherent testing requirements






FIDO Alliance

- Eliminate passwords, while still having strong two-factor authentication
  - ~~What you know (password)~~
  - What you have (mobile device)
  - Who you are (biometric)
- Local authentication (biometric) unlocks the private key 'store'
  - Similar to typing in PIN to unlock CAC/PIV
  - Key 'store' supports separate keys for each RP
- Secure element still part of the architecture
- Commercial effort, but could fit with FICAM




Mobile Security Verification Testing

- Have laid out both the landscape and what needs to be considered for testing in order to assure security in a mobile environment
- Can now identify relevant existing standards and test protocols for each of the implementation permutations discussed
- Can also identify areas where standards will have to be developed in order to verify security

FIPS 140-2 FIPS CRYPTOGRAPHY

GSA FIPS 201 APPROVED

GLOBALPLATFORM

ISO International Organization for Standardization



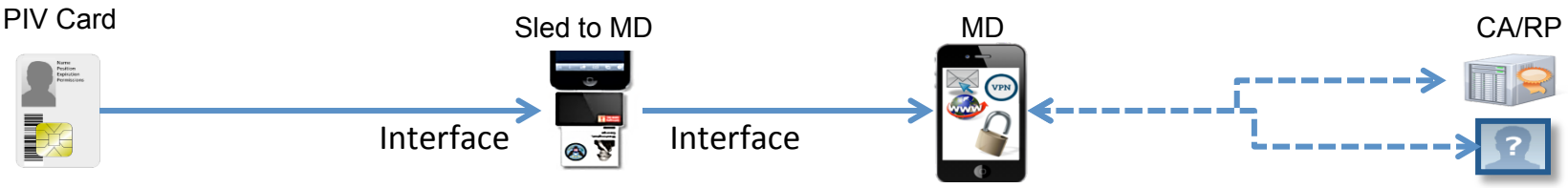

Summary of Approval Procedure Scope

T = Testing/Verification Required

Local credentialed token	Interface	Secure mobile device	Secure communications
External Removable Internal			

Sample MD Approval Procedure

The below list of tests are a partial listing of the standards that this one configuration must show conformance to in order to be approved for use in the federal mobile identity ecosystem



Local credentialed token	Interface	Secure mobile device	Secure communications

Standards examples
• GSA PIV Approval Procedure
  • ISO/IEC 10373
  • ISO/IEC 7816
  • ISO/IEC 7810
  • FIPS 201
  • SP800-73
Test examples
• ISO 7816 report
• FIPS 201 report
• Security lockout protocol
	Standards examples
	• ISO/IEC 10373
	• ISO/IEC 7816
	• ISO/IEC 7810
	Test examples
	• UL certificate
	• Pin position/shape
	• Card reader voltage/ current limit
	• Reader → Phone secure comms
		Standards examples
		• Global Platform
		  • Trusted user interface
		  • Trusted execution
		• Common Criteria
		• ISO/IEC 11889
		Test examples
		• Bad PIN lockout
		• FCC/UL certificate
		• TUI/TEE cert. hierarchy verify
		• Cryptographic zeroing/ tamper-resistance
			Standards examples
			• SP800-63
			• SP800-73
			• PKCS#/SCEP
			• X.509
			• FIPS 186
			Test examples
			• Bad certificate denial
			• Denied access to forbidden RP
			• Denied access to non-approved RP

Conclusion

- There are a significant number of permutations, standards, and test protocols that must be incorporated in order to build a fully-encompassing secure mobile device approval procedure

- The next step is to prioritize development of a test approval procedure for the most popular options, based on the case studies