Identity Management in the Mobile Environment

Framework for Mobile Identity Approval Procedures
Security of Using a Local Credential with the Mobile Device
Using a Local Credential with a MD

Credential Security

Communications Security

CA

MD Security

Secure Channel

RP

Contactless

External

Removable

Internal

Contact

Credentials

Interface
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

**Removable**
- Contact
- UICC/μSD

**Internal**
- MNO UICC / SE-TEE
External Credential Implementation

- Contact
- Contactless
- BaiMobile™
- Thursby PKard®Reader

Durable?  Compatible?  Secure?

Interface

Baidy

QAI#: 1201263.000-4861
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

<table>
<thead>
<tr>
<th>Standards</th>
<th>Interoperability</th>
<th>Security</th>
<th>Questions</th>
<th>Additional</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 201</td>
<td>If follows the standards, will it be compatible?</td>
<td></td>
<td>LOA</td>
<td>Physical prop’s (10373, 7816)</td>
</tr>
<tr>
<td>SP800-73</td>
<td></td>
<td></td>
<td></td>
<td>Integrated Circuit prop’s</td>
</tr>
<tr>
<td>SP800-76</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP800-78</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP800-79</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>w.r.t. Mobile Security</td>
<td>?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standards</th>
<th>Interoperability</th>
<th>Security</th>
<th>Questions</th>
<th>Additional</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 201</td>
<td>If follows the standards, will it be compatible?</td>
<td></td>
<td>LOA</td>
<td></td>
</tr>
<tr>
<td>SP800-73</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP800-76</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP800-78</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP800-79</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14443</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIPS-201</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIPS-140</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Removable

<table>
<thead>
<tr>
<th>PERMUTATIONS</th>
<th>Standards</th>
<th>Interoperability</th>
<th>Security</th>
<th>Questions</th>
<th>Additional</th>
</tr>
</thead>
<tbody>
<tr>
<td>UICC</td>
<td>FIPS 201</td>
<td>If follows the standards, will it be compatible?</td>
<td>LOA</td>
<td>Common Criteria</td>
<td>Physical prop’s (10373, 7816) Integrated Circuit prop’s</td>
</tr>
<tr>
<td></td>
<td>W.R.T. Mobile Security</td>
<td>?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FIPS 201</td>
<td>If follows the standards, will it be compatible?</td>
<td>LOA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>μSD</td>
<td>FIPS-201</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Internal

<table>
<thead>
<tr>
<th>PERMUTATIONS</th>
<th>Standards</th>
<th>Interoperability</th>
<th>Security</th>
<th>Questions</th>
<th>Additional</th>
</tr>
</thead>
<tbody>
<tr>
<td>MNO UICC</td>
<td>• FIPS 201 • FIPS 186 • Cert. Hierarchy Verification</td>
<td>If follows the standards, will it be compatible?</td>
<td>• LOA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>W.R.T. Mobile Security • ?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Credential + Mobile Security

Even the credential! Leave no stone unturned

<table>
<thead>
<tr>
<th>Standards</th>
<th>Interoperability</th>
<th>Security</th>
<th>Questions</th>
<th>Additional</th>
</tr>
</thead>
<tbody>
<tr>
<td>• FIPS 201</td>
<td>If follows the standards, will it be compatible?</td>
<td>• LOA</td>
<td></td>
<td>• Physical prop’s (10373, 7816)</td>
</tr>
<tr>
<td>• CRL</td>
<td></td>
<td></td>
<td></td>
<td>• Integrated Circuit prop’s</td>
</tr>
<tr>
<td>• Certificate hierarchy verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• X.509</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Credentialed Token

<table>
<thead>
<tr>
<th>Location</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>CAC, PIV</td>
</tr>
<tr>
<td>Removable</td>
<td>UICC, μSD</td>
</tr>
<tr>
<td>Internal</td>
<td>Embedded SE, Virtual SE</td>
</tr>
</tbody>
</table>

Interface

<table>
<thead>
<tr>
<th>Type</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>CAC sled</td>
</tr>
<tr>
<td>Contactless</td>
<td>NFC, Bluetooth, LTE</td>
</tr>
<tr>
<td>Interface Policy</td>
<td>Insert-remove, tap, maintained proximity</td>
</tr>
</tbody>
</table>

- Physical durability
- Compatibility
- Security
Security of the Mobile Device
Security of Mobile Device

Mobile device must also be considered as an element
- Durable?
- Compatible?
- Secure?

Interface

Credentials

External
- Contactless
- Contact
Removable
- Secure
- Secure Channel
Internal

CA

Secure Channel

RP
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
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

Sender:  
Message \(\xrightarrow{\text{Symmetric Encrypt}}\) Encrypted Message

NO TLS channel

Receiver:  
Encrypted Message \(\xrightarrow{\text{Symmetric Decrypt}}\) Decrypted Message

Architecture for *Extreme security*; includes all elements

Sender:  
Message  
Digest \(\xrightarrow{\text{PKI Encrypt}}\) Encrypted Message

Encrypted Message \(\xrightarrow{\text{PKI Encrypt}}\) Encrypted Digest

TLS Channel

Receiver:  
Encrypted Message \(\xrightarrow{\text{PKI Decrypt}}\) Decrypted Message

Encrypted Digest \(\xrightarrow{\text{PKI Decrypt}}\) Decrypted Digest

TLS Channel

Digest

Decrypted Message
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

Recently adopted by Visa/Mastercard for NFC-payments

Recently adopted by Visa/Mastercard for NFC-payments

Recently adopted by Visa/Mastercard for NFC-payments

Recently adopted by Visa/Mastercard for NFC-payments

Recently adopted by Visa/Mastercard for NFC-payments
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
# Summary of Approval Procedure Scope

<table>
<thead>
<tr>
<th>Local credentialed token</th>
<th>Interface</th>
<th>Secure mobile device</th>
<th>Secure communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Testing/Verification Required**

---

**Local credentialed token**

- External
  - ID card
  - NFC

- Removable
  - SIM card
  - SD card

- Internal
  - Hardwired
  - Secure Element/Cryptographics
  - Air-Gapped

**Interface**

- Trusted User Interface
- Secure Execution Environment
- Secure Communications

**Secure mobile device**

- Secure mobile device

**Secure communications**

- CA
- RP

---

34
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.

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