Mobile Derived Credentials for Assured Identity within DoD

Dr. Sarbari Gupta

President and CEO, Electrosoft

Pentagon Forum

October 19, 2016

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
FAX: (703) 437-9452

Agenda

- DoD Vision for Assured Identity
- Security Concerns and Mitigations for Mobile Computing
- Derived PIV Credentials for “Assured Identity”
- Wrap-Up

DoD Vision for Assured Identity (I)

- **DoD has issued over 2.8M Common Access Cards (CACs) since 2001; however, the CAC:**
  - ***Is not practical in tactical/constrained environments***
  - ***Is cumbersome to use with mobile devices***
  - ***Does not enable secure interoperability with mission partners***

- **FedForum 2016 (Jun'16) - DoD CIO Terry Halvorsen stated:**
  - ***CAC lacks agility; will be phased out over next 2 years***
  - ***CAC will not be used for access to information systems***
  - ***Continue PKI and Multi-factor authentication using***
    - **Biometrics**
    - **Behavior-based techniques**
    - **Personal data**

DoD Vision for Assured Identity (II)

- **Aug 2016 – DoD IT & Cybersecurity Roadmap released**
  - ***2-year plan to eliminate CAC from DoD information systems***
  - ***Deploy authentication infrastructure to dynamically control authorized user access***
  - ***Integrate commercial mobile IT capabilities***

- **April 2016 – DOD Mobility Strategy - Kim Rice, PM, Mobility PMO**
  - ***Enable Personnel to securely work in any location, over any device across any network***
  - ***Allow use of Various Devices (laptop, smartphone, tablet …)***
  - ***Promote availability of applications developed specifically for small, wireless computing devices***

Security Challenges with Mobile Devices

- **Small form factor makes it easy to lose, misplace**
- **Device passwords seldom enabled**
- **Multiple channels of attack and access**
  - ***Poorly secured communication channels (e.g. WiFi)***
- **Complexity and proprietary nature of Mobile OS**
  - ***Multiplicity of Mobile OS versions in the field***
  - ***Patches and updates implemented sporadically***
- **Plethora of mobile apps**
  - ***Ease of quick download and use of malware***
  - ***Difficulty of source verification and integrity checks***
- **Ease of unauthorized OS modification (e.g. "jailbreak")**

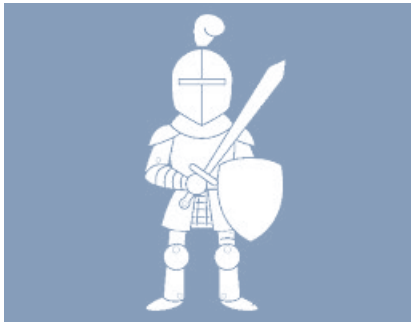
*** Reference: 2012 GAO Report "Better Implementation of Controls for Mobile Devices Should Be Encouraged"**

Mobile Device Attack Paths

- Attacker gains physical control of device
- User visits malicious website
- User download Apps from web (other than from reputable source)
- Attacker eavesdrops on unencrypted communications from device

Securing Mobile Devices – User Controls

- Maintain physical control of device
- Enable user authentication to device
- Use 2-factor to protect sensitive transactions
- Limit use of insecure communication channels
- Download Apps from reputable sources only
- Install security software – firewall, anti-malware
- Install security updates promptly
- Enable remote wipe of data



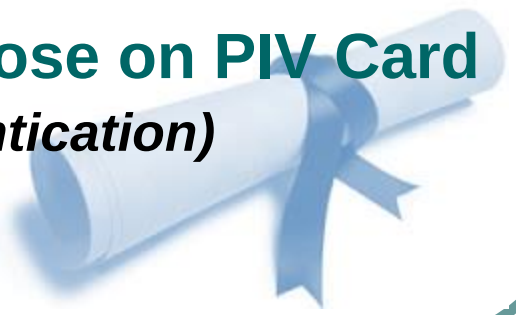
*** Reference: 2012 GAO Report "Better Implementation of Controls for Mobile Devices Should Be Encouraged"**

Securing Mobile Devices - Agency Controls

- **Establish / Implement Mobile Device Security Program**
  - ***Security Policy***
  - ***User Training***
  - ***Deployment Plan***
- **Implement layered security for mobile device**
  - ***Authentication to device***
  - ***Cryptographic protection of data and transactions***
  - ***User training and awareness of security risks***
- **Implement Mobile Device Management (MDM) solution – Server and Client App(s)**
  - ***Run in the background***
  - ***Run in "sandboxed" environment***
  - ***Manage the security configuration of device***
  - ***Implement 2-factor techniques***
  - ***Encrypt stored data***

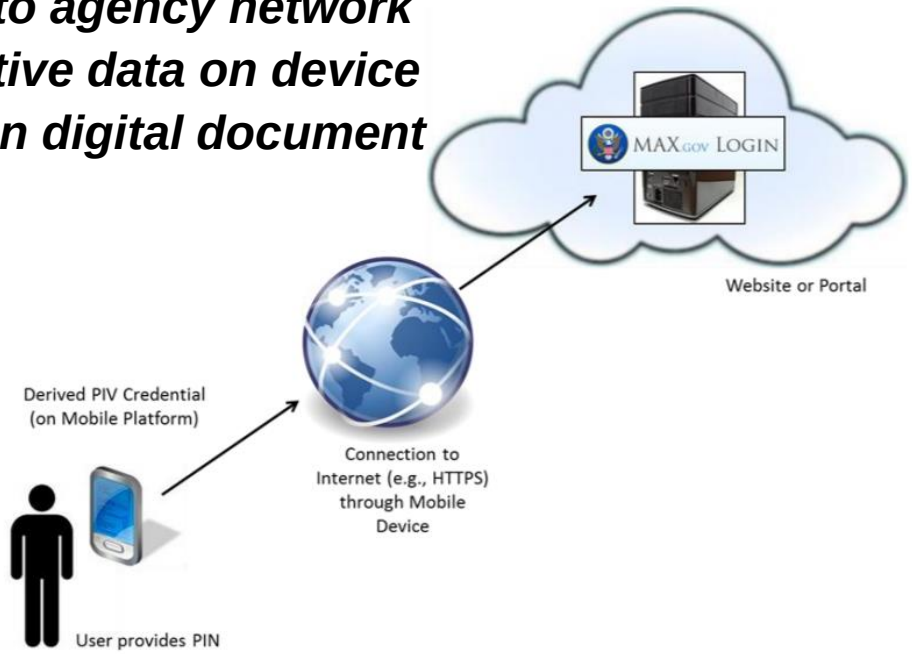
What are Derived PIV Credentials?

- **Specified in NIST Special Publication 800-157**
  - ***Final version published December 2014***
- **A security token, implemented and deployed directly on a mobile device (such as smart phone or tablet)**
- **Issued to holder of a valid PIV Card**
  - ***Trust derived from authenticated possession of PIV Card***
  - ***Identity proofing and vetting not necessary***
- **Set of PKI credentials similar to those on PIV Card**
  - ***PIV Authentication (for identity authentication)***
  - ***PIV Signature (for digital signature)***
  - ***PIV Key Management (for encryption)***



How are Derived Credentials Used?

- **With secure Apps <u>on</u> mobile device**
  - ***Secure Browsing with 2-factor authentication***
  - ***Secure email send and receive (encrypt/sign)***
  - ***IPSEC-based VPN tunnels to agency network***
  - ***Strong encryption of sensitive data on device***
  - ***Sign and verify signature on digital document***



- **Currently, not for use with separate platform (e.g., laptop)**
  - ***Contactless connection to platform not supported***

Derived PIV Credential Implementation

- **Where Derived Credentials are stored/used in Mobile Device:**
  - ***Removable (non-embedded) Hardware Crypto Token (LOA-4)***
    - **Secure Digital (SD) Card**
    - **Universal Integrated Circuit Card (UICC)**
    - **Universal Serial Bus (USB) Token**
  - ***Embedded Crypto Token***
    - **Hardware implementation (LOA-4)**
    - **Software Implementation (LOA-3)**
- **Who can issue**
  - ***Any Agency that issues PIV Card***
  - ***Other Agency***

Derived PIV Credentials - Life Cycle (I)

- **Initial Issuance**
  - ***Subscriber proves possession/control of valid PIV card***
  - ***Issuer checks that PIV Card is not revoked***
  - ***Derived PIV credentials issued to mobile device***
    - **LOA-3 – may be issued through remote session(s)**
    - **LOA-4 – must be issued in person; biometric authentication reqd.**
  - ***Multiple Derived Credentials may be issued to same PIV Cardholder***

- **Derived Credential Maintenance (Rekey, Revoke, Reissue)**
  - ***Can be done remotely or in-person***
  - ***Derived PIV credentials usable even if PIV Card is lost / revoked***

Derived PIV Credentials - Life Cycle (II)

- **Termination**
  - ***When Derived PIV credentials no longer needed***
  - ***When PIV Card is terminated***
- **Linkage with PIV Card to be maintained**
  - ***Active and periodic checks with PIV Card Issuer for termination/change***
  - ***Linkage updated when Subscriber gets new PIV Card***

Assured Identity with Derived Credentials

- **Enables initialization of mobile devices for secure use by Federal mobile worker**
  - ***Agency-issued device***
  - ***Personal device (BYOD)***

- **Challenges**
  - ***Policy with regard to Derived Credential Issuance/Mgmt***
  - ***Secure Remote enrollment and provisioning***
  - ***Maintaining active link to underlying PIV Card***
    - **Update/Terminate in lock step with PIV Card**
  - ***Use in contactless environments (laptop, physical access point)***
  - ***Use with Mobile Device native apps***

Wrap-Up

- **Summary**
  - ***Secure Mobile computing a core part of future DoD IT***
  - ***Mobile security challenges need to be addressed***
  - ***Derived Credentials offer strong foundation for assured identity***
  - ***Multiple use cases to leverage Derived Credentials***

- **Questions / Comments ?**

Contact & Company Information

- **Contact Info: Dr. Sarbari Gupta – Electrosoft**
  - ***Email: sarbari@electrosoft-inc.com; Phone: 703-437-9451 ext 12***
  - ***LinkedIn: http://www.linkedin.com/profile/view?id=8759633***
- **About Electrosoft**
  - ***We deliver a diversified set of technology-based solutions and services with a deep focus on cybersecurity***
  - ***We co-authored over a dozen NIST security publications!***
  - ***Major Customers: DoD, GSA, Treasury, VA, DHS***
  - ***Founded in 2001; Headquartered in Reston, Virginia***
  - ***Socio-economic Certifications: 8(a), SDB, EDWOSB***
  - ***ISO 9001:2008 registered; CMMI Level 2 assessed***
  - ***Website: http://www.electrosoft-inc.com***
- **What Makes Us Different?**
  - ***Cybersecurity is in our DNA! –*** *We inject a cybersecurity risk management/compliance dimension to every effort we undertake*
  - ***Our Core Values guide our every action!*** *– Our six core values of Integrity, Customer Service, Excellence, Teamwork, Accountability and Respect are evident through our attitude and our work*