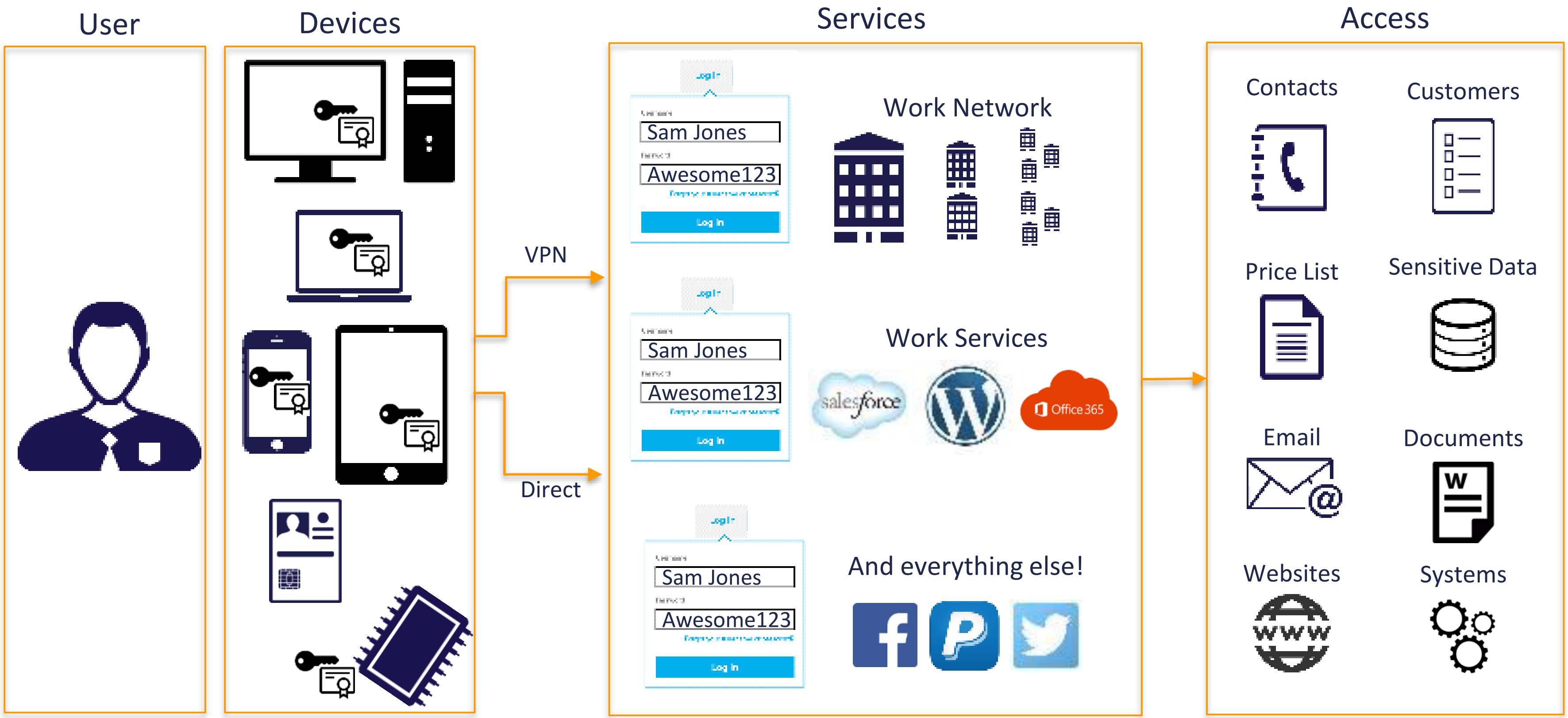
ATARC Mobile Identity Management
Encouraging Use of Derived PIV

David Coley
Sr. Solutions Architect, Intercede
david.coley@intercede.com

intercede

Intercede Enables Strong Authentication

CMS Platform for Credential Issuance & Management



ATARC Mobile Identity Management

Advanced Technology Academic Research Center

- Forum for Industry and Government Collaboration
- Focused on Mobile and Cloud
- Contact Tim Harvey – tharvey@atarc.org – for more information.
- www.atarc.org

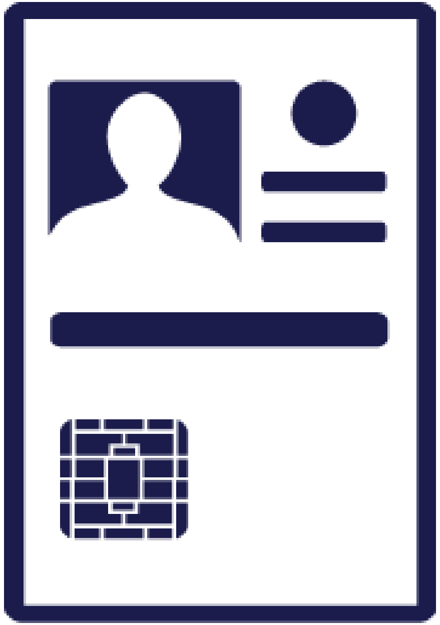
Mobile Identity Management Project Team

- Part of the ATARC Mobile Working Group & Aligned with the Mobile Services Category Team
- Primary Objective is Advancing Use of Derived PIV
- Active participants from multiple corporate partners as well as a half dozen (and growing) agencies and departments from the U.S. Government. Includes NIST and MITRE participation.

intercede

Setting the Stage – PIV (CAC) and Derived Credentials

- Inconsistent Proofing was Considered
  - A Risk for Unauthorized Access
  - An Opening For Terrorism
- Homeland Security Presidential Directive #12, under President George W. Bush was issued on August 27, 2004
  - Directed Secretary of Commerce to Develop New Standard
- NIST (an arm of the Department of Commerce)
  - Developed FIPS-201 as the new standard for identity proofing.
  - Personal Identity Verification (PIV) card was born as the physical implementation of FIPS 201



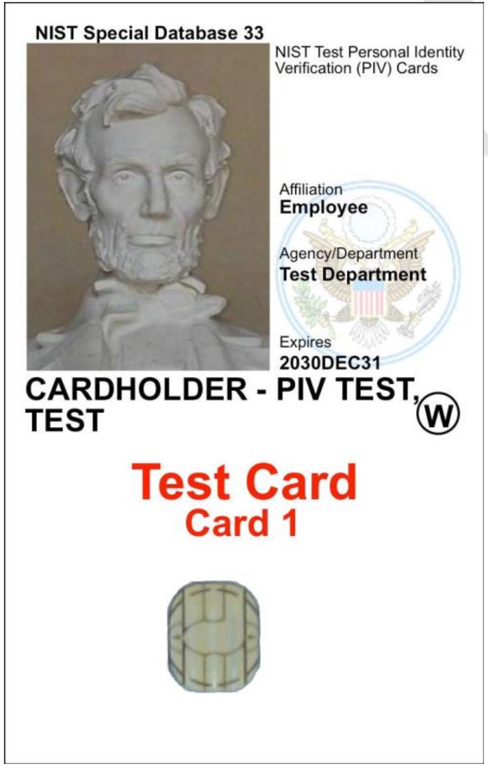
PIV, PIV-I, CIV – Alphabet Soup

- **Personal Identity Verification (PIV**)
  - Accepted by U.S. Government
  - Must follow FIPS 201 standard for identity proofing, documentation, National Agency Check, including biometrics.
  - Specific roles involved in issuance.
- **PIV Interoperable (PIV-I)**
  - Accepted by U. S. Government
  - Must follow FIPS 201 Standard for PIV-I for identity proofing, documentation, and two fingerprints.
  - Specific roles involved in issuance.
- **Commercial Identity Verification (CIV)**
  - Not accepted by U.S. Government
  - No required steps for identity proofing, documentation, etc.
  - Offered as “best practice” framework for identity proofing and credential issuance.

Alphabet Soup: Learn more about PIV, PIV-I, and CIV at http://www.smartcardalliance.org/publications-a-comparison-of-piv-piv-i-and-civ-credentials/

PIV, PIV-I, CIV – Where You Might Find Them…

- PIV Cards
  - U. S. Government Only
- PIV-I Cards
  - Some Defense Contractors
  - First Responders (FRAC – First Responder Authentication Credential)
  - Some Civilian Contractors
- CIV Cards
  - Employees of Companies Contracting to Defense/Civilian Agencies (which do not interact with U.S. Government regularly).
  - Companies Seeking a Strong Physical and Logical Credential Program



NIST Special Database 33

NIST Test Personal Identity Verification (PIV) Cards

Affiliation
Employee

Agency/Department
Test Department

Expires
2030DEC31

**CARDHOLDER - PIV TEST,
TEST**

W

Test Card
Card 1

What’s On a PIV (CAC)?

Standardized Printing

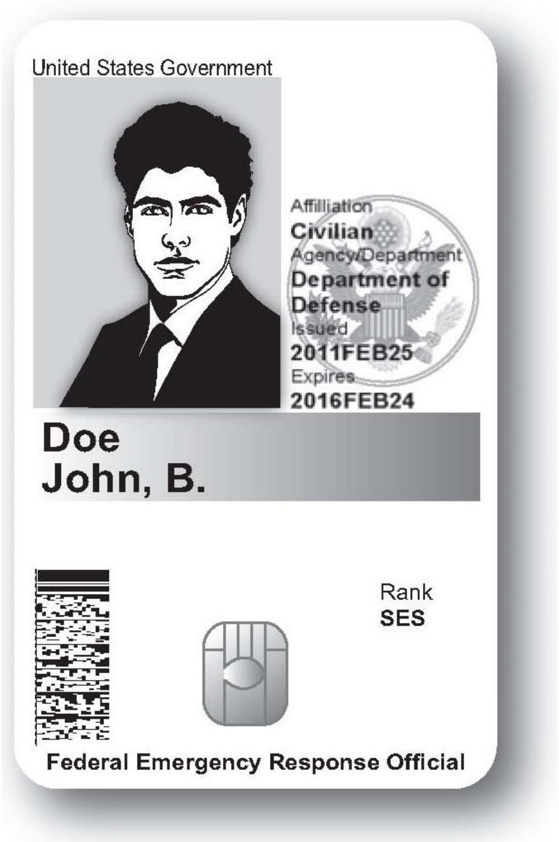
- Photo, Agency, Expiration, etc.

Digital Identity for LACS/PACS

- Unique Card Identifier
- Image of Cardholder
- Fingerprint of Cardholder
- Authentication Certificate
- One or More Encryption Certificates

CAC/PIV is a Level of Assurance 4 (LOA 4) Identity

- Or AAL 3 if you prefer (NIST SP 800-63B)



So You’ve Got a CAC/PIV – Now What?

Physical Access Control System (PACS)

- At its most basic simply showing a CAC/PIV to a guard.
- Swipe badge reader at front entrance.
- Access control to offices within a building.
- Access control for more granular access to specific conference rooms, satellite offices, etc.

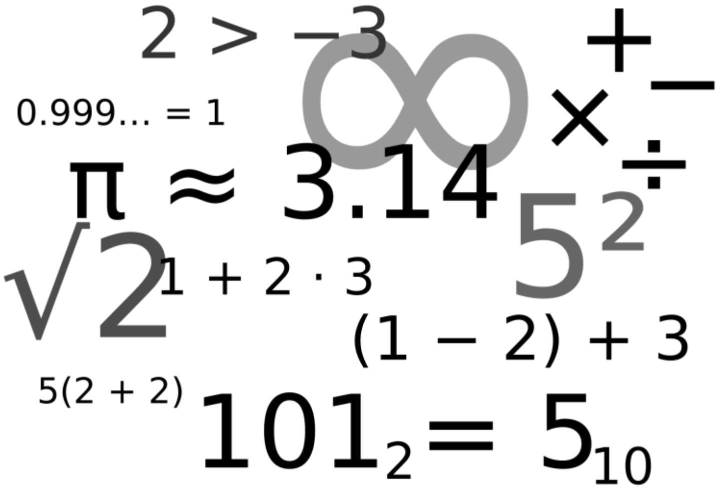
Logical Access Control System (LACS)

- Windows Logon!
- VPN
- Document Signing
- Email Encryption
- Application Authentication

intercede

Enter Derived PIV (or CAC)

- Outlined in NIST SP 800-157 – Guidelines for Derived Personal Identity Verification (PIV) Credentials
- For use where a PIV (CAC) form factor doesn’t work well. The most obvious is a mobile device. Also… infectious disease labs, users with disabilities.
- Derived PIV credentials are not mathematically related to the originating PIV in any way!
- Issuance Requirements for Derived PIV
  - Present valid CAC/PIV
  - Prove Possession by Providing PIN
  - Biometric Match for LOA4 (AAL3)
  - System Must Link DPC to CAC/PIV and Monitor Foundation Credential for Revocation
  - Issue to FIPS 140-2 Level 1 Software Keystore (LOA3/AAL2) or FIPS 140-2 Level 2 (Level 3 Physical Security) Hardware Keystore



Mobile Identity Management Project Team

What We’ve Learned

It’s Early Days for Derived PIV

Significant difference agency to agency*.

- Most Agencies Thinking About DPC – Probably a more accurate graphic would be blueprints.
- Some Agencies Deploying Limited Pilots
- Most are trying to think about the end goal (actually using the DPC once issued).

*Department of Defense

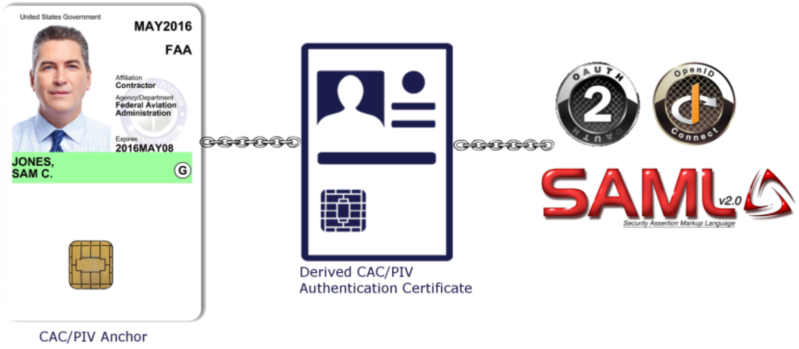
- DoD is actually pretty far along the path of DPC.
- They’ve been issuing mobile credentials for years and developed Purebred as a GOTS solution to meet their needs. This is a relatively large pilot at this point.

Great, I Can Issue DPC. Now What?

The biggest overall question is what’s next. After taking the time and effort to issue a DPC what do we do with the thing?

- This was the primary focus for the team!

- No need to PK enable all your apps!
- Deploy an IdP that is PK enabled.
- Strong, Certificate Based Authentication to IdP Followed by SAML, OAuth, OpenID Connect, Kerberos



Keystores and Keychains

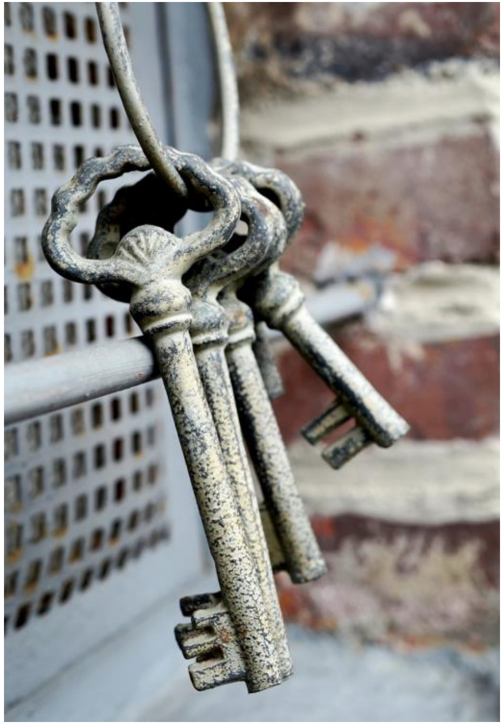
The Good, The Bad & The Ugly

Windows and BlackBerry are Easy (relatively)

- Both platforms provide relatively easy access to key material so that the apps that need access can have it.
- Protections are enforced as needed for local authentication (pin, biometrics, etc).

… And then there was iOS and Android…

- In theory they offer enhanced security by sandboxing apps to limit what they can see. Problem is this also impacts availability of keys.
- Which apps does your agency require? Safari, native mail client, native 1st party apps? Custom apps? Apps deployed in an MDM/EMM container? Does the use case demand LOA4 (AAL4)?
- The apps required drive storage locations for keys. Not the other way around. Its usually more a question of acceptable risk vs a choice on keystore/keychain options.



Enabling use of DPC on iOS and Android

- Agencies must think, in advance, about which apps they want to use and the nuances of various key stores.
- Use of Safari, Native Browsers, other 1st party apps demands keys in the system keystore/keychain. On iOS this means any 1st party app has access with no pin prompt after the device is unlocked. Andoid system keystore means any app has access with no pin prompt after device is unlocked.
- Storage in an app specific keystore/keychain offers high security (limited visibility of keys and obvious user intent enforced by PIN or biometrics prompt). However, it also features limited visibility of keys by other apps so more work may be required to issue keys all around.

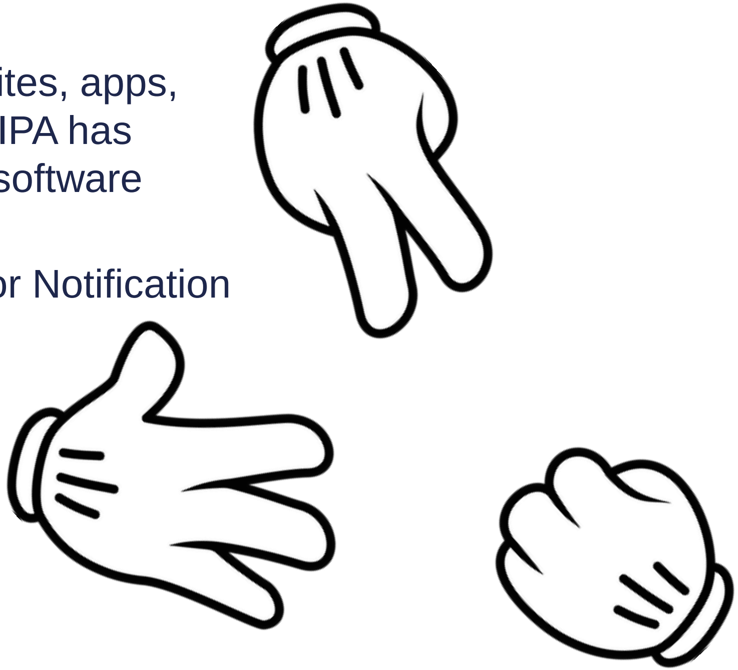
- Don’t forget about lifecycle management… Revocation, Deletion, Renewal

intercede

Misc…

Some Other Concerns

- Integration with MDM/EMM Solutions to automate issuance, ensure issuance to enterprise managed devices, and remotely delete (to offset enterprise delays in revocation).
- Lack of OID Awareness – Many relying parties (websites, apps, etc) do not check OIDs in presented certificates. FPKIPA has outlined specific OIDs for hardware (LOA4/AAL3) vs software (LOA3/AAL2)
- Availability of Interfaces for PIV/CAC Status Checks or Notification by CAC/PIV CMS to DPC CMS.



Next Steps…

The team has released its initial working document. Not final as we seek to incorporate comments from industry and government.

Please contact me for this paper (david.coley@intercede.com).

Making it Real

- 1-2 Page Business Case Paper – Why business owners should care.
- Mapping selected agency use cases to FICAM use cases to see how well the rubber meets the road.
- Cookbook Development – Taking the ideas from the working paper and getting more granular on how to apply them in the real world.

Thank you!

David Coley
david.coley@intercede.com

intercede