Daon your trusted Identity Partner

Derived Credentials – A Use Case

Cathy Tilton
Daon

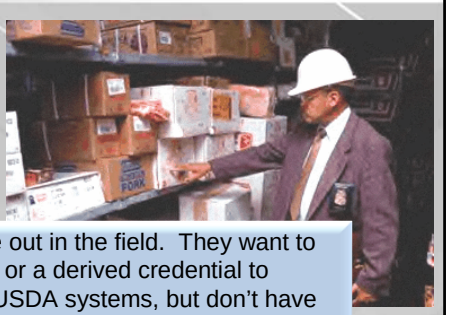
1 February 2012

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD
Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

Derived credentials

- NIST SP 800-63-1 (§5.3.5) provides for 'long term derived credentials'
  - Derived credential can satisfy UP TO the level of the original credential (assuming other provisions of SP 800-63-1 are met for that level)
  - Verification of the original credential satisfies identity proofing requirements.
  - For Level 4, binding must be done in person + biometric validation required.
  - Revocation status(es) may be optionally tightly bound.

Use Case - USDA



USDA has many people out in the field. They want to use the HSPD-12 cards or a derived credential to authenticate access to USDA systems, but don't have an infrastructure in place to read the cards or fingerprints. These people are mobile (inspectors, etc.), and they would like to extend their systems to the field via mobile devices. They need a solution that doesn't require an investment in infrastructure, that would provide LOA3 access.

Use Case - DoD

A member of the forces registers his mobile phone as a credential derived from his CAC card. The phone cannot be used to access any LoA4 or higher services, but while in the field, the member of the forces can get access to critical logistical information that ensures that his operation runs smoothly, even when he is removed from land-based internet access. In addition, there is an application that runs right on his smart phone to access this logistical information - he can access this application and authenticate using his smart phone using only the widely-available cellular telephone data connections

A DOD employee is in the field in a foreign location and needs to validate the folks they are dealing with are folks they are authorized to conduct business with. Using their portable device and the derived credential from their PIV, they call to validate the terms of the transaction and the authorized recipient of the goods or services.

Use Case - CMS

A CMS employee with a PIV card realizes that they will be travelling for the next two weeks with no access to dedicated workstations with PIV card readers. She will need access to patient record maintenance services at CMS that require some form of LoA 3 authentication. She will have her mobile phone with her, as well as access to internet cafes. She enrolls her smartphone as a derived credential for authentication purposes whenever she accesses the patient record maintenance services.

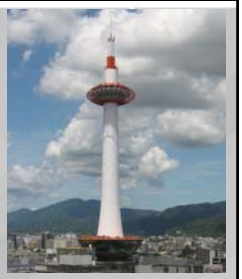
Use Case - CMS

Although not required, she notifies CMS in advance that she will be using the derived credential, so that their centralized Identity Management system can flow down the information to the business unit in CMS responsible for the patient record maintenance service - this action automatically registers the derived credential for use as the primary authentication mechanism during the request period, for access to services requiring LoA3 or below authentication.

Use Case - CBP

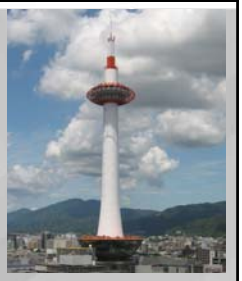
A CBP employee is in the field near the border and needs to call up an application to deal with a person suspected of trying to enter the country illegally. Using their smartphone based derived credential as an alternative, but tied to their PIV, they access the app on their portable device to obtain and enter information and deal with the individual.

Use Case - GSA



GSA has plans to create an MVNO (Mobile Virtual Network Operator), where a contractor (or set of contractors) creates a virtual mobile network from all the carriers' mobile network offerings. This MVNO would address requirements around government only access, and on-campus only access to the network and internal government systems. They want to derive a credential that uses the mobile device as an authentication device based on the employee's/contractor's PIV card to access the network and even to authenticate to systems and physical gates and doors for access.

Use Case - GSA



How this would work – The user:
1)Authenticates to the campus (MVNO) network before entering the building via their smartphone based derived credential;
- This sets a short-time-use code on the NFC chip on the phone;
2)Approaches the door and/or gate and swipes the phone to gain physical access;
3)Once inside the building, requests access to a system (usually using SSO);
- The system requests authentication using the same derived credential and, upon successful authentication, allows them access to the system.

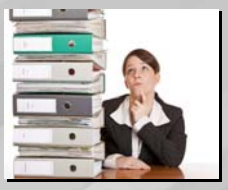
Identity Management Challenges

Security

- Protecting data at rest and in transit
- Users managing multiple identities and passwords
- Termination of entitlements
- Inconsistent policy enforcement

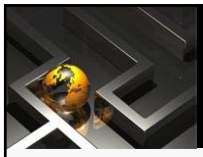
Compliance management

- E-Gov Act 2002, HSPD-12, FISMA, FIPS 201, HIPAA, PHI, CFATS, NERC CIP, EU DPD, JPIPL, etc.
- Knowing who has access to what, proving it, enforcing it, and monitoring it
- Segregation of duties to prevent abuses
- Creating and managing internal and external user identities



Business enablement

- Need for access to information by external users
- Interoperability with agencies, partners, and citizens
- Streamlined user experience and enhanced productivity

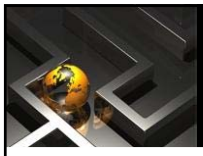


The Future of Identity & Digital Interaction

We are at the pivotal intersection of two fundamental & global paradigm shifts

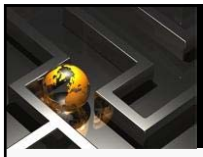
1. The move to **digital interactions**
   - Has been occurring since the web went mainstream
   - Social networking leading to greater online presence
   - Identity fraud rates are high and growing
   - Current methods (PINs/Passphrase based) are woefully inadequate, alternatives are extremely expensive
2. The emerging **ubiquity of connected mobile computing devices** (e.g. smart phones)
   - Massive consumer adoption
   - Always connected, managed computing platform in your hands at all times
   - Greater utility beyond handset

Universal Identity Trust!

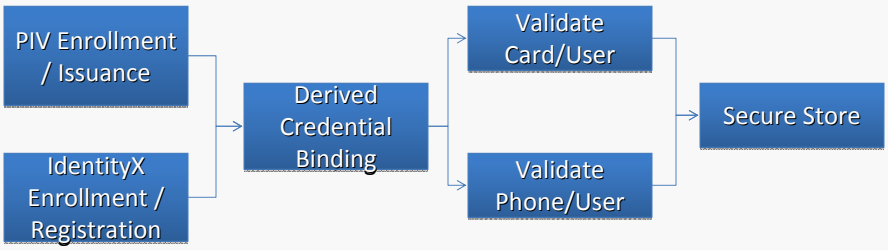


For purpose of discussion only …

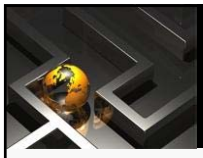
- Assume the following derived credential: Identity X is …
- A unique risk-based, multi-factor authentication capability that leverages latest generation smart phones (e.g., iPhone, Blackberry, Android), smart tablets (e.g., iPhone/Playbook) and traditional mobile devices
- Identity X technology combines multiple authentication techniques for greatest identity confidence:
  - Device (What you have)
  - PKI Certificate (What you have)
  - PIN (What you know)
  - Face (Who you are)
  - Voice (Who you are)
  - Palm (Who you are)
  - GPS (Where you are)
  - (other as devices become enabled)
- Placing biometric levels of identity assurance in the hands of consumers



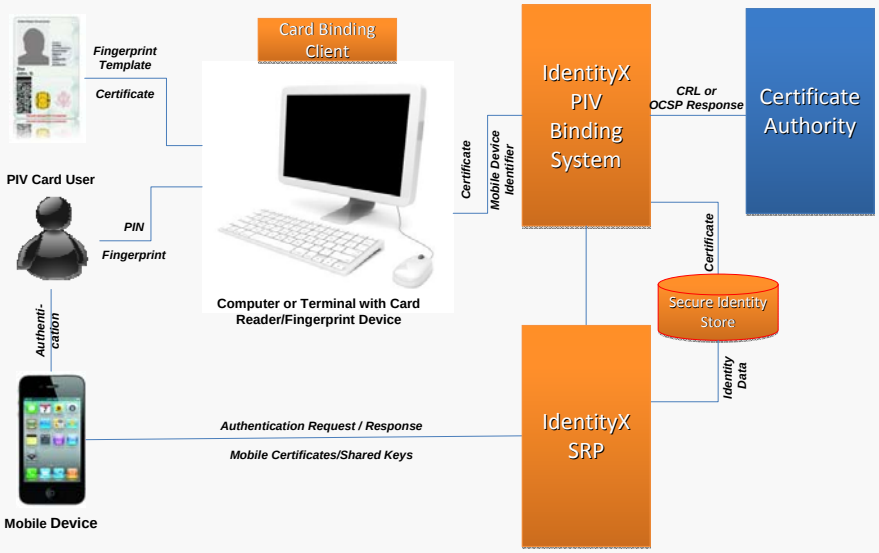
Registration process

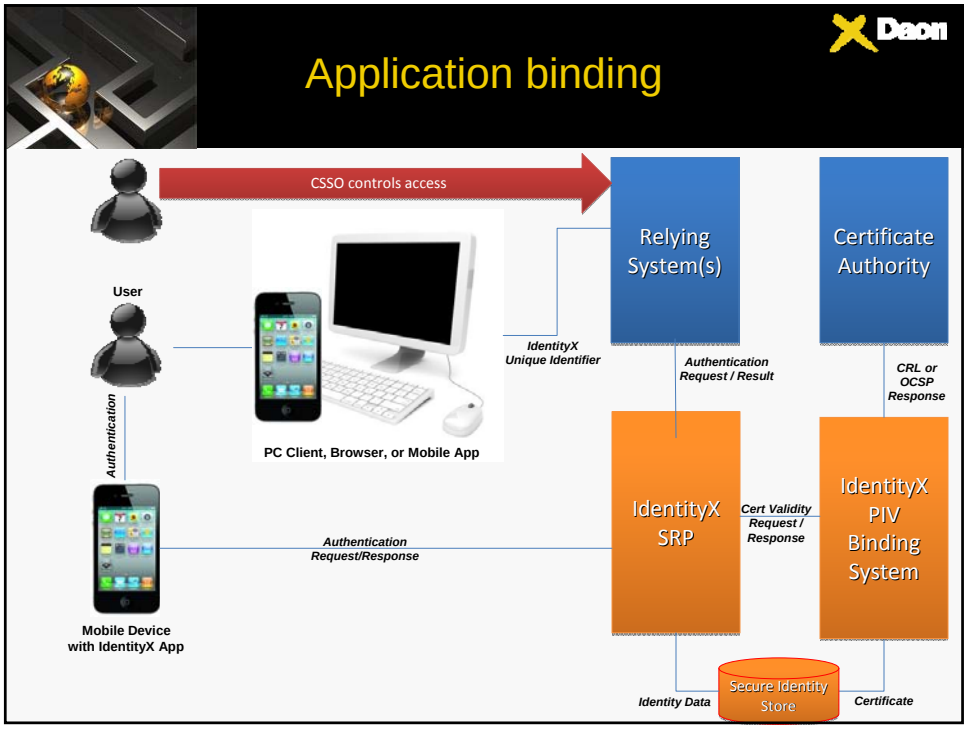


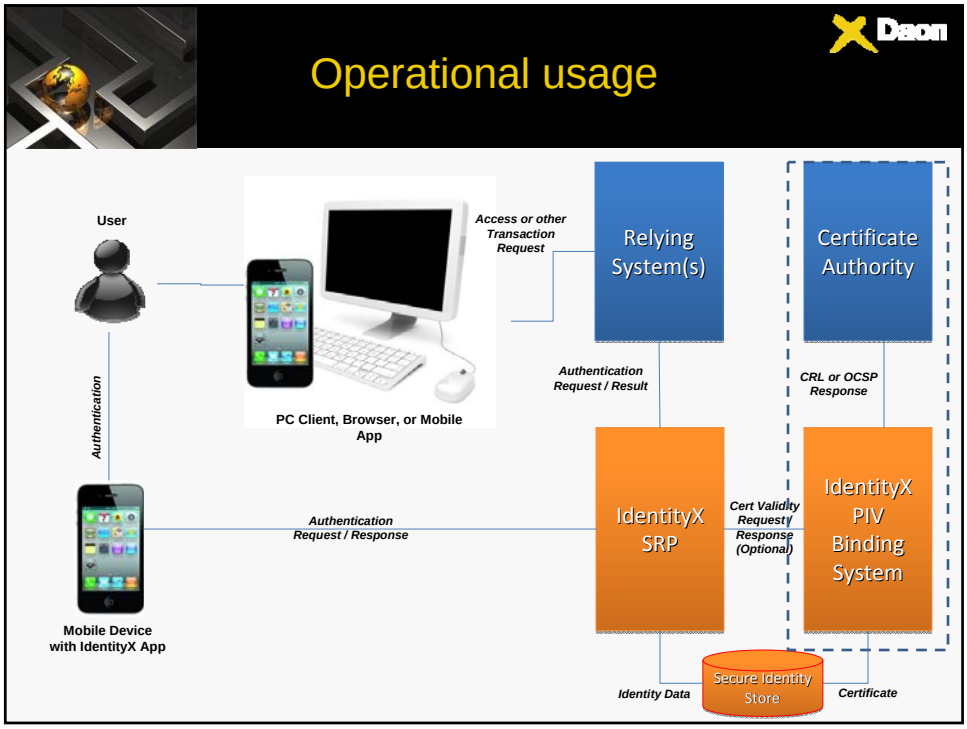
Notes:
1) Assumes user has already enrolled in IdentityX; however, such enrollment could also occur at time of binding.
2) Binding may be performed online or in-person (attended).



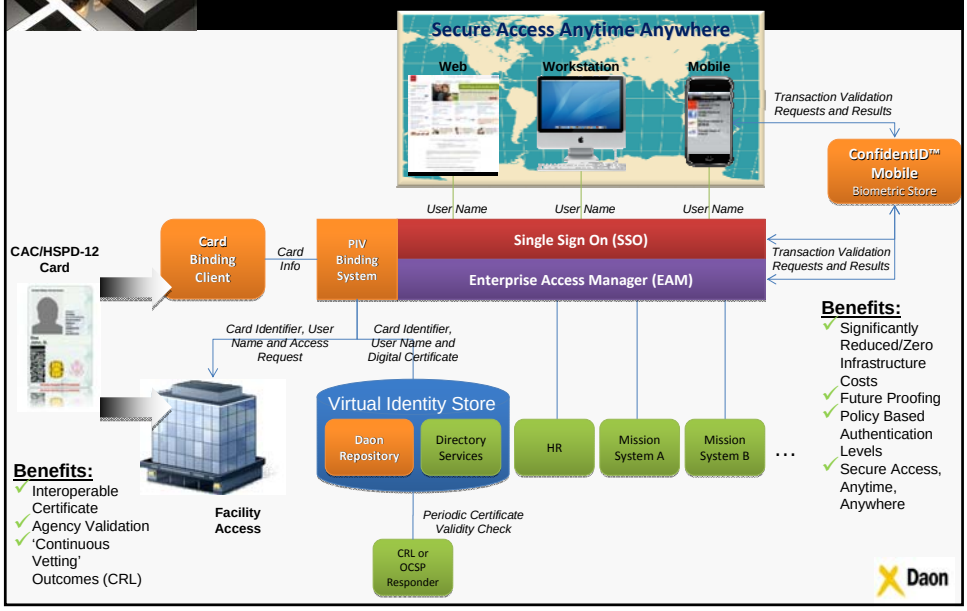
Derived credential binding




Application binding
CSSO controls access
Relying System(s)
Certificate Authority
User
IdentityX Unique Identifier
Authentication Request / Result
CRL or OCSP Response
Authentication
PC Client, Browser, or Mobile App
IdentityX SRP
Cert Validity Request / Response
IdentityX PIV Binding System
Authentication Request/Response
Mobile Device with IdentityX App
Identity Data
Secure Identity Store
Certificate


Operational usage
User
Access or other Transaction Request
Relying System(s)
Certificate Authority
Authentication Request / Result
CRL or OCSP Response
Authentication
PC Client, Browser, or Mobile App
IdentityX SRP
Cert Validity Request / Response (Optional)
IdentityX PIV Binding System
Authentication Request / Response
Mobile Device with IdentityX App
Identity Data
Secure Identity Store
Certificate

Configuration

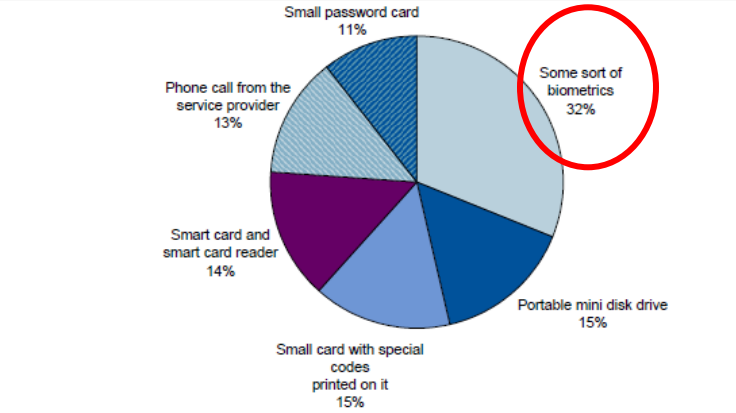


The Key Challenge: Bridging the Gap between Security and Convenience

Trust, Security, Customer Service

User preferences are important

- Biometrics is the most preferred additional form of authentication for US online banking users

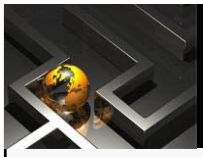


Source: Gartner (June 2008)

The role of risk assessment

- Not every problem is a Level 4 problem

Level	Confidence in Asserted Identity's Validity
1	Little or none
2	Some
3	High
4	Very High



Thanks!

Contact Info:
Catherine Tilton
VP, Stds & Tech, Daon
11955 Freedom Dr, Suite 16000
Reston, VA 20190
703-984-4080
cathy.tilton@daon.com