Identity / Credentialing Programs

Creating an Interoperable Framework
A General Discussion

Screening Coordination Office
May 5, 2009
DHS Daily Screening Opportunities

- Process 1.2 million inbound travelers at POEs - 630,000 aliens
- Screen 1.8 million domestic air travelers
- Conduct 135,000 biometric checks for visa applicants and border crossing
- Process 30,000 immigration benefit applications
- Verify the employment status of 3.2 million new employees
- Manage Trusted Traveler Programs
- Design and execute background checks for critical infrastructure workers
Goal: Enable Benefits of FIPS-201 Interoperability

Identity Assurance by Multiple Users where presented
- Standard provides level of trust and assurance that can be validated across use cases.
- Provides greater assurance that a person is who he/she claims to be.
- Makes it more difficult to tamper with or counterfeit an identity document.
- Distinguishes secure identification from other documents issued according to lesser standards.

Use for Physical Access
- Allows layered protection for buildings/multi-use buildings, complexes, secure areas, etc.
- Provides interoperability among credentials for identity validation/verification – can be used for visitor/varied access privileges.
- Allows the agency to focus its security force at most critical access points.

Use for Logical Access
- Computers/laptops
- Cyber-security benefits
- Single Sign On
- Interoperability

Automates attribute/privilege granting and management for multiple purposes

Provides levels of assurance that can apply to different use cases

Technology & Process best practices for: Registration/Enrollment; Eligibility/Vetting & Risk Assessment; Issuance; Verification/Use; and Revocation
Credentialing Ongoing Activities

- Encourage DHS credentialing programs to interoperate both technologically, but also use common standard policies based on FIPS 201, the PKI Federal Bridge and E-Authentication levels.
- Actively support existing program to take next steps to improve future interoperability / modernization.
  - e.g. - Change TWIC PIV Card Authentication Certificate
- Encourage system owners to fully implement the CFI to reuse critical IdM system components and provide synergies across programs.

| Assurance Level Based on Risk and Consequence: Inconvenience, distress, or damage to standing/reputation; Financial loss or agency liability; Harm to agency programs or public interests; Unauthorized release of sensitive information; Personal safety; Civil or criminal violations. | Examples |
|---|---|---|---|---|
| FIPS 201 & FIPS 201 Interoperable Credentials | Federal Government Credentials | State Credentials | Private Sector Credentials |
| Level 4 - Highest Assurance Level: Very high confidence in asserted identity, transactions needing very high confidence in the asserted identity's accuracy. Users may present Level 4 credentials to assert identity and gain access to highly restricted web resources, without the need for further identity assertion controls. | DHS PIV and Federal Agency HSPD-12 cards, DoD CAC |  |
| Level 3 - High Assurance Level: High confidence in asserted identity. Transactions needing high confidence in the asserted identity's accuracy. Examples might include access restricted web services, account administration, composition sensitive documents. | First Responder Authorization Credential (FRAC) | Previously issued Federally ID FAST NEXUS SENTRI TWIC (Goal FIPS-201 interoperable) | Airport issued SIAD Badges/ Registered Traveler* (e.g. CLEAR) (Goal FIPS-201 interoperable) |
| Level 2 - Some Assurance: Some confidence in asserted identity: Wide range of business with the public where agencies require an initial identity assertion. For example updates to bank accounts, program eligibility, and payment information. | MMD / MMC* (Goal Level 3) | EDL, REAL ID State/Local ID | |
| Level 1 - Low Assurance: Little or no confidence in asserted identity. | Social Security cards | Non-REAL ID driver’s licenses Local Service Cards | Regional Emergency Access Card |

Adopt & Migrate Process Best Practices & Authentication Technology as Appropriate

Balance Commonality / Standardization with Use/Like Use; Risk; & Consequence: Registration/Enrollment; Eligibility/Vetting & Risk Assessment; Issuance; Redress; Verification/Use; and Revocation
Symptoms … from recent Clippings & Conferences

• General Operations – Fraud, Insider Threat
• CC Losses – 9.3% of $3.4T 07; Cards – $42B 08; up 33% 1st Q
  - Total estimated impact $110-15B 08;
  - $4.7K per person, 30 hrs, some never correct; 18-23% Loss
• Identity Breach – 280M individual records in 2008
• System Breach – JSF, $200M IP
• Medical Record Breach – Fraud, Drugs, Blackmail
• Medical Theft / Certainty - Contributor to fraud, complications, death rate
• Identity Assumptions – Spouse/Child Support; Evasion; Employability
• Incident Mgt – Delayed Response, Confusion, Resource Visibility & Use
• Systems Cost – Program Centric: builds, modernization, infrastructure costs
• Fraud, Counterfeit, & Improperly Issued State & Federally Issued Breeder Documents:
  - DMVs, Passports, Vital Health Records, SSN,
  - Organizationally issued Credentials

Certainty, Assurance, Trust ....
Trust – Untrustworthy -- 1. Firm reliance on the integrity, ability, or character of a person or thing, 2. Custody; care., 3. Something committed into the care of another; charge.

Certainty – Uncertainty -- 1. The fact, quality, or state of being certain: 2. a state of being free from doubt, 3. Something that is clearly established or assured Synonyms: certainty, certitude, assurance, conviction These nouns mean freedom from doubt. Certainty implies a thorough consideration of evidence: "the emphasis of a certainty that is not impaired by any shade of doubt" Mark Twain.

Assurance -- 1. The act of assuring, 2. A statement or indication that inspires confidence; a guarantee or pledge: gave her assurance that the plan would succeed, 3. Freedom from doubt; certainty: set sail in the assurance of favorable winds. See Synonyms at certainty.

Consistency -- 1. Possessing firmness or coherence 2. marked by harmony, regularity, or steady continuity : free from variation or contradiction, marked by agreement

Operations – 1. Performance of a practical work or of something involving the practical application of principles or processes 2: an exertion of power or influence 3: the quality or state of being functional or c: a method or manner of functioning
6 thoughts on Trust, Certainty ....

Policy – Trust of Non-Federally Issued Credentials
Standards & Guidance – Identity Proofing; “Levels” of Risk
Valuation – Real Benefits – “total” problem
Performance in Operational Environment
  - Economic impact, impact to business ops, maturity of technology
  - Operational Utility – efficiency, enhancements, multiplier
Certainty – Manufactures, Suppliers, Integrators, Informed Buyers
  - Consistency of Requirements; if not consistent – visibility
  - Consistency in Testing & Certifications
Funding – Clarifying Federal Grants Streams
Evolving Consensus toward Standards

- Growing problem of identity theft/fraud; cyber security.
- Push for enhanced public-private collaboration - similar risks, consequences, use cases; neither can address the problem independently.
- Desire for operational interoperability of credentials - Trust Levels, Risk, Assurance.
- DHS undertook its own effort to develop the Credentialing Framework Initiative consistent with the evolving global consensus.

Federal Identity & Assurance Standards FIPS-201 provides a common baseline

- Applies directly to Federal government and contractors
- Strict adherence to process and technical specification allows distributed networks/backend capabilities
- Framework and momentum for standardization
- Leverages Federal Investments and integrate with private sector planning and identity investments for open standards and specifications for more secure transactions

Private Sector – PIV-I -- Issued Today – WWW.CIO.Gov

- Based on FIPS-201, minimal elements
- Active collaboration; fierce competition on products and services
- Use cases and adoption evolving rapidly for access, privileges, transactions assurance

Federal Government Can Trust Non-Federally Issued Identity / Assurance Document & E-Tokens
Standards - Identity Proofing ....

ANSI – IDSP Workshop 1:
- Issuers of primary USA “identity” documents need a process by which they can achieve a level of assurance whether to accept or reject a person’s claim of identity
  - One or more practical methods to verify identity with very high confidence, high confidence, some confidence or low/no confidence
- Guidelines on identity verification developed with a view toward eventual development of an American National Standard

Development of guidelines in progress
- Phase 1 – Concept Formulation – 8 months
  - How to build certainty in a claimed identity
  - Criteria for the acceptance/rejection of a claim
  - Methods for the detection of fraud
- Phase 2 – Testing – 4 months
  - State vital record offices (birth certificate issuance)
  - State DMV’s (DL & ID card issuance)
  - Release of Guideline
- Phase 3 – Standardization – 8-12 months
  - ANSI/NASPO-IDV-2010 Methods for the Verification of Personal Identity

ANSI - Jim McCabe, 212-642-8921, jmccabe@ansi.org
NASPO - Graham Whitehead, 604-921-9196, gdw@naspo.info
Valuation –
With Consistency – How Do WE – consider the total problem

Valuation Model
Losses, Costs & Benefits

Current Costs models

Logical Assess MGT
Name & Password

System & Data integrity

Physical Access & Credentialing Valuation

Architecture
Cost Avoidance
Future Ops / Pgms

Meta Data Valuation

Network Availability Valuation
Cost & Benefits

Operational Efficiencies
Current Ops / Pgms

IP Losses

ID Theft & Breach

Other Loss Types
Performance in Operational Environment

Ongoing Attribute Research & Proof-of-Concepts
Authorization / ABAC / Privilege Management

Multiple Ongoing Efforts

- DoD and DHS User Attribute Exchange (DHS S&T, FEMA & DoD PFPA)
- DoD and DHS HSPD-12 BAE Implementation Proof-of-Concept (DHS S&T, DoD DMDC, and DHS OCIO)
- Privilege Management Pilot Phase 2 (DHS S&T, OCIO, FEMA; NORTHCOM, NSA, DISA and possibly HSIN next-gen)
- DHS and NIST Efforts Attribute Standard (DHS S&T, FEMA, SCO, & OCIO) - Define 154 ESF code schemas for use for emergency response officials - validation of utility for schemas; Testing attribute use case utility, Integration of schemas with NIEM
- FEMA/Interagency: Establishing guidance for how to assign a (F)ERO attribute to a federal employee or contractor, affecting all PIV card system attribute assignments
- TWIC Reader Pilots.

Related Program Dependencies:

- E-Integration/Authentication TSA TWIC (card) and USCG MMC (attributes)
- E-Integration/Authentication DHSPIV and FEMA Disaster Response Workforce
- E-Integration/Authentication HSPD-12 PIV and F/EROs / Resource Typing

Potential Use Case

- Acquisition Professional Community, National Security Professional Community
Certainty -- Supply & Buyers; Funding

Certainty – Manufactures, Suppliers, Integrators, Informed Buyers
- Consistency of Requirements; if not consistent – visibility
- Consistency in Testing & Certifications
- In Partnership – NIST, GSA, DHS:
  - Establishment of a *Conformity Assessment Program (CCAP)* and of the associated *Qualified Products List (QPL)* for Credentials and Credentials Authentication
  - Development of derived test requirements and, when applicable, associated test harnesses for conformity assessment to existing standards and technical specifications for smart card readers for TWIC, FRAC and ACIS/BASIC programs

Funding – Clarifying Federal Grants Streams
- Past – identity and support systems is a sub-element Identity
- Clarity Supporting Guidance
  - Secure Document, Credentials, & Systems
  - Clarify – Grants Allowability -- equipment, systems, services
Summary - Broad Picture Snap-Shot

Private Sector Standards
- Cross Certification of Non-Federal Entities to the Federal Bridge
- ANSI Standard for Common Identity Proofing – Draft Guideline presented in April. After a trial period, it will be finalized as the national proofing standard for user communities such as notaries, registrars, DMVs, birth certificate issuers.
- Liberty Alliance - Open Standards for secure transactions

Use Case / Communities – Activities & Pilots
- **Notaries** – Public Notaries are working toward identity and community certification standards for the documents they authenticate (direct linkage to I-9; enrollment submittals)
- Incident Management – Arlington Co, Pentagon Force Protection, FEMA Pilots (Since 2006)
- Financial Sector – Integrating “First” Communities (ChicagoFirst Model) with interoperable use cases for access and permissions; WellsFargo-“Wells1st” – pilots to financial/non-financial community trust transaction (financial/physical & logical access).
- Aviation Sector – Cross Certification of Aviation Community Service providers for the Implementation of ACIS as well as integration of services to Federal FIPS-201 card holders.
- Medical/Academic Community – GW University implemented and actively piloting with FEMA Credentialing efforts (since 2005).

Geographic Centers of Public-Private Efforts
- National Capital Region - Federal, State, Local sectors for Incident Mgt/COOP-COG.
- Greater-NYC - Transportation, Emergency Management Communities, Port Authority for multi-jurisdictional access control.
BACK UP SLIDES
Guidelines – Enhanced Assurance Understanding
Proofing, Binding, System Application, Flexability

Certainty of Identity

- Strength / Risk of Usage
- Identity Proofing Standard

Media & System to Binding the Identity

- Strength / Risk of Usage of Media (see system)

Strength / Risk of the Direct System & Applications

- Strength / Risk of System,
- Sensitivity of Data and Information

Strength / Risk of the Indirect Systems & Applications

- Secondary use of Credentials, common of accepted uses
- Exchanges within common communities
- Strength / Risk of data, information, and systems

Current Framework of “4 levels” need to be more comprehensively considered -- at all levels, examples of appropriate and in suboptimal/risky use cases for “self-asserted” to high
Moving into the future …

- Dive into DHS Vetting Processes & Systems
- Support the Person Centric View in screening activities
- Create data inventories or methodologies to share identity and attribute data across programs
- Evaluate shared services models for E-authentication, Credentialing and Enrollment
- Port authorities and other private sector entities must be given guidance on their programs
- Work with NIEM and other attribute schemas to determine metadata requirements/options that constitute sufficient information to form an identity in various use cases
Focus Within IdM

Focus within Identity Management has been to encourage interoperability and the creation of centers of excellence within the following fields, using FIPS 201 as a point of convergence:

- Credentialing
- Authentication and Authorization
- Identity and Attributes
- Standards
  - Identity Proofing
  - Trust Framework
  - Open Standards – Informed Buyers / Qualified Sellers
The Credentialing Framework Initiative outlines many credentialing related services that overlap between Components and programs. The current complex interaction of systems and policies can now be simplified and tied to equivalencies and central data stores. These stores can be tied to various programs, including HSPD-12 credentialing systems.

<table>
<thead>
<tr>
<th>CAPABILITIES</th>
<th>REGISTRATION AND ENROLLMENT</th>
<th>ELIGIBILITY VETTING AND RISK ASSESSMENT</th>
<th>ISSUANCE</th>
<th>VERIFICATION AND USE</th>
<th>EXPIRATION AND REVOCATION</th>
<th>REDRESS / WAIVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government</td>
<td>Terrorism and broad scope criminality, immigration, identity, etc.</td>
<td>Physical credential, detailed security / verification features, developed to widely used specification (e.g. FIPS 201 or ICAO)</td>
<td>High level assurance of identify, authenticity and status validity</td>
<td>Match against central records</td>
<td>Intake</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Terrorism and limited scope criminality, immigration, identity, etc.</td>
<td>Physical credential, detailed security / verification features, developed to limited use specifications</td>
<td>Authenticity and status validity emphasis, lower level or no identity verification</td>
<td>Match against distributed records</td>
<td>Determination of misidentification</td>
<td></td>
</tr>
<tr>
<td>Regulated</td>
<td>Terrorism nexus only</td>
<td>Physical credential with minimal security / verification features or process without physical credential</td>
<td></td>
<td>One time use credential</td>
<td>Determination of Waivability</td>
<td></td>
</tr>
<tr>
<td>Guidelines</td>
<td>Sponsor approved</td>
<td></td>
<td></td>
<td></td>
<td>Availability of misidentification / waiver decision for reuse by other screeners</td>
<td></td>
</tr>
</tbody>
</table>

TREND ANALYTICS
Authentication Activities - Completed

- Established the PKI Federal Bridge as the main hub for credential authentication
- Established authentication levels for many use cases and credential types
- Multiple completed Pilots of FIPS 201 and PIV interoperable credentials and data stores
1. Encourage Non-Federal entities to produce a physical credential that is technically interoperable with the Federal Personal Identity Verification Card (PIV) defined by FIPS-201 and related Special Publications. Interoperability and acceptance relies on several additional factors:
   a. Implementation of an identity authentication certificate (comparable to PIV Authentication) that meets Federal requirements (additional certificates are optional)
   b. Development of a Smart Card Number (comparable to FASC-N) that follows a set guideline to ensure uniqueness
   c. Compatibility of the data model for the card with the Federal PIV data model

2. The PKI credential issuing organization must participate in the trust infrastructure known as the Federal Bridge Certification Authority (FBCA) at the medium hardware level of assurance.

3. Credential issued must satisfactorily pass the electronic personalization requirements of the NIST test tool.

Federal Bridge Authority (FBA) serves as the Certification, Binding, Linking Mechanism between members.