The Rise of Identity Proofing Services in the Federal Government

Jamie Danker, Verification Privacy Officer, Office of Privacy, U.S. Citizenship and Immigration Services
Naomi Lefkovitz, Senior Privacy Advisor, Information Technology Lab, National Institute for Standards and Technology
Dawn Wiggins, Deputy Executive Director, Office of Privacy & Disclosure, Social Security Administration

E-Authentication Guidance For Federal Agencies

- M-04-04: OMB issued in December 2003
- Objective is to ensure that agency authentication processes provide the appropriate level of assurance.
- It establishes and describes four levels of identity assurance for electronic transactions requiring authentication.
- Table 1 provides a risk assessment for potential impact categories for authentication errors
Trust Framework Solutions

- Leverages industry-based citizen credentials
- Identity Providers (IDPs) are certified using FICAM privacy security criteria

http://www.idmanagement.gov/approved-identity-providers

NIST LOA 1
Little or no confidence in asserted identity
Approved IDPs: Google, PayPal, VeriSign

NIST LOA 2
Some confidence in asserted identity
Approved IDPs: Virginia Polytechnic Institute and State University (LOA 1 & 2)

NIST LOA 3
High confidence in asserted identity
Approved IDPs: Symantec, Verizon (LOA 1, 2 & non-PKI 3)

NIST LOA 4
Very high confidence in asserted identity
Approved IDPs: PIV/ PIV-I Cards

Why are We Doing This?

- Changing U.S. demographics with expectations of online service delivery
- Citizen benefit services moving online
  - VA
  - CMS
  - SSA
  - IRS
  - Department of Education
  - More...
- Credential lifecycle management of the U.S. population, by USG is NOT sustainable
Challenges

- Agency requirements for Citizen Services typically start at LOA 2
- LOA 2 requires ID Proofing (i.e. This does not come for free)
- Need an active eco-system of CSPs that meet government requirements for security and privacy

What is a Trust Framework?

- Governance structure for a specific identity system consisting of:
  - **Technical and Operational Specifications** that have been developed
    - to define requirements for the proper operation of the identity system (i.e., so that it works),
    - to define the roles and operational responsibilities of participants, and
    - to provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data (i.e., so that it is trustworthy); and
  - **Legal Rules** that govern the identity system in order to
    - regulate the content of the Technical and Operational Specifications,
    - make the Technical and Operational Specifications legally binding on and enforceable against the participants, and
    - define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.

- American Bar Association’s Federated Identity Management Legal Task Force
What are the expectations of Privacy?

- Privacy policy comparability using the following criteria:
  - **Opt In** – Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction.
  - **Minimalism** – Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile. RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002.
  - **Activity Tracking** – Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002.
  - **Adequate Notice** – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process.
  - **Non Compulsory** – As an alternative to 3rd-party identity providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.
  - **Termination** – In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.
LOA 2 Agency Example: Self Check

- **2009**: Requested by Congress, Self Check is a voluntary, fast and free service that allows an individual to make sure the employment eligibility records used by E-Verify are up to date and accurate.

- **2011**: Self Check was launched in five states and D.C.
  - On August 15, 2011 the service was made available in Spanish and expanded to an additional 16 states.
  - On February 9, 2012 Self Check was made available nationwide.

- **2013**: Over 181,000 individuals have used Self Check since its launch.

### E-Verify and Self Check Comparison

<table>
<thead>
<tr>
<th></th>
<th>E-Verify Program</th>
<th>Self Check Service</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audience</strong></td>
<td>U.S. businesses</td>
<td>U.S. workers</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Verify employment eligibility of workforce</td>
<td>Check your own employment eligibility status</td>
</tr>
<tr>
<td><strong>System Security</strong></td>
<td>Employer registration process and user accounts</td>
<td>Identity assurance process on each use</td>
</tr>
<tr>
<td><strong>Legislative Mandate</strong></td>
<td>Required in certain states and for federal contractors</td>
<td>Voluntary, cannot be required</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>50 states and U.S. territories</td>
<td>50 states and U.S. territories</td>
</tr>
</tbody>
</table>
Self Check Process Overview

1. **Self Check Overview:**
   - The Self Check website offers program information and links to E-Verify, USCIS and DHS sites.

2. **Identity Assurance:**
   - Identity assurance is performed by generating knowledge based questions using the personal information provided by the user.

3. **Employment Eligibility Verification:**
   - A user’s employment eligibility information is gathered and checked through by E-Verify against DHS and SSA records.

4. **Self Check Results:**
   - User is notified of Self Check results and if applicable, receives guidance on how to correct any data mismatches in SSA or DHS records.

Note on Fraud Prevention:
- A user is only able to use Self Check if his or her identity is successfully authenticated.

Employment Eligibility Verification:
- A user’s employment eligibility information is gathered and checked through by E-Verify against DHS and SSA records.

User’s View of the Self Check Process

**Step 1 - Enter ID Data**
- Enter basic identifying information like name, address, date of birth, and Social Security number (SSN).
- Providing SSN is optional in Step 1. If not provided here, SSN will be required in Step 3.
User’s View of the Self Check Process

Step 1 - Enter ID Data

- Enter basic identifying information like name, address, date of birth, and Social Security number (SSN).
- Providing SSN is optional in Step 1. If not provided here, SSN will be required in Step 3.

Self Check Terms of Use & Data Entry Screens
**User’s View of the Self Check Process**

**Step 2 - Take a Quiz**
- The info is sent to a third party identity assurance service to generate a “quiz” for user to prove identity.
- The government will have no knowledge of which questions are presented or how those questions are answered.

**Identity Proofing Quiz**
User’s View of the Self Check Process

Step 3 – Enter Document Data
• If successful in Step 2, go on to complete an employment eligibility query to determine work eligibility.
• Additional required info includes SSN, citizenship status, and details from immigration documentation (e.g., Green card, EA card, etc).

User’s View of the Self Check Process

Step 4 - Get Results
• Information submitted is checked against Department of Homeland Security (DHS) and Social Security Administration (SSA) databases to determine work eligibility.
• A response is given indicating either that the user would likely be employment authorized in E-Verify (if an employer runs the employment authorization check), or that there is a mismatch between the data entered and the DHS and/or SSA databases. If there is a mismatch, user will be given information that outlines how to correct the records if desired.
**Additional Privacy Considerations**

- **Redress**
  - What happens if a quiz cannot be generated for me?
  - What happens if I cannot pass the quiz?
  - What if I cannot pass the quiz, but I believe I answered the questions correctly (i.e., inaccurate commercial information)?

- **Retention** – What does the IDP Retain? What does USCIS Retain?
  - For the identity authentication USCIS receives a transaction ID, date/time of the transaction, pass/fail indicator, and any business rules triggered during the process to facilitate troubleshooting and system management and improvement.
  - The IDP maintains a log of access to your information and the type of inquiry (i.e., identity check) and a log of all identity verification transactions to conduct system management and to generate customer usage statistics.
  - For the E-Verify query, USCIS maintains a record including your name date of birth, work authorization documentation information, the query result, and an E-Verify case number. (The IDP does not have access to this part of the Self Check process).

---

**LOA 2 Example: mySocialSecurity**

**Focus Today**

- **Registration**
  - **Online**
  - **In-Person**
The 5 Steps of Registration

1. Overview and Accept Terms
2. Identity Proofing
3. Out of Wallet Quiz
4. User ID Setup
5. User ID Elevation

Sign In or Create an Account
1. Overview and Accept Terms

Identity Proofing
2. Identity Proofing

- Name
- DOB
- SSN
- Address

Internal Records Check

- Name
- DOB
- Address

External Records Check

- Phone number

3. Out of Wallet Quiz
4. User ID Setup

Current Overview
Recommendations

- Assess your user population to determine whether knowledge based authentication is feasible.
- Have a plan to address individuals who are unable to electronically authenticate.
- Work with your vendor to monitor quiz generation and quiz pass rates and adjust your quiz strategy as appropriate.
- Work closely with your vendors to fully understand retention and use practices.
- Communicate clearly with your customer base about e-authentication practices.
- Use the PIA, privacy notices, and terms of service process to promote transparency.
- Consider data minimization for data collected for authentication.
Resources

• Self Check
  – http://www.uscis.gov/self-check

• mySocialSecurity
  – http://ssa.gov/myaccount/
  – PIA (http://www.socialsecurity.gov/foia/piadocuments/FY11/e-Auth%20PIA%20May%202011.htm)
  – SORN (http://www.socialsecurity.gov/foia/bluebook/60-0373.htm)

National Strategy For Trusted Identities in Cyberspace (NSTIC)

VISION
Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.

NSTIC Objective 2.3: Implement the Federal Government Elements of the Identity Ecosystem
- The Federal Government must continue to lead by example and be an early adopter of identity solutions that align with the Identity Ecosystem Framework.
- The Federal Government must also continue to leverage its buying power as a significant customer of the private sector to motivate the supply of these solutions.
Solution Overview

Federal Cloud Credential Exchange (FCCX) accelerates NSTIC and FICAM by allowing agencies to securely interact with a single “broker” to authenticate consumers.

Market Challenge

- Requires agencies to integrate with multiple Identity Service Providers (IDPs), each independently paying for authentication services
- Limited LOA 2 & 3 credentials due to limited demand

The Solution (FCCX)

- Centralized interface between agencies and credential providers – reduces costs and complexity, speeds up integration timeline for new IDPs
- Enhanced consumer privacy and experience; citizen does not have to get a new credential for each agency application
- Decreased Federal government authentication costs

Privacy Architecture

- Phase I: The broker prevents the IDP from knowing at which agencies citizens are using their credentials, and can prevent the agencies from knowing which IDP supplied a citizen’s credential
  - Every user is represented by an internal identifier called an MBUN
    - (i-MBUN) Internal – Meaningless, But Unique Number
    - Internal mapping between the user identifier provided by a IDP and the internally generated MBUN that is sent to the RP.
- Phase II: Use of privacy-enhancing cryptography so citizens remain anonymous to the broker
High Level Process Flow and Key Decision Points for Release 1

Decision 1 – How to present IDPs to users?
1. Customer chooses to use an identity provider or navigate to his/her agency website.
2. FCCX routes the customer to the identity provider's login page.
3. Customer logs into the identity provider.
4. Customer navigates to his/her agency website.
5. Access to the agency website is granted.

Decision 2 – Informed Consent
FCCX relays an assertion to the Agency website that the customer has logged into the identity provider. This is done without storing any sensitive user data.

Decision 3 – What attributes are needed?
- Informed consent (display attribute values / names)
- Release consent (RP, scope)
- Implicit consent (scope, RP name in selector)
- Pass-thru consent (mapping only)

Consent Model Options
- Informed consent (display attribute values / names)
- Release consent (RP, scope)
- Implicit consent (scope, RP name in selector)
- Pass-thru consent (mapping only)

ACTION: Privacy working group team to recommend consent handling user experience at IDPs and within FCCX
Assurance Vs. Resolution

Assurance
- The degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and
- The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Resolution
- The degree of confidence in the vetting process used to establish the identity of an individual to whom the credential was issued, and
- The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

ANSI/NASPO IDPV Standard

Attribute bundles to resolve to single US Person

<table>
<thead>
<tr>
<th>Category</th>
<th>Attribute</th>
<th>Description</th>
<th>Attribute Bundle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name</td>
<td>(First Name) AND (Last Name)</td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Location</td>
<td>Partial Address</td>
<td>Postal Code OR (City and State)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Place of Birth</td>
<td>(City or County) AND (State or Foreign Country)</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Partial Date of Birth</td>
<td>(Month and Day) OR Year</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Date of Birth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identifier</td>
<td>Partial Social Security Number</td>
<td>Last 4 Digits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Social Security Number</td>
<td>Full 9 Digits</td>
<td></td>
</tr>
</tbody>
</table>

Each of the above attribute bundles equally RESOLVES TO ONE PERSON in the US Population 95% of the time (or greater)
QUESTIONS?

- Jamie Danker (jamie.danker2@uscis.dhs.gov)
- Naomi Lefkovitz (naomi.lefkovitz@nist.gov)
- Dawn Wiggins (dawn.wiggins@ssa.gov)

Resources

- OMB E-Authentication Guidance for Federal Agencies (OMB-M-04-04)
- NIST Electronic Authentication Guideline (NIST SP-800-63-2)
- Trust Framework Provider Adoption Process (TFPAP) for Levels of Assurance 1, 2, 3 and 4
  http://www.idmanagement.gov/sites/default/files/documents/FICAM_TFS_TFPAP_v1_1.0.pdf
- Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance v2.0
- Federal ICAM Privacy Guidance for Trust Framework Assessors and Auditors
- OMB Requirements for Accepting Externally-Issued Identity Credentials