FCCX Briefing

Information Security and Privacy Advisory Board

June 13, 2014
Agenda

- Overview
  - NSTIC
  - FICAM
  - Federal Cloud Credential Exchange

- Lessons Learned

- Enhancing Federation Privacy

- Questions
Challenge with Digital Identities

Average users have 6.5 web passwords, 25 accounts requiring passwords, and enter approximately 8 passwords per day.

76% of network intrusions exploited weak or stolen credentials.

75% of customers will avoid creating new accounts.

54% leave the site or do not return when asked to create a new password.

45% of consumers will abandon a site rather than attempt to reset their passwords or answer security questions.

The rise of Bring Your Own Identity is being driven by users’ “identity fatigue” and the need to bring convenience, security and privacy to on-line interactions.
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.
FICAM Trust Framework Solutions
Approved Identity Services

LOA 4
• Very High Confidence in Asserted Identity
• PIV, CAC, PIV-I, xCertified w/ Federal Bridge @ LOA4

LOA 3
• High Confidence in Asserted Identity
• LOA 4 + Symantec + Verizon Business

LOA 2
• Some Confidence in Asserted Identity
• LOA 4/3 + Virginia Tech

LOA 1
• Little or No Confidence in Asserted Identity
• LOA 4/3/2 + LOA 1 TMs

Current & Complete listing @
http://www.idmanagement.gov/approved-identity-services
The Federal Cloud Credential Exchange (FCCX) accelerates NSTIC and FICAM by allowing agencies to securely interact with a single “broker” to authenticate consumers.

**Current State**
- 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; user does not have to get a new credential for each agency application
- Decreased Federal government authentication costs
Sample User Experience

1. Consumer navigates to Agency website that has decided to accept interoperable credentials and identities.

2. Consumer chooses to use Identity Provider credential to log into the Agency website (2 options: imbedded selector on agency page or standalone page).

   - Imbedded Selector
   - FCCX Sign-In Page

3. Consumer browser is routed via FCCX to the Identity Provider login page (Identity Provider only knows it has an authentication request from FCCX and no consumer information is in the transfer).
Sample User Experience - continued

4. Consumer logs into the Identity Provider website and provides consent to allow attributes to be shared

IDP – Informed Attribute Consent

The application you requested is asking for attribute information in order to process your log-in request. Please approve the secure transmission of the values below. Note that the requested application may not function correctly without these values.

First Name: John
Middle Name or Initial: Doe
Last Name: Smith
Address: 123 Christmas Way, North Pole, North Pole, 00000
Date of Birth: 12-25-1970

5. Identity Provider sends credential assertion and attributes via FCCX to the requesting Agency. This is done without storing any personal consumer data in FCCX. Agency resolves identity to single account utilizing attributes and may ask additional identity related questions during initial log-in to resolve identity to a single person/account.
High Level Architecture

Relying Parties (e.g., Agencies' Web Sites)

- RP1
- RP2
- RP3
- RPn

FCCX

- Federation Manager
- Attribute Broker*
- Credential Broker

Attribute Providers

- Ap1
- Ap2
- Ap3

Credential Service Providers and Token Managers

- CSP1
- CSP2
- CSP3
- CSPn

* Roadmap Item
Ensuring Privacy by Design

The system generates and stores a different anonymous identifier for each web application. FCCX does not store any PII.
Interoperable Credential and FCCX Benefits

For Agencies:

- Enables acceptance of full range of FICAM-approved third-party credentials for online services
- Avoids need for separate contracts with each credential provider
- Increases efficiency and ease of credentialing and integration, enhancing ability to provide digital services to citizens
- Reduces total investment – password renewal, helpdesk, and credentialing costs

For Citizens and other users:

- Allows the citizen to use credential(s) of choice for interactions with multiple agencies
- Provides a more secure environment that is easier to manage – one username and password. More secure than multiple agency passwords.
FCCX Roles

NSTIC
National Strategy for Trusted Identities in Cyberspace – overall vision

GSA
Program Management Office (PMO), IDP Contracts and FICAM Program

USPS
Operating Entity for FCCX Broker

SecureKey
Technology Provider for FCCX Broker

Credential Providers
Credential/Identity Providers

Agencies
Relying Parties
Lessons Learned
User Experience & Relying Party Considerations
Have you used a login from any of the following companies to log in to other websites?

% of respondents, by age bracket

<table>
<thead>
<tr>
<th>Company</th>
<th>Age 18-34 (n=216)</th>
<th>Age 35-54 (n=374)</th>
<th>Age 55+ (n=410)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>75%</td>
<td>57%</td>
<td>39%</td>
</tr>
<tr>
<td>Google</td>
<td>57%</td>
<td>34%</td>
<td>21%</td>
</tr>
<tr>
<td>PayPal</td>
<td>44%</td>
<td>24%</td>
<td>22%</td>
</tr>
<tr>
<td>Amazon</td>
<td>32%</td>
<td>20%</td>
<td>19%</td>
</tr>
<tr>
<td>Yahoo</td>
<td>31%</td>
<td>22%</td>
<td>18%</td>
</tr>
<tr>
<td>Twitter</td>
<td>30%</td>
<td>18%</td>
<td>10%</td>
</tr>
<tr>
<td>Linkedin</td>
<td>14%</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td>Pinterest</td>
<td>13%</td>
<td>7%</td>
<td>8%</td>
</tr>
<tr>
<td>Apple</td>
<td>18%</td>
<td>5%</td>
<td>4%</td>
</tr>
<tr>
<td>No, I have not</td>
<td>12%</td>
<td>32%</td>
<td>47%</td>
</tr>
</tbody>
</table>

- n=1000
- Online survey
- Conducted February 2014
- Representative sample by age, household income and gender
- Respondents recruited online, using AYTM.com
Many users understand logging in with a social account. They do not understand the difference between an unverified identity (LOA 1) and a verified identity (LOA 2+) plus the many have other questions on privacy, security, etc.

Next Step: Developing User Experience Guidance and Communications
Federated Identities – Relying Party Considerations

- RP is responsible for maintaining a user profile and for managing user access to their system.

- Identity resolution – the ability to uniquely resolve to an individual in a database is a core issue for agencies.
  - Gaining access to existing PII – RP must ensure it is granting access to the right person.
  - Users may change CSPs over time – RP needs to have the ability for user to map different credentials to the same user profile.
Core set of attributes required from LOA2/LOA3 Credential Service Providers (examples:)

- Legal First Name, Legal Last Name, Middle Name or Initial
- Current Address: (Parsed or Full)
- Date of Birth: (Parsed or Full)
- Social Security Number: (Parsed or Full)
- Email Address

Next Step: working with agencies to determine appropriate minimum combinations or bundles that will enable identity resolution for their needs
Enhancing Federation Privacy
Ensuring Privacy by Design

The system generates and stores a different anonymous identifier for each web application. FCCX does not store any PII.
Direct CSP and RP Integration

1. **AuthN Request** (No attributes)

2. **Signed AuthN Response** with MBUN (No Attributes)
   - **Optional**: Query AP

3. **Signed AuthN Response** (MBUN, Assertion, Encrypted Attribute Values)

**1st Time Credential** (New MBUN)

**Existing Credential** (Existing MBUN)

© 2014 United States Postal Service. All Rights Reserved.
Current FCCX Flow

1st Time Credential (New MBUN)

1. AuthN Request (No attributes)
2. Strip Headers & Re-sign
3. AuthN Request (No attributes)
4. User Consent
5. Signed AuthN Response (MBUN, Assertion, Encrypted Attribute Values)
6. Decrypt values, Map to Common Name Space, Re-encrypt & Sign AuthN Response
7. Signed AuthN Response (rpPAI, Assertion, Encrypted Attribute Values)

Existing Credential (Existing MBUN)

1. AuthN Request (No attributes)
2. Strip Headers & Re-sign
3. AuthN Request (No attributes)
4. User Consent
5. Signed AuthN Response (MBUN, Assertion, Encrypted Attribute Values)
6. Decrypt values, Map to Common Name Space, Re-encrypt & Sign AuthN Response
7. Signed AuthN Response (rpPAI, Assertion, Encrypted Attribute Values)

Considerations:
- Attributes are passed to the RP every time - based on the attribute group requested - regardless of new or existing credential
Future State Enhancement Option

1st Time Credential
(New MBUN)

RP

1. AuthN Request
   (No Attributes)

2. Strip Headers & Re-sign

FCCX

3. AuthN Request
   (No Attributes)

4. Signed AuthN
   Response
   (MBUN Only)

Diffie-Hellman
key exchange

5. Query Repository
   for MBUN

6. Request attributes
   based on Agency
   Request (MBUN only)

7. User Consent

CSP

8. Signed AuthN
   Response (MBUN,
   Assertion, Encrypted
   Attribute Values)

9. Signed AuthN
   Response

10. Signed AuthN
    Response
    (rpPAI, Assertion,
    Encrypted Attribute
    Values)

Existing Credential
(Existing MBUN)

RP

1. AuthN Request
   (No attributes)

2. Strip Headers & Re-sign

FCCX

3. AuthN Request
   (No attributes)

4. Signed AuthN
   Response
   (MBUN Only)

5. Query repository
   for MBUN

6. Strip headers & re-sign

CSP

7. 1 Query
   AP (Optional)

Attribute
Provider
(AP)
Questions
NSTIC
Jeremy Grant – jeremy.grant@nist.gov
Naomi Lefkovitz – naomi.lefkovitz@nist.gov

GSA
PMO – Kathy Conrad - kathy.conrad@gsa.gov
PMO – Jennifer Kerber - jennifer.kerber@gsa.gov
PMO – Zach Baldwin - zachary.baldwin@gsa.gov
FICAM – Dominic Sale - dominic.sale@gsa.gov
FICAM – Deb Gallagher - deborah.gallagher@gsa.gov
FICAM – Anil John - anil.john@gsa.gov

USPS
Randy Miskanic – rsmiskanic@uspis.gov
Doug Glair – douglas.p.glair@usps.gov
Angela Lagneaux – angela.m.lagneaux@usps.gov