Spring 2014 ICAM Information Sharing Day and Vendor Expo

Federal Cloud Credential Exchange
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.
FCCX – FICAM TFS Approved 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 TM

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
FCCX and FICAM Relationship

- FICAM sets the policy for acceptance of externally-issued credentials at federal applications

- FCCX is a service that supports the implementation of FICAM policy
  - enables federal agencies to accept externally-issued credentials more easily and at lower cost than on their own.

- FCCX requirements are consistent with FICAM policy, but may be more extensive than what FICAM specifies to meet multiple agency needs.
Consumer navigates to Agency website that has decided to accept interoperable credentials and identities

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

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)
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

Allow   Deny

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.
Breakout Session Content - FCCX

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

- RP1
- RP2
- RP3
- RPn

FCCX

- Federation Manager
- Attribute Broker*
- Credential Broker

Attribute Providers
- Ap1
- Ap2
- Ap3
- IDPn

Identity Providers
- IDP1
- IDP2
- IDP3

* Roadmap Item

SAML 2.0, OpenID 2.0, PKI

https

Consumer Accessing Protected Resource
Ensuring Privacy by Design

The system generates and stores a different anonymous identifier for each web application.
Breakout Session Content – FCCX Value

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 the same credential 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.
Breakout Session Content – FCCX Roles

- **NIST/NSTIC – Overall Vision for Interoperable Credential Ecosystem**

- **GSA**
  - FCCX Program Management Office
  - FICAM Program
  - Contracting for Credential Service Providers (CSPs)

- **USPS – Operating Entity**
  - Contract in place for the FCCX Exchange (SecureKey)

- **Agencies**
  - Initial Participating Agencies - VA, USDA, NIST, GSA
  - Interested Agencies – DHS, State, OPM, SSA, RRB and others
Broker Technology Implementation
• Configuration is complete
• Environments complete and tested
• Ready for pilot production use – under USPS ATO
• FedRAMP certification – August, 2014

Identity Attributes and CSP Contracts
• FICAM Identity Resolution Attributes Technical Exchange Meeting (TEM) on 5/1/14
• GSA releasing updated solicitation in May

Long-term Items In-Progress
• Consumer Outreach (positioning on agency pages, user experience, communications, help desk preparations, etc.)
• Business Model (operating agreements, funding structure, etc.)
Get Involved - Contact Us

**NSTIC**
Jeremy Grant – jeremy.grant@nist.gov
Naomi Lefkovitz – naomi.lefkovitz@nist.gov

**GSA**
PMO – Kathy Conrad - kathy.conrad@gsa.gov
PMO – Zach Baldwin - zachary.baldwin@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