Research and Development: Innovative – Identity and Access Management

Attribute Based Access Control
Operationalizing the Backend Attribute Exchange profile
S&T Identity Management Testbed

Internet Zone

DMZ

Protected Zone

- Externally facing clustered Hardware XML Security Gateways Hosting both the BAE External Service and protecting externally facing Web Services (PEP)

- Internally facing Hardware XML Security Gateway Hosting both the BAE Internal Service and protecting other internal Web Services (PEP) + Security Token Service (STS)

- Proxy Server

- Federation Server

- SharePoint Portal Server (w/ PEP)

- Authorization Service / Privilege Management Server (PDM)

- Application Servers hosting both .NET and Java Web Applications and Web Services

- PKI Server

- LDAP/AD Server(s)

- SQL Server

- Virtual/Meta Directory Server
Attribute Exchange for Access Control

1. User needs access to resource (e.g. portal)

2. User is authenticated and identified via Unique Identifier

3. Resource owner needs additional attributes about the person ("off-card") in order to authorize the user. It "asks" its Attribute Authority to fetch for attributes.

4. RP Attribute Service sends a query for the required attributes in order to make an access control decision

5. User's Attribute Service responds with the User's attributes from an authoritative source

6. User is granted access
Federated Attribute Exchange

BAE Profile
SAML v2
Governance
Processes

Metadata Distribution Service

BAE Broker
Agency A

BAE Broker
Agency B

BAE Broker
Agency C

BAE Broker
Agency D

BAE Broker
Agency E

BAE Broker
Agency F

Attribute Service
Org E-1

Attribute Service
Org C-1

Federated Attribute Exchange

Federal
BAE
CA
Technology Transition Working Group

- PIV-I/FRAC Technology Transition Working Group (TTWG)
  - Public Safety/Emergency Response
  - Security
  - Federated Identity for First Responders
    - National standard, Interoperable, and trusted ID credential
  - One voice from the TTWG to policy makers
  - Sharing lessons learned
  - Provide innovative, Cost-effective solutions

- West Virginia
- Hawaii
- Rhode Island
- Nevada
Incident Scene Access Provisioning Pilot

DHS S&T IdM Testbed  Chester County - PA

F/ERO Entitlements
Authoritative Source

SPML Read-Only Profile Web Service

SPML Read-Only Request

Unique F/ERO Identifier

Field Station
Handheld
Credential

1. DHS, FEMA (PIV)
2. DOD (CAC)
3. Chester Co PA (PIV-I)

NO COMMUNICATIONS

PIV: Personal Identity Verification
PIV-I: PIV– Interoperability
CAC: Common Access Card
OASIS: Organization for the Advancement of Structured Information Standards
F/ERO: Federal/Emergency Response Official
SPML: Service Provisioning Markup Language
End-to-End Attribute Exchange Using Standards

Agency 1 Authoritative Source
Agency 2 Authoritative Source
Agency 3 Authoritative Source

SPML Gateway
SPML Create, Read, Update, Delete Profile

F/ERO Repository (Attributes)

SAML Service

SPML Service

SPML Read-Only Profile Web Service

Tablet
Smartphone
Local Workstation
Handheld
Verification using Smart Phone

- “Give me a list of all Users with Attribute X, Y, and Z”
- “Give me all the Emergency Support Function (ESF) attributes of User X”
- “Give me all authorized users for the incident”

Samsung Galaxy Nexus smartphone
Permit or Deny

Attributes
Cyber-Physical Convergence

- Platform collects sensor data from various sources
- Platform provides interoperability between the reader/control and logical policy decision based on standard (XACML)
BAE and GFIPM interoperability

- Authoritative Attribute Source 1
- Authoritative Attribute Source 2
- Authoritative Attribute Source 3

User with PIV or PIV-I Card

Virtual/Meta Directory

XML Security Gateway (BAE)

- Trusted Identity Broker
- GFIPM Relying Party

State & Local Agency Attribute Service

Federal Agency Attribute Service
- Educating our upcoming workforce on defensive skills in cyberspace
- Providing real-world, hands-on experience
- Educating students in securing network infrastructures
- Inserted the Backend Attribute Exchange and learned some real world lessons
Resources

- **Websites**
  - [http://www.ahcusa.org/PIV-I%20TTWG.htm](http://www.ahcusa.org/PIV-I%20TTWG.htm)
  - [https://www.cyber.st.dhs.gov/idmdp.html](https://www.cyber.st.dhs.gov/idmdp.html)
Karyn Higa-Smith
DHS Science and Technology Directorate
Cyber Security Division
Identity Management Research Program Manager
Homeland Security Advanced Research Projects Agency
Karyn.Higa-Smith@hq.DHS.gov
202.254.5335