Research and Development: Innovative – Identity and Access Management

Homeland Security
Science and Technology

Attribute Based Access Control

Operationalizing the Backend Attribute Exchange profile
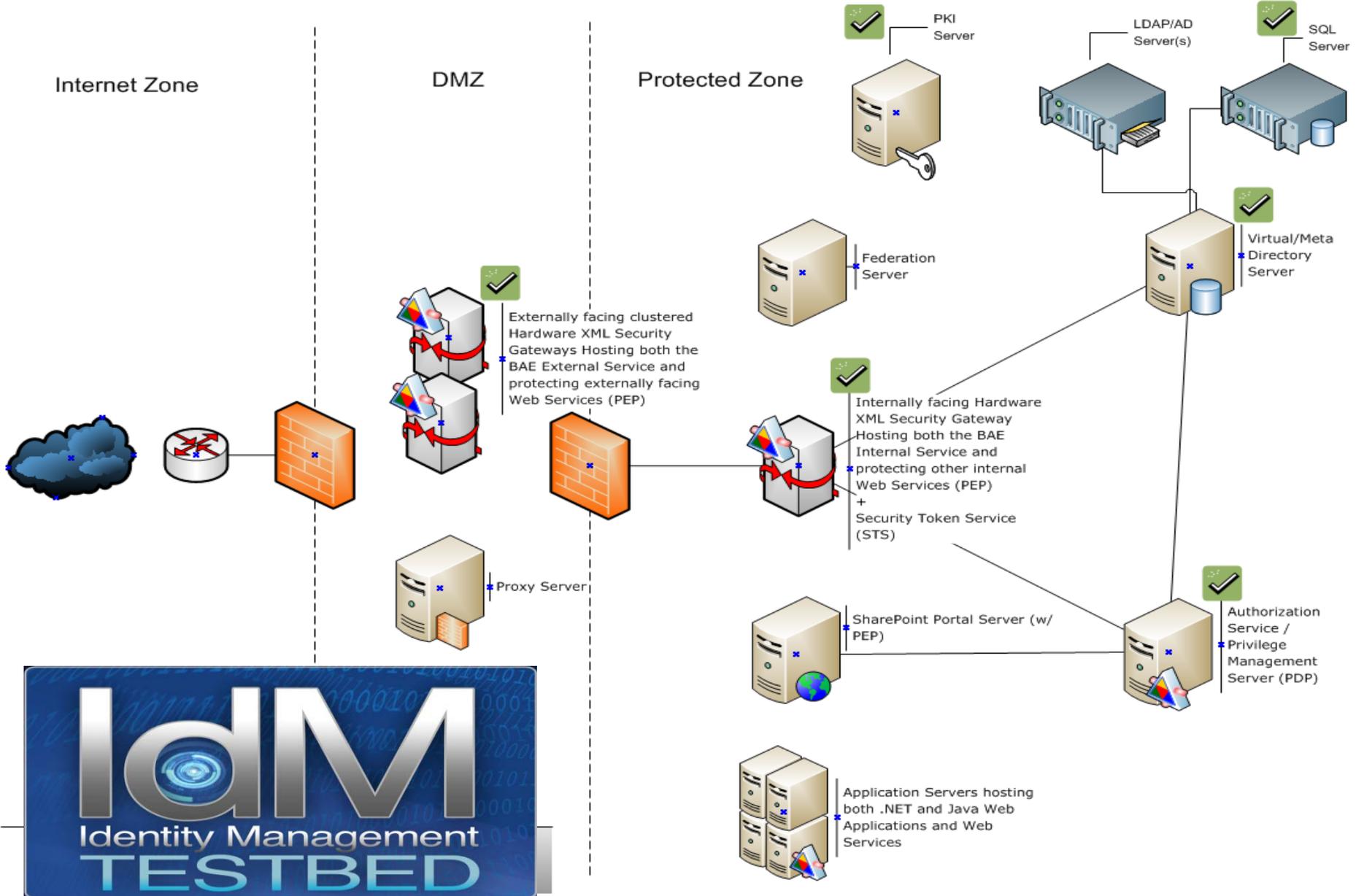
Attribute Exchange for Access Control

POLICY

Homeland Security
Science and Technology

User w/PIV or PIV-I Card

Strong Authentication PKI / X.509

Policy Driven Access Control

Resource of the Relying Party

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

2. User is *authenticated* and identified via Unique Identifier

6. User is granted access

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.

Virtual Directories & XML Security Gateways

Auth. Attribute Store

Auth. Attribute Store

User's Home Organization Attribute Service (BAE)

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

Standards-based Communication (SAML)

Relying Party (RP) Attribute Service

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

Federated Attribute Exchange

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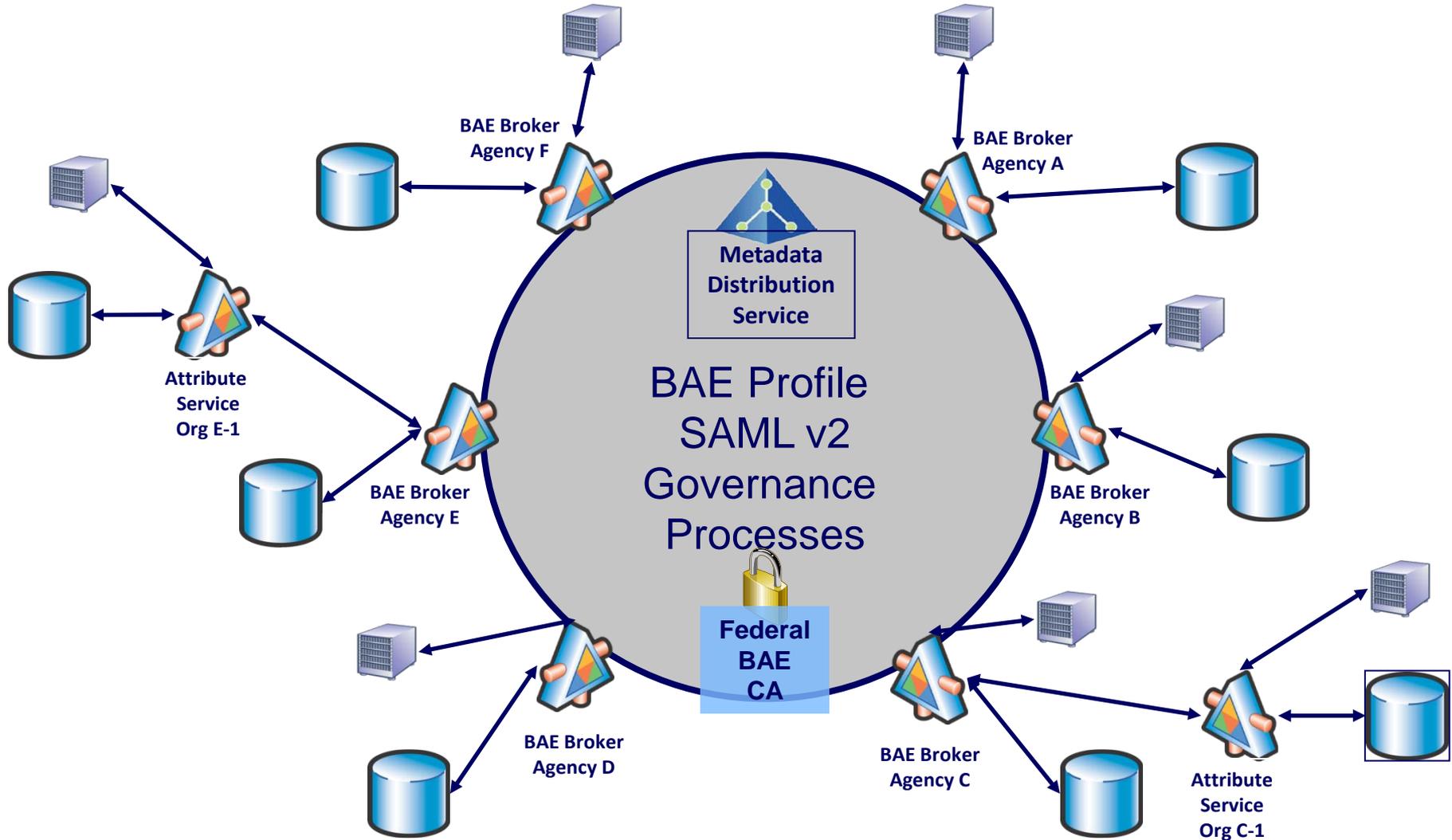
- PIV-I/FRAC Technology Transition Working Group (TTWG)
  - Public Safety/Emergency Response
  - Security
  - Federated Identity for First Responders
    - National standard, Interoperable, and trusted ID credential
  - One voice from the TTWG to policy makers
  - Sharing lessons learned
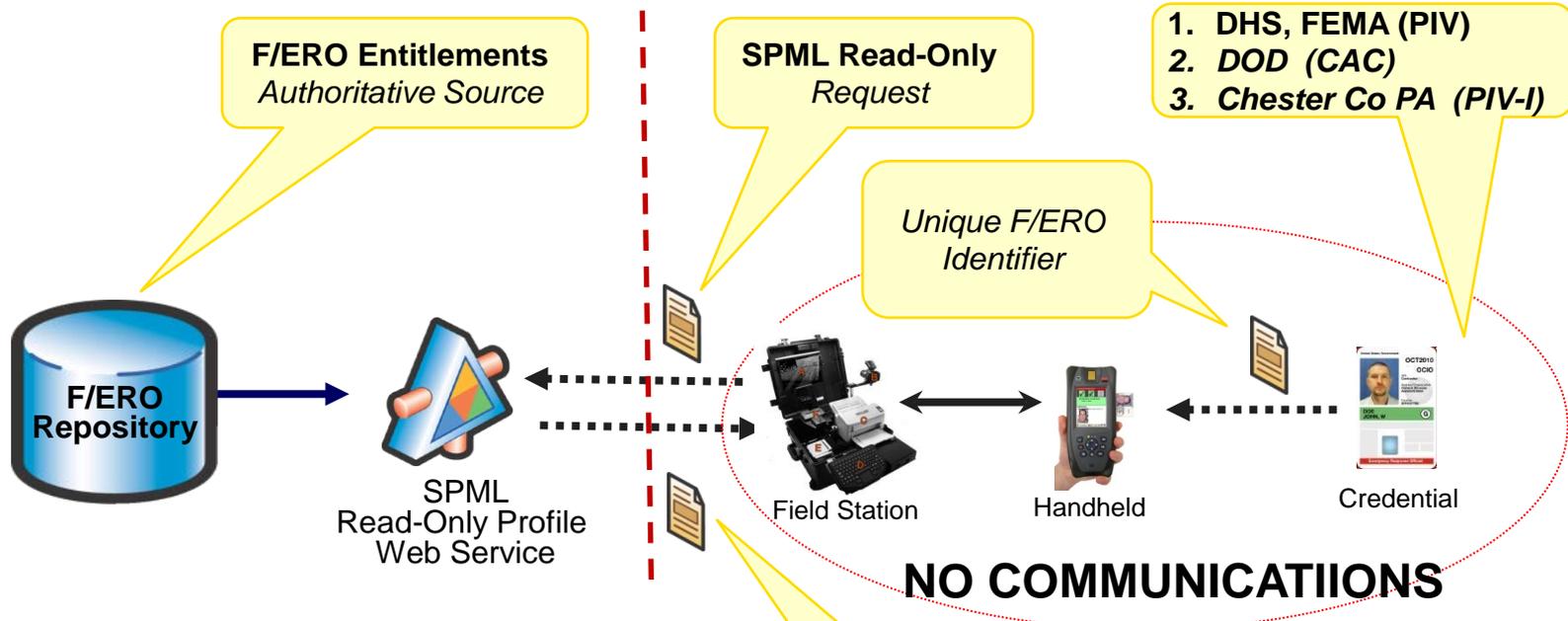 - **Provide innovative, Cost-effective solutions**
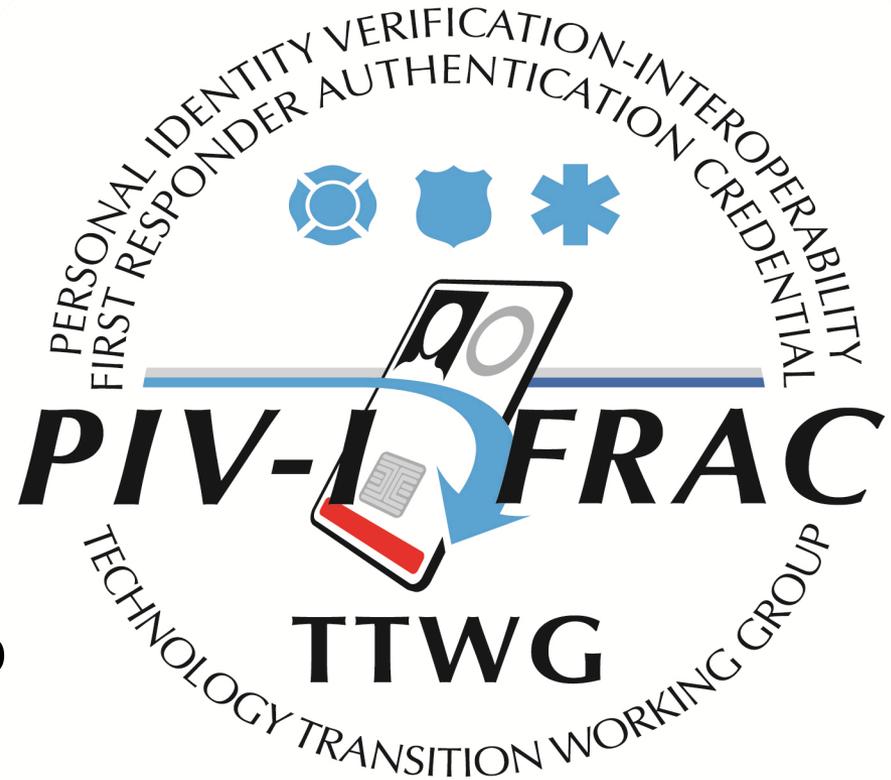
- West Virginia
- Hawaii
- Rhode Island
- Nevada

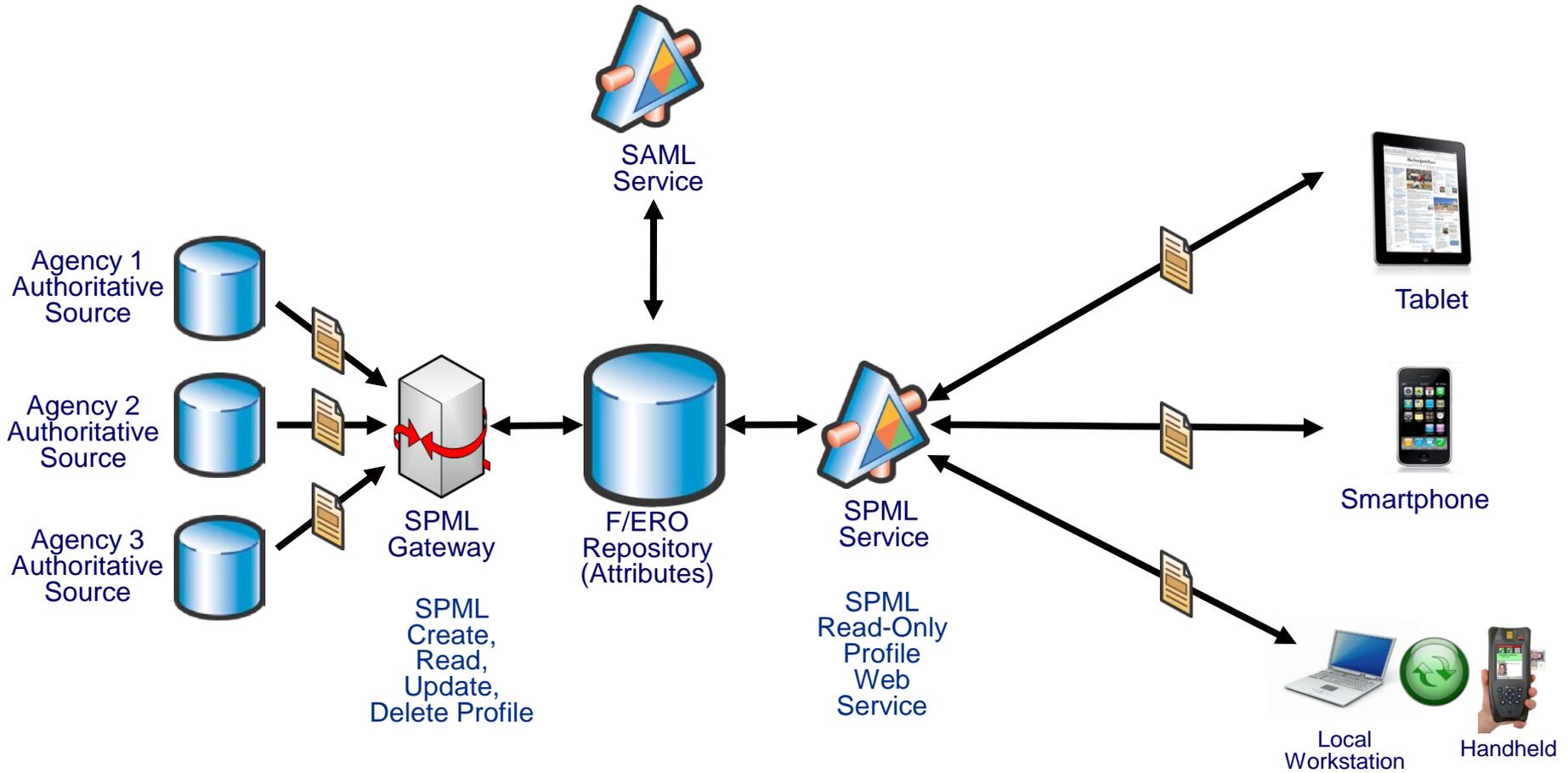# Incident Scene Access Provisioning Pilot

DHS S&T IdM Testbed

Chester County - PA

F/ERO Entitlements
Authoritative Source

SPML Read-Only
Request

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

Unique F/ERO Identifier

F/ERO Repository

SPML
Read-Only Profile
Web Service

Field Station

Handheld

Credential

NO COMMUNICATIIONS

SPML Read-Only
Response

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
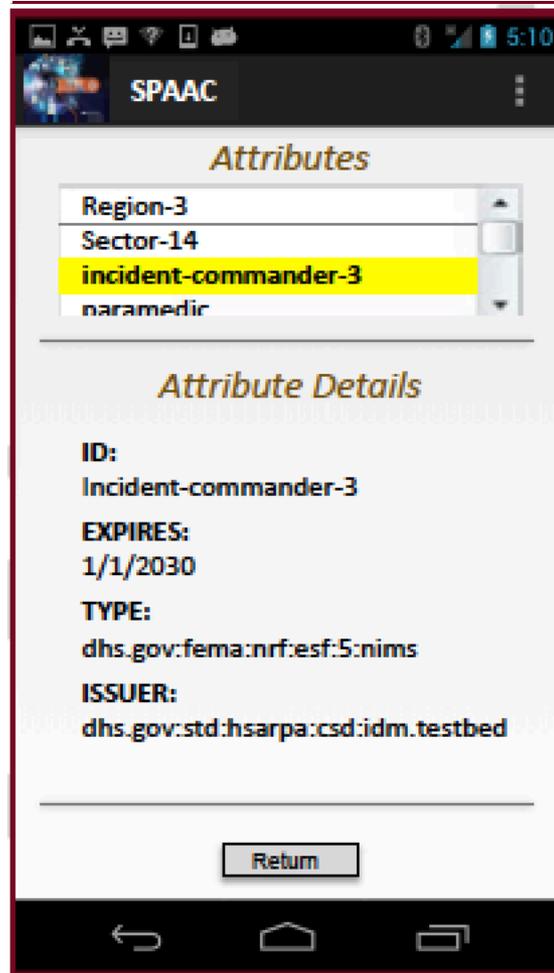**SPML**: Service Provisioning Markup Language

6

Homeland Security
Science and Technology

SAML Service

Agency 1 Authoritative Source

Agency 2 Authoritative Source

Agency 3 Authoritative Source

SPML Gateway

SPML Create, Read, Update, Delete Profile

F/ERO Repository (Attributes)

SPML Service

SPML Read-Only Profile Web Service

Tablet

Smartphone

Local Workstation

Handheld

Verification using Smart Phone

Samsung Galaxy Nexus smartphone

✓ "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"
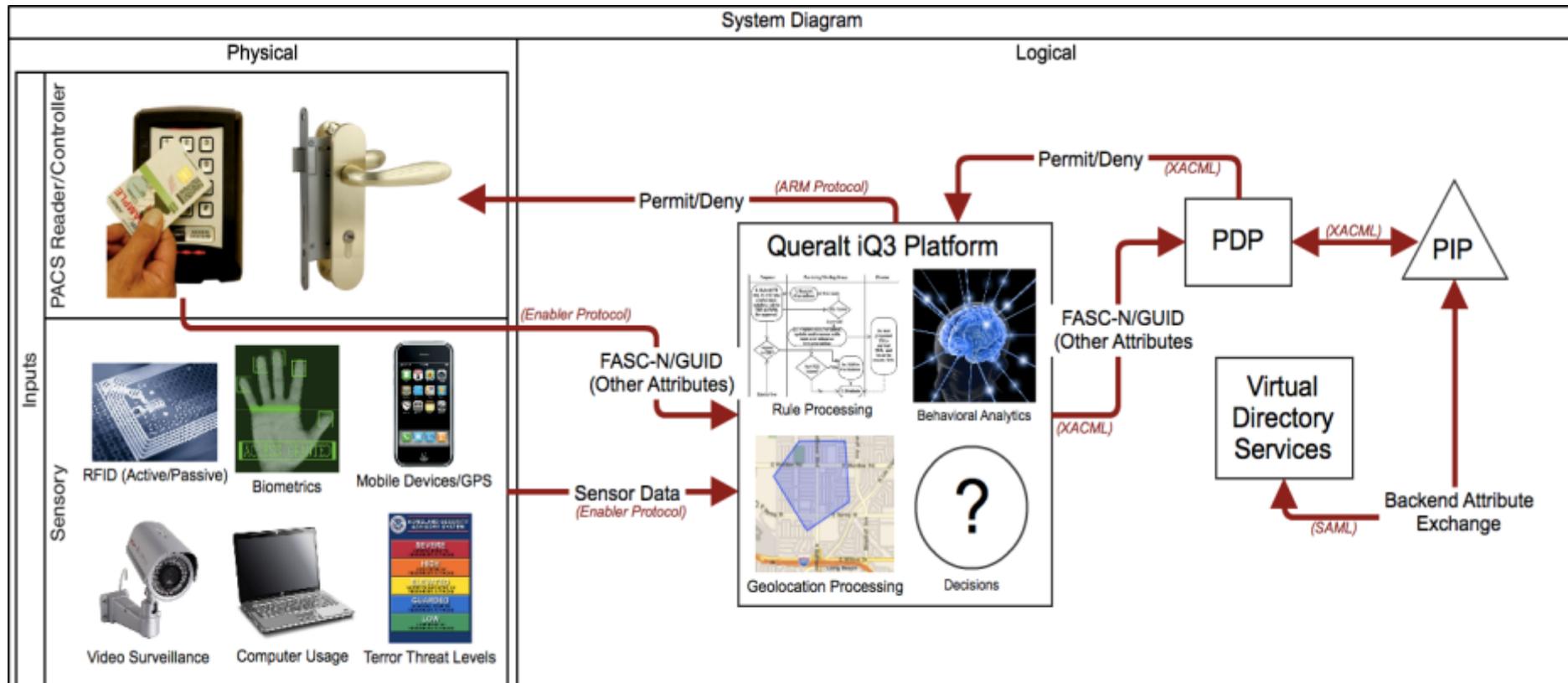
✓ "Give me all authorized users for the incident"
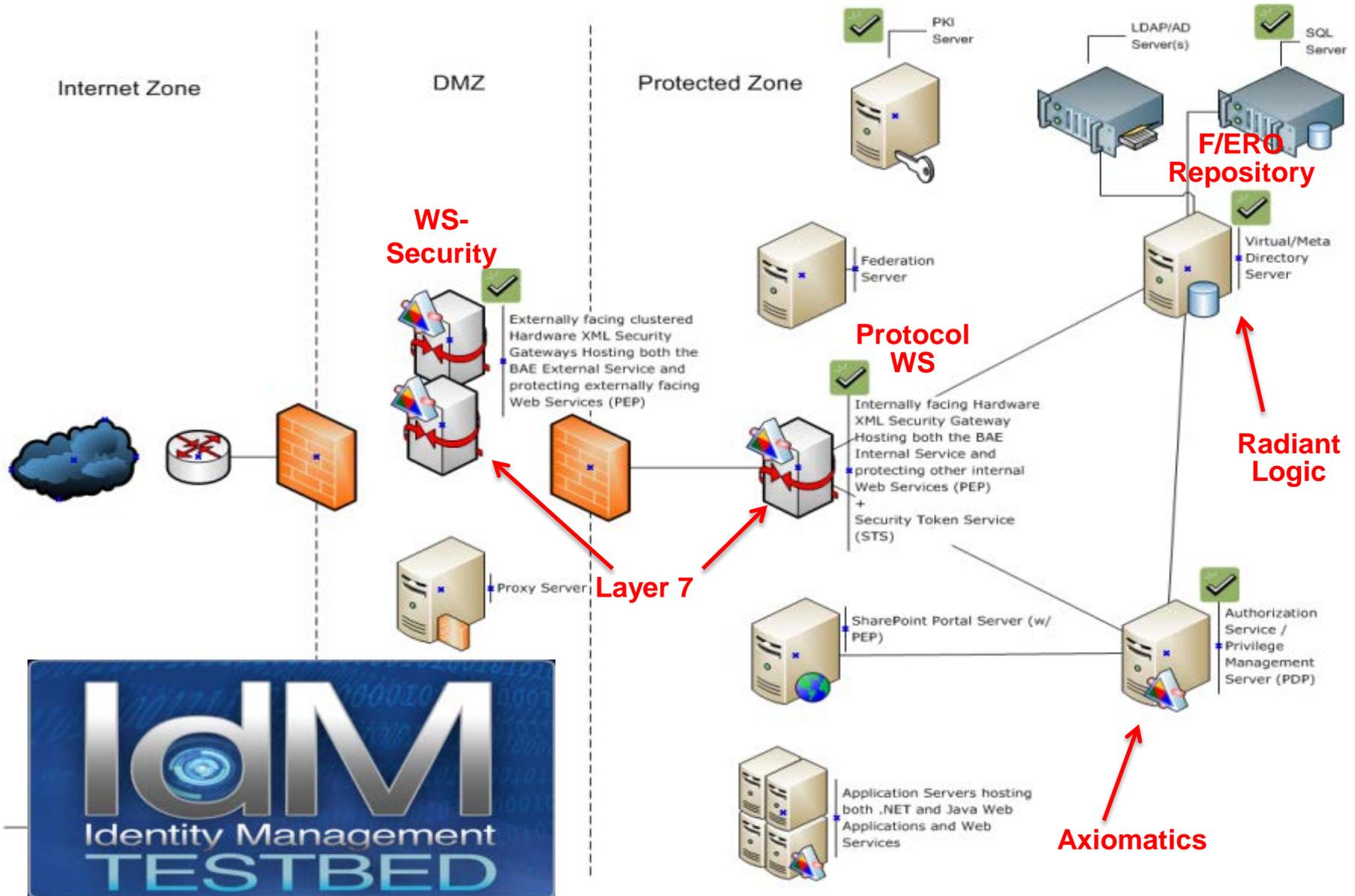
Demonstration Flow
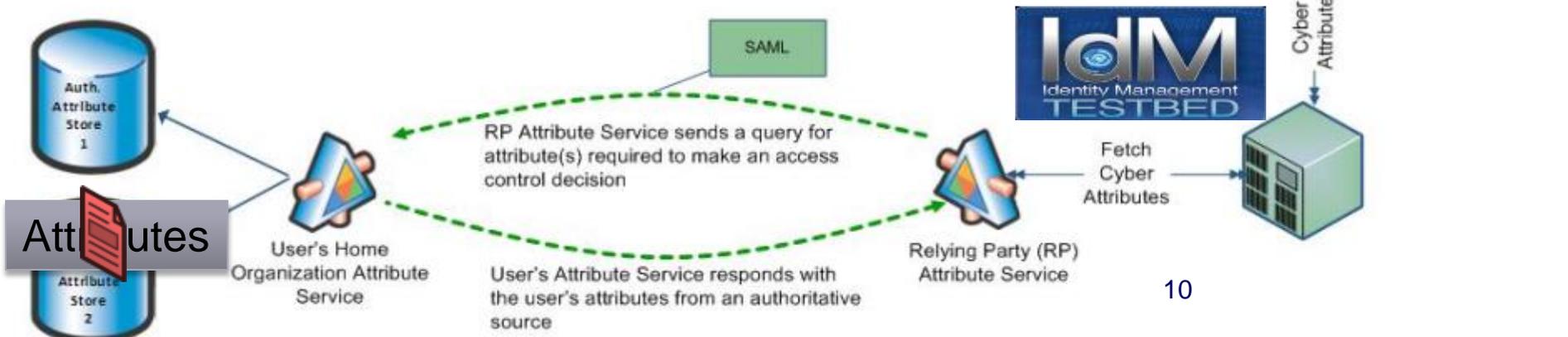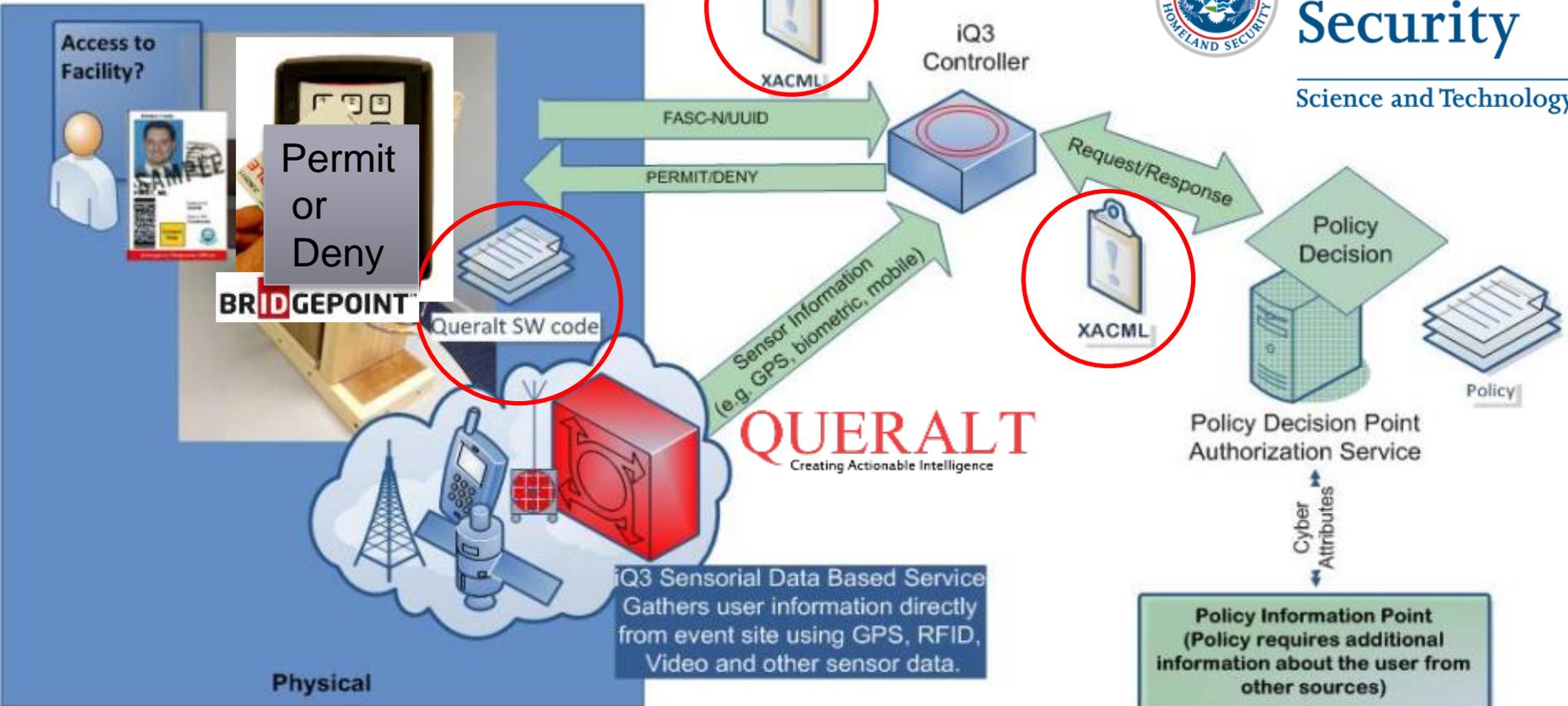
Cyber-Physical Convergence

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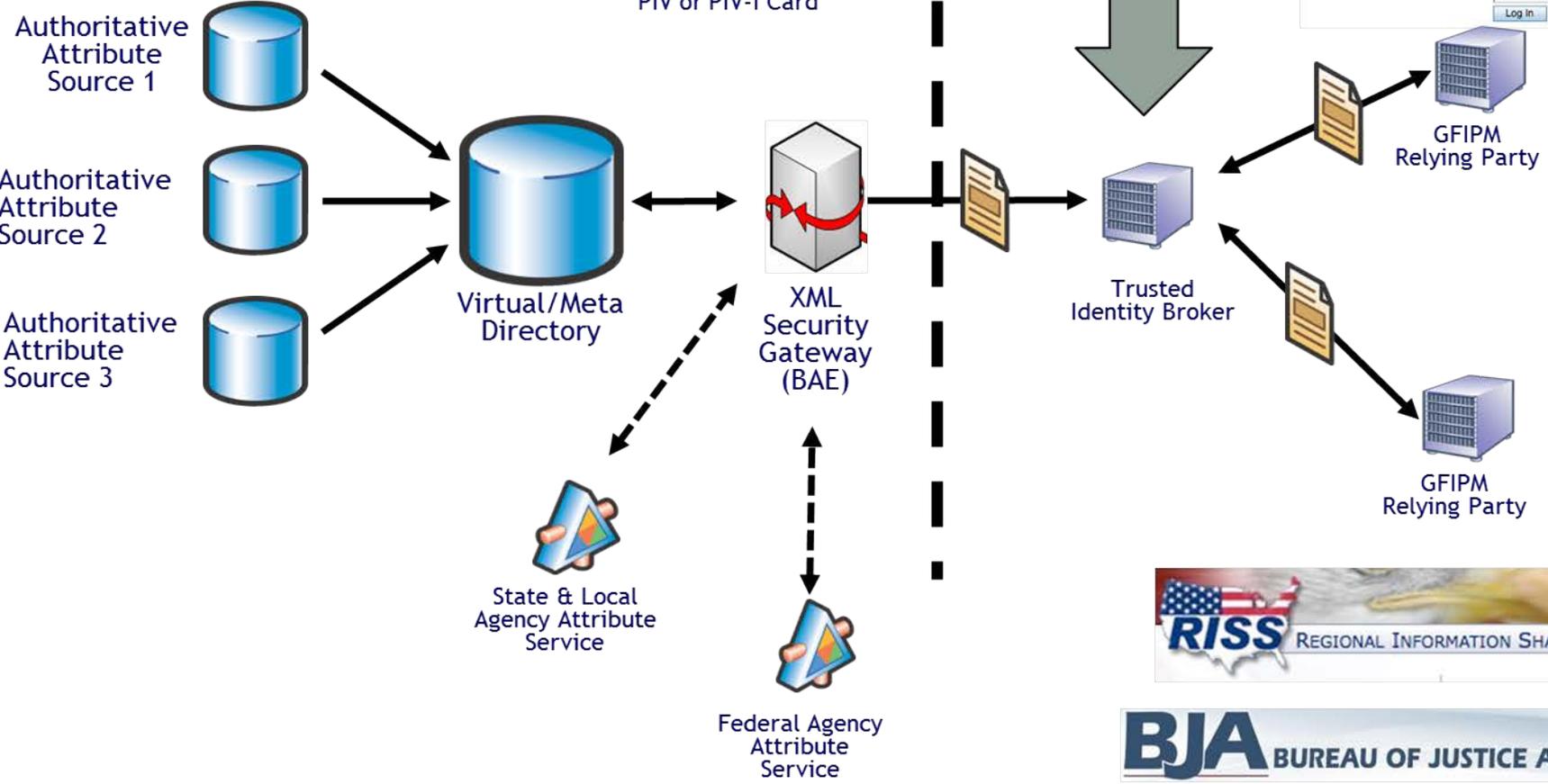- Platform provides interoperability between the reader/control and logical policy decision based on standard (XACML)

System Diagram

BAE and GFIPM interoperability

- 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

National Collegiate Cyber Defense Competition

Resources

- Websites
  - http://www.ahcusa.org/PIV-I%20TTWG.htm
  - https://www.cyber.st.dhs.gov/idmdp.html
  - http://www.idmanagement.gov/documents/BAE_v2_Overview_Document_Final_v1.0.0.pdf

Contact Information

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