CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS

DHS S&T
IdM Testbed Activities

JHU/APL

09/18/2013

Team Profile
- Johns Hopkins University Applied Physics Lab

APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

What Are We?

- Division of Johns Hopkins University
- University Affiliated Research Center
- Trusted Agent

Who Are We?

- Technically skilled and operationally oriented
- Objective and independent

Who Are Our Sponsors?

- DoD
- NASA
- Other Federal/State
- DHS
- IC

What Is Our Goal?

- Critical Contributions to Critical Challenges

Statistics

Employees: >5,000 Staff

Revenues: >$1.1B

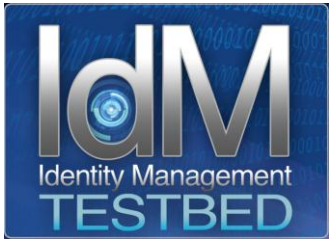
393 acre campus in Howard County, MD

Customer Need

- Customers
  - Federal (DISA, NSA, DOL, GSA, BJA, FEMA, TSA…)
  - State and local (VA, WV, Chester Co PA…)
  - Vendors (Radiant Logic, Layer 7, Oracle, ID Dataweb…)
- Needs
  - Real-time, fine grained, and situational access control
    - Logical, Physical, and Unified
    - Federated
  - Federal ICAM compliance
    - Roadmap Guidance
    - Product Verticals
      - Standardization (OASIS, NIST, IETF…)
      - Cross-product Integration
  - Cost effective solutions
    - Vendor and Open Source

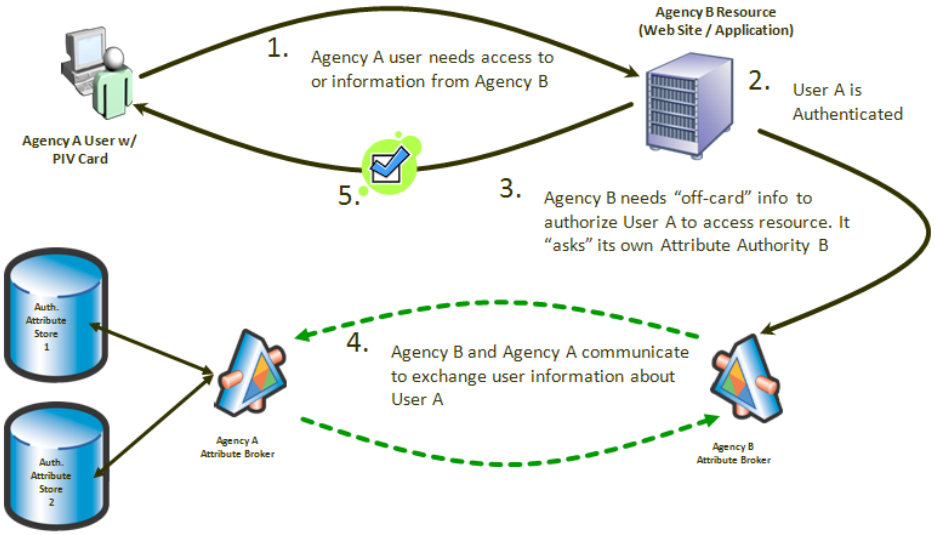
Approach

- Identity, Credential, and Access Management (ICAM) R&D
  - Technology Evaluation
    - Guide developers in implementing standards based enhancements
    - Mitigate technical risk and demonstrate utility
    - Identify product integration issues
    - Identify areas for research investment
  - Systems Engineering
    - Explore architectural approaches and models
    - Develop proof-of-concepts, reference architectures, best-practices, lessons learned
- Collaborating across the community
  - Government: Federal, State, Local and Regional
  - Standards Bodies
  - Commercial Sector / Vendors
  - Open source
  - Analyst firms



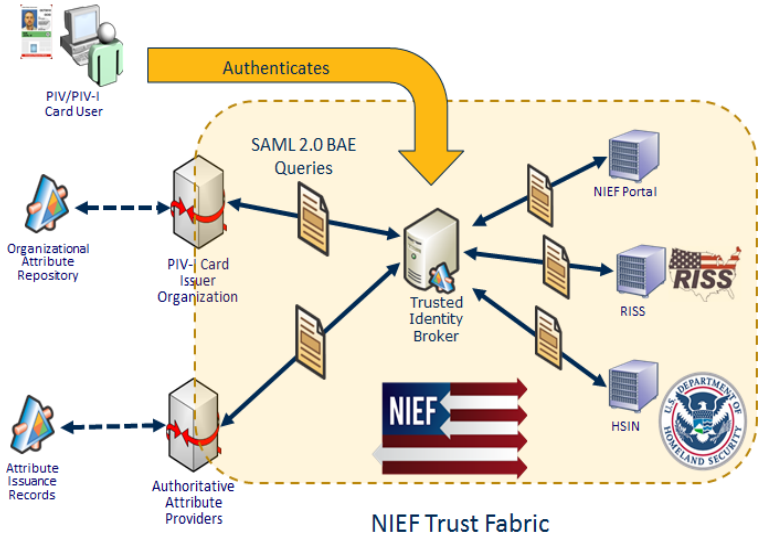
Approach
- BAE Single-User Attribute Retrieval

- **Developed SAML 2.0 Profile of BAE**
  - Prototyped GSA HSPD12 specification as v1.0 standard
  - Defense Manpower Data Center (DMDC) Pilot
  - Incorporated into the FICAM Segment Architecture Roadmap by the Federal CIO Council ICAM Subcommittee (SC)
  - Added lessons learned into v2.0
- **FICAM Reference Implementation**
  - Privilege Management Pilot
    - DHS (S&T, OCIO, PKI, FEMA, HSIN)
    - DOD (NORTHCOM, NSA, DISA)
  - Digital Policy Analysis (MIT)
  - Layer 7 (COTS) Beta Testing
  - GFIPM PIV/PIV-I Interoperability Demo (GTRI)
- **Interoperability T&E**
  - Vendor
    - Layer 7, Oracle, Axiomatics, Intel, Verizon
  - Government
    - BJA (IIR), DOJ (GFIPM/GTRI), USDA, DC Government, STRAC, Chester Co PA, West Virginia



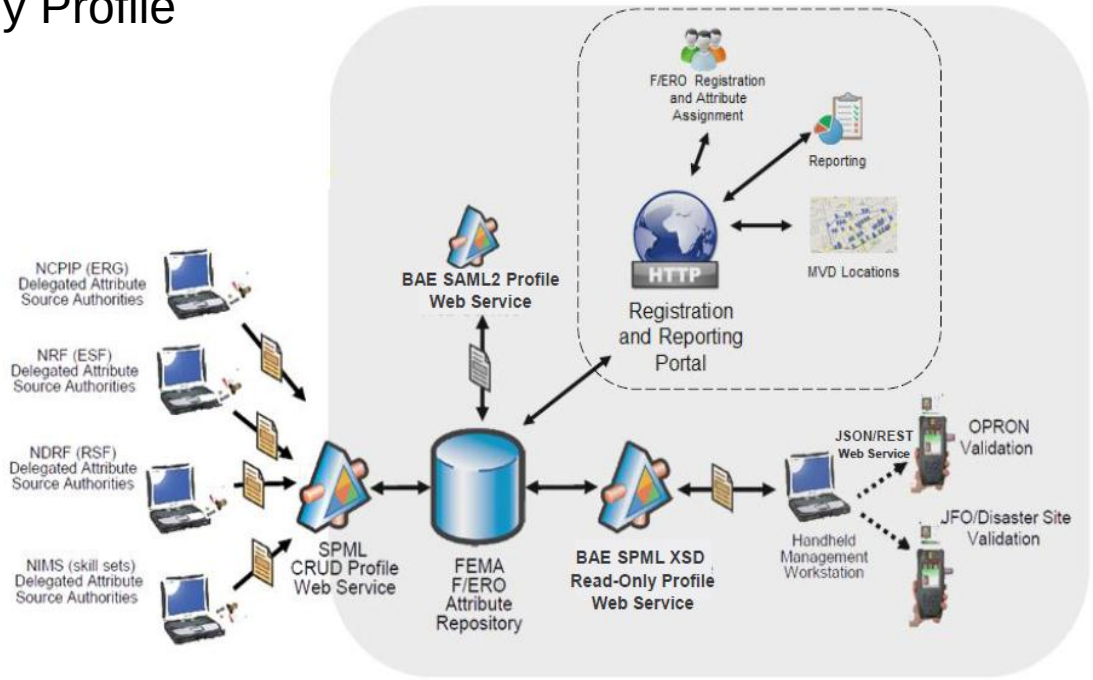
Approach
- GFIPM and PIV/PIV-I Interoperability

- **Need**
  - National Identity Exchange Federation (NIEF) access for PIV/PIV-I card holders
- **BAE Reference Implementation**
  - Developed synthetic NIEF users
    - Added NIEF attributes
    - NIST test cards
  - Provisioned GTRI
- **GTRI updated the Trusted Identity Broker**
  - Support PIV/PIV-I credential authentication
  - Support SAML 2.0 BAE attribute retrieval
- **Interoperability T&E**
  - Demonstration at https://piv.ref.gfipm.net
  - Pilot with BJA (28 CFR Certification) and Texas Department of Public Safety for RISS access



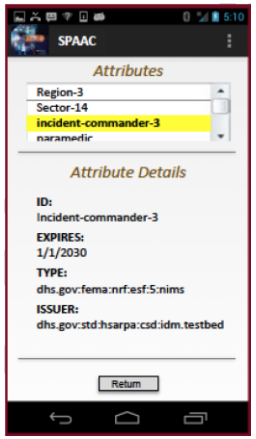
Approach
- BAE Multi-User Attribute Retrieval

- **Developed Read-Only Profile of BAE**
  - Prototyped SPML DSML Read-Only Profile
  - F/ERO Pilot with Chester Co PA
  - Submitted to ICAM-SC for the FICAM Segment Architecture Roadmap
  - SME for CTC Operational F/ERO
    - SPML XSD Read-Only Profile
    - JSON over REST
- **Reference Implementation**
  - WV F/ERO Pilot
  - Radiant Logic (COTS)
    - SPML DSML
      Beta Testing
- **Interoperability T&E**
  - FEMA F/ERO Repository



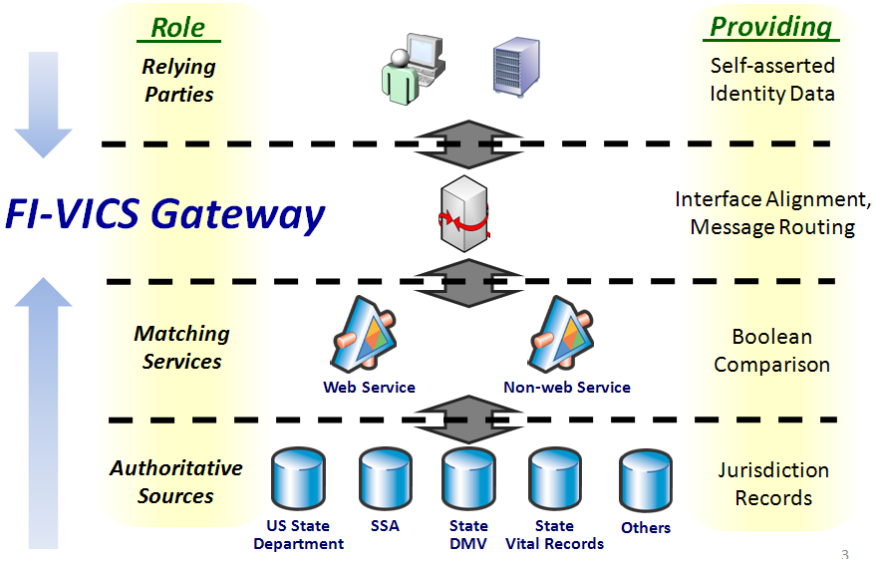
Approach
- Physical Access Control on the Tactical Edge

- **Need**
  - Use mobile handhelds available at incident scene
  - “An app for that”
- **Develop**
  - SmartPhone Attribute-based Access Control (SPAAC)
    - Android smartphones and tablets
    - PIV/PIV-I/CAC authentication
    - Wireless attribute retrieval
- **Interoperability T&E**
  - Proof-of-Concept Demonstration
    - DHS S&T IdM Testbed
  - Interoperability demonstration
    - F/ERO Repository Testbed (CTC)



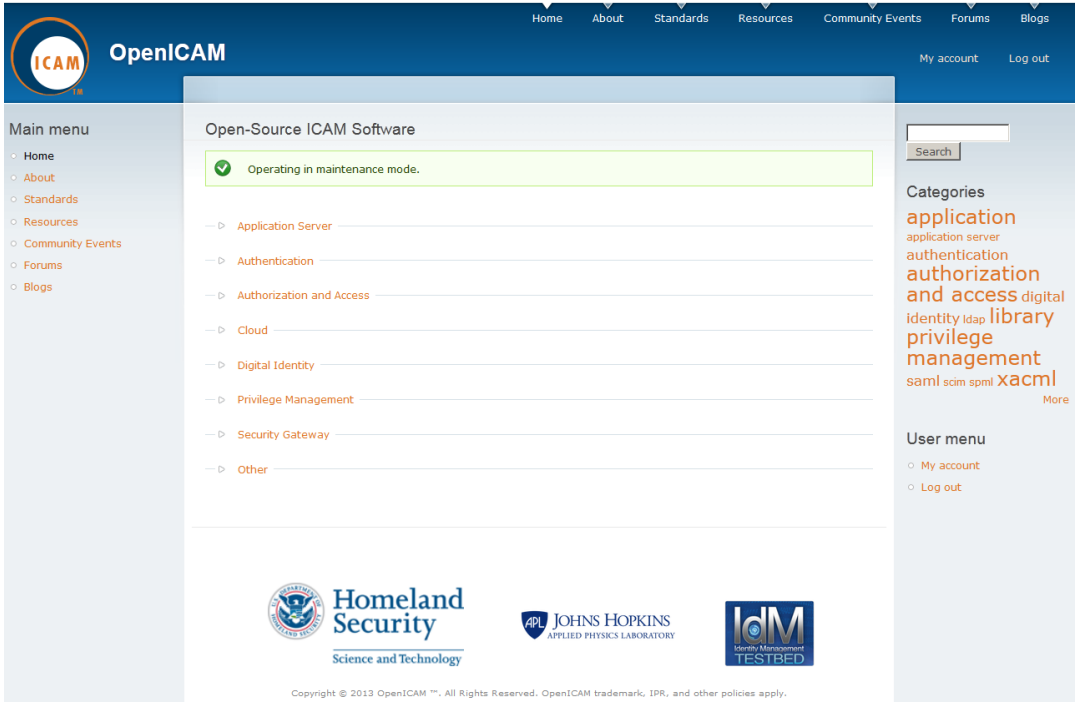
Approach
- Verifying Identity Credentials Service (VICS)

- **Developed Profile**
  - Architect *Subject Assertion Verification* Transaction Flow
    - Financial Services Sector Coordinating Council (FCSSC)
    - National Institute of Standards and Technology (NIST)
  - Prototyped XACML 3.0 Subject Assertion Verification Profile
- **Reference Implementation**
  - Interoperability T&E
    - American Association of Motor Vehicle Administrators
    - Florida
- **Value T&E**
  - Early Warning Systems (EWS)

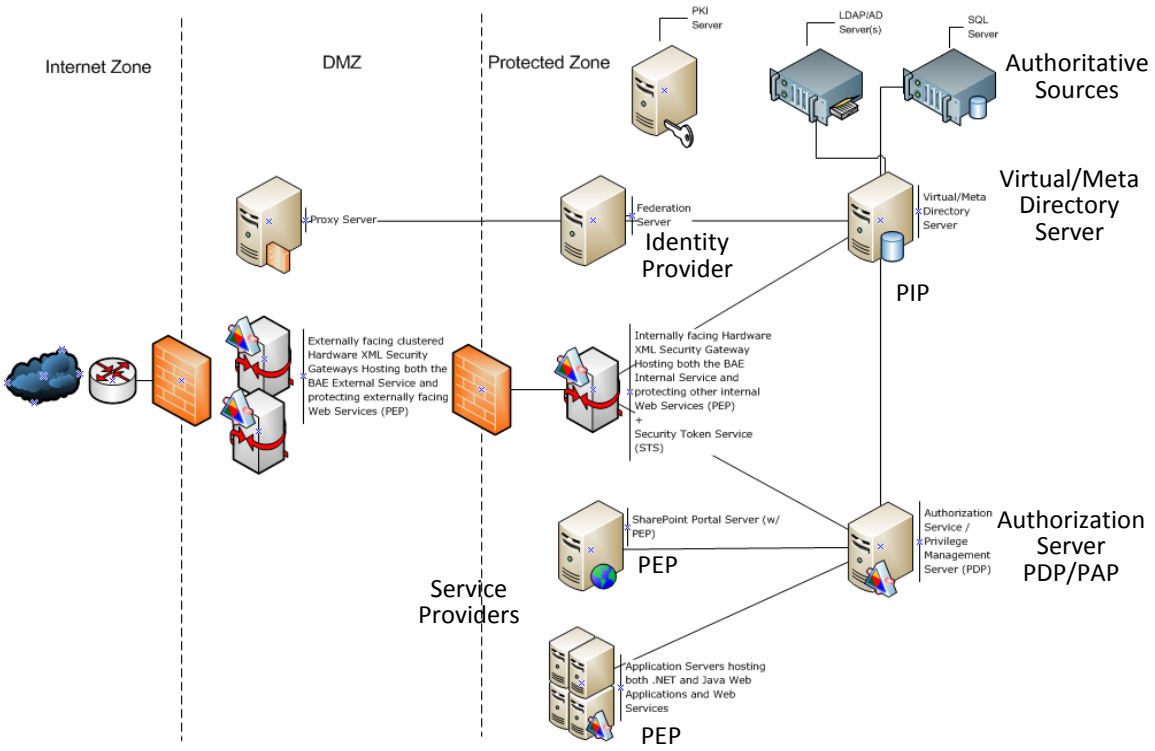


Approach
- OpenICAM.org

- **Create a Resource for the ICAM Community & Developers**
  - OpenICAM.org launched August 2013
- **OpenICAM.org – a Collaborative site**
  - Open Source ICAM Software
    - Categorized by type
    - Relationship to FICAM, NIST, & standards
    - Reviews
    - Links
  - Community Resources
    - ICAM events
    - ICAM standards
    - Forum



Benefits
- DHS S&T IdM Testbed



- **Standards promote interoperability**
- **Reference architectures provide solutions**
- **Collaboration builds acceptance**

Current Status

- BAE
  - SAML Profile
    - Accepted by ICAM Subcommittee under the Federal CIO – Jun 2009
  - SPML DSML Read-Only Profile
    - Submitted to ICAM-SC under the Federal CIO – Sep 2012
- VICS
  - Proof-of-concept Presentation and Demo – Aug 2012
  - Paper and Presentation at ID360 – Apr 2013
  - Final Report and Transition Package – Aug 2013
- Open Source
  - FASC-N encoder/decoder tool - 2010
  - VICS Gateway Library - Aug 2013
  - OpenICAM.org – Sep 2013
- FEMA F/ERO Repository design and operational transition – 2012
- SPAAC Android App
  - Proof-of-concept Demonstration – Dec 2012
  - Interoperability Demonstration – Mar 2013

Next Steps

- F/ERO Repository Operational Capability
  - Submit SPML XSD Read-Only Profile to ICAM-SC
  - Mobile BAE profile
  - Investigate System for Cross-domain Identity Management (SCIM)
  - Law Enforcement Officer (LEO) Biometric Access Management System
    - TSA LEO flying armed use case
- Enabling PIV/PIV-I and FICAM BAE
  - GFIPM TIB (GTRI)
  - IPAWS clients (NC4)
- Open Source Development
  - SPAAC Android Application and enhancements
  - SAML BAE client, server, and testing harness
  - BAE standard for mobile clients
  - PIV/PIV-I reading and authentication tools

Contact Information

- Tom.Smith@jhuapl.edu, Technical Lead
- Maria.Vachino@jhuapl.edu, Project Manager