DHS
&
Identity Management

Anil John

Telephone: (443) 778-0612
Email: anil.john@jhuapl.edu

APL

Identity Management (IdM) is a cross-cutting focus area for DHS

Enabling Homeland Capabilities

- EHC #1: Cross-Agency Information Distribution
- EHC #2: Dynamic Data Processing, Fusion, and Visualization
- Cross-Cutting EHC Projects
  - **Network Identity Management**
  - Data Privacy Technologies

The IdM S&T Project IPT provides a cross-component collaborative mechanism

- Information Sharing
- Identify DHS-wide IdM research requirements (Medium to Long Term i.e. 1-5 Years)
- Identify DHS technology acquisition plans that may benefit from S&T support. Support may include:
  - Research & Development
  - SME & Engineering Support
  - Exploration of architectural approaches to IdM
  - T&E, validation of technologies and technical approaches via the DHS S&T IdM Testbed

3

Implementation priorities may differ across the Enterprise, Components & External partners

4

"Develop a highly scalable architecture for managing identities, rights, and authorities used within and external to DHS"

5

Which brings us to…
- Agenda

- S&T IdM Project
  - Priorities
  - Stakeholders
  - Challenges
  - Research and T&E
  - IdM Testbed
  - IdM Community of Practice
- Backup Slides
  - The many faces of IdM
  - Current IdM Projects
  - IdM Standards

6

DHS S&T IdM Project IPT
- IdM Research and T&E Selection Principles

7

DHS S&T IdM Project IPT
- IdM Research Topic Selection Principles

- Internally facing and externally facing research topics are NOT mutually exclusive
- S&T IdM research and T&E should:
  - Provide a link between existing IdM projects and DHS operational needs that require IdM capabilities
  - Provide recommendations to current projects on architectural and/or technology choices that will align them with DHS Enterprise goals
  - Help to mitigate risks related to choices in technology approaches
  - Leverage industry and partner best practices

8

DHS S&T IdM Project IPT
- DHS Stakeholders

DHS/CIO
- Responsible for overall policy and guidance on implementing identity management solutions within the DHS enterprise

Intelligence and Analysis (I&A) CIO
- Responsible for developing and implementing an identity management solution for classified networks in DHS and ensuring that all DHS identity management solutions are compatible with those of other agencies at the federal and state level

Immigration and Customs Enforcement (ICE)/CIO
- Identified by DHS/CIO as the steward organization for developing and implementing a single sign-on solution for the DHS Enterprise

DHS Science &Technology (S&T)
- Responsible for providing research, development, test and evaluation to assist DHS identity management stakeholders with efficient and effective design and implementation of an identity management system for homeland security

Identity store owners
- Individuals throughout the homeland security community who manage, safeguard, and share within policy limits information about the personnel within their cognizance

Application owners
- Individuals throughout the homeland security community who develop and maintain applications which rely upon authentication of users against identity stores.

Others?

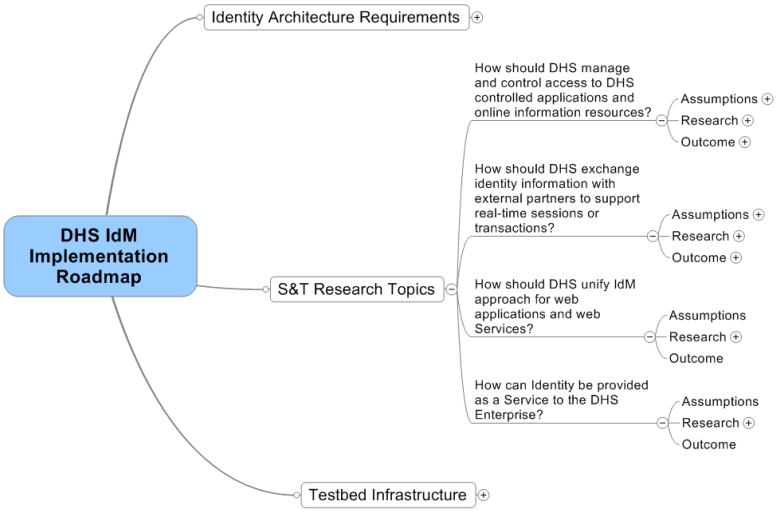
9

DHS S&T IdM Project IPT
- Key Challenges

- Synchronization of information regarding identity management activities across DHS, DOJ, DOD, IC, and other agencies
- Reconciling short term and long term needs of various DHS components
- Ensure standards-based identity federation to solve the information sharing needs of DHS
- Overcoming the concerns of identity store and application owners

10

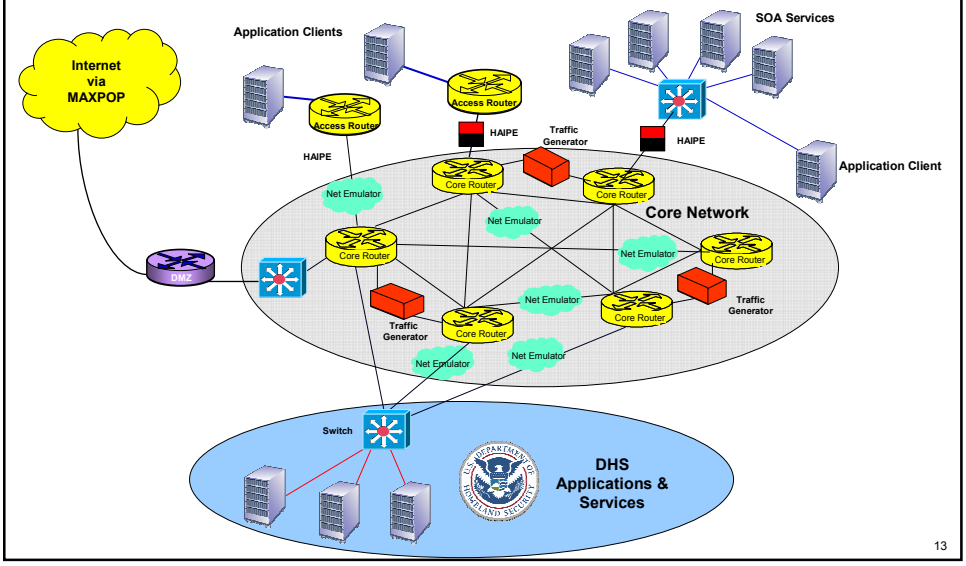
DHS S&T IdM Project IPT
- Research and T&E Topics



11

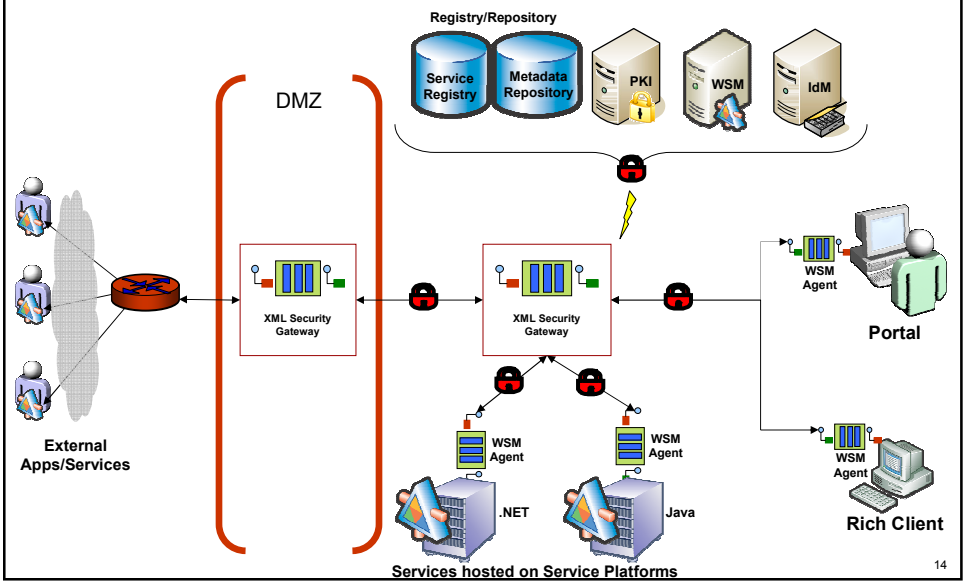
To Seek Identity Management Solutions…
To Boldly Go…

DHS S&T IdM Testbed
= S&T Lab Facilities + APL SOA Testbed



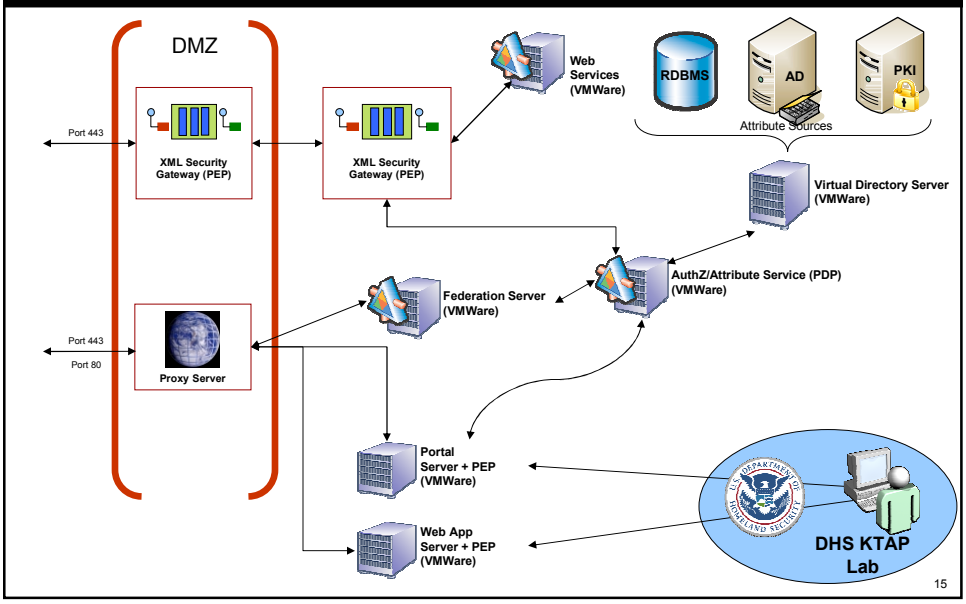
13

DHS S&T IdM Testbed
- SOA Infrastructure



14

DHS S&T IdM Testbed (In Progress)
- IdM Infrastructure



IdM Community of Practice Listserv
- Sharing & Keeping up on IdM information

- Share news, events and other items of interest in the area of IdM
- Explore, ask questions and share industry and community best practices, lessons learned, standards etc.
- To subscribe:

Send an e-mail to:
LISTSERV@LISTSERV.jhuapl.edu
With the following in the message body:
subscribe IdM-L

16

Points of Contact

- Karyn Higa
  - DHS Program Manager
  - Karyn.Higa@dhs.gov
- Terry Gantenbein
  - Project Manager
  - Terry.Gantenbein@jhuapl.edu
  - (443) 778-6504
- Anil John
  - Technical Lead
  - Anil.John@jhuapl.edu
  - (443) 778-0612

17

JOHNS HOPKINS UNIVERSITY
Applied Physics Laboratory

JHU/APL - http://www.jhuapl.edu

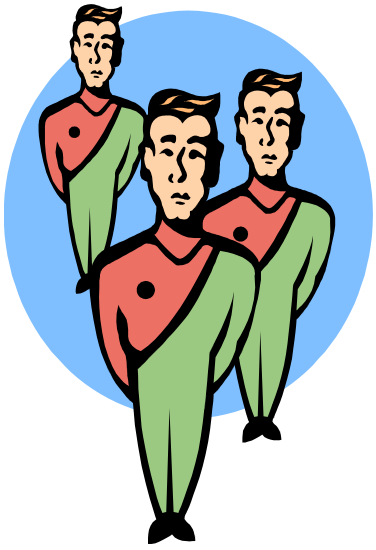
- Not-for-profit university research & development laboratory
- Division of the Johns Hopkins University founded in 1942
- Staffing: 4,000 employees (69% scientists & engineers)
- Comprehensive Knowledge of Sponsors' Requirements & Applicable Disciplines
- **Independence & Objectivity *(no conflicts of interest)***
- Current Operational Experience
- Responsive To Sponsors' Requirements & Schedules
- Broad Access To & Protection Of Sensitive Proprietary Information
- On-site graduate engineering program in 8 degree fields

18

Backup Slides

19

What is Identity Management?
- The Many Faces of IdM…



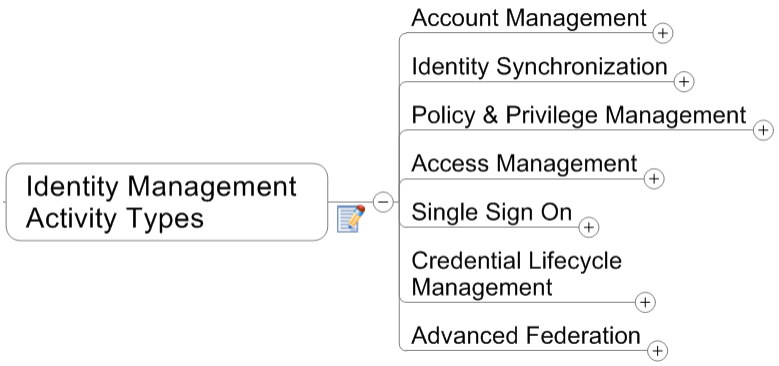
Identity management is the set of business processes, and a supporting infrastructure, that provides:

- identity-based access control to systems and resources
- in accordance with established policies

{ Content Courtesy: Burton Group }

20

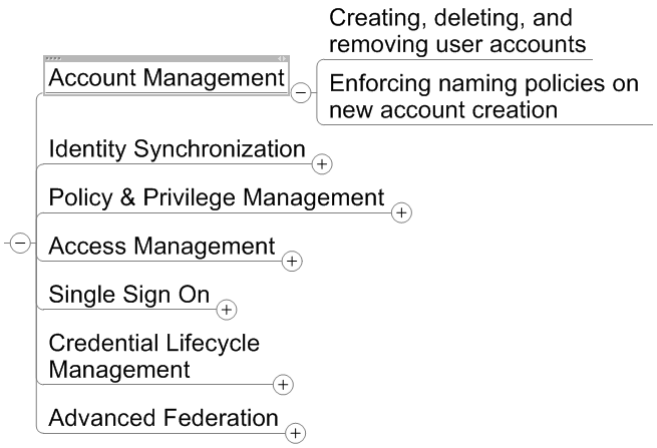
What is Identity Management?
- Typical Activity Types



{ Content Courtesy: Burton Group }

21

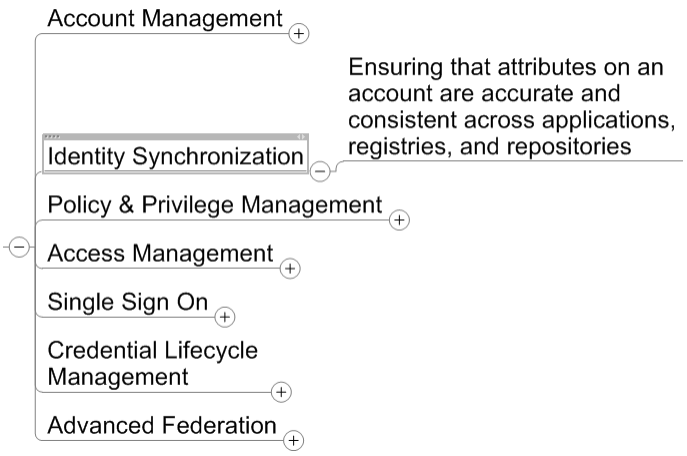
Identity Management Activity
- Account Management



{ Content Courtesy: Burton Group }

22

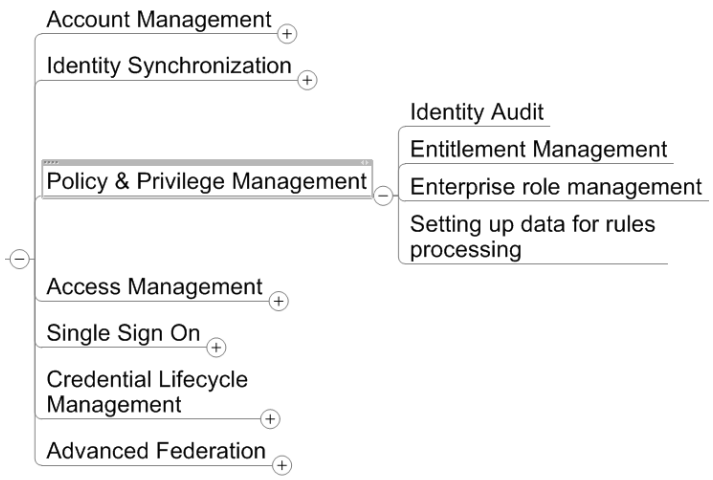
Identity Management Activity
- Identity Synchronization



Content Courtesy: Burton Group

23

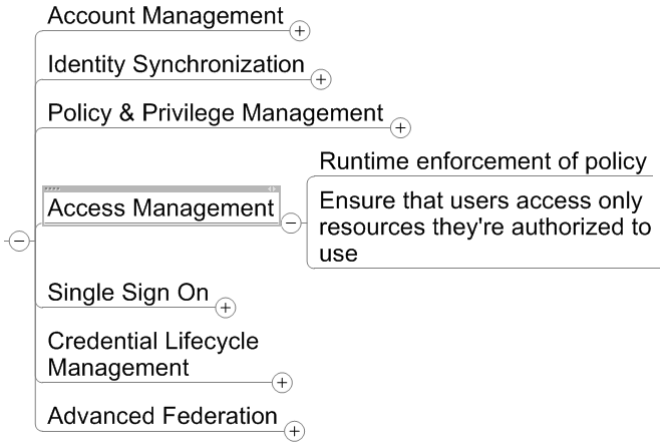
Identity Management Activity
- Policy & Privilege Management



Content Courtesy: Burton Group

24

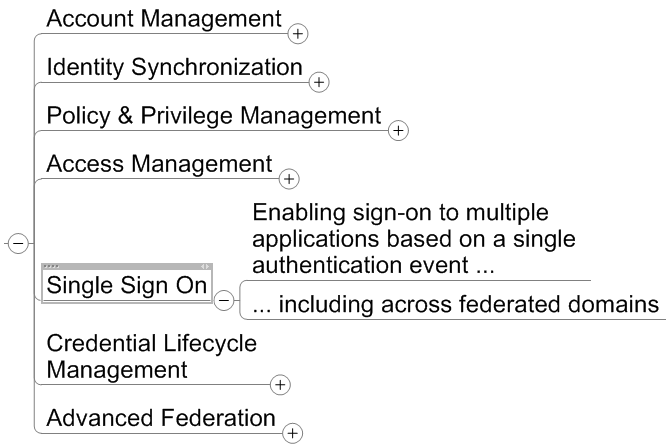
Identity Management Activity
- Access Management



{ Content Courtesy: Burton Group }

25

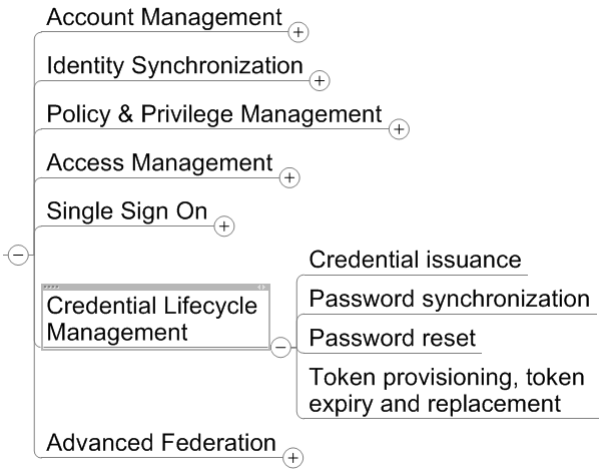
Identity Management Activity
- Single Sign-On



{ Content Courtesy: Burton Group }

26

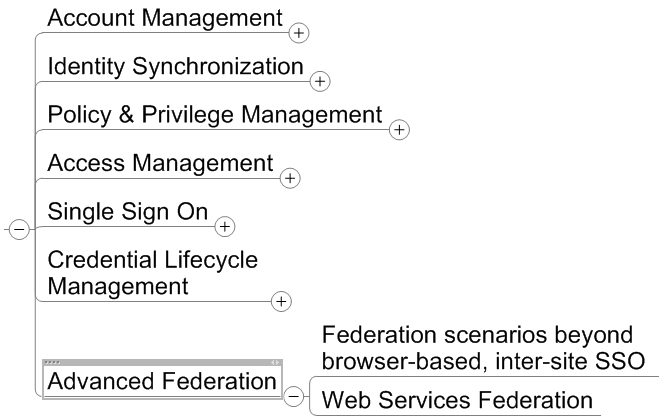
Identity Management Activity
- Credential Lifecycle Management



{ Content Courtesy: Burton Group }

27

Identity Management Activity
- Advanced Federation



{ Content Courtesy: Burton Group }

28

Current IdM Projects
- A Common Framework for Questions

- Who?
- What?
- Activity Type?
- Implementation Technology?
- Status

29

IdM Projects
- What activities are they working on?

	Account Mgmt.	Identity Synch.	P & P Mgmt.	Access Mgmt.	SSO*	Credential Mgmt	Advanced Fed.
ICABAAD		✓	✓				
JEDS		✓					
DHS SSO				✓	✓	✓	
GFIPM				✓	✓		✓
LEISP					✓		✓
PRIV. MGMT.			✓	✓			
TPIAS				✓			
CVS	✓						

30

IdM & Standards

31

Standards allow for flexibility and vendor diversity

Standards Organizations

33

IdM Standards

- Security Assertion Markup Language (SAML)
  - Assertions
  - Protocol
- OpenID
- InfoCard
- Web Services Secure Exchange (WS-SX)
  - WS-Trust
  - WS-SecureConversation
- Web Services Federation (WS-Federation)
- eXtensible Access Control Markup Language (XACML)
- Web Services Policy (WS-Policy)
  - WS-PolicyAttachment

34