Applying Identity Federation to Enable Secure Information Sharing

“A Case Study on Identity Federation between NASA and Lockheed Martin”

Presented By: Anthony Bass, Lockheed Martin
In collaboration with: Dennis Kay, NASA ICAM
In this session we will ...

• Discuss NASA Business Driver & Requirements
• Identify Project Timeline & Risks
• Follow the Six Steps Used to Establish Trust
• See a demo of the In-Production Solution
• Hear Experience & Lessons Learned
• Have time for Audience Q&A
Business Problem

- NASA’s major programs aligned with the nation’s exploration objectives involve extensive collaboration with commercial and academia partners.

- Information exchange takes place...
  - Between geographically dispersed sites
  - Among collaborators of various roles and responsibilities
  - Throughout the Programs’ lifecycles

- Program execution requires extensive exchange of design, configuration and change management information while maintaining integrity and confidentiality.

- Traditional means of managing identity for business partners no longer cost effective and does not align with ICAM Strategy.
High Level Requirements

• Increase Security for NASA Programs & Applications
  - Align to Federal ICAM approved identity and credentialing methodologies
  - Higher Identity Assurance (Overall Identity Assurance Level 3)
  - Strong 2-Factor Authentication (e.g., Smart Card)
  - Higher quality attributes asserted directly by “Sponsored Organization”
  - Map to existing Role-based Access Controls (RBAC) & Entitlements Management

• Reduce 3rd Party Credentialing Costs to NASA Programs
  - Need a sensible approach to accept Non-Federally Issued (NFI) Credentials
  - Reduce End User complexity
  - Reduce Account Management & Support Costs
  - Leverage Industry Standards
Time Frame & Risks

- Need to deliver initial capability within the 2013 fiscal year
- No uniform contract clauses exist that enable use of integrated Identity Federation services to efficiently establish secure collaboration relationships with NASA’s business partners
- ICAM Trust Frameworks were still incubating
- NASA needed a business partner that can operate at Identity Assurance Level 3
- Little experience with Identity Hub Integration

Biggest risk to delivery is that there was “no established precedent”
The Approach

• Selected Exostar as the Identity Hub Provider
  - Proven track record for credentialing and managing small to medium sized suppliers
  - Mature capability to bridge Identity Federation protocols and assertions

• Selected Lockheed Martin as the 1st Business Partner
  - Contractor operating on Orion and GSDO Programs
  - FBCA \ CertiPath Cross-Certified PKI Med HW Credential Issuer
  - LOA3 Identity Provider connected to the Exostar Identity Hub
  - An experienced Relying Party to the Exostar Identity Hub

• NASA Space Act Agreement (SAA) selected to establish the legal basis for trust
  - An established precedent within NASA to support innovative partnerships
  - Well documented and easy to understand by General Counsel of Business Partners
The 6 Steps Used to Execute the Approach

Identity Federation “By the Numbers”

1. Community: Defense Program X
   - Policy Scope: “Simulated” Critical Program Information (SCPI)

2. Partner Y
   - Federation Identity Provider (IdP)
     - Federated Trust Agreement
     - Federated Attribute Synchronization
     - Federated Authentication

3. Partner Z
   - Federation Identity Provider (IdP)
     - Federated Trust Agreement
     - Federated Attribute Synchronization
     - Federated Authentication

4. Federated Service Provider (SP)
   - Authentication Binding
   - Federated Applications
   - Federated Synchronization

5. Community Management
   - Add / Remove

6. Validate Trust
“Sensible” Approach to Establish Trust

• Step 1 - Establish Collaboration Community & Willingness to Trust
  - Lockheed Martin contractually obligated to certain NASA FARs (flow downs)
  - NASA recommended Exostar Hub as the strategy for Federated Identity
  - Goodwill and opportunities emerged from working together in TSCP
    • NASA FICAM sponsored a NASA, Air Force, & LMCO proof of concept demonstration

• Step 2 - Establish Trust (Non-Technical)
  - Required Lockheed Martin to respond to a Security Control Questionnaire
    • Adequate disclosure was required in order to assess “trustworthiness”
    • Deemed “Proprietary Information” and Freedom of Information Act (FOIA) exempt
  - Negotiated Lockheed Martin Space Act Agreement (LM SAA) Partnership
    • Detailed terms, conditions, and limitations of liability for Identity Federation
    • Subject to Freedom of Information Act (FOIA)
  - Lockheed Martin Users
    • Proofed & Vetted by Lockheed Martin @ Medium Identity Assurance
    • Subject to National Crime Information Center (NCIC) Background Check
“Technical” Approach Establish Trust

- **Step 3 - Implement & Test Federation Trusts**
  - Lockheed Martin already “In Production” with Exostar as an “Identity Provider”
  - NASA integrated with Exostar as a “Relying Party”
  - Exostar enabled “Account Linking and Hub Connectivity” between Parties
  - All Parties conducted system and user acceptance testing

- **Step 4 - Pre-provision User Data**
  - LM Users “Just In Time (JIT)” provisioned into Exostar
  - NASA enrolled LMCO Users into Entitlement Management System
  - All Parties may synchronize supplemental user attributes (if required)

- **Step 5 - Community & Entitlement Management**
  - LMCO Org. Administrator initiated onboarding & authorized use of Exostar
  - NASA Administrator invited, reviewed, and approved LM Users to use NASA System
“Verifiable” Approach Maintain Trust

• Step 6 - Trust but Verify
  - Perform to expectations on NASA Programs and Space Act Agreement
  - Support “organic” growth across NASA Programs and Partnerships
  - Maintain Adequate Security Disclosure
    - Annual review & renewal of FOIA-exempt security questionnaire
    - Contribute security thought leadership to Exostar-related forums
    - Apply Lockheed Martin Cyber Kill Chain™ methodologies to proactively remediate and mitigate potential LMCO Insider Cyber Threats
  - Mutual Intent to Optimize
    - Seek out NASA ICAM Approved Trust Frameworks & Security Controls
    - Reduce the labor burden of maintaining multiple bi-lateral agreements
    - Increase scale utilizing existing investments
    - Maintain or decrease related risk levels
The Result: Operational Identity Federation with NASA

**LMCO User**
- Presents *Medium Hardware* FBCA Cross-Certified Credential to LMCO Identity Provider

**LMCO Identity Provider**
- Authenticates Credential
- Asserts User Identity to Exostar

**Exostar**
- Validates Inbound Assertion
- Transitions Federation Protocol
- Issues New Assertion @ NASA Compatible Profile

**NASA Service Provider**
- Validates Inbound Assertion
- Transitions Federation Protocol
- Issues New Assertion @ Application Compatible Profile

**NASA Application**
- Validates Inbound Assertion
- Authorization decisions based upon assertion or pre-provisioned data

**SharePoint 2010**
- Data Lists & Files
- Libraries
- Site \ User Interface
- Site Collection
- Application

**Potential For Expansion**
- Supply Chain (SMB)
- Other NASA Centers

**FBCA Cross-Certified Partners**
- PIV-I
- Med HW
NASA Business Benefits Realized

- Partner identity proofing management and credentialing services can be leveraged, reducing duplication of background checks and local credential issuance.

- The implementation of integrated federated identity and access management services enabled a common framework to provision and remove access to logical assets managed by the respective partners.

- Leveraging standardized guidance reduced the need for partner unique logical access integrations.

- Reduced overhead for technical personnel enabling them to stay focused on performing tasks aligned with program objectives.
Summary of Lessons Learned

• “Program-Level Leadership” is in best position to quantify legal and policy issues that impede Secure Collaboration with Customer and Business Partners (e.g., source of “focused” legal and technical requirements)

• Continue to establish precedence within Legal Communities of Interest
  - Develop uniform contract clauses that enable rapid expansion and use of Identity Federation to secure collaboration relationships (e.g., B2G, B2B)
  - Endorse Trust Frameworks & 3rd Party Assurance Model(s)
  - Model arguments for/against inadvertent or deliberate activity related to Identity & Access of Business Partner Information Systems
  - Help to quantify security controls to support your arguments
  - Sponsor innovations in International Law for the “Internet of Everything”

• Continue to Defend Against the Advanced Persistent Threat
  - Apply sound “Security Engineering” principles, strategies, and techniques
  - Improve event correlation and attribution techniques and technologies
  - Help less capable partners shore up their infrastructure
  - Invest in Programs that inspire security leadership & technical innovation
Thank you for attending!
Sign In

KSC Federation Service

This is a U.S. Government system and is for authorized users only. By accessing and using this computer system, you are consenting to system monitoring, including the monitoring of keystrokes. Unauthorized use of, or access to, this computer system may subject you to disciplinary action and criminal prosecution.

The site that you are accessing requires you to sign in. Select your organization from the following list. If you are unsure of which selection to make, choose KSC Federation Service (recommended).

KSC Federation Service

Exostar

LaunchPad

Smartcard

Privacy Policy & Important Notices
Exostar - Login Selection Page

Sign In

Login
- User ID
- Password
- Login

First Time Login?
- Establish your account

Not Registered Yet?
- Register for Exostar services

Advanced Login Options
- Active One-Time Password Hardware Token
- Phone Based One-Time Password
- Digital Certificates (Software)
- Digital Certificates (Hardware)
- Enterprise Single Sign On (EAS)

Announcements
Need your First Time Login Information?
You can go to our Forgot First Time Login wizard for self service assistance.

Forgot your password?
To retrieve your password, please go to our Password Reset page.
Click here for additional help.

Security Alert
Unauthorized access to this computer system may constitute a criminal offense.
Exostar EAG Connected Home Realms

EAG User Login

Please select an Identity Provider for login:

Lockheed_Martin_US

Login

Enterprise Access Gateway

Enterprise Access Gateway (EAG) is an Exostar service that allows users to access Managed Access Gateway (MAG) and applications and services accessible through MAG using their company issued credentials.

To take advantage of EAG, an organization must be enabled to allow users to link MAG accounts to corporate credentials. EAG roll-out is typically an enterprise-wide activity for which users will be provided notification by their organizations in advance.

For additional information on EAG and to learn about linking MAG accounts, refer to the MAG User Guide, section: "Update Enterprise Access Gateway (EAG) Account Settings".

Terms of Access | Privacy | Contact Us |
Copyright © 2013 Exostar LLC. All rights reserved
Ready to Collaborate