



Engineering, Operations & Technology
Phantom Works

Phantom

Identity Federation for SOAs





Agenda

Boeing AATM | Phantom Works

- **Joint Network Enabled Operations Program**



Joint Network Enabled Operations

Boeing AATM | Phantom Works

- **NEO Mission**
 - Use of Network enabled information systems to advance interagency communication and collaboration
- **Jointly Funded DoD, DHS, DOT**
 - Initial spiral “0” in 2005
 - Current spiral “1” ends 2008
- **Industry Team**
 - Boeing, Raytheon, CSC, LMCO
 - ERAU, TBE, ARINC
- **NEO Challenge**
 - Interagency collaboration is important ...
 - Funding i\$ not Network Centric
- **NEO Value Proposition**
 - Environments dedicated to the development of interagency operations
 - The only NextGen program focused on interagency operations



Premise

Boeing AATM | Phantom Works

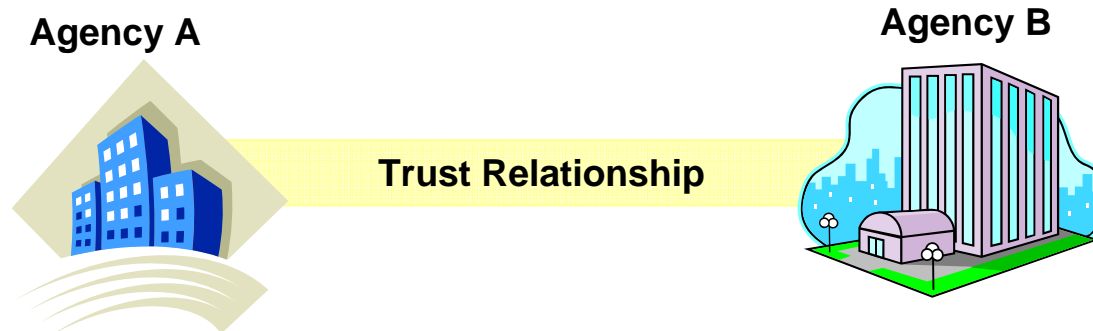
- **NEO program requires interagency collaboration**
 - **Establish FAA - DOD trust relationship**
- **Interagency collaboration complicated by security requirements of multiple agencies**
 - **Data at varied levels of sensitivity, etc.**
- **NextGen security architecture needs to find a way to meet security challenges**
 - **This is a highly complicated task!**
 - **Agencies must be able to control access to their own data and share it with confidence**
- **Federated Identity Management (FIM) provides a way to extend user identities across organizations**
 - **Research and limited experimentation were done to see if FIM could be used to facilitate secure interagency information exchange**



What is Federated Identity Management?

Boeing AATM | Phantom Works

- **FIM – provides cross-organizational, role-based access controls – transformation of local user credentials into standards-based security token that a remote system can trust**
 - **Exchange some token to establish user identity on a remote system**
 - Can use attributes in token to determine user roles and privileges
 - **How can identity federation be useful?**
 - Don't have to replicate or synchronize local user repositories
 - Users need to remember/maintain fewer logon credentials
 - Dynamic access improves efficiency and security
 - **2 Parts – Business agreement & technical implementation**



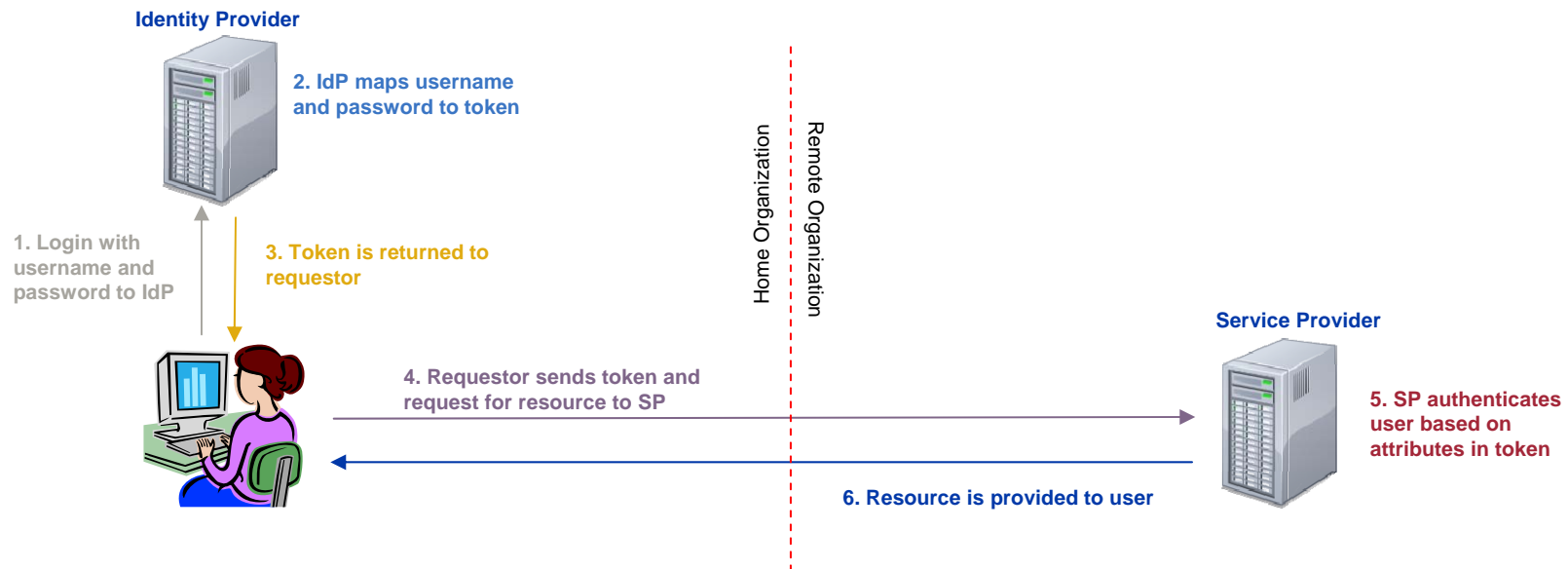


Identity Federation

Boeing AATM | Phantom Works

Steps in establishing a trust relationship

1. Designate identity provider, service provider, and what data they will share
2. Agree upon a token type to exchange
3. Determine how token mapping and generation by identity provider will be done
4. Determine how tokens will be parsed and access decisions will be made by service provide





Enabling Federation – Tokens and SAML

Boeing AATM | Phantom Works

- **Tokens need to be tamper proof and contain some information that the SP will use to make an access decision**
 - **Passwords, biometrics, and certificates are static tokens**
- **SAML – Security Assertion Markup Language**
 - **Dynamically created token type**
 - **OASIS standard for “communicating user authentication, entitlement, and attribute information”**
 - **OASIS Security Services (SAML) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security**
 - **An XML based approach to extension of user credentials**
 - **2 parts – Assertion and Protocol**
 - **We will only use the assertion (token) piece**

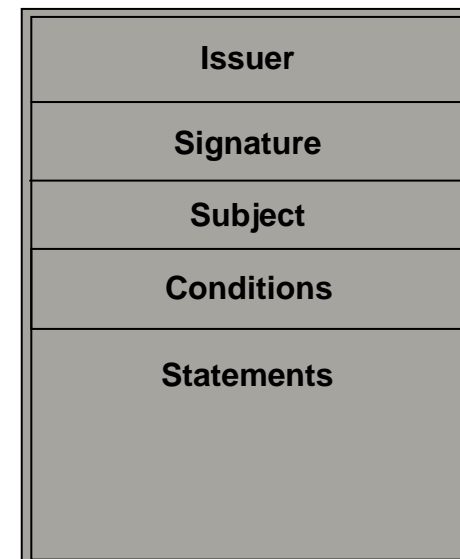


SAML Tokens

Boeing AATM | Phantom Works

- **Assertions contain information that the receiver can use to make an access decision**
 - **Issuer ID**
 - **XML encrypted signature**
 - **Time frame for which the token is valid**
 - **Extensible element**
 - **Group memberships**
 - **Additional user attributes**
 - **Anything else the receiver needs to authenticate the user**

SAML Assertion



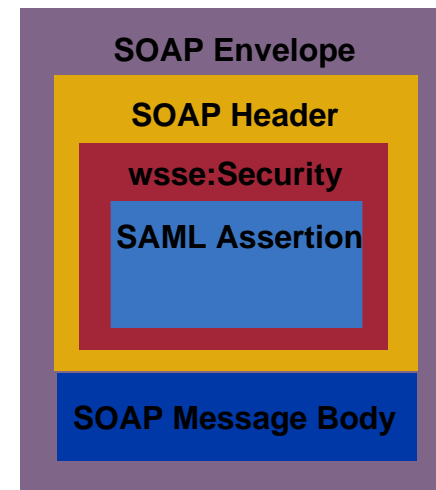


WS-Security

Boeing AATM | Phantom Works

- **WS-Security – OASIS standard that defines security for web services**
 - **3 Parts – Authentication, Encryption, and Integrity**
 - **WS-Security Core Specification 1.1**
 - 5 token profiles – Username, X.509, SAML, Kerberos, and Rights Expression Language (REL)
 - SAML Token profile 1.1 followed in FIM experiment
 - **Tokens are embedded in SOAP message headers**

WS-Security enabled SOAP message with a SAML Token





Experiment Objectives

Boeing AATM | Phantom Works

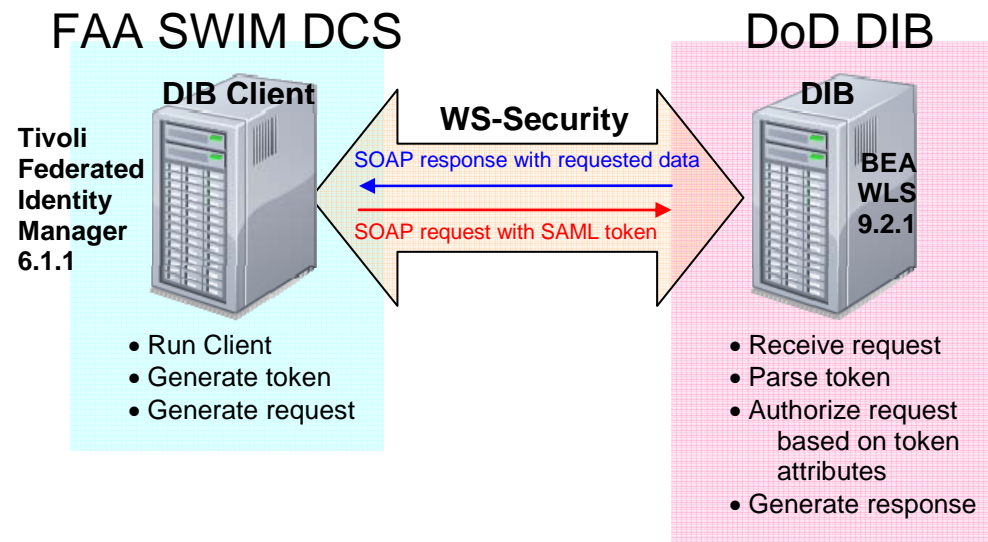
1. Research and learn about Identity Federation and associated technologies
2. Implement cross-vendor federated identity management (FIM) for web services in compliance with the WS-Security SAML token profile



FAA/DoD System Trust Relationship

Boeing AATM | Phantom Works

- **Trust relationship was established between the FAA SWIM DCS and the DOD DIB**
 - **Identity provider = FAA SWIM DCS – Tivoli Federated Identity Manager 6.1 (TFIM)**
 - **Service provider = DOD DIB – BEA WebLogic Server 9.2 (BEA WLS)**





Analysis

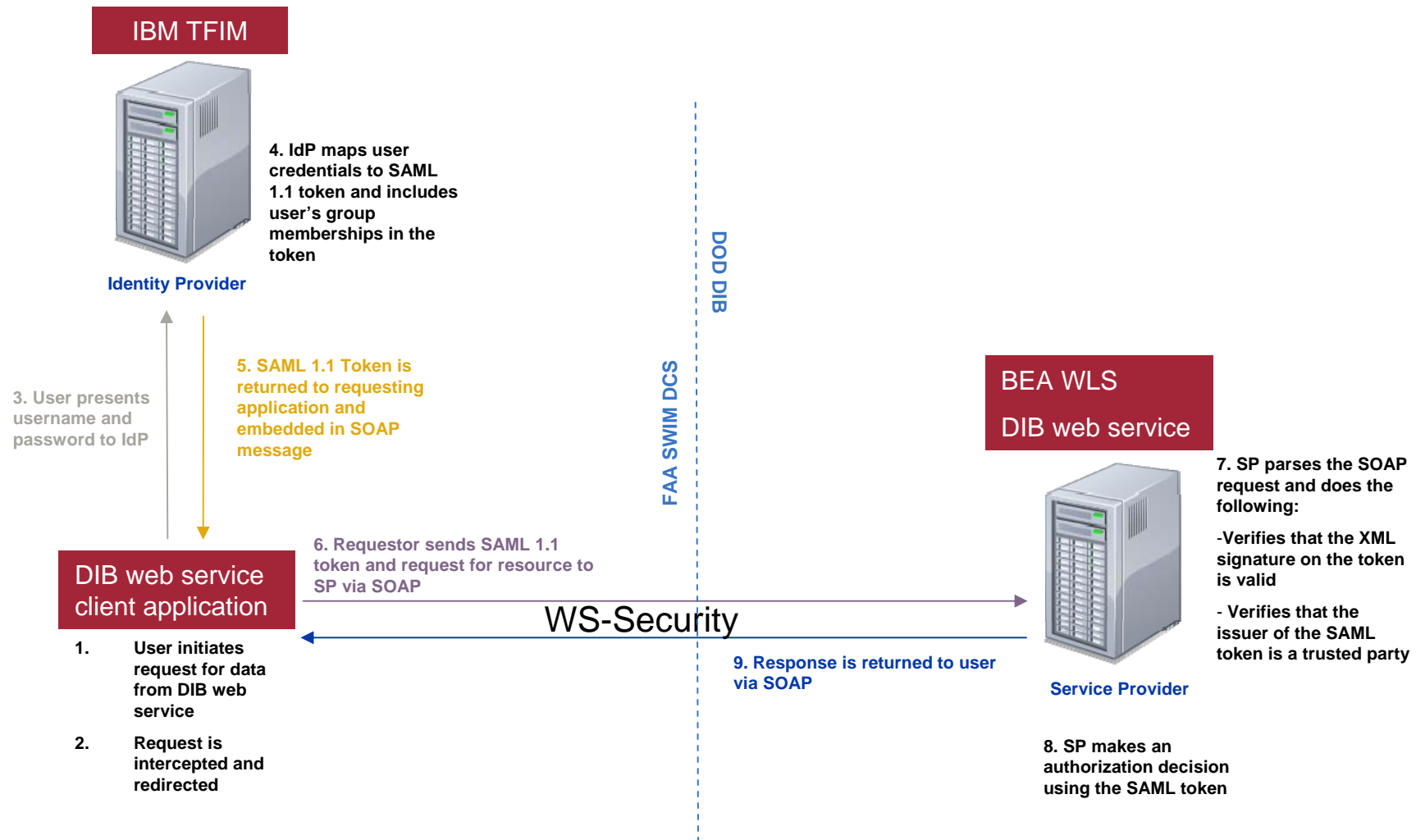
Boeing AATM | Phantom Works

- **Studied FIM, SAML, and WS-Security specification to provide background for subsequent work**
- **Investigated how the WS-Security SAML token profile is implemented by BEA WLS 9.2**
 - **Found that WLS 9.2 only supports SAML 1.1 token type**
 - **SAML 2.0 is supported by BEA WLS 10**
 - **Found that BEA WLS requires that a subject confirmation method of “sender-vouches” or “holder-of-key” be specified in incoming SAML tokens**
- **Investigated how the WS-Security SAML token profile is implemented by IBM TFIM 6.1**
 - **Found that TFIM does not, by default, include a subject confirmation element in the SAML tokens it generates**
 - **This discrepancy between BEA WLS and IBM TFIM’s implementations of the WS-Security SAML token profile specification would prove to be a major complication**



Token Exchange Design

Boeing AATM | Phantom Works





Implementation

Boeing AATM | Phantom Works

- **Took over 320 hours of work to implement the design**
- **It was necessary to obtain assistance directly from the vendors (BEA and IBM) for both identity federation products**
 - **Using the BEA system, developers were able to receive and validate SAML tokens, per the WS-Security SAML token profile using an example provided by BEA support**
 - **It was necessary to bring an IBM consultant onto the team to code a custom token mapping module for TFIM so that the subject confirmation element would be included in SAML tokens bound for the BEA system**



Results

Boeing AATM | Phantom Works

- **Design was successfully implemented**
 - **Users of the FAA SWIM DCS were able to use a simple client application to access data on the DOD DIB using their local system credentials**
 - **Credential mapping, token issuing, and user authentication to the DIB all happened automatically in the background and went completely unnoticed by the users**
 - **User experience was greatly improved and data was shared securely**
- **Team learned about and gained experience working with WS-Security, SAML, and FIM**



Conclusion

Boeing AATM | Phantom Works

- **FIM has great potential to provide more efficient, secure information sharing for SOAs**
 - **Still labor intensive and costly to implement**
 - **Vendor interoperability out-of-the box is not guaranteed**
 - **Tools need to further evolve to make implementation and maintenance more efficient**
 - **Continued research to follow the evolution of FIM and associated tools is recommended**



References

Boeing AATM | Phantom Works

- **OASIS Security Services (SAML) TC**
 - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
- **OASIS Web Services Security (WSS) TC**
 - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss