

Cryptologic Systems Group

“Securing the Global Information Grid (GIG)”

AF SOA IIB Pilot Security Approach & Lessons Learned



Michael Leonard

CPSG/NI

May 21, 2009

Unclassified



Overview



-
- ◆ IIB / SMI-ELS Background
 - ◆ Federation & WS-Trust Security Flows
 - ◆ IIB Configuration
 - ◆ Resources for Service Developers
 - ◆ Lessons Learned
 - ◆ IIB Challenges



SMI-ELS Vision



The SMI-ELS vision is to support Warfighter mission assurance by providing access to mission critical information through secure, trusted sharing mechanisms that protect the integrity of the information from its creation to its utilization by the Warfighter

SMI-ELS will accomplish this mission assurance through the implementation of the two components of SMI-ELS, the Singularly Managed Infrastructure and the Enterprise Level Security



CPSG Support to SOA IIB Pilot



- ◆ **SAF/XC driven initiative**
- ◆ **CPSG support focused on PKI, Identity Federation and Security Token Services**
- ◆ **Accomplishments & Ongoing Activities**
 - Supported AF SOA IIB Spiral 1&2 activity managed by 554th ELSW
 - Supporting IIB extended pilot security and performance/load testing
 - Supported installation & configuration of Identity Federation, Security Token Service (STS) capabilities in Surrogate Forest, Pods A & B at DISA DECC in San Antonio and Pod C in DISA DECC in Montgomery
 - Supporting standup of future installs in AFNET (Scott AFB APC) & on SIPRNET
 - Supported Interoperability demonstrations between PingFederate (IIB Federation Server) and the IBM and Oracle Identity Federation products
 - Supporting GCSS-AF and AF SOA IIB Identity Federation effort



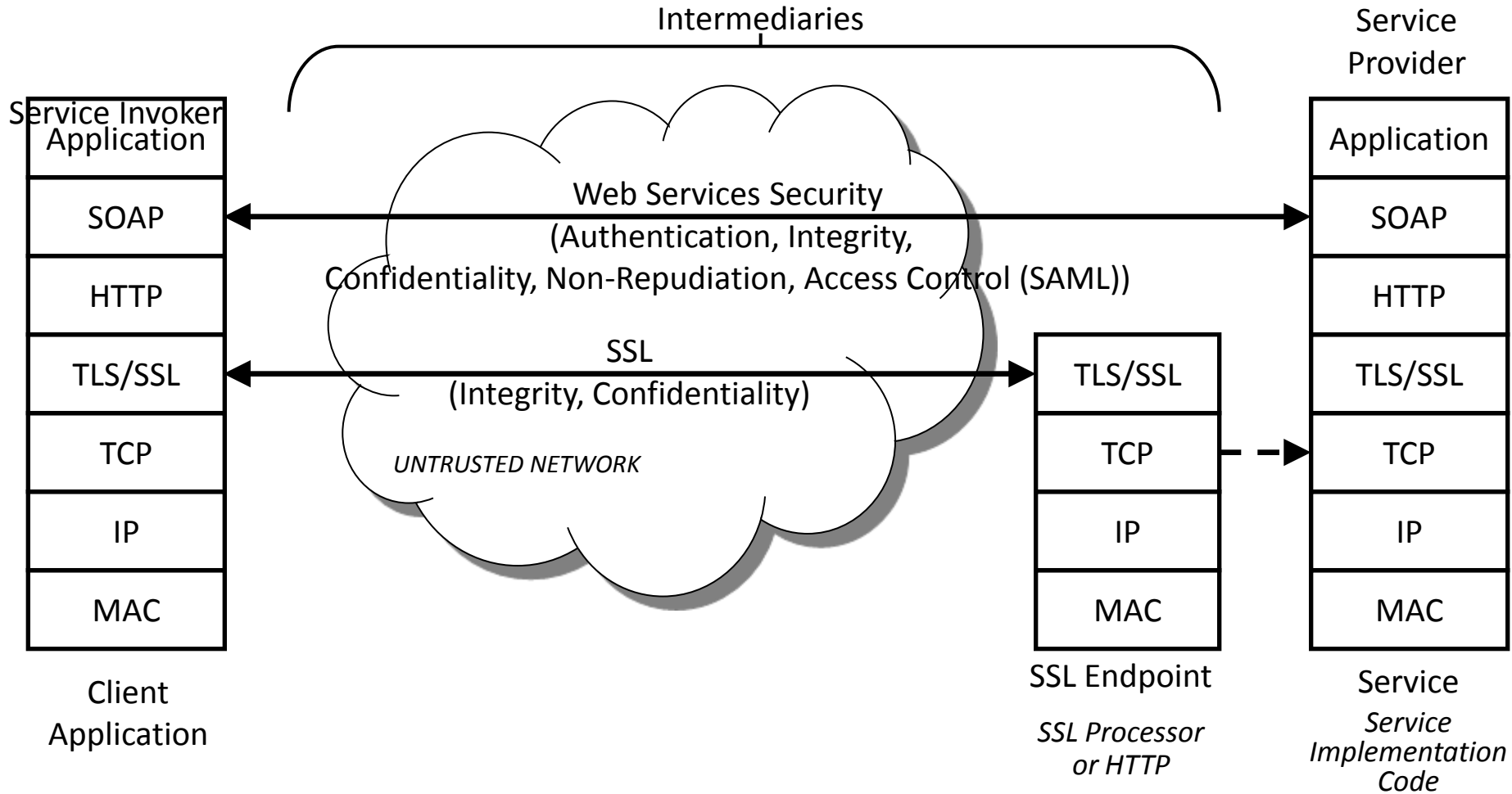
Requirements Snapshot (Spiral 1/2 of IIB Pilot)



- ◆ Common Criteria
- ◆ FIPS 140-2 HSM
- ◆ WS-Federation
- ◆ SAML 2.0 Federation
- ◆ SAML 1.1 Federation
- ◆ WS-Trust
- ◆ WS-Security
- ◆ Ability to support signed and/or encrypted SAML 2.0 assertions
- ◆ SSL/TLS
- ◆ Integration with .NET & J2EE Apps / Services
- ◆ Support user authentication to IdP via PKI, IWA or Forms based authentication
- ◆ Interoperable with DoD PKI
- ◆ Web Service client authentication via PKI
- ◆ Integration with LDAP data store / AD
- ◆ Support multi-valued attributes, and ability to prune attributes based on target application / service
- ◆ Revocation Status checking via OCSP / DoD RCVS
- ◆ Support High Availability
- ◆ Support expected Enterprise Load through clustering / load balancing



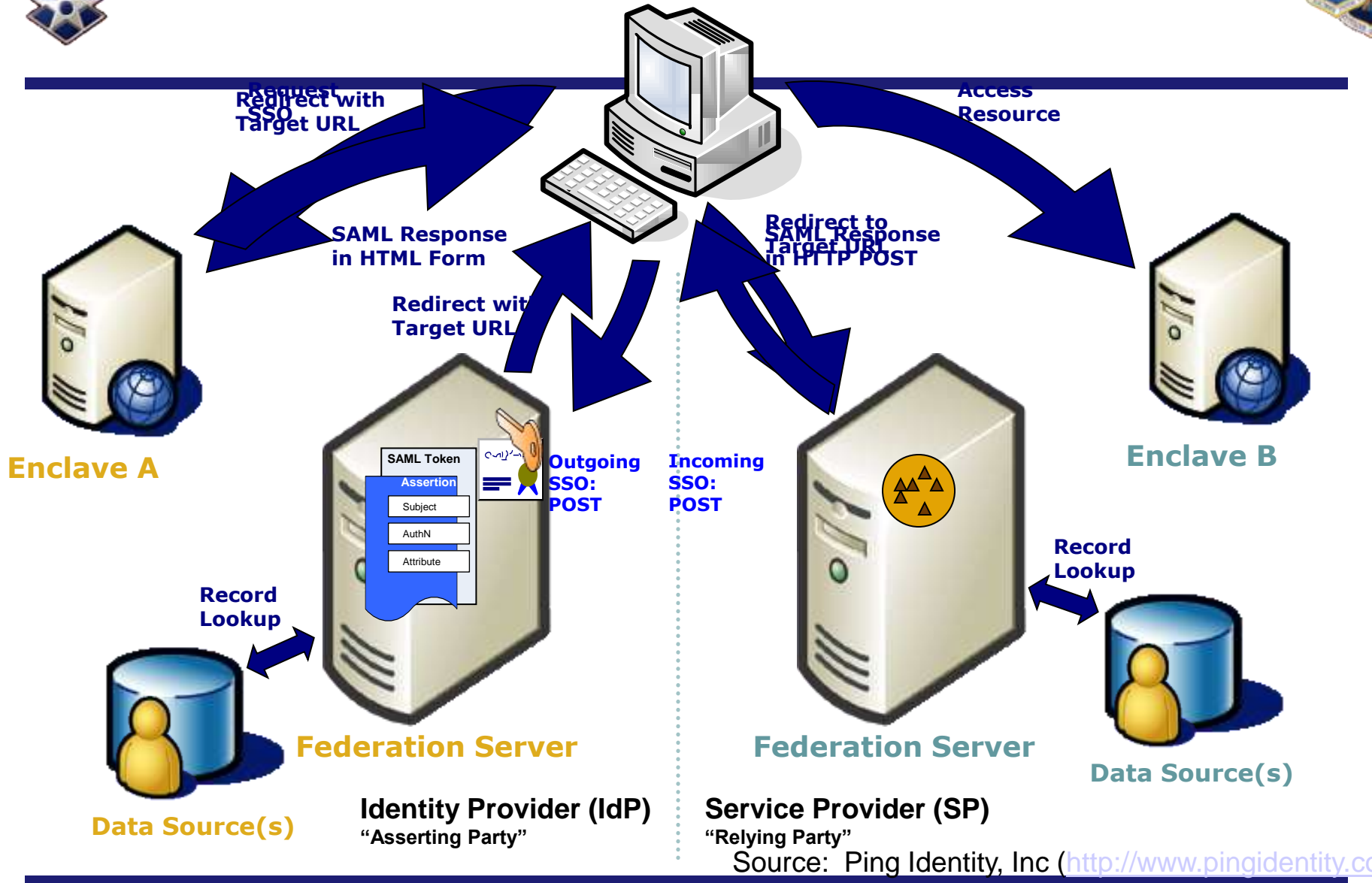
End-to-End 2-way Authentication



Source: IBM

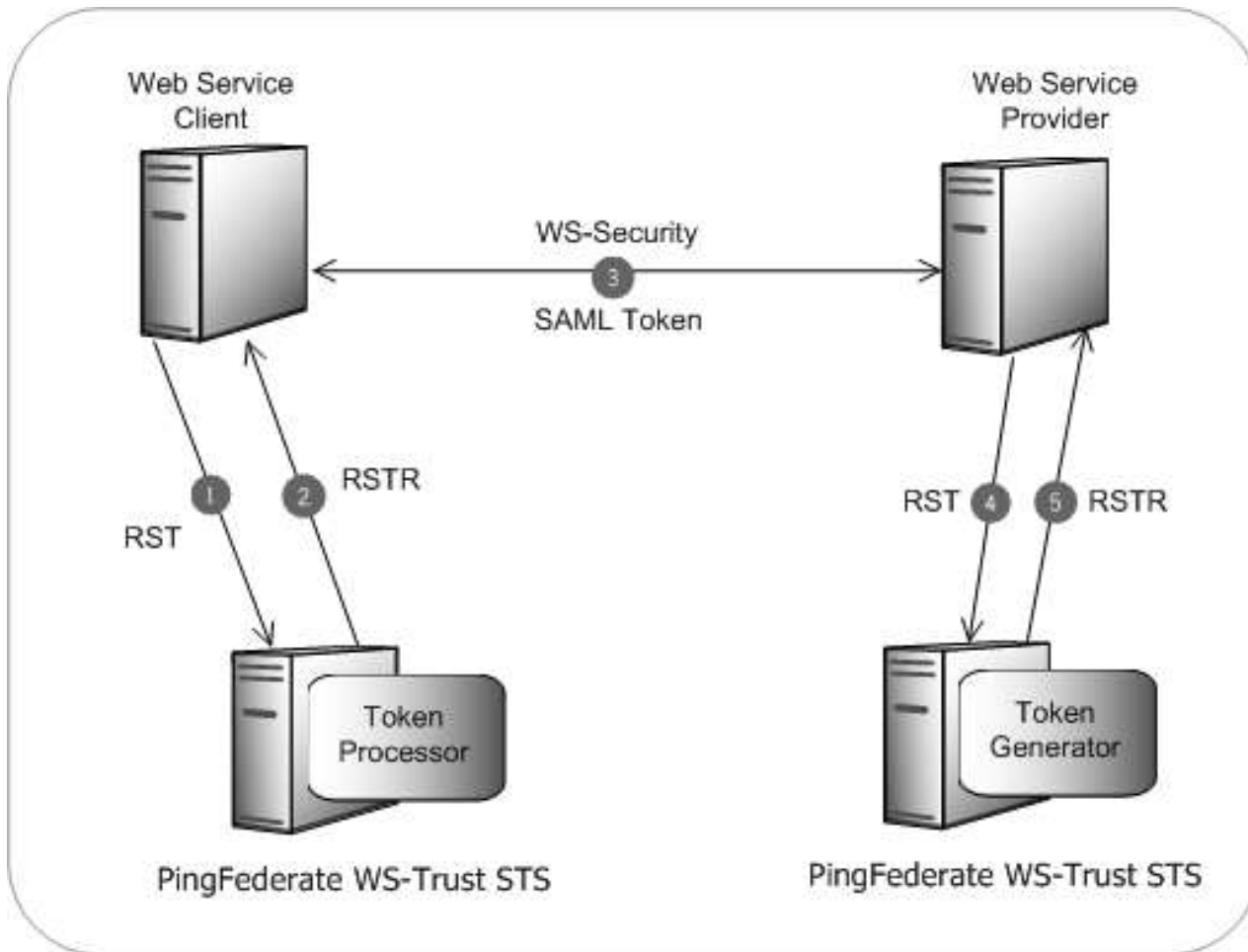


IdP Initiated SSO: POST
 POST SAML Assertion to SP Federation Server
 Retrieve Assertion from Federation Server
 Access Target Resource





WS-Trust Security Token Service (STS)

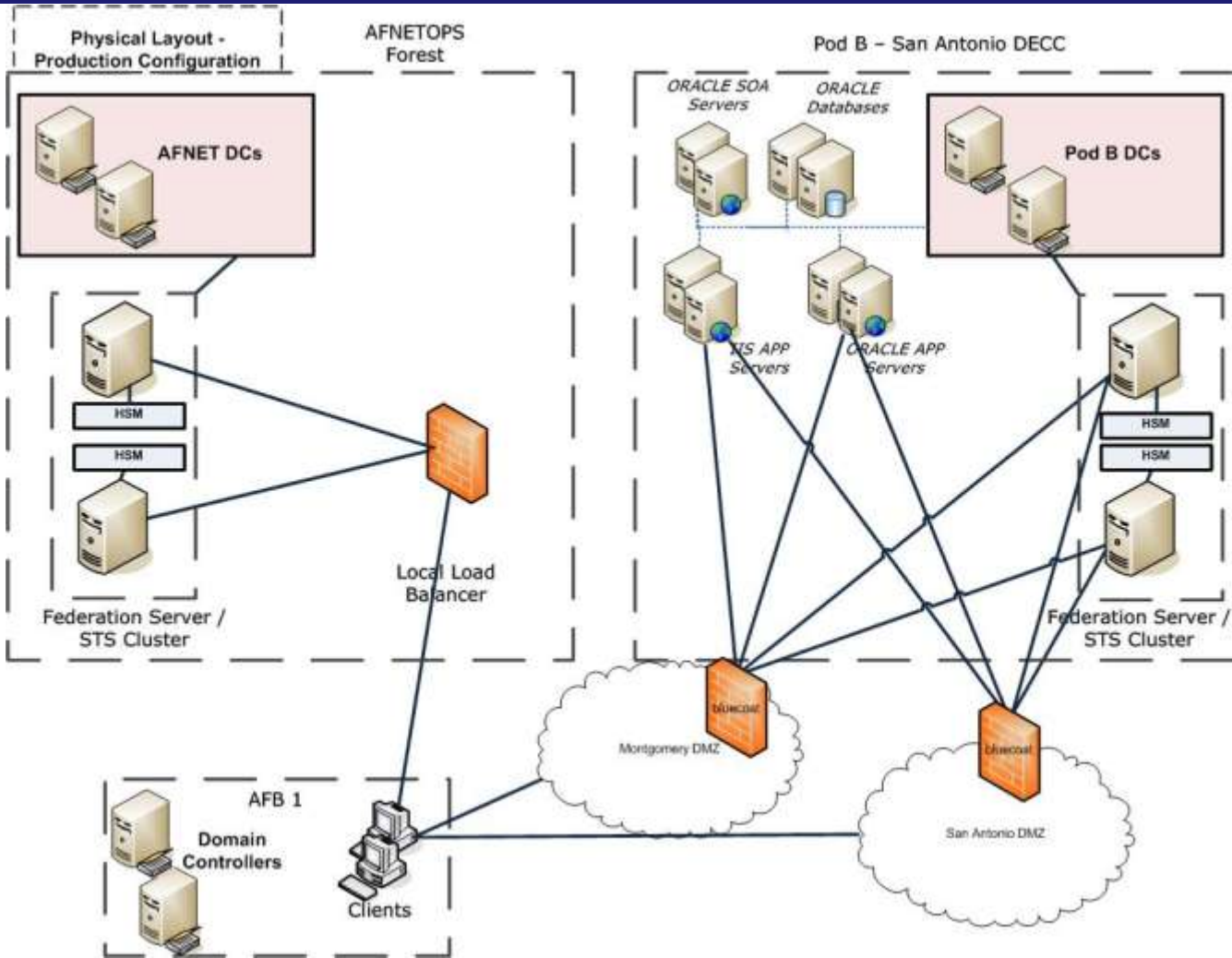


- ◆ STS Implements Federated Identity Concepts
- ◆ Attribute Contracts
- ◆ Attribute Retrieval
- ◆ Subject, Attribute and Role Mapping

Source: Ping Identity, Inc (<http://www.pingidentity.com>).



IIB Configuration





Resources for Application / Service Developers



- ◆ **Caveat – Pilot not Production – product selection for Federation Server/STS TBD**
- ◆ **PingFederate SSO Integration Overview**
 - <http://www.pingidentity.com/support-services/product-documentation/pingfederate/6-0/loader.cfm?csModule=security/getfile&pageid=14006>
- ◆ **SP Integration Kits**
 - Java, .NET, PHP, CA Siteminder, OAM, IIS, Apache, WebLogic, WebSphere, SAP NetWeaver, Salesforce.com, Citrix, Sharepoint
- ◆ **SDK for WS-Trust**
 - Used to support MDE and DRS Service Developers
 - WS-Trust Issue & Validate
- ◆ **IIB Developers Guidance**
 - Includes sample services, source code, sample COI products, instructions for how to realize COI products as runtime objects, requirements for registering users and services in AD and in the MDE, and test definitions services are expected to pass.



Lessons Learned



- ◆ **Use of a robust SOA testing tool(s) during development / deployment extremely helpful**
 - IIB team has experience with both ITKO LISA and Loadrunner
 - Useful for troubleshooting, optimization, load / performance testing, even monitoring
- ◆ **Testing in standalone lab environment is a good start – but evaluation in a more representative production environment is key**
- ◆ **ELS comes at a price - performance**
 - **Federation, TLS & Message Layer Security**
 - **As we move forward – tradeoffs may be required**
 - **Examples**
 - ~ If we implement message layer signatures/encryption, or use WS-Secure Conversation – do we also need TLS on top of that?
 - ~ Do all Services require the same security measures?
 - ~ Is PKI based authentication of all Active Entities achievable (or warranted) in ALL cases?
- ◆ **Caching can really improve performance**
 - **SAML tokens issued by STS valid for more than one time use**
 - **SAML tokens issued by STS cached by Web Service Clients until expiration**



Lessons Learned (cont.)



- ◆ **Standards are critical for interoperability – and they really do work**
 - Demonstrated Federation interoperability between PingFederate and IBM & Oracle Identity Federation products, using SAML 2.0 IdP Initiated SSO with both POST and Artifact bindings
- ◆ **State of Practice & current technologies limit achievement of long term ELS vision**
 - Example – No SOAP / WS* from standard web browser
 - No clean solution for Constrained Delegation with SAML (capability similar to Kerberos Constrained Delegation (KCD))
 - Many app servers can't consume SAML 2.0 tokens directly
 - Federation Servers – no common token format (examples, opentoken w/ PingFederate, OBSSO cookie w/ Oracle, HTTP headers w/ IBM TFIM)
- ◆ **Common Criteria challenges for small companies with rapid development / release schedule**



IIB Continuing Challenges



- ◆ **Chained authentication & authorization**
- ◆ **Extending security to the browser – true end-to-end**
- ◆ **Auditing across Service chain**
- ◆ **Authorization strategy (ABAC, GBAC, etc) – one size may not fit all**
- ◆ **Where is the Policy Enforcement Point – at the service?**
- ◆ **Performance and Scalability with an undefined number of requestors (may grow rapidly)**
- ◆ **Delegation of authorizations**
- ◆ **Monitoring of the system – requestor to provider across all layers of the stack**
- ◆ **Acceptance criteria (testing and certification) before a service is released for use**
- ◆ **Federating with multiple types of security environments**