Shibboleth-WS vs. WS-Shibboleth vs. SAML 2.0 SSO with Constrained Delegation

JISC Core Middleware Autumn Programme Meeting

Session 2, Technical Strand: Web Services

Francisco Pinto and Christian Fernau

Oxford University

14 November 2005

Overview

- Context
- N-Tier AuthN/AuthZ Problem
- Shibboleth Architecture
- Web Services and Security
- Shibboleth-WS
- WS-Shibboleth
- SAML 2.0 SSO w/ Constrained Delegation
- Discussion

Context (1)

- Shibboleth 1.x
  - Implements SAML 1.1 Profiles w/ Extensions
    - SP-first Access
    - User Privacy
  - Requires a Web Browser
    - Exchange Information
  - Might use WSs to Exchange Attributes
    - SOAP endpoint at the AA
  - Doesn't Currently Address Use Cases
    - Requiring n-tier authN/authZ

Context (2)

- WS-Security (WSS)
  - Several Implementations Available
    - Apache WSS4J
  - Would Help Shibboleth
    - Address the n-tier authN/authZ problem
  - Might Also be Used as
    - An alternative to Shibboleth
  - However
    - None Will be a Shibboleth Native Solution
    - Anyway, Shibboleth uses parts of WSS
      - XML Encryption
      - XML Signature

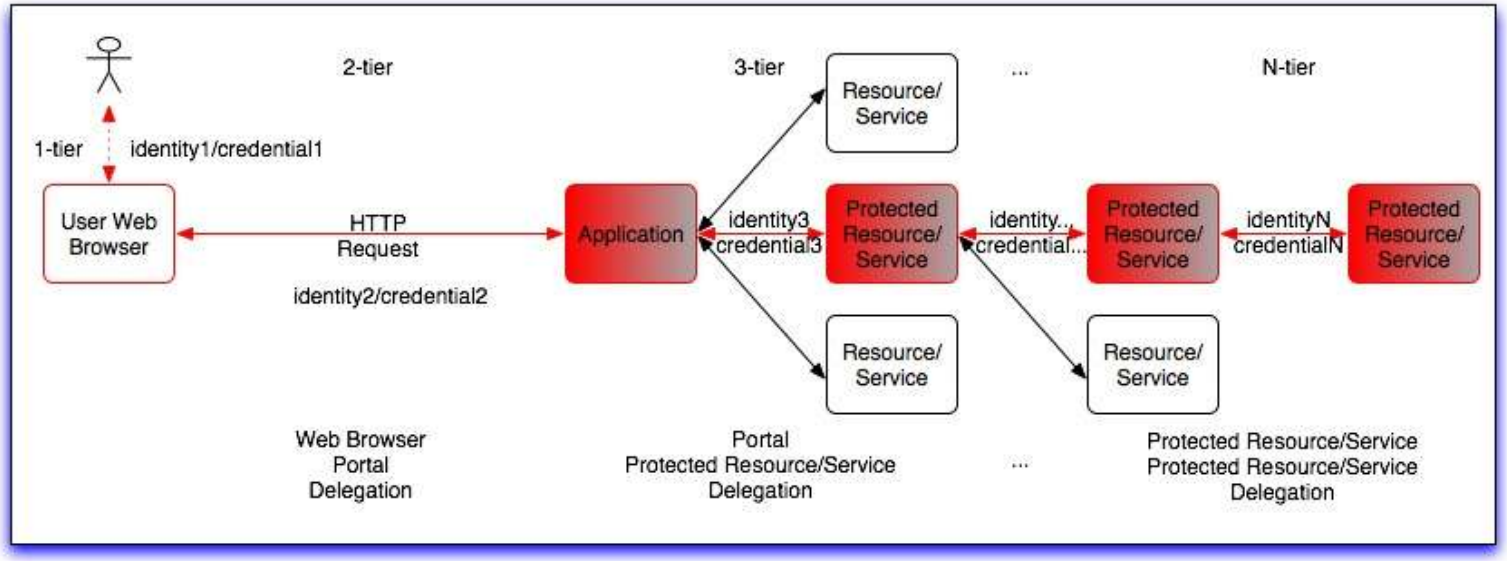
Context (3)

- SAML 2.0 SSO with Constrained Delegation
  - Working Draft Written by Scott Cantor (Internet2)
  - Currently Open for Discussion
  - Will Probably Drive the Shibboleth 2.0 Roadmap
  - Addresses Use Cases
    - Requiring n-tier authN/authZ
  - Shibboleth Native Way
  - However
    - Not Yet Implemented!!!

Context (4)

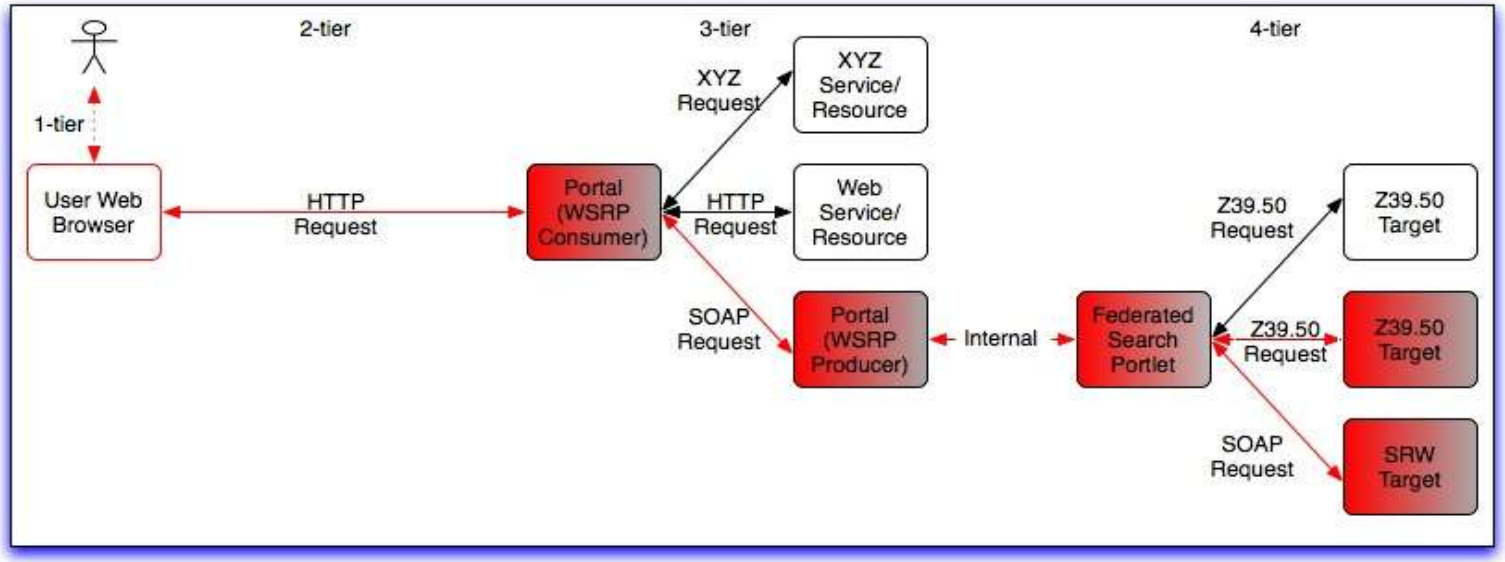
- This Presentation
  - Explores Alternative Paths
    - Based on Web Services and/or Shibboleth
      - Looking at aspects such as:
        - » Effectiveness
        - » Time-Scales
        - » Privacy
        - » Complexity
        - » Performance
        - » Etc.

N-Tier AuthN/AuthZ Problem (1)



- Defining the Problem Space (from a Web-based perspective)
  - User behind a Web Browser at the 1-Tier
  - Authenticates Against a Web-based Application at the 2-Tier
  - From the Application On (n > 2)
    - There is no user interaction anymore, but m2m interactions
    - Application and following Apps have to act on behalf of the user
    - Need to Delegate identity/credentials to the next tier
      - In a Trust and Secure way

N-Tier AuthN/AuthZ Problem (2)



- Use Case: Federated Search via a Portal using WSRP
  - User AuthN Against the Portal with WSRP Consumer Capabilities
  - Offers a Federated Search (aka x-search, meta-search) Portlet
  - This Remote Portlet is Provided by a 3rd Party Remote Application
    - Typically Another Portal with WSRP Producer Capabilities
  - Remote Portlet Might Require AuthN/AuthZ on its Own
    - e.g., to know which Data Sources the User is allowed to access
  - Some Protected Data Sources also Need AuthN/AuthZ

N-Tier AuthN/AuthZ Problem (3)

Resources / User Access	Local	Remote
Local		
Remote		

- Redefining the Problem Space (using the Access Management Matrix)
  - SSO Access to Local/Remote Protected Resources
    - Local User Access/Local Resource
      - Intra-Institutional Access
    - Local User Access/Remote Resource
      - Inter-Institutional Access
    - Remote User Access/Local Resource
      - Intra-Institutional Access
    - Remote User Access/Remote Resource
      - Inter-Institutional Access

N-Tier AuthN/AuthZ Problem (4)

Resources / User Access	Local	Remote
Local	☺	😐
Remote	☺	😐

- Users Access Protected Resources Directly (via a Web Browser)
  - Local User Access/Local Resource
    - Intra-Institutional Access: WebISO (e.g. CAS, WebAuth)
  - Local User Access/Remote Resource
    - Inter-Institutional Access: AthensSSO
  - Remote User Access/Local Resource
    - Intra-Institutional Access: WebISO (e.g. CAS, WebAuth)
  - Remote User Access/Remote Resource
    - Inter-Institutional Access: AthensSSO
- Not Devolved AuthN/AuthZ, so...

N-Tier AuthN/AuthZ Problem (5)

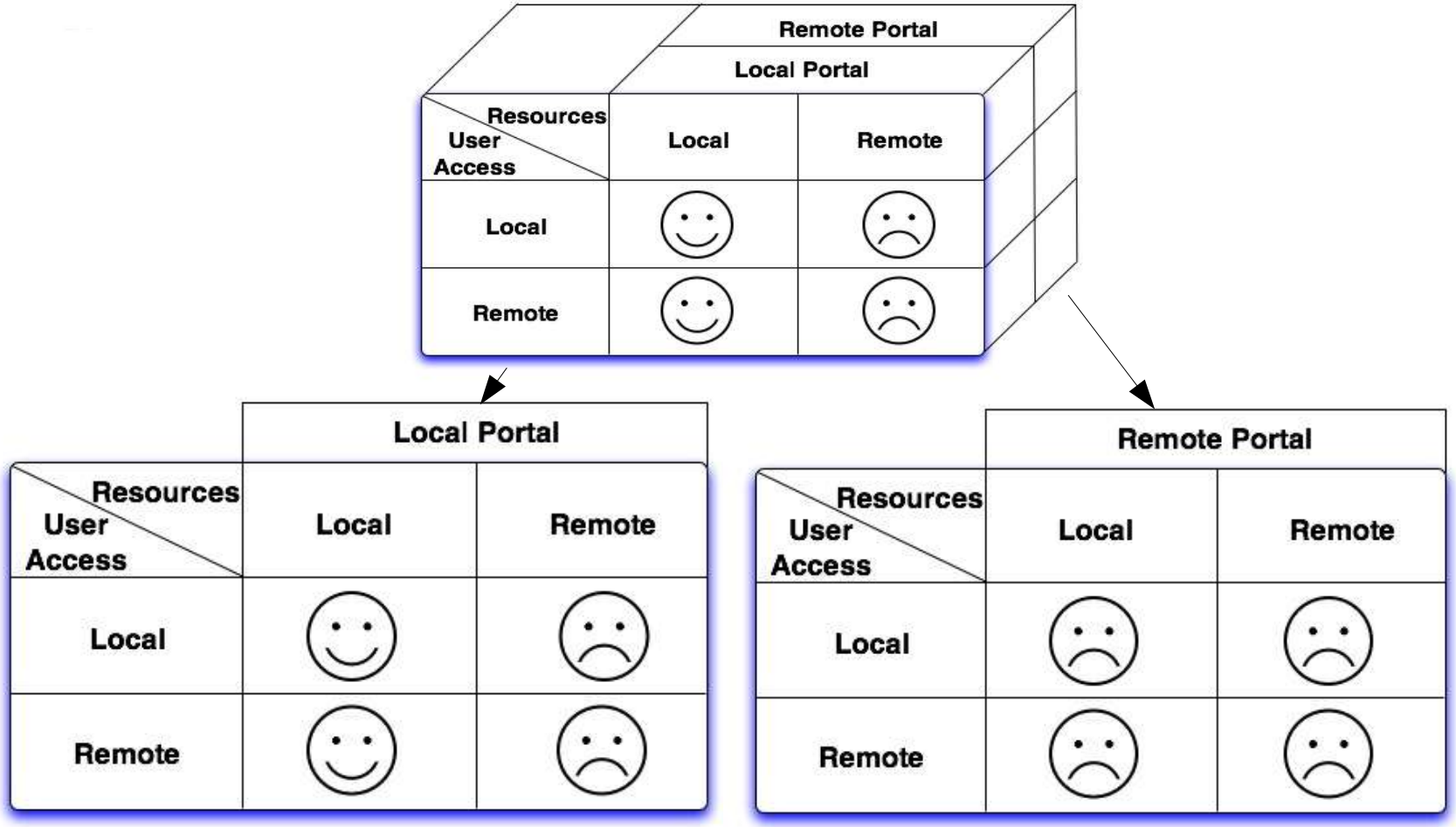
Resources / User Access	Local	Remote
Local	☺	☺
Remote	☺	☺

- Users Access Protected Resources Directly (via a Web Browser)
  - Local User Access/Local Resource
    - Intra-Institutional Access: WebISO
  - Local User Access/Remote Resource
    - Inter-Institutional Access: Athens(SSO)DA/Shibboleth 1.x
  - Remote User Access/Local Resource
    - Intra-Institutional Access: WebISO
  - Remote User Access/Remote Resource
    - Inter-Institutional Access: Athens(SSO)DA/Shibboleth 1.x
- Devolved AuthN/AuthZ, but...

N-Tier AuthN/AuthZ Problem (6)

- World Wild Web
  - Not ALL Important Resources are Web-based
  - Browsers Don't Go Further Than Tier-2
  - Portals are Typically Used
    - Expose the Hidden Web
    - With all Known Advantages, but ...
      - They have to act on behalf of the Users
      - Translate
        - » Web requests into 'Other Protocol' requests
        - » 'Other Protocol' responses into Web responses
    - In terms of Access Management
      - Brings a New Dimension to the Access Management Matrix
        - » Is the Portal Local or Remote to the Resources?

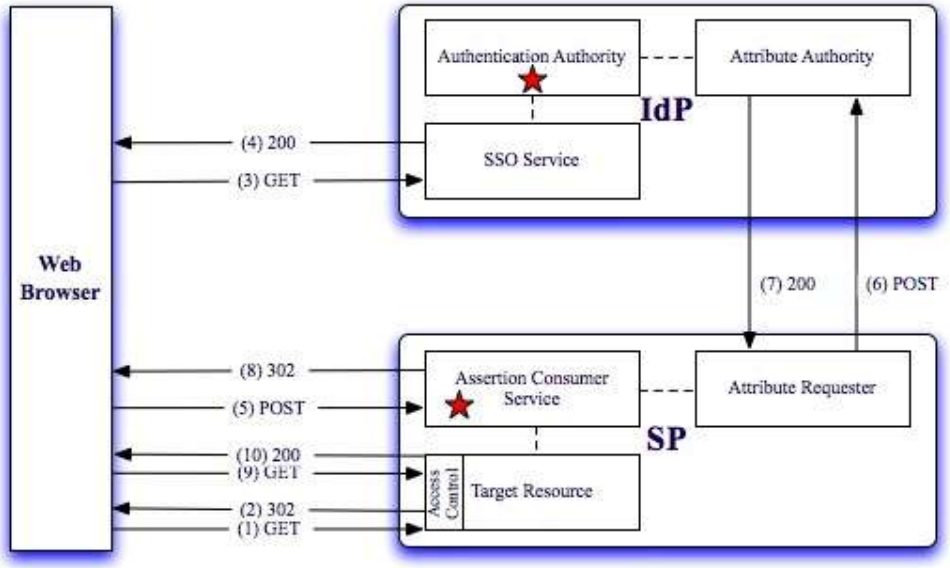
N-Tier AuthN/AuthZ Problem (7)



N-Tier AuthN/AuthZ Problem (8)

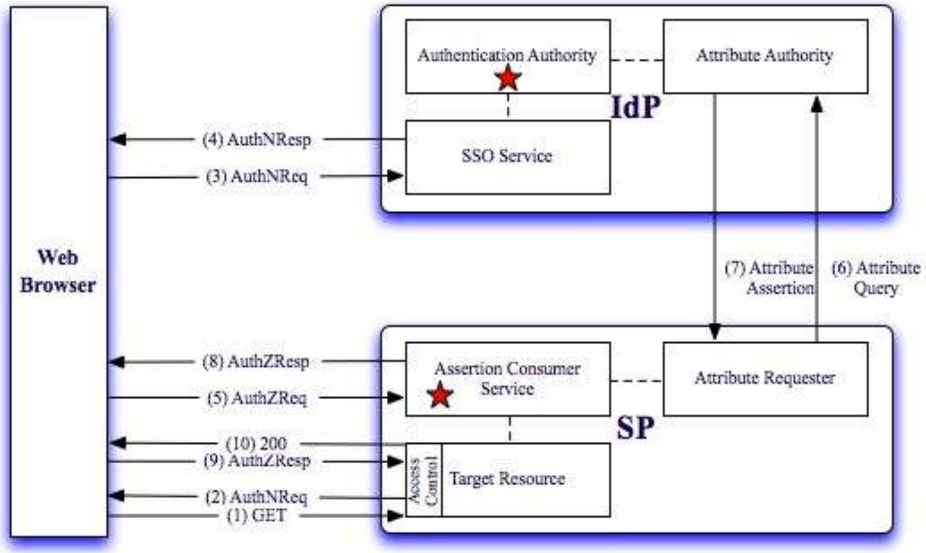
- Shibboleth, Portals & Web Services
  - Shibboleth
    - Designed for Web-based Services
      - Not for Web Services
  - Portals
    - As a Front Door suits well Shibboleth, but...
      - Portals typically need to access other back-end resources
      - Some of the resources are protected
      - If they live in the same administrative security domain
        - » Impersonation
        - » Shared secrets (e.g. Kerberos/WebISO Tickets)
    - Web Services
      - Increasingly used for accessing back-end resources
  - Lets look at...

Shibboleth Architecture (1)



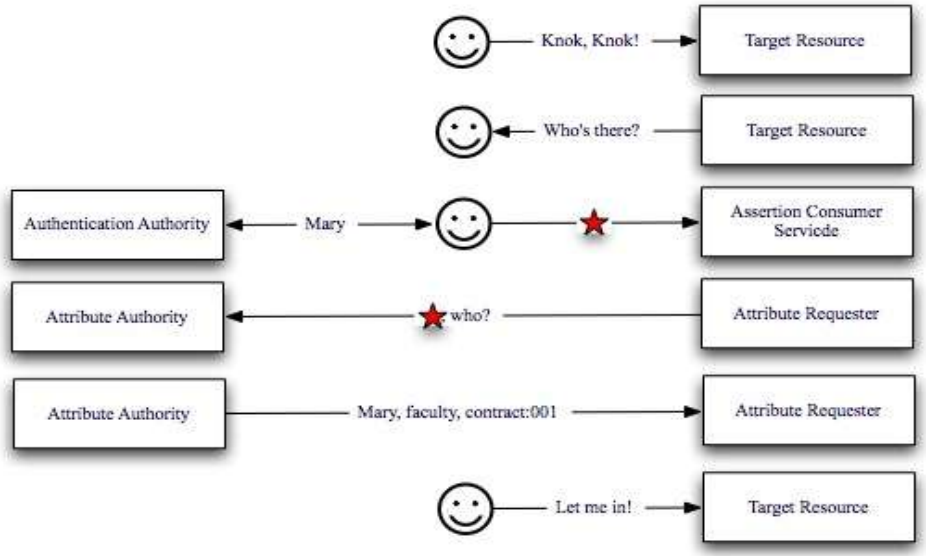
- Shibboleth Browser/POST Profile with Attribute Exchange
  - Basic Model taken from the Specifications
  - Security Context at the IdP and SP
  - Back-end Channel for Attribute Exchange Bypassing the Browser
    - Might be SOAP 1.1 Binding
      - HTTP POST of a SOAP Envelope with a SAML Assertion

Shibboleth Architecture (2)



- Shibboleth Browser/POST Profile with Attribute Exchange
  - The same diagram with more Semantics...

Shibboleth Architecture (3)



- Shibboleth Browser/POST Profile with Attribute Exchange
  - The same diagram with even more Semantics...
    - Credits to Scott Cantor

Web Services and Security (1)

- Web Services (WS)
  - Trend to use WSs for Everything
    - Wrap Business Logic/Processes
    - Expose them as Services
    - M2M Interactions
  - Advantages
    - Flexibility, Integration, Interoperability, ...
    - Usability?
  - Disadvantages
    - Increased Risk... So Secure Them
      - Transport-level Security vs. Message-level Security
        - » point-to-point vs. end-to-end
        - » encryption/decryption, digital signatures, granularity, ...

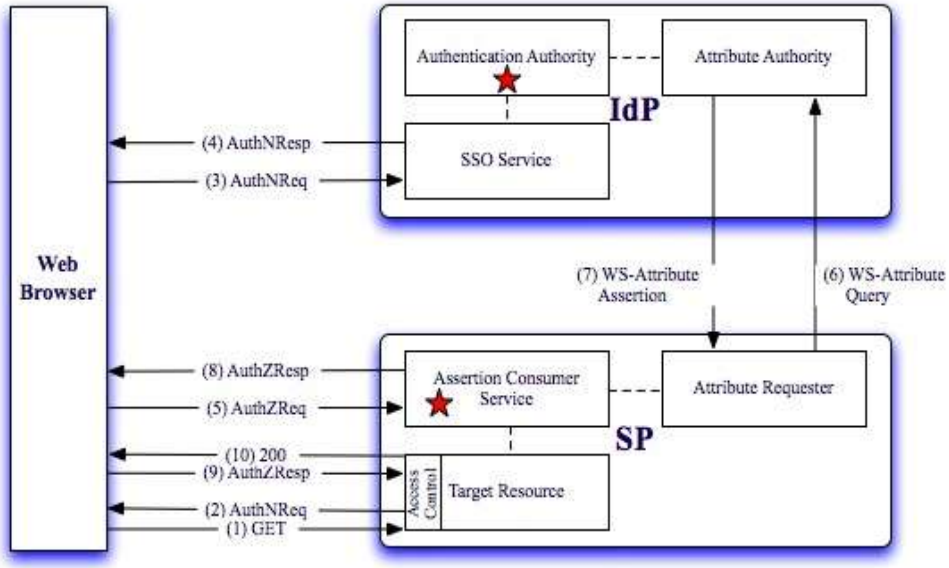
Web Services and Security (2)

- OASIS WS-Security (WSS)
  - WS Extensions Providing Msg-Level Security
    - Integrity via XML Signature
      - Guaranties unchanged information and non-repudiation
    - Confidentially via XML Encryption
      - Sensitive information parts are kept unseen
    - Authentication via Security Token Validation
      - Claims: authN assertions made by principals (e.g. SAML)
  - Cross Administrative Security Domains
  - Addresses SSL Limitations

Web Services and Security (3)

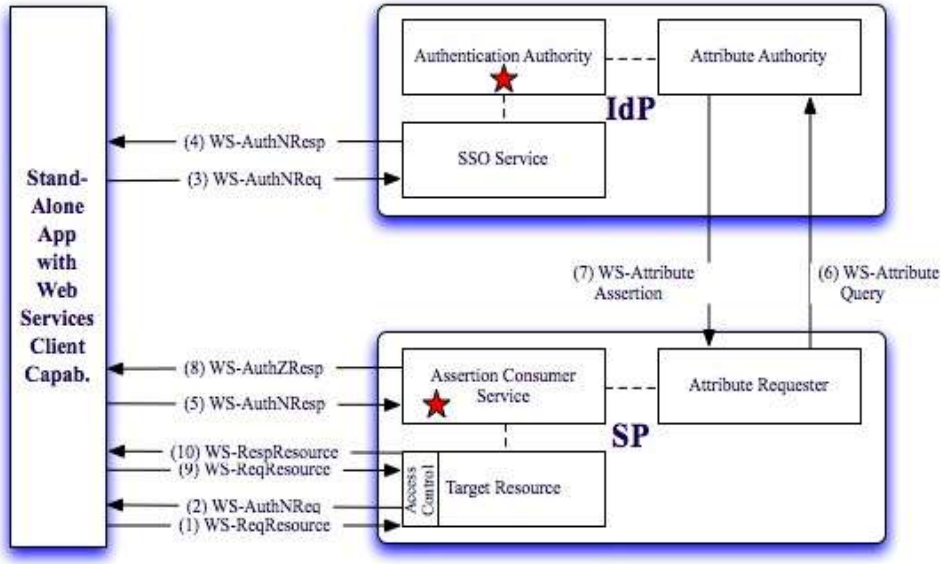
- Apache WSS4J
  - Java Implementation of WSS
  - Uses Apache Axis and XML Security Projects
  - Interoperates with Sun's JAX-RPC and M's .Net
  - Implements Username and X.509 Token Profiles
  - Can Secure any WS
    - Application Level (Java API)
    - Support for Axis SOAP Framework via Axis Handlers
      - Tandem with Axis
        - » Secure XML Elements within a SOAP Envelope

Shibboleth-WS



- Shibboleth Browser/POST Profile with Attribute Exchange
  - WS Endpoint at the AA

WS-Shibboleth



- Shibboleth WS Client/POST Profile with Attribute Exchange
  - Why Not Taking Advantage WSS for...
    - Extend WS endpoint at the AA to other Shibboleth components
    - Develop a Standalone Application with WS capabilities
      - Getting rid of HTTP Redirects (302)
    - Use it for Delegation solving the n-tier authN/authZ Problem
  - Requirements
    - Standalone Application to Orchestrate the authN/authZ Flows
  - Or, even better...

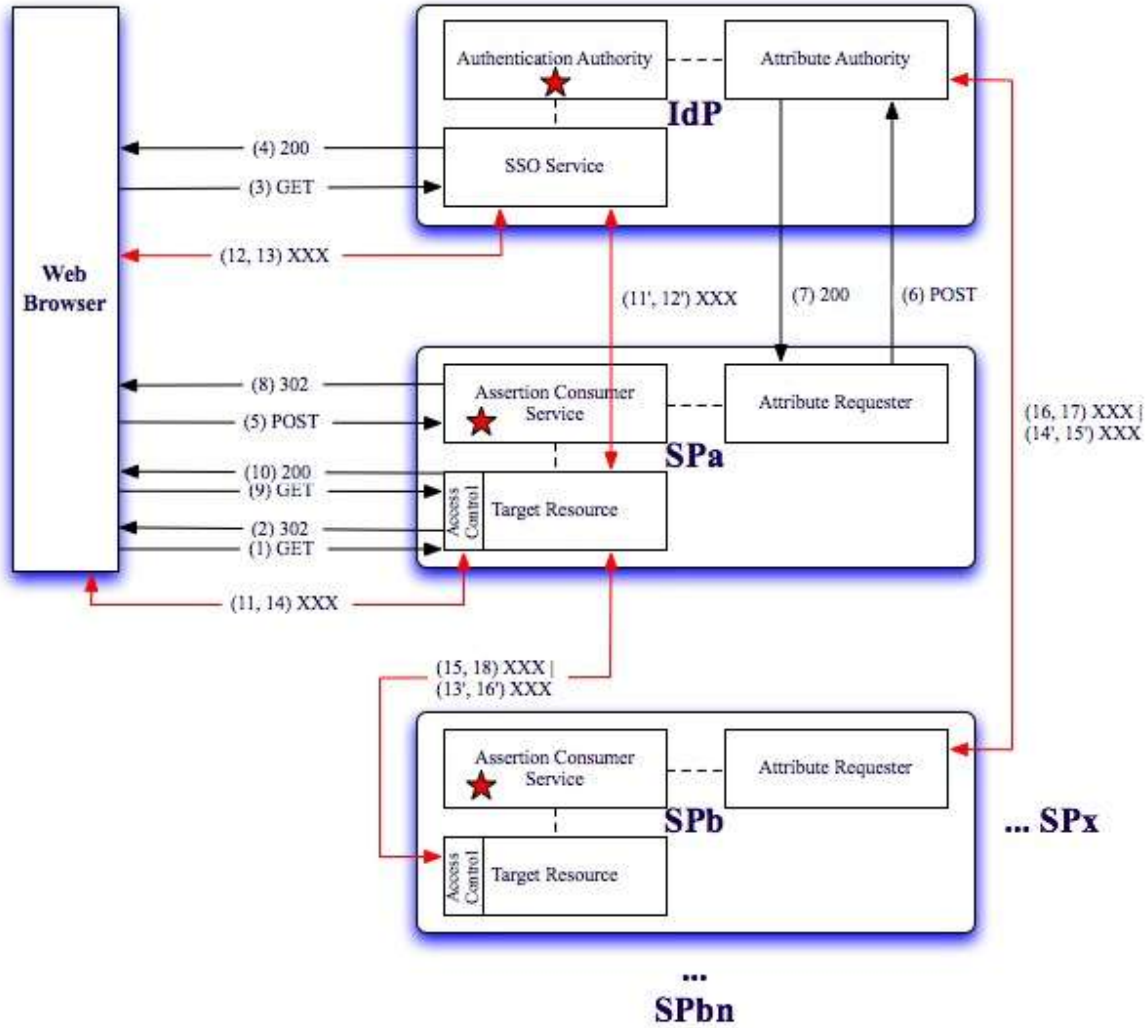
SSO with Constrained Delegation (1)

- Set of Profiles
  - Conjunction with SAML 2.0 authNReq Protocol
  - Context of Web Browser SSO and ECP Profiles
- Enable Constrained Delegation
  - AuthN via Web Browser or Enhanced Client
    - Profile encompasses all authN exchanges
      - To back-end resources on Principal's behalf
  - Extends Shibboleth to Solve Natively
    - N-tier authN/authZ problem
      - Within a Federated context

SSO with Constrained Delegation (2)

- SAML Assertions to Enable an SP
  - Act in a Limited (but Transparent) Way
    - On behalf of the Principal (via the IdP)
    - To access other SP(s)
    - Provide means by which the Principal authNs to IdP
      - Keeping authN Mechanism Unspecified
      - Using SAML Assertions to authN against a SP
  - Requires Policy Enforcement Between
    - All 4 parties: Principal; IdP; delegateSP; back-endSP
    - Specially between the Principal and IdP

SSO with Constrained Delegation (3)



SSO with Constrained Delegation (4)

- Allows SPa to Access SPb
  - On Principal's Behalf, but in a Limited Context
    - SPa could authN to SPb Using
      - SSL/TLS; or
      - Digital Signatures
      - But...
  - This Profile
    - Gives SPa the Ability to Prove to SPb That
      - It is authorised to act on behalf of the Principal
        - » At a particular point in time
      - By presenting the SAML Assertion to SPb as evidence
        - » Which, might not always or even happen again

SSO with Constrained Delegation (5)

- AuthNRequest Delegation Profile
  - Optional Elements
    - <saml:Subject>; <saml:Conditions>
  - Mechanism by Which
    - An <samlp:AuthnRequest> can include a Request
      - Embeding delegation support in the Result
    - The Result is an <samlp:Response> Assertion
      - That contains Subject and Conditions confirmation rules
      - Taken together
        - » Makes it usable as a Delegation Token
    - Indicates that this Token (assertion)
      - Can be used by a given SPa
      - To access SPb on behalf of the Principal

SSO with Constrained Delegation (6)

- Token Contains Specific Content
  - <saml:Subject>
    - NameID; SubjectConfirmation (holder-of-key)
  - <saml:Conditions>
    - AudienceRestriction; Audience
  - Enabling SPb to Securely Establish SPa
    - The right to Delegate in a Trust and Secure way
  - Request Optimisation
    - Allowing a Token to be used simultaneously by SPa
      - Access multiple Relying Parties (e.g. IdPs, SPs)

N-Tier AuthN/AuthZ Problem (again)

	Local Portal	
Resources / User Access	Local	Remote
Local	☺	☺
Remote	☺	☺

	Remote Portal	
Resources / User Access	Local	Remote
Local	☺	☺
Remote	☺	☺

- Users Access Protected Resources Directly (via a Web Browser)
  - Local User Access/Local Resource
    - Intra-Institutional Access: WebISO/Shibboleth 2.0
  - Local User Access/Remote Resource
    - Inter-Institutional Access: Shibboleth 2.0
  - Remote User Access/Local Resource
    - Intra-Institutional Access: WebISO/Shibboleth 2.0
  - Remote User Access/Remote Resource
    - Inter-Institutional Access: Shibboleth 2.0

Discussion (1)

- Effectiveness
  - WS-Security Based
    - Seems possible, but Requires Extra Logic
      - Orchestrate authN/authZ flows
    - Which leads to...
      - Kind of RDF vs. XML discussion, and
      - A Delegation Profile has to be implemented anyway...
    - Will not work from a Browser
  - SAML 2.0 SSO with Constrained Delegation
    - Strong Federated Security w/out too much complexity
    - SOAP Application Profile
      - Applies to multiple (and increasing number of) Use Cases
        - » Portals/WSRP, Grid Apps, Native WS Apps, SRW, ...
    - Independent of Browser or Standalone Applications

Discussion (2)

- Time-Scales
  - WS-Security Based
    - 6 months to 1 year (depends on resources...)
      - Basically, new Protocol for Applications
        - » Enhanced Clients
        - » Plugin Approach
  - SAML 2.0 SSO with Constrained Delegation
    - Not before Mid 2006 (extrapolation)
      - Basically, a set of new Profiles
      - Depend on SAML 2.0 Profiles
        - » Web Browser SSO
        - » ECP

Discussion (3)

- Privacy
  - WS-Security Based
    - Fine-Grain Integrity and Confidentially
      - At the XML element level (within a SOAP Envelope)
    - However
      - Issues Might Happen at the Application Level
  - SAML 2.0 SSO with Constrained Delegation
    - IdP and delegateSP(s) Might Be able To
      - Aggregate and Correlate Information
        - » About the SPs a user wants to access
      - This Might be Mitigated
        - » Using WSS fine-grain integrity and confidentially

Discussion (4)

- Complexity
  - WS-Security Based
    - WS-enable Shibboleth
      - Is not complex
    - Standalone App to implement the authN/authZ flows
      - Relatively complex
    - Implement a delegation feature
      - Might be as complex as the SAML 2.0 SSO w/ CD Profile
  - SAML 2.0 SSO with Constrained Delegation
    - Not so complex as Liberty Alliance (LA)
      - But not as complete & flexible
    - But, still requires
      - All supporting and new profiles

Discussion (5)

- Performance
  - WS-Security Based
    - Message-level Security
      - Is more Expensive than Transport-level Security
        - » Globus Toolkit 4.0 implemented it, but doesn't use...
  - SAML 2.0 SSO with Constrained Delegation
    - Not anticipated to be very resource intensive
    - However
      - In order to address Privacy Issues
        - » Might require fine-grain enc/decryption and signatures
      - This might well change the scenario

Discussion (6)

- Etc
  - WS-Security Based
    - Your turn...
    -
    -
    -
  - SAML 2.0 SSO with Constrained Delegation
    - Your turn...
    -
    -
    -

References

Federated Security: The Shibboleth Approach, R. L. "Bob" Morgan, Scott Cantor, Steven Carmody, Walter Hoehn, and Ken Klingenstein, http://www.educause.edu/apps/eq/eqm04/eqm0442.asp

Shibboleth Architecture: Protocols and Profiles, Internet2/MACE, http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-latest.pdf

Shibboleth Architecture: Technical Overview, Internet2/MACE, http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf

Shibboleth Architecture: Conformance Requirements, Internet2/MACE, http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-conformance-latest.pdf

Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS, http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

SAML 2.0 Single Sign-On with Constrained Delegation, Internet2/MACE, http://shibboleth.internet2.edu/docs/draft-cantor-saml-sso-delegation-01.pdf

SAML, Shibboleth & PK[Ili], Scott Cantor, Internet2/MACE & OSU, http://middleware.internet2.edu/pki03/presentations/Shibboleth-PKI2.pdf

Security in a Web Services World: A Proposed Architecture and Roadmap, A joint whitepaper from IBM Corporation and Microsoft Corporation, http://www.verisign.com/wss/architectureRoadmap.pdf

OASIS WS-Security, OASIS, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

Secure Web Services, Java World, http://www.javaworld.com/javaworld/jw-03-2003/jw-0321-wssecurity.html

Web Services for Java, XML.com, http://webservices.xml.com/pub/a/ws/2003/10/28/jwss.html

Implementing WS-Security with Java and WSS4J, devX, http://www.devx.com/Java/Article/28816/1954?pf=true

Apache WSS4J, Apache Foundation, http://ws.apache.org/wss4j/

The Venn of Identity Federation, and Secure Web Services, Gary Ellison, Sun Microsystems, http://web.princeton.edu/sites/isapps/jasig/2003winterMiami/presentations/ellisonkeynote.pdf

Digital Identity: Planning and Creating an Identity Management Architecture, Phillip J. Windley, O'Reilly, http://press.oreilly.com/lpt/pr/1415

Web Services Security, Chapter 9, Mark O'Neill, http://searchwebservices.techtarget.com/searchWebServices/downloads/WebServSecC09.pdf