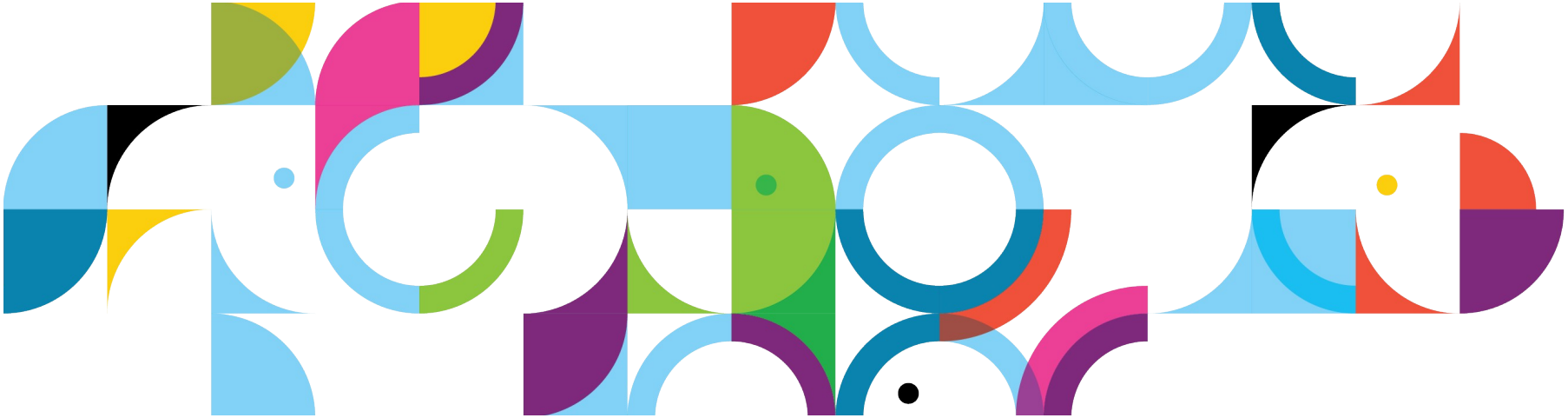
Configuring an IBM Domino Web server to use SAML-based single sign-on
Open Mic

Date: 08/14/2013

Joshua Tsai | IBM Domino Support Engineer
Panelists : Jane Marcus, Andrew Quap, Brandon Kutsch, William Raffety

IBM Collaboration Solutions



Agenda

- What is SAML
- SAML Concepts
- Benefits and Restrictions
- SAML Exchange
- Configuring SAML in Domino
- Debugging SAML on Domino
- Resource Links

- Q&A

What is SAML (Secure Assertion Markup Language)

- Method of exchanging authentication and authorization between two parties using an XML based open standard.
- Product of OASIS that began with SAML 1.0 (2002), SAML 1.1 (2003) and SAML 2.0 (2005)
- Key parties of SAML
  - Identity Provider (IdP)
    - Tivoli Federated Identity Manager (TFIM)
    - Active Directory Federation Services (ADFS)
  - Service Provider (SP)
    - Domino
  - Client
    - Browsers
- Link to SAML 2.0 Specifications
  - https://www.oasis-open.org/committees/download.php/27819/

SAML Concepts

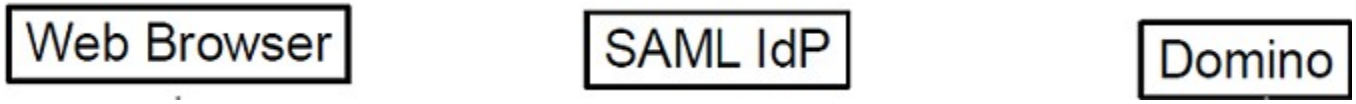
- Identity Provider
  - Performs the authentication with the client
  - Maintain the user's information
  - Maintain the list of relying parties
  - Creates the Assertions
- Assertion
  - User information represented in a XML format
  - Secured by PKI-based encryption pre-exchanged between IdP and SP
- Service Provider
  - Check for validity of the Assertion
  - Process the Assertion to identify the user
  - Provides application service

Benefits and Restriction

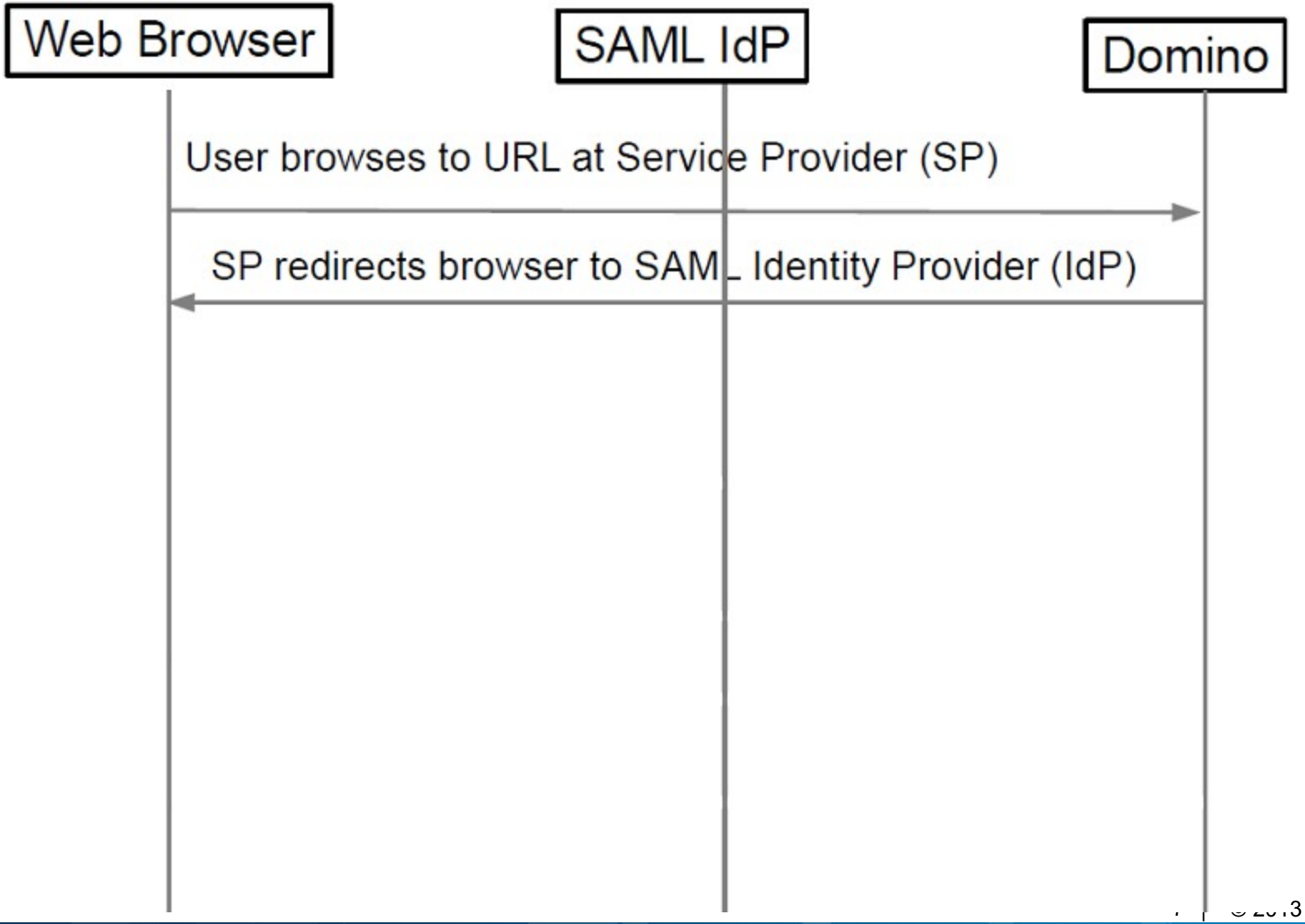
- Benefits
  - Provides a single sign on experience across multiple platforms
  - Reduces the need for users to manage multiple username/password
  - Reduces the administrative cost for maintaining multiple directories
  - Reduces user data redundancy

- Restrictions
  - Notes Domino version 9.0 +
  - SAML 1.1 or SAML 2.0
  - TFIM or ADFS
  - Client devices that can work with SAML exchange

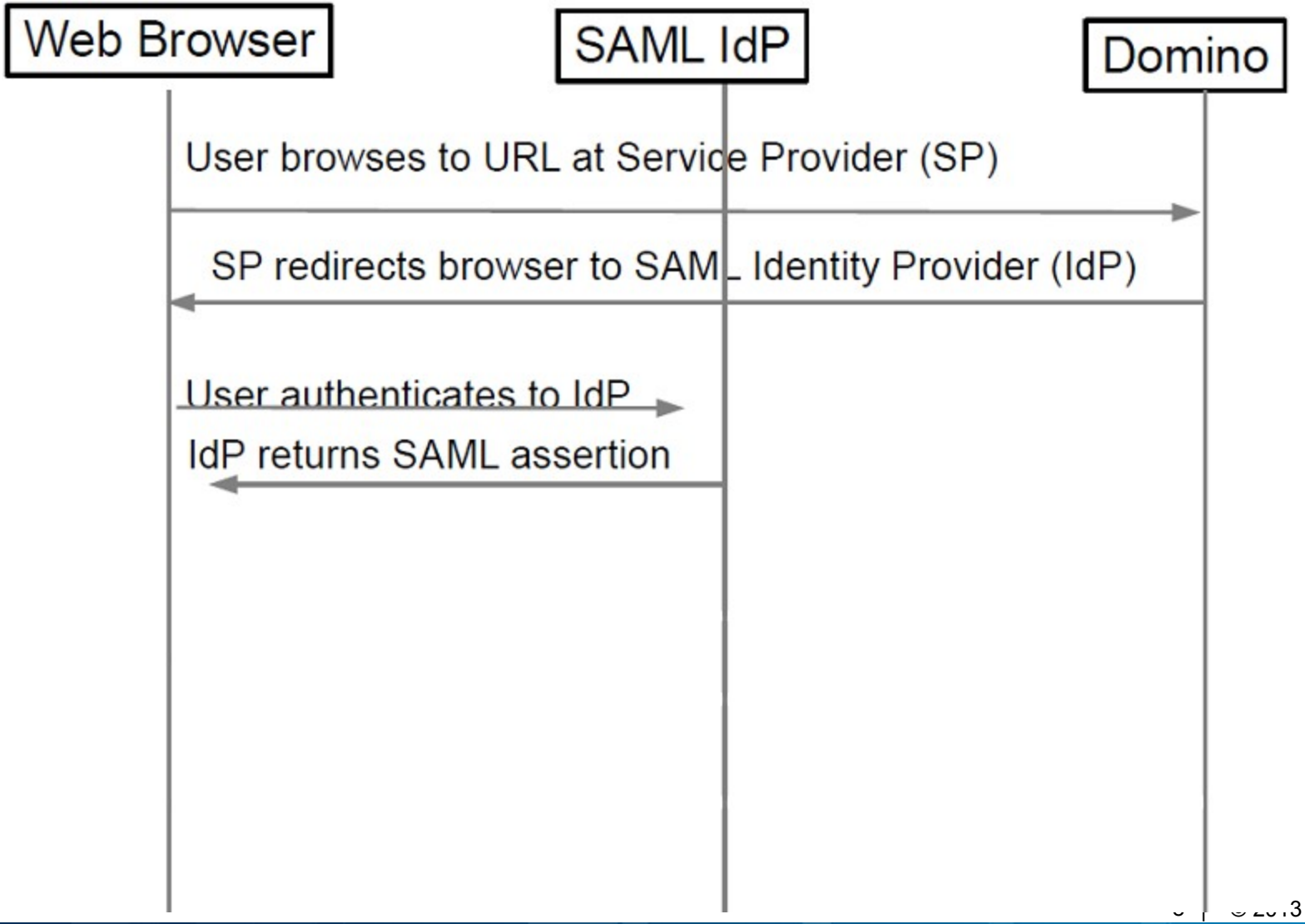
SAML exchange



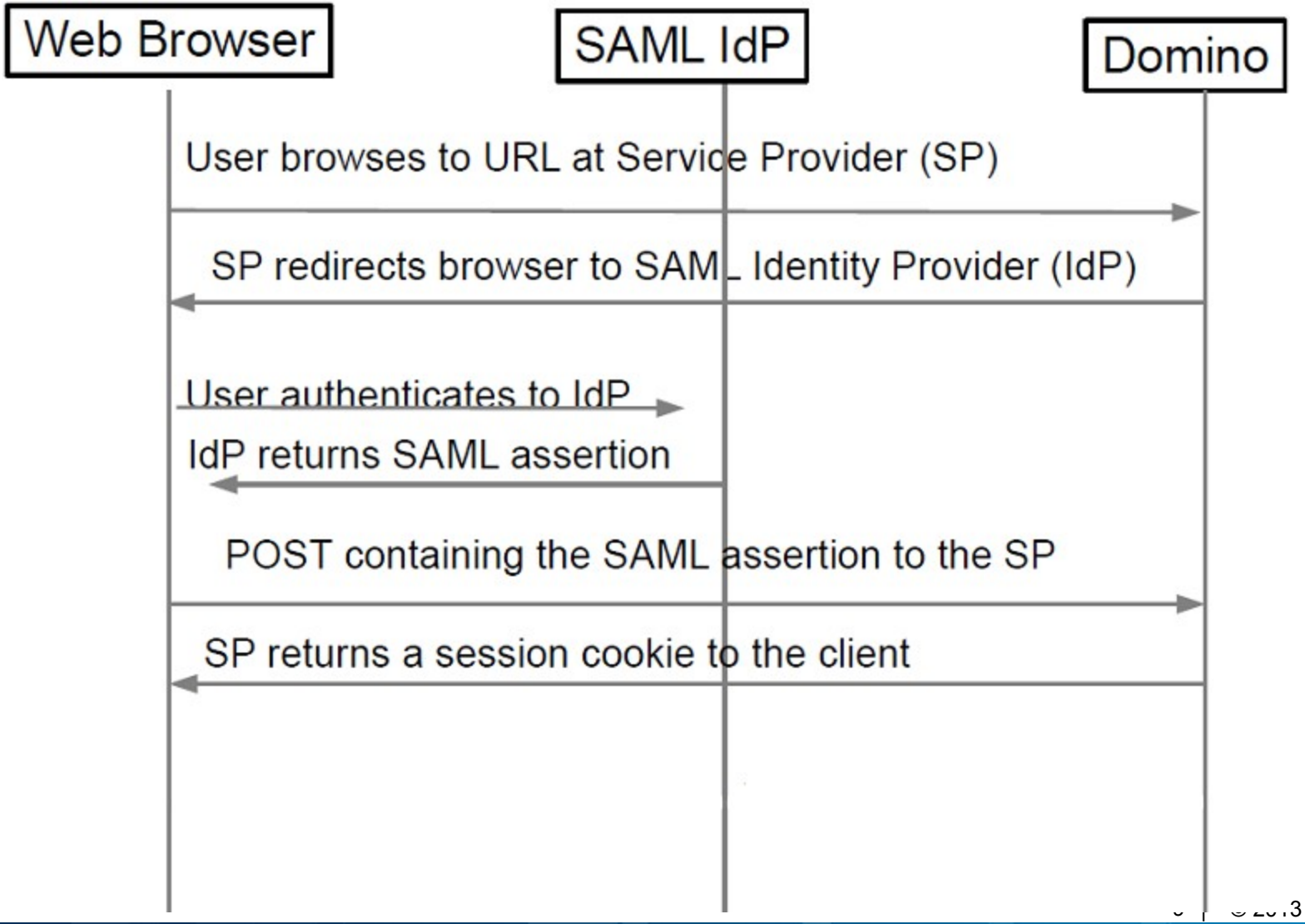
SAML exchange



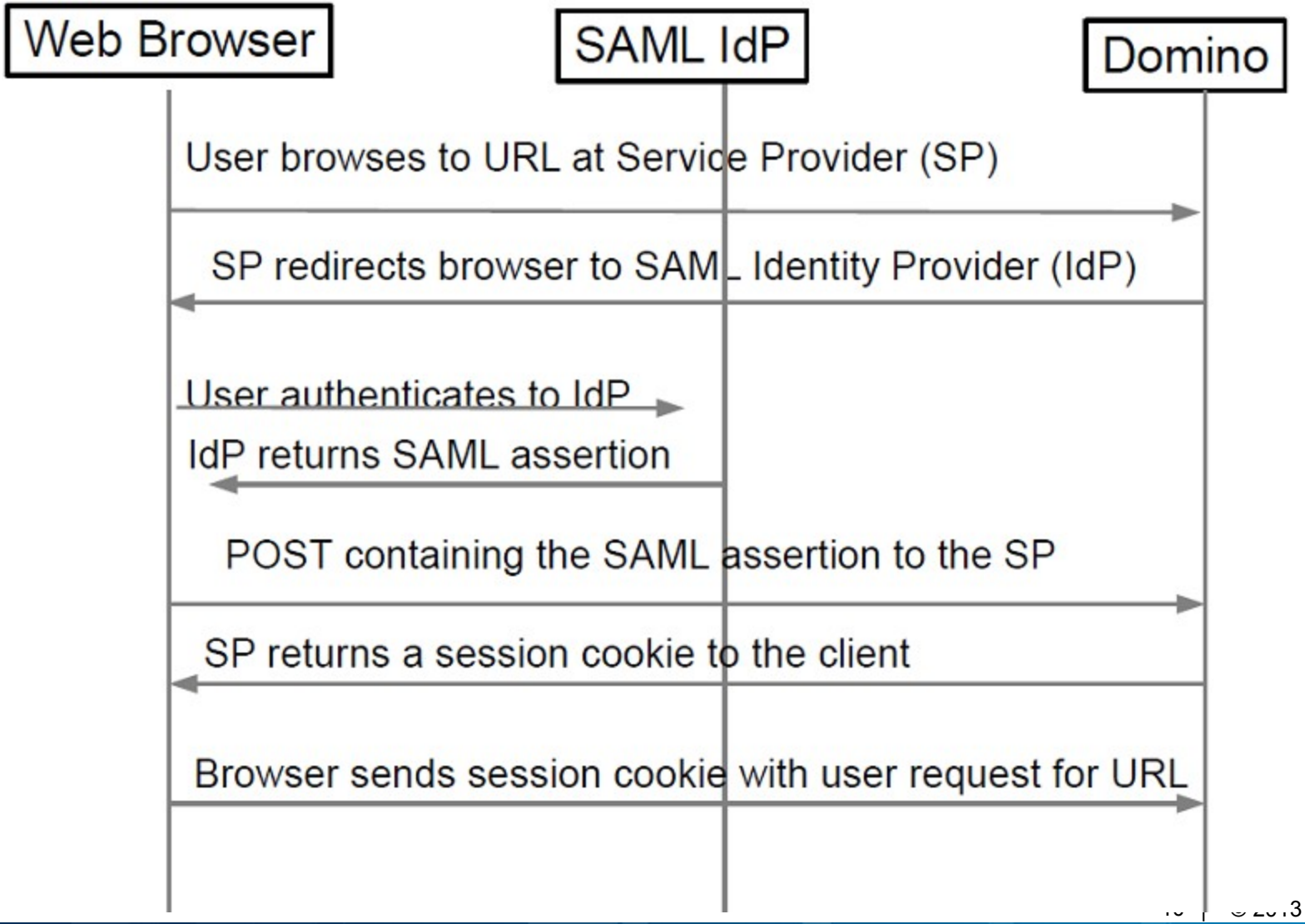
SAML exchange



SAML exchange

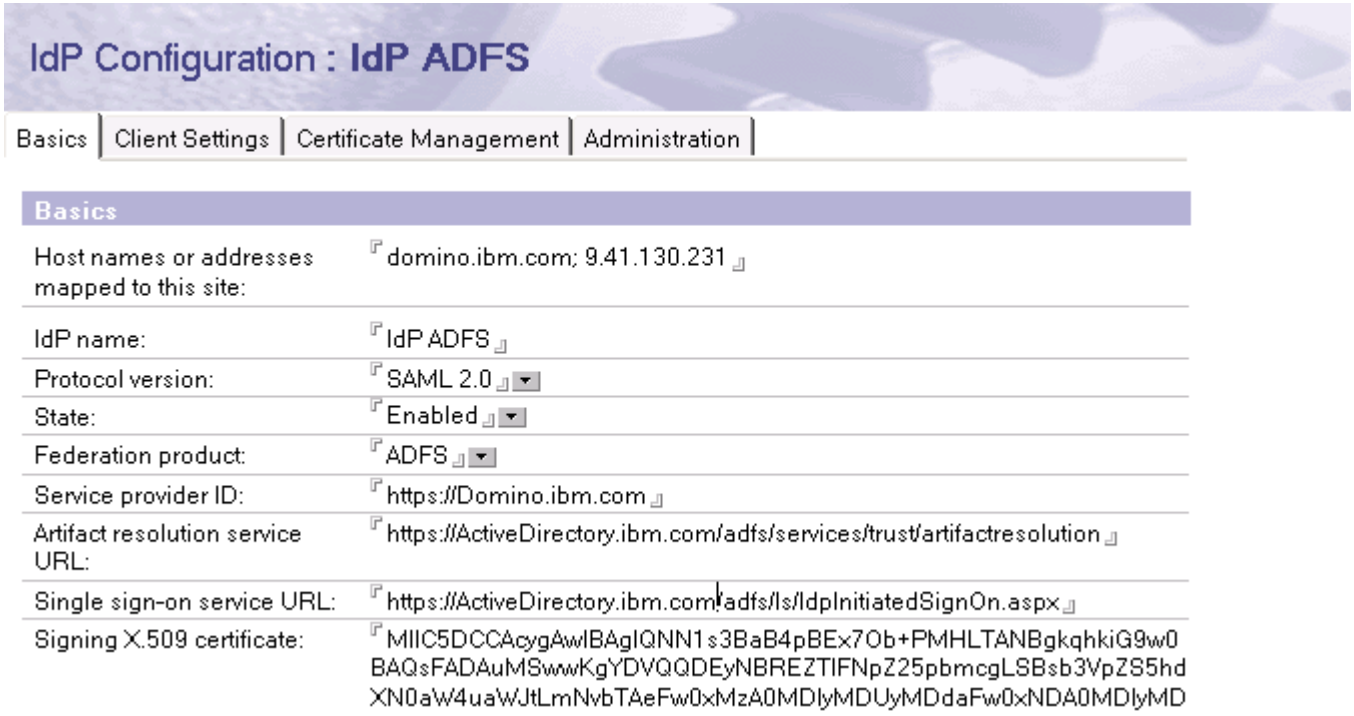


SAML exchange



Configuring SAML on Domino

- Export the IdP's configuration.
- Create and idpcat.nsf based on the IdP Catalog template
- Create the IdP Config document and import the IdP Configuration



IdP Configuration : **IdP ADFS**

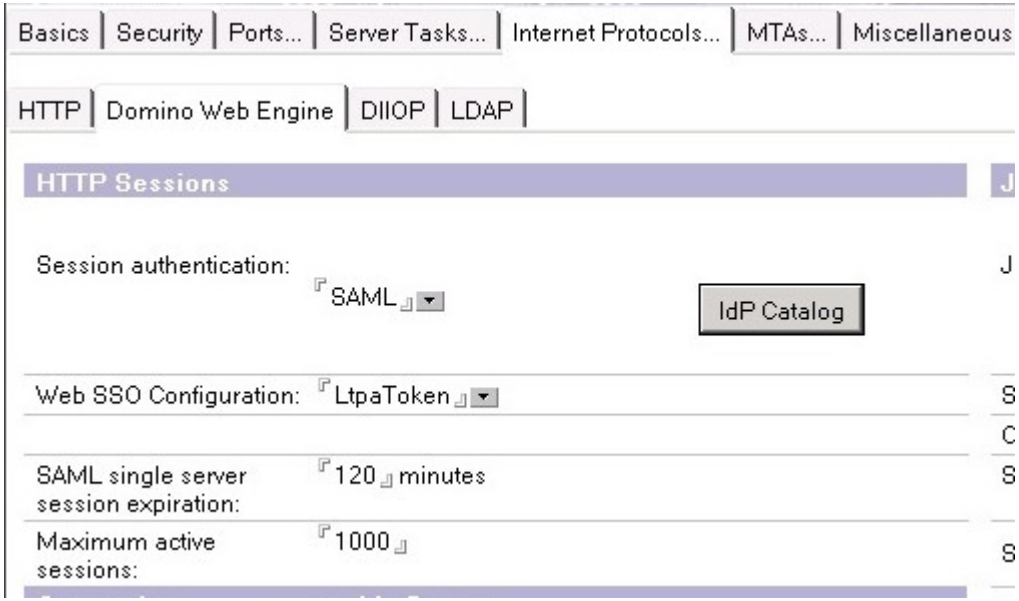
Basics | Client Settings | Certificate Management | Administration

Basics

Host names or addresses mapped to this site:	domino.ibm.com; 9.41.130.231
IdP name:	IdP ADFS
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	ADFS
Service provider ID:	https://Domino.ibm.com
Artifact resolution service URL:	https://ActiveDirectory.ibm.com/adfs/services/trust/artifactresolution
Single sign-on service URL:	https://ActiveDirectory.ibm.com/adfs/ls/IdpInitiatedSignOn.aspx
Signing X.509 certificate:	MIIC5DCCAcygAwIBAgIQNN1s3BaB4pBEx7Ob+PMHLTANBgkqhkiG9w0BAQsFADAuMSwwKgYDVQQDEyNBREZTIFNpZ25pbmcgLSBsb3VpZS5hdXN0aW4uaWJtLmNvbTAeFw0xMzA0MDIyMDUyMDdaFw0xNDA0MDIyMD

Configuring SAML on Domino

- Configure the server to use the new SAML session based authentication
  - You can either populate the Web SSO configuration in a multi server environment or leave it blank for a single server environment



Debugging SAML on Domino

- 0x0001 (1) /* Debug output contains information from http side. */
- 0x0002 (2) /* Debug output contains SAML parse information. */
- 0x0004 (4) /* Debug output only contains errors. */
- 0x0008 (8) /* Debug to dump decoded assertion. */
- 0x0010 (16) /* Debug to trace idpcat activity */
- Example:
  - DEBUG_SAML = 31
- 0x0020 (32) /* Trace replay prevention */
- 0x0080 (128) /* Dump the entire XML tree */
- 0x0100 (256) /* Dump canonicalized buffers */
- 0x0200 (512) /* Debug for the library sort */
- 0x0800 (2048) /* Debug for namespace use */
- 0x2000 (8192) /* Debug output for certificate management */

Debugging SAML on Domino

- Example of Debug_SAML=15

```
[1284:000A-0B78] Decoded SAML assertion:
[1284:000A-0B78] <samlp:Response ID="_5984a166-e4ee-4008-b98f-0ea4e806638b" Version="2.0" IssueInstant="2013-08-0
[1284:000A-0B78] <samlp:Response ID="_5984a166-e4ee-4008-b98f-0ea4e806638b" Version="2.0" IssueInstant="2013-08-0
[1284:000A-0B78] [The previous line was truncated]
[1284:000A-0B78]   <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
[1284:000A-0B78]     http://louie.austin.ibm.com/adfs/services/trust
[1284:000A-0B78]   </Issuer>
[1284:000A-0B78]   <samlp:Status>
[1284:000A-0B78]     <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
[1284:000A-0B78]   </samlp:Status>
[1284:000A-0B78]   <Assertion ID="_313e3a8f-58f4-45d8-9fb9-7f94518ca1c6" IssueInstant="2013-08-09T03:18:22.829Z"
[1284:000A-0B78]     <Issuer>
[1284:000A-0B78]       http://louie.austin.ibm.com/adfs/services/trust
[1284:000A-0B78]     </Issuer>
[1284:000A-0B78]     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
[1284:000A-0B78]       <ds:SignedInfo>
[1284:000A-0B78]         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
[1284:000A-0B78]         <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
[1284:000A-0B78]         <ds:Reference URI="#_313e3a8f-58f4-45d8-9fb9-7f94518ca1c6">
[1284:000A-0B78]           <ds:Transforms>
[1284:000A-0B78]             <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
[1284:000A-0B78]             <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
[1284:000A-0B78]           </ds:Transforms>
[1284:000A-0B78]           <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
[1284:000A-0B78]           <ds:DigestValue>
[1284:000A-0B78]             e1qFCBTSmHki0nqu80YI2YyJIOVyxqhOGebeLv0OjSY=
[1284:000A-0B78]           </ds:DigestValue>
[1284:000A-0B78]         </ds:Reference>
[1284:000A-0B78]       </ds:SignedInfo>
[1284:000A-0B78]       <ds:SignatureValue>
[1284:000A-0B78]         SBijvohwQu2g1hAQf+s4DBHcmHfm1YZuCcP/jH+g1dRDlksxhCqX7SzCJU5XIQDt/tmKidftkQtXMCZPBqzF6Nvl
[1284:000A-0B78] [The previous line was truncated]
[1284:000A-0B78]       </ds:SignatureValue>
[1284:000A-0B78]       <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
[1284:000A-0B78]         <ds:X509Data>
[1284:000A-0B78]           <ds:X509Certificate>
[1284:000A-0B78]             MIIC5DCCAcygAwIBAgIQNN1s3BaB4pBEx7Ob+PMHLTANBgkqhkiG9w0BAQsFADAuMSwwKgYDVQQDEyNBREZT
[1284:000A-0B78] [The previous line was truncated]
```


Resource Links

- OASIS
  - https://www.oasis-open.org/
- Cookbooks
  - http://www-01.ibm.com/support/docview.wss?uid=swg21614543
    - Setting up TFIM (1.1 and 2.0)
    - Configuring Relying parties for TFIM
    - Setting up ADFS
    - Configuring Relying parties for ADFS

Press *1 on your telephone to ask a question.

Visit our Support Technical Exchange page or our Facebook page for details on future events.

To help shape the future of IBM software, take this quality survey and share your opinion of IBM software used within your organization: https://ibm.biz/BdxqB2

Find us on Facebook

IBM Collaboration Solutions Support page
http://www.facebook.com/IBMLotusSupport

follow us on twitter

ICS Support
http://twitter.com/IBM_ICSSupport

