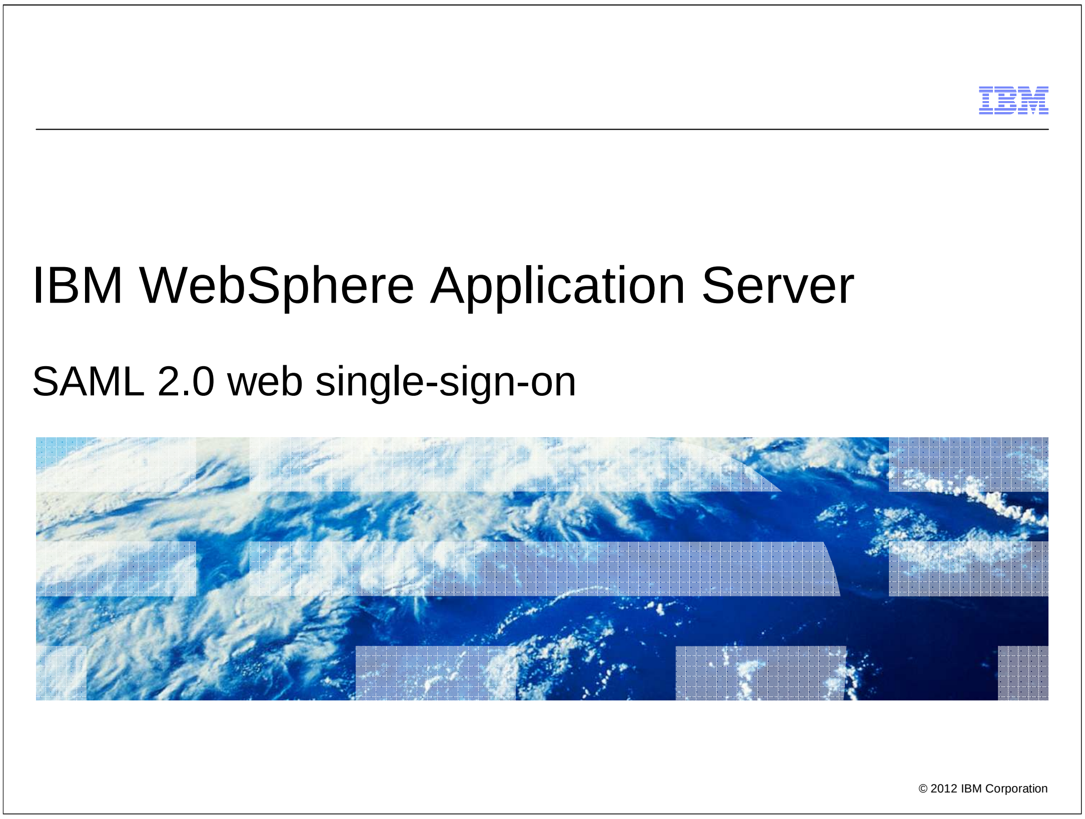
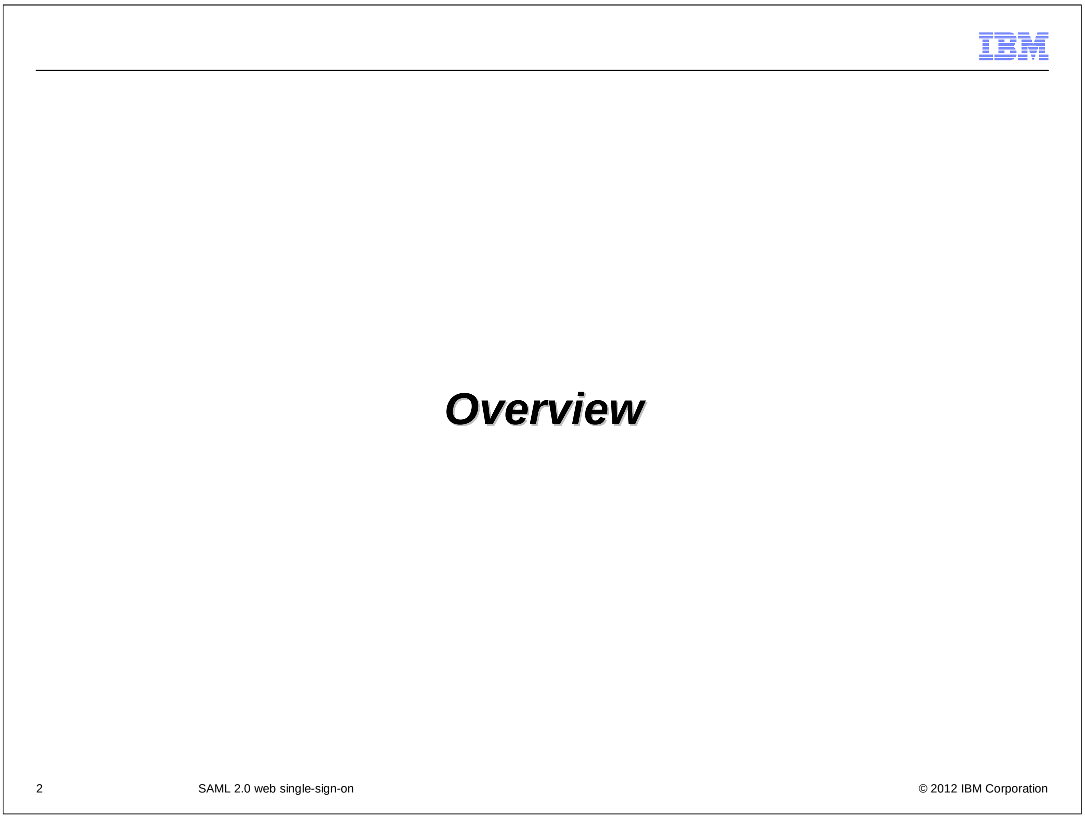


IBM WebSphere Application Server

SAML 2.0 web single-sign-on

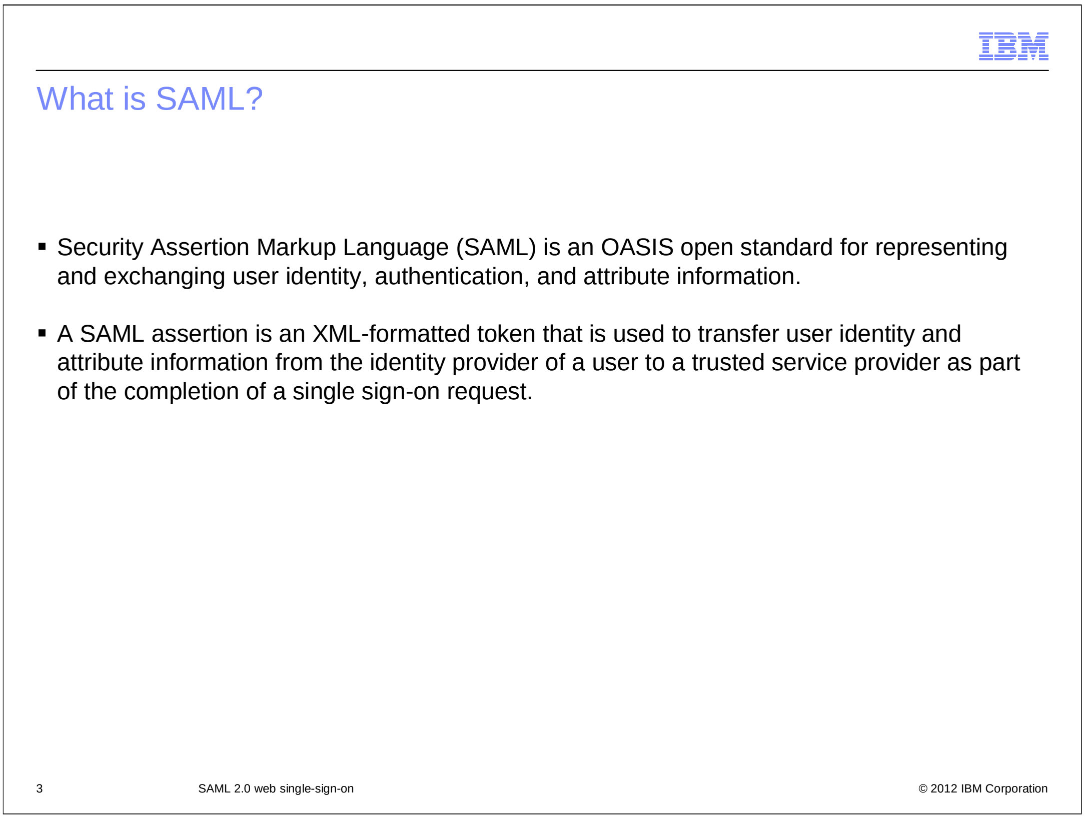
This presentation describes support for SAML 2.0 web browser Single Sign On profile included in IBM WebSphere® Application Server V7.0.0.23.



Overview

2 SAML 2.0 web single-sign-on © 2012 IBM Corporation

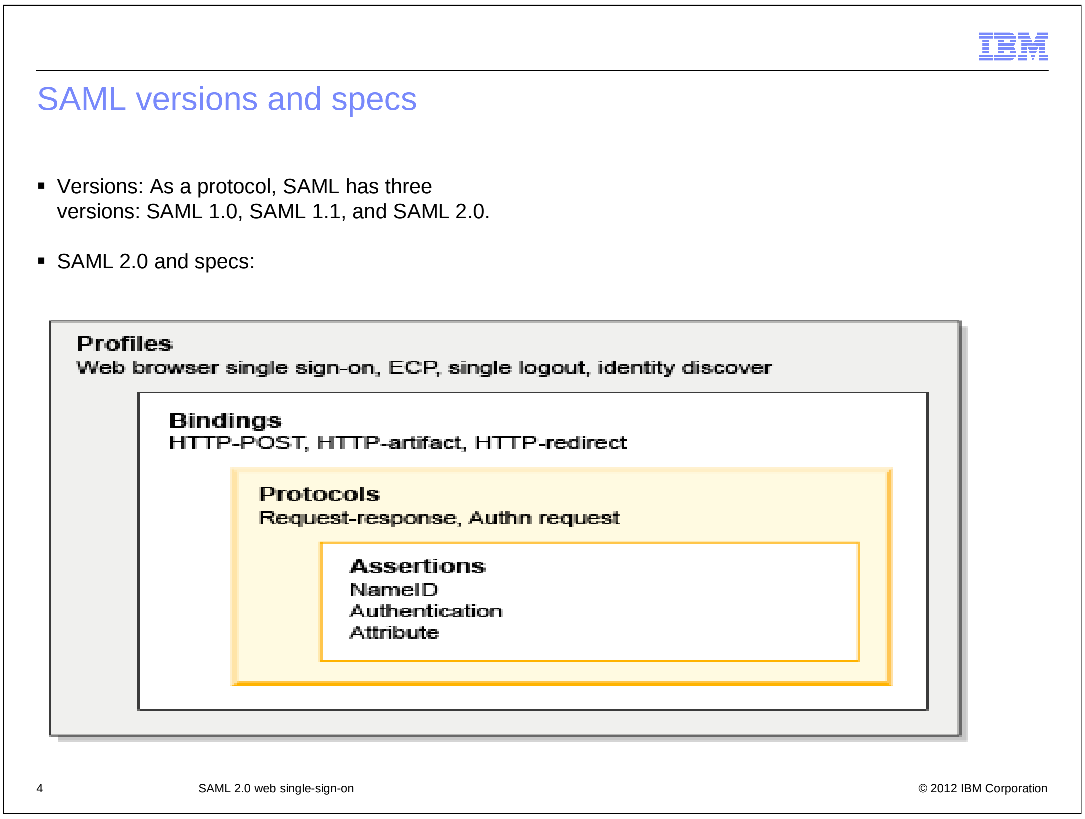
This feature provides a service provider for SAML 2.0 web browser SSO profile, which supports Identity Provider initiated post binding.



What is SAML?

- Security Assertion Markup Language (SAML) is an OASIS open standard for representing and exchanging user identity, authentication, and attribute information.
- A SAML assertion is an XML-formatted token that is used to transfer user identity and attribute information from the identity provider of a user to a trusted service provider as part of the completion of a single sign-on request.

A SAML assertion provides a vendor-neutral means of transferring information between federation business partners.



SAML versions and specs

- Versions: As a protocol, SAML has three versions: SAML 1.0, SAML 1.1, and SAML 2.0.
- SAML 2.0 and specs:

Profiles
Web browser single sign-on, ECP, single logout, identity discover

Bindings
HTTP-POST, HTTP-artifact, HTTP-redirect

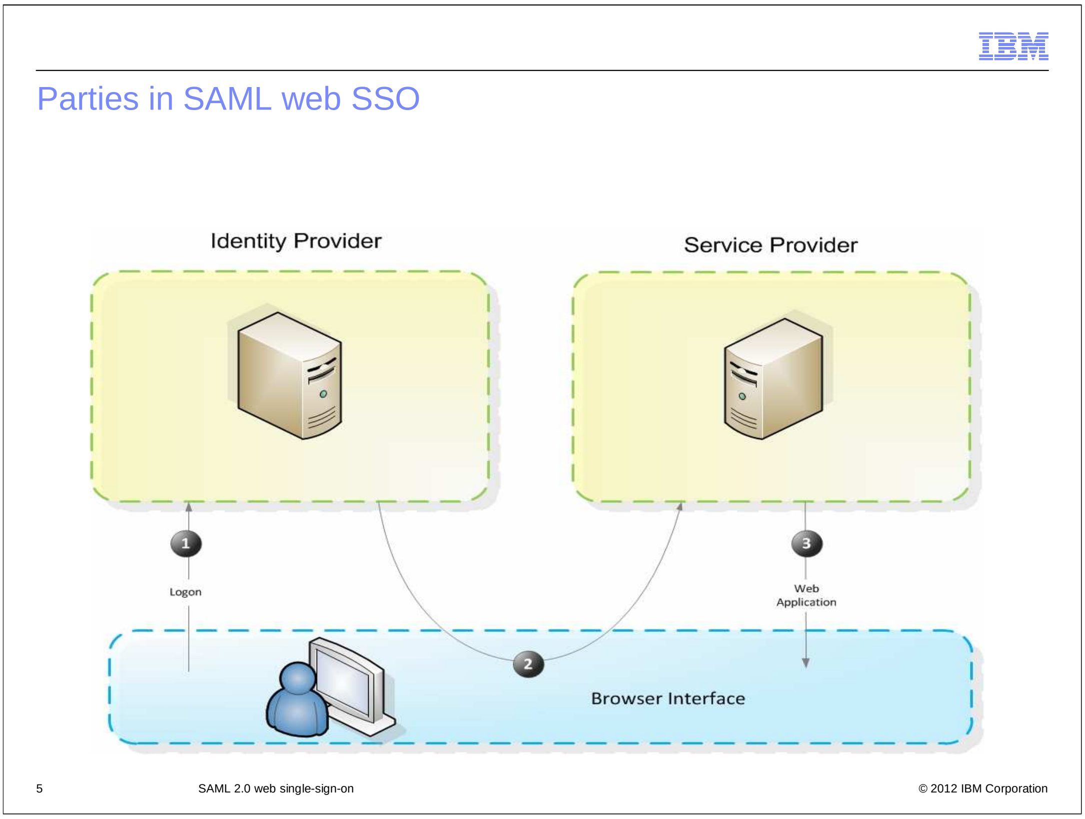
Protocols
Request-response, Authn request

Assertions
NameID
Authentication
Attribute

4 SAML 2.0 web single-sign-on © 2012 IBM Corporation

SAML 2.0 is an enhancement to the previous SAML 1 and 1.1 specifications, but is not compatible with those versions.

SAML 2.0 defines several request-response protocols, which all correspond to the action being communicated in the message. These protocols are HTTP-redirect based and involve the user's browser. SAML 2.0 has defined several binding options, HTTP redirect, HTTP POST, HTTP artifact, and SOAP. These options specify the way in which messages can be transported. SAML 2.0 HTTP POST enables SAML protocol messages to be transmitted within an HTML form using base64- encoded content. SAML 2.0 HTTP POST enables the SAML provider and consumer to communicate using an HTTP user agent as an intermediary. HTTP POST is sometimes called Browser POST, particularly when used in single sign-on operations. SAML 2.0 web Browser SSO Profile is defined to support web single sign-on. A web user either accesses a resource at a service provider, or accesses an identity provider such that the service provider and required resource are understood or implicit. The web user authenticates to the identity provider, which then produces an authentication assertion, and the service provider consumes the assertion to establish a security context for the web user.



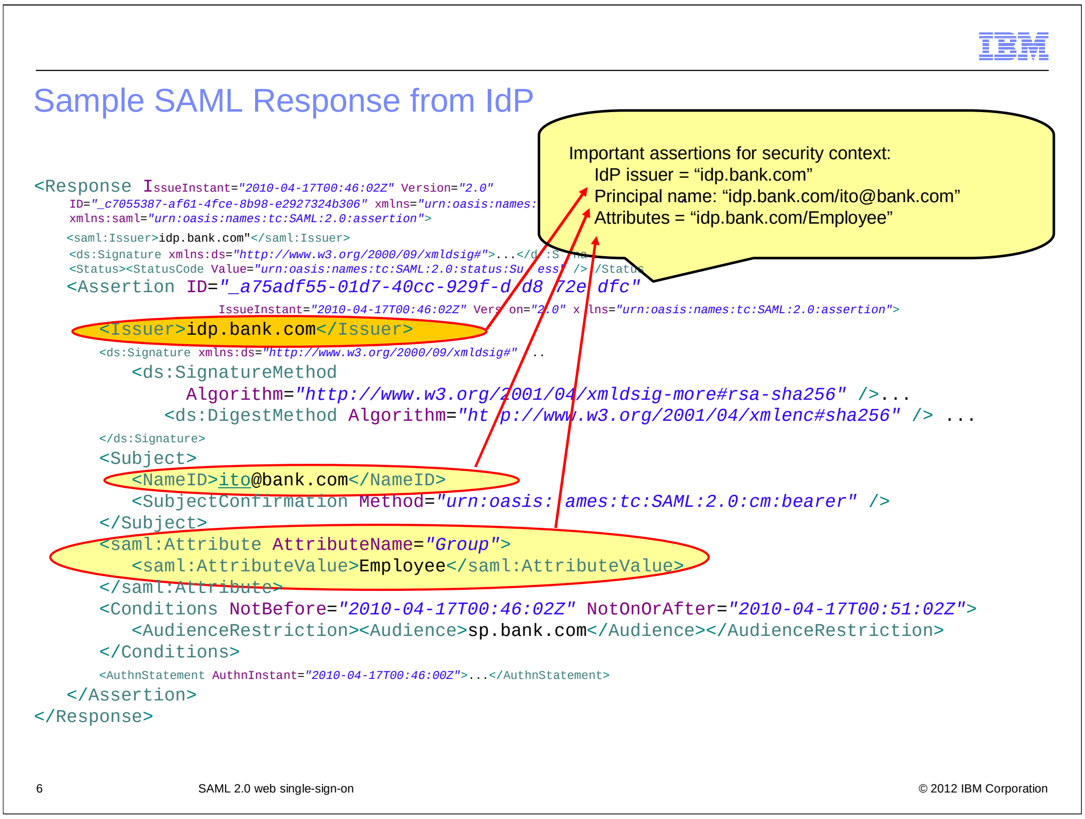
Parties in SAML web SSO

5 SAML 2.0 web single-sign-on

User authenticates to Identity provider (IdP), IdP sends SAML assertion to Service Provider (SP). SP validates SAML assertion and authorize web resource request.

Identity Provider (IdP) –is a producer of assertions that authenticates a principal.

Service Provider (SP) is a consumer of assertions that relies on the identity provider to identify and provide a principal. The SP will receive a SAML assertion containing the principle and security attributes to be used for a given request.



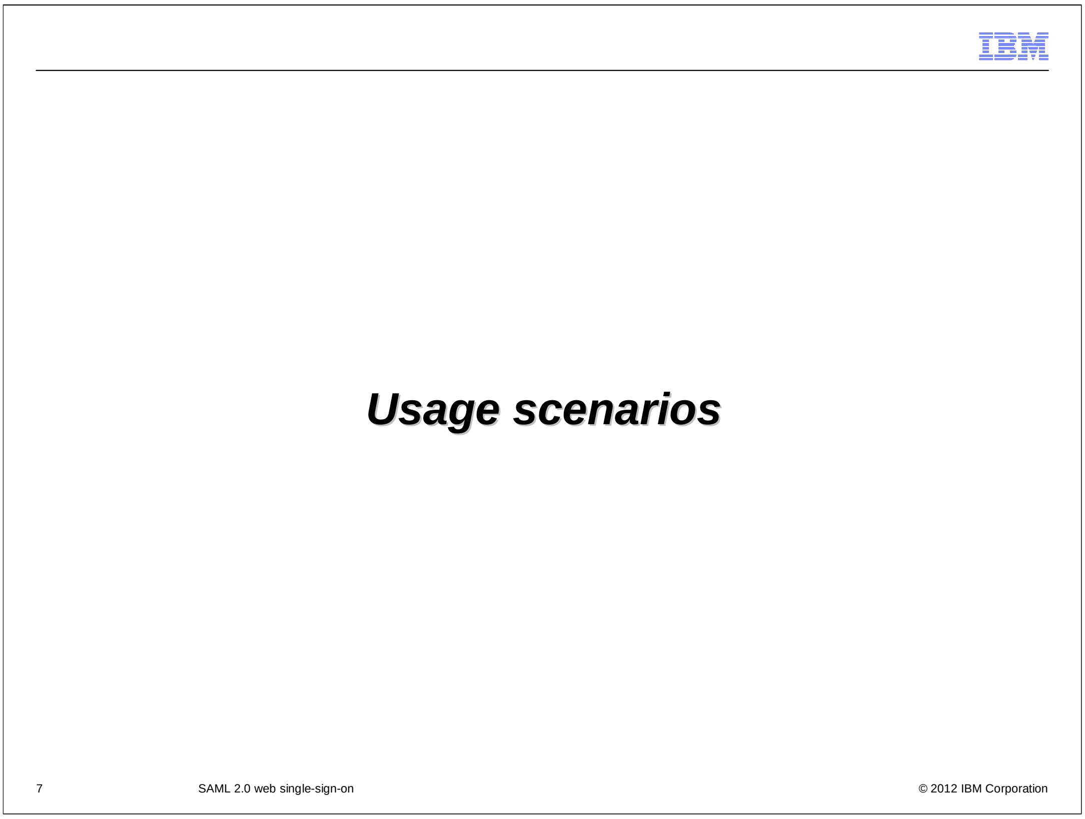
Sample SAML Response from IdP

Important assertions for security context:
IdP issuer = “idp.bank.com”
Principal name: “idp.bank.com/ito@bank.com”
Attributes = “idp.bank.com/Employee”

```
<Response IssueInstant="2010-04-17T00:46:02Z" Version="2.0"
     ID="_c7055387-af61-4fce-8b98-e2927324b306" xmlns="urn:oasis:names:
     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml:Issuer>idp.bank.com"</saml:Issuer>
     <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signa
     <Status><StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" /></Status
    <Assertion ID="_a75adf55-01d7-40cc-929f-d d8 72e dfc"
                  IssueInstant="2010-04-17T00:46:02Z" Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
       <Issuer>idp.bank.com</Issuer>
       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" ..
          <ds:SignatureMethod
               Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />...
             <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" /> ...
       </ds:Signature>
       <Subject>
          <NameID>ito@bank.com</NameID>
          <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer" />
       </Subject>
       <saml:Attribute AttributeName="Group">
          <saml:AttributeValue>Employee</saml:AttributeValue>
       </saml:Attribute>
       <Conditions NotBefore="2010-04-17T00:46:02Z" NotOnOrAfter="2010-04-17T00:51:02Z">
          <AudienceRestriction><Audience>sp.bank.com</Audience></AudienceRestriction>
       </Conditions>
       <AuthnStatement AuthnInstant="2010-04-17T00:46:00Z">...</AuthnStatement>
    </Assertion>
</Response>
```

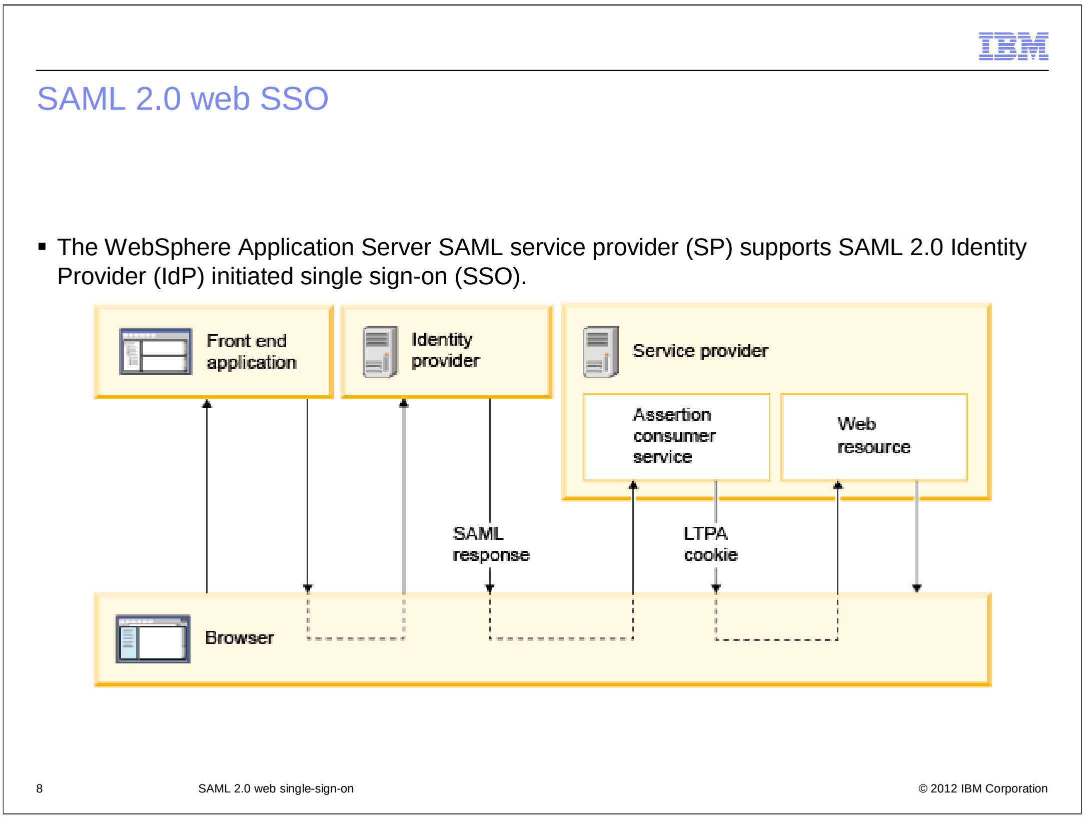
6 SAML 2.0 web single-sign-on © 2012 IBM Corporation

This is a sample SAML protocol message from IdP



Usage scenarios

This section shows an example use case of this new feature.



SAML 2.0 web SSO

- The WebSphere Application Server SAML service provider (SP) supports SAML 2.0 Identity Provider (IdP) initiated single sign-on (SSO).

8 SAML 2.0 web single-sign-on © 2012 IBM Corporation

WebSphere IdP initiated SSO service is implemented as a Trust Association Interceptor, and can be described as follows:

1. User accesses a front end web application that can reside on the IdP, SP, or elsewhere.

2. Front end web application redirects user to IdP and user authenticates to IdP.

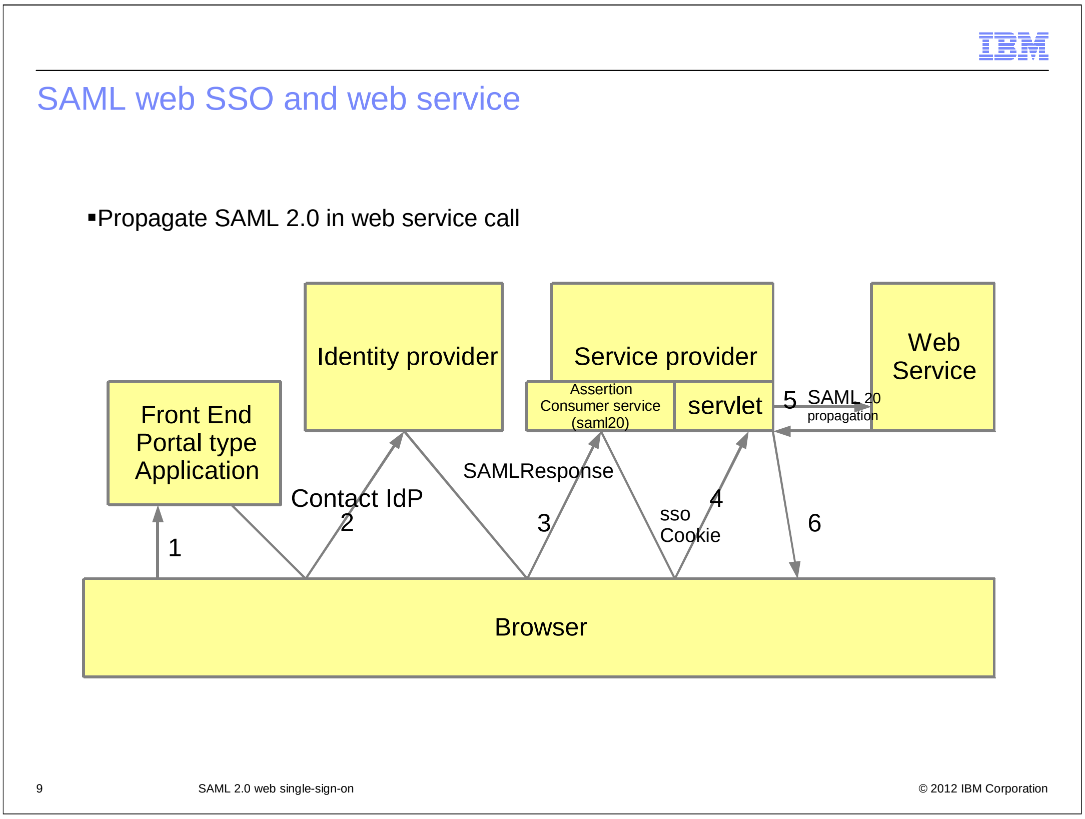
3. IdP redirects user to Assertion Consumer Service (ACS) in SP by sending SAML response over HTTP POST inside a hidden form.

4. SP processes SAML response and creates WebSphere security context.

5. SP adds LTPA cookie to HTTP response and redirects request to web resource or business application.

6. WebSphere Application Server intercepts request, and maps LTPA cookie to security context and authorizes user access to the requested web resource.

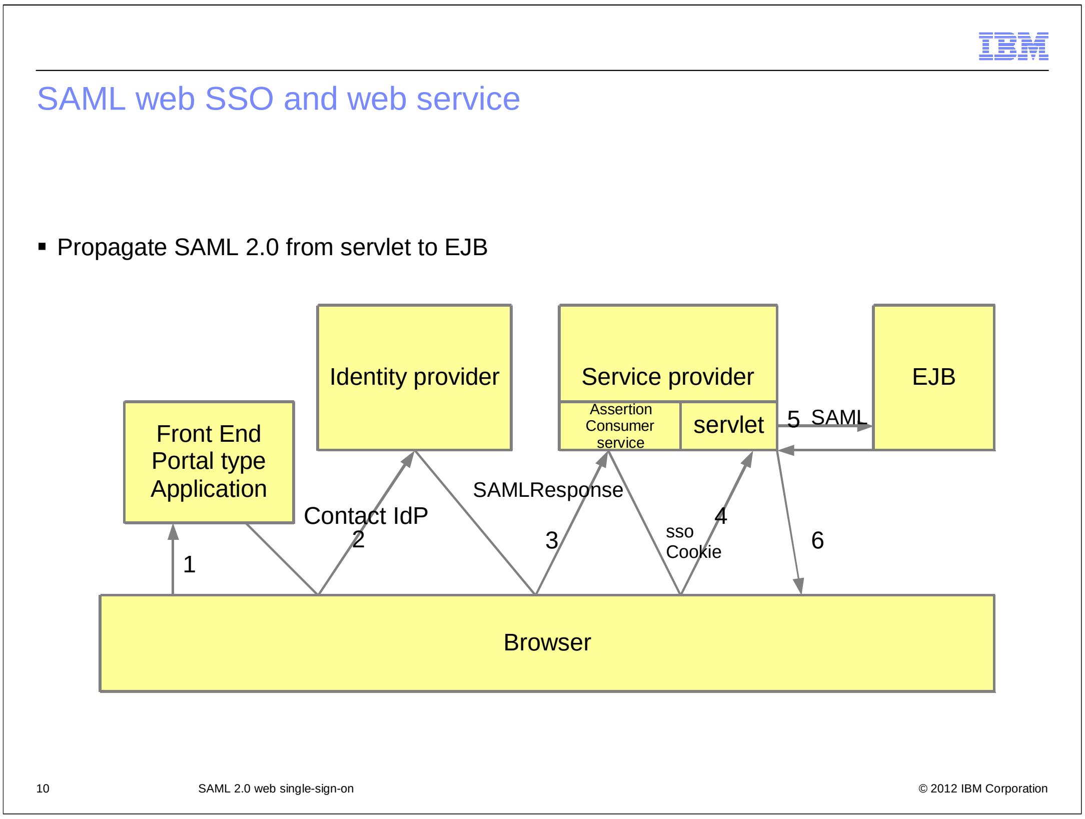
7. WebSphere Application Server sends HTTP response back to user.



SAML web SSO and web service

- Propagate SAML 2.0 in web service call

In a SAML web SSO scenario, you can propagate a SAML assertion from a service provider to a downstream web service. After SSO is completed and the user is authorized to access the web resource, you can make a web service call within the servlet with the SAML assertion as a caller token.



SAML web SSO and web service

- Propagate SAML 2.0 from servlet to EJB

10 SAML 2.0 web single-sign-on © 2012 IBM Corporation

In a SAML web SSO scenario, you can propagate a SAML assertion from a service provider to a downstream EJB. After the SSO is completed and the user is authorized to access a web resource, you can make an EJB call within the servlet with the SAML assertion as a caller token.

Summary of features inside WebSphere

11 SAML 2.0 web single-sign-on © 2012 IBM Corporation

1. The WebSphere SAML TAI, or trust association interceptor, can be configured not to require SAML users in WebSphere Security’s user registry. That is, the WebSphere user registry does not contain any users as long as the user is authenticated by a SAML identity provider. The WebSphere runtime subject is build from the SAML assertion without calling into WebSphere user registry.

2. The WebSphere SAML TAI can be configured to verify a SAML user in the WebSphere user registry, and the WebSphere runtime subject is built based on the user’s attributes in the user registry.

3. When using ID assertion to create a WebSphere runtime subject, WebSphere SAML TAI can extract SAML token attributes, and use those attributes to create the WebSphere security subject’s realm, principal, unique ID, and group memberships.

4. The WebSphere SAML TAI supports using a plug-in for external identity mapping before creating the security subject.

5. While doing SAML user ID assertion, this TAI can optionally retrieve the SAML user's groups from the user registry.

6. The WebSphere SAML TAI provides several administrative commands to simplify enablement and configuration; those commands include Add, show, and delete tasks to configure and manage the SAML web SSO TAI; and import or export metadata to establish SSO partnership with an IdP.

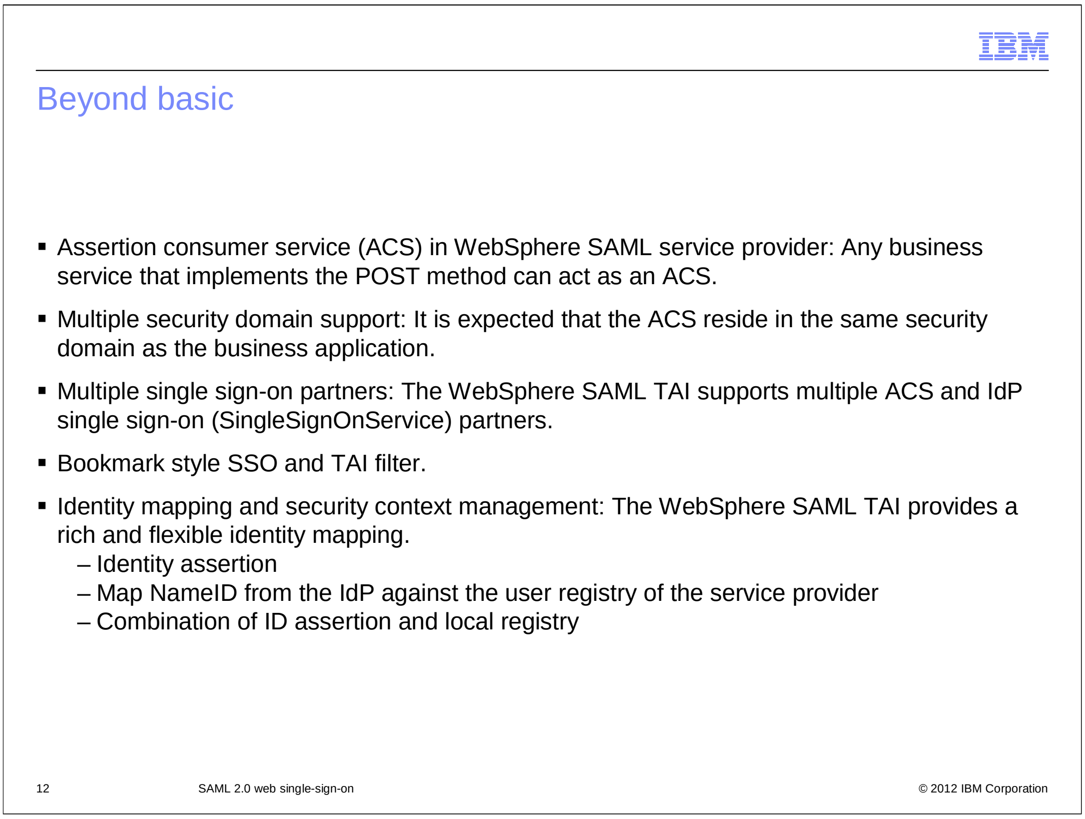
7. The WebSphere SAML TAI supports single-sign-on with multiple identity providers. Within TAI, you can have one AssertionConsumerService instance working with multiple identity provider’s SingleSignOnService, and you can also have multiple AssertionServiceprovider instances working with multiple SingleSignOnServices.

8. The WebSphere SAML TAI has an IdP selection filter that routes request back to the proper IdP if a request has not yet been authenticated.

9. The WebSphere SAML TAI supports both RSA-SHA1 and RSA-SHA256 signature methods.

10. WebSphere SAML TAI preserves the SAML token in the subject, so an application can retrieve a SAML token from the executed thread for additional authorization.

11. Any business application that implements HTTP POST method can act as SAML AssertionConsumerService.



Beyond basic

- Assertion consumer service (ACS) in WebSphere SAML service provider: Any business service that implements the POST method can act as an ACS.
- Multiple security domain support: It is expected that the ACS reside in the same security domain as the business application.
- Multiple single sign-on partners: The WebSphere SAML TAI supports multiple ACS and IdP single sign-on (SingleSignOnService) partners.
- Bookmark style SSO and TAI filter.
- Identity mapping and security context management: The WebSphere SAML TAI provides a rich and flexible identity mapping.
  - Identity assertion
  - Map NameID from the IdP against the user registry of the service provider
  - Combination of ID assertion and local registry

12 SAML 2.0 web single-sign-on

1.Any business service that implements the POST method can act as an ACS. Using a target business servlet as an ACS is preferred, because it reduces one round trip between the browser and the service provider server.

2. The WebSphere SAML TAI supports multiple ACS and IdP SingleSignOnService partners. One SSO partner is defined as one ACS URL, and multiple SingleSignOnServices. Each SSO partner can have its own validation rules, mapping rule from assertion to subject, or a rule to start the SSO with its own IdP.

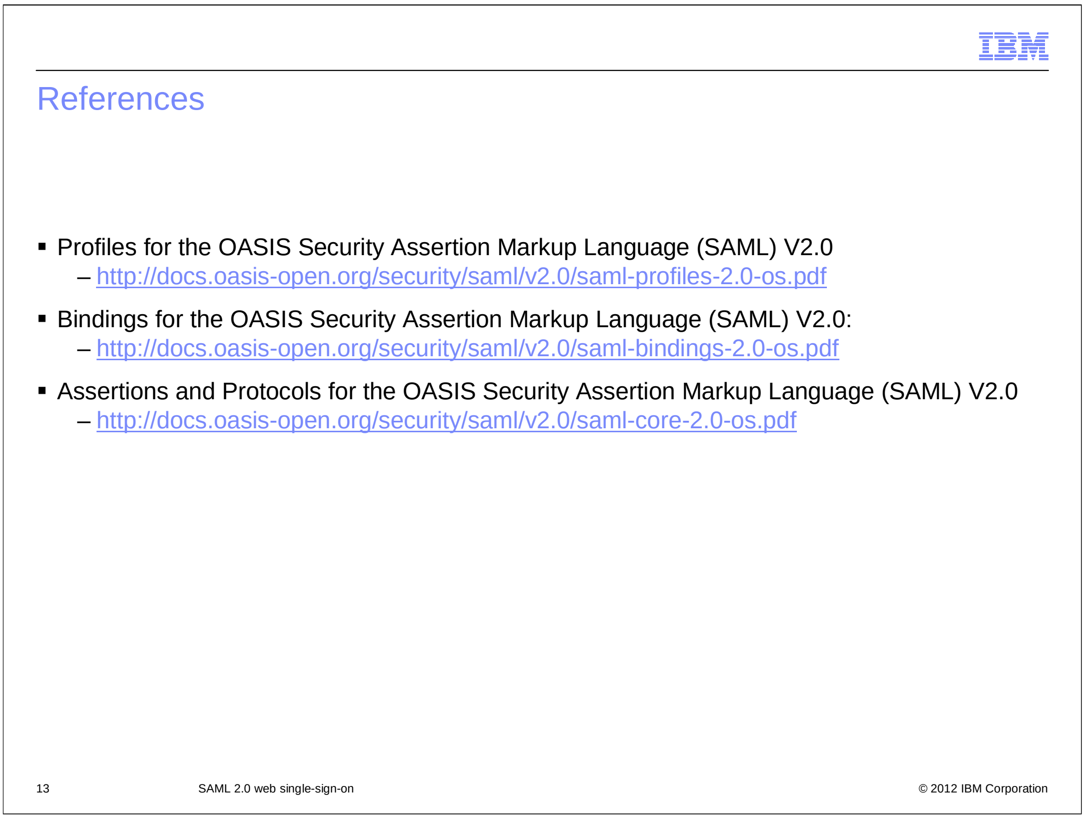
3. If a user accesses the business application without authenticating to the IdP first, the WebSphere SAML TAI can be configured to initiate an SSO. Each SSO partner configuration contains an IdP login application and a routing filter. The TAI filter allows an IdP-initiated SSO to provide similar functionality as the combination of an SP-initiated SSO and an IdP discovery service.

4. The WebSphere SAML TAI provides a rich and flexible identity mapping, and can be classified as follows:

Identity assertion maps the SAML assertion to the WebSphere platform subject without a local registry.

Map NameID from the IdP against the user registry of the service provider, and build the subject from the registry. Three scenarios are supported: Directly map the SAML NameID to the local registry, a plug-in point for custom mapping, followed by using a new user to build the subject, and Map NameID to the user registry, and fall back to ID assertion.

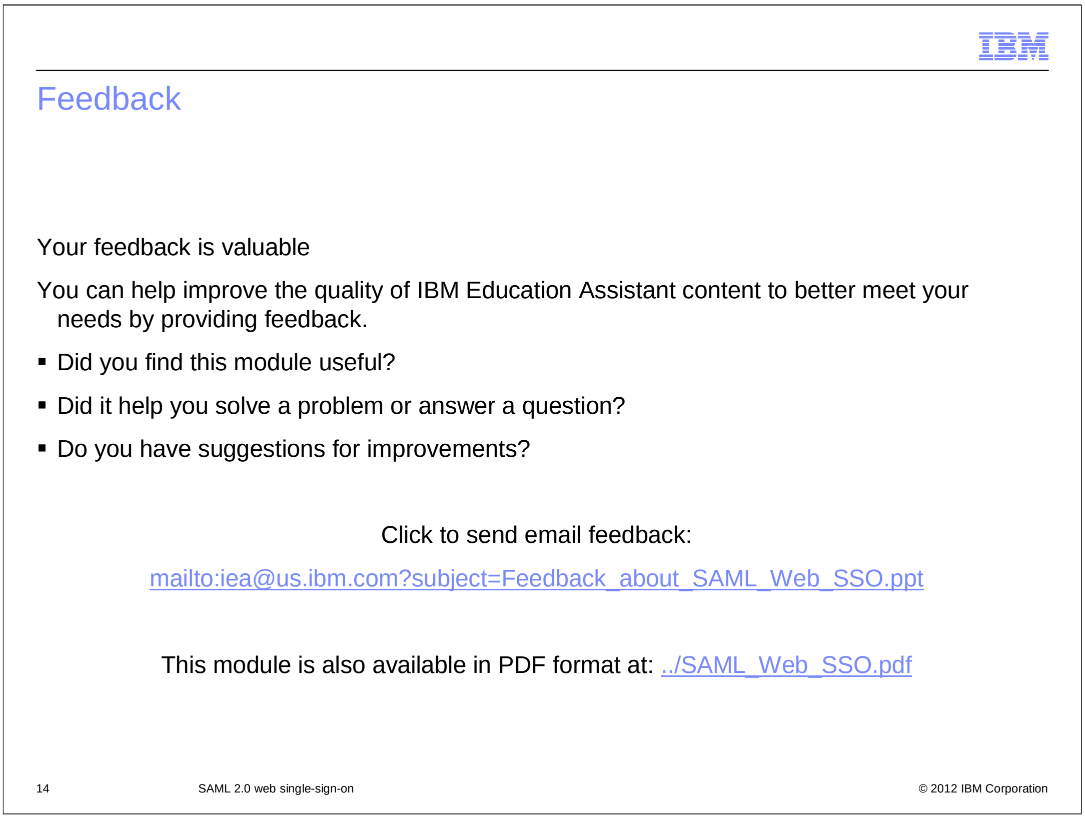
Combination of ID assertion and local registry: In addition to ID assertion, TAI searches parent groups of the asserted groups in the user registry of the service provider, and includes the parent groups into the subject. For example, authorization is granted to parent groups, but the identity provider does not know the parent group names.



References

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

These links access additional information about SAML 2.0 web browser Single Sign On profiles.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

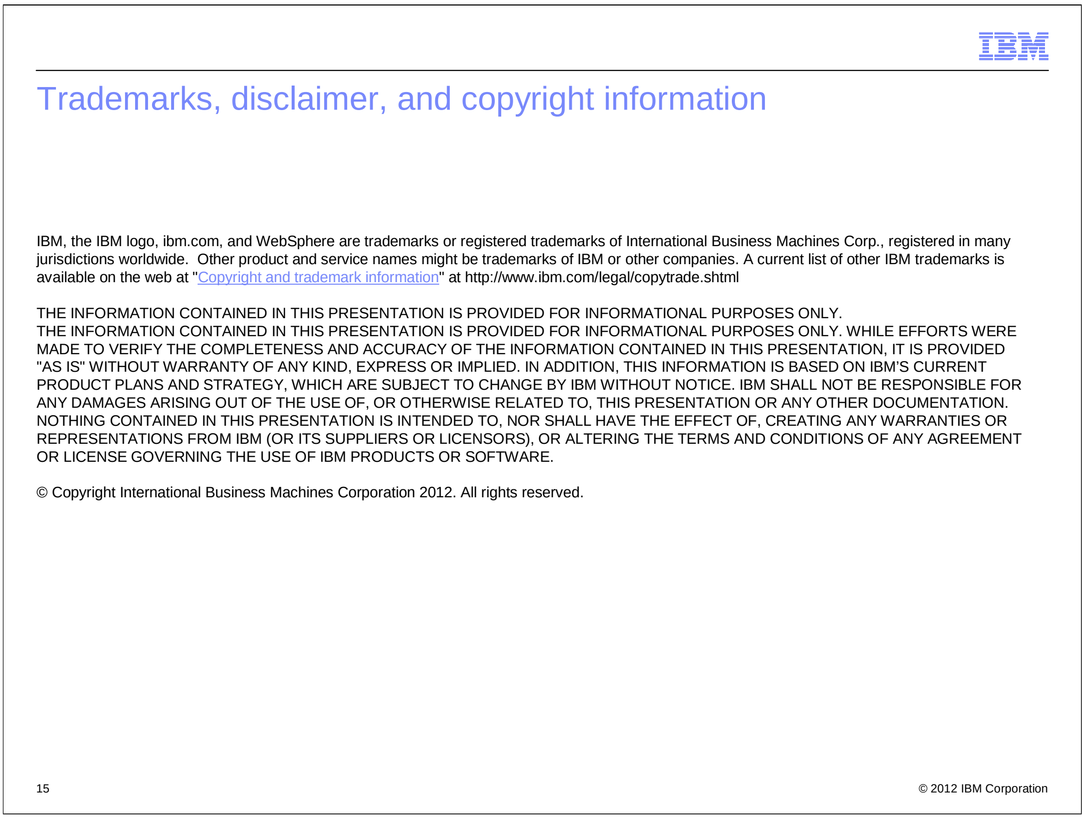
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_SAML_Web_SSO.ppt

This module is also available in PDF format at: ../SAML_Web_SSO.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.