Federated SSO Authentication Service

Technical Overview

July 2009

Table Of Contents

Introduction

Federated single-sign on (SSO) standards like SAML and WS-Federation provide secure mechanisms for passing credentials and related information between different web sites that have their own authorization and authentication systems. SAML is an open standard developed by the OASIS Security Services Technical Committee. SAML 1.0 was ratified as an OASIS standard in November, 2002. WS-Federation was developed by a group of companies led by Microsoft and it offers equivalent federated SSO functionality to SAML.

The SAML protocol has seen significant success, gaining momentum in financial services, higher education, government, and other industry segments. SAML support has been broadly implemented by all major Web access management vendors. The U.S. Government General Services Administration (GSA) requires all vendors participating in the US E-Authentication Identity Federation program to be SAML 2.0 compliant.

SAML compliant web sites exchange user credential information via SAML assertions. A SAML assertion is an XML document containing trusted statements about a subject including a username, privileges, etc. SAML

assertions are usually digitally signed to ensure their authenticity. For more information on the SAML standard, refer to Appendix B – Resources.

Many large enterprises have deployed federated Identity and Access Management (IAM) systems such as CA SiteMinder, Sun Microsystems Open SSO, or Windows ADFS on their corporate intranets. These IAM systems handle the user authentication and single sign-on (SSO) requirements for employees and partners. IAM systems use the SAML or WS-Federation protocols to interoperate with partner web sites outside their firewalls. Customers can utilize their IAM systems to automatically authenticate their users to WebEx services. This will increase efficiency since users do not have to remember their WebEx username and password to host meetings. Security is increased over current URL API based SSO integrations since no WebEx passwords will be stored or transmitted.

WebEx Federated Authentication Service

The WebEx Federated Authentication Service (FAS) allows employees and affiliates of a WebEx customer organization to authenticate with a WebEx site using the SAML 1.1, 2.0 or WS-Federation 1.0 protocols.

The WebEx FAS accepts SAML assertions using the Browser/POST or "push" model profile. The customer web site acts as the Identity Provider (IdP) and the WebEx site acts as the Service Provider (SP) or Relying Party (RP).

The WebEx FAS functions as a SAML Assertion Consumer. The WebEx FAS accepts a signed SAML Response HTTP POSTed from the customer web site. FAS verifies the assertion signature and checks if the included username is a valid WebEx host. If so, the user will be logged into the WebEx site and they can schedule and host meetings.

Requirements

Identity and Access Management System

Customers need an Identity and Access Management (IAM) System that conforms to the SAML v 1.1, 2.0 or WS-Federation 1.0 standard. Customers can develop their own SAML-compliant IAM system using programming libraries such as OpenSAML (http://www.opensaml.org/) or they can purchase a commercial third party IAM system.

The IAM system should function as a SAML or WS-Federation Identity Provider (IdP). The IAM system should be able to produce SAML Assertions or WS-Fed tokens digitally signed with X.509 certificates

The WebEx FAS has been tested with the following commercial IAM systems:

- CA SiteMinder
- Ping Identity PingFederate
- Sun Microsystems OpenSSO Enterprise
- Microsoft Windows Server ADFS and Geneva
- Novell Identity Manager
- IBM Tivoli Federated Identity Manager
- Siemens IT Solutions DirX
- TriCipher Armored Credential System
- Fugen Solutions
- Cloud-Identity

- Google Enterprise SAML IDP

X.509 Certificate

Customers need to acquire an X.509 digital certificate from a Certificate Authority. Certificate Authorities are trusted institutions including government agencies and companies such as Verisign and Thawte. Customers can serve as their own Certificate Authorities rather then using trusted third party organizations.

To use WebEx FAS, the customer's should upload a valid X.509 certificate in PEM format to their WebEx meeting site. Each SAML assertion that is posted to the WebEx FAS must be digitally signed with the private key from the X.509 certificate.

Single Sign On

The WebEx FAS can be used to implement robust Single Sign-On (SSO) functionality between a corporate portal and a WebEx meeting site. Customers can implement SSO functionality with FAS in a manner similar to implementations using the current WebEx URL API. In place of the URL API login command, the portal is the IdP posting a SAML assertion to the WebEx FAS.

Each corporate user needs to have their own WebEx user account in order to host meetings. The SAML assertion posted to the WebEx FAS includes a unique WebEx username or email address but no password. Thus, SSO systems using WebEx FAS do not require corporate portals to store and forward user passwords from their intranet to the WebEx site.

IdP Initiated SSO

WebEx FAS supports IdP initiated SSO with the Browser/POST binding for SAML 1.1 and 2.0. In this scenario, users would access WebEx through their corporate IAM system. The IAM system acts as an IdP which would authenticate the user and verify they are authorized by the company to use WebEx. The IAM posts a signed SAML assertion to the WebEx FAS which verifies the signature and authenticates the user or optionally provisions a WebEx account.

WebEx FAS also supports IdP-initiated SSO with the Browser/Artifact binding for SAML 1.1 only.

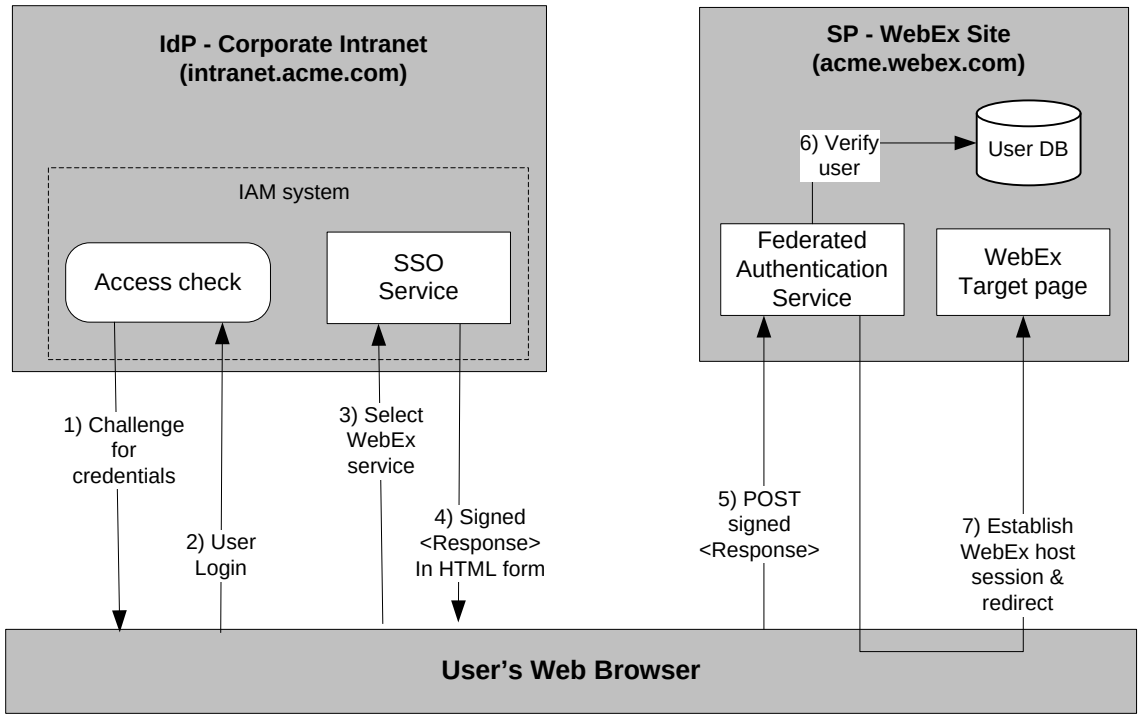

Fig. 1 – IdP initiated SAML SSO to WebEx FAS

Process Flow

1. An Acme employee user attempts to access a resource on intranet.acme.com. If the user does not have a valid local security context with the IAM (IdP) system, she will be challenged to supply their credentials.
2. The user provides valid company credentials and a local security context is created for the user at the IdP.
3. The user selects a menu option or link in the IdP to request access to the company WebEx meeting site, acme.webex.com. This causes the IdPs Single Sign-On Service to be called.
4. The IdP SSO Service builds a SAML assertion containing the user's corporate email address or username and digitally signs it before placing it within a SAML <Response> message. The <Response> message is then placed within an HTML FORM as a hidden form control named SAMLResponse. The IdP SSO service sends the HTML form back to the browser in the HTTP response.
5. The browser, issues an HTTP POST request to send the form to the WebEx FAS which obtains the <Response> message from the HTML FORM and validates the digital signature.
6. FAS verifies the user has a matching account in the WebEx user database or automatically provisions a new account.
7. FAS establishes a WebEx host session and redirects the browser to the standard WebEx meeting page. The user can now schedule and host WebEx meetings.

SP Initiated SSO

WebEx FAS supports SP-initiated SSO with the Redirect/POST bindings for SAML 2.0. In this scenario, users start at the WebEx meeting site and are redirected to their IAM (IdP) system for authentication. The IdP authenticates the user and sends a SAML assertion back to the WebEx FAS. See Fig. 2 and the process flow below.

WebEx FAS also supports SP-initiated SSO with the Passive Requester binding for WS-Federation 1.0.

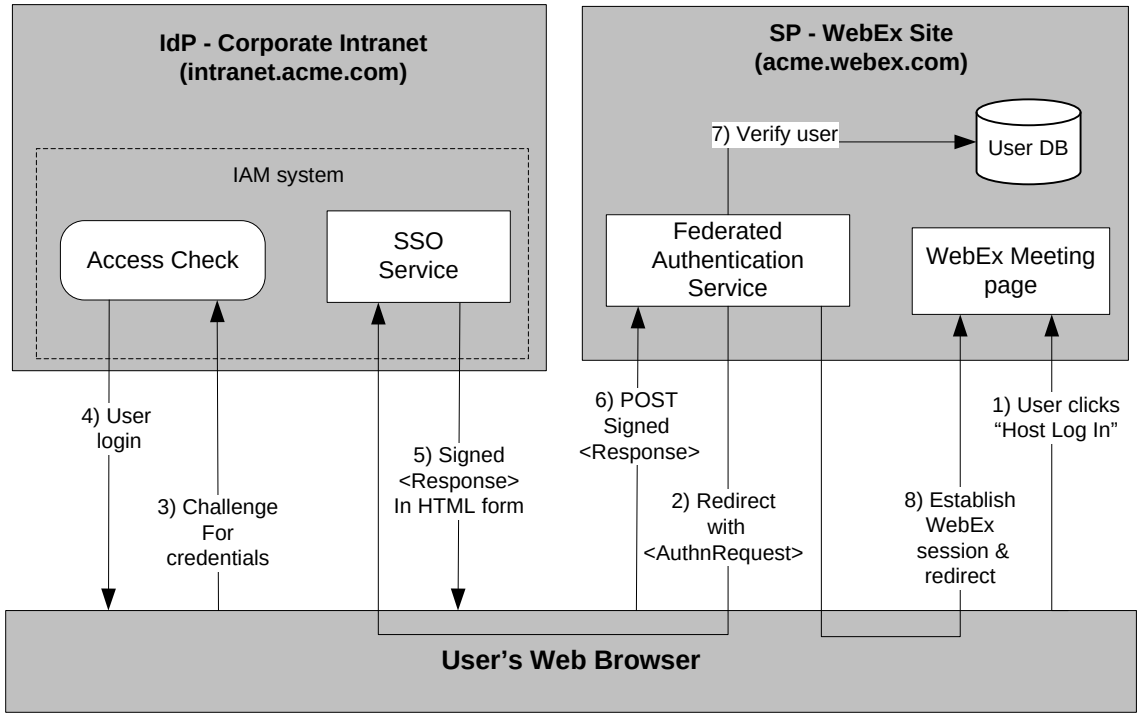

Fig. 2 – WebEx FAS (SP) initiated SAML SSO

Process Flow

1. The employee user opens their WebEx meeting site (acme.webex.com) and clicks “Host Log In”.
2. The WebEx FAS acting as a Service Provider (SP) sends an HTTP redirect response to the browser pointing to the corporate IdP SSO service. The HTTP response includes an <AuthnRequest> that contains information about the SP including the FAS URL.
3. The IdP SSO service determines whether the user has an existing IdP logon security context. If not the IdP challenges the user to provide valid company credentials.
4. The user provides valid company credentials and a local logon security context is created for the user at the IdP.
5. The IdP SSO service builds a SAML assertion containing the user’s corporate email address or username and signs it before placing it within a SAML <Response> message. The <Response> is placed within an HTML FORM as a hidden form control named SAML Response. The SSO Service sends the HTML form back to the browser in the HTTP response.
6. The browser, issues an HTTP POST request to send the form to the WebEx FAS which obtains the <Response> message from the HTML FORM and validates the digital signature.
7. FAS verifies the user has a matching account in the WebEx user database or automatically provisions a new account.
8. FAS establishes a WebEx host session and redirects the browser to the standard WebEx meeting page. The user can now schedule and host WebEx meetings.

Integrated Windows Authentication

Integrated Windows Authentication (IWA) allows a user to log into their Microsoft Windows PC and authenticate to web applications supporting IWA without having to re-enter their username and password. Windows generates a Kerberos or NTLMSSP token upon login and this SSO token is passed on to all IWA compatible web applications.

WebEx FAS can use IWA If the customer’s IAM (IdP) supports IWA. Thus a user could log into their Windows PC and automatically authenticate to their WebEx meeting site without having to login again.

Automatic Account Provisioning

If the IAM supports SAML 2.0, FAS can be configured to automatically create and update WebEx user accounts. If auto account creation is enabled for the site, then the SAML assertion should specify the following user attributes in a SAML 2.0 assertion to automatically provision a new WebEx user account. If auto account update is enabled and the user in the assertion already exists in the WebEx database, the specified user fields will be updated.

Mandatory Parameters

```
uid = WebEx username, usually set to the corporate username.
lastname, firstname = user first and last name
email = user email address
```

Optional Parameters

```
OPhoneCountry, OPhoneArea, OPhoneLocal, OPhoneExt = Office Phone Number
FPhoneCountry, FPhoneArea, FPhoneLocal, FPhoneExt = Alternate Phone Number
Addess1, Address 2 = User Street Address
City, State, ZipCode = User City, State & ZipCode
Country = User’s country
TC1…TC10 = User tracking Codes, often used to identify departmental usage.
MT = WebEx Meeting Types specified as “MT=<151,345,587>”
```

Process Flow

1. User authenticates to their corporate portal via their IAM system.
2. User selects a portal option to access WebEx Meeting services.
3. IAM system posts a signed SAML assertion containing the WebEx username to the WebEx SAML Authentication Service.
4. For a first time WebEx user:
   - If auto account creation is enabled for the site, then the IAM system should specify new user profile attributes in the SAML Assertion and the new user will be provisioned in WebEx.
   - Typically, the new user's WebEx username is set to the corporate portal username. WebEx will automatically set the new WebEx user's password to a random string.
   - If auto account creation is not enabled for the site then FAS will return a user not found exception.
5. The user is successfully authenticated to the WebEx site. She can now schedule, edit and host WebEx meetings.

Since corporate employees do not know their WebEx passwords, they cannot login to the site outside of their corporate portal. When an employee leaves the company, they will lose access to their corporate portal and to the WebEx site accordingly.

WebEx Productivity Tools SSO

WebEx Productivity Tools allow users to schedule and launch online meetings from Microsoft Outlook, PowerPoint, Word, Excel, Lotus Notes, WebEx One-Click, instant messaging and other applications. WebEx Productivity Tools support SAML 2.0 and WS-Federation 1.0 SSO with WBS 27+.

The WebEx Productivity Tools configuration screen requires meeting hosts to configure their WebEx site URL. If the user specifies a site with WebEx FAS enabled, they no longer have to enter their WebEx User name and Password. Instead, the WebEx Productivity Tools configuration screen will open a browser window and redirect to the customer's IAM system. The IAM system acts as an IdP which would authenticate the user and verify they are authorized by the company to use WebEx. The IAM posts a signed SAML assertion or WS-Federation token to the WebEx FAS which verifies the signature and authenticates the user or optionally provisions a WebEx account.

Single Logout

With single sign is implemented, an IdP usually shares a single authentication context with multiple service providers. WS-Federation 1.0 and SAML 2.0 offers a single logout profile which allows a user to easily terminate each session across multiple service providers at once. As a service provider (SP), the WebEx FAS can initiate a single logout request to the customer's IdP which will propagate the logout request to other SPs. The IdP or other SPs can also initiate a single logout request which will be propagated to WebEx FAS which will then terminate the WebEx session.

With Single Logout enabled, when a user presses the "Log Out" button on the WebEx meeting site, WebEx FAS will send a signed <LogoutRequest> message to the IdP. The IdP will then send <LogoutRequest> messages to all the SPs that the user is logged into. Each SP will respond to the IdP with a <LogoutResponse> message. After the IdP receives <LogoutResponse> messages from each SP, it sends a final <LogoutResponse> message to the WebEx FAS. WebEx FAS then terminates the WebEx meeting session to complete the single logout process.

WebEx FAS Capability Matrix

The following table summarizes WebEx FAS functionality when used with each of the supported federated SSO protocols.

	WS-Federation 1.0	**SAML 1.1**	**SAML 2.0**
IdP Initiated SSO	No	Yes	Yes
SP Initiated SSO	Yes	No	Yes
Productivity Tools SSO	Yes	No	Yes
Integrated Windows Authentication	Yes	No	Yes
Automatic Account Provisioning	Yes	Requires custom Java programming	Yes
Single Logout	Yes	No	Yes

Appendix A - Example SAML Responses

SAML 1.1 Authentication

Here is an example of a digitally signed SAML response document containing a SAML 1.1 assertion. The assertion should include a valid WebEx username in the <NameIdentifier> element. Site specific options are highlighted in bold.

```
<Response xmlns="urn:oasis:names:tc:SAML:1.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
IssueInstant="2005-01-23T00:54:48.913Z"
MajorVersion="1" MinorVersion="1" Recipient="www.webex.com"
ResponseID="d0aac0fb9e6b4ffda4576e7a15e55b5d">
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
         c14n#"></ds:CanonicalizationMethod>
         <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
         sha1"></ds:SignatureMethod>
         <ds:Reference URI="#d0aac0fb9e6b4ffda4576e7a15e55b5d">
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
               signature"></ds:Transform>
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                  <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-
                  c14n#" PrefixList="#default code ds kind rw saml samlp typens">
                  </ec:InclusiveNamespaces>
               </ds:Transform>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
            </ds:DigestMethod>
            <ds:DigestValue>Jwpxb7znm1FNpTnvlnGdHPTF2I0=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>
      FoRuDU5BWuY7+Jng9Hmt8WjHbNn++kDsRIfLNR5XhtxwESZIvqafXTPmSEEWBRxYWcPEjfsq62jQ
      hDP5BvnSX16SR1wlvLJs+unpBeq/xAAGfQV+rXM+UqQoDQhGdTdfRnPs9aItJT0uZF9vL/M1eD/l
      NiAkoPfFusYVyoVVfZlpsZMc7yRH1w7+ke82daF6GZfwkGL9YmROHoVfgFIS1K+Mt+ZgXP/zI90o
      1BSaVlo9I5nk12AapiIYihrpyZH5Wnpvwk3HCv9ySmsDpG2B6SevXZeBsclJ3f6PFYhDNmmPq+Q8
      9u/VUBPVwfRzEmvC1dOCJCYws2oX0sBXqhPnNA==
      </ds:SignatureValue>
   </ds:Signature>
   <Status>
      <StatusCode Value="samlp:Success"></StatusCode>
   </Status>
   <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
   AssertionID="c65e497d8174d27be68eafd787bb29fd" IssueInstant="2005-01-
   23T00:54:48.913Z" Issuer="www.webex.com" MajorVersion="1" MinorVersion="1">
      <Conditions NotBefore="2005-01-23T00:54:48.663Z" NotOnOrAfter="2007-01-
      31T08:00:00.000Z"></Conditions>
      <AuthenticationStatement AuthenticationInstant="2005-01-23T00:54:48.600Z"
      AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
         <Subject>
            <NameIdentifier NameQualifier="acme.webex.com">uid=johnd</NameIdentifier>
            <SubjectConfirmation>
               <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer
               </ConfirmationMethod>
            </SubjectConfirmation>
         </Subject>
         <SubjectLocality IPAddress="127.0.0.1"></SubjectLocality>
      </AuthenticationStatement>
   </Assertion>
</Response>
```

SAML 2.0 – Auto Account Creation

Here is an example of a signed SAML response containing a SAML 2.0 assertion. This response includes mandatory and optional user profile attributes used for automatic account creation. Site specific options are highlighted in bold.

```
<Response xmlns="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://acme.webex.com/dispatcher/SAML2AuthService?siteurl=acme"
ID="_06bff71973342ad24ba31790591bb010e963"
InResponseTo="s250ce91cf92b24a7694686158ddea33b6c1ce7fa9" IssueInstant="2008-09-
05T19:08:05Z" Version="2.0">
   <ns1:Issuer xmlns:ns1="urn:oasis:names:tc:SAML:2.0:assertion"
   Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">acme</ns1:Issuer>
   <Status>
   <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
   </Status>
   <ns2:Assertion xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="_e72cfdeffbf9288cfa75e2423a932abb35d5" IssueInstant="2008-09-05T19:08:05Z"
   Version="2.0">
   <ns2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
   acme</ns2:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      <ds:Reference URI="#_e72cfdeffbf9288cfa75e2423a932abb35d5"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:Transforms xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
      <ds:DigestValue
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">p5AbejgL5K4nGDp3HXHfp3VPhmE=</ds:D
      igestValue>
      </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      TtMcc6pnIxbDcLulI8/hJS9A74dR2w05dO676PK7KT48d8sGFoXXTgpWgy++7+AZTpQCjHPcv88c
      dAh4PtripoBlpZ++xErKQ/ee/rxsP2mOr7LrNE4QoqUbiOCd68kHz9Qjx0ApTIr6d4YXNfeHD62O
      iEBnixRE5c6hlnn263U=
      </ds:SignatureValue>
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Certificate xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      MIIErjCCA5agAwIBAgIQZMQJL9PYyWwQloty2TFcIzANBgkqhkiG9w0BAQUFADBrMQswCQYDVQQG
      EwJVUzEtMCsGA1UEChMkVHJ1c3RlZCBTZWN1cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MS0wKwYD
      VQQDEyRUcnVzdGVkIFNlY3VyZSBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwHhcNMDgwNTE2MDAwMDAw
      WhcNMTAwNTE2MjM1OTU5WjCB/TELMAkGA1UEBhMCVVMxFDASBgNVBAgTC0NPTk5FQ1RJQ1VUMRIw
      EAYDVQQHEwlGQUlSRklFTEQxITAfBasdawerweasdmVyYWwgRWxlY3RyaWMgQ29tcGFueTEwMC4G
      A1UECxMnR0UgQ29ycG9yYXRlIENJUyhjb3JwdDUwOCBwb2xpY3lzZXJ2ZXIpMS0wKwYDVQQLEyRQ
      cm92aWRlZCBieSBHZW5lcmFsIEVsZWN0cmljIENvbXBhbnkxFzAVBgNVBAsTDkVudGVycHJpc2Ug
      U1NMMScwJQYDVQQDEx5mZWRlcmF0aW9uLnN0YWdlLmdlY29tcGFueS5jb20wgZ8wDQYJKoZIhvcN
      AQEBBQADgY0AMIGJAoGBALxifpE26Rq2/uu6aykFJs3FqVg8/jh+F52JFRFdqmE6X2BHwIvTyrAe
      Xxa3qCBrFuUkmuopAMB9Fa0EF/JRSTvCyrPbls2ad3f34fvfAsCspdorx4d/Bc57UiqBXD/MSRWD
      S4lIYu9z2HXP1VTmu8zn4pkGCKatwvzmyX8kHjQbAgMBAAGjggE9MIIBOTAfBgNVHSMEGDAWgBQx
      lflM+yx445/iHjtrODIv/ZeZ5jAdBgNVHQ4EFgQUWO9diqLaKUpW5v0i6jJvLck3z9owDgYDVR0P
      AQH/BAQDAgWgMAwGA1UdEwEB/wQCMAAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBEG
      CWCGSAGG+EIBAQQEAwIGwDCBpgYDVR0fBIGeMIGbMEugSaBHhkVodHRwOi8vY3JsLmNzY3RydXN0
      ZWRzZWN1cmUuY29tL1RydXN0ZWRTZWN1cmVDZXJ0aWZpY2F0ZUF1dGhvcml0eS5jcmwwTKBKoEiG
      Rmh0dHA6Ly9jcmwyLmNzY3RydXN0ZWRzZWN1cmUuY29tL1RydXN0ZWRTZWN1cmVDZXJ0aWZpY2F0
```

```
     ZUF1dGhvcml0eS5jcmwwDQYJKoZIhvcNAQEFBQADggEBAHj2uj/f18c7PhYBenQJPgIFd179gR3/
     Ac+fB4PEnkJnpA5bQmHM3S1C/yCI8HOfihlucw4ckZsYjcdd8PmbrrtMdTqz5LaBL9i3OVDgEd9h
     mvIw0obHA6TM+hhSCdhpFOkaWaeYjd8ueDkO2/rqu96gvL0uDKMjbrKIvowtW3y3UFKUcyRs3SdU
     YPh1mwGJZ+4eq8WaLA+zH1UX37Mu4ErW4YA7vJapNn4K/ODax85zc/Wu4Dq15pPwW4HQzhXEHCoc
     i2n/cUVgq/QH1TF5spK/JCNxBsvzFmxn+qrkq9k+cQsIZGyAKDiQzaFXNE44c6mNOqDRw0PkXPZz
     lGOyPDE=
     </ds:X509Certificate>
     </ds:X509Data>
     </ds:KeyInfo>
   </ds:Signature>
   <ns2:Subject>
      <ns2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
      format:unspecified">johnd</ns2:NameID>
     <ns2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <ns2:SubjectConfirmationData
        InResponseTo="s250ce91cf92b24a7694686158ddea33b6c1ce7fa9" NotOnOrAfter="2008-
        09-05T19:09:35Z"
        Recipient="https://acme.webex.com/dispatcher/SAML2AuthServlet?siteurl=acme"/>
     </ns2:SubjectConfirmation>
   </ns2:Subject>
   <ns2:Conditions NotBefore="2008-09-05T19:07:35Z" NotOnOrAfter="2008-09-
05T19:09:35Z">
     <ns2:AudienceRestriction>
          <ns2:Audience>http://www.webex.com</ns2:Audience>
      </ns2:AudienceRestriction>
      <ns2:AudienceRestriction>
          <ns2:Audience>http://www.webex.com</ns2:Audience>
      </ns2:AudienceRestriction>
   </ns2:Conditions>
   <ns2:AuthnStatement AuthnInstant="2008-09-05T19:08:05Z"
SessionIndex="VOZ+dlWSTR33dFexpmtMlIFti7M=KDtVbw==" SessionNotOnOrAfter="2008-09-
05T19:09:35Z">
     <ns2:AuthnContext>
     <ns2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtect
     edTransport</ns2:AuthnContextClassRef>
           </ns2:AuthnContext>
   </ns2:AuthnStatement>
        <ns2:AttributeStatement>
           <ns2:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
           format:unspecified">
            <ns2:AttributeValue>johnd</ns2:AttributeValue>
            </ns2:Attribute>
            <ns2:Attribute Name="firstname"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <ns2:AttributeValue>John</ns2:AttributeValue>
            </ns2:Attribute>
            <ns2:Attribute Name="lastname"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <ns2:AttributeValue>Doe</ns2:AttributeValue>
            </ns2:Attribute>
            <ns2:Attribute Name="email"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <ns2:AttributeValue>johnd@acme.com</ns2:AttributeValue>
            </ns2:Attribute>
            <ns2:Attribute Name="optionalParams"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <ns2:AttributeValue>OPhoneCountry=1</ns2:AttributeValue>
            <ns2:AttributeValue>OPhoneArea=408</ns2:AttributeValue>
            <ns2:AttributeValue>OPhoneLocal=323.2345</ns2:AttributeValue>
            <ns2:AttributeValue>Address1=4610 Patrick Henry Dr.</ns2:AttributeValue>
            <ns2:AttributeValue>City=Santa Clara</ns2:AttributeValue>
            <ns2:AttributeValue>State=CA</ns2:AttributeValue>
           <ns2:AttributeValue>MT=<10,101,234,543></ns2:AttributeValue>
            <ns2:AttributeValue>TC1=Engineering</ns2:AttributeValue>
            <ns2:AttributeValue>TC2=8723</ns2:AttributeValue>
            </ns2:Attribute>
        </ns2:AttributeStatement>
    </ns2:Assertion>
</Response>
```

Appendix B - Resources

Cisco - WebEx Resources

WebEx Product Website

http://www.webex.com

WebEx Developer Connection SSO Portal

http://developer.webex.com/web/meetingservices/sso

CA SiteMinder Configuration Guide for WebEx FAS

SAML SSO Configuration Guide for Cisco - WebEx Meeting Center and CA SiteMinder.
http://developer.webex.com/c/document_library/get_file?p_l_id=10914&folderId=22041&name=DLFE-1803.zip

Ping Federate Server Configuration Guide for WebEx FAS

SAML SSO Configuration Guide for Cisco - WebEx Meeting Center and Ping Federate Server.
http://developer.webex.com/c/document_library/get_file?p_l_id=10914&folderId=22041&name=DLFE-1802.doc

SAML 2.0 Technical Overview

Technical Overview of the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC,
http://www.oasis-open.org/committees/download.php/11511/sstc-saml-tech-overview-2.0.pdf

WS-Federation 1.0 Specification

http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/ws-fed.pdf

X.509 Certificates

Public key certificate, Wikipedia, See http://en.wikipedia.org/wiki/Digital_certificate

X.509 Certificates and Certificate Revocation Lists, Sun Microsystems, May 2001.
http://java.sun.com/j2se/1.4.2/docs/guide/security/cert3.html