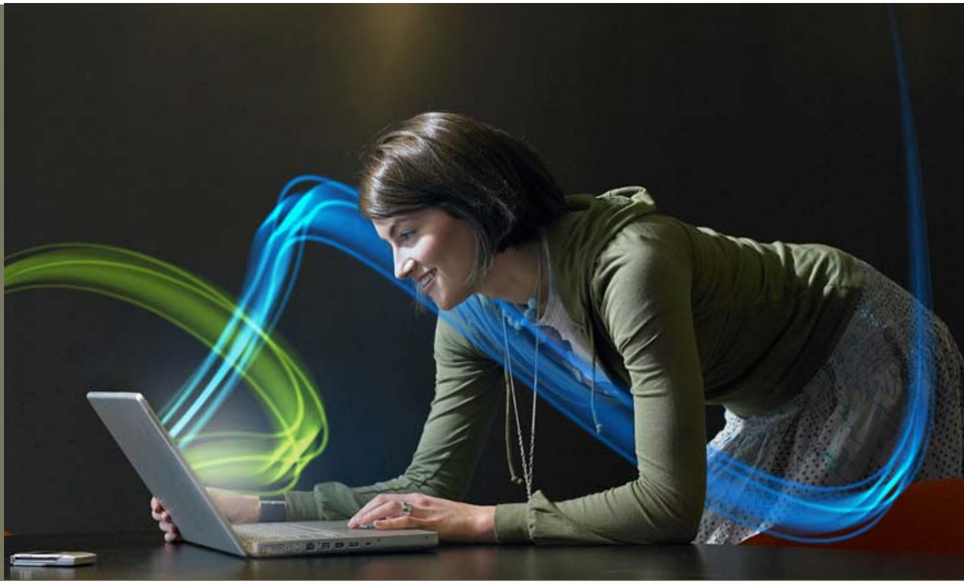


Federated SSO Authentication

Phillip Liu

Sr. Product Manager

February 2009

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Agenda

- Traditional SSO Offerings
- Federated SSO Authentication Service
- Productivity Tool Authentication
- Enterprise SSO T27 Architecture

Traditional SSO Offerings

Professional Services (PSO) package

- PSO develops custom pages hosted on customer servers.
- WebEx URL API used to login and create user accounts.
- WebEx Username usually set to customer intranet username.
- WebEx site login pages are usually deactivated

Active Directory Integration

- Can create, delete, update WebEx accounts from Microsoft Management Console and Sharepoint.
- AD Snap-In calls WebEx XML API for user management

Federated SSO Customer Requirements

SAML Compliant Identity & Access Management System

- CA SiteMinder
- Sun Access Mgr
- Ping Federate
- Oracle CoreID

X.509 Digital Certificate

- Granted by Certificate Authority
- Or Customer generated

What is SAML?

- Security Assertion Markup Language
- Standard for passing credentials between different Internet domains that have their own authentication systems.
- OASIS
  - – SAML 1.0, Approved Nov. 2002
  - – 1.1, Sep. 2003
  - – 2.0, Mar. 2005

WebEx SAML Assertion format

```
<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=“customer.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>
```

Federated SSO Authentication Use Cases

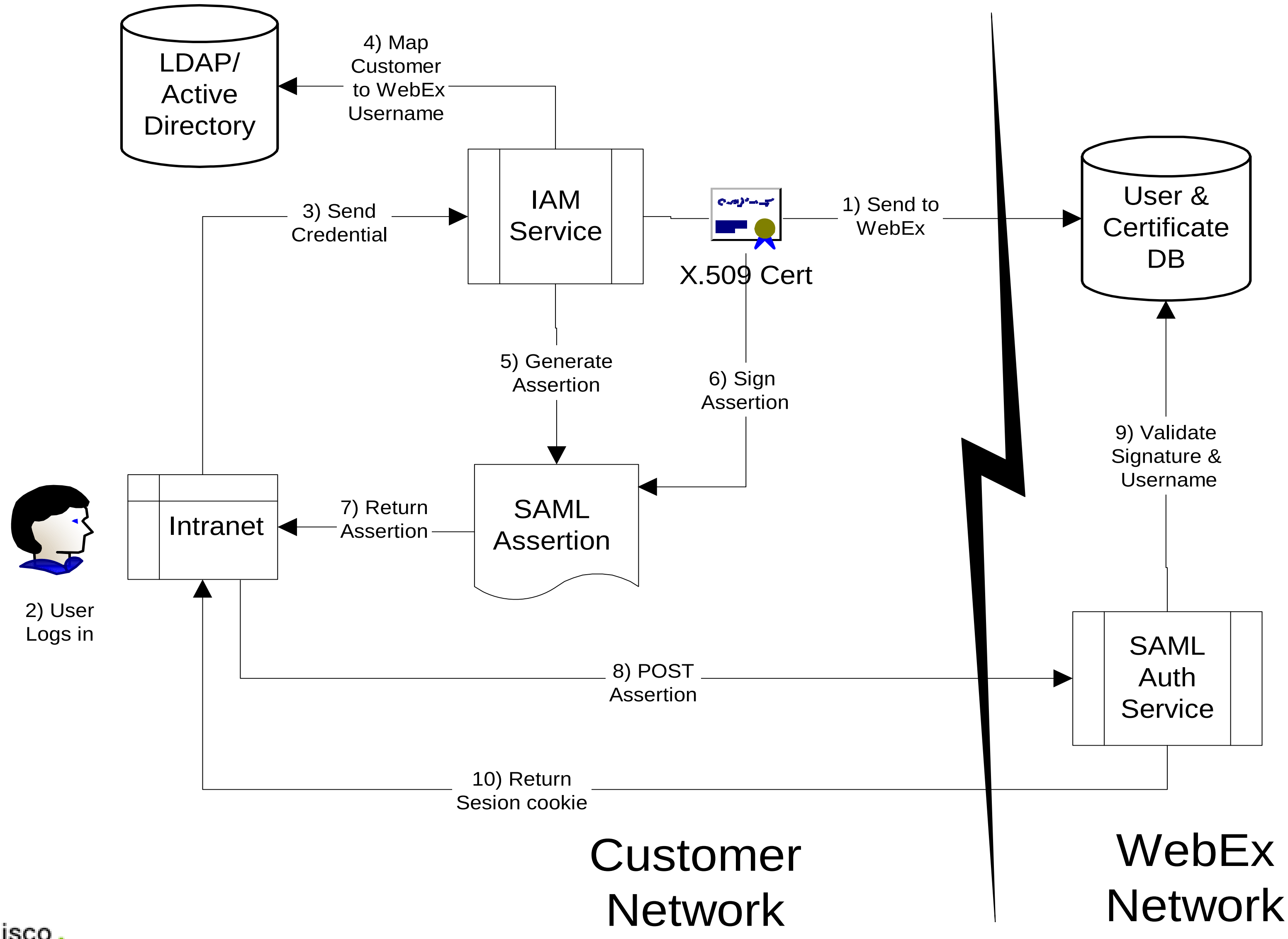
Browser Authentication

- Customer sends WebEx an X.509 certificate which is associated w/their site.
- User authenticates to their corporate intranet and wants to schedule a WebEx meeting.
- Identity Management System (IDMS) generates signed SAML assertion containing WebEx username and posts it to WebEx.
- PSO option to automatically create new WebEx account if necessary.
- WebEx SAML Auth. Service verifies SAML assertion and creates browser session cookie.
- User is now authenticated to WebEx meeting site and can schedule meetings.

API Authentication

- Integration sends a signed SAML assertion in an XML API request.
- XML API calls SAML Auth Service to authenticate user and returns a WebEx session ticket.
- If WebEx user account doesn’t exist, XML API CreateUser can be used create account.
- WebEx session ticket is used in subsequent XML API requests that require user authentication.

Federated SSO Authentication Process flow



Cisco webex

WebEx Productivity Tool Authentication

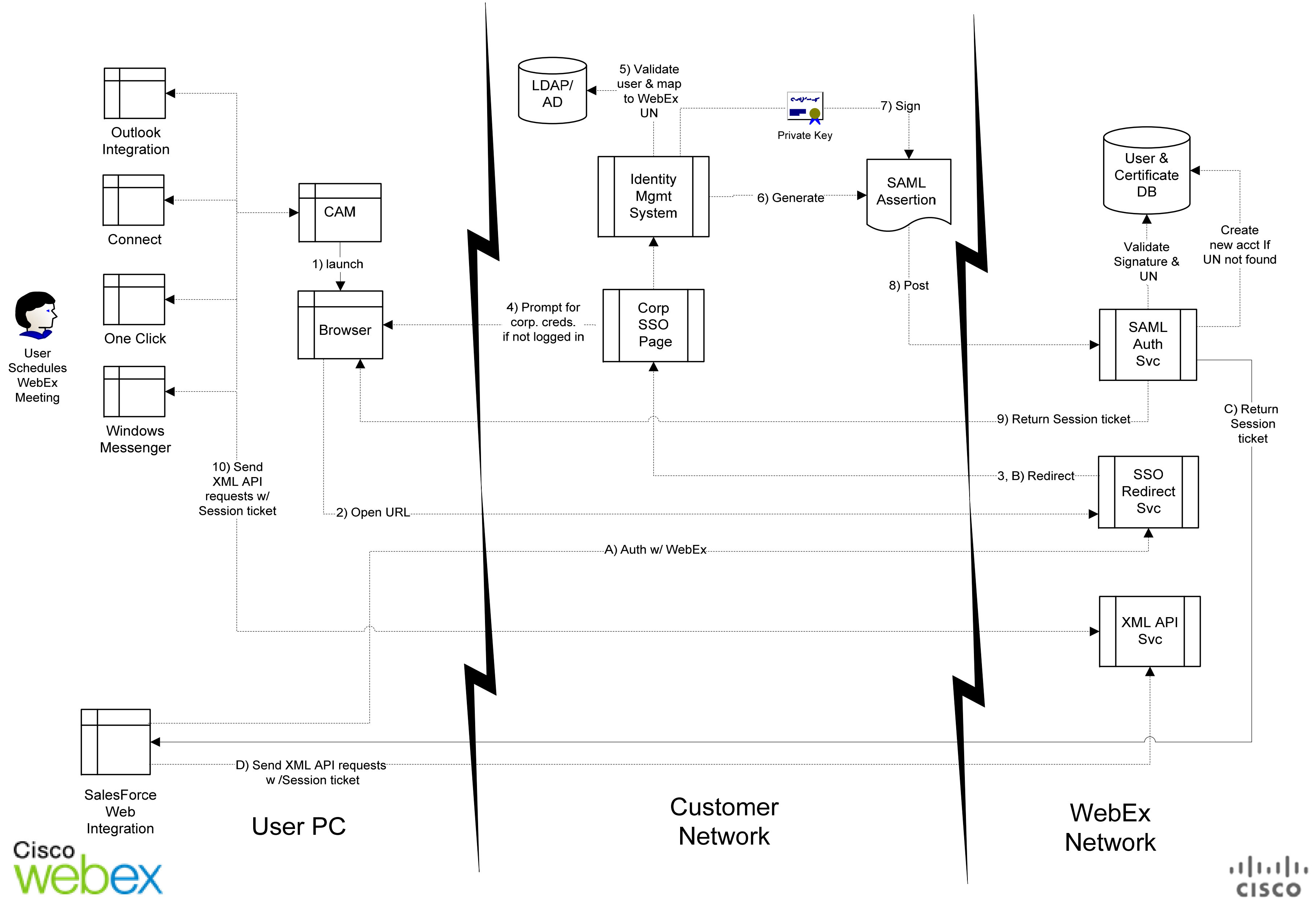
T26 UN / PW Authentication

- WebEx productivity tools (Outlook/Noted Integration, One Click, etc) share a common Client Authentication Module (CAM).
- CAM provides a single place to enter WebEx site, username and password.

T27 SSO Authentication

- CAM opens a browser window to a customer-hosted authentication web page.
- Customer’s IDMS generates a SAML assertion and posts to WebEx.
- WebEx authenticates and optionally provisions the user and returns a session ticket
- Productivity tools then collectively utilize the session ticket for subsequent XML API requests.
- SAML 1.1, 2.0, WS-Fed 1.0 (MSFT ADFS) Assertion formats supported

T27 Federated Authentication Architecture



Cisco webex