MIT Touchstone

DSPS team meeting

May 6, 2008

Who?

- Bob Basch
- Vijay Konda
- Arnis Kletnieks
- Laura Watts
- Joanna Proulx
- Brian Knoll
- Paul Hill

Why?

- Support situations where x.509 certificates are not practical
- Federated web authentication
- Web SSO
- Provide a clear integration strategy to MIT web developers
- Ability to adopt new technologies

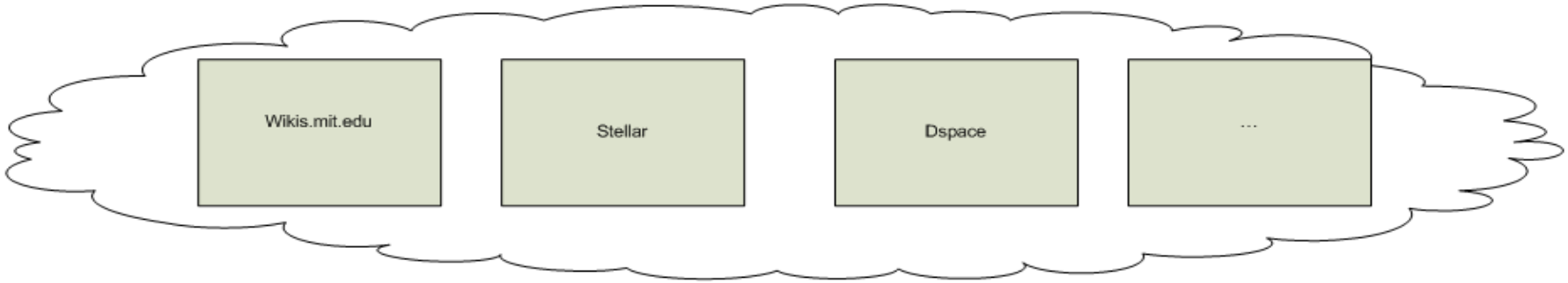
How?

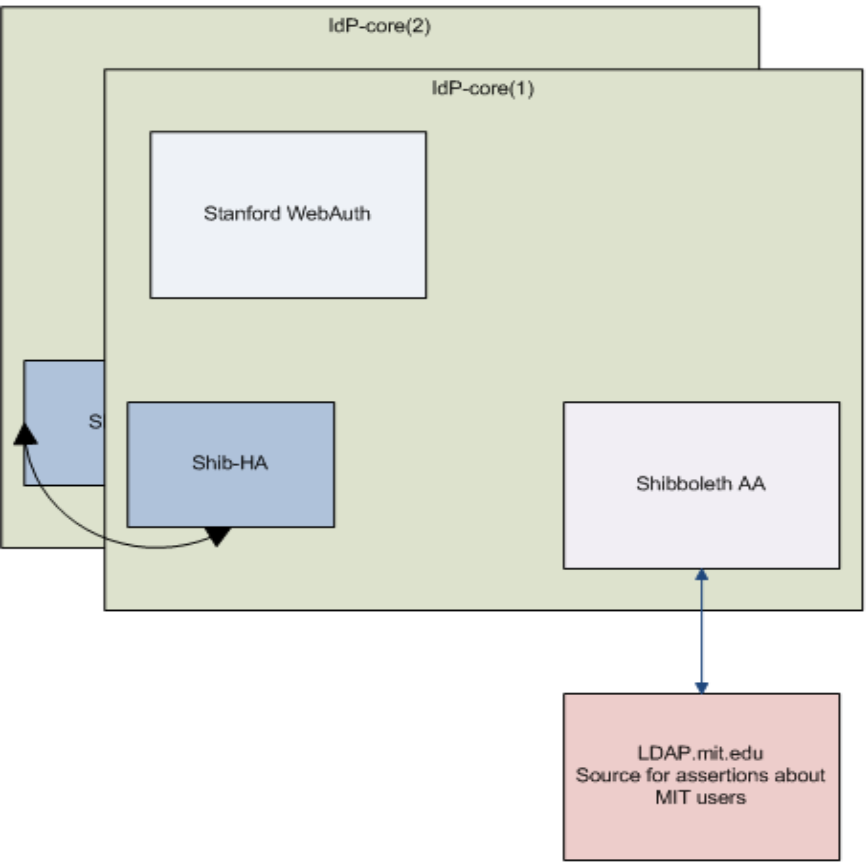
- MIT – a federation of (at least) two
  - People with a Kerberos account and the ability to obtain a certificate
  - External collaborators – know by an email address

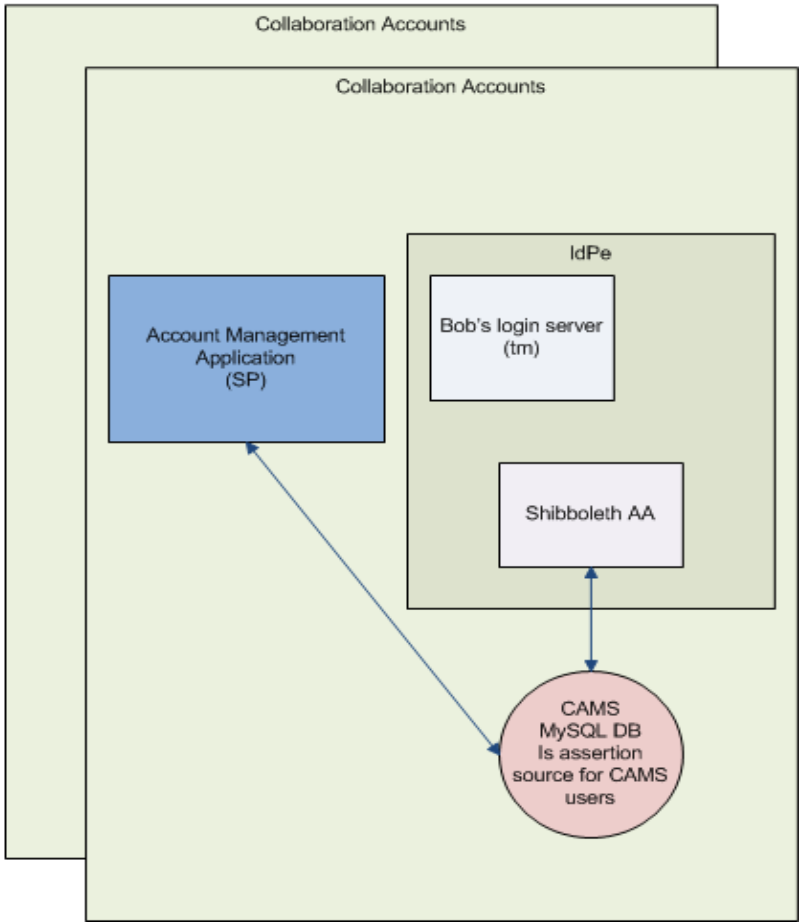
What?

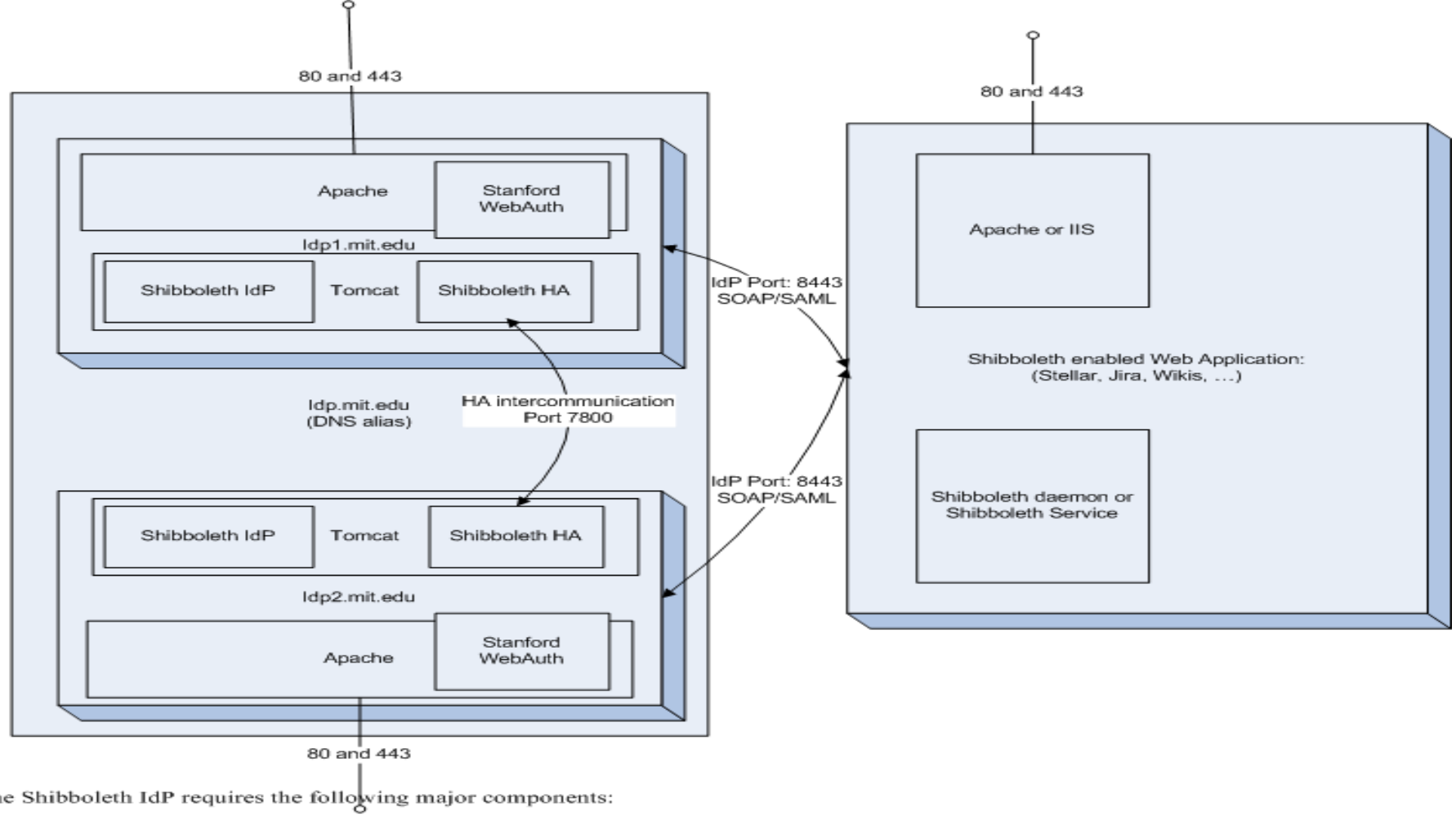
- Shibboleth
- IdP
- Shib-HA
- LDAP
- SP
- InCommon
- WAYF

- Stanford WebAuth
  - Username and password
  - X.509
  - http-spnego
- CAMS
  - Account management application
  - Authentication server
    - Email address and password
    - http-spnego (x-realm)
    - OpenID


Wikis.mit.edu
Stellar
Dspace
...


IdP-core(2)
IdP-core(1)
Stanford WebAuth
Shib-HA
Shibboleth AA
LDAP.mit.edu
Source for assertions about
MIT users


Collaboration Accounts
Collaboration Accounts
IdPe
Account Management
Application
(SP)
Bob's login server
(tm)
Shibboleth AA
CAMS
MySQL DB
Is assertion
source for CAMS
users



The Shibboleth IdP requires the following major components:

Apache web server (2.0+) , Tomcat, mod_jk, Java, HA Shib extension (to maintain consistent state across multiple IdPs), log4j (recommended for improved logging)

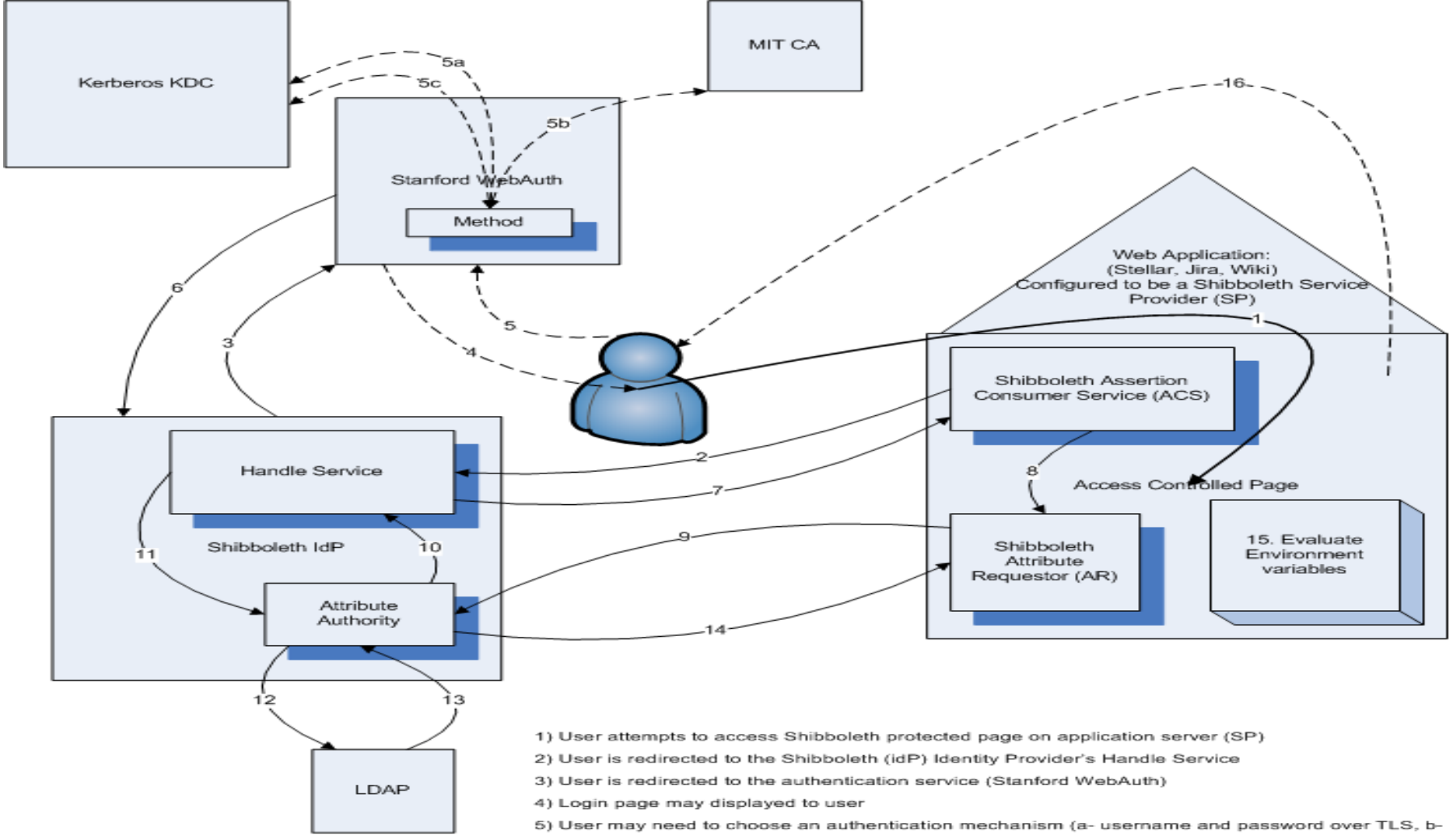
WebAuth requires the following major components:

> Apache web server (2.0+, preferably 2.0.51 or higher), OpenSSL, Kerberos v5 (1.4.1 or higher for our mod_auth_kerb patch), cURL, Perl, including the following modules: HTML::Template, FCGI, Crypt::SSLeay, LWP and HTTP (libwww-perl package), XML::Parser, mod_auth_kerb (for authentication via HTTP/SPNEGO), mod_fastcgi (recommended for performance)

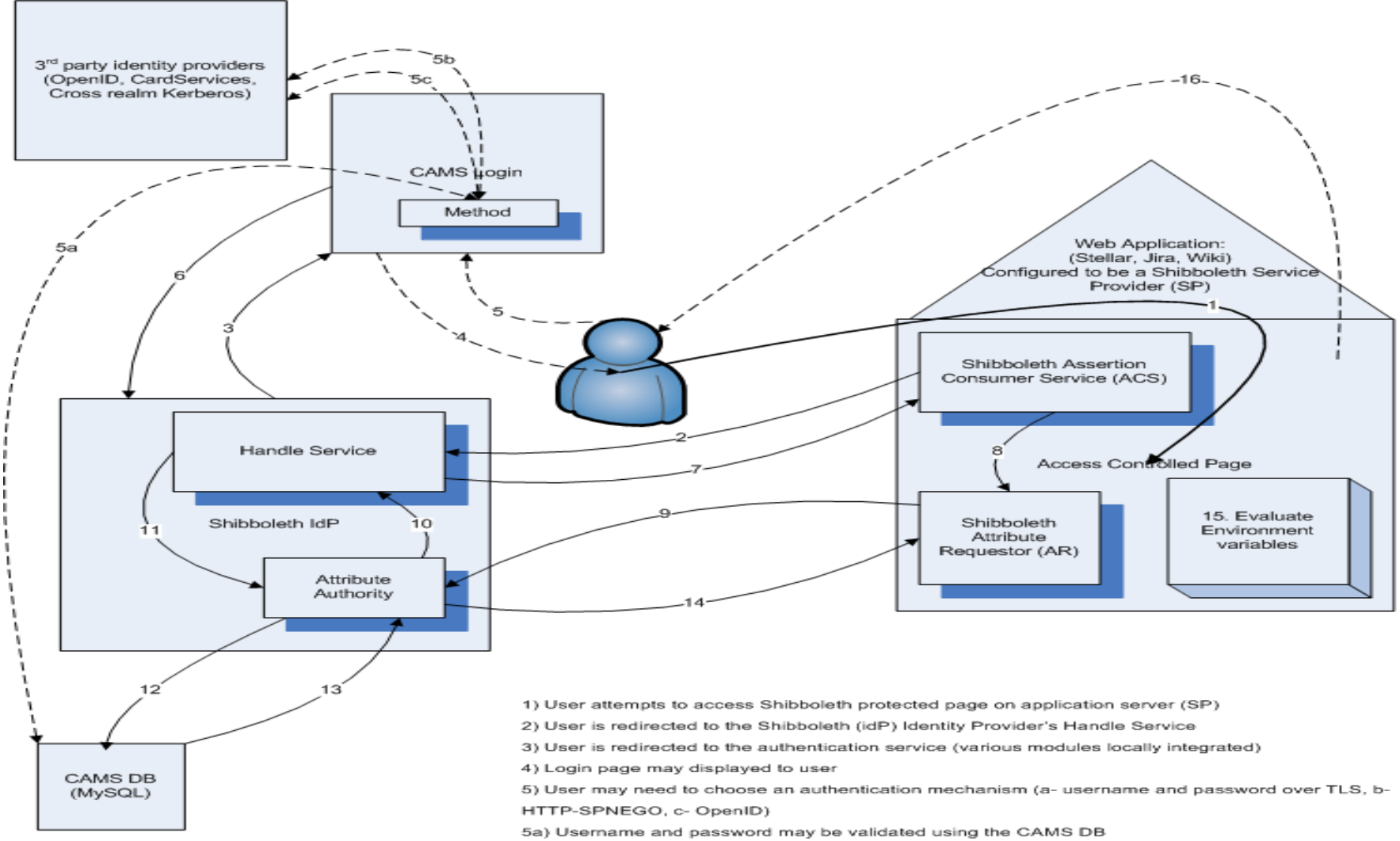
In the recommended configuration, the Apache web server will listen on the following TCP ports:

> 80 (HTTP), 443 (virtual host for HTTPS), 8443 (virtual host for SP's back-channel SOAP calls for attributes), 9443 (virtual host to work around re-negotiation issues when authenticating via user certificates), 7800 (used by the Shibboleth HA package to keep state in sync between the clustered servers; the firewall can be configured so that only other members of the cluster can connect to it)

> See: <https://wikis.mit.edu/confluence/display/ZEST/IdP+run+book+%28including+WebAuth%27s+WebKDC+login+server%29+for+NIST>



1) User attempts to access Shibboleth protected page on application server (SP)
2) User is redirected to the Shibboleth (idP) Identity Provider's Handle Service
3) User is redirected to the authentication service (Stanford WebAuth)
4) Login page may displayed to user
5) User may need to choose an authentication mechanism (a- username and password over TLS, b- HTTP-SPNEGO, c- X.509 certificate)
5a) Username and password may be validated by Kerberos KDC
5b) Existing Kerberos tickets from KDC may be used
5c) MIT X.509 certificate may be validated via trust path
6) State of authentication is communicated to IdP
7) IdP's Handle service returns opaque handle to SP
8) SP ACS provide handle to SP's AR
9) SP makes attribute request about user to the IdP, identifying the user by the opaque handle
10) IdP AA passes the handle to IdP HS in order to de-marshall the opaque handle
11) IdP HS tells the AA the local username
12) IdP AA queries MIT LDAP server about the user
13) LDAP server responds with requested info
14) IdP AA forms SAML assertions about the user and passes this back to the SP
15) SAML assertion is turned into Apache or IIS environment variables which the application can evaluate
16) Application can deliver the requested page to the user



1) User attempts to access Shibboleth protected page on application server (SP)
2) User is redirected to the Shibboleth (idP) Identity Provider's Handle Service
3) User is redirected to the authentication service (various modules locally integrated)
4) Login page may displayed to user
5) User may need to choose an authentication mechanism (a- username and password over TLS, b- HTTP-SPNEGO, c- OpenID)
5a) Username and password may be validated using the CAMS DB
5b) Existing Kerberos tickets from KDC may be used
5c) OpenID may optionally be used by some users
6) State of authentication is communicated to IdP
7) IdP's Handle service returns opaque handle to SP
8) SP ACS provide handle to SP's AR
9) SP makes attribute request about user to the IdP, identifying the user by the opaque handle
10) IdP AA passes the handle to IdP HS in order to de-marshall the opaque handle
11) IdP HS tells the AA the local username
12) IdP AA queries MIT CAMS DB about the user
13) CAMS DB responds with requested info
14) IdP AA forms SAML assertions about the user and passes this back to the SP
15) SAML assertion is turned into Apache or IIS environment variables which the application can evaluate
16) Application can deliver the requested page to the user

It’s XML so it must good, right? (A SAML Assertion)

```
<Response xmlns="urn:oasis:names:tc:SAML:1.0:protocol" InResponseTo="_0a189e60e90898256cfb267f4e9166e5" IssueInstant="2008-05-06T18:10:02.569Z" MajorVersion="1"
        MinorVersion="1" ResponseID="_aacbbada3fe6ff28a28f7180c7e511ef" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <Status>
  <StatusCode Value="samlp:Success"/>
 </Status>
 <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="_001a35010c27af0867ff2c9fda6b6397" IssueInstant="2008-05-06T18:10:02.569Z"
        Issuer="https://idp.foonalagoona.mit.edu/shibboleth" MajorVersion="1" MinorVersion="1">
  <Conditions NotBefore="2008-05-06T18:10:02.569Z" NotOnOrAfter="2008-05-06T18:40:02.569Z">
   <AudienceRestrictionCondition>
    <Audience>
     https://posteverything.mit.edu/shibboleth
    </Audience>
    <Audience>
     https://isda-shib-test.mit.edu
    </Audience>
   </AudienceRestrictionCondition>
  </Conditions>
  <AttributeStatement>
   <Subject>
    <NameIdentifier Format="urn:mace:shibboleth:1.0:nameIdentifier" NameQualifier="https://idp.foonalagoona.mit.edu/shibboleth">
     _9c6b3a718cc609ccb55286bc18b17ad7
    </NameIdentifier>
   </Subject>
   <Attribute AttributeName="urn:mace:dir:attribute-def:eduPersonNickname" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <AttributeValue>
     Paul B Hill
    </AttributeValue>
   </Attribute>
   <Attribute AttributeName="urn:mace:dir:attribute-def:eduPersonScopedAffiliation" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <AttributeValue Scope="mit.edu">
     staff
    </AttributeValue>
   </Attribute>
   <Attribute AttributeName="urn:mace:dir:attribute-def:eduPersonAffiliation" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <AttributeValue>
     staff
    </AttributeValue>
   </Attribute>
```

SAML Assertion (2)

```
<Attribute AttributeName="urn:mace:dir:attribute-def:ou" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
     <AttributeValue>
       Information Services &amp;amp; Technology
     </AttributeValue>
    </Attribute>
    <Attribute AttributeName="urn:mace:dir:attribute-def:givenName" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
     <AttributeValue>
       Paul B
     </AttributeValue>
    </Attribute>
    <Attribute AttributeName="urn:mace:dir:attribute-def:mail" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
     <AttributeValue>
       pbh@mit.edu
     </AttributeValue>
    </Attribute>
    <Attribute AttributeName="urn:mace:dir:attribute-def:eduPersonPrimaryAffiliation" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
     <AttributeValue>
       staff
     </AttributeValue>
    </Attribute>
    <Attribute AttributeName="urn:mace:dir:attribute-def:telephoneNumber" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
     <AttributeValue>
       617-253-0124
     </AttributeValue>
    </Attribute>
    <Attribute AttributeName="urn:mace:dir:attribute-def:cn" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
     <AttributeValue>
       Paul B Hill
     </AttributeValue>
    </Attribute>
    <Attribute AttributeName="urn:mace:dir:attribute-def:sn" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
     <AttributeValue>
       Hill
     </AttributeValue>
    </Attribute>
    <Attribute AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName" AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
     <AttributeValue Scope="mit.edu">
       pbh
     </AttributeValue>
    </Attribute>
  </AttributeStatement>
 </Assertion>
</Response>
```

Some of the environment variables

HTTP_REMOTE_USER HTTP_SHIB_APPLICATION_ID default
HTTP_SHIB_AUTHENTICATION_METHOD urn:oasis:names:tc:SAML:1.0:am:unspecified
HTTP_SHIB_EP_AFFILIATION staff@mit.edu
HTTP_SHIB_EP_ENTITLEMENT
HTTP_SHIB_EP_NICKNAME Paul B Hill
HTTP_SHIB_EP_PRIMARYAFFILIATION staff
HTTP_SHIB_EP_PRIMARYORGUNITDN
HTTP_SHIB_EP_UNSCOPEDAFFILIATION staff
HTTP_SHIB_IDENTITY_PROVIDER https://idp.foonalagoona.mit.edu/shibboleth
HTTP_SHIB_INETORGPERSON_GIVENNAME Paul B
HTTP_SHIB_INETORGPERSON_MAIL pbh@mit.edu
HTTP_SHIB_ORGPERSON_ORGUNIT Information Services & Technology
HTTP_SHIB_ORIGIN_SITE https://idp.foonalagoona.mit.edu/shibboleth
HTTP_SHIB_PERSON_COMMONNAME Paul B Hill
HTTP_SHIB_PERSON_DESCRIPTION
HTTP_SHIB_PERSON_SURNAME Hill
HTTP_SHIB_PERSON_TELEPHONENUMBER 617-253-0124
HTTP_SHIB_TARGETEDID REMOTE_USER pbh@mit.edu

When?

- Stellar, Jira, and Wikis started last fall
- CAMS portion – July 2008 (service readiness)
- Developer outreach September 2008
- Libraries: Dspace, Document Delivery, GeoWeb, EZ Proxy – working with them.
- SDLS – dependent on
- NIST Citrix farm – in development

Future?

- Shibboleth and Liberty convergence
- Shibboleth and ADFS interoperability