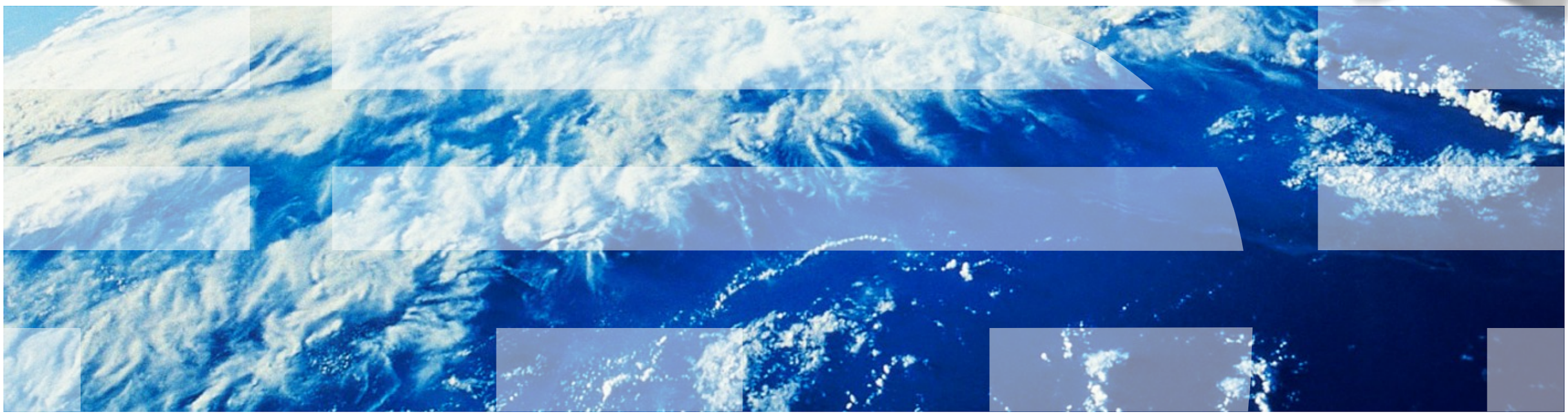
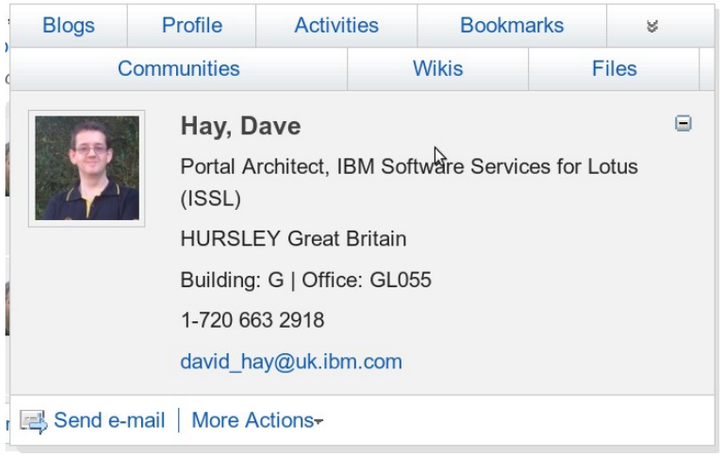
WebSphere User Group
March 2012
IBM South Bank, London

about.me/david_hay

Desktop Single Sign-On in an Active Directory World
21 March 2012



Introduction



With IBM since 1992

Experienced with hardware, software and services

- Started with AS/400 and iSeries
- Moved onto Network Station
- Working with WebSphere and Lotus software since 2000
- Linux and Mac advocate
- Collaboration evangelist
- Serial blogger

Infrastructure Architect

- Focused on IBM middleware and integration with client hardware, software and services

With ISSC since 2009

- Wide range of projects, including Collaboration Portal, Secure Portal, Process Portal, Google Search Appliance integration and, most recently, WAS integration with Active Directory .....

Session objectives

This presentation tells the story of a particular ISSC project – however, the story is relevant to many other clients, projects and requirements

- **Understand how to integrate WebSphere Application Server, and related products, with Active Directory**
- **Understand how to implement desktop single sign-on with WebSphere Portal, IBM Web Content Manager, IBM Connections etc.**
- **Share the lessons that we learned**
- **Consider the next steps**

What is this Active Directory thing ?

- **Central to Microsoft Windows network administration and security**
- **Responsible for authenticating and authorising users and computers within Windows networks**
  - Assigns and enforces security policies
  - Installing and updating software
  - Authenticating users for Windows desktop login
  - Locating network resources (e.g. printers)
- **Implements LDAP v2 and v3**
- **Can act as DNS in Windows networks**
- **Can implement a complex domain architecture**
  - Domains and sub-domains
  - Concept of trust between domains to allow resources in one domain to access those in another

- **IT'S MORE THAN JUST ANOTHER LDAP SERVER .....**

Client Requirements / desired outcomes

- **Many of our clients use Active Directory as their main user authentication mechanism**

- **Requirement is generally to provide "seamless login" to WebSphere Portal and IBM Connections for those users who are authenticated to a Windows desktop**
  - User logs in to Windows desktop using AD credentials
  - User accesses IBM software without providing further credentials (explicitly)
  - Portal, Connections etc. recognizes the user and provides access to her personal resources

  - But... we also need to consider mobile device authentication, and these aren't Windows desktops ...

Kerberos and SPNEGO

- **Kerberos is a 3-party security system developed at MIT – The requestor of a service, the service itself, and a trusted 3rd party**
  - Named from Greek mythology, Cerberus/Cerberos/Kerberos was the 3 headed dog guarding the gates to Hades.
  - Cryptographic Tokens are exchanged, not userids/passwords (passwords only flow when users change them)
  - MIT makes Kerberos freely available, and Microsoft has an implementation in Windows

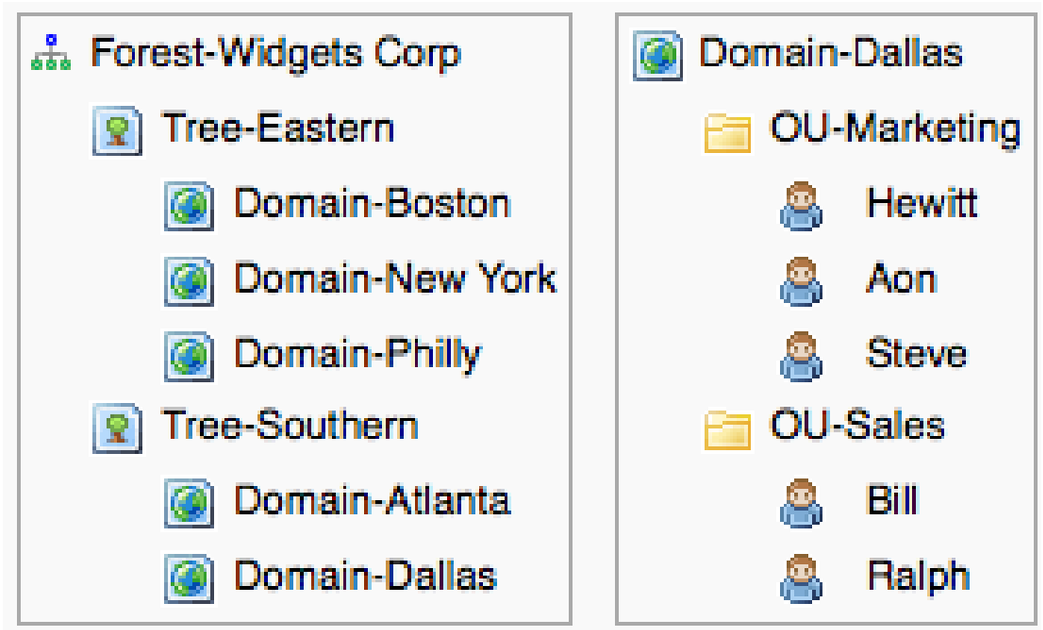
- **Generic Security Services API – a C API that abstracts security services. Kerberos is reference implementation.**
  - Java SDK implements Java GSS API.
  - WebSphere Application Server (at sufficient service level) includes JGSS SPNEGO Provider for parsing SPNEGO tokens

- **SPNEGO: Simple and Protected GSS-API Negotiation Mechanism**
  - Defined IETF RFC 2478
  - SPNEGO over HTTP was defined by Microsoft for exchanging credentials to a webserver via HTTP (the focus of the TAI)
  - SPNEGO token wraps a Kerberos Token

- **WebSphere Application Server (WAS) has only recently supported Kerberos and SPNEGO right out-of-the box**
  - In the past, support was via a custom IBM Software Services for WebSphere asset
  - WAS v7 introduced native support for both
  - We use SPNEGO, not Kerberos here, will explain the difference later ....

AD bring with it lots of terminology to get used to

- **Forest**
  - Top-level structure in Active Directory
  - Collection of Trees that share a common global catalogue, schema, structure and configuration
  - Represents the security boundary in which users, computers, groups and other resources are accessible
- **Tree**
  - Collection of domains in a contiguous namespace
- **Domain**
  - Grouping of objects in a single structure and database, identified by DNS name / namespace
  - Sometimes modified by an adjective to indicate the kind of resources stored in the entity (e.g. Resource Forest, User Domain)
- **Trust**
  - AD forests and domains can trust each other to allow users to access resources without further authentication



Kerberos terms

- **Kerberos resources are represented by "principals"**

- **User principals take the form principal@REALM**
  - In AD, the user MYDOMAIN\david will have a user principal of david@MYDOMAIN
    - This is the **User Principal Name** aka **UPN**
  - WAS will extract this from the token to locate the user in the WebSphere registry

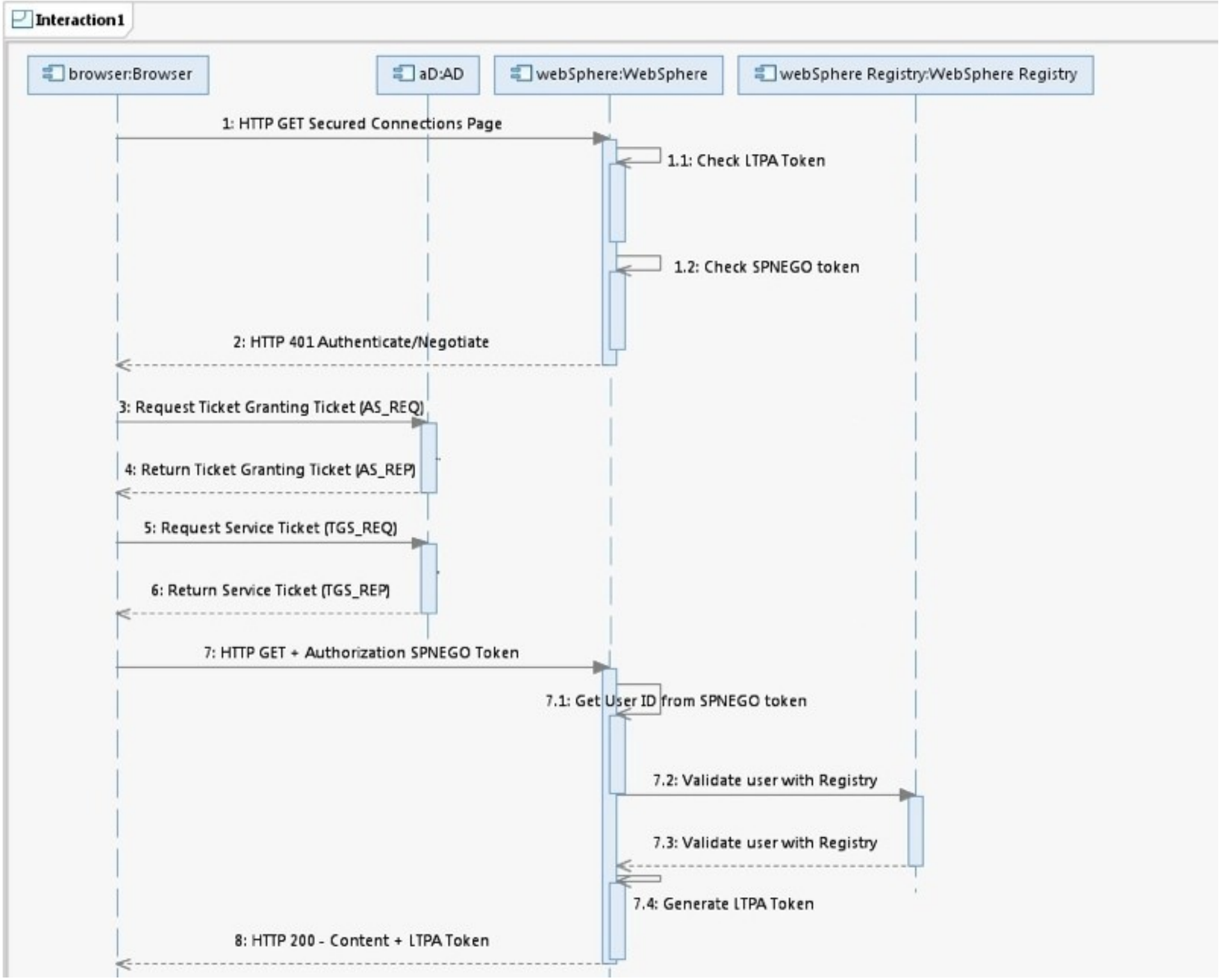
- **Service principals take the form service/server.fqdn@REALM**
  - For example a Connections service in the domain foo.net might have the service principal connections/connections.foo.net@REALM
    - This **is the Service Principal Name** aka **SPN**
  - Note that AD uses the domain to identify where to find the SPN for your service
  - e.g. when a user accesses connections.foo.net, AD will look for the foo.net domain to retrieve the SPN (and may have to navigate AD trusts to do so)
  - This is used to generate the cryptographic token used to pass the user's identity

- **Servers in a Kerberos authentication realm must have a FQDN that is both forward and reverse resolvable**
  - AD depends heavily on DNS - check that each server to be used has an FQDN assigned

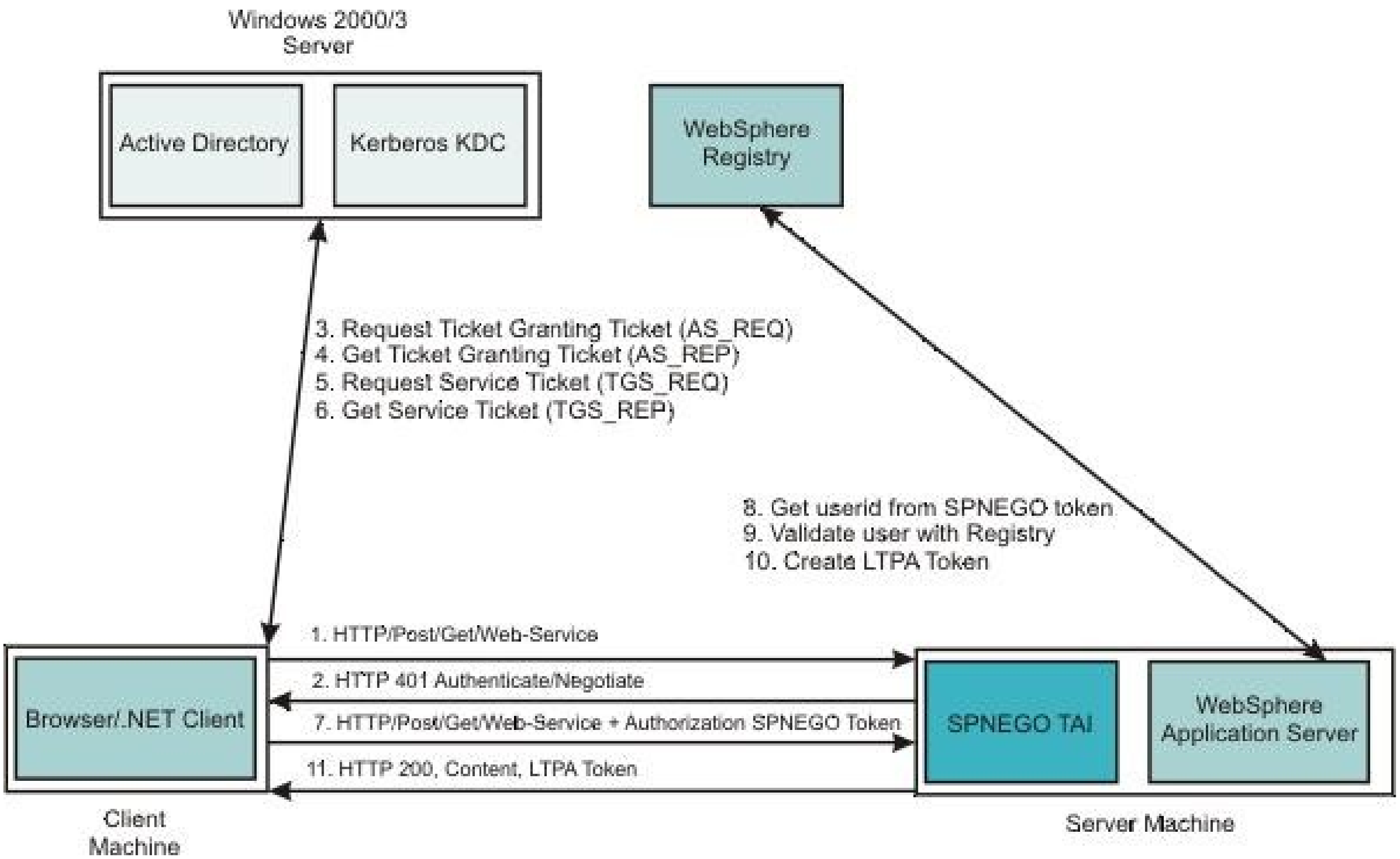
Desktop SSO requires Integrated Windows Authentication

Don't assume that the user can edit these settings – they may/should be controlled by a central Group Policy Object in Active Directory ....

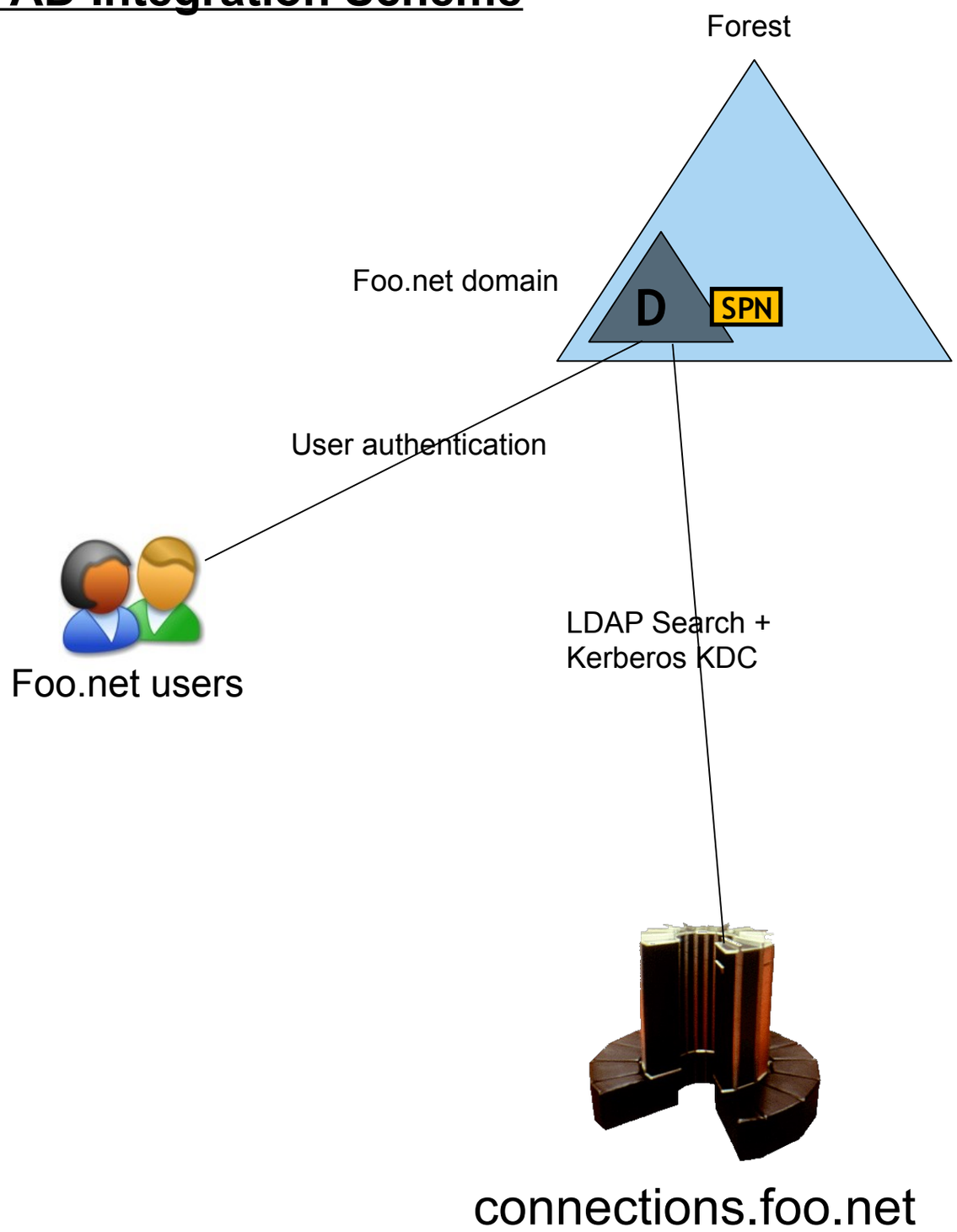
Interaction Diagram



Another way of looking at it ....

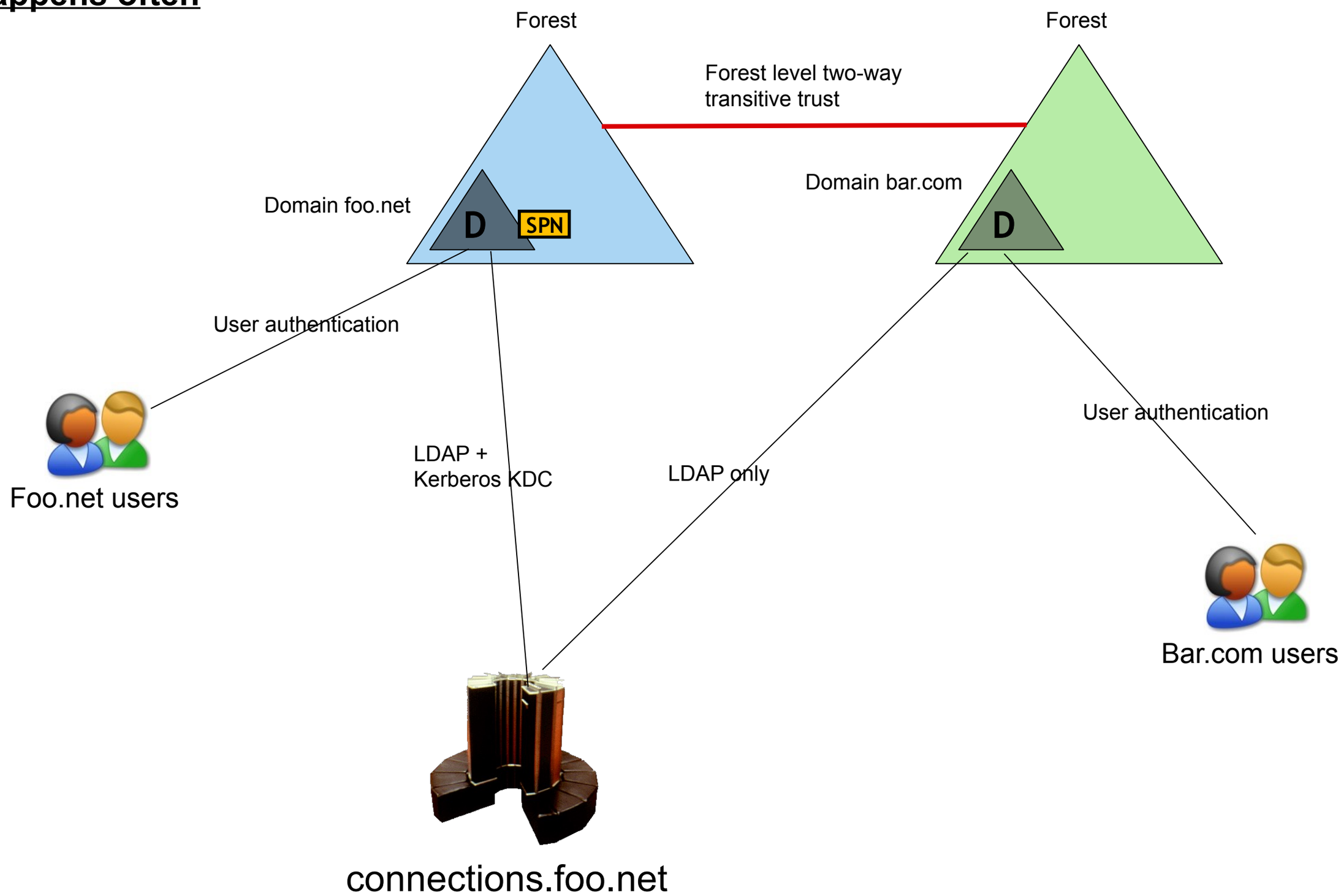


Simple AD Integration Scheme

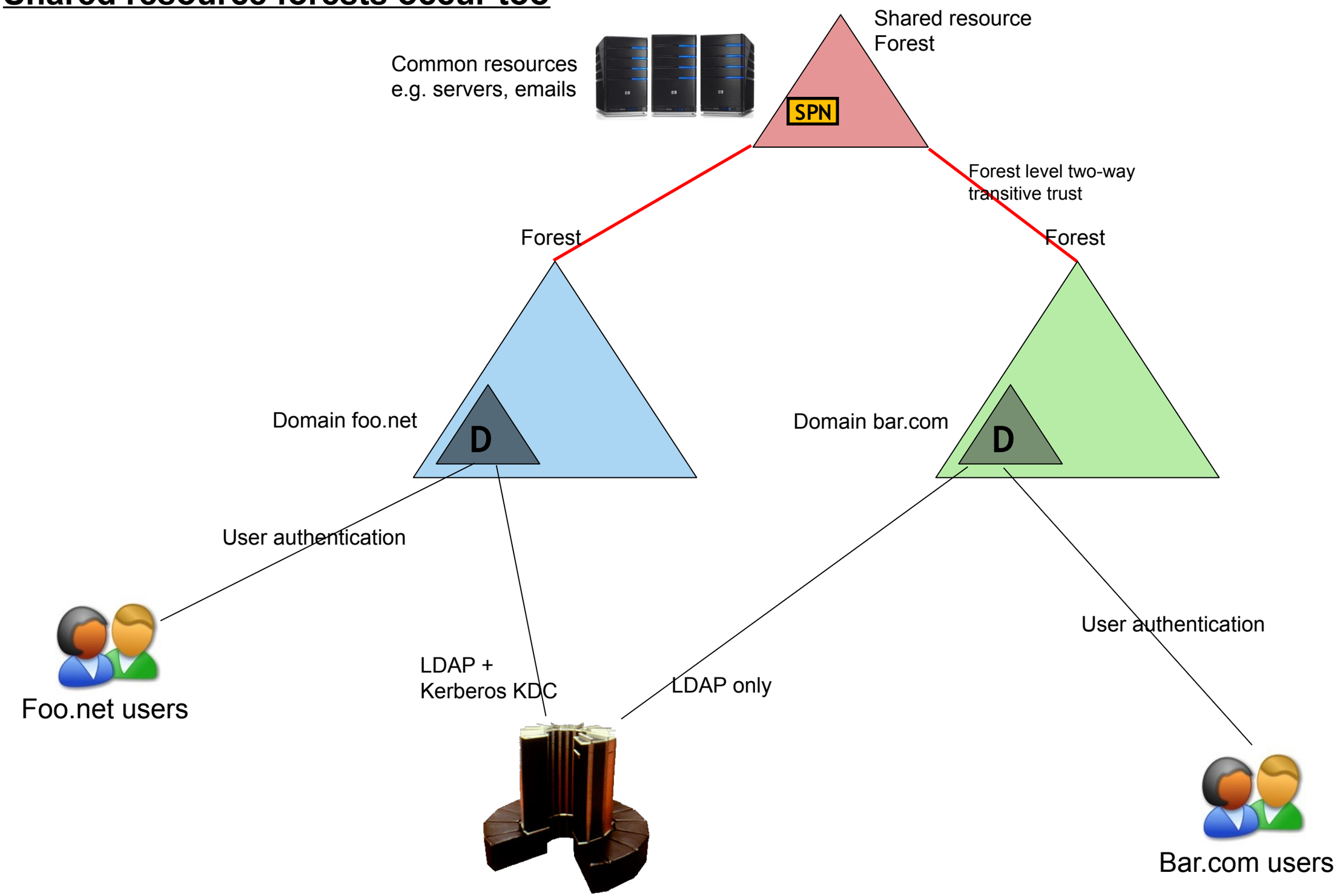


But: Any manual Login will require LDAP Authentication

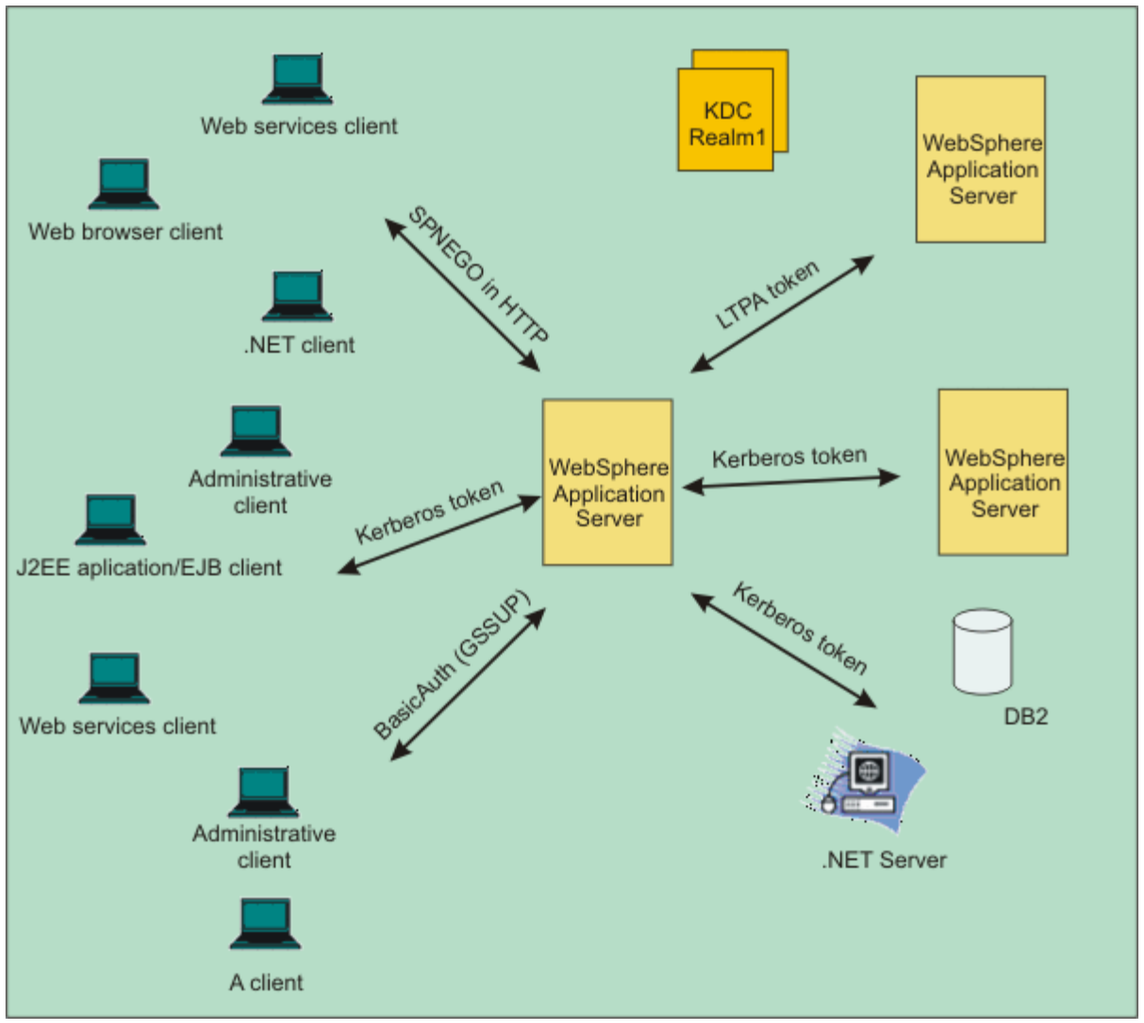
This happens often



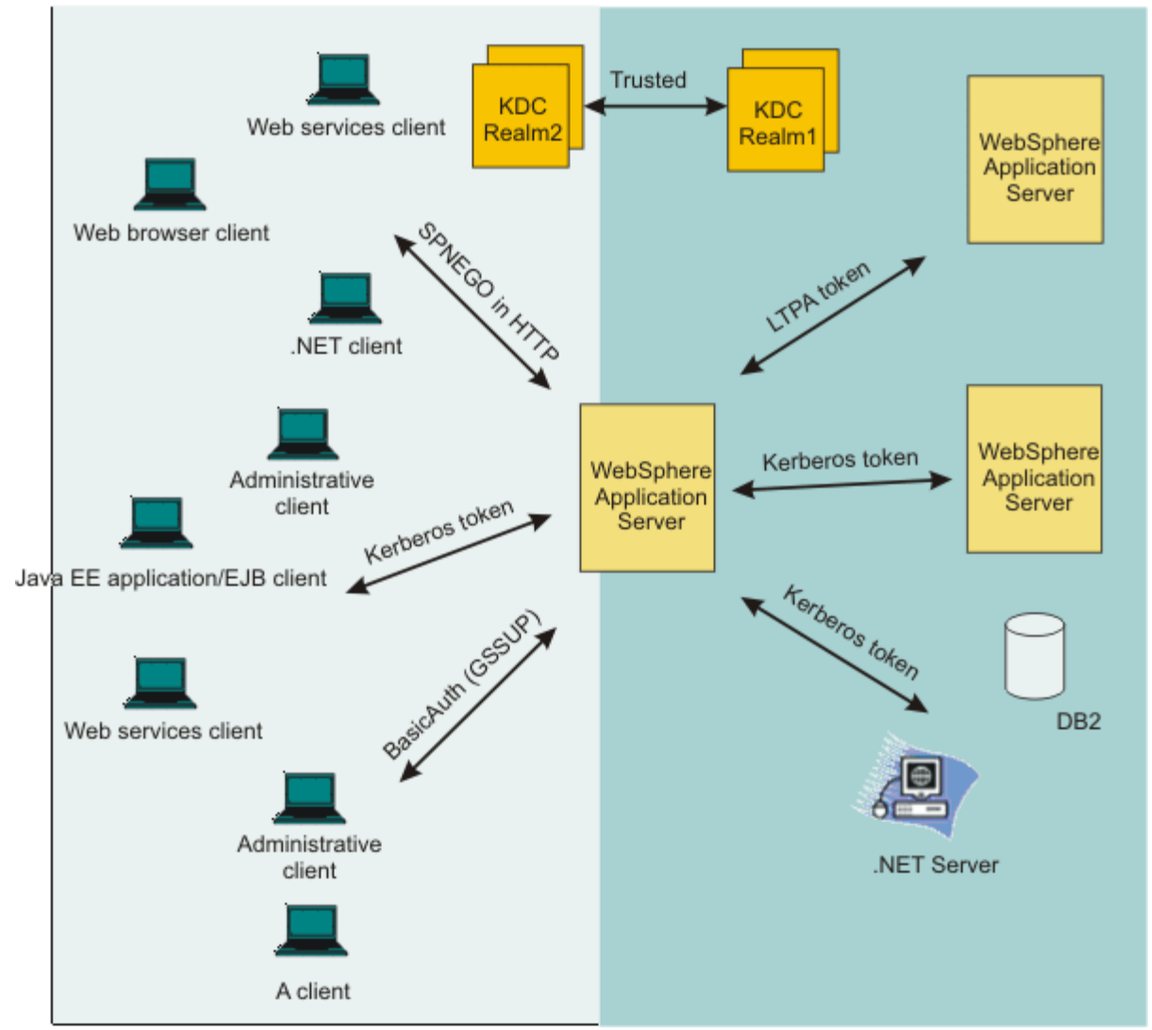
Shared resource forests occur too



Kerberos authentication in a single Kerberos realm environment



Kerberos authentication in a cross or trusted Kerberos realm environment



Note that we're using SPNEGO / Kerberos from client to server, but using Lightweight Third Party Authentication (LTPA) from server to server. This is more efficient, as there's less need to call back to the Active Directory KDB

Active Directory and Windows Desktop Pre-requisites

- **The right Microsoft software versions**
  - Active Directory 2003 or 2008 (AD2000 not supported for SSO)
  - Windows XP SP3 or above
  - Internet Explorer 6.0 or above (Firefox works ...)
- **A web server - not as important as it used to be :-)**
  - No longer have a dependancy on Internet Information Server (IIS)
  - We used IBM HTTP Server - however, not mandatory
- **Typical AD connectivity details (as used for Federated Repository)**
  - Hostname (load balanced is preferable) and ports
  - SSL certificate (if relevant)
  - Bind credentials
  - Base Distinguished Name
  - Search filters
- **Kerberos Keytab**
  - Contains Kerberos principal name and encrypted key to allow authentication
  - Generated / updated using the **ktpass** command
- **Service Principal Name (SPN)**
  - Maps a user account to a service - typically one per hostname (fully-qualified)
  - Generated / updated using the **setspn** command

Notes on a keytab

- **Option exists to generate multiple keytabs, one per domain**
  - This would be required in an environment without trust
  - If two-way forest-level transitive trust is NOT in place between domains, multiple keytabs MAY be the only option
  - Keytabs are really just text files
  - They can be merged
  - WAS supports the use of a merged keytab
  - HOWEVER, optimum route is to use two-way forest-level transitive trusts

WebSphere Application Server pre-requisites

- **WebSphere Application Server**
  - We used 7.0.0.11 (Connections) and 7.0.0.13 (Portal)
    - We're now upgrading to 7.0.0.17 and 7.0.0.19 respectively
  - Also needed additional iFixes, recommended for Connections 3.0.1 : -
    - PM19604 SPNEGO web authentication always interacts with theSPNEGO interceptor even though URLs are not protected
    - PM21308 CWSIT0034E and CWSIT0110E caused by SECJ9314E exception in Service Integration Bus
    - PM30108 Cannot forward. Response already committed on SPNEGO system
- **SDK levels**
  - Important to be on correct WAS SDK - minimum is pxa6460sr7ifix-20100824_01
- **MS change Kerberos implementation from time to time, be vigilant!**
  - This caught us out; SDK fix helped here
- **LDAP referrals - perhaps a special case**
  - This is where user accounts are in one domain, with groups in other domain(s)
  - To build a valid session, WebSphere tries to follow the referrals
  - Do NOT enable LDAP referral following in WAS via WIMConfig.xml - breaks WAS :-(
  - Required additional iFix PM47036 for both WAS 7.0.0.11 and 7.0.0.13

AD configuration requires WAS Federated Repository - 1/4

- **To be 100% clear, WAS needs to "bind" to each and every AD domain within which are users needing to access WAS**
  - The two-way forest-level transitive trust is MERELY to provide seamless Single Sign-On
  - It does NOT take away the need for WAS → AD binding via LDAP
  - Same is true for other related services e.g. IBM Tivoli Directory Integrator, used to "feed" IBM Connections
- **Same as for "normal" WAS <-> Active Directory configuration**
  - In most cases, SSL is used so there's a need to import certificates
  - Ideally, use "proper" CA-generated certificates rather than short-lived domain-level certificates
    - Requires a WAS iFix PM37795 prior to 7.0.0.19 to correctly retrieve "root" CA certificates rather than intermediate/chained certificates
  - TDI needs same set of SSL certificates for Connections user data population
- **User and Group search filters are defined as per the default for WAS <-> Active Directory**
  - This can and should be tuned
  - LDAP search / browser tools are good here e.g. LBE, Softera, Apache Directory Studio etc.

19

AD configuration requires WAS Federated Repository - 2/4

- **Two login attributes used**
  - Defined in WAS Integrated Solutions Console, mapped in WIMConfig.xml – see next slide
  - Common Name (**cn**) mapped to **sAMAccountName** == Windows login ID e.g. **haydb**
  - User ID (**uid**) mapped to **userPrincipalName == sAMAccountName** plus **realm** e.g. haydb@foo.net

- **Changes made to WebSphere security e.g. Federated Repository, SSO, SPNEGO etc. are reflected in WIMConfig.xml**
  - HOWEVER, the attribute mappings: -

    cn → sAMAccountName
    uid → userPrincipalName

  are NOT supported via ISC
  - This means that manual updates to WIMConfig.xml are over-written by changes in the ISC :-(
  - Therefore **cn** and **uid** mappings will be LOST
  - Highlights the **need** for change/version management of this critical file

AD configuration requires WAS Federated Repository - 3/4

```
...
    <config:repositories xsi:type="config:LdapRepositoryType"
adapterClassName="com.ibm.ws.wim.adapter.ldap.LdapAdapter"
        id="FOOBAR" isExtIdUnique="true" supportAsyncMode="false" supportExternalName="false"
        supportPaging="false" supportSorting="false" supportTransactions="false" certificateFilter=""
        certificateMapMode="exactdn" ldapServerType="AD" translateRDN="false">
      <config:baseEntries name="dc=foo,dc=net" nameInRepository="dc=foo,dc=net"/>
      <config:loginProperties>uid</config:loginProperties>
      <config:loginProperties>cn</config:loginProperties>
...

...
          <config:attributes name="userPrincipalName" propertyName="uid">
                <config:entityTypes>PersonAccount</config:entityTypes>
          </config:attributes>
          <config:attributes name="sAMAccountName" propertyName="cn">
                <config:entityTypes>PersonAccount</config:entityTypes>
          </config:attributes>
...
```

This will be lost if changes are made to the Federated Repository configuration via the Integrated Solutions Console

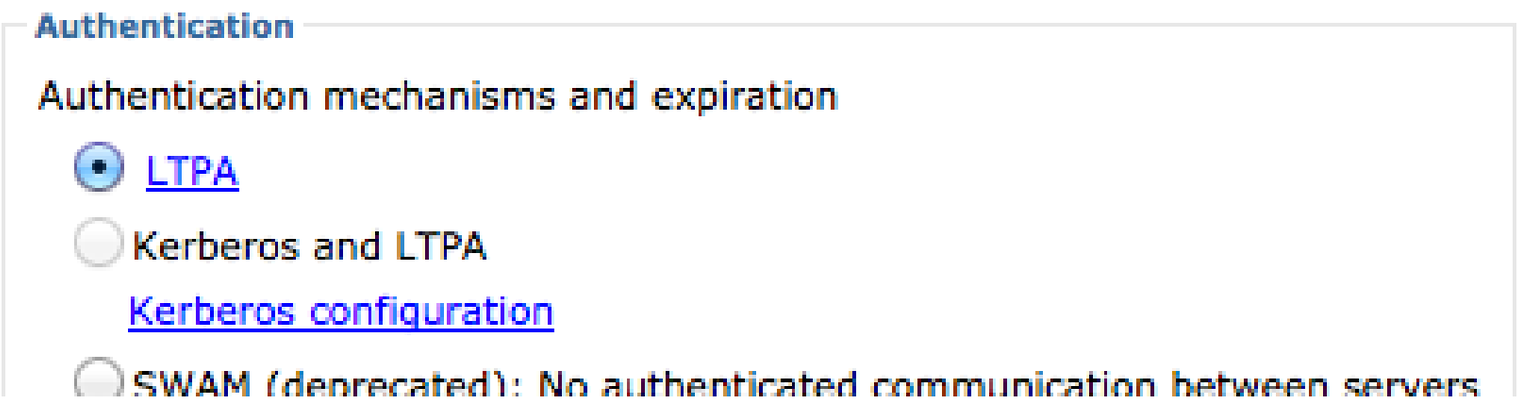
AD configuration requires WAS Federated Repository - 4/4

```
…
  <config:realmConfiguration defaultRealm="Collaboration">
    <config:realms delimiter="/" name="Collaboration" securityUse="active" allowOperationIfReposDown="true">
      <config:participatingBaseEntries name="ou=groups,o=foo"/>
      <config:participatingBaseEntries name="ou=users,o=foo"/>
      <config:participatingBaseEntries name="ou=systems,o=foo"/>
      <config:participatingBaseEntries name="ou=admins,o=foo"/>
…
…
```

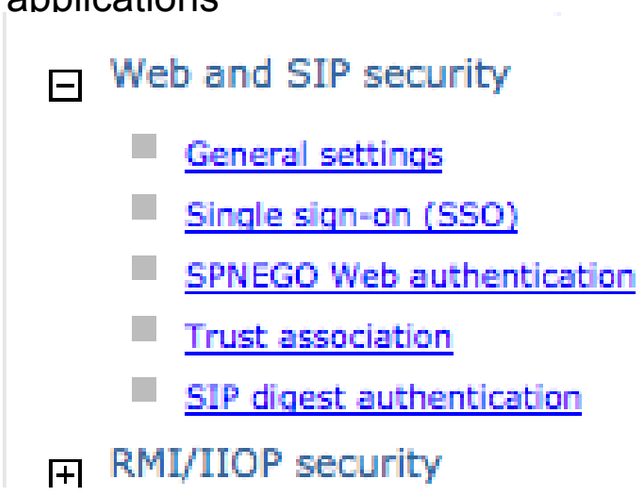
*This setting is NOT the default, but it really really should be. It's absence means that WAS will **NOT** handle **ANY** logins if it's unable to connect to **ANY ONE** of the Federated Repositories*

Kerberos vs SPNEGO in WAS

- **Need to differentiate between SPNEGO and Kerberos**
  - WAS supports both
  - Configuration via ISC varies
- **WebSphere supports native Kerberos authentication; we do NOT use that**
  - Kerberos can be used for primary authentication, including EJB access
  - For this scenario, we're using Kerberos for web authentication, rather than enterprise applications



WRONG



RIGHT

Global security

Global security > Kerberos

When configured, Kerberos will be the primary authentication mechanism. Configure EJB authentication to resources by accessing the resource references links on the applications details panel.

Kerberos Authentication Mechanism

* Kerberos service name
WAS

* Kerberos configuration file with full path
Browse...

Kerberos keytab file name with full path
Browse...

Kerberos realm name

☑ Trim Kerberos realm from principal name

☑ Enable delegation of Kerberos credentials

Apply OK Reset Cancel

Related Configuration

- SPNEGO Web authentication
- LDAP user registry filter settings
- CSIv2 inbound communications
- CSIv2 outbound communications

WRONG

Global security

Global security > SPNEGO Web authentication

SPNEGO provides a way for Web clients and the server to negotiate the web authentication protocol used to permit communications.

General Properties

☐ Dynamically update SPNEGO

☐ Enable SPNEGO

☐ Allow fall back to application authentication mechanism

* Kerberos configuration file with full path
Browse...

Kerberos keytab file name with full path
Browse...

SPNEGO Filters:

New Delete

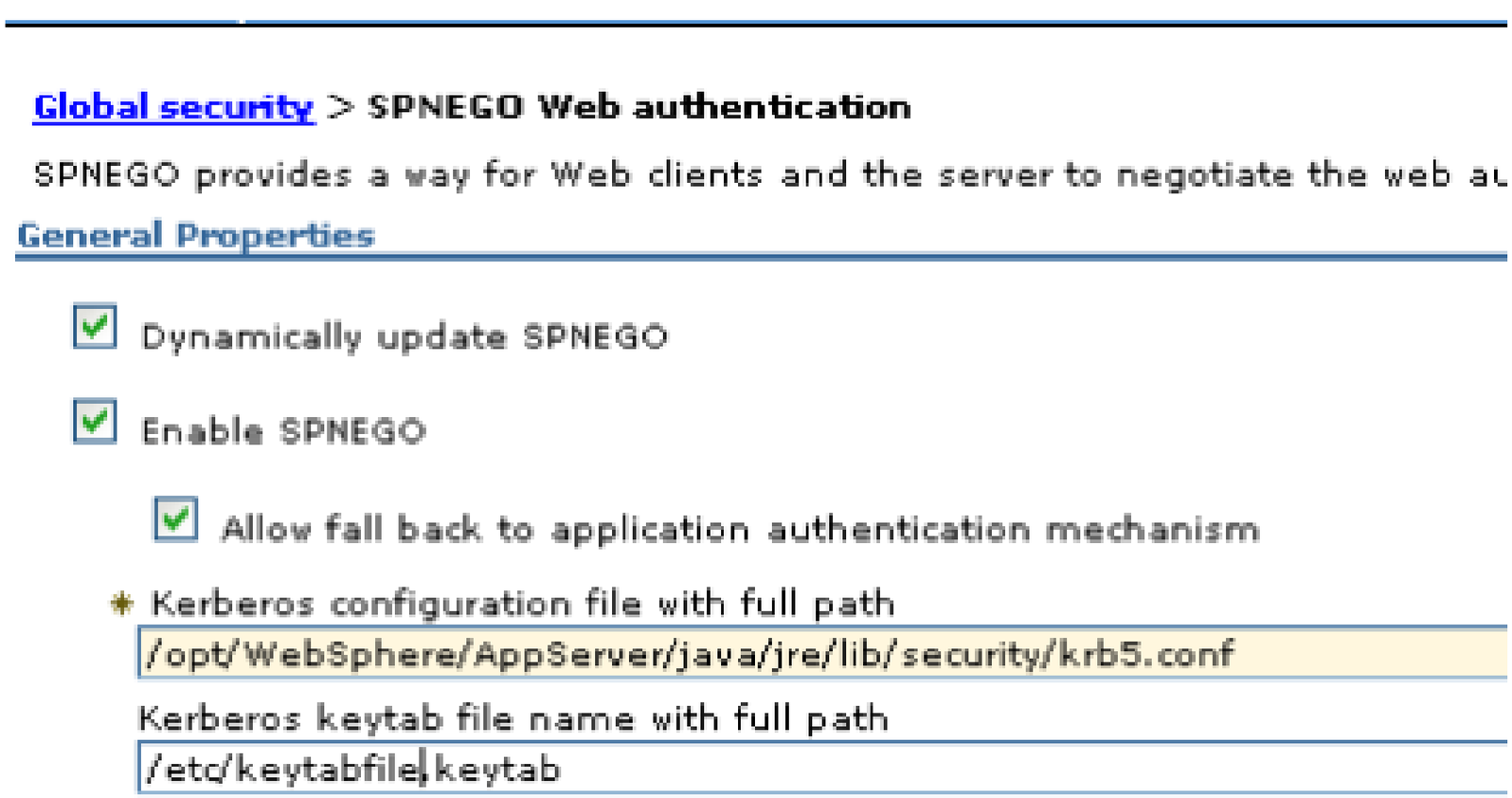
Select	Host Name	Kerberos Realm Name	Filter Criteria
None			
Total 0			

Apply OK Reset Cancel

RIGHT

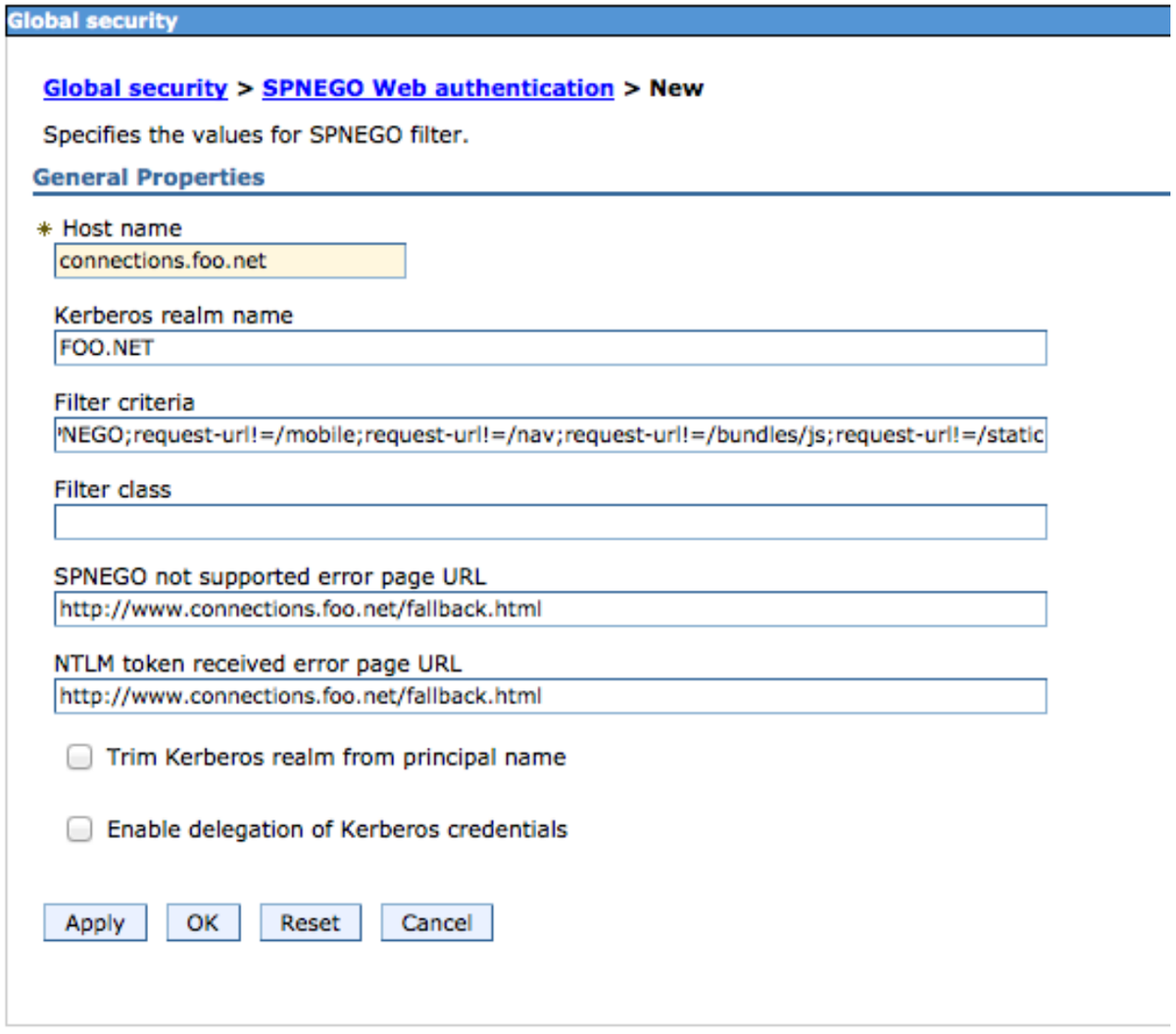
SPNEGO configuration in WAS

- **WebSphere krb5.conf file is created, referencing the Kerberos keytab file and realm definitions: -**
  - *$AdminTask createKrbConfigFile { -krbPath /opt/WebSphere/AppServer/java/jre/lib/security/krb5.conf -realm FOO.NET -kdcHost myad.foo.net -dns DNSName.foo.net -keytabPath /etc/keytabfile.keytab }*
- **Resulting file AND keytab are then referenced in WAS ISC as per example: -**



Configuring SPNEGO Filter

- **This defines the conditions under which SPNEGO is/not used**
- **References the Fallback Login page (more to follow)**
- **Examples of "Filter criteria" on next slide**
- **Note that "Trim Kerberos realm from principal name" is left UNCHECKED**
  - WAS uses the untrimmed User Principal Name, retreived from the Kerberos ticket, to find the user in the right Kerbeos realm / AD domain
  - If we chose to "trim" the "Kerberos realm" from the ticket, we'd only know the sAMAccountName, not the userPrincipalName



Examples of SPNEGO Filter Criteria

IBM Connections

request-url!=noSPNEGO;
request-url!=/mobile;
request-url!=/nav;
request-url!=/bundles/js;
request-url!=/static

IBM WebSphere Portal / IBM Web Content Manager

request-url!=/nameTypeahead.do;
request-url!=/serviceconfigs;
request-url!=/atom;
request-url!=noSPNEGO;
request-url!=/FileTransfer;
request-url!=/mobile;
request-url!=/nav;
request-url!=/bundles/js;
request-url!=/static;
request-url!=/wps/portal/;
request-url!=/portal_dojo/;
request-url!=/my_custom_webdav.theme/;
request-url!=/wps/contenthandler/;
request-url!=/wps/menu/;
request-url!=/wps/redirect;
request-url!=/wps_semanticTag/

The Fallback Login Page

- **Fallback Login - what is it ?**
  - A “simple” page of HTML, typically hosted by the web server - IHS in our case
  - Connections Wiki includes a sample
  - Users who cannot use SPNEGO will be redirected to this page
- **Required to support users for whom SPNEGO does not work**
  - Examples include mobile devices e.g. iPad and non-IE browsers e.g. Safari, Chrome etc.
  - Firefox CAN support SPNEGO, but doesn’t by default - requires host-by-host configuration via about:config - property name is network.negotiate-auth.trusted-uris
- **Page created in IHS, configured in WAS**
  - Could be hosted from WAS but no benefit in doing so
- **Don’t try and access Fallback Login page directly; browser will go into a “spin cycle” :-)**

28

Post-SPNEGO configuration of IBM Connections - 1/2

- **Once SPNEGO is configured, Connections needs additional configuration**
- **Major dependancy is to ensure that Connections uses “real” Active Directory accounts in admin roles**
  - Technote 1454540 (Additional fixes required to use Windows desktop single sign-on for Lotus Connections 3.0 security) states this: -

    The connectionsAdmin J2C alias that you specified during installation must correspond to a valid account that can authenticate with Active Directory. It may map to a back-end administrative user account that must be capable of authenticating for single sign-on with Active Directory. If you need to update the user ID or credentials for this alias, see the Changing references to administrative credentials topic.

    The WebSphere administrative account that you use to administer WebSphere Application Server or IBM Connections through the WSADMIN command utility must be a valid account that can authenticate with Active Directory. Users specified in the WebSphere Internal File Repository (WIM) will not function properly.

Post-SPNEGO configuration of IBM Connections - 2/2

- **The Connections documentation (Wiki) is almost accurate, but still needs some work**
  - Ensure that you are using the latest version of the documentation
  - Need to update the Service Integration Bus configuration and map an AD user to the Bus Connector Role
  - Also need to clear down the bus contents having changed the admin alias
  - Relevant Wiki URLs are provided at the end of this deck

Lessons Learned

- **If your AD environment is in any way complicated, hire AD experts**
  - Seriously; don't assume that your AD knowledge is good enough
- **WIMConfig.xml is a fragile entity; keep it backed up and, if things don't work, it's a good place to start looking**
- **Kerberos and SPNEGO logging in WAS is useful**
  - However only turn on when debugging
- **If using SSL, consider top-level certificates rather than one per domain controller**
  - AD has an interesting "feature" in terms of certificate expiration, any time from 6-12 months in
  - You find out that it's expired after a DC reboot, when WAS fails to establish a secure connection
  - If you're missing **allowOperationIfReposDown="true"** in **WIMConfig.xml**, then NOBODY can log in, not even WAS administrator
    - That's how we learned about this parameter :-)
- **Make sure that browser is correctly set up for Integrated Windows Authentication, correct internet/intranet zones etc.**
- **In a multiple-domain environment, hope that sAMAccountName is unique**
  - If not, then users will need to log in using User Principal Name
  - This may be common for IT support staff who use the same **sAMAccountName** across domains
- **Understand that changes to Service Principal Name will require new Kerberos keytab files**
  - Make sure that there's time in the project to manage this change
- **Test, test and test again**

What's Next ?

- **Bring on additional Active Directory domains**
  - Today we have eight
  - There are another four or five out there
  - Apply judgement (cost/benefit analysis), perhaps based upon number of users in a given domain
    - It may be more cost effective to “move” the users
  - Consider alternatives e.g. directory aggregation “*One Directory to rule them all*”
- **Tuning and Optimization**
  - Make better use of WAS tuning and pooling
  - Look at LDAP search filters and more closely targeting user groups and Organizational Units
  - Consider an improved Fallback Login Page
    - Today users need to know their **userPrincipalName** or WAS will need to find their **sAMAccountName** across 8+ domains
    - Most users don't know their **userPrincipalName** ....
- **Make use of User Groups in AD for “personalizing” access to functionality and resources**

Questions ?

Further Reading and Reference - 1/2

- **IBM Connections 3.0.1 System Requirements**

  https://www-304.ibm.com/support/docview.wss?uid=swg27021342

- **Additional fixes required to use Windows desktop single sign-on for Lotus Connections 3.0 security**

  https://www-304.ibm.com/support/docview.wss?uid=swg21454540

- **WebSphere Application Server 7 - Kerberos (KRB5) authentication mechanism support for security**

  http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/csec_kerb_auth_explain.html

- **IBM Connections Wiki - Enabling single sign-on for the Windows desktop**

  http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Enabling_single_signon_for_the_Windows_desktop_ic301

- **Kerberos (KRB5) authentication mechanism support for security**

  http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/tsec_aumech.html

Further Reading and Reference - 2/2

- **Mapping an Active Directory account to administrative roles**

  http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Mapping_an_Active_Directory_account_to_administrative_roles_ic301

- **Updating the messaging bus configuration when the connectionsAdmin user ID changes**

  http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Updating_the_messaging_bus_configuration_when_the_connectionsAdmin_user_ID_changes_ic301

- **Creating a redirect page for users without SPNEGO support**

  http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Creating_a_redirect_page_for_users_without_SPNEGO_support_lc3

- **Kerberos (KRB5) authentication mechanism support for security**

  http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/csec_kerb_auth_explain.html

- **Introducing the single sign-on diagnostic tool for IBM Lotus Connections**
- **http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Introducing_the_single_sign-on_diagnostic_tool_for_IBM_Lotus_Connections**