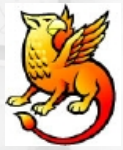
Shibboleth on Windows Installer Experience

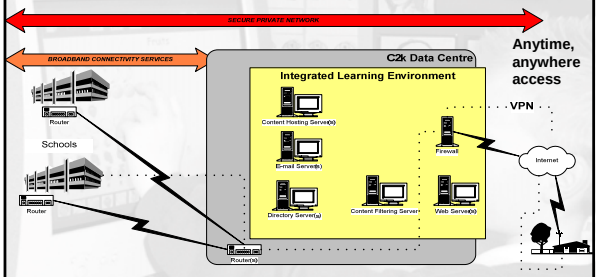


Ian Burgess – HP Technology Services

C2k Background & Statistics

- C2k is responsible for the provision of an ICT managed service to all schools in N. Ireland
- 330,000+ school children
- 5 Educational administrative regions (ELBs)
- 900 Primary Schools (4-11 years)
- 230 Post-primary Schools (11-18 years)
- 50 Special Schools (4-16 years)
- Infrastructure established in CY2003

The C2k Schools Environment



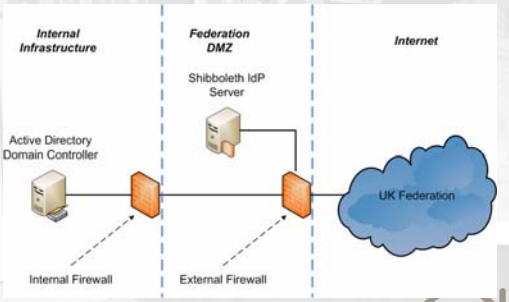
Directory Services & Identity Management

- Solid & reliable Identity Management is a pre-requisite for Shibboleth
- C2k use a single Microsoft Active Directory
- All user objects are created centrally; via
  - Be-spoke provisioning software
  - NO manual creation of accounts is permitted
- Strict rules enforce the quality of data e.g. username = "*jbloggs123*"
- Other considerations: technology is easy; the process is more challenging

Shibboleth on Windows Implementation Summary

Category	Implementation Details
Hardware	1 x server to host Shibboleth 1 x DMZ (De-Militarized Zone) for Shibboleth server
Software	Windows Server 2003 R2 operating system 1 x Digital Certificate Security & System Management software
Services	• Install and configure dedicated DMZ for the Shibboleth server • Configure necessary rules on the internal and external firewalls • Install Shibboleth via the Shibboleth on Windows Installer • Integrate Shibboleth with Active Directory • Install and test Digital Certificate • Test access to services

Shibboleth Infrastructure



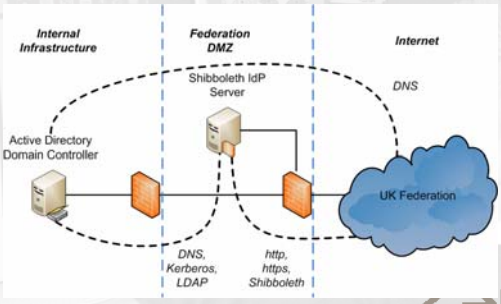
Internal Firewall

Source	Source Port	Target	Target Port	Action	Comment
Shibboleth IdP	*	AD Domain Controller	88/TCP & 88/UDP	Permit	Shibboleth IdP --- {Kerberos} ---> AD Domain Controller
Shibboleth IdP	*	AD Domain Controller	389/TCP	Permit	Shibboleth IdP --- {LDAP} ---> AD Domain Controller
Shibboleth IdP	*	Internal DNS Server	53/UDP	Permit	Shibboleth IdP --- {DNS} ---> AD Domain Controller/DNS

External Firewall

Source	Source Port	Target	Target Port	Action	Comment
Shibboleth IdP	*	*	80/TCP	Permit	Shibboleth IdP --- {HTTP} --> Internet
Shibboleth IdP	*	*	443/TCP	Permit	Shibboleth IdP --- {HTTPS/SSL} ---> Internet
*	*	Shibboleth IdP	8442/TCP	Permit	Internet --- {Shibboleth} ---> Shibboleth IdP
*	*	Shibboleth IdP	8443/TCP	Permit	Internet --- {Shibboleth} ---> Shibboleth IdP

Shibboleth Communications



Shibboleth on Windows Installer Installation

Parameter	Input Value
AD Domain:	ACME.NET
DNS Name for IDP:	shibboleth.acme.com
Scope to	acme.com
Kerberos:	DC01.ACME.NET:88
LDAP:	DC01.ACME.NET:389

Changes to “resolver.xml”

```
<JNDIDirectoryDataConnector id="directory">
  <Search filter="sAMAccountName=$PRINCIPAL$">
      <Controls searchScope="SUBTREE_SCOPE" returningObjects="false" />
  </Search>
  <Property name="java.naming.provider.url"
  value="ldap://DC01.ACME.NET:389/CN=Users,DC=ACME,DC=NET" />
  <Property name="java.naming.security.principal"
  value="shibboleth@ACME.NET" />
  <Property name="java.naming.security.credentials"
  value="C0mplexPassw0rd" />
  <Property name "java.naming.referral" value "follow"/>
</JNDIDirectoryDataConnector>
```

Attributes in the C2k AD

Data Stored	AD Attribute	Examples
Surname	Sn	Bloggs
Salutation	Title	Typically used for teachers e.g. Dr. Jones
First/Chosen Name	givenName	Joe
Email	Mail	jbloggs123@school.town.ni.sch.u
DENI Number, Unique user id (Pupil No./Teacher No.), DoB, Intake year, Gender, Curriculum	extensionAttributes1-6	
Secondary email address(es)	proxyAddresses	jbloggs123@school.org jbloggs123@c2kni.net

Shibboleth Attributes

Shibboleth Attribute	Publis	Initial C2k Decision
eduPersonScopedAffiliation	Y	Published as follows: •member@c2kni.net
eduPersonTargetedID	Y	Published to the UK Federation and distinct for each Service Provider •SID/GUID is hashed to give unique value
eduPersonPrincipalName	N	Potential issue with the following: •sAMAccountName – *bloggsj123* •secondary email – *bloggsj123@c2kni.net*
eduPersonEntitlement	N	As Shibboleth evolves in C2k we anticipate the creation of Shibboleth specific security groups within each school.

Current Considerations

- Scalability
  - How many users can we support on a Shibboleth IdP?
  - https://spaces.internet2.edu/display/SHIB/JMeterTesting
- Availability
  - VMware (& VMotion)
  - HA-Shib from https://spaces.internet2.edu/display/SHIB/Contributions
  - Deploying the IdP in a Load Balanced Environment https://spaces.internet2.edu/display/SHIB/LoadBalancedIdP
- Manageability
  - How do we monitor usage of Shibboleth?
- Supportability
  - How do we craft a SLA for Shibboleth?

Currently Considerations (2)

- Security
  - Credentials for internal AD stored in "resolver.xml"
- Portal Integration
  - Pre-Authentication to limit user exposure to WAYF
- C2k functioning as a Service Provider (SP)

For More Information

- UK Access Management Federation for Education and Research http://www.ukfederation.org.uk/
- JANET Shibboleth on Windows project http://www.ja.net/development/middleware/shibboleth-on-windows.html
- IdP installer for Active Directory https://spaces.internet2.edu/display/SHIB/IdPActiveDirectory

Questions?