C2K

Ian Burgess

Table of Contents

These case studies, prepared by organisations who participated in the JANET Shibboleth on Windows project, are provided for information purposes only and reflect the particular arrangements and experience of those concerned. In each case, the configuration, installation and implementation of the Shibboleth on Windows software will vary according to the type of infrastructure and technical resources involved.

Executive Summary

For a number of years the focus for the C2k[1] infrastructure has been on services that can be offered from within the internal network to the user community. With recent advances in federation software, the scope for offering services has broadened to include services hosted externally on the Internet.

Over the 2006/2007 timeframe C2k made a strategic decision to investigate how federation software could facilitate the seamless provision of external services to users.

In November 2006 the UK Access Management Federation for Education and Research was launched. Current membership of the UK federation includes organisations from the Schools, FE, HE and Research sectors, as well as organisations providing services to these sectors. C2k made another strategic decision to join the UK federation.

JANET(UK)'s Shibboleth on Windows Installer[2] pilot provided an opportunity to bring both of these strategic strands together. Installation and configuration of the software provided a mechanism to educate the technical teams, whilst an output of the pilot was a system pre-configured to function within the UK federation. C2k believes that the

[1] http://www.c2kni.org.uk/

[2] http://www.ja.net/development/middleware/shibboleth-on-windows.html

Shibboleth on Windows Installer software and the associated JANET(UK) pilot programme were key enablers in addressing both of these areas.

Background Information

C2k is responsible for the provision of an ICT (Information and Communications Technology) managed service to all schools in Northern Ireland. The managed service comprises of >80,000 networked computers connected across 1200 sites, together with a rich mix of educational content and services.

C2k combines a number of services from multiple service providers to deliver the overall ICT managed service. HP (Hewlett-Packard Limited) has responsibility for delivering the wide area services which include connectivity, systems integration and a new Northern Ireland Data Centre. Northgate Information Solutions is responsible for the delivery and management of >80,000 PCs along with specialised educational software, servers, switches and LAN infrastructure to the primary, post-primary and special schools sectors. BT provides the communications infrastructure which underpins the entire network across the Northern Ireland Education Service.

Resources from both C2k and HP often combine to form virtual teams with responsibility for different aspects of the wide area services. Senior management from both organisations focus on the high-level strategy aspects of the ICT managed service, whilst the technical teams focus on the day-to-day aspects of delivering both current and new services to the user population.

From a technology perspective, C2k utilises a single directory service for authenticating and authorising all 350,000 users comprising all students, teaching staff and non-teaching staff. Where it is both possible and appropriate the internal applications and services within the C2k infrastructure leverage the single sign-on capabilities of Microsoft Windows and Microsoft Active Directory.

Access Management

A combination of bulk provisioning and ad hoc provisioning tools are used to control the creation and deletion of user accounts and groups within the C2k infrastructure.

A GUI-based management tool called CC3 (Community Connect 3) from RM enables the simple management of user accounts and security groups at the school level. The CC3 Management Console is designed to hide some of the complexity of the standard Active Directory user management utilities behind a simple GUI.

In general access management in the C2k infrastructure relies upon and leverages security groups within each school. Users are either added or removed from security groups to grant and deny access to specific resources.

The overall strategy and administrative model for access management in the C2k infrastructure could be summarised as a centralised provisioning solution with on-going management delegated appropriately to IT administrators in individual schools.

When initiating access to the C2k infrastructure from an internal network location the users go through the usual Windows login process. After successful authentication the

users have a single sign-on experience and seamlessly access all of the resources to which they have been granted access.

By implementing Shibboleth, C2k hope to extend the scope of the single sign-on experience to include external applications and services residing on the Internet outside of the C2k core services.

Initially C2k wishes to function as an IdP (Identity Provider) and consume services offered by members of the UK federation. A longer-term objective is for C2k to function as a SP (Service Provider) and offer services back into the UK federation.

Aims and Objectives

C2k set a number of aims and objectives for the Shibboleth on Windows Installer Pilot:

- Increase knowledge across both C2k and HP on the process, benefits and implications of federating the C2k infrastructure with other organisations on the Internet.
- Confirm that Shibboleth can be integrated into the C2k infrastructure.
- Implement the C2k infrastructure as an IdP in the UK federation.

Implementation

The implementation of Shibboleth required integration with a number of people, processes and technologies in the C2k infrastructure.

Table 1 summarises the categories and details for the integration.

Category	Details of Integration
Hardware	1 x dedicated DMZ for Shibboleth server 1 x dedicated server to host Shibboleth
Software	Windows Server 2003 R2 operating system 1 x Digital Certificate Security management software System management software

Category	Details of Integration
Services	Network Team • Install and configure dedicated DMZ for the Shibboleth server Security Team • Configure necessary rules on the internal and external firewalls Server Team • Install Shibboleth via the Shibboleth on Windows Installer • Integrate Shibboleth with Active Directory • Install and test Digital Certificate • Test access to services

Table 1: Components required for Implementation

The exact installation and configuration tasks are described in detail in two additional documents that C2k delivered as part of the Shibboleth on Windows Installer pilot:

- Integrating a Shibboleth IdP with Microsoft Active Directory
- Sample Security Configuration for a Shibboleth IdP.

These documents also contain a number of hints and tips that C2k uncovered during their implementation of Shibboleth.

Methodology

The C2k deployment of federated access management (via Shibboleth) was essentially a hybrid approach. C2k has deployed an in-house implementation with the help of a third-party service provider i.e. HP. C2k's contract with HP for service provision covers services hosted within a central data centre, and this was deemed to be the most appropriate route for introducing Shibboleth into the C2k environment.

A number of people from C2k and HP were involved in integrating Shibboleth into the C2k infrastructure. Table 2 identifies the specific roles and responsibilities within the Shibboleth project.

Organisation	Role	Responsibilities
C2k	Integration Director	Setting the strategy for the overall C2k infrastructure. Specifically in relation to Shibboleth, determining the role that Shibboleth could/should play in the wider ICT managed service.
C2k	Contracts Manager	Reviewing and approving contractual documents for the UK federation.

Organisation	Role	Responsibilities
C2k	Solution Owner	Day-to-day running of Shibboleth specific proof-of-concept, pilot or production rollout.
HP	Service Delivery Manager	Overall responsibility for the central services in the C2k infrastructure (both existing and new services).
HP	Solution Architect	Design and implementation of the integration of Shibboleth into the C2k infrastructure.
HP	Technical Teams e.g. • Network Team • Security Team • Server Team	Implementing and integrating Shibboleth into the C2k infrastructure.

Table 2: Roles and Responsibilities

As the strategy for the C2k ICT managed service evolves, the C2k Integration Director and C2k Integration & Development team regularly assess the technologies that should be part of the C2k infrastructure. During one of the previous review cycles C2k decided to investigate the role that Shibboleth could play in the functional area of identity and access management.

The process of planning the actual design and integration of Shibboleth into the C2k infrastructure began in September 2007. To kick-start this process representatives from both C2k and HP attended a number of JANET(UK) workshops:

- one day access management workshop on 17th September 2007 at Woburn House, London
- one day schools sector discussion of UK federation services on 10th October 2007, Church House Conference Centre, London.

C2k then applied for and was granted membership of the Shibboleth on Windows Installer Pilot in 2008. C2k's participation in the pilot lasted from March 2008 to September 2008.

Although the process of designing and implementing Shibboleth has taken one year, this was due to the size and complexity of the C2k environment rather than the Shibboleth technology itself. Given the scale and nature of the C2k infrastructure, many initiatives run in parallel throughout each year and resources are assigned and distributed accordingly.

The implementation of Shibboleth was broken down into a number of project phases:

1. Proof of concept within the Shibboleth project team.
2. Pilot on Shibboleth in one or more schools.
3. Implementation of Shibboleth as a service to the entire C2k infrastructure.

Table 3 provides a summary of the phases, objectives, status, timeframes and outputs for the C2k Shibboleth project.

Phase	Objective	Status	Timeframe	Deliverables
1	Conduct a proof of concept for Shibboleth	Complete	Mar 2008 – Sep 2008	1 x Shibboleth server integrated into the C2k infrastructure The C2k infrastructure is linked to the UK federation.
2	Pilot of Shibboleth	Open	Starting Oct 2008 End date to be confirmed	Detailed design document for a resilient Shibboleth solution. Highly-available and scalable Shibboleth solution implemented within the C2k infrastructure. Feedback from pilot schools on user experience when using Shibboleth
3	Production rollout of Shibboleth	Open	To be determined	Federation solution which can be leveraged by the entire C2k user population. Introduction and benefits statement for the user community.

Table 3: Project Summary

To date the first phase of the project has been completed. It is anticipated that the remaining phases will be conducted during the remainder of 2008 and early 2009.

Given that Shibboleth has yet to be utilised by the C2k user community, the roll-out experiences are limited to the technical community that was tasked with implementing Shibboleth.

The initial installation of the Shibboleth on Windows Installer software was a great success. The software allowed C2k to rapidly implement the core software and immediately focus on detailed integration tasks. To understand the amount of manual configuration work that the installer eliminates please refer to the following thread from the Shibboleth Users mailing list:

https://mail.internet2.edu/wws/arc/shibboleth-users/2007-01/msg00207.html

The two main challenges encountered by C2k during the Shibboleth pilot were:

1. Identifying technical documentation that specifically addressed the customisation of Shibboleth (especially when running on a Windows platform).

2. Developing the required knowledge across a broad range of technologies.

Regarding the first point, most environments require a level of customisation to close out the implementation within their own infrastructure. This process typically requires editing a number of XML configuration files, e.g. resolver.xml & arp.site.xml. The Shibboleth project team from C2k was unable to locate comprehensive documentation which specified problems, discussed potential options and progressed through to the implementation of technical solutions.

The second point may only be an issue in large scale environments such as the C2k infrastructure. The main technical teams in C2k (e.g. Network, Security and Server) support well defined but distinct technology areas. Shibboleth as a technology requires a level of technical knowledge across a broad range of components. Table 4 identifies the components that require installation or configuration in the C2k infrastructure.

Infrastructure Category	**Infrastructure Components**
Overall Architecture	• Internally and externally facing systems/services
Network	• VLAN(s) to host the Shibboleth server • IP subnet(s) and IP addresses • IP address and port translation
Security	• Firewalls and firewall rule sets • Digital certificates
Server	• Active Directory integration • Shibboleth software e.g. XML configuration files

Table 4: Infrastructure Categories and Components

C2k has yet to realise the anticipated benefits of implementing Shibboleth. It is hoped that Shibboleth will improve the end-user experience when accessing external services, and align with existing de-centralised administration model that governs the C2k infrastructure.

C2k believes that the process of deployment could be made easier with centralised effort (i.e. JANET assistance) in the following areas:

1. Detailed implementation case studies on how other organisations have implemented Shibboleth (with a particular focus on Windows-based infrastructures).

2. Prescriptive technical guidance on the implementation and usage of attributes within the UK federation.

The first of these points could be viewed as a 'chicken and egg' scenario. The type of documentation being requested is actually being produced within the Shibboleth on Windows Installer Pilot, which the C2k organisation is participating in.

As a possible solution to the second point, JANET could provide step-by-step guidance on how to implement, customise and release the four core attributes utilised within the UK federation.

Project Experience

C2k's overall experience of implementing Shibboleth within the C2k infrastructure has been very positive. The Shibboleth on Windows Installer software has fast-tracked the integration of an entirely new technology into a large and diverse infrastructure. The technical teams have been able to focus on pure integration issues and devote a minimal amount of effort to installing the core Shibboleth software components.

Conclusions and Implications

Whilst the majority of infrastructure components are commonly utilised in customer environments, the fact remains that the core Shibboleth software is a very specialised and specific piece of software. This may be of limited concern to an in-house implementation but it presents some challenges to an out-sourcing arrangement.

Large out-sourcing companies traditionally prefer commercial software as opposed to open source equivalents. The use of Shibboleth within an outsourcing contract will therefore require discussion and agreement on:

- Service Level Agreements (and any associated penalty clauses and charging)
- cost for on-going support and maintenance.

The Shibboleth on Windows Installer software configures a single server solution. In large scale environments like C2k with a user population of over 350,000 this poses a problem, particular as the software becomes more and more utilised. Shibboleth ultimately becomes a single point of failure. High availability solutions and components can be applied to Shibboleth but it is not yet known if a solution created using the Shibboleth on Windows Installer can be evolved into the desired configuration. This is an area that C2k hopes to investigate in a later project phase.

Recommendations

Having completed the first phase of its Shibboleth implementation, C2k would make a number of recommendations to other organisations embarking upon a similar project. These recommendations are derived from C2k's experiences. Considering the scale and complexity of the C2k environment, the recommendations may not be totally applicable in other less complex infrastructures.

- Contractual and Legal Considerations
    - At the start of the project, identify the personnel that will be required to review and approve contractual and legal documents. This process could take longer than the implementation of the technical solution. The principles of the Data Protection Act apply to the use of the eduPersonPrincipalName attribute.
- Project Related Issues

  - Ensure that all project team members (both managerial and technical) have baseline knowledge of the entire solution.
  - Establish a small test environment in parallel to any production solution, and leverage the online testing facilities of TestShib (https://www.testshib.org/). This allows an organisation to test the impact of changes to XML configuration files before rolling out organisation-wide.

- Technical Recommendations
  - Use a dedicated DMZ for the Shibboleth Server.
  - Use a dedicated server (physical or virtual) to host the Shibboleth software.
  - Take one of the core attributes of the UK federation and review its use across the entire solution. Identify any changes that are required to the XML configuration files e.g. resolver.xml & arp.site.xml. Repeat the process for the remaining attributes.