Proposal by
Oxford Computer Group
for:
Identity & Access Management

Prepared for:

Department for International Development

By:

David Wozny

Security Architect

Version 1.1

Document Management

Distribution

Team Member	Company	Role
David Wozny	OCG	Security Architect
Simon Veale	OCG	Senior Architect
Steve Mitchell	OCG	Technical Director
Jeremy Wilson	OCG	Practice Manager
Alison Werkman	OCG	Account Manager
Neil Coughlan	OCG	Sales Director

Revision History

Version	Date	Updated or Reviewed By	Details
V0.1	4th December, 2007	David Wozny	First draft
V0.2	4th December, 2007	Simon Veale	Review
V0.3	4th December, 2007	Alison Werkman	Adding commercial information
V1.0	7th December, 2007	Alison Werkman	Release Final Version
V1.1	7th December, 2007	Alison Werkman	Alteration to Pricing

Contents

Introduction

Following a consultative workshop with the Department for International Development (DFID) on 27th November 2007 in East Kilbride, Oxford Computer Group (OCG) has prepared this report and proposal to address DFID's requirements to implement Two Factor Authentication (2FA) for Windows logon using digital certificate credentials stored on smart cards.

This document serves as both a record of the requirements discussed, along with a high-level architecture design and proposal for services (as well as indicative hardware / software costs) should DFID decide to engage OCG in the deployment of the proposed solution.

This document is organized as follows:

- Executive Summary
- Background, Current Situation and Requirements
- Proposed Solution and Statement of Work

Executive Summary

The Case for Two Factor Authentication

DFID staff presently logon to Windows (Active Directory) with password protected user credentials. In the present security climate this is considered *weak* due to the fact passwords are vulnerable to *hostile parties* acquiring encrypted passwords (by means such as *network snooping*) which can then be subjected to brute force tools, amongst other forms of attack. Passwords are also particularly vulnerable to social engineering based attacks.

As a primary defence to mitigate password vulnerabilities, organisations implement strong password requirements in combination with routine enforcement of password changes to make passwords less *discoverable* and reduce a hostile party's window of opportunity. The trade-off is additional complexity for the user, and the social engineering vulnerability of passwords is still not addressed.

2FA for Windows logon strengthens the security of the user's credential by *replacing* the password with a digital certificate (and corresponding cryptographic private key). The digital certificate is issued to the user in a controlled, workflow based process from a Certification Authority (CA) which is implemented into the DFID estate in a strictly controlled and audited manner such that DFID has utmost confidence in the trustworthiness of any digital certificates it issues henceforward.

The digital certificate (and private key) is stored on smart card, which is a cryptographically secure token, requiring a Personal Identification Number (PIN) be entered during logon to access key material in secure containers on the smart card. Unlike passwords, PINs never traverse a network (encrypted or otherwise) and are therefore not discoverable; this allows use of shorter, more memorable PINs, with the added benefit that they do not need to be changed on a periodic basis.

For a hostile party to impersonate a user requires possession of the private key (associated with the user's digital certificate) hosted on the smart card and knowledge of the PIN to unlock the container storing the aforementioned private key. This is commonly referred to as… *something you have and something you know*.

2FA overcomes the majority of social engineering attacks since knowledge of a PIN is useless without possession of the smart card, and likewise, a lost / stolen card is of no value without possession of the PIN.

Solution Overview

Smart card logon to Windows is natively supported in Windows 2000, Windows Server 2003 and Windows XP by extensions to the Kerberos protocol. Therefore no fundamental change to the Active Directory logon servicing infrastructure is required.

The primary new components which need to be introduced to the DFID IT environment are CAs and Registration Authorities (RAs). CAs *manufacture* and issue digital certificates to subscribing entities; RAs handle request / approval notification and generally all processes required in the verification of digital certificate requests prior to submission to a CA. In the context of digital certificates being issued onto smart cards, the RA is also combined with a smart card management system capability.

Certification Authorities

The CA requirements are met by implementing a two-tier architecture, consisting of an *offline* Root CA server (meaning it is physically disconnected from any networks at all times) and an online Issuing CA server. The Root CA server is the *trust anchor* of the DFID Public Key Infrastructure (PKI), enabling ultimate protection of the DFID trust chain in the event of a compromise of a *downstream* Issuing CA server. The Root CA server is also where cross-certification with any other *foreign* PKIs (OGDs, etc.) would likely occur in the event that future trust service interoperability is required. The Issuing CA server would be implemented as an Active Directory (AD) member server and rely upon AD for much of its operating capability and configuration.

Both CA server types would be deployed on the Windows Server 2003 platform and employ Hardware Security Modules (HSMs) to secure their signing key material; this key *stamps* all digital certificates which it issues and is critical to the authenticity of issued digital certificates. If a CA server's signing key is compromised, it is relatively simple for a hostile party to impersonate a CA server and fraudulently issue digital certificates to compromise identities.

Registration Authority

The RA abstracts users and operators from the CA server in the context of handling certificate lifecycle processes such as enrolment, renewal and revocation requests, etc. Most smart card management processes are handled at the RA, facilitating PIN resets, smart card duplication, temporary smart card issuance, etc. Microsoft Identity Lifecycle Manager (ILM) is proposed, deployed extremely tightly to Active Directory and Microsoft Issuing CA servers. Users and operators access ILM (a .NET 2.0 application running on IIS 6.0) using the Internet Explorer web browser.

The flexibility of ILM in terms of its comprehensive workflow capability is extremely valuable in a distributed environment such as that of DFID, facilitating development of unique management processes to support the UK / overseas office *communities*, with perhaps even finer refinement within certain overseas offices. The auditing capability of ILM is another extremely strong area, in terms not only of the richness and depth of information captured, but also its ease of accessibility. Smart card printers deployed centrally in combination with ILM enable visual personalisation of smart cards prior to distribution.

As with the CA servers, the RA server requires access to security sensitive cryptographic key material necessitating the use of HSMs to protect that key material.

Supporting Infrastructure

In addition to the primary new components described above, further supporting infrastructure is required such as Microsoft SQL Server for ILM to store audit data and user workflow tracking data. It is preferred that *new* SQL Servers would be deployed to support ILM, rather than deploy on existing SQL Server farms. Dependant upon workflow choice (though very likely to be required), email notification requires access to messaging servers; existing Exchange Servers would be used.

Summary

The solution proposed in this document provides a 2FA solution that meets DFID's immediate known requirements, whilst not constraining future scope extension. Any subsequent phases will build on the solution proposed here without the need for re-architecting, and new components will be able to be "plugged in" as required without disrupting the existing service.

With Microsoft Certificate Services and Identity Lifecycle Manager (ILM) 2007 at its heart the solution is robust, scalable and extensible.

Current Situation

Environment Overview

DFID has a distributed environment, with two primary sites in Glasgow and London complemented by 62 overseas offices. There are approximately six hundred users in Glasgow and nine hundred users in London; the overseas offices range from between five and eighty users. A very high level representation of the DFID "network" is shown in Figure 1. IT infrastructure is managed in-house, i.e. not outsourced.

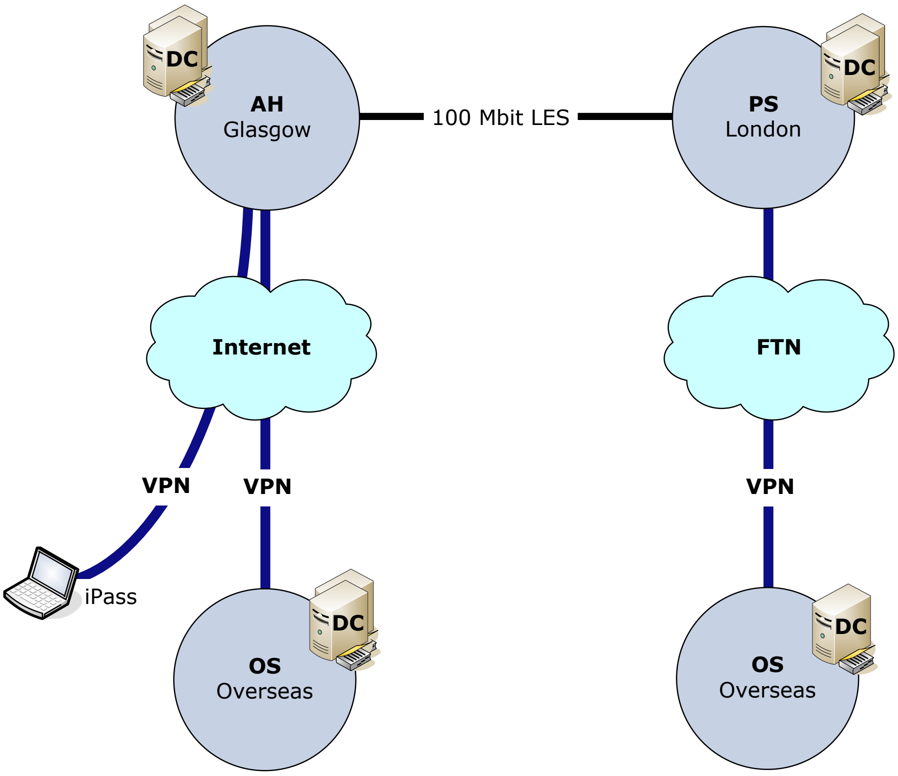

Figure 1: DFID Network

The overseas offices are connected to the UK sites via VPN technology over the internet or FTN services; in addition there are mobile users who connect over the internet by means of iPass initiated VPN sessions.

There is a single AD forest comprising a root domain (DFID) and child domain (GSX); all user accounts *participating in* the 2FA project exist in the DFID domain.

Connectivity between offices is generally very good with a maximum of fifteen minutes replication latency between offices; all offices have at least one domain controller, though two is more common.

Some Windows 2000 CA servers are implemented in the DFID estate, though they are not *legitimate candidates* for leveraging for the 2FA project.

Helpdesks in the UK and India provide approximately 90% round the clock coverage to the user population.

Business Drivers

The critical business driver is to strengthen assurance around authentication by implementing two-factor authentication to Windows using smart cards, in overseas offices worldwide as well as the two *UK hubs* in Glasgow and London.

A complementary driver is to demonstrate DFID's commitment to secure, robust IT infrastructure to enhance its reputation within government.

Requirements

The following requirements have been identified:

- Implementation of two factor authentication capability for Windows logon, incorporating PKI and smart card management systems with worldwide scope
- Enforcement of aforementioned smart card logon for all users with the exception of a limited number of external users who solely access DFID hosted messaging services via Outlook Web Access (OWA)
- A rich workflow capability for the entire smart card management lifecycle, enabling a flexible approach to be taken; it is recognised that many administrators in overseas offices are not security cleared and certain smart card management activities need to reflect that. A typical approach would be:
    - Centralised management of smart card issuance
    - Delegated smart card lifecycle management activities such as PIN resets, temporary card issuance, etc. (incorporating the use of *kiosks* in certain circumstances when appropriate)
- Printing onto smart cards to visually personalise smart cards
- Production of design guides and implementation ceremony documentation ready for review by DFID's *security guidance advisors*, understood to be CESG
- Production of operational and recovery guides
- Knowledge transfer to designated DFID staff

Scope Statements

- All Windows Server infrastructure accessed via smart card logon is based upon the Windows Server 2003 platform; likewise all Windows client infrastructure is based upon the Windows XP platform.
- Windows 2000 and Windows Vista are not supported platforms within the scope of this project, though the design will ensure that future scope extension to use Windows Vista is not prohibited.
- Integration with the Microsoft Identity Integration Services (MIIS) infrastructure in place at DFID is outside of the scope of this project, though the design will ensure that future scope extension to integrate with this solution is not prohibited.
- Issuance of certificates for any purpose than supporting the 2FA project is outside of scope, though the PKI being implemented could clearly be extended by DFID for use to issue client authentication certificates for wireless authentication etc.
- Migration of certificates from the existing PKI is out of scope, though assistance will be given by OCG on a best endeavours basis.
- Deployment Online Certificate Status Protocol (OCSP) to complement Certificate Revocation List (CRL) based validation technology to improve *revocation propagation freshness* is out of scope for the present phase of the project.

Existing Infrastructure

There may not be a suitable development and test environment at present. It may necessary that one is developed to enable the detailed design, engineering and operational / recovery procedures to be produced.

Existing Skills and Resource Availability

Internal DFID resource has some experience of PKI, though it is likely that this will need to be enhanced either by external training or very close engagement with OCG during development and further stages of the project.

Easy access to various DFID resources in multiple teams (network, monitoring, messaging, DBA, etc.) is essential for successful execution of the project.

Proposal

Stages

OCG proposes that DFID address the requirements that have been identified in the following staged manner:

- Proof of Concept
- Low Level Design and Engineering
- Production Implementation

These three stages are expanded upon in greater detail in the *project approach* section of this document.

2FA Solution High Level Architecture

Figure 2 illustrates the proposed solution to meet DFID's 2FA requirements, High Availability (HA) and Disaster Recovery (DR) are not considered in this section and therefore only single instances of each component are described. HA / DR scenarios and options are addressed later in a later section in this chapter.

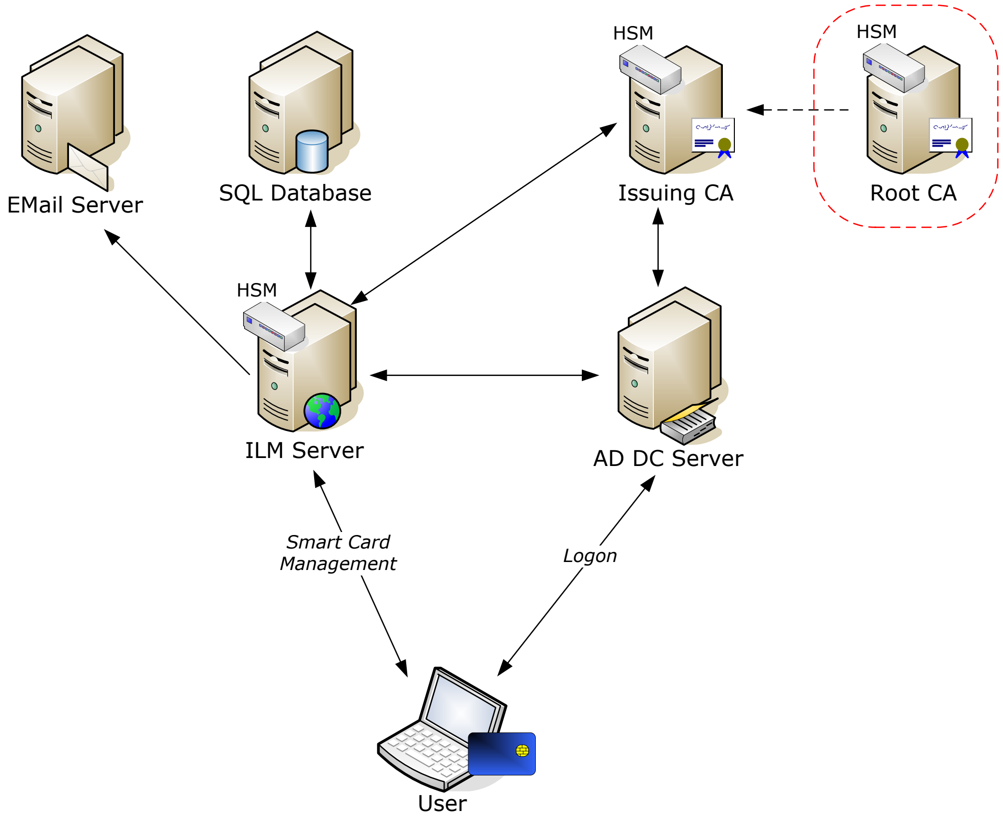

Figure 2: 2FA Solution Overview

Solution Elements

Root CA Server

The solution incorporates a single Root CA server, deployed on Windows Server 2003 Standard Edition. As previously stated this server will be deployed with no network connectivity and be built using a standard Windows Server media installation rather than a "gold disk" approach or scripted installation. Performance requirements are extremely slight and therefore any server which can satisfactorily run Windows Server

2003 will suffice; the only important specification *gotcha* is that it supports PCI-X expansion cards (which is the nCipher nShield format) – certain new servers only support PCIe by default and need different expansion cages specifying.

The Root CA server needs to be deployed in a physically secure situation, which might dictate whether a rack or tower type server profile is required. The Root CA server is powered-off ordinarily once the 2FA solution has been commissioned. The Root CA server is powered up on an infrequent basis (typically six or twelve months – dependant upon Root CA CRL validity period design) to publish a fresh CRL.

The Root CA server has special management requirements due to its offline nature and is not expected to have anti-virus software installed, nor would it participate in routine software updates.

A tape backup drive should be installed in-line with DFID preferences, be it DAT, DLT, AIT, etc. In addition, an external USB attached disk should be connected directly to the Root CA server for copying of certain backup material; this facilitates rapid restore in certain scenarios without having to resort to tape, and also serves as a useful additional backup location. The Windows Backup utility software can perform backup of the Root CA server satisfactorily, and will be used unless DFID express a requirement for a third-party solution.

An nCipher nShield PCI 500 TPS HSM shall be installed in the Root CA server, the precise model may be dictated by DFID accreditor guidance as there are FIPS 140-2 Level 2 or Level 3 models, the prices of which vary significantly and ordinarily the Level 2 unit would be preferred unless the accreditor indicates otherwise.

HSM Primer

Hardware security modules are used to protect security sensitive / high entitlement cryptographic key material: typically symmetric keys or private keys which are part of a public / private key pair. HSMs ensure the confidentiality of key material they protect both at rest and in use, as well as provide an authorisation mechanism to access the key material or to perform management operations on it. In combination with these logical controls, they also provide physical tamper resistance and tamper evident capability.

nCipher HSMs are proposed for the DFID 2FA project because not only do they provide requisite security controls around keys they protect, but also because their key management controls are extremely flexible and relatively simple to operate compared to some other HSM vendor solutions. Experience has shown this is an extremely important aspect since most organisations demand that PKI is no longer the realm of specialists, but likely to be supported by *Wintel type* support teams.

Issuing CA Server

The solution incorporates an Issuing CA server, deployed on Windows Server 2003 Enterprise Edition. This server is fully integrated in Active Directory and would be expected to be deployed using standard DFID build procedures. Performance requirements are not extreme since cryptographic operations are offloaded to an HSM (described later). The biggest bottleneck with a Microsoft Issuing CA tends to be AD lookups, so it is useful to have a fast *infrastructure* AD Domain Controller (DC) (rather than a DC handling user logons) *nearby* to improve lookup performance. As with the Root CA server, the only important specification *gotcha* is that it supports PCI-X expansion cards.

The Issuing CA server must be deployed in a physically secure situation, though still in a data centre environment, typically a *private rack* is assigned to the Issuing CA server and would also be expected to house RA server(s)).

The Issuing CA server will participate in anti-virus, patching and general service management regimes; however, the Windows host based firewall will be implemented to reduce the network attack surface of the Issuing CA server.

The standard data centre server backup regime (and media type / backup software standards) should be followed in-line with DFID policy. In addition, an external USB attached disk should be connected directly to the Issuing CA server for the same purpose as described for the Root CA server. Due to the key material protection afforded by the attached HSM, it is satisfactory for backup tapes / snapshots of the Issuing CA server to be stored without any specific additional controls.

An nCipher nShield PCI 500 TPS HSM shall be installed in the Issuing CA server, with the same provisos described for the Root CA server.

As well as manufacturing and issuing certificates to subscribers, the Issuing CA server also automatically publishes a Certificate Revocation List (CRL) on a frequent basis; this will automatically be published to all domain controllers (LDAP servers) and using a batch copy mechanism to a specific location on the ILM server, which is accessible to relying parties via HTTP.

ILM Server (RA)

The ILM server is deployed on Windows Server 2003 Enterprise Edition. Similar to the Issuing CA server, a significant bottleneck is related to AD lookups and hence it would benefit from placement near to a relatively quiet infrastructure DC. As with the Issuing CA server there must be a PCI-X slot in the server which would be expected to be physically deployed alongside the Issuing CA server.

The physical and logical architecture of ILM and it's interaction with infrastructure services is shown in Figure 3.

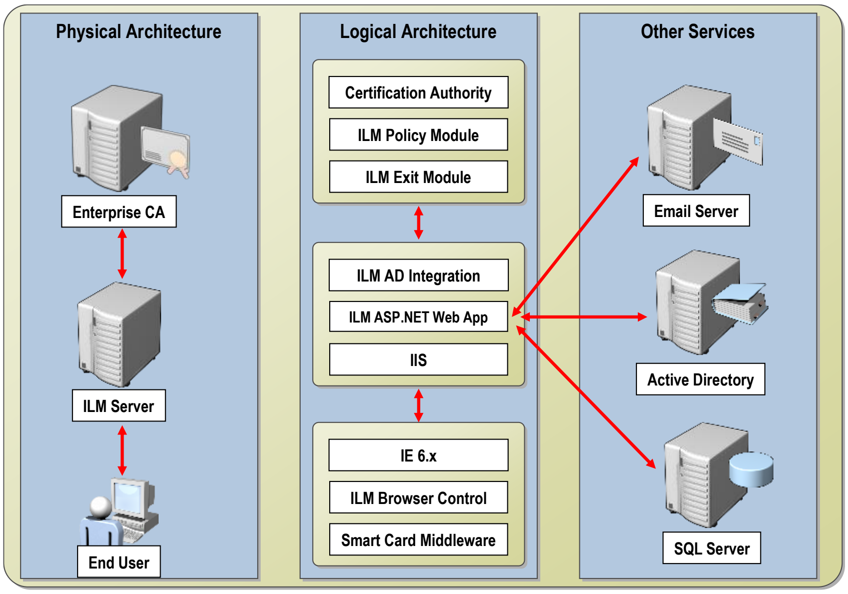

Figure 3: ILM Architecture

ILM is implemented as a .NET 2.0 application running on IIS 6.0 and therefore suitable hardware optimised for this role is considered. Operators and users interact with ILM via Internet Explorer web browsers.

All ILM configuration material is stored in Active Directory in a combination of both the configuration naming context (profile templates), domain naming context (service connection point) and Access Control Lists (ACLs) on various objects. ILM components are installed on the Issuing CA server for which it acts as an RA. User data, audit information, workflow processing status, etc. is stored in a SQL Server database.

The ILM server will be leveraged as an HTTP CRL Distribution Point (CDP) as described in the previous section, by specifying an additional virtual directory on Internet Information Services (IIS) deployed for the ILM server.

Three distinct AD user accounts enrol for high value certificates from the Issuing CA to perform certificate requests on behalf of others, perform certificate recovery on behalf of others and to encrypt certain data in the SQL Server database. Key material associated with the aforementioned certificates must be secured in an HSM and the same HSM provisos described for the CA servers apply to the ILM Server.

SQL Server

ILM relies upon SQL Server as a data store as described in the previous section; ILM 2007 supports both SQL Server 2000 SP4 and SQL Server 2005 SP1 (and above). It is proposed that due to new SQL Server instances being deployed to support ILM that SQL Server 2005 is employed as it clearly has a longer roadmap shelf-life than SQL Server 2000 but also supports better clustering / log shipping for warm standby capabilities which may be implemented (see later section on HA / DR).

The ILM database would be deployed using Windows integrated authentication rather than SQL native authentication as it generally affords easier management and reduces SQL account password attack surfaces. Certain HA ILM / SQL Server integrations are also only supported when using Windows integrated authentication.

Although ILM stores some encrypted material in the SQL Server database, there is no sensitive key material implemented at the SQL Server and hence there is no requirement for HSMs be deployed.

AD Domain Controllers

ILM requires a schema update be applied to add additional objects and extended permissions to Active Directory, this is applied to all domain controllers in the DFID AD forest.

Windows Server 2003 SP2 introduces new functionality, exclusive to smart card logon, which allows domain controllers to trust stale CRLs for a specified period of time (the *value* of this capability is described in the HA / DR section). It is recommended that SP2 be implemented on all DFID DCs prior to the 2FA project going into production.

Messaging

ILM workflows can make extensive use of messaging to support management policies for enrolment, PIN unblock, renewals, etc.; ILM determines recipient email addresses from AD users' email attribute.

ILM connects to a single SMTP server anonymously, which may be against DFID messaging policy. To overcome this limitation, it is proposed to install the SMTP service on the ILM server so that ILM can send messages to *itself*, and then the SMTP service use DNS MX records to direct messages onward to the DFID Exchange servers.

Client Side Elements

All desktop / laptops are understood to be Windows XP, which makes deployment of client side elements straightforward.

ILM has a client element which must be installed on all computers where smart card management operations are performed (strictly speaking it's not required for smart card logon); however, the ILM client would be expected to be deployed on all clients in the estate. Similarly, smart card middleware will need to be deployed to all clients and given that the cards selected for DFID will support the Microsoft Smart Card Base CSP architecture this simply a matter of implementing a Microsoft provided package (KB909520). It should be noted that this package will also need to be deployed on any server which a smart card enforced user (administrator) is performing a Remote Desktop Connection to, or performing a drive mapping, etc. The ILM client software is not required on these target servers.

Smart card readers will be required for any user attempting smart card based logon; it is understood that new laptops will possess suitable readers whereas desktop scenarios present the option of attaching USB connected smart card readers or replacement of existing keyboards with new keyboards containing an embedded smart card reader.

Suitable smart cards will be sourced with mind to the ILM smart card support roadmap, to ensure that selected smart cards can make use of future enhancements to the ILM system and Windows platform development such as Windows Vista, Windows Server 2008, etc. Smart cards will contain physical access proximity loops in addition to smart card processor chips to enable potential integration with DFID physical access solutions and potentially enable a *one-card* opportunity.

High Availability and Disaster Recovery

Multiple Issuing CAs for Availability

Windows Server 2003 Enterprise Issuing CA servers cannot be clustered and there are no supported high-availability options available.

It is possible to deploy multiple Issuing CA servers in combination with ILM; however, there are many limitations which must be fully considered before taking this approach.

Firstly, the Issuing CA server must be available to handle any revocations of certificates which it issues and secondly it must be available for retrieval of archived certificates (if this capability is employed). If the Issuing CA server is unavailable then smart cards cannot be disabled or retired; for signing certificates such as those used for smart card logon a second Issuing CA server could be configured for issuance of new certificates. This then causes complications since even though the original Issuing CA server will become available again in the future, smart cards issued from it still cannot be terminated properly since the second Issuing CA server has become the active Issuing CA server.

The main value from a second Issuing CA server is the ability to issue temporary cards, which might be a suitable option for DFID.

Issuing CA server availability is a complex discussion area and best resolved by OCG leading a workshop where all of the advantages and disadvantages are raised and then DFID can make an informed decision of the most appropriate solution.

ILM High Availability Option 1

The first option presented here is high availability in the ILM server infrastructure and a warm standby SQL server; this is shown in Figure 4.

The ILM server nodes would be considered active / active, i.e. under normal circumstances they would both be servicing inbound connections.

This option is provisionally recommended by OCG and hardware prices included in this proposal are based upon this option being selected by DFID.

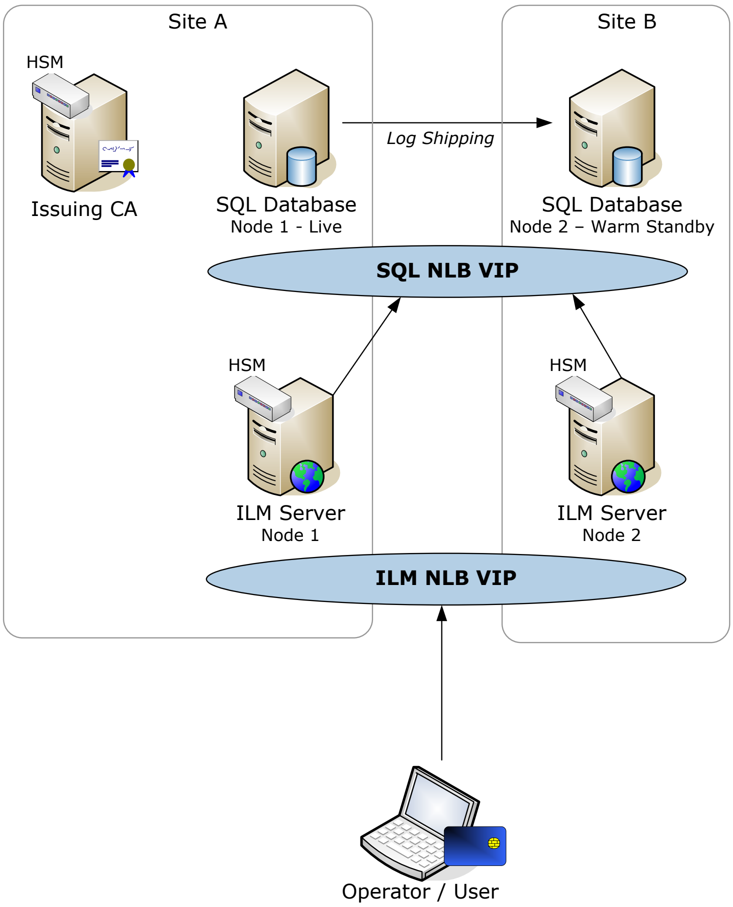

Figure 4: HA Option 1

Any clients would connect to the ILM servers via a new DNS “A” record which corresponds to a VIP established on a load balancer (this is preferably a hardware load balancer service in use in the DFID estate). The load balancer would distribute connections to either of the ILM servers and also perform a TCP/IP layer 4 poll of the ILM servers to determine whether they are available (if not they would be deselected). A similar process would be established for the HTTP based CRLs located on the ILM servers.

The connection to the SQL server would be a DNS “CName” record, which would ordinarily *reference* the SQL server in data centre site A, but would be manually changed to the SQL server in data centre site B in the event of a requirement for a warm failover. Alternatively, a *static VIP* “hosted” on the load balancer could be used; this wouldn’t be used to load balance, but could be used to manually switch a VIP from one node to the other.

Additional benefits of HA on the ILM servers is the ability to perform scheduled maintenance of nodes without taking the ILM service down.

ILM High Availability Option 2

The second option presented here is high availability in both the ILM server infrastructure and an active / passive SQL server cluster implementation as shown in Figure 5.

The advantage of HA option 2 over HA option 1 is that the SQL server element is truly highly available and able to automatically handle failures in a single SQL server instance.

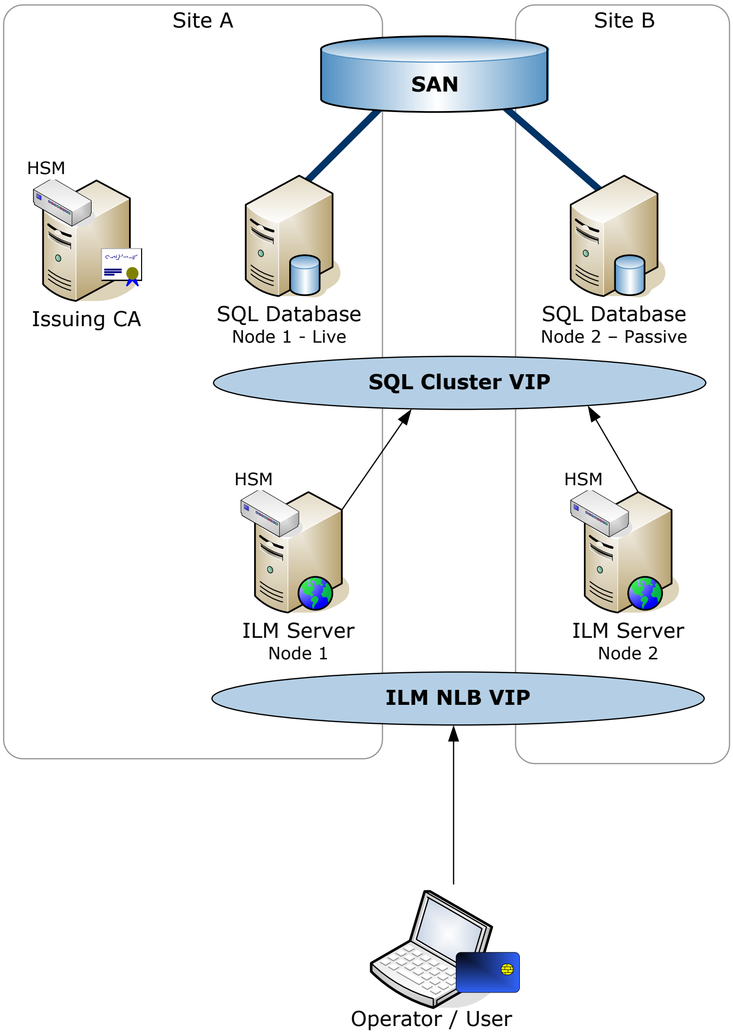

Figure 5: HA Option 2

The SQL server cluster could be implemented using:

a) Shared storage on a SAN enabling a SQL server node in each data centre site (preferred);

b) Shared storage on a *local disk array* with all nodes in a single cabinet.

General Considerations

CRL Maintenance

A critical business continuity consideration with smart card logon is CRL validity periods and the consequences of CRL expiry (stale CRLs). Ordinarily, PKI relying parties which cannot consult a time valid CRL will fail safe, e.g. a user presenting a certificate (via smart card logon) to a DC which cannot retrieve a fresh CRL will deny logon. It is important to note that CRLs generally become stale in the event that a CA server is not available to publish a fresh CRL (typically because the CA server is *broken*).

The scenario described above often results in a temptation to extend the validity period of CRLs such that the broken CA server scenario affords greater time before the CRL becomes stale, this is still susceptible to a CA server breaking just before the publication interval, hence CA servers may over-issue CRLs (publish CRLs before the scheduled publication interval). However, due to the way in which Windows relying parties cache CRLs, extending CRL validity periods often means that propagation of revocation status of newly revoked may not be apparent at relying parties for a substantial period of time, perhaps as much as the CRLs entire validity period.

The issue described above is a classic PKI dilemma between security (freshness of revoked certificates being apparent) and availability (being able to cope with a CA server which is broken and cannot publish a fresh CRL).

Stale CRL Workarounds

There are two principal methods for overcoming the problem of stale CRLs:

- Resign stale CRLs: this option requires the Issuing CA server's private key be available at another computer to, 1), take an existing stale CRL, 2), add an extension to the validity period and then, 3), re-sign it. Given that the Issuing CA server's private key will be protected by the same Security World as implemented at the ILM server this is relatively simple to achieve.
- Allow stale CRLs for smart card logon to Windows: this option is implemented as a registry setting on domain controllers whereby an additional validity period can be configured for stale CRLs.

Monitoring

Monitoring of PKI infrastructure is of paramount importance, given that many elements: CA server certificates, CRLs, etc. have finite lifetimes; compounded by the fact that some PKI infrastructure elements are naturally offline.

Pro-active monitoring is essential using scheduled monitoring tasks, complemented by GUI based tools. These scheduled tasks would ordinarily be run on the Issuing CA server and write events to the event log (and send SMTP messages if required) on the occasion of critical events happening, such as CRLs nearing expiry thresholds or CA servers being "down". Both Issuing CA server and Root CA certificate and CRL material can be monitoring in this manner.

DFID monitoring infrastructure will need to pre-actively monitor the Issuing CA server's event log and trigger actions as deemed appropriate. Trigger behaviour will need to be carefully tuned to prevent too many false positives, which often causes support staff to become de-sensitised to act on events.

Backup & Restore

All elements of the infrastructure will have system state backups taken to facilitate rapid recovery in the event of failure. However, additional measures will be taken to backup critical CA database, registry hives, key material, configuration scripts, etc. to file based locations which will be picked up in the full system backup as well as being copied to USB attached disks.

The additional backups mean there is greater flexibility (and often quicker restore capability) in scenarios where it may not necessarily be desirable or possible to perform a full system restore. Experience has shown that Windows Server 2003 Enterprise Issuing CA servers can sometimes pose particular challenges for recovery due to the fact that they can never be disjoined from the AD domain. Very carefully developed and tested recovery procedures are required for Issuing CA servers.

Disaster Recovery

Disaster recovery is such a wide topic with so many cost / benefit arguments that it is not deemed practical to address in this proposal given the lack of any firm DR requirements. As previously stated, it would be beneficial to hold a workshop where DR (and indeed HA) scenarios are fully played out to enable a more *focussed* HA / DR proposal to be prepared.

Project Approach

OCG proposes the following general project approach to meet DFID's requirements for the two factor authentication project.

Stage 1 – Proof of Concept

- Implement a Proof of Concept (POC) environment incorporating the functional elements of the solution, without consideration to security aspects such as HSMs nor HA / DR; the environment to be provisioned on virtualised guest operating systems
- The POC will enable DFID staff to become familiar with some of the new technology / processes introduced by the 2FA project
- OCG to provide design for POC consolidation and support for implementation
- OCG will lead a workshop to explore management policy options for all scenarios and consider different smart card enforcement strategies
- OCG to author high-level design document

The POC would remain in place throughout the duration of the project to support inevitable review and refinement of management policies and workflows, etc.; this will allow the detailed design, engineering and build out of infrastructure into test and production to be executed in parallel with policy refinement. Experience on similar projects has shown detailed design and engineering often gets *bogged down* by inevitable ongoing dialogue and changes to workflow policy.

Stage 2 – Design and Engineering

- Production of detailed design documentation and supporting engineering (such as scripts)
- Development of detailed installation guides to such a standard that they can be used in implementation ceremonies satisfying any DFID PKI accreditation guidelines
- Development of recovery guides for all aspects of the solution, e.g. to cater for a *broken* HSM, CA server, ILM server, SQL Server, etc.
- Development of any disaster mitigating elements, such as mass disabling of smart card enforcement, re-signing of stale CRLs, etc.
- Testing of aforementioned scripts, operating guides and disaster mitigating elements
- Engagement of all necessary impacted IT design / support teams for knowledge sharing and awareness; to include at least the following areas: Wintel / AD, database administration, server backup and restore, messaging, network and security, disaster recovery, monitoring, key custodians
- Training of staff identified to support the 2FA solution, incorporating not just infrastructure support but also helpdesk operators, workflow approvers, etc.

Hardware procured for production purposes would be diverted for implementation into the development and test environment to support the activities described above; once completed satisfactorily, the equipment would be decommissioned ready for implementation into production.

Stage 3 – Production Implementation

It is understood that a pilot will be first run in production to a small user community prior to being rolled out across the entire estate.

- Implement an nCipher HSM at the server identified to be the offline Root CA server and establish a DFID Security World at that unit; install Microsoft Root CA services
- Implement an nCipher HSM at the server identified to be the Issuing CA server and incorporate it into the DFID Security World; install Microsoft Issuing CA services and certify it by the DFID Root CA server
- Implement SQL Server in readiness for ILM installation
- Create all necessary service and agent accounts for ILM, as well as all group accounts to support ILM workflows, and certificate templates
- Implement nCipher HSMs at the servers identified to be the ILM Servers and incorporate them into the DFID Security World; enrol requisite agent accounts for certificates at the ILM servers (with keys protected by the HSMs)
- Update the AD schema to include new objects and extended permissions required by ILM
- Install ILM onto the servers and perform all necessary post-install configuration; make ILM servers available as hosts for the Certificate Revocation Lists (CRLs) published by the CA servers
- Execute all necessary integration with messaging, network, backup infrastructure, etc.

Statement of Work

Task	Consultant (days)	Notes
Proof of Concept Stage		
POC Design, Implementation and Workshop Support	3	Production of a consolidated design suitable for implementation on a single virtual server; support in implementing the POC solution and leadership of workflow workshops
Solution High Level Design	5	Production of high level design document, suitable for DFID security accreditor *validation*
Design and Engineering Stage		

Task	Consultant (days)	Notes
Solution Low Level Design and Engineering	37	Production of PKI design: - nCipher Security World - Root CA server & HSM - Issuing CA server & HSM - CRL publication design - Smart card logon enforcement strategy - Disaster mitigation Production of ILM design: - HA ILM servers - SQL servers - Workflow design - HSM - Printing - Client elements - Disaster mitigation Documentation - Implementation ceremonies - Operating and recovery guides Integration dialogue - AD, monitoring, network, backup, messaging, security, database , etc.
Integration Testing	3	End to end solution testing, followed by equipment decommissioning
Training	2	Knowledge transfer to support teams (to complement external training)
Production Stage		
Production Deployment	3	Presence at implementation ceremonies
Pilot Support	1	Provide assistance and support during the pilot stage
Total	54	