Dual Factor Authentication Project

Certificate Lifecycle Manager (CLM) Design

31st December, 1999

Change History

Revised Date	Version	Author	Nature of Change
31.12.1999	1.0	David Wozny	Draft for Review

Distribution List

Name	Role	Representing
David Wozny	Author	XYZ
AN Other	Infrastructure Architect	ABC

References

Ref.	Document Name	Author
1	ABC DFA Solution High Level Design	D. Wozny

Abbreviations

Term	Definition
AD	Active Directory
CA	Certification Authority
CAPI	(Microsoft) Cryptographic Application Programming Interface
CDP	CRL Distribution Point
CP	Certificate Policy
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DBMS	Database Management System
DR	Disaster Recovery
HSM	Hardware Security Module
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
VIP	Virtual TCP/IP Address

Table of Contents

1. Introduction

1.1 Background

The Dual Factor Authentication Project is being implemented in the ABC estate to support strong authentication to Windows for ABC users, centred on smart cards issued with authentication certificates from a new Microsoft Public Key Infrastructure (PKI) instantiation and Microsoft Certificate Lifecycle Management (CLM).

1.2 Objective

This document describes an architectural overview of the new CLM design, which is a sub-system of the Dual Factor Authentication Project system. This document describes both the individual components which constitute the CLM sub-system and the interaction with other elements of the overall Dual Factor Authentication Project *system*.

1.3 Scope Elements

The following elements are within the scope of this document:

- CLM server design and specification
- Hardware Security Module (HSM) design and specification
- Certificate Revocation List (CRL) publication, availability and monitoring
- Security aspects of the design

The following elements are outside the scope of this document:

- CLM workflow definition (see Reference [3])
- Detailed information regarding the implementation of a clustered SQL service

1.4 Scope Statement

This solution is provided solely for the issuance of certificates to end entities within the ABC organisation, specifically to users in the `ABC.gov.uk` Active Directory forest.

The solution is provided solely for management of smart cards and certificates for the DFA project, although it is designed in such a way that it can be leveraged in the future for other projects which incorporate certificates / smart cards.

1.5 None

The following design constraints are known:

- None

2 CLM Sub-System Architecture

2.1 Introduction

The CLM sub-system provides two principal capabilities:

- A registration authority: providing an interface to perform workflows supporting business rules for management policies for the lifecycle of smart cards and certificates
- A smart card management system: providing smart card management operations and abstracting operators and users from the underlying PKI

In addition, the CLM sub-system provides an HTTP based location for hosting CA certificates and revocation lists used by certain relying parties when building certificate chains and performing revocation checks.

Figure 1 illustrates the CLM sub-system components and the relationship with *infrastructure elements*.

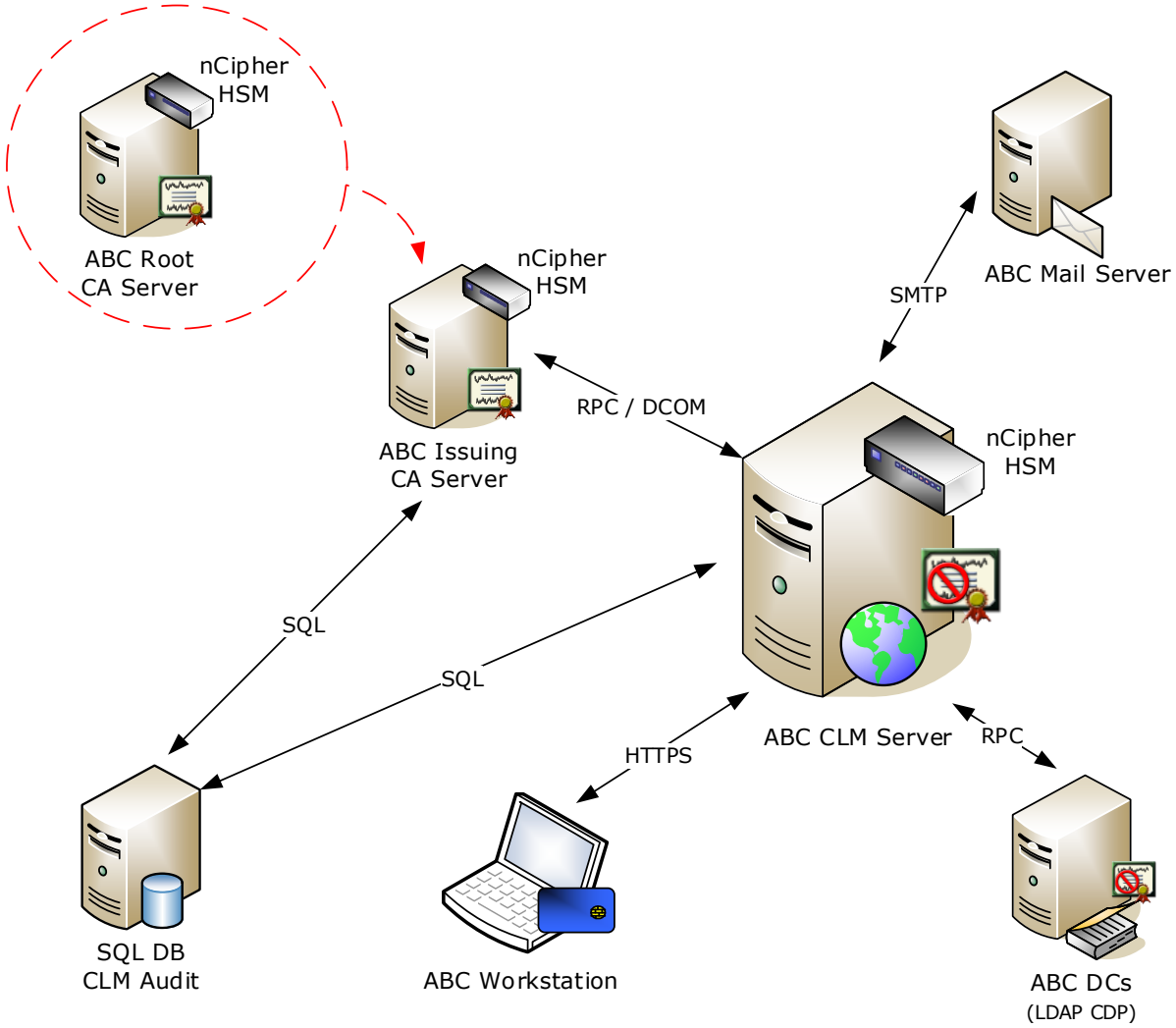

Figure 1: CLM Sub-System Logical Overview

The CLM sub-system is essentially constituted by the following principal components:

- CLM servers
- CLM modules on the ABC Issuing CA Server
- Hardware Security Modules (HSMs)

- SQL Server database
- CLM client software

The CLM sub-system interacts with the following infrastructure elements:

- ABC Active Directory (AD) Domain Controllers (DCs)
- ABC messaging servers
- Network load balancing services
- Smart cards

2.2 CLM Servers

The "CLM server" is a .Net application running the CLM web portal on Internet Information Services, clients connect to CLM using Internet Explorer web browser over HTTPS. The CLM web site hosts both an operator portal and user self-service portal – the same URL is used for both portals – AD group membership dictates which portal is presented to a user when accessing CLM.

The CLM servers are essentially stateless, with configuration settings generally being held in AD by means of the following:

- A service connection point
- Profile and certificate templates
- AD extended permissions applied on a number of AD objects, as detailed in Reference [2]

The service connection point, profile templates and AD extended permissions are implemented by means of an AD schema update.

The CLM servers make use of SQL server for storing audit information of all registration processes and actions as well as tracking the stages of workflow execution.

2.3 CLM Modules

CLM Exit and Policy modules are installed on the Enterprise CA server. The policy module determines whether a certificate request should be automatically approved, denied or marked as pending; the exit module performs post-processing such as updating certificate records in the CLM database.

2.4 Hardware Security Modules

As part of the commissioning of the CLM web portal, there are three "CLM agent accounts" which are enrolled for certificates, these include the capability to perform key recovery and act as an enrolment agent. Compromise of the private key material associated with these agent accounts would enable a hostile party to fraudulently issue certificates on behalf of users and to recover decryption key material.

To mitigate the risk of the above, nCipher Hardware Security Modules are installed on the CLM servers to protect the private key material of the CLM agent accounts.

2.5 SQL Server Database

To support the DFA project, a new SQL Server cluster based upon SQL Server 2005 SP2 and utilizing the ABC SAN for shared storage is to be implemented.

Both the CLM web portal and the CLM exit modules on the ABC Issuing CA Server will connect to the SQL cluster via its *virtual server (host) name*.

Although precise metrics are difficult to establish for sizing of the CLM database, empirical data has shown that a CLM instantiation with 200,000 records in the certificates table resulted in a database approximately 750MB in size. The database size requested of the SQL DBA team on the clustered SQL service is 1000MB, which is significantly greater than expected utilization.

Further information on the design of the clustered SQL service is available in Reference [4].

3 CLM Servers

3.1 Availability

Two CLM servers are implemented to provide high availability; this is illustrated in Figure 2. A DNS host record (`ABC.gov.uk`) is implemented to host a virtual TCP/IP address (VIP) for the DFA CLM service. The VIP corresponds to a listening address on a network appliance based load balancing capability hosted on Cisco Content Switches – these load balancers are already implemented within the ABC estate for other purposes.

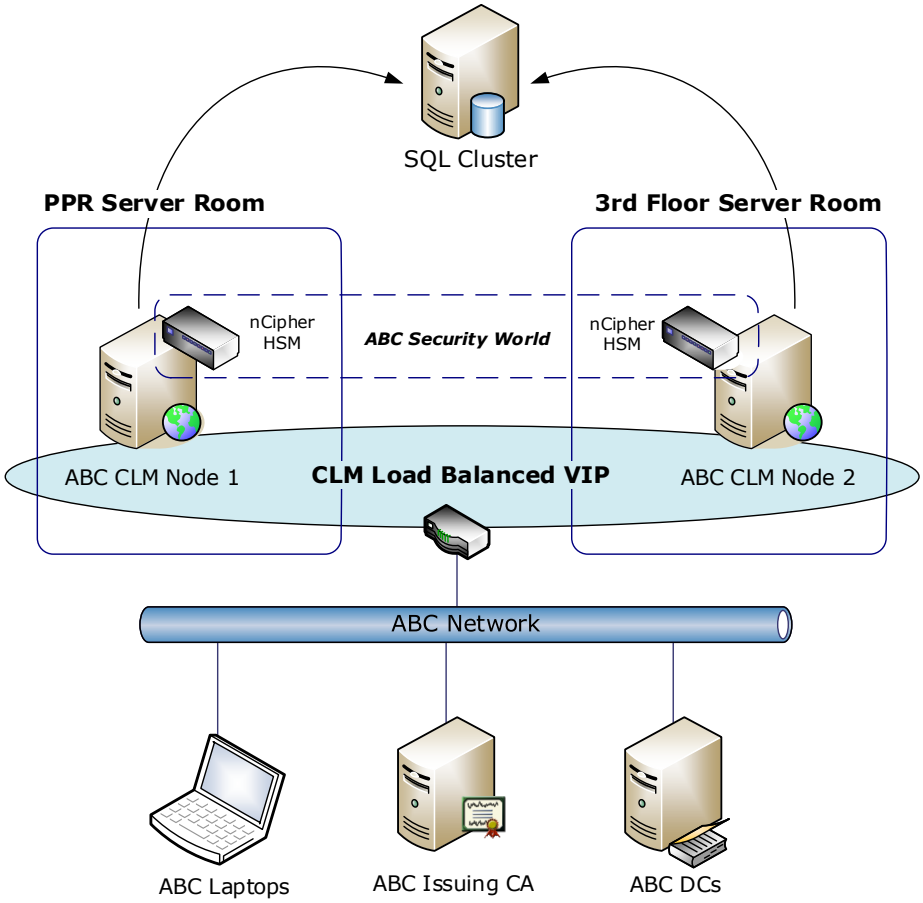

Figure 2: CLM Physical Design

3.1.1 DNS Records

The URL used by operators and users to connect to the CLM web portal is `https://ABC/clm`. The DNS host record, `ABC.gov.uk` is implemented in the ABC AD DNS.

A second DNS host record is implemented, `PKI.ABC.gov.uk`, which is employed as part of the AIA and CDP extensions, often referred to as Issuing Distribution Points (IDPs), in all certificates issued by the ABC Issuing CA1. These extensions enable relying parties to retrieve CA certificates and CRLs from an IIS virtual directory hosted on both the CLM servers, the URL is `http://PKI.ABC.gov.uk/idp`.

Although it would be possible to use the same VIP for both the CLM and IDP requirements, it is practical to make them unique to enable potential service separation possible in the future.

3.2 CLM Agent Accounts

3.2.1 Introduction

Implementation of CLM requires a number of agent accounts be implemented, as summarized in Table 1.

User Account Name	Description
SVC_CLM-Agent	*CLM Agent* Protects communication between the CLM server and the CA; revokes certificates and encrypts data collection information
SVC_CLM-Auth-Agent	*CLM Authorisation Agent* Determines access rights and privileges of users
SVC_CLM-CA-Manager	*CLM CA Manager* Performs CA management activities such as the publication of CRLs; management activities on the CA
SVC_CLM-EA	*CLM Enrolment Agent* Requests certificates on behalf of another account
SVC_CLM-KRA	*CLM Key Recovery Agent* Recovers private keys from blobs recovered by the CLM agent
SVC_CLM-WebPool	*CLM Web Pool* Runs the CLM web application in IIS; the identity for the IIS application pool
SVC_CLM-Service	*CLM Service* Runs the CLM service, which runs automated tasks such as creating renewal requests for certificates entering their renewal threshold

Table 1: CLM Agents

Three of the agent accounts enroll for certificates (and corresponding private keys) which in the possession of a hostile party could be employed to compromise *the system*. It is therefore necessary to implement hardware security modules to protect this key material, as described in Chapter 4.

3.3 Service Connection Point (SCP)

3.3.1 Introduction

The Active Directory schema defines a Service Connection Point (SCP) object class to make it easy for a service to publish service-specific data in the directory. CLM clients use SCP data to locate, connect to and authenticate an instance of the service. The CLM SCP is created during the configuration process and is used to determine who can access the CLM portals and which portal, "operator" or "user", they can access; this access is controlled through permissions set on the SCP object.

3.3.2 DFA Project

A single SCP is defined for the DFA project, `DFA-CLM`, both CLM nodes use this same SCP which is essential otherwise they will essentially be logically distinct entities.

The DFA SCP is illustrated in Figure 3.

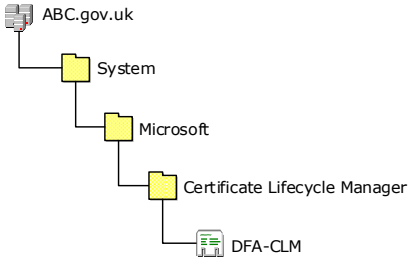

Figure 3: CLM Service Connection Point

3.4 Profile Templates

3.4.1 Introduction

The profile template is the fundamental configuration model employed by CLM, the profile template object type is implemented in the configuration naming context of Active Directory by the CLM schema update.

The profile template provides a single administrative object that combines the following:

- Certificate templates
- Profile details
- Management policies for workflow definition

A certificate template defines the characteristics which will be enforced in any certificate requested which is based upon that certificate template; one or more certificate templates can be implemented within a profile template.

Profile details provide information such as whether the certificates are stored in software (in the user's profile) or on a physical device such as a smart card. They also designate which CA issues certificates for the profile and which certificate templates are included in the profile template.

The management policies define the workflows used for certificate management within the profile template. The management policies also determine who performs specific, workflow-management tasks and provides certificate lifecycle management details within the profile template.

3.4.2 Profile Template Design

The DFA solution incorporates two profile templates, one for UK / India users and one for all overseas users. The majority of settings in the two profile templates are identical, with the exception of permissioning within the workflows. Given that UK / India users have local helpdesk staff in their region it is practical for them to share a single profile template, whereas all overseas users adhere to the Overseas administrators model and therefore a single profile template satisfies their requirements.

The two profile templates implemented for the DFA project are illustrated in Figure 4.

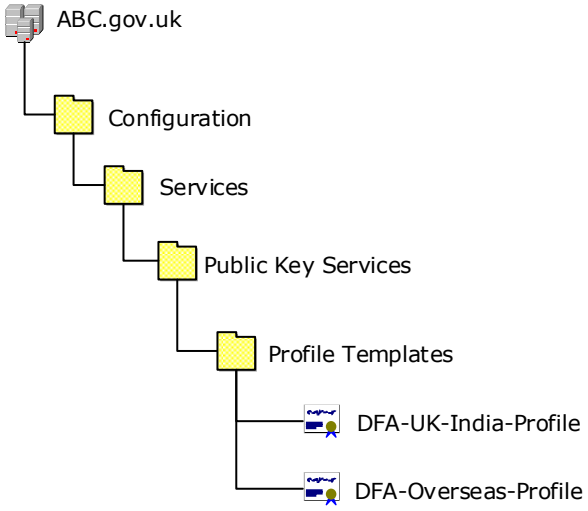

Figure 4: DFA Profile Templates

A single authentication certificate template is designated in the profile template, since users will only be issued certificates for authentication purposes, i.e. there is no requirement presently for signing or encryption certificates.

A number of management policies are defined, as follows:

- **Enroll**

  The initial enrolment of smart cards is a two step process; the request creation will always be performed by a member of the helpdesk. Card personalisation (the injection of certificates onto the smart card) will be performed for UK / India users by the helpdesk, whereas Overseas users will have their card personalised by the Overseas admin.

- **Online Unblock**

  The online unblock management policy is employed when a user wishes to do an operator assisted smart card PIN unblock, i.e. the user visits the helpdesk / OSAdmin to execute the unblock.

- **Offline Unblock**

The offline unblock management policy is used for situations where a user wants to perform a smart card PIN unblock when they are away from the office; the kiosk account is used to log on to the computer, from whence an offline unblock challenge / response process can be initiated.

- **Renew**

  Certificates have a finite lifetime, for the DFA project this is five years. CLM will automatically send users a renewal email containing a CLM URL and one-time password six weeks prior to their certificate expiry. The email enables users to perform certificate renewal without any operator assistance.

- **Replace**

  If a smart card is broken or stolen, the replacement management policy facilitates issuance of a new smart card which is linked (for audit purposes) to the prior smart card. As part of the replacement process the certificate on the original smart card is revoked.

- **Temporary Cards**

  The temporary card management policy enables issuance of smart cards with a short lifetime (four days); temporary cards can only be issued to users with existing primary smart cards. This management policy is typically to be used in scenarios where a user has forgotten their smart card / left it at home.

- **Disable**

  If a user reports their smart card stolen / lost then the disable management policy immediately revokes the certificates on their smart card. This management policy would typically be executed when a user is not able to come to the office for a replacement card for a period of time. This management policy is also executed as part of housekeeping tasks identifying active user accounts for staff that have left ABC, etc.

- **Retire**

  The retire management policy is used to "reformat" primary smart cards handed in by leavers / temporary smart cards.

The business rules and procedures for each of these management policies are defined in Reference [3]; the precise settings for each management policy is defined in Reference [2].

3.5 CLM Permissioning

Permissions are set on a total of five places for a CLM management policy (workflow) to properly execute, as listed below:

- Certificate Template Object (A)
- Profile Template Object (B)
- Profile Template Management Policy (C)
- Service Connection Point Object (D)
- AD Subscriber Group Object (E)

The permission locations are illustrated in Figure 5. Detailed information on the permissioning employed for the DFA project is included in Reference [2].

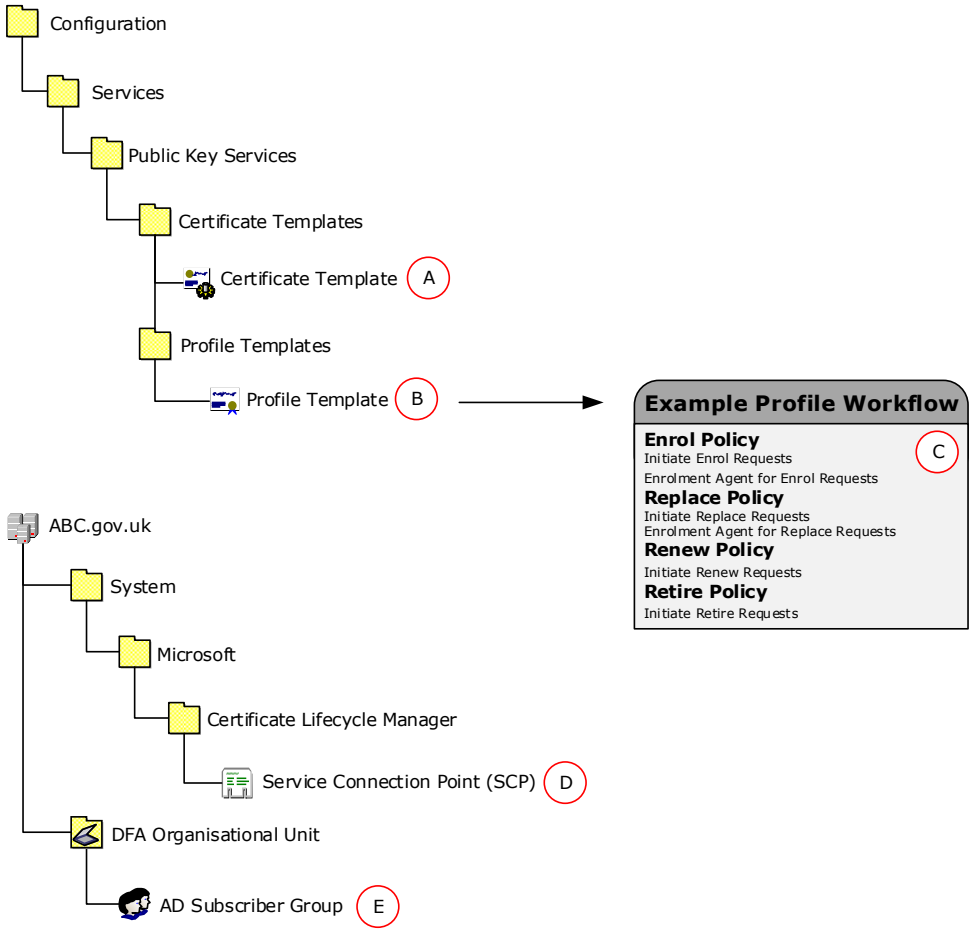

Figure 5: CLM Permissions Model

3.6 Security Groups

3.6.1.1 Introduction

Permissions can only be assigned to Global and Universal security groups, Domain Local groups are not enumerated by CLM; permissions can be directly assigned to user accounts, though this is poor practice and avoided for ABC.

Since Active Directory typically relies upon Organisational Units as the centre of its delegation model, a new security group structure is developed to ensure suitable administrative delegation for CLM.

3.6.1.2 DFA

A permissioning model is implemented whereby permissions are generally applied to aggregator groups, expect where specific permissions are necessary. It is generally the norm that the specific permissions only apply to OSAdmins for a specific country on users in their specific country.

The nesting of DFA users into security groups is illustrated in Figure 6.

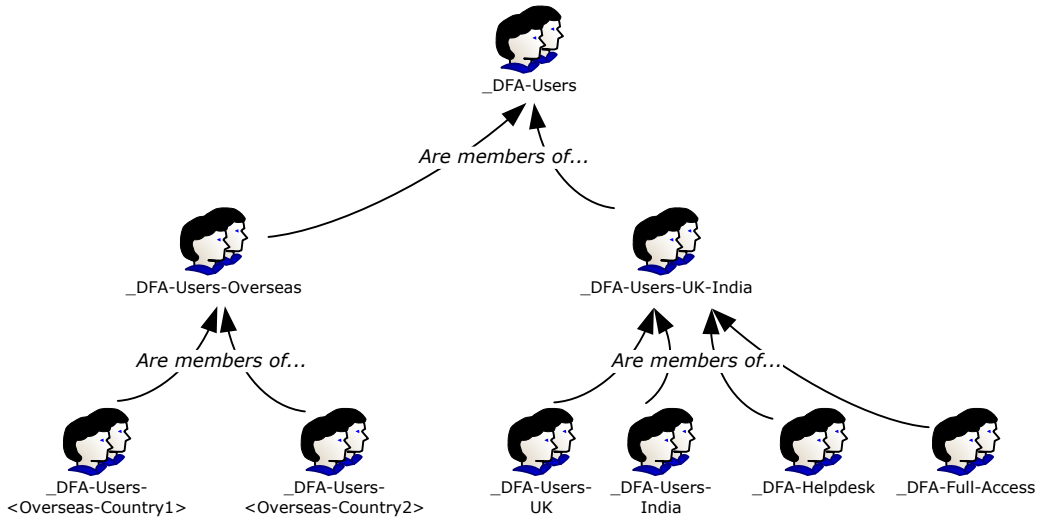

Figure 6: User Group Nesting

Overseas Administrators are similarly nested into *aggregator* security groups, is illustrated below in Figure 7.

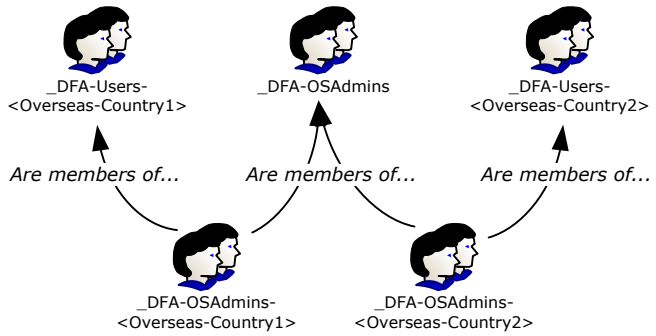

Figure 7: OSAdmin Group Nesting

The illustrations here do not provide proper context, security group definitions and memberships are addressed in greater detail in their proper context in Reference [2].

4 Hardware Security Modules

4.1 Introduction

The following CLM agent accounts enroll for certificates:

- `svc_clm-agent`
- `svc_clm-ea`
- `svc_clm-kra`

The private keys associated with these certificates are protected by HSMs.

4.2 HSM Type and Commissioning

nCipher nShield PCI HSMs are installed in both CLM servers, the servers are configured in the same DFA security world as the ABC Master Root CA and ABC Issuing CA1. As a consequence, the same set of administrator cards are used to commission the HSM and perform future administration.

4.3 Agent Key Protection

The HSMs are configured with module only protection, meaning that Operator Card Set (OCS) is not required to authorise access to private key material. Given that the CLM servers are always online, it is not appropriate to have this additional layer of security control.

It is not possible for a hostile party to execute a compromise of agent key material using purely *logical* attacks, i.e. by logging on with high entitlement accounts or retrieving material from backup tapes. Any attack requires physical possession of the HSM installed in the CLM servers; suitable controls are in effect in the ABC estate to make that likelihood extremely remote.

4.4 Consideration for CLM Commissioning

Given that both CLM servers require access to the exact same key material, and that export of key material is not possible when keys are protected by HSMs a special procedure is required to transport key material between the two CLM servers.

By ensuring that key material is only ever transferred whilst encrypted under the *governance* of the DFA security world, the key material is never exposed in the clear and therefore can be exchanged between the two CLM servers without ever being at the risk of compromise.

5 CLM Exit Module

5.1 Introduction

CLM Exit and Policy modules are installed on the ABC Issuing CA server. The policy module determines whether a certificate request should be automatically approved, denied or marked as pending; the exit module performs post-processing such as updating certificate records in the CLM database.

5.2 Configuration

5.2.1 Exit Module

The CLM Exit module is configured with a connection string specifying how to communicate with the SQL server, including which database to access and the account used to establish the communication.

The database created on the SQL server for CLM is indeed named CLM, this is specified in the connection string.

The connection string specifies integrated (SSPI) authentication (the ABC Issuing CA server's computer account is used to authenticate to the SQL database); as a consequence, the computer account is explicitly granted necessary entitlement to the CLM database as part of the commissioning process. Finally, the data source is specified.

The connection string is shown below:

```
Connect Timeout=15;Persist Security Info=True;Integrated Security=sspi;Initial
Catalog=CLM;Data Source=eks096.abc.gov.uk;
```

The data source is the virtual server name of the clustered SQL service.

In addition, a Service Principal Name (SPN) is established for the SQL Service (`MSSQLSvc`) for this SQL virtual server, for the service account used to start the SQL service (`svc_sqlsa`).

5.2.2 Policy Module

No specific configuration is made of the default CLM policy module, such that the exit module allows processing of both CLM initiated and non-CLM initiated certificate requests.

It should be noted that future extension of CLM may include adding custom policy modules to enable management of certificates issued outside of CLM (e.g. autoenrolment) to enable them to be managed by CLM.

6 Smart Cards

6.1 Introduction

CLM supports management of smart cards based upon the *traditional* PKCS#11 standard for managing cryptographic tokens; this standard often requires a monolithic middleware stack to be provided by the smart card supplier be deployed on all computers where the smart card is to be used. However, this PKCS#11 support in CLM is limited to a specific set of smart cards from a short list of manufacturers; in addition, Microsoft has stated that it will not extend the list from its current inclusions.

Microsoft has introduced a new standard for managing cryptographic tokens on Microsoft platforms, called the Base CryptoGraphic Service Provider (CSP) model. This approach brings the majority of cryptographic functions which would traditionally be implemented in middleware, into the operating system. In an approach roughly analogous to the Windows printer driver model, the smart card provider only needs to produce a mini-driver which handles the native calls required of the smart card.

Some of the cryptographic functionality available in CLM, and Windows platforms relies upon smart cards based upon the Base CSP; an example of such being offline unblock functionality.

6.2 Smart Card Selection

ABC has chosen to adopt a smart card utilizing the Base CSP model, the GemAlto .Net smart card. Smart cards procured by ABC will also incorporate a HID proximity loop to enable the combination of physical and logical access using a single card.

6.3 Smart Card Software

In Windows XP the Smart Card Base CSP is implemented as a hotfix on Windows XP (it is bundled into SP3) and Windows Server 2003; it is native on both Windows VISTA and Windows Server 2008.

In combination with the smart card base CSP middleware is the mini-driver – this is specific to the particular smart card selected. The mini-driver for the GemAlto .Net cards selected for ABC DFA project is actually incorporated in the Base CSP hotfix package – this is a special case as the .Net smart card was the first to be qualified by Microsoft. All smart cards which conform to the Base CSP model must be qualified by Microsoft, the mini-drivers subsequently being available from Windows update.

6.4 Admin Key Diversification

Whereas PKCS#11 smart cards are generally managed through knowledge of an admin PIN, smart cards based upon the Base CSP use the concept of an Admin key. The default admin key of a GemAlto .Net smart card is all zeroes; this is *well known* and therefore a potential attack surface. Knowledge of the admin key enables a PIN to easily be reset by an attacker in possession of a stolen smart card and hence issuing smart cards from CLM with this admin key is not safe. CLM is therefore configured such that the admin key is diversified during the issuance process.

Smart cards which have their admin keys diversified are only manageable from the CLM system which maintains the diversified value of the admin key. Any other *system*, without knowledge of the diversified admin key, cannot manage the smart card (e.g. perform a PIN unblock).

6.5 PIN Policy

ABC security policy mandates that a four digit numeric only PIN should be implemented. Additionally, more than two repeating identical characters are disallowed (111 is illegal), as are numeric sequences longer than two characters (123 is illegal).

PIN policy is enforced by registry settings applied at the computer where a PIN set / change is executed. The registry settings are configured by group policy by implementing an administrative template (ADM) file containing the requisite settings.