Document Control	
Title	PKI Design
Description	ABC PKI Design
Version	0.3
Issue Status	Draft
Author	David Wozny
Customer Organisation	ABC

Change Record

Issue No.	Date	Issued By	Reason for Issue
0.1	31/12/1999	David Wozny	First draft

Distribution List

Copy	Issued To	Position
1	AN Other	ABC Head of Compliance, PKI PMA Chair

References

ID	Description	Document
01	Requirements	
02	Promulgation Design	
03	IL4 AD Design	
04	IL3 AD Design	
05	Certificate Profiles	
06	Root CA DR	
07	IL4 Virtualisation	
08	IL4 SAN	
09	Internet CDP	
10	IL4 Auditing	
11	IL4 Platform Backup	
12	IL4 Patching	
13	IL3 Virtualisation	
14	IL3 SCOM	
15	IL3 Platform Backup	
16	IL3 Patching	
17	Code Signing	

Table of Contents

1. Management Summary

1.1. Background

One of the main drivers of the ABC Central Back End (CBE) project is providing secure access to systems that require HMG IA Business Impact Level 4 (IL4) authentication credentials. *National applications* such as LMN and *ABC local applications* such as JKL demand IL4 authentication credentials. The Home Office Prang ICT Directorate (PID) via the IAM Strategic Management Authority (SMA) and the ABC via the Policy Management Authority (PMA) both dictate that a compliant IL4 authentication credential requires using a digital certificate stored on a PIN protected cryptographic module (smart card). Digital certificates require a Public Key Infrastructure (PKI), which forms the basis for the design content of this document.

The ABC's PKI requirement goes beyond the *IL4 user authentication* use cases referenced above as it also encompasses high assurance digital certificate fulfilment to subscribing devices (such as web servers). Furthermore, there are requirements for *mass enrolment* of digital certificates to devices deployed in the IL3 network (such as routers) where a less demanding registration process is demanded (i.e. low assurance).

1.2. Objective

This document describes the design of the target PKI deployed for ABC commonly referred to as the "Microsoft PKI". As well as the Certification Authority (CA) capability, the document also describes existing PKI services, such as Hardware Security Modules (HSMs), where they are leveraged by the Microsoft PKI. The document does not describe further any of the wider PKI known as the "tPKI" or any migration activities involved in attaining the target PKI.

This document describes both the individual components which constitute the PKI system and its interaction with other sub-systems such as the Intercede MyID Smart Card Management System and Active Directory (AD) infrastructure.

1.3. Scope

1.3.1. In Scope

- Ø Target PKI system architecture
- Ø CA server design and specification
- Ø HSM design and specification
- Ø Revocation status design and specification

1.3.2. Out of Scope

- Ø tPKI system architecture
- Ø Governance and policy
- Ø Smart card management system
- Ø Network segregation / separation

1.4. Requirements

The fundamental requirements of the target PKI system are specified in Reference [01].

2. PKI Introduction

2.1. Overview

The PKI provides the capability for issuance x.509 digital certificates to subscribing entities. A digital certificate issued by a trusted CA asserts a logical binding between a subject (typically a user or device) and a public key in a cryptographically secure *envelope*.

A two-tier approach is implemented for the ABC PKI, comprising:

- Tier One: Root CA (offline)
- Tier Two: Issuing CAs (online)

Whilst ensuring that a secure, available, robust and flexible PKI is implemented for ABC, a prime design goal was to not engineer in complexity anywhere that it is not strictly necessary. This design philosophy is reflected in much of the design documented herewith.

Figure 1 illustrates the ABC PKI components and their relationship with infrastructure elements:

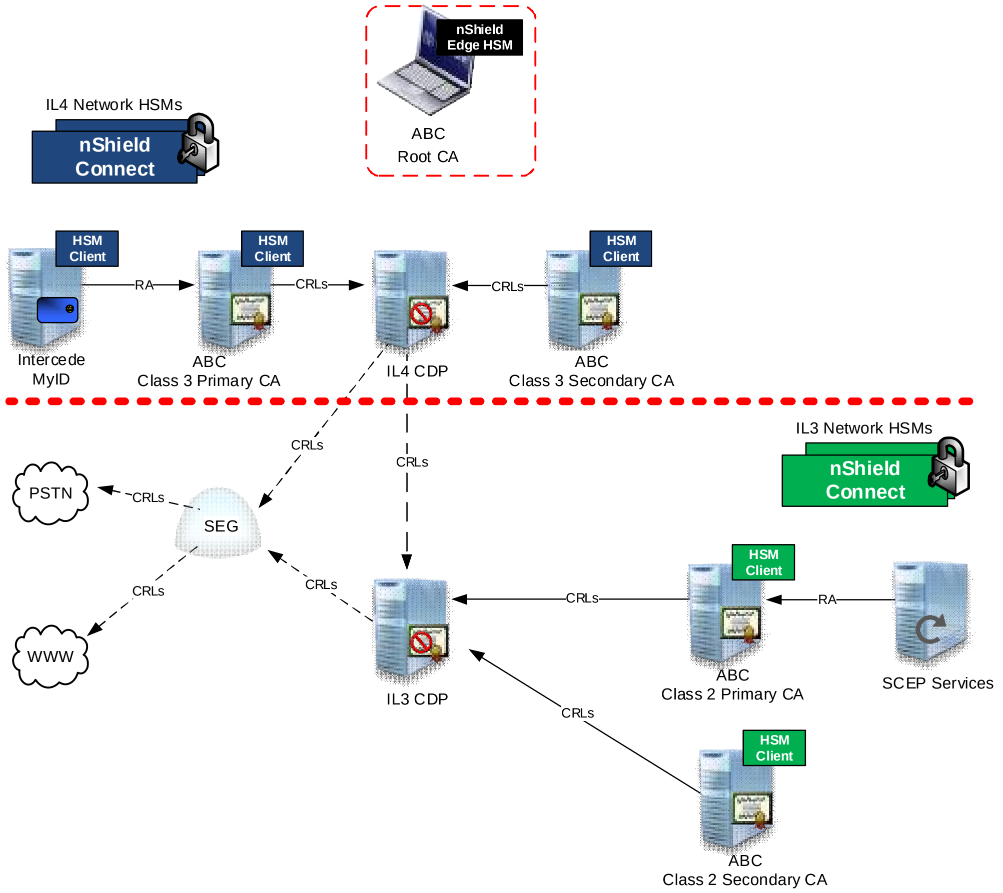

Figure 1: ABC PKI Overview

The PKI essentially comprises the following principal elements:

- Root CA (standalone)
- Issuing (Enterprise) CAs in IL4 and IL3 networks

- Ø Certificate Revocation List (CRL) Publication and Distribution
- Ø Hardware Security Modules (HSMs)
- Ø SCEP[1] Services

The PKI principally interacts with the following infrastructure elements:

- Ø Intercede MyID Smart Card Management System (SCMS)
- Ø ABC Active Directory Domain Controllers

2.2. PKI Core Elements

2.2.1. Trust Model

2.2.1.1. Introduction

The ABC PKI two-tier architecture is illustrated in Figure 2.

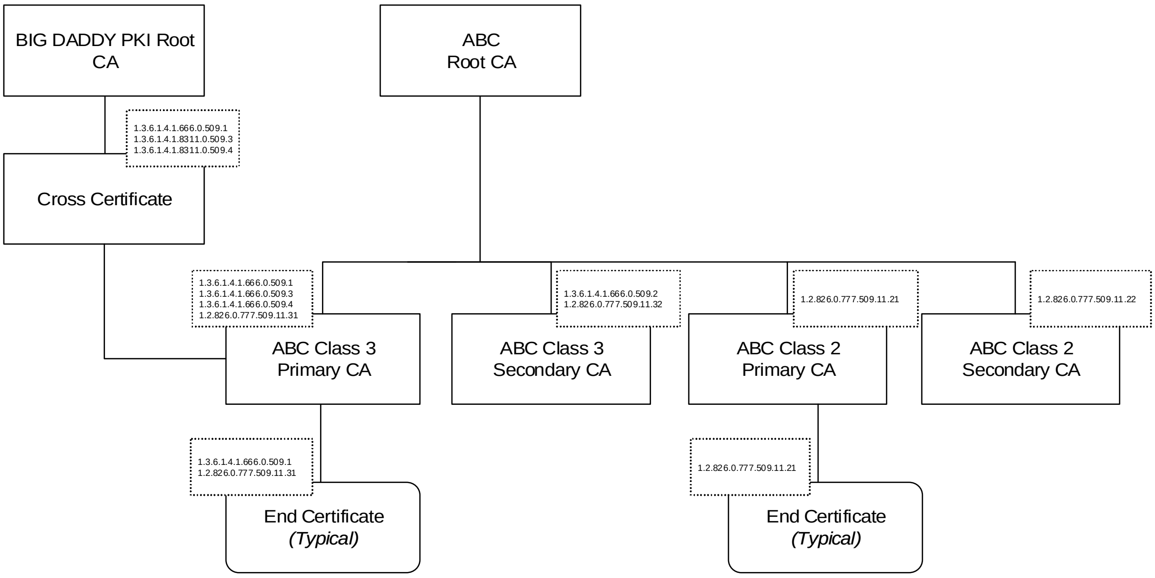

Figure 2: ABC Two-Tier PKI Hierarchy

The two-tier approach provides ABC with the requisite trust anchor of an offline Root CA, while enabling the following Issuing CA capability:

- Ø A high assurance CA implementing PID Certificate Policies for authentication and encryption - deployed in the ABC IL4 network (Class 3 Primary CA)
- Ø A high assurance CA implementing PID Certificate Policies for digital signature - also deployed in the ABC IL4 network (Class 3 Secondary CA)
- Ø A low assurance CA solely implementing ABC Certificate Policies initially for the RTC programme's WAN encryption requirement - deployed in the IL3 network (Class 2 Primary CA)

[1] Simple Certificate Enrolment Protocol (SCEP)

- A low assurance CA solely implementing ABC Certificate Policies initially for the Mobility programme's authentication requirement - deployed in the IL3 network (Class 2 Secondary CA)

2.2.1.2. Distinction between the Class 3 and Class 2 CAs

The Class 3 CAs are deployed for issuing certificates based on a high assurance registration policy – this can be to either IL4 or IL3 entities. With Class 3 user certificates there is typically a requirement for a face-to-face registration exercise and presentation of identity information (e.g. passport) before an issuance officer issues the certificate (on a smart card) on behalf of the subscriber. With Class 3 device certificates there must be a sponsor identified for the certificate and a prescribed registration process followed (using the eCE SharePoint site).

The Class 2 CAs are implemented for mass enrolment type scenarios where the registration process is significantly lesser than that required at the Class 3 CAs. The initial deployment of Class 2 CAs are to support the RTC WAN encryption and Mobility programs; this isn't to infer that projects will have "their own" CAs[2] and these two CAs will be leveraged for other certificate requirements as and when they surface.

2.2.1.3. Cross Certification

Further to initial commissioning, certificates issued by the ABC Root CA (and subordinates) are solely trusted within the ABC estate. Subsequent to a cross certification exercise with the PSP PKI, certificates issued by the ABC PKI are recognised by applications hosted on the PXD JAM Central Services platform. Constraints are placed on the cross certification process such that only certificates issued by the ABC PKI asserting PXD certificate policies are deemed trustworthy by the Central Services platform.

The *linkage* shown in Figure 2 between the PSP PKI (PSP) Root CA and the ABC Class 3 Primary CA represents a one-way trust established via a cross-certificate (allowing PXD IAM applications to recognise ABC issued certificates as legitimate).

The ABC implements a *fundamental* trust of the PSP Root CA through configuration of Active Directory trusted root CA certificate stores, i.e. there is no cross-certification involved.

2.2.2. Root Certification Authority

A Root CA is deployed as the trust anchor of the ABC PKI; to afford maximum logical and physical security it is deployed offline (physically disconnected from any networks) and located in a secure facility.

The ABC Root CA is implemented as a *guest* Operating System (OS) on a laptop computer. The laptop *host* runs the Windows Server 2008 R2 operating system and VMWare Workstation v10 virtualisation technology.

The ABC Root CA itself is deployed on the Windows Server 2012 R2 Standard OS as a *standalone CA*[3], it is not connected any networks whatsoever. The ABC Root CA's signing key is protected by a

[2] For example, enrolment of Mascara AD domain controller certificates will leverage the Class 2 Secondary CA

[3] Microsoft CAs fall into two categories: Standalone and Enterprise. Standalone describes a CA that does not leverage AD for its configuration information (typical for a Root CA). Enterprise describes a CA that does leverage AD for its configuration information (typical for Issuing CAs).

USB attached Thales nShield Edge HSM such that it is never *available* or activated outside of a FIPS 140-2 Level 3 accredited cryptographic enclosure.

The ABC Root CA is hosted *alongside* the legacy eRoot on the Root host laptop; for information, the eRoot is deployed on the Windows Server 2003 R2 platform.

Both the ABC Root CA and eRoot leverage the same HSM and Security World construct and *card set apparatus*.

2.2.3. Online (Issuing) Certification Authorities

2.2.3.1. Introduction

While the Root CA is essentially deployed to establish a trust hierarchy, Issuing CAs implemented on the Active Directory Certificate Services (ADCS) platform are the workhorses of the PKI. Issuing certificates to end entities such as users and devices, the Issuing CAs are deployed subordinate to the Root CA and are fully online.

There are two Issuing CAs deployed in the IL4 network and two Issuing CAs deployed in the IL3 network.

The **ABC Class 3 Primary CA** deployed in the IL4 network issues high assurance certificates for both authentication and encryption purposes - it does not issue certificate where non-repudiation is to be asserted. Certificates issued by this CA all bear an OID representing ABC certificate profiles, some certificates (deemed National) will also bear a PID certificate profile OID.

The **ABC Class 3 Secondary CA** deployed in the IL4 network issues high assurance certificates solely for non-repudiation - also referred to as Digital Signature (or DigSig). Certificates issued by this CA all bear an OID representing ABC certificate profiles, some certificates (deemed National) will also bear a PID certificate profile OID.

The ABC Class 3 Secondary CA has a shorter CRL validity period than the ABC Class 3 Primary CA – the integrity of the certificates issued (for non-repudiation) can be said to trump the availability requirements[4]. Furthermore, given the non-repudiation requirements key archival is disallowed at the ABC Class 3 Secondary CA and all subscriber key generation must take place on the subscriber's smart card.

The **ABC Class 2 Primary CA** deployed in the IL3 network issues low assurance certificates solely for authentication, primarily for the RTC WAN programme.

The **ABC Class 2 Secondary CA** deployed in the IL3 network issues low assurance certificates solely for authentication, primarily for the Mobility programme.

In practical terms, inspection of the certification path of a certificate issued to a user entity by an Issuing CA indicates a certificate chain construction as illustrated by the example in Figure 3 (the right hand picture).

[4] The validity period of the ABC Class 3 Primary CA CRL is a compromise between revocation status freshness and practical availability constraints

<IMAGES REMOVED>

Figure 3: ABC PKI Certificate Chain

2.2.3.2. Implementation

Issuing CAs in the ABC PKI are all implemented on Windows Server 2012 R2 as *Enterprise CAs*, meaning that they are reliant upon the underlying Active Directory infrastructure. This approach means the Issuing CAs can leverage the Active Directory for the following:

- Operator access permissions leverage Active Directory (rather than local accounts)
- Configuration information such as certificate templates is published to AD domain controllers and therefore have greater resilience to failure
- Configuration information on Enterprise CAs is propagated to all domain joined computers, enabling those computers to “find” Enterprise CAs for purposes such as auto-enrolment
- Certificates and CRLs can automatically be published to Active Directory
- Supports Microsoft Management Console (MMC) based certificate enrolment processing
- Subject information (DNS for devices, UPNs, etc. for users) can automatically be retrieved for certificate requests

The **Class 3 CAs** are implemented as guest operating systems on the VMWare ESX platform in the IL4 network - they are joined to the ConfMascara Active Directory domain. The Class 3 CAs have their signing keys protected by a highly available pair of Thales nShield Connect network HSMs[5] deployed in the IL4 network.

The **Class 2 CAs** are implemented as guest operating systems on the Microsoft Hyper-V platform in the IL3 network - they are joined to the Mascara Active Directory domain. The Class 2 CAs have their signing keys protected by a highly available pair of Thales nShield Connect network HSMs deployed in the IL3 network.

2.2.4. CRL Distribution Points

A PKI must provide a mechanism to enable time valid certificates which are considered untrustworthy (typically due to a lost / stolen smart card) to be deemed *illegal*, enabling relying parties[6] to reject them. The ABC PKI utilises Certificate Revocation Lists (CRLs[7]) to achieve this end, each CA publishes CRLs to CRL Distribution Points (CDPs) from where relying parties can retrieve them.

CRLs in the ABC PKI are solely published using HTTP protocol - there are no LDAP CDPs. HTTP provides greater universality than LDAP as all relying parties support it and there is comprehensive cross-platform support whereas LDAP CDPs are generally geared towards Active Directory domain joined computers.

[5] The same HSMs are used to protect key material of the tPKI SubCA1 / SubCA2, ActivIdentity CMS and Intercede MyID

[6] A relying party is an entity which decides whether to accept / reject a certificate presented to it, such as a Citrix Access Gateway (CAG) or JAM Central Services (for PID etc.)

[7] Online Certificate Status Protocol (OCSP) is not implemented in the ABC PKI

Certificates issued by the Root CA and Class 3 CAs have four CDP extensions[8]. The first CDP is primarily for use by relying parties within the ABC estate – it is dual published (in IL3 and IL4 networks) leveraging Global Server Load Balancing[9] (GSLB) DNS intelligence to ensure high availability of CRLs across datacentres. By way of example, the ABC Root CA's primary CDP URL is:

- Ø `http://tPKI.gslb.ABC/tPKI/ABC Root CA.crl`

Second and third CDPs are employed to facilitate relying parties located on the Criminal Jun Extranet (CJP) for RESTRICTED material and the xCJP for CONFIDENTIAL material – and the to be implemented Public Sector Network (PSN). *Note: The precise CDPs are yet to be determined.*

A fourth CDP is implemented to facilitate relying parties on the internet, an example is shown below (again illustrated using the ABC Root CA).

- Ø `http://www.abc.bobby.uk/tPKI/ABC Root CA.crl`

CRLs are signed objects (a CRL is signed by a CA in much the same way that a CA signs certificates that it issues) and therefore integrity is assured – there are no special cryptographic measures required for securing CDPs other than best practice hardening to prevent potential denial of service attacks.

2.2.5. Hardware Security Modules

All "ABC PKI services" (with the exception of the Root CA which has a direct attached nShield Edge HSM) utilise network attached Thales nShield Connect to protect key material – the servers are said to be clients of the nShield Connect units. Figure 4 illustrates the Thales nShield HSMs supporting clients in the ABC IL3 and IL4 networks.

[8] A relying party attempts to retrieve a CRL from each CDP in turn, only if a CRL cannot be retrieved from the first CDP will the relying party (after a timeout period) attempt further CDPs

[9] This service is managed by BT and provides active monitoring (at OSI Layer 7) of the nodes prescribed in the GSLB virtual address configuration

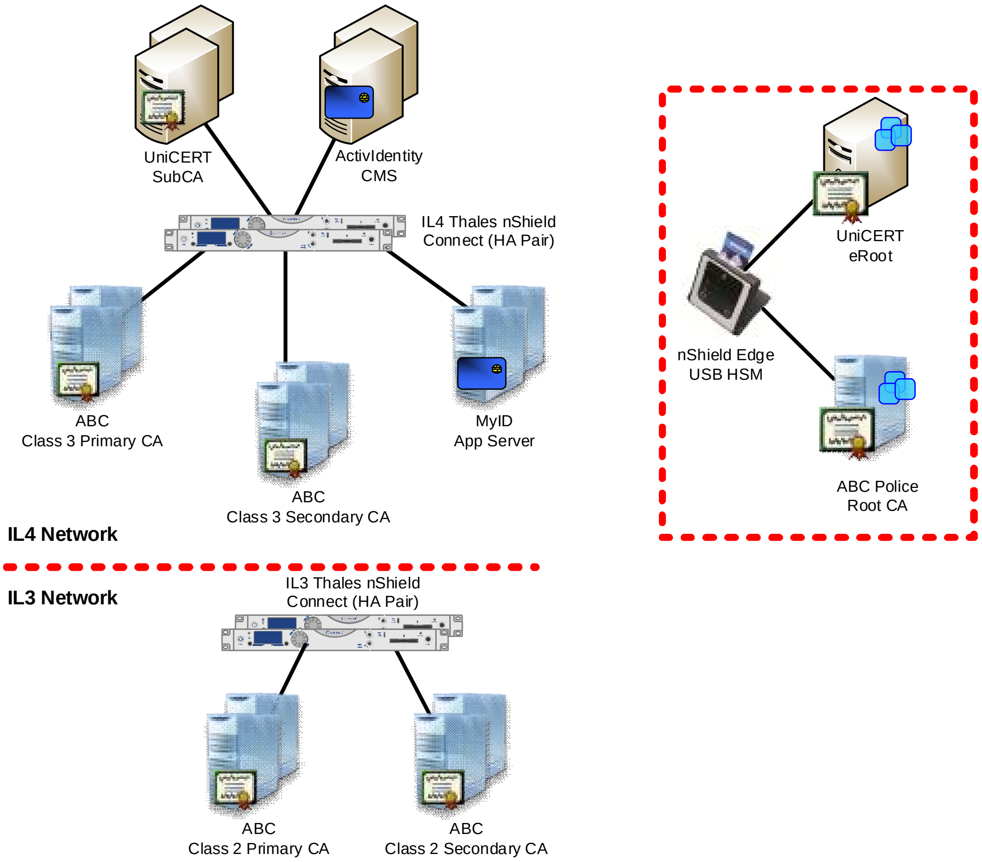

Figure 4: ABC PKI HSM Design

The nShield Hardware Security Modules (HSMs) are employed to protect security sensitive key material which would ordinarily be susceptible to compromise if stored in software in an application or operating system. In the context of the ABC PKI, the HSM protected key material is:

- All CA signing keys
- Registration Authority (RA) keys
- Key Recovery Agent (KRA) keys
- CMS master diversification (symmetric) keys

There are three distinct Security Worlds (management scope) employed in the solution, each implementing a distinct set of access and authorisation controls:

- The offline nShield Edge (Root CA)
- The IL4 nShield Connect Pair
- The IL3 nShield Connect Pair

The use of Operator Card Sets (OCS) to protect signing keys enables a flexible and discrete[10] approach to be taken for authorisation of key activation at each individual client if desired.

[10] Such as multi-operator participation to perform security sensitive operations on protected keys

2.2.6. Promulgation Service

The promulgation service is responsible for the dissemination of certificate and CRL material from their source generation (CAs) to their target locations - effectively to the prescribed CDPs.

The promulgation service incorporates a series of file transfer protocols, staging servers and proxy services to provide the requisite capability, this is described in detail in Reference [02].

2.2.7. Simple Certificate Enrolment Protocol

A Registration Authority for the ABC Class 2 Primary CA based upon the Simple Certificate Enrolment Protocol (SCEP) standard is implemented to simplify enrolment of certificates onto network devices such as routers.

2.2.8. AD CS Database

2.2.8.1. Introduction

The database underpinning the AD CS service is based on the Extensible Storage Engine (ESE) database technology, aka Jet database; in many ways it can be seen as a *proprietary* database to AD CS as third-party databases such as SQL Server or Oracle cannot be leveraged by AD CS.

The AD CS database maintains records for the following:

- Every certificate request received, regardless of whether the request is approved or denied
- Every certificate issued
- Every certificate revoked by the CA
- Every private key archived by the CA
- Every CRL published

The AD CS database largely uses native commands (to AD CS) to perform database operations, although there are a limited number of ESE commands that can also be used for certain maintenance tasks such as compacting the database. The most *impactful consequence* of the ESE database is on availability and recovery time which is addressed in the relevant section, though a brief overview is provided here.

2.2.8.2. Recovery

The AD CS database is backed up to a *flat file* on a regular basis[11], planned to be every four hours; this flat file is transferred to the SAN where it then incorporated in the *SAN availability capability*. The result is that in the event of a CA failure resulting in a requirement to resort to database restore that the maximum recovery interval would be four hours.

In addition to the database restore recovery capability, every certificate issuance triggers an email to the eCE service manager detailing pertinent information about the certificate issuance, such as the certificate subscriber, issuance date and certificate serial number.

To mitigate the potential for loss of integrity in the CA database following a CA restore (certificate orphaning), the information in the emails (specifically the certificate serial numbers) can be used to

[11] This short explanation covers the Issuing CAs only, the Root CA doesn't have any tight availability / recovery interval requirements

replay the certificate records into the AD CS database. The proposed backup method ensures that all certificates can then be revoked[12] (if required) following a recovery event.

2.3. PKI Infrastructure Elements

2.3.1. Smart Card Management System

Intercede MyID smart card management system performs the role of an RA for the ABC Class 3 CAs, whereby it executes certificate requests, revocations, etc. on behalf of users; there is no direct interaction between a user / MyID operator and the ABC Class 3 CAs.

MyID also manages the secure injection of key material and credentials onto smart cards as well as enabling smart card lifecycle event management such as PIN resets, smart card replacement, smart card termination, etc.

Both the RA signing key and smart card diversification master keys are protected by the Thales nShield Connect HSM HA pair deployed in the IL4 network.

2.3.2. Active Directory

The Issuing CAs rely heavily upon (they cannot function without) an Active Directory to store, locate and distribute critical supporting elements such as CA certificates and certificate templates. PKI elements are created in the configuration naming context[13] partition on domain controllers in their respective forest root domain, and subsequently distributed to all domain controllers within the AD forest. The ABC Class 3 CAs are joined to the ConfMascara AD domain, the ABC Class 2 Primary CA is joined to the Mascara AD domain.

Detail of the AD design for IL4 (ConfMascara) is available in Reference [03]; the AD design for IL3 (Mascara) is available in Reference [04].

Users in both the IL3 and IL4 Active Directories share a common User Principal Name (UPN) suffix (Mascara.abc.bobby.uk) therefore a singular authentication certificate can be used to assert identity to either of the Active Directories via smart card logon.

[12] This method doesn’t allow recovery of archived decryption keys issued beyond the primary recovery point (i.e. the time of the AD CS backup)

[13] A directory services partition storing configuration information that is replicated to all domain controllers in the AD forest