3 CERTIFICATION AUTHORITY KEY PROTECTION (HSMS)

3.1 Introduction

In any public key infrastructure deployment, the protection of private key material (application keys) associated with the public/private key pair of certification authorities' CA server certificates is of paramount importance. If the private key of a certification authority is compromised then any certificate signed by that CA server is also considered to be compromised as it would be possible for a "rogue" CA server that was installed and configured with the compromised CA server application key to issue impersonated certificates.

Application keys are created in volatile RAM during the certificate request process and are by default stored in an encrypted format in the user's profile within the "Application Data" container on the CA server's hard disk. The fact that the application key is stored on the hard disk means that it is vulnerable to penetration attacks and stronger protection than that provided by the operating system is required.

In addition to signing certificates, the application key is accessed during certain CA server administrative functions such as restarting the CA server service or signing CRLs. To further strengthen security of the CA, it is possible to mandate that in addition to securing the CA server private key from penetration attacks, that strengthened operator access procedures are implemented whenever any event that requires access to the application key is required.

HSMs fall into two broad groups, dedicated HSMs and network attached HSMs.

- Dedicated HSMs

  A dedicated HSM is directly attached to a CA through either a SCSI card or a proprietary PCI card inserted into the CA computer. All communications with the CA computer are performed through the PCI or SCSI connection and (dependent upon the deployment configuration) the application key material need never leave the protective space of the dedicated HSM. To facilitate communications with the HSM, a proprietary CSP must be installed on the CA computer.

- Network HSMs

  Network HSMs enable two or more CA servers to share a single HSM unit to store application key material, again, all cryptographic operations occur within the HSM. As per the dedicated HSM, a proprietary CSP must be installed on CA servers that need access to application key material stored on the HSM. To protect communications between the CA and the HSM, the network channel is secured through authentication and encryption.

Further to the completion of an evaluation, the SafeNet Luna SA based HSM solution was selected for deployment into the ABC CA server infrastructure. See PE-TEN03 HSM Product Selection – Ref [3] for a report of the HSM product evaluation.

3.2 Luna SA Concepts

The aim of the Luna SA is to provide a secure management framework for cryptographic keys. Key management involves the procedures and protocols that are used throughout the entire life-cycle of cryptographic keys; these procedures and protocols include the generation, distribution, use, storage, destruction, archival and disaster recovery of cryptographic keys.

Luna SA protected keys are stored and activated in a physically secure, tamper resistant device independent of the host application (in this instance the Windows Server 2003 CA service) and the server hosting the application. The independence is defined as being demarcated by a security boundary, the areas within the boundary are only accessible through the HSM's firmware to prevent exposure of cryptographic elements to the "outside world".

The main elements of a Luna SA solution are:

- Luna SA appliance: (2U, 19” rack mount device);
- Luna SA software: including Luna SA Client and Luna SA CSP;
- Luna PED: PIN entry device;
- Luna PED Keys: used to authenticate a secure, trusted path to the HSM;
- Backup PC Card: to create secure backups of the HSM partitions;
- Application keys: the CA server private keys which are to be protected.

A high-level conceptual representation of the Luna SA in relation to the CA server is shown in Figure 2.

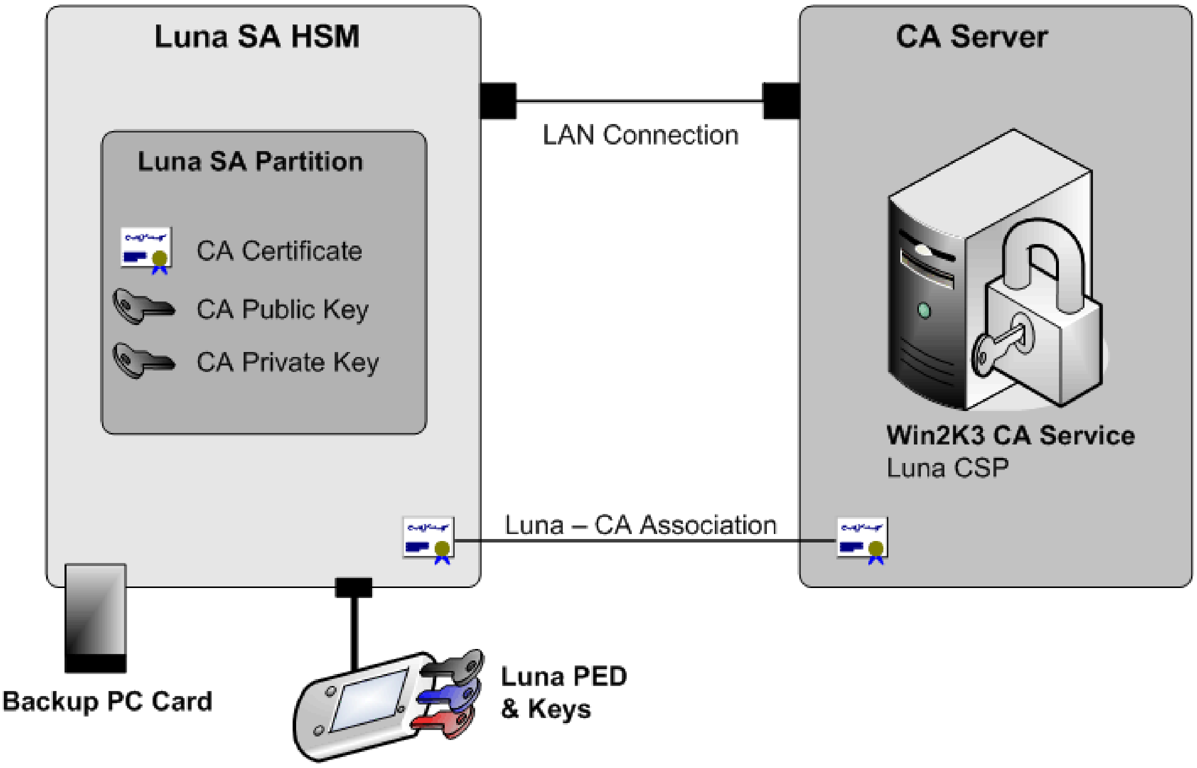

Figure 2 - Luna SA Concepts

The Luna SA concept is platform neutral: HSM deployment and management is compatible with both Windows and UNIX systems. The bulk of administration and maintenance is executed using the Secure Shell (ssh) interface; a distribution of the PuTTY ssh client is included with the Luna SA client software installation.

3.2.1 Luna SA HSM Device

The Luna SA is an Ethernet-attached device that can be shared amongst multiple “applications” such as CA servers; each instance of an application is referred to as a client, clients connect to the Luna SA over TCP/IP. The Luna SA has two network interfaces, giving it the capability for Luna SA management traffic to be routed through a separate physical network to the cryptographic traffic if required – in many circumstances this “bridging” might be considered undesirable.

The Luna SA physical HSM hosts partitions which are independent logical HSMs, each HSM partition having its own data, access controls, security policies, administration access, etc. A Luna SA can have up to twenty partitions, each of which can hold up to eighty data objects. When storing material generated on a Microsoft CA server, three objects are stored per server: the digital certificate, the private key and the public key. Partitions can be dedicated to a single client or multiple clients can all share access to a single HSM partition. Note: there is an additional licence cost involved in deploying more than two partitions.

3.2.2 Access Control Paths

There are two principal control paths to access the Luna SA:

- Client Path (Network Trust Link)

  The client path is an SSL secured channel achieved by the generation, sharing and registering of Luna SA certificates on the Luna SA HSM partition and the client operating system. The client path is the “operational path” for cryptographic functions between the CA server and the CA server’s key material stored on the HSM partition function.

- Trusted Path

  The trusted path is used for data passed from the Luna PED and PED keys to the Luna SA, typically for administrative purposes. The trusted path ensures that HSM authenticated data does not pass through a host or terminal computer where it might be subject to attack.

3.2.3 Luna SA HSM Backup

The Luna SA HSM is backed up to a backup token, which is a PC Card format device which is inserted into the PC Card reader slot in the Luna SA. The PC card is in fact an HSM, and can contain backups of the HSM, individual partitions, or both; authentication for backup tokens would typically follow those of the HSM partition, i.e. require a Luna PED unit to establish an authenticated “trusted path”. Backups of Luna SA HSMs and HSM partitions need only be taken when changes are made to either. Ordinarily, very few changes should need to be made to the Luna SA HSM once it has been installed and configured correctly. Changes to the HSM partitions would generally only occur when the data objects (key material) stored on them changes. In the circumstance of the offline CA servers, these changes (typically a CA server key renewal) occur every four years for the root and policy CA servers and every two years for the online issuing CA server.

3.2.4 Luna SA PED and Keys

The Luna PED is a pin entry device which works in conjunction with the Luna SA HSM and Luna SA backup tokens via a dedicated data port. The PED has an LCD display, a numeric key pad and a PED key slot for insertion of PED keys. Luna PED keys, which are assigned to various different role owners, are inserted into the Luna PED as part of the trusted path authentication process. Figure 3 shows a representation of a Luna PED unit.

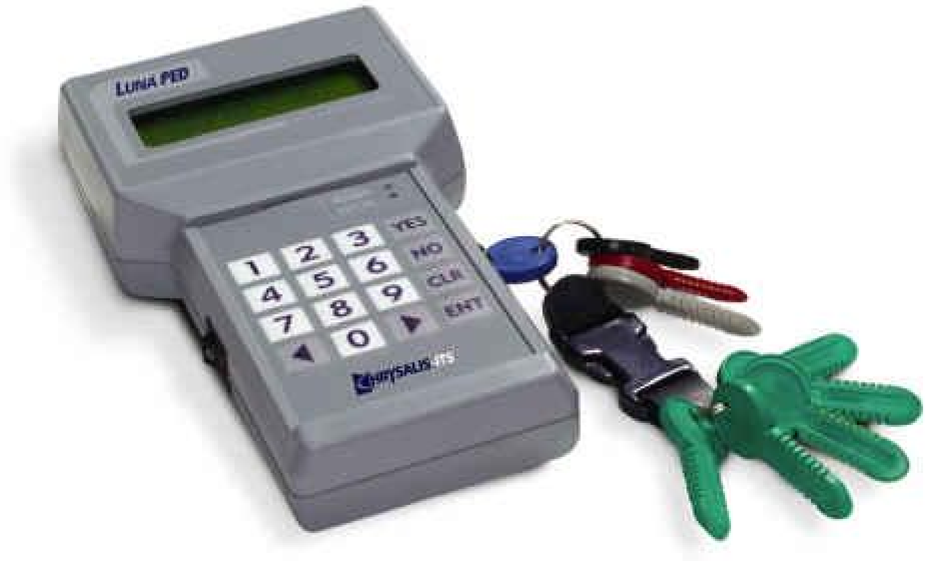

Figure 3 - Luna PED

A PED key is an electronically programmable memory chip, embedded in a coloured, moulded plastic body – it essentially carries the same functionality as a smart card but in a different form factor. In conjunction with a Luna PED, PED keys can be electronically imprinted with identifying information which it retains until deliberately changed.

Luna PED and PED keys are the only means of authenticating to, and accessing the Luna SA administrative interface.

There are five different PED key colours employed with the Luna PED, each associated with a different role; Figure 4 shows each of the PED key colours.

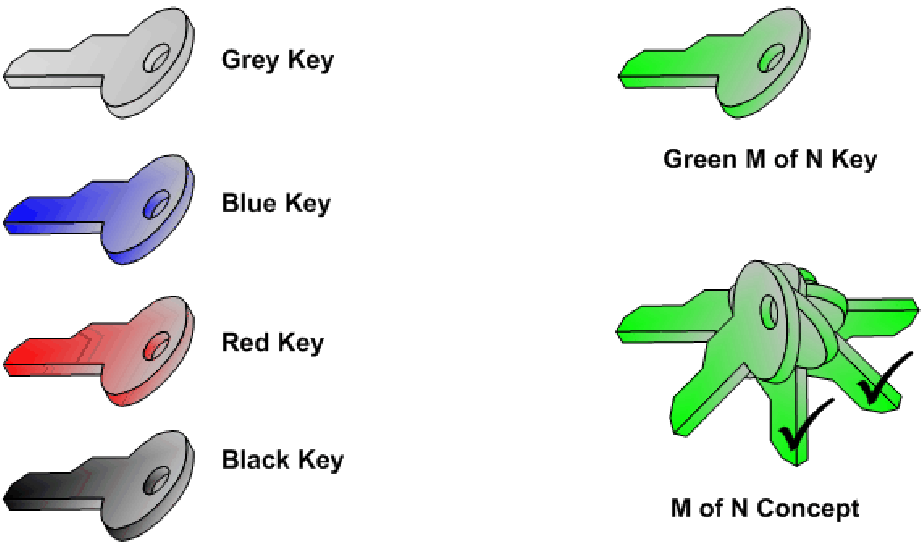

Figure 4 – Luna PED Keys

3.2.4.1 *Grey Key*

The grey PED key contains the default password that permits initial access to the Luna SA, it is not normally used once the blue key has been imprinted. The grey key will be required if the Luna SA is restored from a backup token; all grey PED keys are identical.

3.2.4.2 Blue Key

The blue PED key carries the HSM admin's (or security officer) role. The blue key is used for administrative actions on the Luna HSM, such as creating users or HSM partition owners and changing passwords, cloning or backing up HSM objects. A PED key PIN can be assigned to the blue key for added authentication strength. Blue PED keys can be duplicated to mitigate against loss or damage to a primary blue PED key. The blue PED key can be "shared" amongst HSMs by enabling the "group PED key" option. Group PED keys can be used across multiple HSMs to facilitate easier distribution and operation of PED keys amongst similarly administered HSMs.

3.2.4.3 Red Key

The red key is known as the domain key, meaning that it carries the domain identifier for use in any group of Luna SA HSMs for "cloning" operations; cloning being the secure method of copying HSM partition information or token object such that they can be replicated between HSMs. An HSM or backup token can only be the member of one domain.

Operations with the red PED key copy the domain identification information carried on the key onto new HSM partitions or backup tokens so that they can participate in backup and restore operations.

3.2.4.4 Black Key

The black PED key is the HSM partition owner's key, it is required for login to an HSM as the partition owner. The black PED key is required for partition maintenance and creation / destruction of objects, etc. As with the blue PED key, a PIN can be assigned to the black PED key, it can be duplicated and it can also be shared between HSMs using the group PED key option.

3.2.4.5 Green Key

The green PED keys are known as the M of N PED keys and are only used if the optional M of N security feature is activated on a Luna SA. The M of N is an additional layer of authentication which complements the blue and black PED keys. The green PED keys are imprinted with shares of a secret, the overall number (or pool) of shares can be as many as sixteen, this pool is known as "N". When initialised, a token is shared amongst the keys and a the specified prescribed number of keys, known as "M" is assigned. The M number of green PED keys must be brought together to form the token which can then be used in combination with either the black or blue PED keys to authenticate the trusted path.

The green PED keys (when employed) do not have PINS associated with them and would be shared amongst trusted individuals who must come together when any future activities requiring the use of the HSM partition owner's black PED key or the HSM administrator's blue PED key are undertaken.

3.2.5 Remote Console Operation

As the HSM units will be deployed "alongside" the CA servers in data centres, and remote operators will generally be sited in the separate support centres, to enable an operator to establish a trusted authentication path it is necessary to deploy an HSM in the support centre with a Luna PED attached whereby the operator can authenticate to the local HSM. The credentials established during the "local authentication" can then be used to access a data centre based HSM over the network providing the HSM is deployed in the same HSM domain.

3.3 Proposed ABC Luna SA Design

3.3.1 Overview

The Luna SA HSM model is proposed for use in both the offline and online CA servers; the deployment of the Luna SA for the offline CA servers will be limited in terms of connectivity to a private network. It is proposed that the Luna SA be deployed in a high-availability pair for access by online CA server(s).

CA server key material for the offline CA servers will be stored in separate HSM partition on the "offline" Luna SA HSM; similarly, CA server key material for the proposed issuing CA will be stored on a single HSM partition on the Luna SA supporting the issuing CA. It is anticipated that any future developments requiring additional issuing CA servers would store their CA server key material on a new partition on the same Luna SA "online CA server HSM".

Two Luna domains are proposed for the ABC live estate, one associated with offline CA servers and one associated with online CA servers; this configuration enables better separation of HSM admin and HSM partition group administration roles.

Figure 5 gives an overview of the various deployment elements.

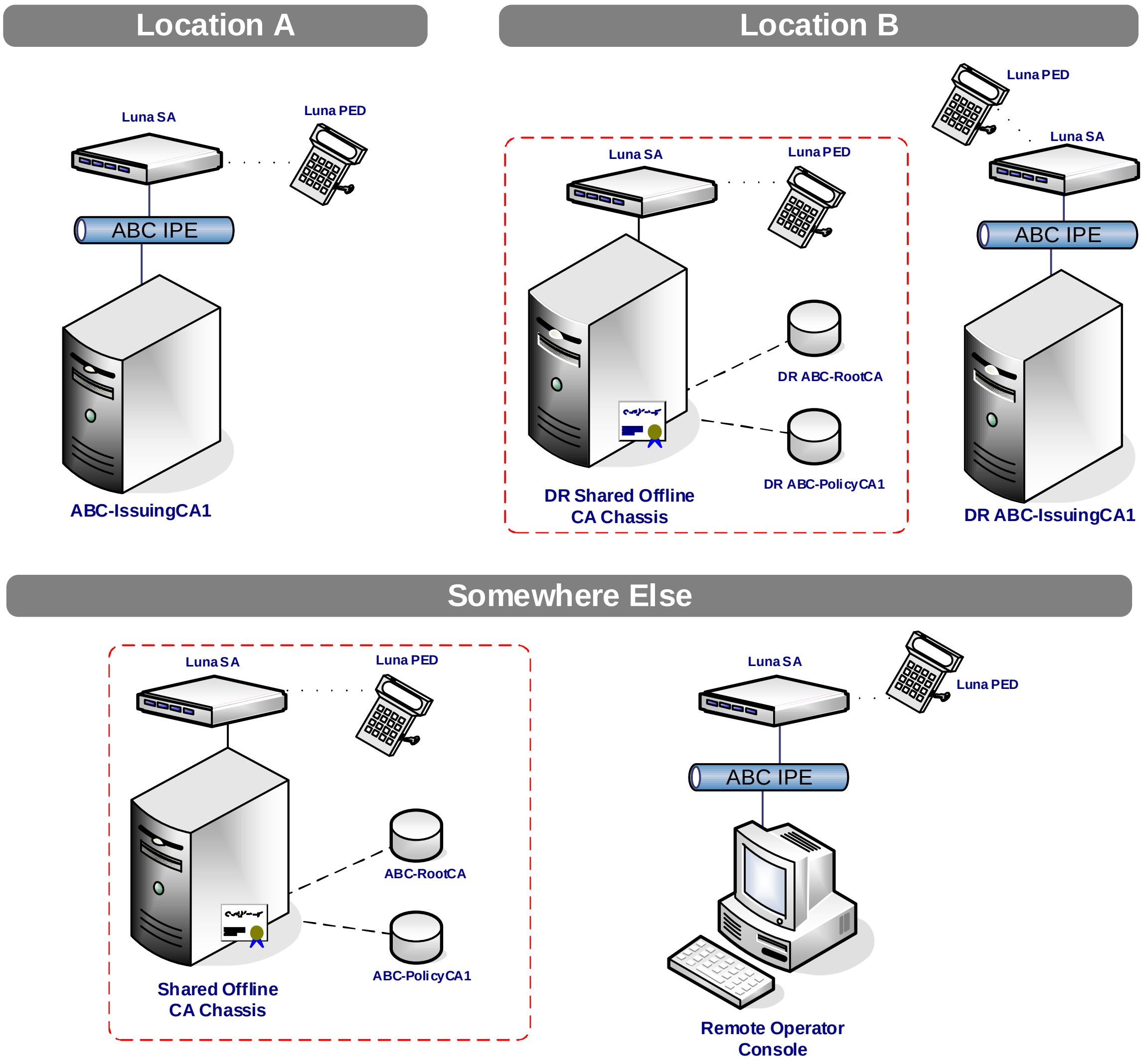

Figure 5 - HSM Overview

3.3.2 Offline CA Servers

The requirement for a Luna SA connected to the offline CA servers (which use a "common shared" offline CA server chassis - details of which are discussed in section 4.1 of this document) mandates the requirement that the offline CA servers be network attached. However, the extent of the network will only be from the CA server to the Luna SA unit by means of a cross-over cable, i.e. there will be no further connectivity to the “wider” Barclays network. The Luna SA deployed for the offline CA servers in the Location B DR site, ABC Section 7.2, will be installed into the same Luna domain to enable backup and restore of HSM partitions between the two units.

3.3.3 Online CA Server(s)

The proposal for online issuing CA servers is to deploy a single Luna SA unit. The unit will be installed into a separate Luna domain than the Luna domain employed for the Luna SA HSM units supporting the offline CA servers, the Luna SA deployed for the online CA server in the Greenford DR site will however be a member of the same Luna domain as the issuing CA’s HSM in Gloucester, see Section 7.3.

3.3.4 PED Units and Keys

To facilitate management of the HSM units, by means of authenticating a “trusted path” to the HSM, a PED unit is required. The same PED unit can be shared between multiple Luna SA units if so desired as all configuration is held in the PED keys, not the PED itself. To provide a level of redundancy in the event of a PED unit failure, it is proposed that two PED units are deployed into Location A.

For each of the domains, it is proposed that a minimum of two sets of PED keys are mastered (via the duplication feature), the keys being Blue, Red and Black. Each of these keys will be deployed into group mode such that they can be used on each Luna SA in the participating domain. It is not proposed to use the M of N function (Green PED keys) as the CA servers’ private key material remains persistently available to the CA server at all times and operator intervention would be expected to be extremely limited. In the event of performing a backup or restore, the three key role holders (Blue, Red and Black) need to come together to perform that function which gives a suitable degree of role separation to protect the integrity of the HSM infrastructure.

3.3.5 HSM Backup

Two, separate backups of each of the partitions on the offline Luna SA HSMs (root and policy) will be taken to a total of four HSM backup PC cards; one “pair” to be stored in a secure vault in the Poole facility and one “pair” to be stored in a secure vault off-site near the Poole facility.

Two, separate backups of the partition hosting the issuing CA key material on the “online” Luna SA will be taken, one to be stored in a secure vault in the Location A facility and one to be stored in a secure vault in the Location B facility.

Figure 6 presents an overview of the backup requirements.

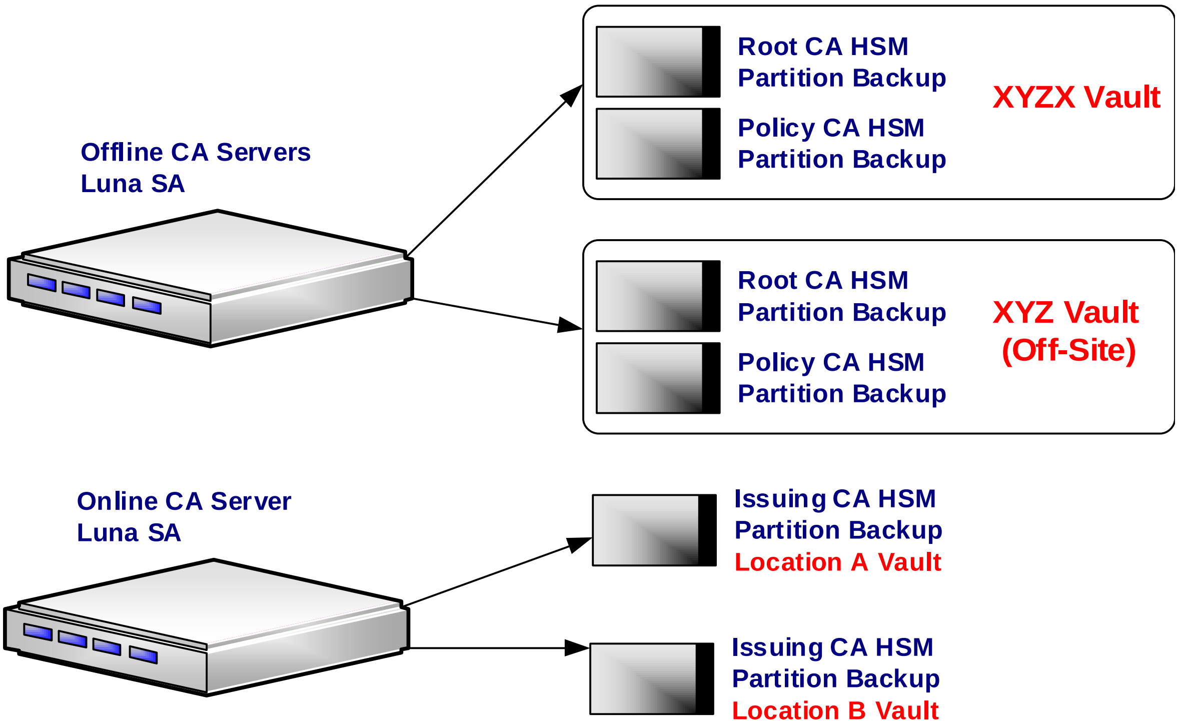

Figure 6 - Overview of HSM Backups

3.3.6 Deployment Summary

The following three tables detail the HSM product requirements and specifications for deployment into the main and DR data centres as well as the remote support centre.

3.3.6.1 HSM Deployment in Operational Data Centre (Location A)

FUNCTION	PRODUCT
Issuing CA Server	One Luna SA (inc. one PED)
Backup Tokens	One for issuing CA

Table 1 – Location A HSM Requirements

3.3.6.2 HSM Deployment in Disaster Recovery Data Centre (Location B)

FUNCTION	PRODUCT
DR Shared Offline CA Servers	One Luna SA (inc. one PED)
DR Issuing CA Server	One Luna SA (inc. one PED)
Backup Tokens	One for issuing CA

Table 2 – Location B HSM Requirements

3.3.6.3 HSM Deployment in Support Centre (XYZ)

FUNCTION	PRODUCT
Shared Offline CA Servers	One Luna SA (inc. one PED)
DR Shared Offline CA Servers	One Luna SA (off-site)

CA Remote Management Console	One Luna SA (inc. one PED)
Backup Tokens	One “pair” of offline CA tokens in Poole and one “pair”of offline tokens off-site

Table 3 - XYZ HSM Requirements

3.3.7 Audit of PED Key Apparatus

The PED keys must be regularly audited to ensure that all PED key holders still have possession of a PED key. Any lost or damaged PED keys must be replaced immediately to ensure that critical levels of PED keys are always available.