FiReControl Trust Services Paper

Contents

Figures

1. Introduction

The requirement for digital certificates in the FiReControl project requires careful inspection of application and infrastructure services since the BAFO is unclear in respect of any specific requirements.

An approach has been taken to consider the aforementioned services and present digital certificate requirements into two categories: *known* and *possible*. For each service which is identified as requiring certificates, a functional use case is presented for ease of understanding.

Further to the presentation of digital certificate requirements, a candidate design for a Public Key Infrastructure (PKI), incorporating both logical and physical aspects, is included. The candidate design is for indicative purposes only and re-evaluation will need to be undertaken before a suitable design is proposed.

RADIUS (Remote Authentication Dial In User Service) type authentication and authorisation services are included in the paper, as they will most often be used in solutions which incorporate digital certificate based authentication. It is for this reason that a generic title (Trust Services) for this document is suggested, rather than purely focus on PKI.

2. Known Requirements

2.1 Authentication of MDT Wireless Devices

2.1.1 Overview

MDTs associate with Fire Station WLAN access points to establish connectivity to LAN / WAN based services. WPA-2 is mandated for wireless security, this naturally leads to the imposition of IEEE 802.1x based authentication of wireless devices – this is achieved using digital certificates.

The process whereby MDTs (endpoints) authenticate using digital certificates over a TLS secured channel is referred to as EAP/TLS. EAP (Extensible Authentication Protocol) is a modular authentication framework extending basic authentication protocols such as PAP, CHAP, MSCHAP, etc. A RADIUS server is required to perform authentication and authorisation of endpoints via their "submitted certificates".

The following certificate types are required to support IEE 802.1x authentication:

- Wireless Devices: Computer certificate with the client authentication purpose, it is enrolled via auto-enrolment capability
- RADIUS (IAS) Servers: Computer certificate with the server authentication purpose, it is enrolled via auto-enrolment capability

Figure 1 illustrates certificate deployment and usage in an 802.1x wireless authentication context.

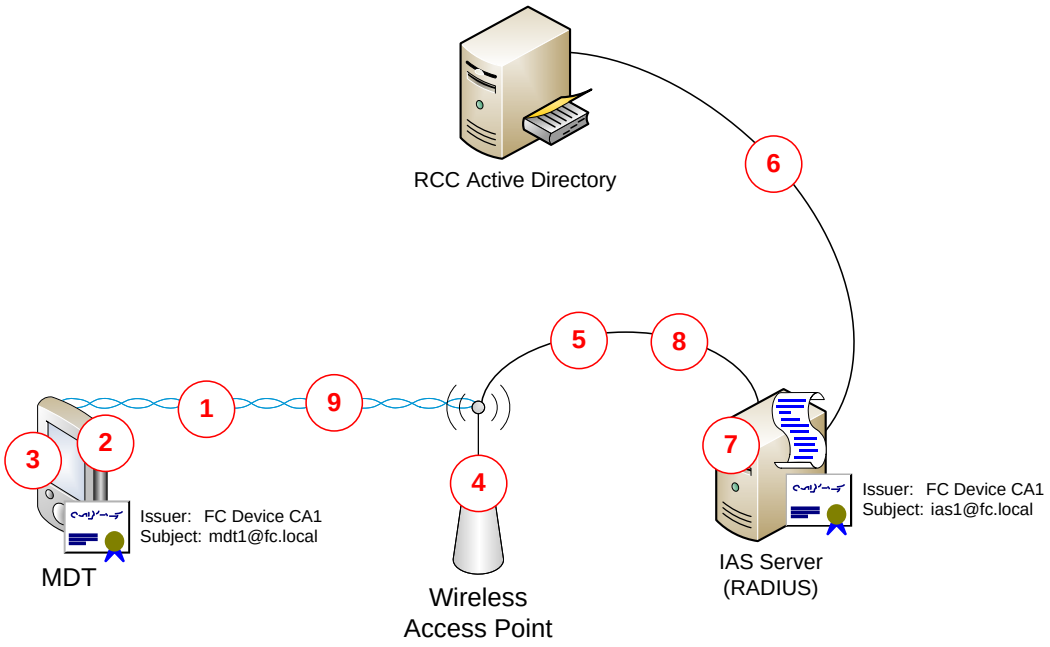

Figure 1: Wireless IEEE 802.1X Authentication

2.1.2 Functional Process Narrative

Step 1: The MDT attempts to associate with the wireless access point, the wireless access point responds that the MDT must provide EAP (certificate) authentication; the RADIUS server's certificate is sent to the client

Step 2: The MDT verifies that the RADIUS server's certificate is trusted and has correct purpose, etc.; the revocation status is not verified.

Step 3: The MDT signs a nonce (arbitrary scrap of information) with its private key and sends the signed nonce (and its certificate) to the wireless access point

Step 4: The wireless access point translates EAP authentication packets into RADIUS authentication packets

Step 5: The wireless access point sends the RADIUS authentication packets to the RADIUS (IAS) server

Step 6: The RADIUS server determines the MDT certificate's UPN and contacts the AD DC, which *maps* the certificate to a computer account in AD. The RADIUS server verifies that the presented certificate is trusted and not revoked, etc.

Step 7: The RADIUS server determines whether the identified computer is granted access to the network based on Remote Access (RAS) policies

Step 8: The RADIUS server sends an authentication success or failure message to the wireless access point

Step 9: The wireless access point sends an EAP success or failure message to the MDT; if successful, suitable encryption keys are generated and shared between the MDT and wireless access point

2.2 Authentication of SEPC "Wired" PCs

2.2.1 Overview

Device authentication is mandated for any PCs attached to the fire station LAN; this is achieved using suitably configured switches which only enable the port in the event that certificate based authentication of the endpoint is successful. The use of certificate based authentication of switch ports is commonly known as "wired IEEE 802.1x authentication". In this context, the PCs are considered to be *supplicants*, the switch the *authenticator* and IAS servers perform the authentication / authorisation role. It should be noted that switches may not always be deployed at fire stations, however, whatever "network connection devices" are used, they will be configured for wired 802.1x.

The functional processes involved in a wired and wireless 802.1x authentication are very similar, with the switch / wireless access point in the role of the authenticator service.

The following certificate types are required to support wired 802.1x authentication:

- PCs: Computer certificate with the client authentication purpose, it is enrolled via auto-enrolment capability
- IAS Servers: Computer certificate with the server authentication purpose, it is enrolled via auto-enrolment capability

It should be noted that the switches themselves are relatively passive in the authentication sequence and do not require certificates themselves, they simply take the certificate based authentication package (EAP/TLS) and convert it into a RADIUS payload for passing to the IAS servers.

Figure 2 illustrates certificate deployment and usage in an 802.1x wired authentication context.

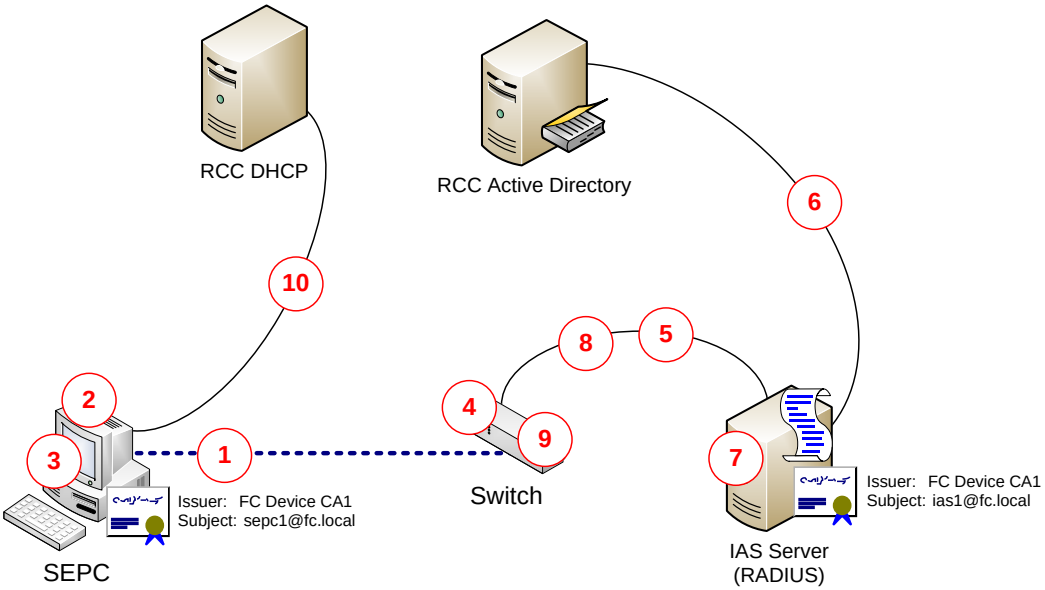

Figure 2: Wired IEEE 802.1X Authentication

2.2.2 Functional Process Narrative

Step 1: The SEPC attempts to *light-up* a port on the 802.1x enabled switch, the switch responds that the SEPC must provide EAP (certificate) authentication; the RADIUS server's certificate is sent to the client

Step 2: The SEPC verifies that the RADIUS server's certificate is trusted and has correct purpose, etc.; the revocation status is not verified.

Step 3: The SEPC signs a nonce with its private key and sends the signed nonce and its certificate to the switch

Step 4: The switch translates EAP authentication packets into RADIUS authentication packets

Step 5: The switch sends the RADIUS authentication packets to the RADIUS server

Step 6: The RADIUS determines the SEPC certificate's UPN and contacts the AD DC, which maps the certificate to a computer account in AD

Step 7: The RADIUS server determines if the identified computer is granted access to the network based on remote access policies

Step 8: The RADIUS server sends an authentication success or failure message to the switch

Step 9: The *switch lights* up (if authentication is successful), enabling access by the SEPC

Step 9: The SEPC continues boot strapping on the network for a DHCP address, etc.

2.3 IPSec Site-to-Site Tunnels

2.3.1 Overview

IPSec site-to-site tunnels are established between:

- Fire Stations and FRS HQs
  and
- SOC / ASOC / RCCs

IPSec site-to-site tunnels ensure that all traffic passing between the Fire Stations / FRS HQ to the aforementioned centres is encrypted; the endpoints are firewalls - certificates are used to authenticate the endpoints of the IPSec tunnels.

The following certificate types are required to support IPSec site-to-site tunnels:

- Firewall Certificates: Computer certificate with the IPSec IKE purpose, it is enrolled manually and the subject information supplied in the request

Certificates deployed to support IPSec site-to-site tunnels are illustrated in Figure 3.

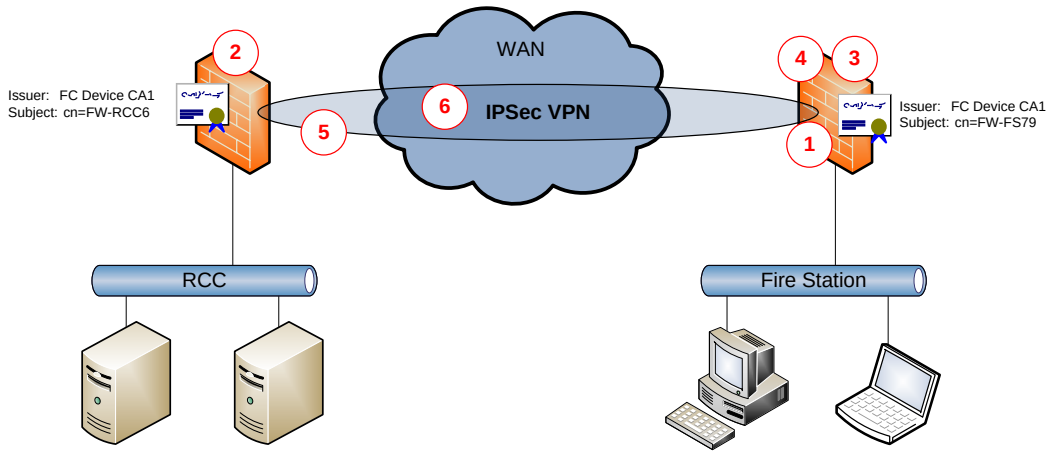

Figure 3: IPSec Site-to-Site Tunnels

2.3.2 Functional Process Narrative

Step 1: The firewall in the fire station is configured to establish an IPSec tunnel with corresponding firewalls in target sites (such as each RCC); as part of the establishment of the tunnel, the *originating* firewall's certificate is presented to the *target* firewall

Step 2: The target firewall validates the certificate presented and sends its own certificate to the originating firewall

Step 3: The target firewall's certificate is validated at the originating firewall

Step 4: A negotiation takes place between the two endpoints and a symmetric key is established at the originating firewall

Step 5: The symmetric key is distributed to the target firewall (encrypted with the target firewall's public key); the symmetric key is decrypted at the target firewall

Step 6: Both endpoints possess the symmetric key and can use this key for encryption of traffic (the symmetric key is rotated on a periodic basis)

2.4 Remote Access VPN

2.4.1 Overview

Remote access VPNs are established between MDTs and remote access firewalls in the hosting centres, certificates are used for machine authentication of the IPSec tunnel only. User authentication is performed with password based credentials which are validated by RADIUS (IAS) services.

The following certificate types are required to support remote access VPNs:

- Firewall Certificates: Computer certificate with the server authentication purpose, it is enrolled manually and the subject information supplied in the request
- Clients: Computer certificate with the client authentication purpose, enrolled via auto-enrolment

Certificates deployed to support remote access VPN tunnels are illustrated in Figure 4.

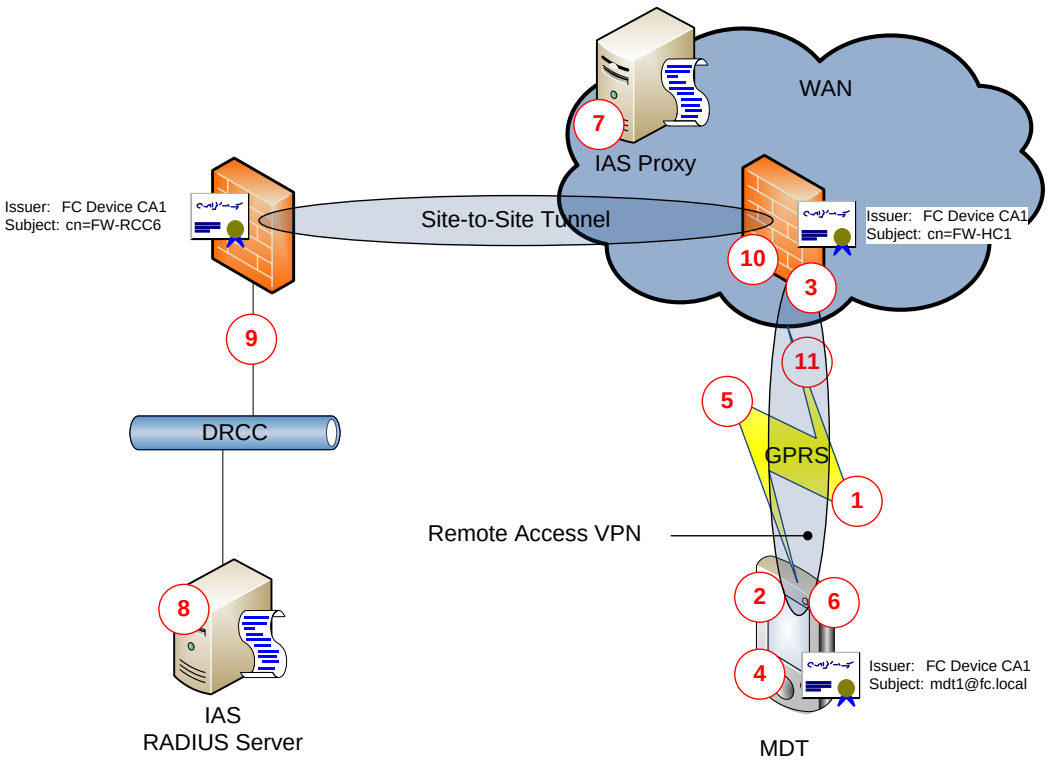

Figure 4: Remote Access VPN

2.4.2 Functional Process Narrative

Step 1: The MDT establishes an internet connection via GPRS

Step 2: The MDT initiates an IPSec VPN connection to a hosted gateway firewall and transmits its certificate to the hosted gateway firewall

Step 3: The firewall validates the presented certificate and transmits its own certificate to the MDT

Step 4: The MDT validates the firewall's certificate (this essentially completes the machine authentication requirement of the IPSec CPN)

Step 5: A pre-master key is established for communication between the MDT and the firewall

Step 6: The user at the MDT is prompted to enter their username and password into the VPN client software which is submitted to the firewall

Step 7: The firewall passes on the authentication payload to an IAS proxy server in the hosting centre, which forwards the request to a RADIUS server in a DRCC

Step 8: The RADIUS server authenticates the user against an Active Directory global catalogue and evaluates remote access policies to determine whether the VPN connection attempt should be authorised

Step 9: The RADIUS server returns an accept / deny response to the firewall

Step 10: The firewall establishes the VPN connection if user authentication is successful

Step 11: Communication between the MDT and the hosting centre firewall is encrypted via the VPN.

Note: Upstream communication between the hosting centre and the RCC / SOPC / etc. is encrypted using the already established IPSec site-to-site tunnels.

2.5 Web Server SSL

2.5.1 Overview

There are known requirements for providing basic “SSL functionality” (often referred to as server-side SSL) to protect credentials passed to web sites, specifically accessing the HP Integrated Lights Out (iLO) remote server management controllers.

The following certificate types are required to support HTTPS:

- Web Server: Computer certificate with the server authentication purpose, it is enrolled manually

Figure 5 illustrates certificate deployment and usage in an HTTPS context.

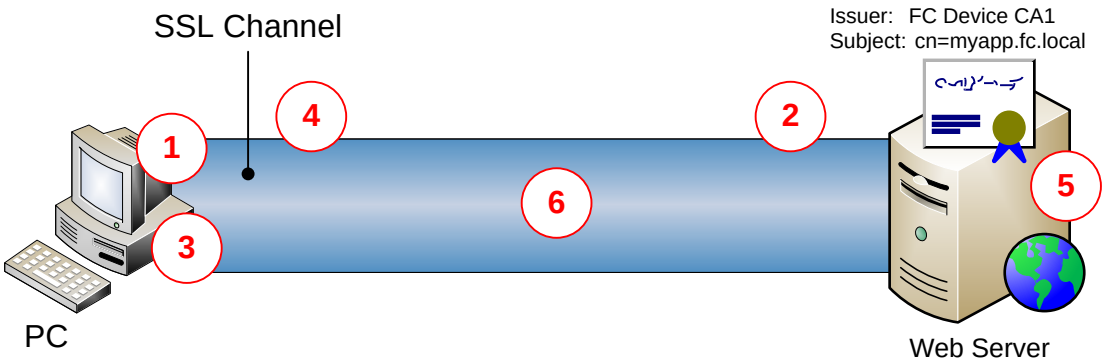

Figure 5: HTTPS Server-Side Authentication

2.5.2 Functional Process Narrative

Step 1: The client attempts to connect to an HTTP service which is protected by SSL (HTTPS)

Step 2: The client retrieves the web server’s SSL server certificate and validates it for trust, purpose, subject information, revocation status, etc.

Step 3: The application generates a session key which is encrypted with the public key in the SSL server certificate

Step 4: The encrypted session key is transmitted to the web server

Step 5: The web server decrypts the session key (both parties now share the same session key)

Step 6: All application traffic between the client and the web server is encrypted

3. Possible Requirements

3.1 Strong Authentication to Windows

3.1.1 Overview

Role holders with high entitlement credentials, such as Active Directory domain admins, must have those credentials protected by strong authentication; the only natively supported strong authentication capability for Kerberos based logons is by smart card / certificate.

Smart card logon to Windows requires users to be enrolled for smart cards; this is facilitated by a Registration Authority (RA) and Smart Card Management System (SCMS). Generally speaking, except on the very largest implementations, the SCMS and RA are combined and singularly referred to as the SCMS.

The following certificate types are required to support smart card logon authentication:

- Smart Card User: User certificate with the client authentication and smart card authentication purposes, it is enrolled in a workflow based process onto the user's smart card
- Domain Controller: Computer certificate with the server authentication and smart card logon purpose, it is enrolled via auto-enrolment capability

Figure 6 illustrates certificate deployment and usage in a smart card logon context.

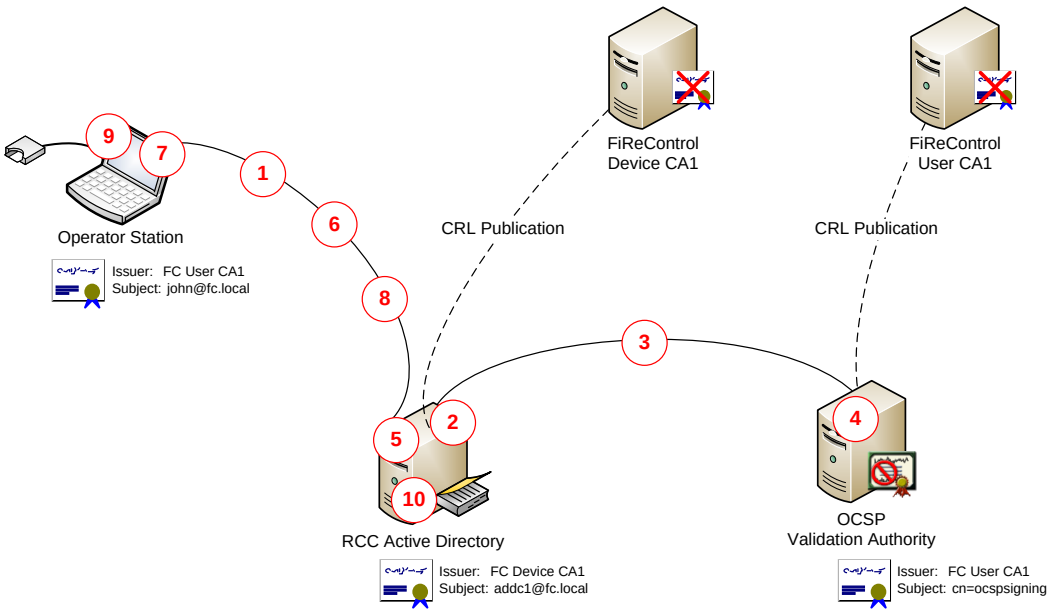

Figure 6: Strong Authentication to Windows

3.1.2 Functional Process Narrative

Step 1: Logon commences after smart card insertion and PIN entry. The client signs a nonce with its private key and transmits its user certificate, along with the signed nonce, to the Active Directory domain controller

Step 2: The AD DC verifies that the user's certificate chains to a trusted root; the AD DC verifies the signature on the nonce correlates with the certificate presented

Step 3: The OCSP client on the AD DC inspects the user certificate for its serial number and sends an OCSP request (asking for the revocation status of the certificate) to the OCSP Validation Authority (VA)

Step 4: The VA generates an OCSP response (signing it with its delegated OCSP signing key); the OCSP response is retrieved by the relying party (AD DC)

Step 5: The OCSP client on the AD DC validates the OCSP response

Step 6: The AD DC signs a nonce with its private key and transmits its AD DC certificate to the client

Step 7: The client verifies that the AD DC's certificate chains to a trusted root; the client PC verifies the signature on the nonce correlates with the certificate presented

Step 8: The client inspects the AD DC certificate for its CRL Distribution Point (CDP) and retrieves the Device CA CRL from the AD DC (the CRL is stored within the configuration partition and therefore available on all AD DCs)

Step 9: The client validates that the AD DC certificate's serial number isn't present on the CRL

Step 10: After successful authentication, a Kerberos TGT is granted to the user which can subsequently be used to request Kerberos service tickets when needing to access Kerberos protected resources

3.1.3 Comments (BAFO Security Annex E – Access Control)

3.1.3.1 Section 3.2 (Identification Mechanisms)

Authentication mechanisms at client: For RCC, SOC and FRS HQ, two-factor authentication based on smart card tokens with embedded X.509 digital certificates matches security to access privileges.

3.1.3.2 Section 4.3 (Password Policy)

SOC, RCC and FRS HQ Users: Smart card authentication requires the entry of a single passphrase or PIN in order to access the private key operation necessary for certificate login. This single authentication will enable single sign-on to all enabled applications.

MDT OS administrative account: This is the privileged account that may be infrequently used to allow a field service engineer to configure or investigate an MDT when physically present. Access will require network access, for which the SecurID token will be used for authentication.

3.1.3.3 Section 5.1 (Technical Mechanisms: Users at Protected-Site Clients)

Risk calculations in Rationale [AD 9] illustrate the need for two-part authentication at FRS HQ. This is a result of the level of system access in conjunction with the potential for uncleared, unauthorised users. In contrast, there is a minimum of BC clearance at RCC that reduces the risk such that two-factor authentication may not be strictly necessary. However, RRI is an indicator only, and two-factor authentication is retained for RCC and SOC users to give strong authentication.

3.2 Protecting Application Binds to AD

3.2.1 Overview

Some applications leverage Active Directory as a “proxy” user repository, often these applications need to be able to write / update user information held in AD and this is achieved using a “high entitlement” user account. By default, binds to LDAP are not protected and it is therefore necessary to perform the binding over SSL, such that the credentials used for the binding are suitably encrypted, as well as ensuring that subsequent traffic between the application and AD DC is encrypted.

The following certificate types are required to support LDAP/S:

- Domain Controllers: Computer certificate with the server authentication purpose, it is enrolled via auto-enrolment capability

Figure 7 illustrates certificate deployment and usage in an LDAP/S context.

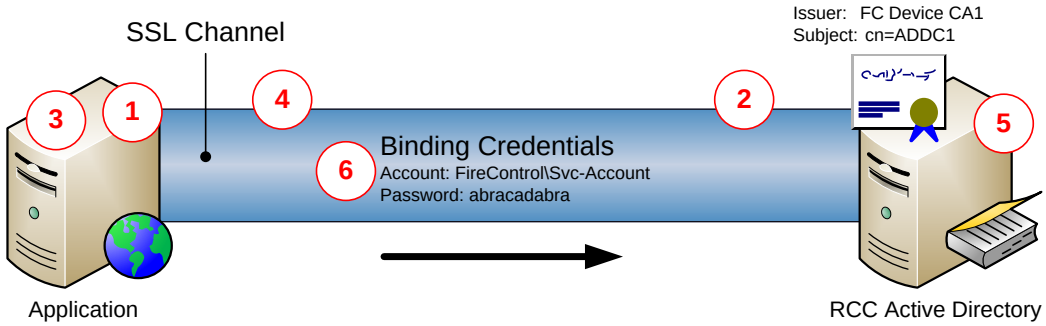

Figure 7: LDAP/S Authentication

3.2.2 Functional Process Narrative

Step 1: The application attempts to bind to an Active Directory domain controller, LDAP/S is specified in the connection properties

Step 2: The application retrieves the AD DC’s server certificate and validates it for trust, purpose, subject information, revocation status, etc.

Step 3: The application generates a session key which is encrypted with the public key in the DC certificate

Step 4: The encrypted session key is transmitted to the AD DC

Step 5: The AD DC decrypts the session key (both parties now share the same session key)

Step 6: The binding credentials are encrypted with the session key and transmitted to the AD DC

3.3 HTTPS Mutual Authentication

3.3.1 Overview

There are some HTTP based applications which may require certificate based authentication to provide stronger credentials than simple user name and password; a typical example is external parties accessing applications via the *FRS API*.

The following certificate types are required to support mutual authentication HTTPS:

- Web Servers: Computer certificate with the server authentication purpose, it is enrolled manually and the subject information supplied in the request
- Clients: User certificate with the client authentication purpose, it could be enrolled manually or via auto-enrolment dependent upon the specific scenario

Figure 8 illustrates certificate deployment and usage in an HTTPS context.

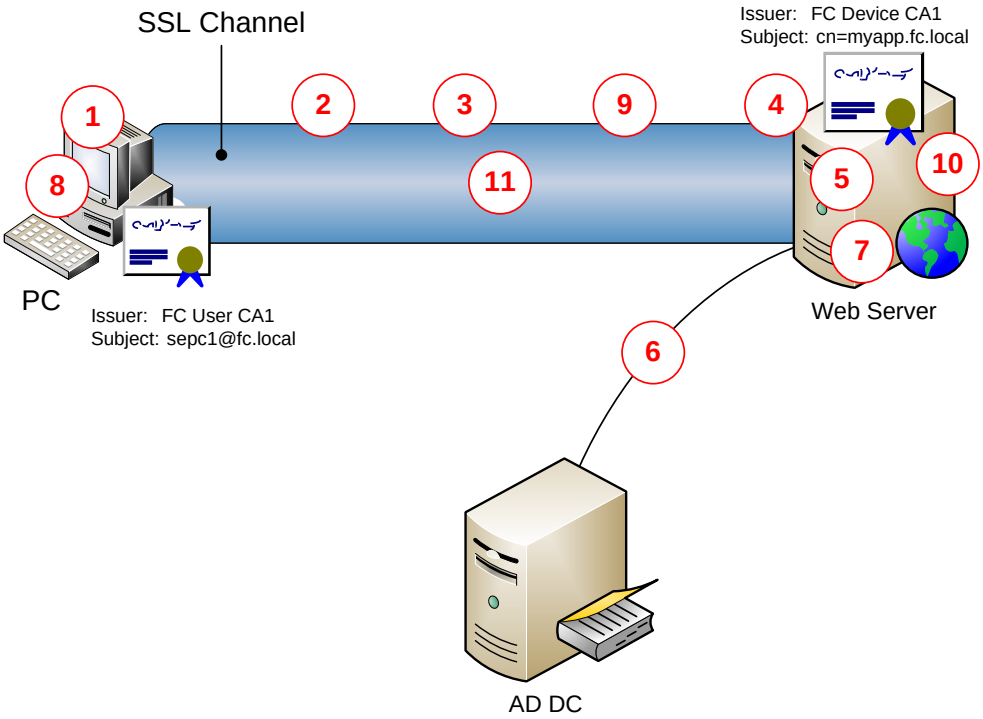

Figure 8: HTTPS Mutual Authentication

3.3.2 Functional Process Narrative

Step 1: The client attempts to access a service on the web server where mutual HTTPS is mandated

Step 2: The client retrieves the web server's certificate and validates it for trust, purpose, subject information, revocation status, etc.

Step 3: The client is challenged for their certificate

Step 4: The client presents its certificate to the web server

Step 5: The web server inspects the UPN in the presented certificate

Step 6: An AD GC is queried and the user identity established

Step 7: The web server grants access to the application based upon the identity established

Step 8: The client generates a session key which is encrypted with the public key in the web server certificate

Step 9: The encrypted session key is transmitted to the web server

Step 10: The web server decrypts the session key (both parties now share the same session key)

Step 11: Application traffic is transmitted within the SSL channel

Note: An assumption is made in this narrative that the web server is running IIS and can take advantage of implicit certificate mapping (where UPN in certificate is mapped to a user by a GC).

4. Candidate Design

4.1 Logical Design

To support the PKI / trust services in the FiReControl project, a candidate design has been prepared as illustrated in Figure 9.

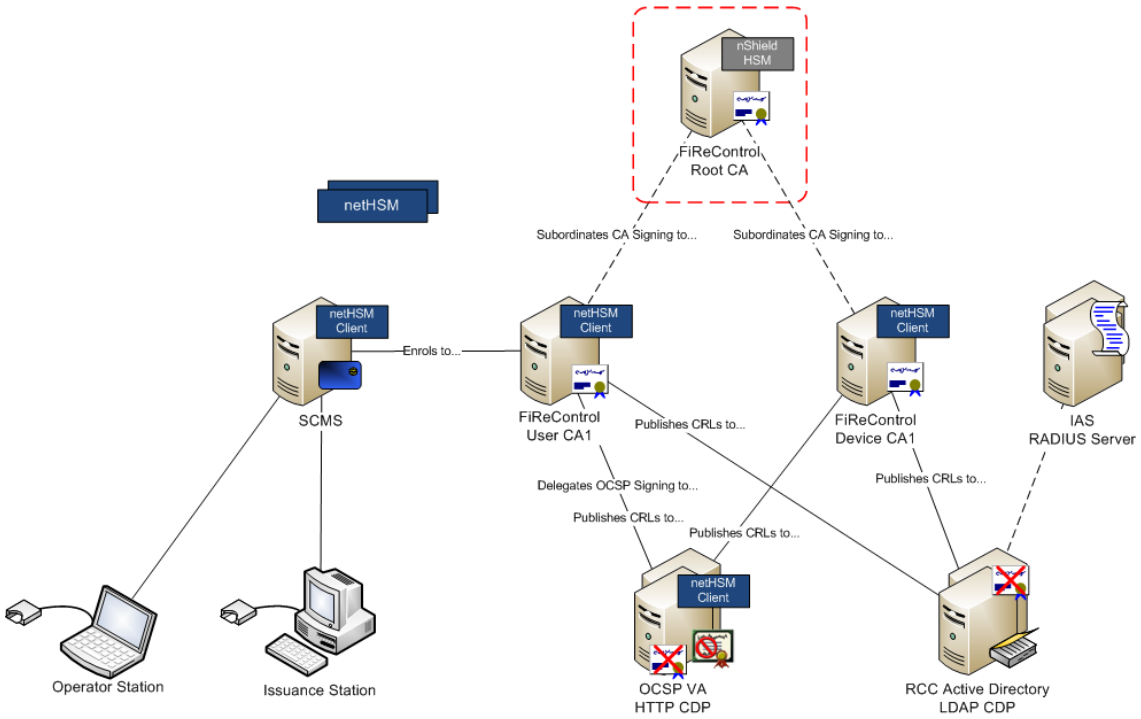

Figure 9: Candidate Logical Design

4.1.1 CA Services

A classic two-tier approach is proposed in the PKI, incorporating an offline Root CA and two subordinate Issuing CAs, deployed for issuing certificates to users and devices respectively. The separation of the Issuing CA capability onto two platforms enables a more flexible approach to be taken in respect controlling bandwidth consumed in revocation checking, etc.

All CA servers are deployed on the Microsoft Windows Server platform, the Root CA on Windows Server 2003 R2 standalone and the Issuing CAs on Windows Server 2003 R2 enterprise.

4.1.2 Hardware Security Modules

Security sensitive key material (such as CA and OCSP signing keys and SCMS diversification keys) is protected by network based Hardware Security Modules (HSMs); the sole exception being the Root CA where a PCI based HSM is deployed.

Thales (nCipher) HSMs are proposed due to their extremely close integration with the Windows platform and their common abstraction platform regardless of whether the HSMs are deployed in direct attached (PCI) or network form factors.

4.1.3 Revocation Services

As well as providing traditional monolithic revocation services using Certificate Revocation Lists (CRLs), Online Certificate Status Protocol (OCSP) is implemented to enable near real-time revocation status to be effected. Implementing solely CRL based revocation status checking introduces a dilemma between freshness and *system availability* due to non-publication of CRLs in the event of a disaster; OCSP mitigates this dilemma.

OCSP services are deployed in two principal components, OCSP clients and OCSP servers (validation authorities). OCSP client software must be deployed on the Active Directory DCs and this is natively supported on the Windows Server 2008 platform, likewise Windows Server 2008 also provides OCSP server capability natively.

Given that Windows Server 2008 is not the preferred platform in FiReControl and that the native OCSP services available in that platform are rudimentary at best, it is preferred to implement OCSP using components of the Axway (Tumbleweed) Validation Suite. This results in OCSP client software being implemented on all FiReControl Active Directory DCs; and OCSP Validation Authority servers deployed to support OCSP response generation. The platforms employed to host the Validation Authorities also host HTTP CRL Distribution Points (CDPs).

4.1.4 RADIUS Servers

To support IEEE 802.1x and remote access authentication, it is necessary to deploy RADIUS server services (the wireless access point / 802.1x enabled switch / remote access VPN firewall are considered the RADIUS clients). On the Windows Server 2003 platform RADIUS server services are provided by the Internet Authentication Service (IAS).

A combination of IAS policy servers (IAS is installed as a Windows server service) and IAS proxy servers (essentially RADIUS request forwarders) are deployed.

4.1.5 Smart Card Management System

There are three smart card management systems which might be considered for the FiReControl project:

- Microsoft CLM (Certificate Lifecycle Manager)
- Intercede MyID CMS (Card Management System)
- ActivIdentity CMS

Microsoft CLM is ideally suited to environments which are heavily “Microsoft orientated”, i.e. based upon Active Directory, with Microsoft CAs and Windows server / client platforms, much like that of FiReControl. However, CLM is relatively weak in respect of capability over and above the most basic smart card management capability, such as identity vetting, smart card printing, managing biometrics, physical access system integration, etc.

CLM lacks FIPS 201 support which is becoming a standard requirement for government and public sector bodies, providing strong ID registration and validation. FIPS 201 is mandated by (US) based programs such First Responders Access Program for emergency services, however, it is also being adopted in the UK by the National Police Improvement Authority (NPIA) for force wide adoption of smart cards and it is prudent to adopt this standard given potential scope for future interoperability between emergency services in the UK.

Intercede myID CMS and ActivIdentity CMS both support FIPS 201, as well as integration with various third-party infrastructure components such as directories, databases, printers, etc. They are very rich smart card management systems which meet the requirements of the FiReControl project.

It is proposed that a technical / commercial evaluation exercise is carried out to determine the best fit SCMS for the FiReControl project.

4.2 Physical Design

To support the PKI / trust services in the FiReControl project, an indicative design for the physical deployment is illustrated in Figure 10; this is extremely primitive and requires significant refinement.

All services are capable of deployment on a virtualised platform, with the exception of:

- The Root CA (deployed on a *physical server*)
- The netHSMs (deployed on dedicated appliances)

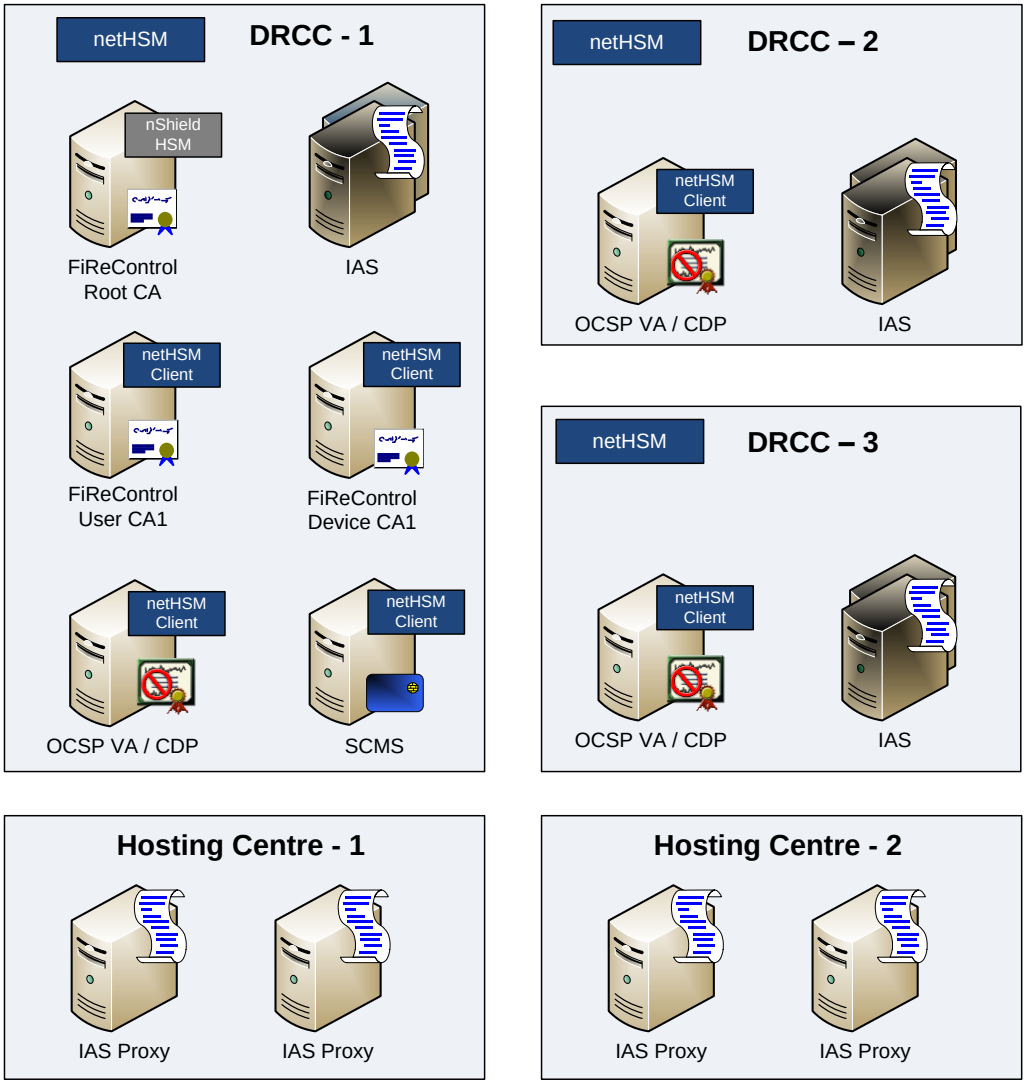

Figure 10: Indicative Physical Design

4.2.1 CA Services

It is not proposed to deploy any of the CA services in a highly available configuration as clustering of Windows Enterprise CA is only possible on Windows Server 2008 – and then only in a two-node configuration. Failure of a CA server would not have an immediate impact on system availability providing all systems enrolled for certificates perform renewals at a suitable interval prior to expiry.

Provision of CA services in the event of a disaster at the *primary site* would be achieved by restoring *backups* onto suitable *shadow platforms* in *secondary sites*.

4.2.2 Hardware Security Modules

Issuing CAs, OCSP VAs and SCMS all rely upon network HSMs for accessing security sensitive key material; network HSMs are deployed in each DRCC and highly available to each “client”.

4.2.3 Revocation Services

Generally speaking, revocation services are the most critical elements of a PKI since non-availability of revocation status information often results in certificate based services failing. Revocation services (both CRL hosting and OCSP response signing) are deployed in each DRCC; in addition, CRLs are published to all Active Directory domain controllers.

4.2.4 RADIUS Servers

IAS proxy servers are deployed in each of the hosting centres, IAS policy servers are deployed in pairs in each DRCC onto existing DHCP servers. The IAS service is deployed onto dedicated servers in the hosting centres.

4.2.5 Smart Card Management System

Given that there is no highly available configuration of CA services, there is little value in deploying SCMS in an HA configuration. SCMS services availability follows that of the CA services, such that in event of a disaster at the *primary site*, SCMS service availability would be achieved by restoring *backups* onto suitable *shadow platforms* in *secondary sites*.

This is the last page of the document