‘Trust Services Security Components’

David Wozny, Infrastructure Support

Agenda

- Public Key Infrastructure (PKI) Basics
- FiReControl PKI Candidate Design
- RADIUS Basics and FiReControl Candidate Design
- Known Use Cases (Requirements)
- *Tentative* Use Cases

PKI Services - CIA

- Public Key Infrastructure
  - A capability - it’s not *the application*
  - Harnesses the strength of asymmetric key cryptography
- Confidentiality
  - Encryption: In transit and / or at rest
- Integrity
  - Tamper *proofing*
- Authentication
  - Assertion of identity by evidencing possession of private key

PKI Basic Components

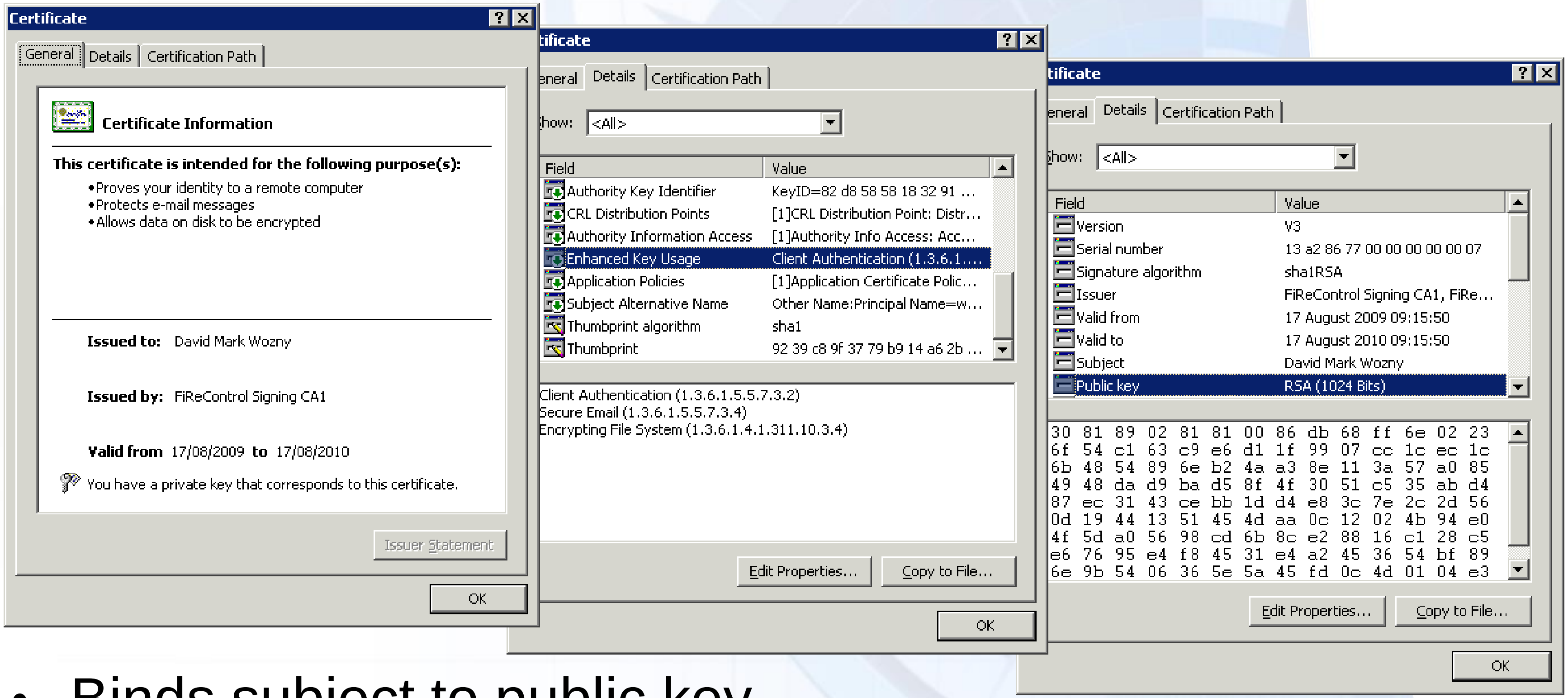
- Certification Authorities
  - Issue digital certificates
  - Publish Certificate Revocation Lists (CRLs)

- Subscribers
  - End entities such as users, computers or services; *owner* of the private key

- Revocation Providers
  - Somewhere to retrieve a CRL from

- Relying Parties
  - Decision maker on whether to *allow* certificate

A Digital Certificate – Look See



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Protects e-mail messages
- Allows data on disk to be encrypted

Issued to: David Mark Wozny

Issued by: FiReControl Signing CA1

Valid from 17/08/2009 **to** 17/08/2010

You have a private key that corresponds to this certificate.

how: <All>

Field	Value
Authority Key Identifier	KeyID=82 d8 58 58 18 32 91 ...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Application Policies	[1]Application Certificate Polic...
Subject Alternative Name	Other Name:Principal Name=w...
Thumbprint algorithm	sha1
Thumbprint	92 39 c8 9f 37 79 b9 14 a6 2b ...

Client Authentication (1.3.6.1.5.5.7.3.2)
Secure Email (1.3.6.1.5.5.7.3.4)
Encrypting File System (1.3.6.1.4.1.311.10.3.4)

how: <All>

Field	Value
Version	V3
Serial number	13 a2 86 77 00 00 00 00 00 07
Signature algorithm	sha1RSA
Issuer	FiReControl Signing CA1, FiRe...
Valid from	17 August 2009 09:15:50
Valid to	17 August 2010 09:15:50
Subject	David Mark Wozny
Public key	RSA (1024 Bits)

```
30 81 89 02 81 81 00 86 db 68 ff 6e 02 23
6f 54 c1 63 c9 e6 d1 1f 99 07 cc 1c ec 1c
6b 48 54 89 6e b2 4a a3 8e 11 3a 57 a0 85
49 48 da d9 ba d5 8f 4f 30 51 c5 35 ab d4
87 ec 31 43 ce bb 1d d4 e8 3c 7e 2c 2d 56
0d 19 44 13 51 45 4d aa 0c 12 02 4b 94 e0
4f 5d a0 56 98 cd 6b 8c e2 88 16 c1 28 c5
e6 76 95 e4 f8 45 31 e4 a2 45 36 54 bf 89
6e 9b 54 06 36 5e 5a 45 fd 0c 4d 01 04 e3
```

- Binds subject to public key
- Private key is stored securely in Windows (or smart card)
- Subscriber certificate is digitally signed by CA
- Certificate has validity period, purpose, extensions

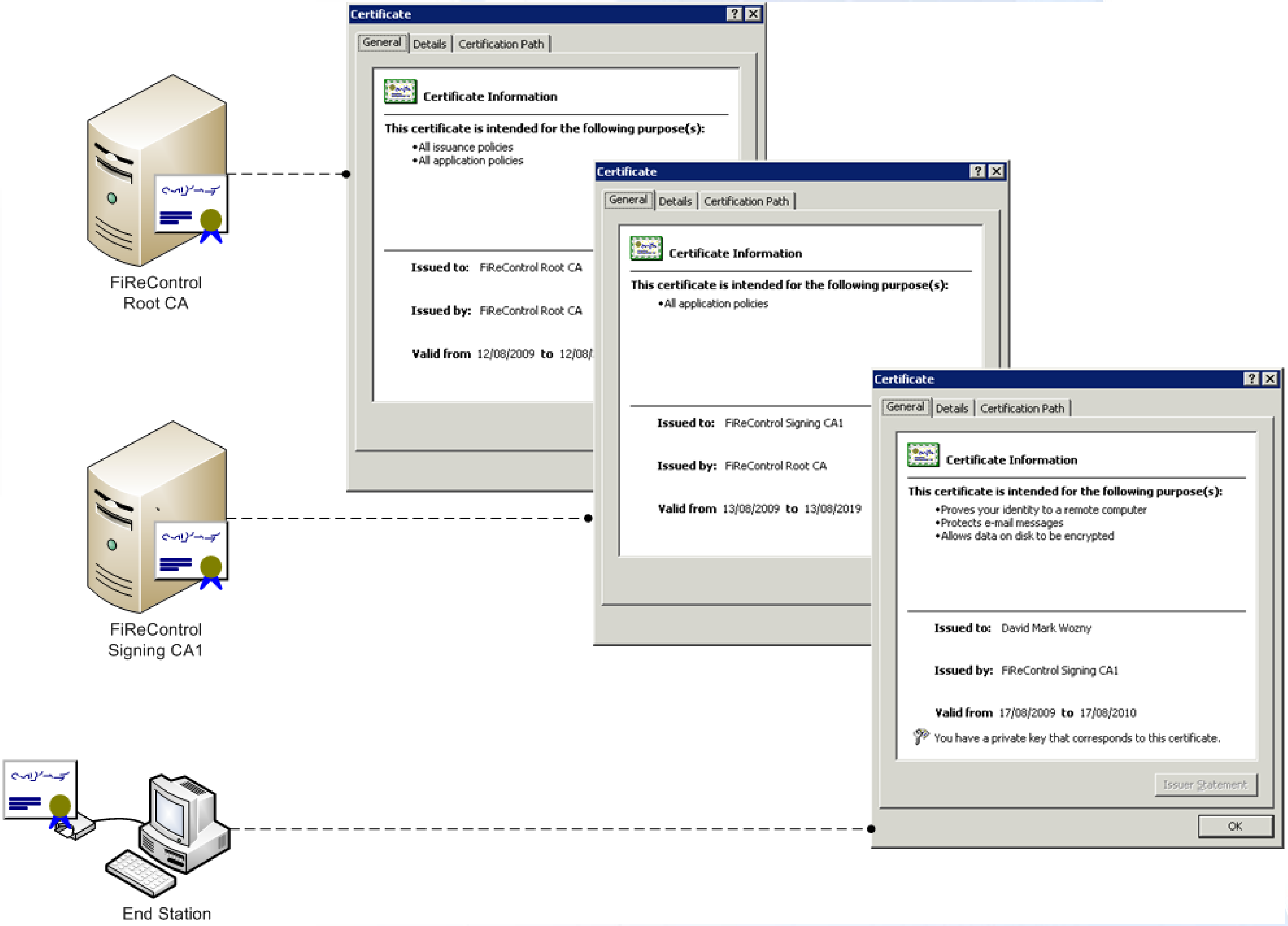
Trust Chain

- Trusted Root Certification Authority
  - Trust anchor – implicitly trusted by all computers and users
  - Extremely security sensitive
  - Protecting CA’s private key necessary to prevent impersonation
  - Best practice is to deploy disconnected from network
- Signing (Issuing CA)
  - Issues all certificates to subscribers
  - Publishes CRLs
- Subscriber (End Entity)
  - Typically user or computer

FiReControl Candidate PKI Design

- Microsoft Certification Authority Service
  - EAL4+ accreditation
  - Tightly integrated with Active Directory
  - *Relatively uncomplex*
  - Nil licence cost
- Design: Two Tiers
  - FiReControl Root CA (offline)
  - FiReControl Signing CAs (one in each DRCC)

Certification Authority Trust Chain



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: FiReControl Root CA

Issued by: FiReControl Root CA

Valid from 12/08/2009 to 12/08/

Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued to: FiReControl Signing CA1

Issued by: FiReControl Root CA

Valid from 13/08/2009 to 13/08/2019

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Protects e-mail messages
- Allows data on disk to be encrypted

Issued to: David Mark Wozny

Issued by: FiReControl Signing CA1

Valid from 17/08/2009 to 17/08/2010

You have a private key that corresponds to this certificate.

Critical Design Issues

- Protection of CA Private Keys
  - Use Hardware Security Modules (HSMs)
  - Virtualisation isn’t practicable

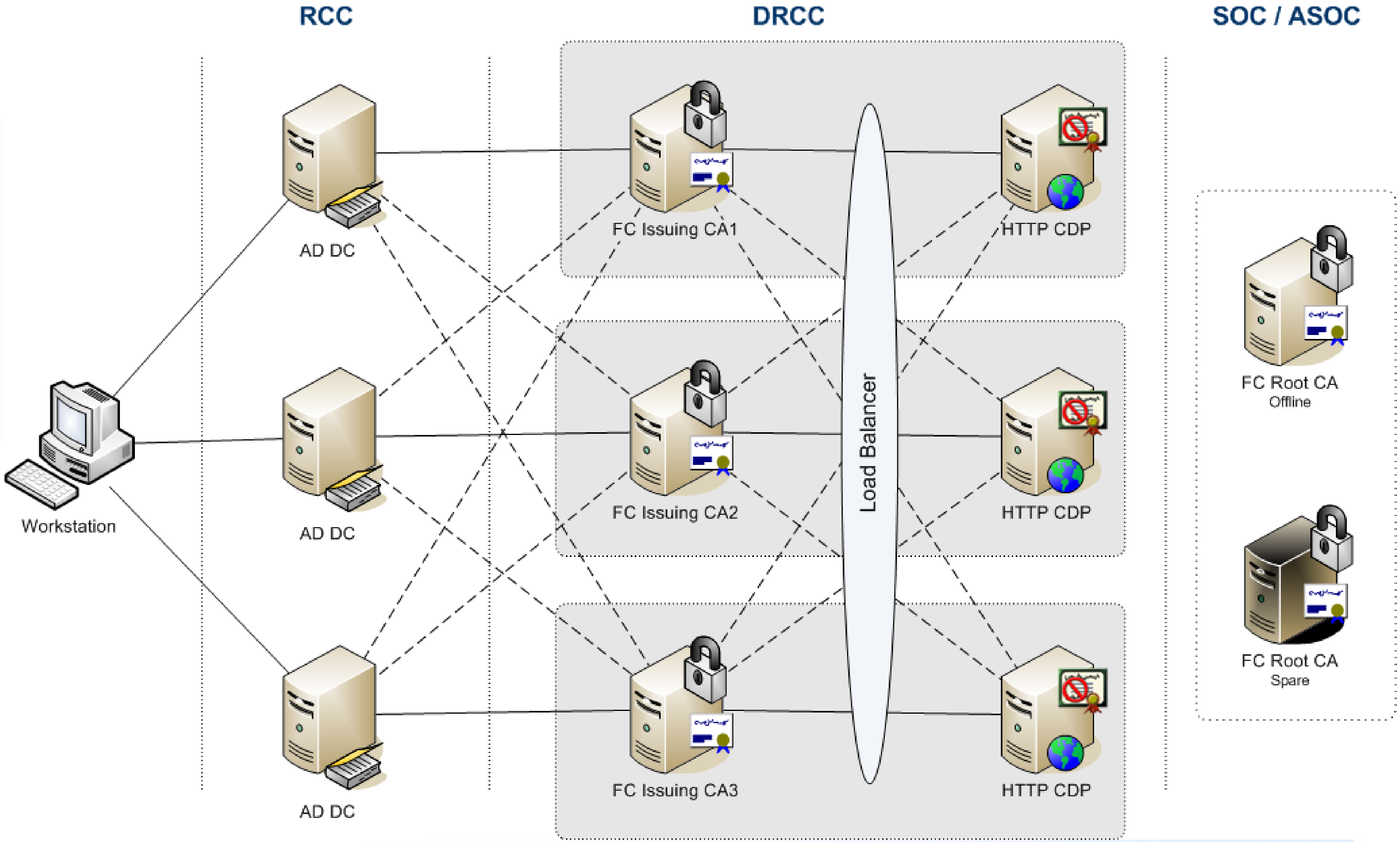
- Something *critical here*

- Availability...

Availability

- Signing CA in each DRCC
  - – Can sign CRLs on behalf of other CAs
  - – Maintain certificate issuance capability
  - – Use auto-enrolment where possible
  - – Sensible CRL validity periods
- Revocation Points in each DRCC
  - – LDAP availability is *implicit* (AD DCs in DRCC / RCC)
  - – HTTP revocation points (web sites) in DRCC

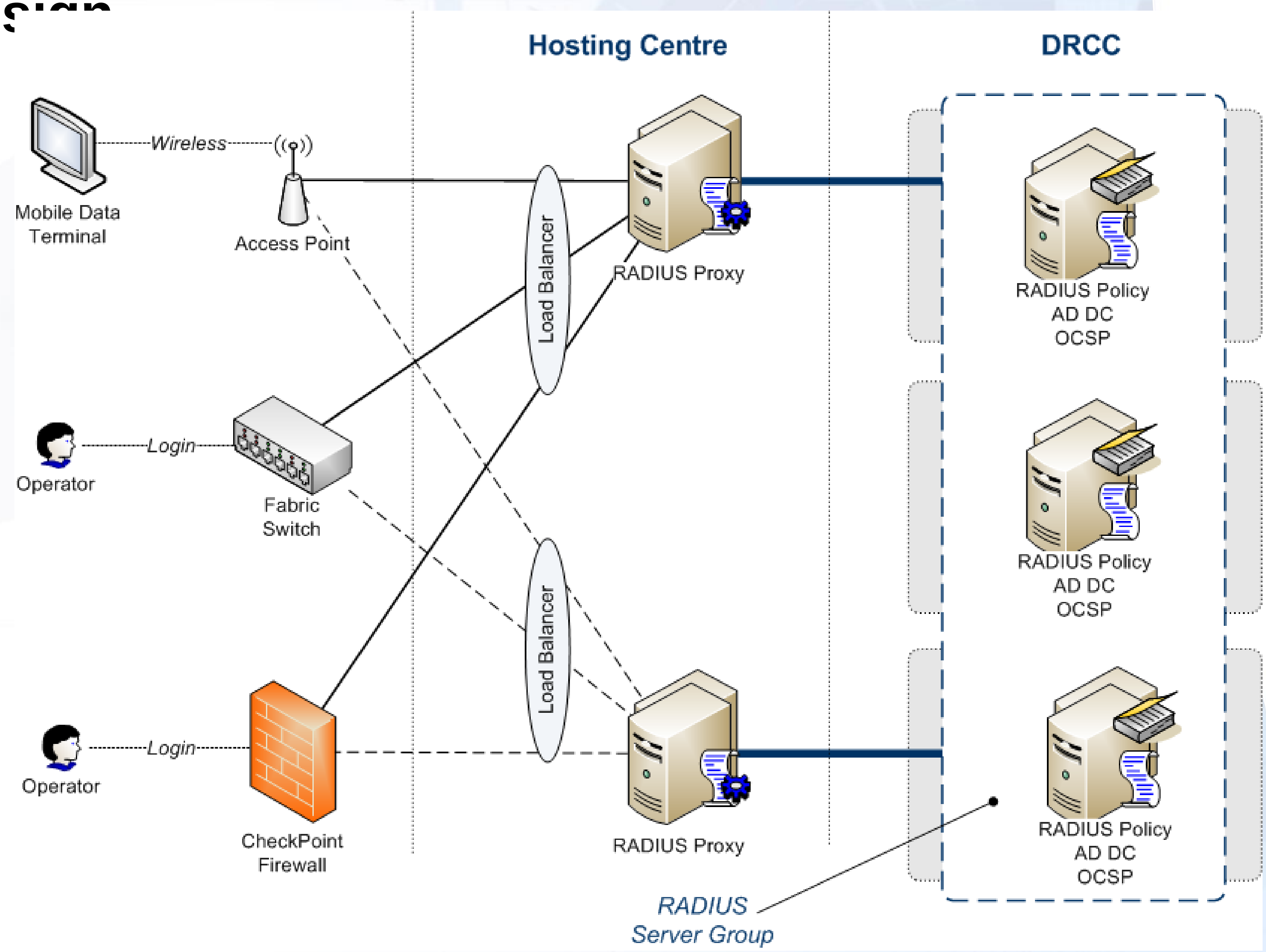
Physical System Design



RADIUS Services - Basics

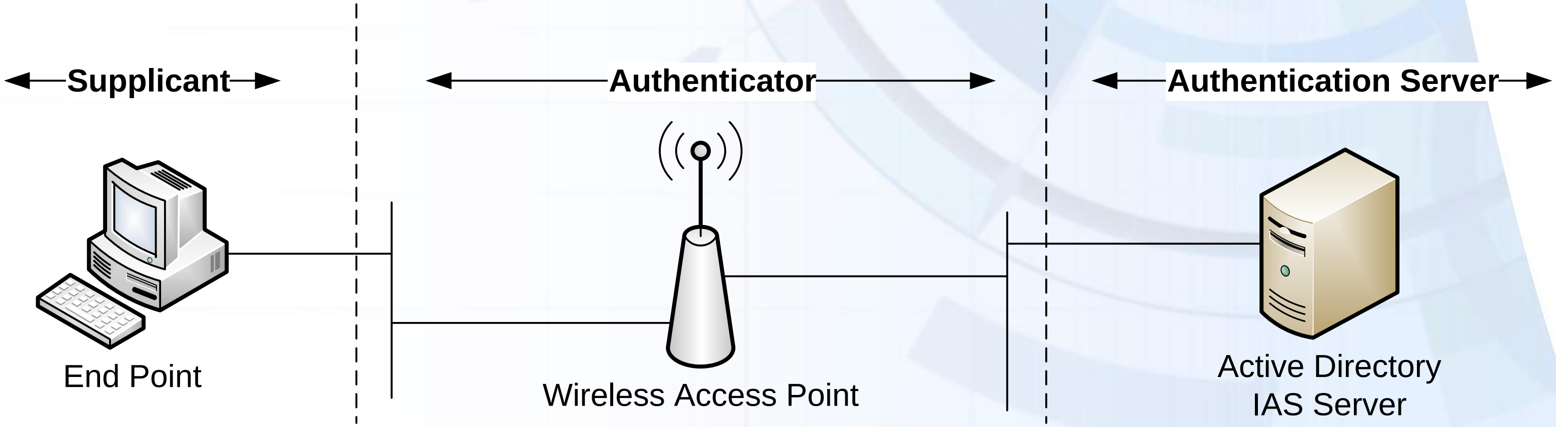
- Provide Authentication and Authorisation Services
  - Authentication is achieved using computer and user accounts in Active Directory
  - Authorisation is achieved by evaluation of remote access policies
- Use the Internet Authentication Service (IAS)
  - Native on the Windows Server platform
  - Leverages Active Directory accounts database
  - Nil licence cost
- Essential for 802.1x Based Authentication

FiReControl Candidate RADIUS Physical Design



IEEE 802.1x Concepts

- Supplicant
  - – MDT / SEPC
- Authenticator
  - – Wireless Access Point / Station End Firewall
- Authenticating Server
  - – RADIUS Server

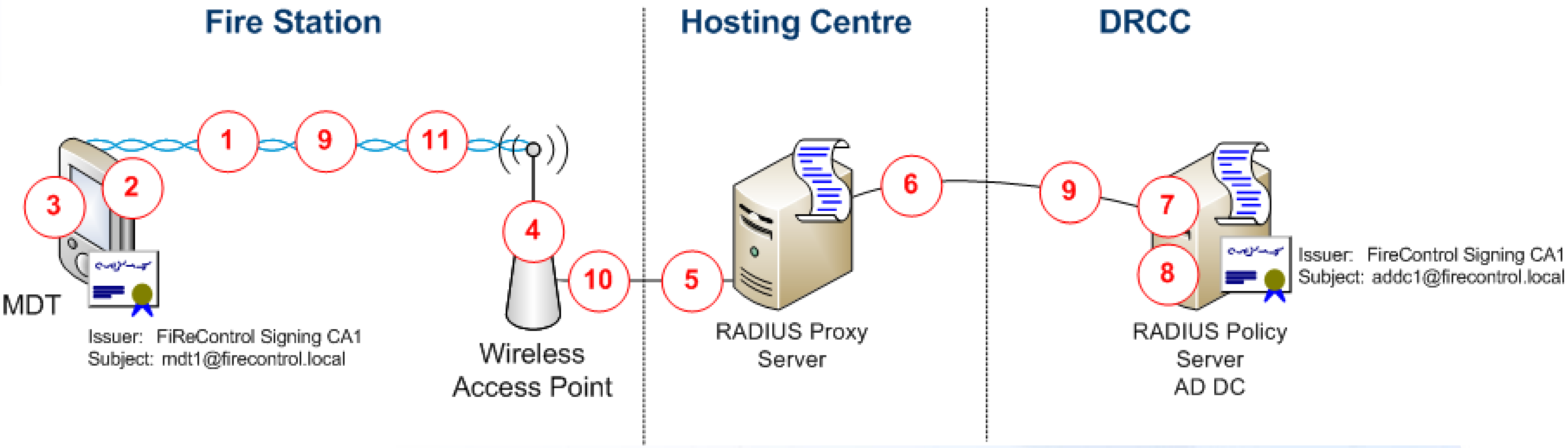


Known Use Cases for Trust Services

- MDT Wireless Authentication
- IPSec Site-to-Site Tunnels
- Web Server Authentication
- AD Integrated Appliance Authentication

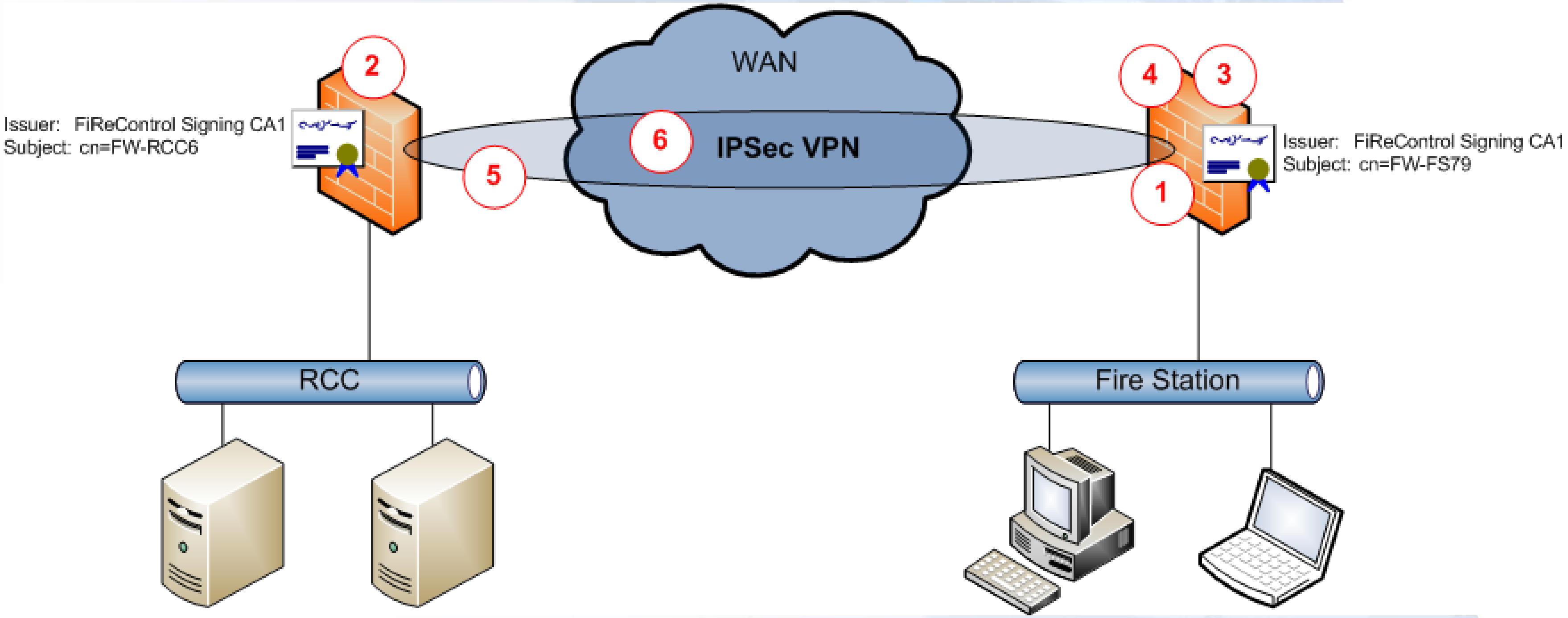
MDT Wireless Authentication

- IEEE 802.1x
- MDT Autoenrolls Certificate from FiReControl PKI
- WiFi Protected Access (WPA)2
  - – Configured by AD Group Policy (ESSID, etc.)


Fire Station
Hosting Centre
DRCC
1
9
11
2
3
4
10
5
6
9
7
8
MDT
Issuer: FiReControl Signing CA1
Subject: mdt1@firecontrol.local
Wireless Access Point
RADIUS Proxy Server
RADIUS Policy Server
AD DC
Issuer: FireControl Signing CA1
Subject: addc1@firecontrol.local

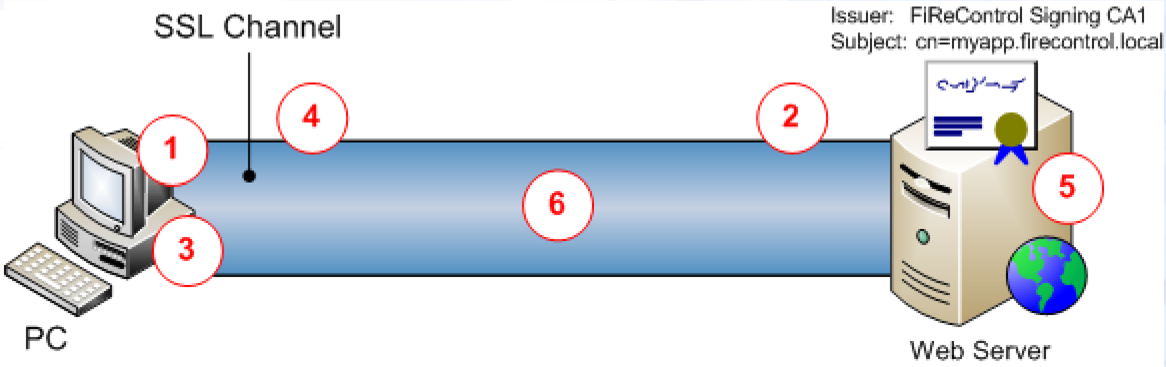
IPSec Site-to-Site Tunnels

- Fire Stations and FRS HQs to SOCs and RCCs
- IKI Peer Authentication



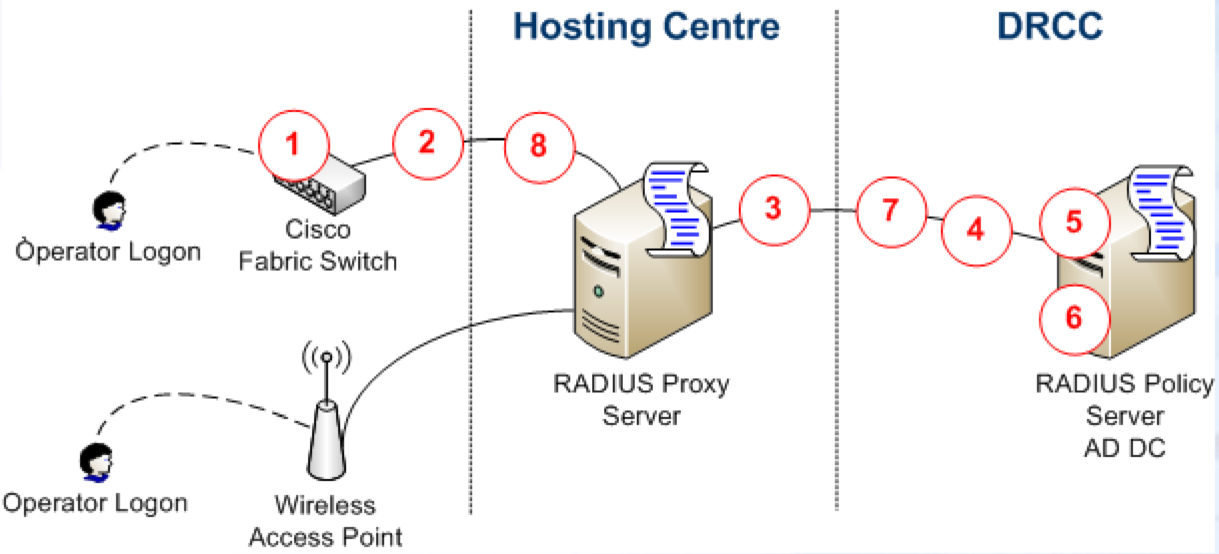
Web Server SSL

- Internal Applications
  - Server-side certificate authentication
- External Applications
  - May be a requirement for *some SSL* using “commercial” PKI providers, e.g. VeriSign


SSL Channel
Issuer: FiReControl Signing CA1
Subject: cn=myapp.firecontrol.local
1
2
3
4
5
6
PC
Web Server

Appliance Authentication via RADIUS

- Operator Access to:
  - Cisco fabric switches
  - Checkpoint firewalls
  - HP wireless access points

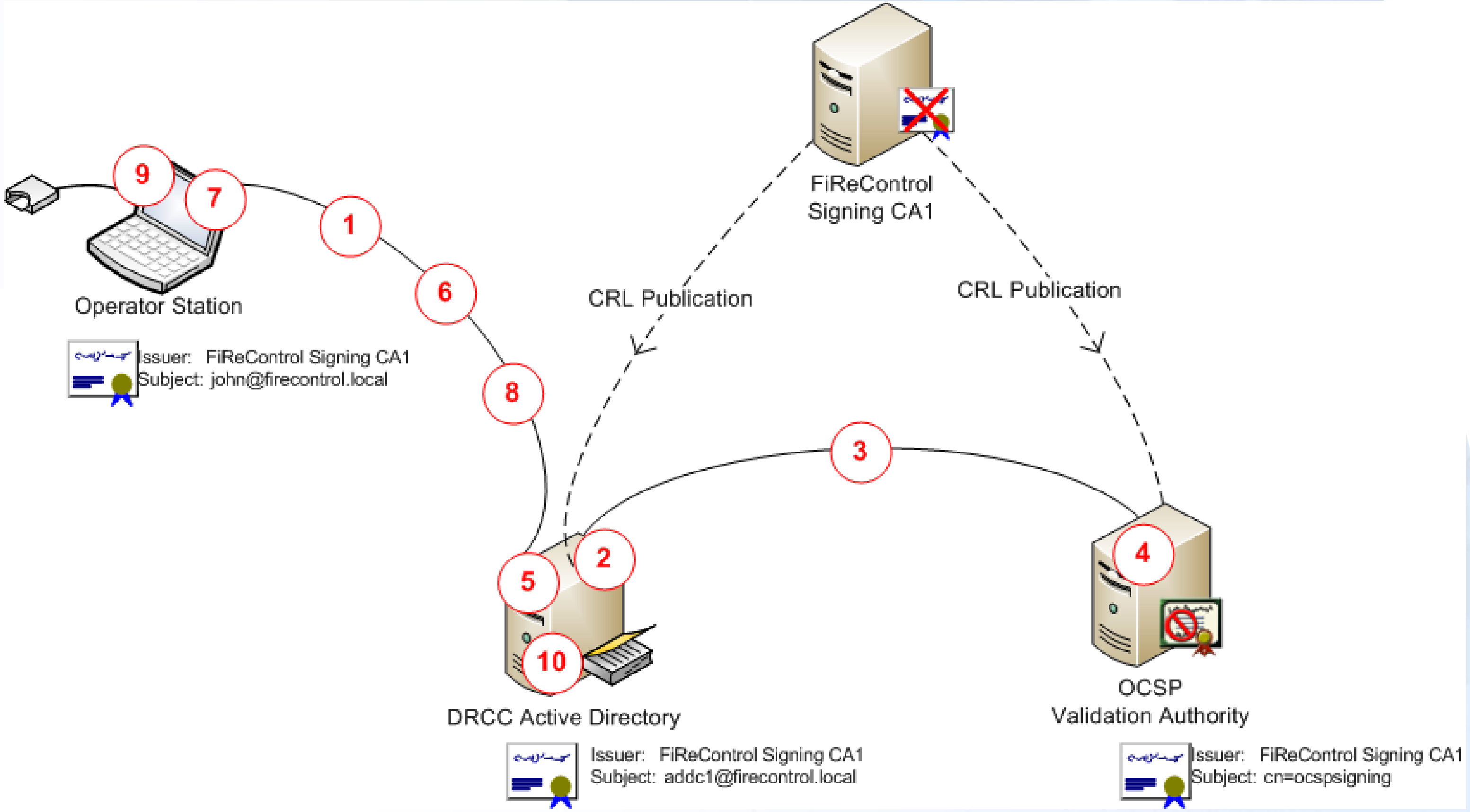


Tentative Use Cases

- Strong Authentication to Windows
- SEPC *Wired* Network Authentication
- Email Message Signing
- Protecting Application Binds to AD
- HTTPS Mutual Authentication
- Remote Access VPN

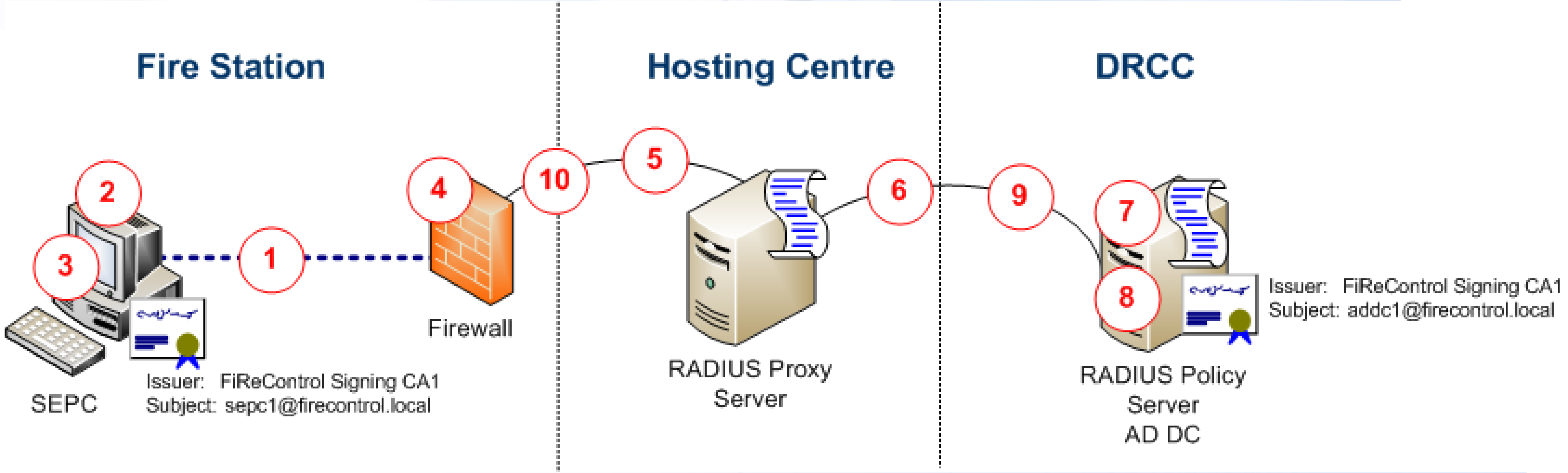
Strong Authentication to Windows

- Two Factor (Smart card) Protected Credentials
  - Smart card management system required
  - Online certificate status protocol (OCSP) becomes important


FiReControl
Signing CA1
9
7
1
6
8
Operator Station
Issuer: FiReControl Signing CA1
Subject: john@firecontrol.local
CRL Publication
CRL Publication
3
2
5
10
4
DRCC Active Directory
Issuer: FiReControl Signing CA1
Subject: addc1@firecontrol.local
OCSP
Validation Authority
Issuer: FiReControl Signing CA1
Subject: cn=ocspsigning

SEPC *Wired* Network Authentication (EAPOL)

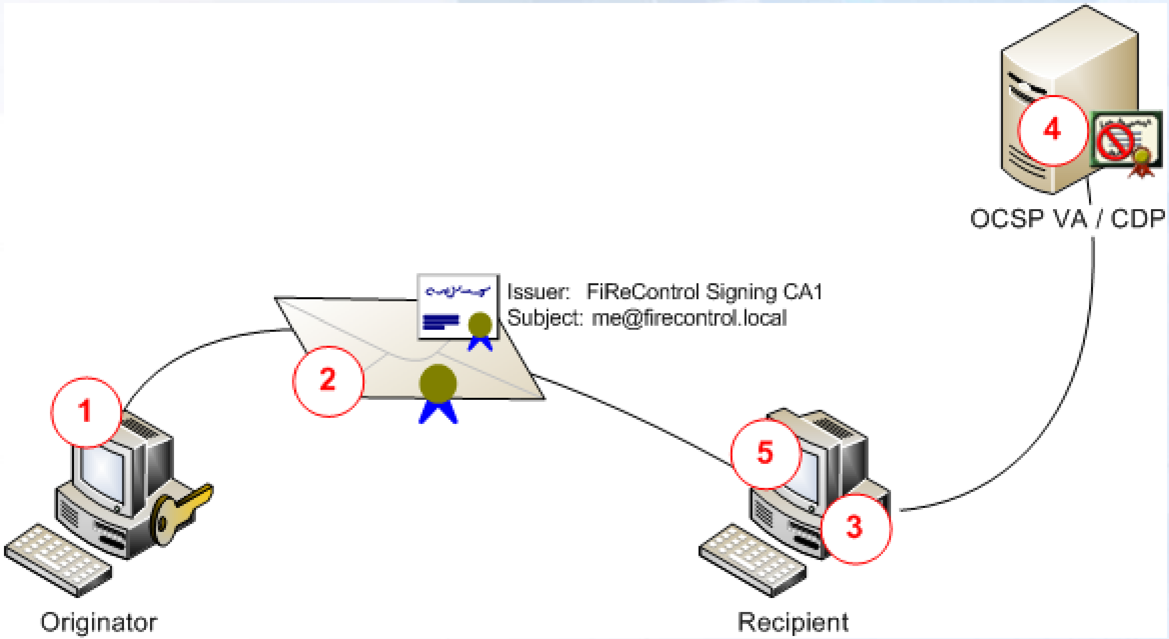
- IEEE 802.1x Authentication
  - Device authentication for PCs at station end
  - Firewall port isn't *activated* until an authenticated connection has been established
  - Prevents rogue PCs being attached to the station end network
    - Combats MAC spoofing, IP address re-use, etc.



Fire Station
Hosting Centre
DRCC
2
3
1
4
10
5
6
9
7
8
Firewall
SEPC
Issuer: FiReControl Signing CA1
Subject: sepc1@firecontrol.local
RADIUS Proxy Server
RADIUS Policy Server
AD DC
Issuer: FiReControl Signing CA1
Subject: addc1@firecontrol.local

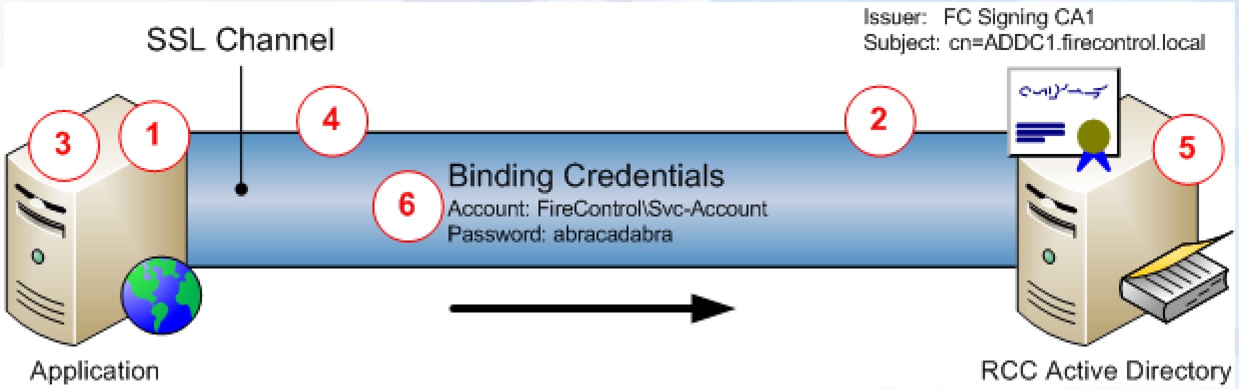
Email Message Signing

- Waiting on Clarification of CCN105
- What it Achives...
  - Recipient can be confident of the message originator and that message hasn’t been modified in transit


4
OCSP VA / CDP
Issuer: FiReControl Signing CA1
Subject: me@firecontrol.local
2
1
5
3
Originator
Recipient

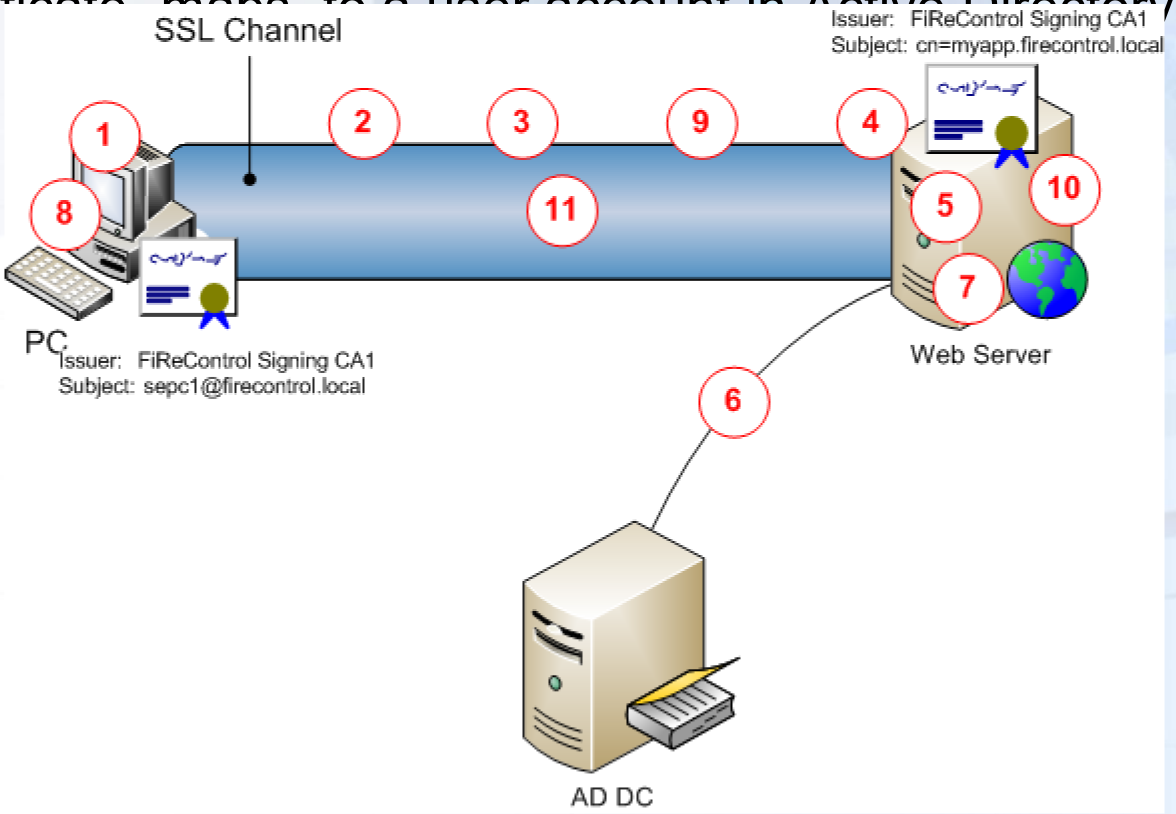
Application Binds to Active Directory

- LDAP Bind over SSL
  - Credentials are transmitted over an SSL channel
- No Applications Identified Yet



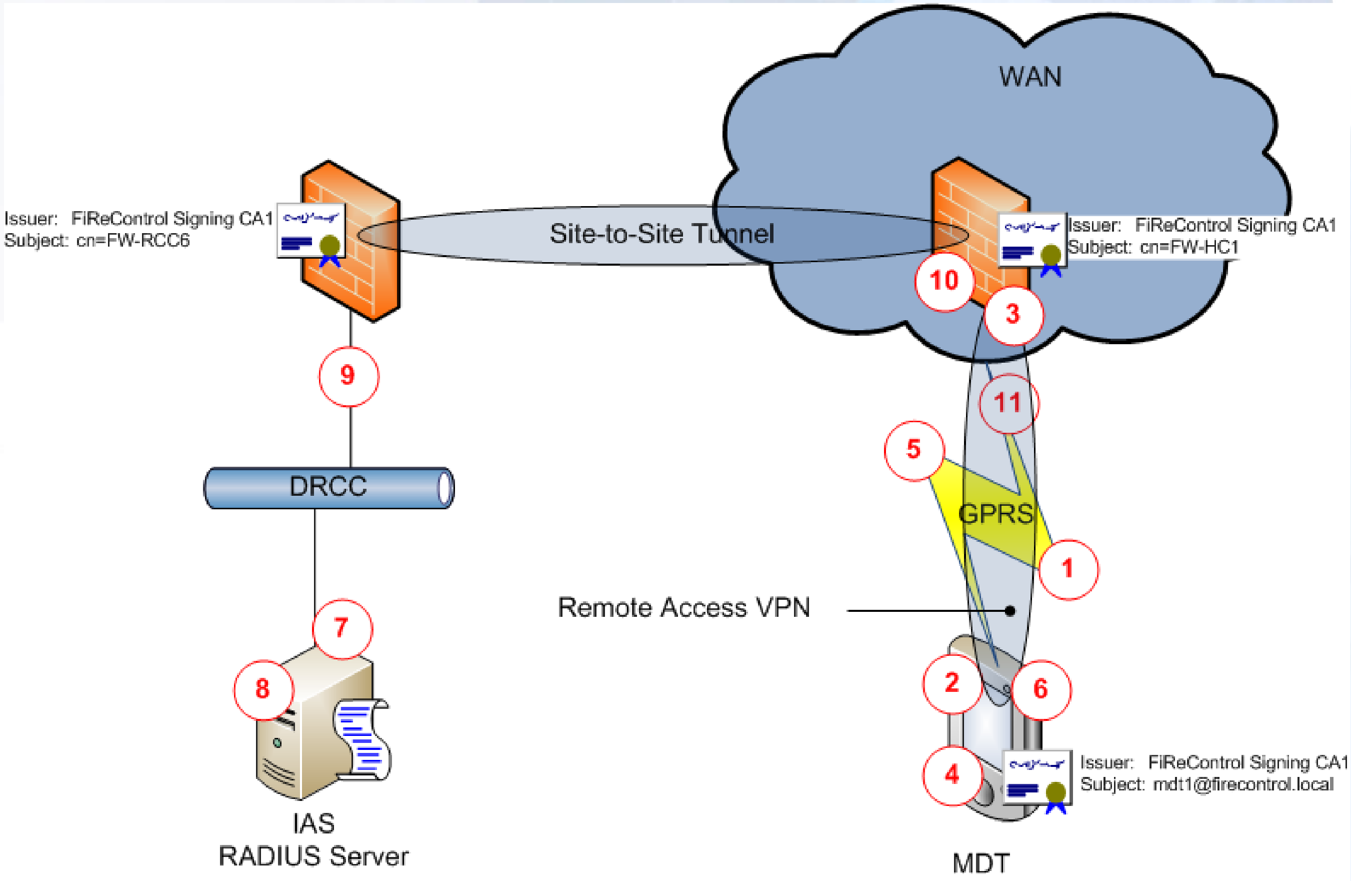
HTTPS Mutual Authentication

- Client User Certificates
  - Certificate is presented to the web server for authentication purposes
  - Certificate “maps” to a user account in Active Directory


SSL Channel
Issuer: FiReControl Signing CA1
Subject: cn=myapp.firecontrol.local
1
2
3
9
4
8
11
5
10
7
PC
Issuer: FiReControl Signing CA1
Subject: sepc1@firecontrol.local
Web Server
6
AD DC

MDT Remote Access VPN

- Make VPN over GPRS connection
  - – Unsure yet of any requirement yet


WAN
Issuer: FiReControl Signing CA1
Subject: cn=FW-RCC6
Site-to-Site Tunnel
Issuer: FiReControl Signing CA1
Subject: cn=FW-HC1
10
3
9
11
5
DRCC
GPRS
1
Remote Access VPN
7
8
2
6
4
Issuer: FiReControl Signing CA1
Subject: mdt1@firecontrol.local
IAS
RADIUS Server
MDT

Wrap Up

- Critical Outstanding Issues
  - Requirement for smart card logon to Windows
  - Understand load balancing solution
  - Where to place IAS proxies
  - Tease out remaining use cases
- Anticipated Other Requirements
  - Mobile code signing?
- Other
  - Important to not focus solely on implementation
    - Ticking time bomb