18 Apr 2007

ABC 2FA NG Mini Workshop

Presentation by David Wozny, EDS Integration Engineering, Security and Privacy

Agenda

- WAMB… Recap
- SSO/2FA… Overview
  - CMS Servers, Load Balancers, HSMs, Databases, VeriSign, Smart Cards, etc.
- 2FA NG… Interim Solution
- 2FA NG… Backstage Pass and Kicking the Tyres
  - CMS Configuration, CMS Repositories, Card Profiles, etc.
  - Demo of card issuance / management

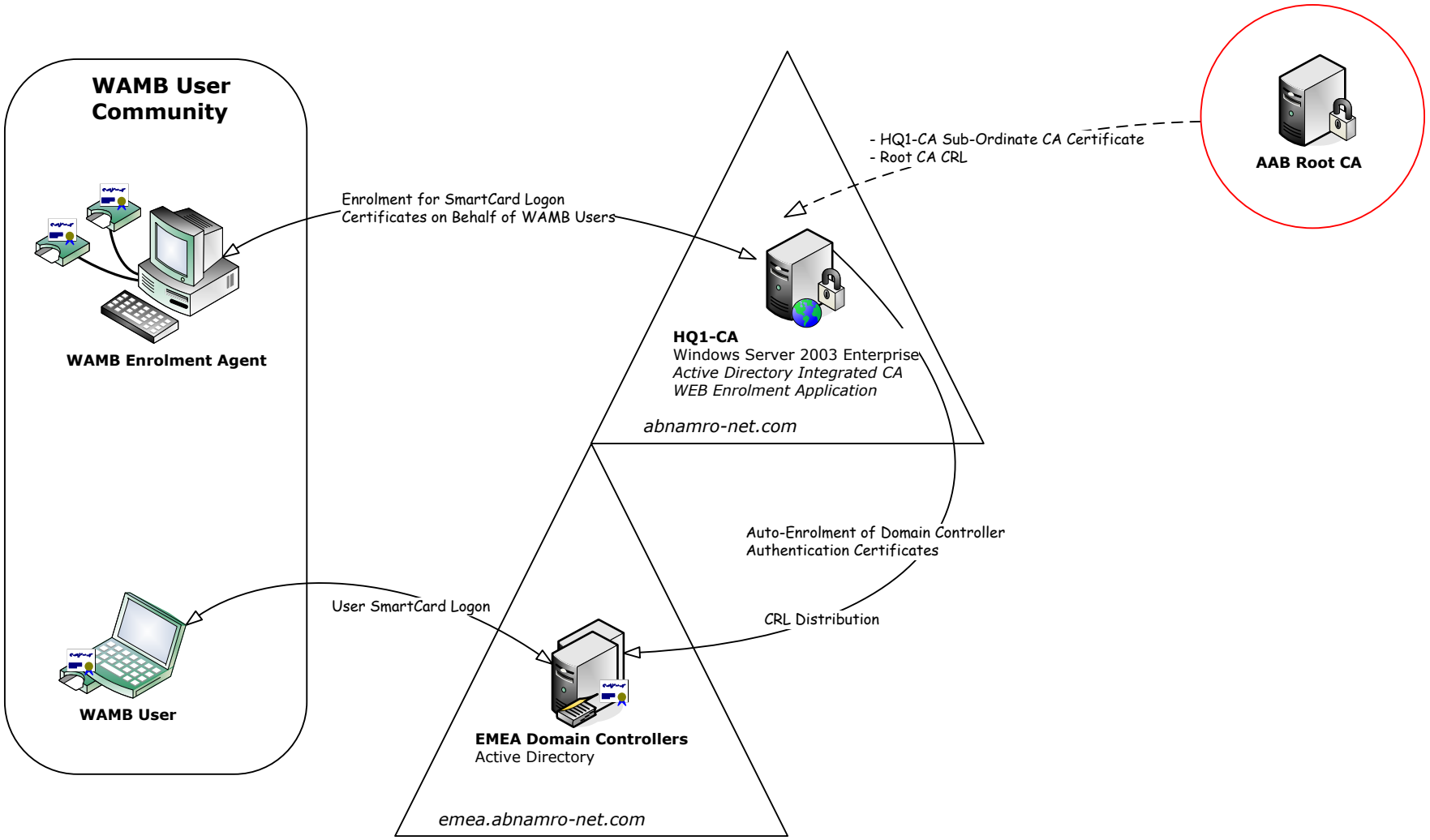
WAMB… Recap

Main Elements

- Smart Card Logon to Windows
  - Microsoft Enterprise CA (*Beneath* ABC Bank Root CA)
  - Basic Smart Card Enrolment Facilities
  - Lack of Sophisticated Smart Card Management
- SafeBoot Device and Content Encryption
- Smart Card Authentication to TTS-RAS Service

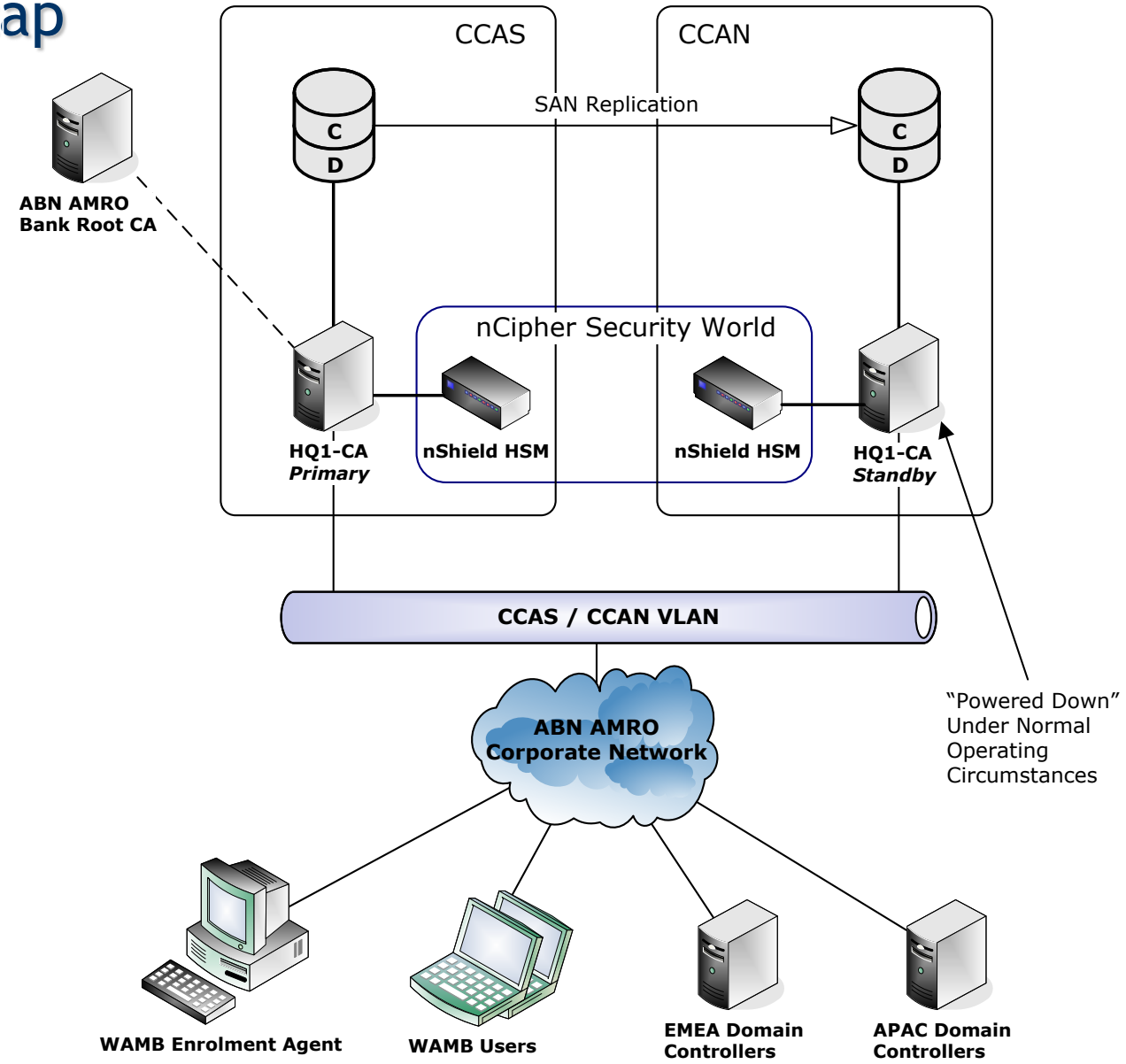
WAMB… Recap

Logical



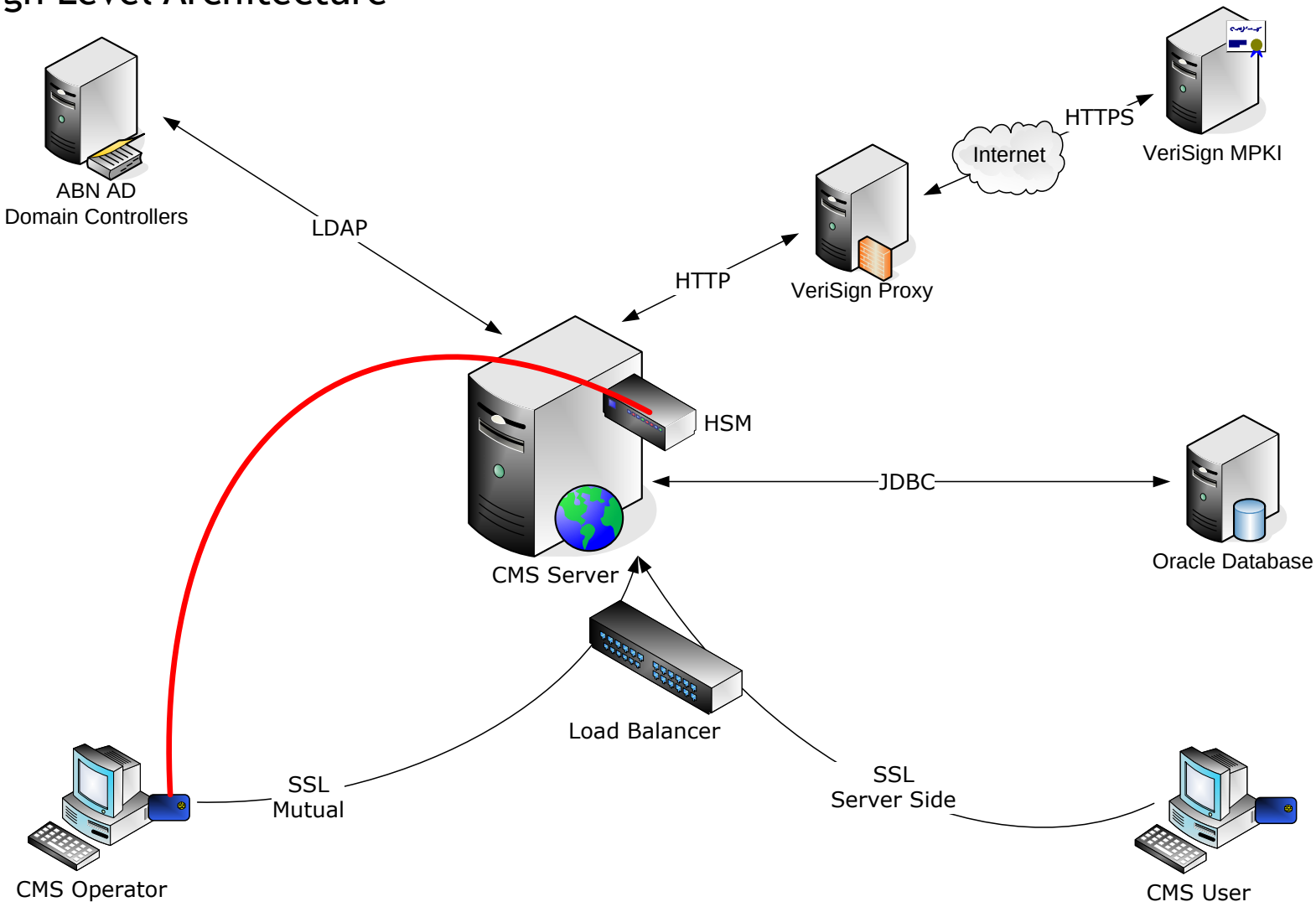
WAMB… Recap

Physical



SSO/2FA... Overview

High Level Architecture



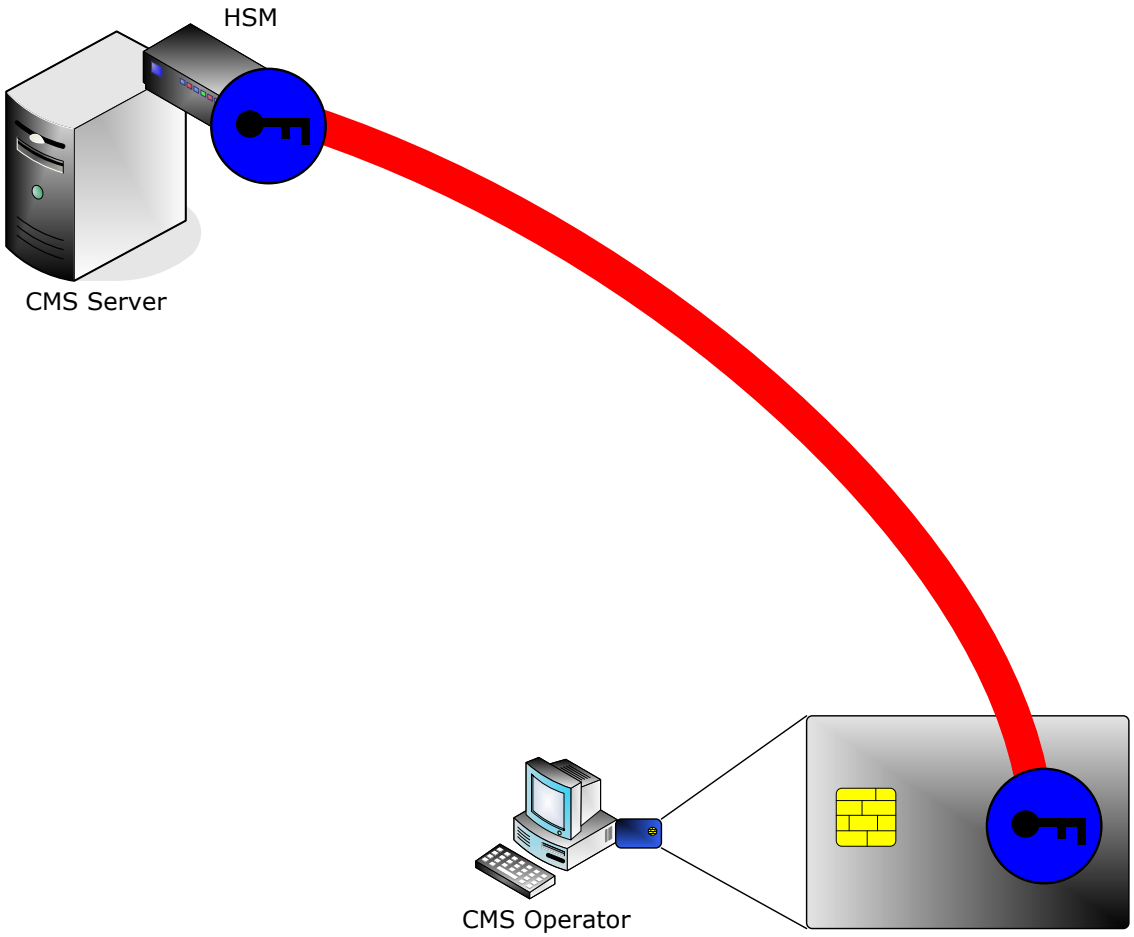
SSO/2FA... Overview

CMS Servers / Peers

- Hosted on Windows Server 2003
  - Running on IIS 6 and TomCat Servlet / JSP
  - Two IIS Web Sites
    - User Portal (server-side SSL auth'n)
    - Operator Portal (mutual SSL auth'n)
- CMS Peering
  - Six Nodes all Participating in a Single Peer Group
  - Peering is Entirely Transparent to the User / Operator
- VeriSign Managed PKI
  - Hosted in VeriSign Facilities in US
  - Access is via the Internet

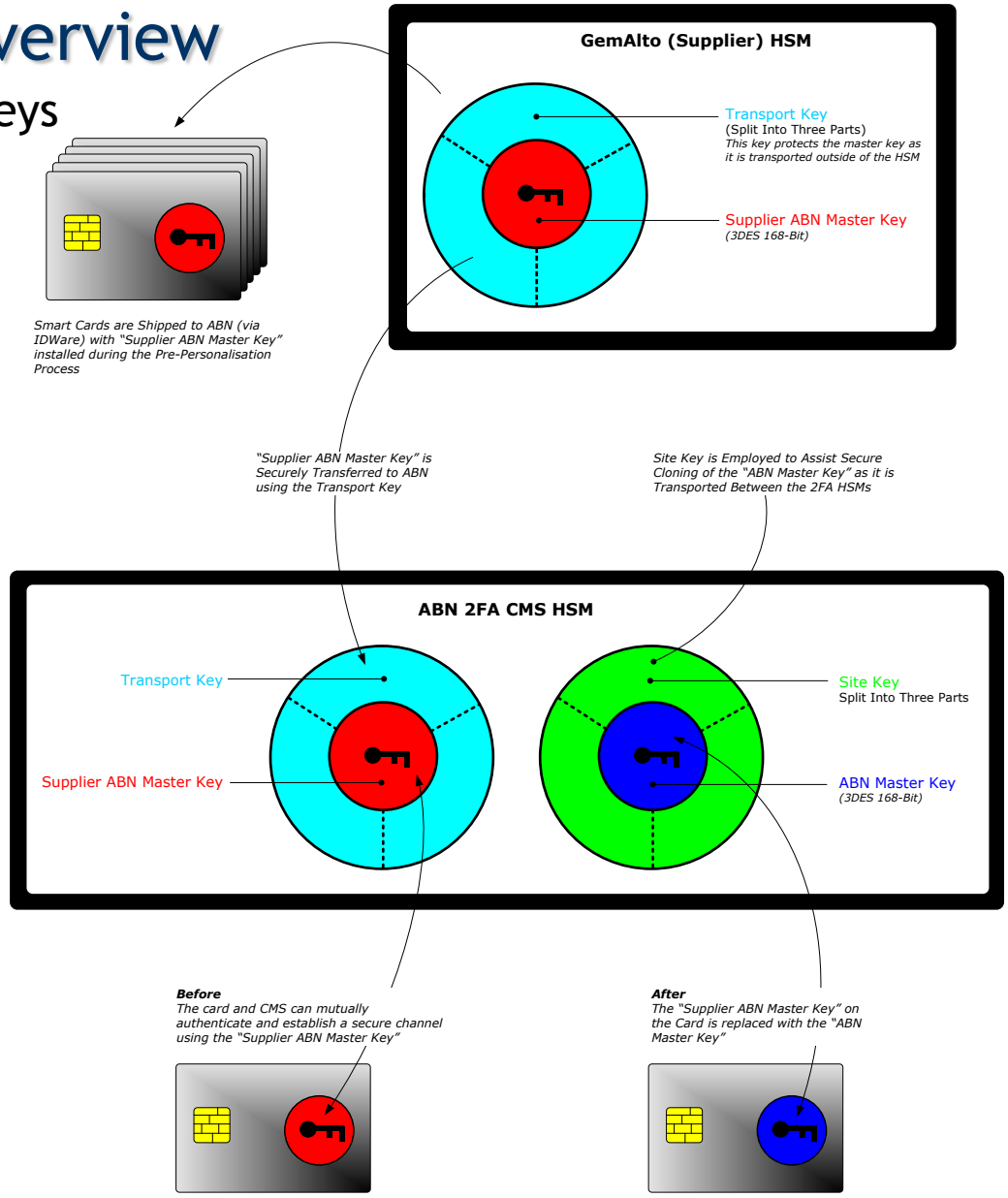
SSO/2FA... Overview

Secure Channel



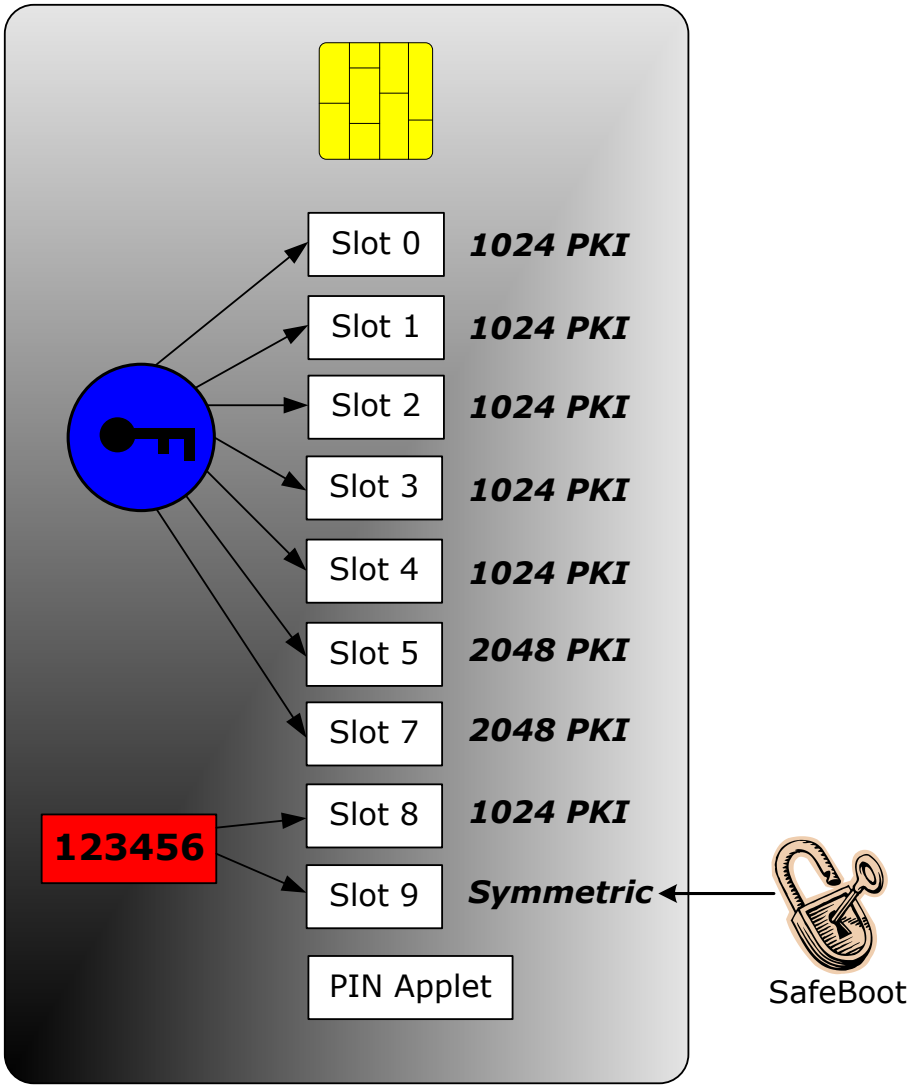
SSO/2FA... Overview

Global Platform Keys



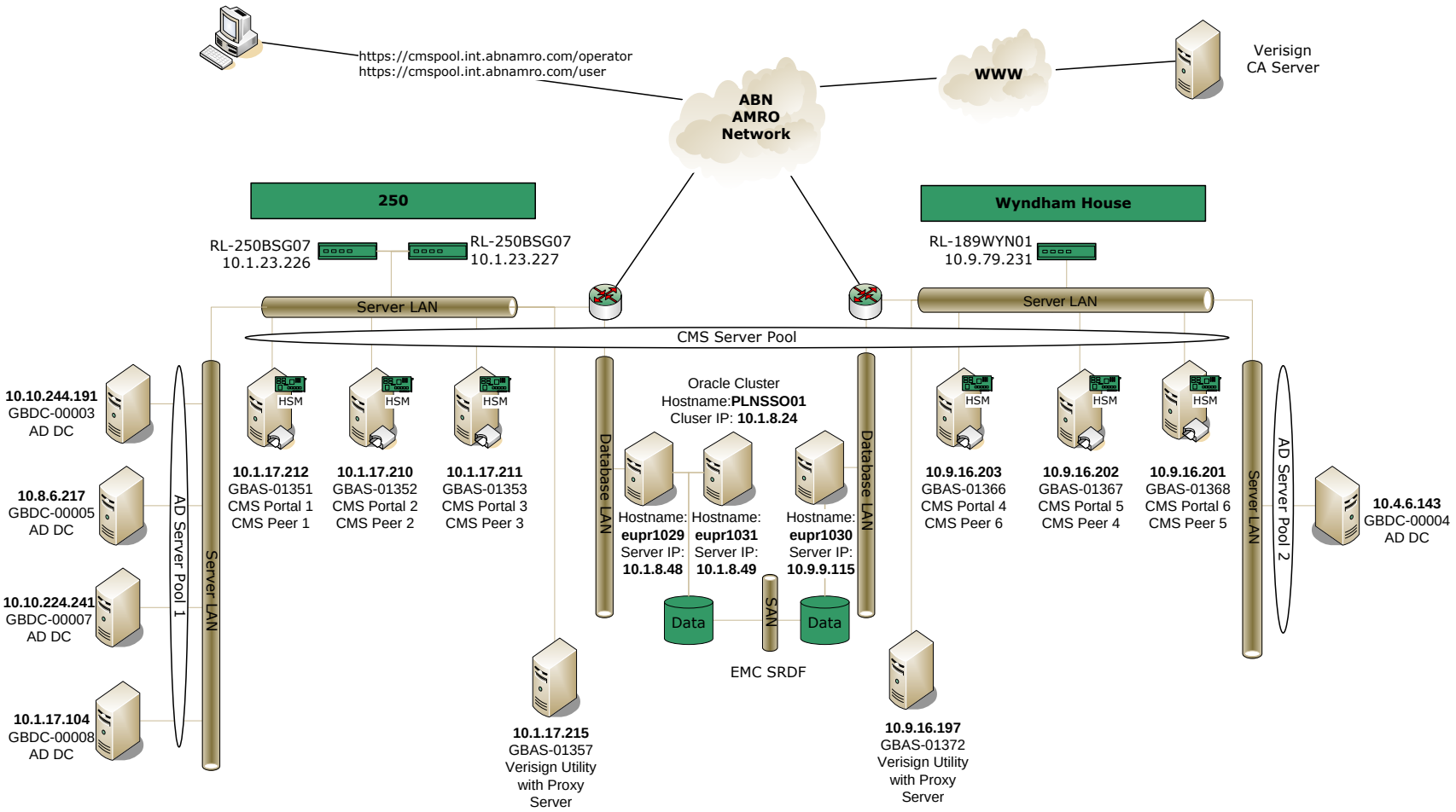
SSO/2FA… Overview

ABN Card Profile



SSO/2FA… How it Works

Technical Architecture



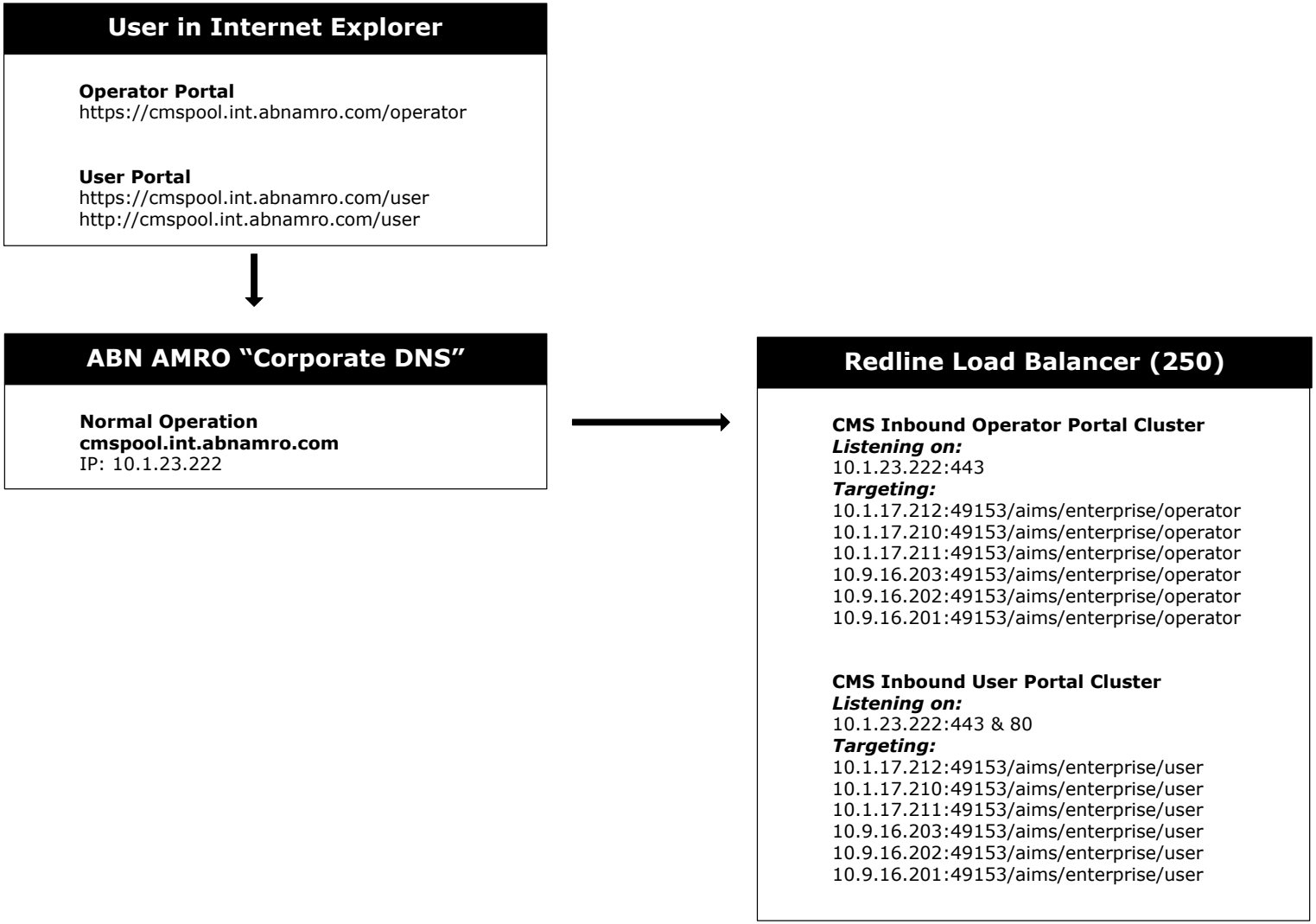
SSO/2FA… Overview

Load Balancing

- Main Load Balancing Groups
  - Juniper (Redline) Hardware Appliances
  - CMS Inbound Connections
  - LDAP Outbound Connections
- CMS Inbound
  - SSL Termination & Re-Direction
  - Listening and Targeting Port 49153
- LDAP Outbound
  - Listening and Targeting Port 636
  - Six DCs Listed as Targets (Different Affinities)

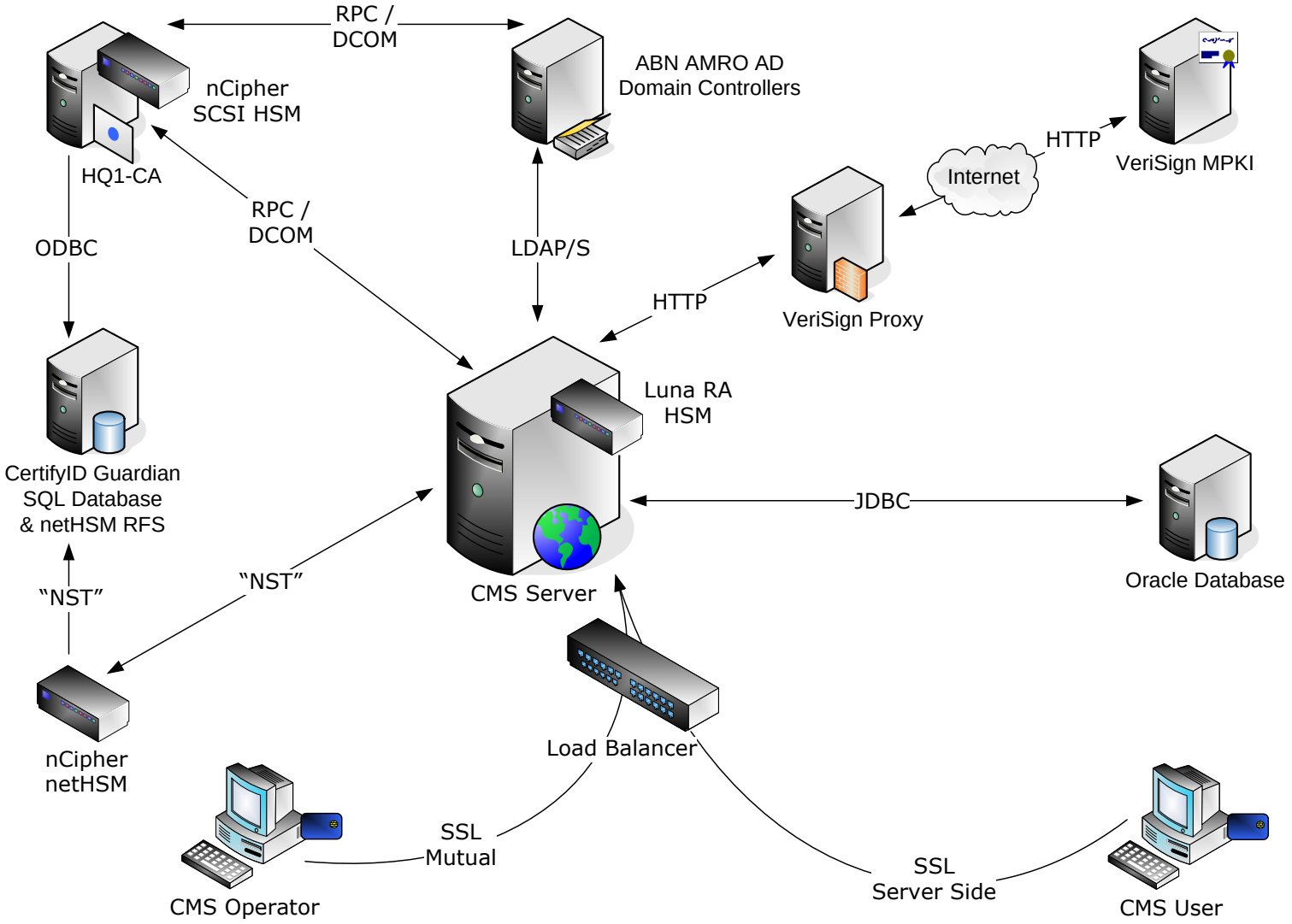
SSO/2FA… Overview

Load Balancing: CMS Inbound



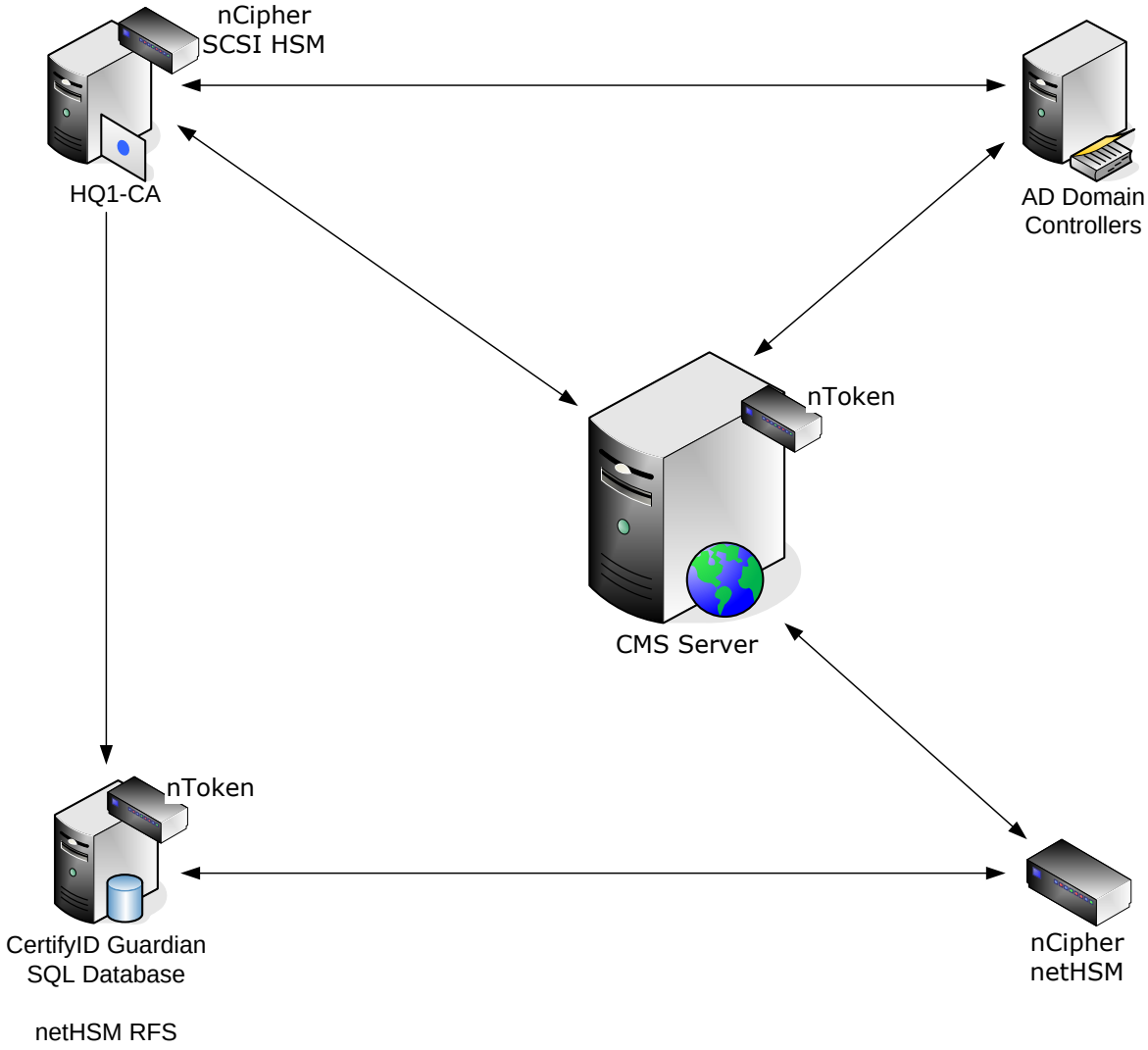
2FA NG… Interim Solution

The Bigger Picture



2FA NG… Interim Solution

The Smaller Picture



2FA NG… Interim Solution

Principal Engineering Areas

- netHSMs
  - Securing of Enrolment Agent Private Keys
- Certificate Orphaning Mitigation
  - SQL Database
- CMS Changes
  - Integration with HQ1-CA
- HQ1-CA Changes
  - Additional Certificate Templates and Controls

2FA NG… Interim Solution

Certificate Orphaning Mitigation

- The Problem
  - After a Restore we get Orphaned Certificates
- The Solution
  - Install Exit Module on the CAs to Publish Issued Certificates to a SQL Database
  - In a Recovery Scenario Orphaned Certificates are Replayed to the CA
  - WISeKey CertifyID Guardian to be Deployed

2FA NG… Interim Solution

CMS Changes

- Setup of New Smart Card Policies
- Integration with HQ1-CA
- Make LDAP Binds Over SSL

2FA NG… Interim Solution

HQ1-CA Changes

- New Certificate Templates
  - EA Certificate Valid for Ten Years
  - User Certificate Valid for Three Years
- New Permissioning

2FA NG… Interim Solution

Why Only Interim

- Doesn’t Provide High Availability in the HQ1-CA

- Full 2FA NG Will Include
  - High Availability in the CA System
  - Improved CRL Freshness… from 7 Days to 1 Hour… *Probably*
  - Revised DR Approach

- However
  - New Bank PKI Strategy to be Published… so who knows?

2FA NG… Interim Solution

Known Issues

- UPN Problems
  - NL Users Have UPN which Matches their LoNo Address
- Controls around Operator Role Usage and Assignment
  - Need Enhancing

2FA NG… Interim Solution

Scope

- Deployment of Infrastructure Capability

- Does NOT Include
  - WAMB Users (& CMS Cannot Issue Multiple Cards to Same Identity)
  - NL Roll Out
  - Fixing UPN Problem

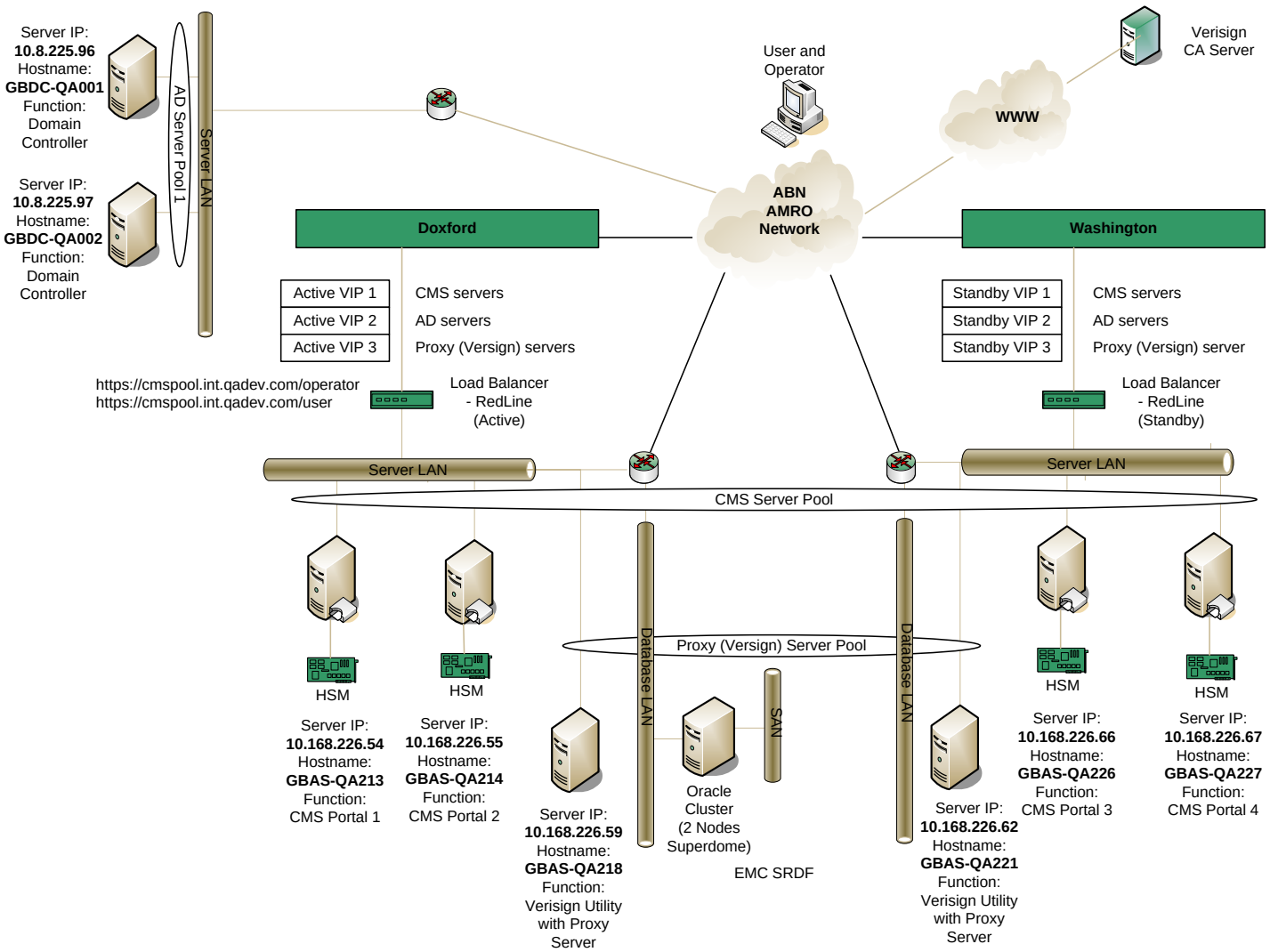
2FA NG… Interim Solution

Catch-Up in Development and QA

- GB Based Dev and QA Networks Extended into Foppingadreef
  - GBDEV.Test
  - EMEA-QADEV.Com

2FA NG… Interim Solution

QA Network



2FA NG… Interim Solution

Dev Network