Microsoft

Windows Server Managing and Supporting Active Directory Certificate Services (ADCS)

Module 03: Planning Two-Tier PKI Hierarchy

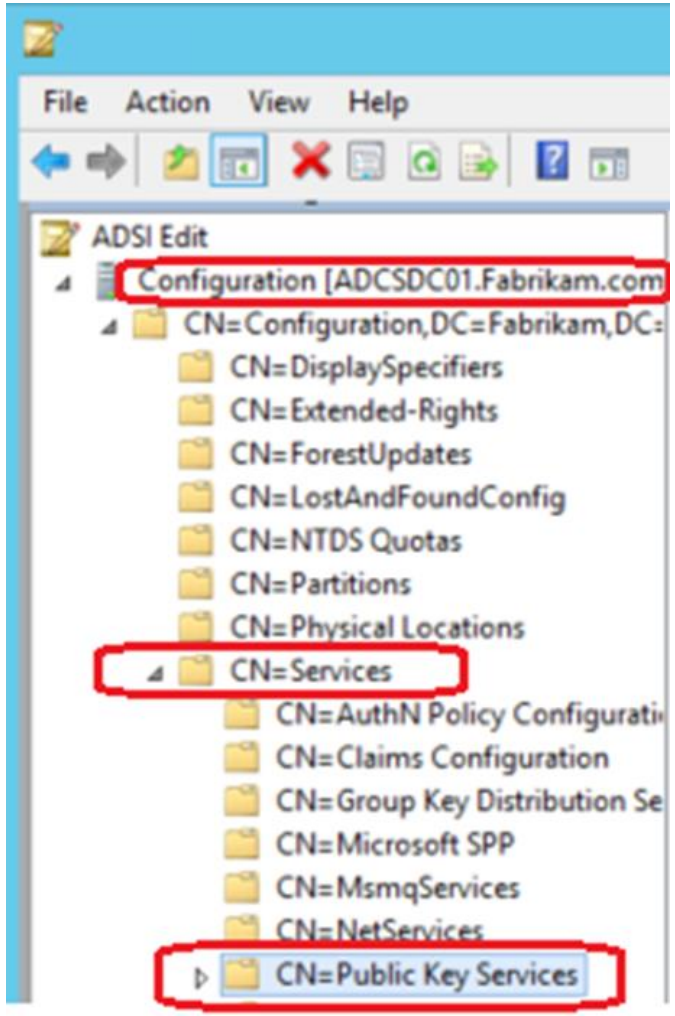
Module Overview

- PKI Objects in AD
- Planning necessary Roles
- Planning ADCS Deployment
  - Design considerations
  - Security Posture
  - Configuration
  - Revocation Infrastructure
  - Availability

PKI Objects in AD

Forest Configuration Container

- A PKI has no relationship to any AD.
- But when installing an AD integrated CA, AD will be used to store PKI related information
- This information can be used by clients



Public Key Services Container in AD

Container Name	Description
AIA (Container)	Contains CA certificates that can be retrieved by clients using the AIA.
CDP (Container)	Contains all base CRLs and delta CRLs published in the forest.
Certificate Templates (Container)	Contains all certificate templates available in the forest.
Certification Authorities (Container)	Certificates contained in this container are downloaded by each member of the forest by the Autoenrollment process.

Public Key Services Container in AD (cont.)

Container Name	Description
Enrollment Services (Container)	For each Enterprise CA there is a corresponding pKIEnrollmentService object in this container. Clients use these objects to request certificates from Enterprise CAs.
KRA (Container)	Contains the certificates for key recovery agents for the forest.
OID (Container)	Contains forest registered OIDs for PKI objects
NTAuth Certificates (Object)	CAs issuing certificates used for authentication (e.g. Smart Card authentication) have to be contained in this object.

Adding related Information to AD Container

AIA

- Will be populated automatically by Enterprise CAs.
- Manual population:

  certutil –dspublish –f <PathToCertFile.cer> SubCA
  certutil –dspublish –f <PathToCertFile.cer> CrossCA

CDP

- Will be populated automatically by Enterprise CAs.
- Manual population:

  certutil –dspublish –f <PathToCRLFile.crl>

Certificate Templates

- Can only be populated by using the Certificate Template Management Tool.

Adding related Information to AD Container (cont.)

Certification Authorities

- Will be populated automatically by Enterprise Root CAs.
- Manual population:

  certutil –dspublish –f <PathToCertFile.cer> RootCA

  (will also populate into AIA)

Enrollment Services

- Will be populated automatically by Enterprise CAs.

KRA

- Will be populated automatically based on the appropriate Certificate Template.

Adding related Information to AD Container (cont.)

OID

- New OIDs should be registered via Certificate Templates MMC snap-in by adding new Application or Issuance (Certificate) Policy in certificate template Extension tab.

NTAuthCertificates

- Will be populated automatically by Enterprise CAs
- Manual population:

  certutil –dspublish –f <PathToCertFile.cer> NTAuthCA

Planning necessary Roles

Common Criteria Roles

Roles	Security Permission	Description
CA Administrator	Manage CA	Configure and maintain the CA. This CA role includes the ability to assign all other CA roles and to renew the CA certificate
Certificate Manager	Issue and Manage Certificates	Approve certificate enrollment and revocation requests
Backup Operator	Back up and restore files and directories	Perform system backup and recovery. Backup is an OS feature
Auditor	Manage auditing and security log	Configure, view and maintain audit logs. Auditing is an OS feature

Planning ADCS Deployment

ADCS Design –

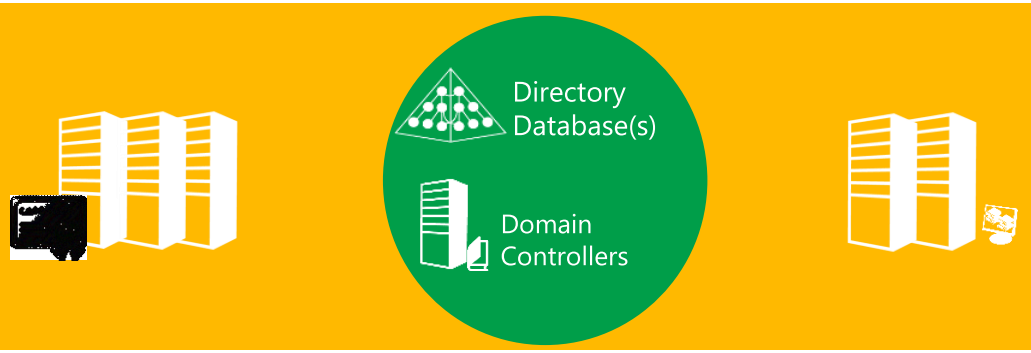
Items to consider (some examples)

- Certificate Use Cases (Certificate Policy)
- Hardware Vs Virtualization
- Azure Vs On-premise
- Hardware configuration – CPU, Memory, Disk etc.
- Hardware Security Module (HSM) – No HSM Vs 3rd party HSM On-Premise Vs Azure Dedicated HSM
- CA Hierarchy and CA Architecture
- No of CA servers/High availability
- Business Continuity and Disaster Recovery
- Credential Tier – Location of each CA server and components
- PKI implementation for Zero Trust – More on this in M05

PKI and Credential Tiering

Tier 0

Identity Store(s)
Active Directory
Identity Services
→ PKI:
Certification Authorities
Auxiliary Services (CES/CEP/OCSP/NDES)



Tier 1

Servers, Apps, Data
PKI:
Auxiliary Services (NDES)
CDPs

Tier 2

Workstations and
Devices

Tier 0

T0 credentials only usable in T0, for T0 (Identity) management tasks

Tier 1

T1 credentials only usable in T1 for T1 management tasks

Tier 2

T2 credentials only usable in T2

PKI and Asset Tiering

Tier 0
Authoritative Services


RootCA


Issuing CAs


NDES


CES/CEP


OCSP

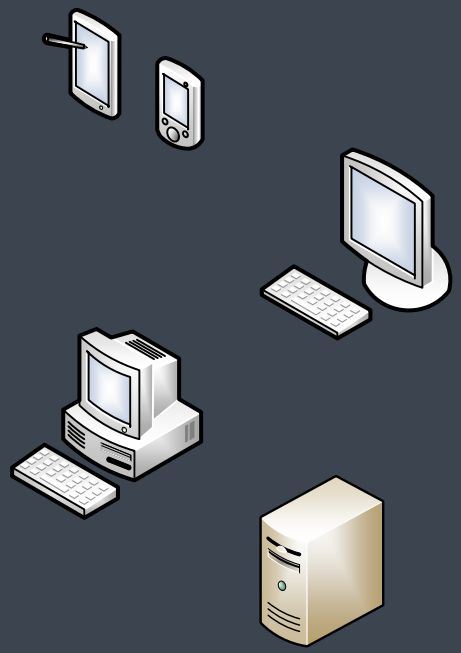
Tier 1
Supporting Services

CDP/AIA


WebServer


NDES

Tier 2
End Entities



Planning ADCS Deployment - HSMs

Azure Dedicated HSM

- Microsoft provides Azure Dedicated HSM service for CA servers (both on-premises and cloud)
- Microsoft uses **SafeNet Luna Network HSM 7** (Model A790 and above) appliance from Gemalto. This device offers the **highest levels of performance and cryptographic** integration options.
- Azure Dedicated HSM is the ideal solution for customers who require **FIPS 140-2 Level 3 and eIDAS Common Criteria EAL4+**validated devices and **complete and exclusive control** of the HSM appliance.
- Azure Dedicated HSM(s) is/are deployed globally across several Azure regions for high availability and as regional-level failover.
- They can also be accessed by on-premises application and management tools using point-to-site or site-to-site VPN connectivity.

Azure Dedicated HSM(s) (Contd.)..

- Customers get the software and documentation to configure and manage HSM devices from Gemalto's support portal.
- Azure Dedicated HSM is most suitable for "lift-and-shift" scenarios that require direct and sole access to HSM devices. Examples include:
  - Migrating applications from on-premises to Azure VMs
  - Migrating applications from Amazon AWS EC2 to virtual machines that use the AWS Cloud HSM Classic service (Amazon is not offering this service to new customers)
  - Running shrink-wrapped software such as Apache/Ngnix SSL Offload, Oracle TDE, and ADCS in Azure VMs
- Azure Key Vault CAN be used as Azure based HSM, but Microsoft does not offer an appropriate KSP. For that you need to look for 3rd Party…

Why Trust Azure Dedicated HSM?

- You have full administrative and cryptographic control over your HSMs. Microsoft has no access to or visibility into the keys stored in them.
- Each HSM device comes validated against **FIPS 140-2 Level 3 and eIDAS Common Criteria EAL4+**, ensuring **tamper resistance**. This enables you to meet a wide variety of security and compliance requirements.
- Microsoft invests more than USD1 billion annually on cybersecurity research and development.
- We employ more than 3,500 security experts completely dedicated to your data security and privacy.
- Azure has more compliance certifications than any other cloud provider:

Planning ADCS Deployment – CA Configurations

ADCS Hierarchy –

Offline Root CA

Items to consider (some examples)

An offline Root CA **must be** truly offline:

- Has never been attached to a network
- Service packs/cumulative updates deployed offline
- No Windows updates, no AV
- Secure location (secured server rack, special virtualization environment…

CA common name and domain membership status cannot be changed without uninstalling CA

- Machine name can be changed during migration

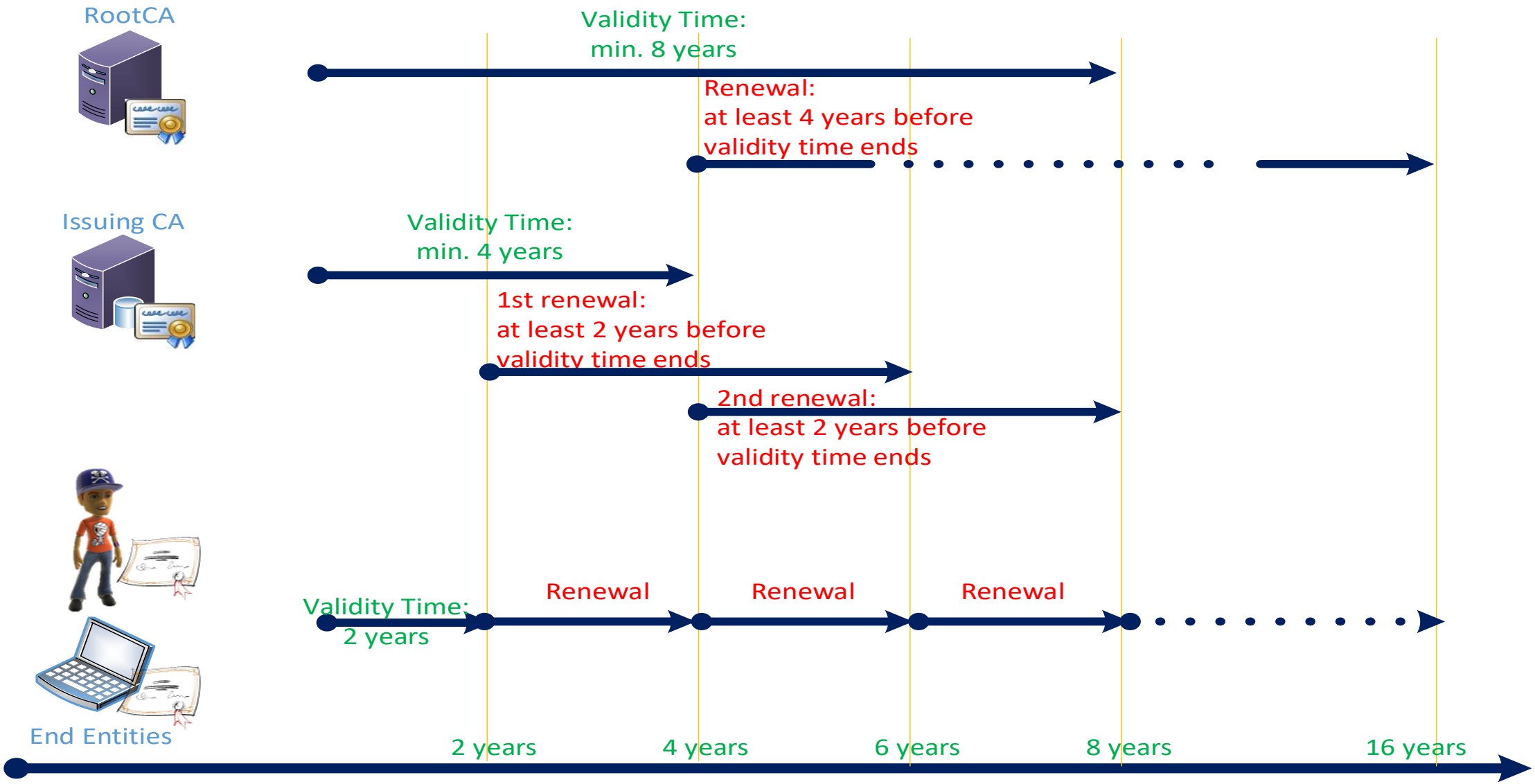
ADCS Configuration Settings –

Items to consider (some examples)

- Certificate Practice Statement (CPS)
- CA Certificate Validity Period
- CA Database and Log file location
- Base, Delta and Overlap CRL validity period
- CDP and AIA locations –
  - Stated and Physical
  - LDAP vs HTTP
  - Internal Vs External
- Leaf certificate validity period
- Password policies
- Auditing – CA auditing and security policy auditing
- Required Certificate Templates

Planning ADCS Deployment – CA Hierachies and Lifecycle

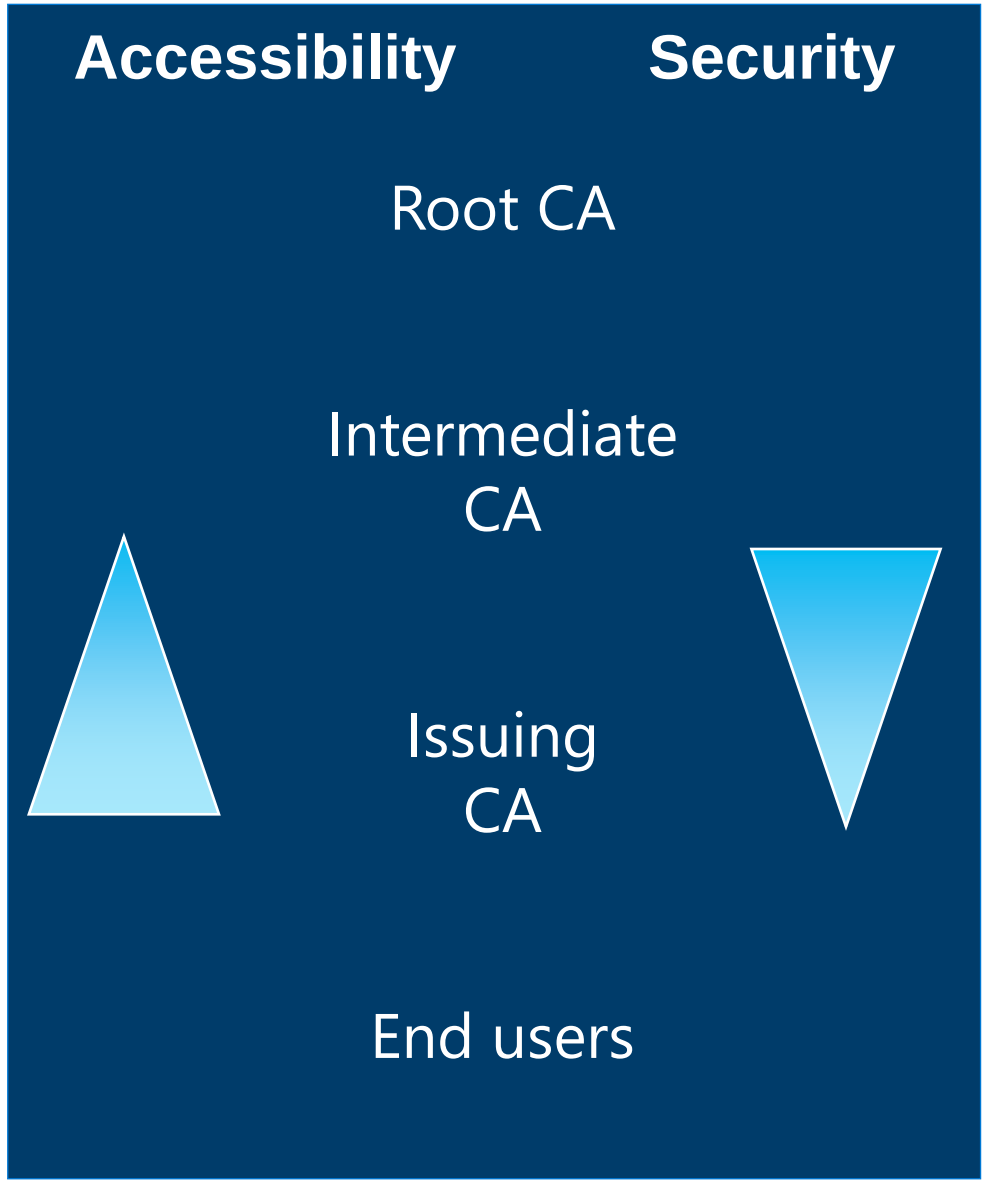
CA Lifetime Planning



CA Security vs. CA Access

- Root CAs
  - Most trusted certificate
  - Best security
  - Least accessibility

- Others
  - With distance from root
  - Decreasing security
  - Increasing accessibility



CA Security and Key Length

- Root CAs
  - Most trusted certificate
  - Should run on the maximum security level with the highest key length possible and supported by clients (e.g. RSA 4096 or ECC 512 and SHA2)

- Issuing or subordinate CAs
  - Should focus on the planed security level (ideally, based on a security needs assessment)
  - Can use DSA or RSA (if RSA then key size 4096bit is recommended)
  - *But* must orientate at the necessary compatibility level that applications or hardware is able to support

Planning ADCS Deployment – Revocation Infrastructure

Defining Revocation Configuration URLs – CDP

LDAP CDP:

- Default

  ldap:///CN=%7%8,**CN=%2**,CN=CDP,CN=Public Key Services,CN=Services,%6%10

- Alternative:

  ldap:///CN=%7%8,CN=FabrikamCorporatePKI,CN=CDP,CN=Public Key Services,CN=Services,%6%10
  (replacing **CN=%2** with an independent container name)

HTTP CDP:

- Default

  http://**%1**/CertEnroll/%3%8%9.crl

- Alternative:

  http://pki.fabrikam.com/CertData/%3%8%9.crl

Defining Revocation Configuration URLs - AIA

LDAP AIA:

- Default

  ldap:///CN=%7,CN=AIA,CN=Public Key Services, CN=Services,%6%11

- Will not be changed!

HTTP AIA:

- Default

  http://**%1**/CertEnroll/**%1**_%3%4.crt

- Alternative:

  http://pki.fabrikam.com/CertData/%3%4.crt

CDP URL Attributes

RootCA:

AddToCertCDP (do we want root CA CRL in AD?)

- *ldap:///CN=%7%8,CN=FabrikamCorporatePKI,CN=CDP, CN=Public Key Services, CN=Services,%6%10*
- *http://pki.fabrikam.com/CertData/%3%8%9.crl*

CDP URL Attributes (cont.)

IssuingCA:

ldap:///CN=%7%8,CN=FabrikamCorporatePKI,
CN=CDP,CN=Public Key Services,
CN=Services,%6%10

- PublishToServer
- PublishDeltaToServer
- AddToCertCDP
- AddToFreshestCRL

http:// pki.fabrikam.com/CertData/%3%8%9.crl

- AddToCertCDP
- AddToFreshestCRL

AIA URL Attributes

RootCA:

AddToCertCDP

- *ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11*
- *http://pki.fabrikam.com/CertData/%3%4.crt*

AIA URL Attributes (cont.)

IssuingCA:

ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11

- PublishToServer
- AddToCertCDP

http://pki.fabrikam.com/CertData/%3%4.crt

- AddToCertCDP

ADCS Strategies

– Items to consider (some examples)

- Monitoring
- Security Controls – Technical, Physical and Process
- Revocation
- Backup and Restore
- Decommissioning (if applicable)
- Documentation
- Windows update
- ADCS Management and Administration

Planning ADCS Deployment - Availability

Planning for High Availability

Good resilience to failure and ensuring that in the event of failure of any part of your Public Key Infrastructure (PKI) is vital for productivity. Recover should be done in a timely manner and with as little effect to the organization as possible.

2 available options:

- semi redundant

- fully redundant

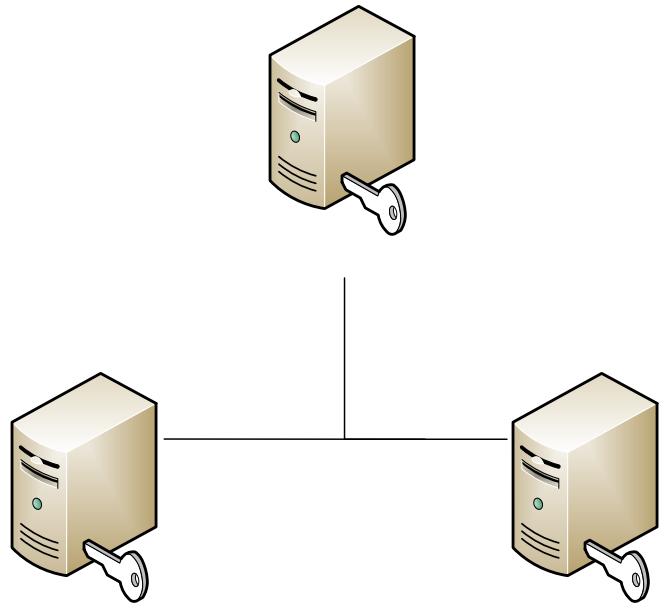
Semi redundant

2 separate issuing CA with the same templates published

Database #1

Private key #1

CRL #1



Database #2

Private key #2

CRL #2

Contoso Issuing CA 1
Published templates:
-Contoso VPN
-Contoso User
-Contoso WebServer

Contoso Issuing CA 2
Published templates:
-Contoso VPN
-Contoso User
-Contoso WebServer

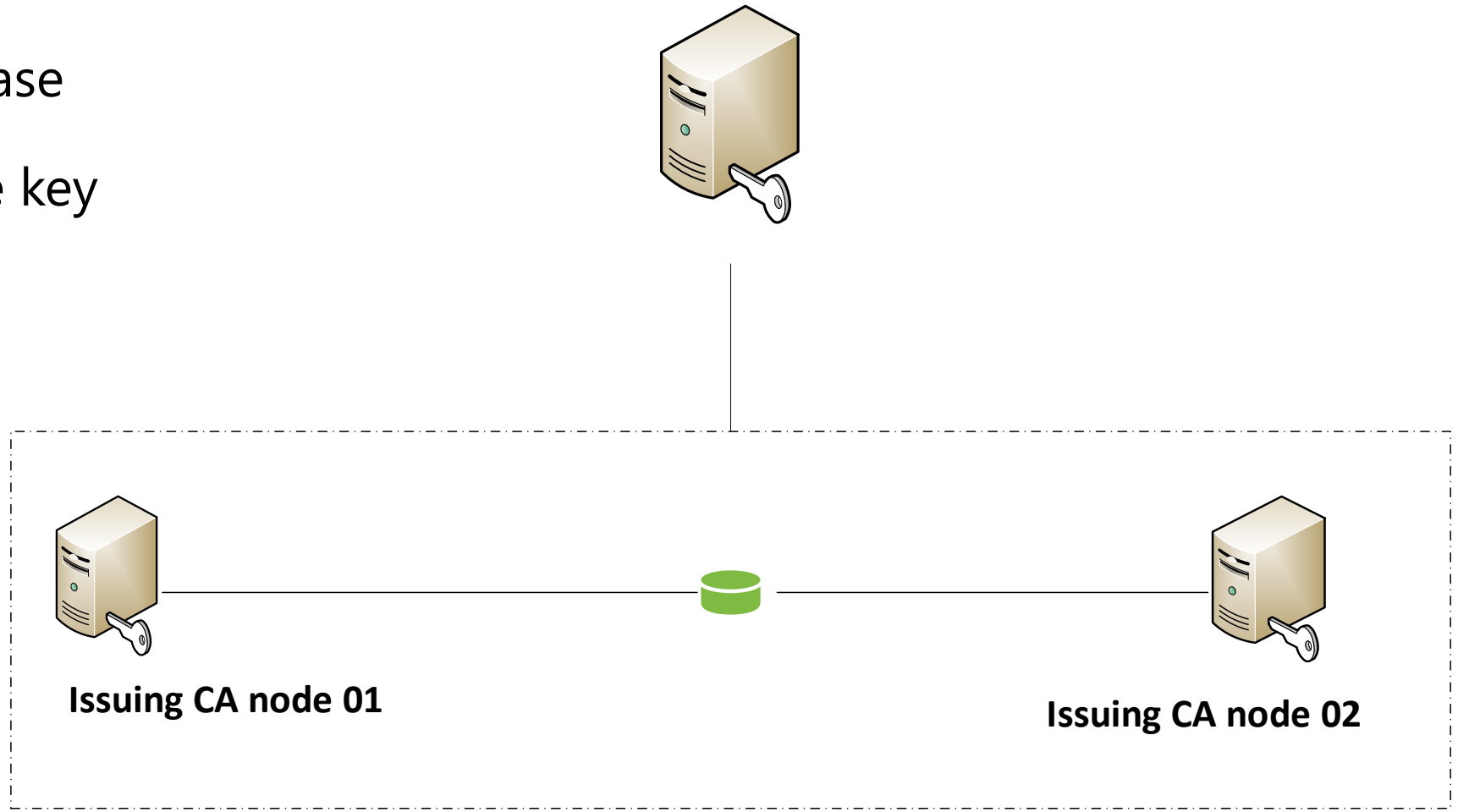
Fully redundant

One issuing CA clustered using Windows Failover Clustering

One Database

One Private key

One CRL



Planning for High Availability

Planning for a highly available PKI involves thinking of the following when designing the solution:

Hardware	Software	Processes
Redundant issuing Certificate Authorities (CAs)	Virtualization	Recovery procedures
Hardware selection	Clustering (Fail-over and Network Load Balancing (NLB))	Recovery contingency
Resilient disk layout	Built-in HA logic for CEP/CES	Testing and change procedures
Cold standby	Redundancy for Certificate Revocation List (CRL) and Authority Information Access (AIA)	
Hardware Security Module Availability	CRL overlap and extended validation period	

Module 3:

Planning a PKI Deployment

Microsoft

Contact

(800) 123-4567

www.microsoft.com/microsoftservices