Global Information Assurance Certification Paper

Implementing Public Key Infrastructure Using Microsoft Windows Server 2012 Certificate Services

GIAC (GSEC) Gold Certification

Author: Michael Naish, mnaishjr@gmail.com
Advisor: Rob VandenBrink

Accepted: September 13th, 2014

Abstract

Public Key Infrastructure (PKI) is a critical application that provides confidentiality and integrity to the Enterprise and its Customers. Microsoft Windows Server 2012 Certificate Services is a capable solution that creates a high assurance PKI, but there are many design decisions to make before implementation. By understanding prerequisites and configuration options, an organization can quickly develop a strategy to construct a PKI that meets its assurance needs. A clear strategy will shorten implementation time and reduce errors due to insufficient planning. This paper explains the critical prerequisites in addition to the configuration steps for a rapid deployment of Microsoft Windows Server 2012 Certificate Services.

1. Introduction

Public Key Infrastructure (PKI) can be distilled into two critical parts: a public and a private key. Keys use asymmetric encryption algorithms to ensure that the encryption only works 'one way' (Hirsch). Each key in a public/private pair can be used to encrypt (or decrypt) data that only the corresponding key in the pair can decrypt (or encrypt) (Hirsch). Asymmetric encryption is considered to be slower than symmetric encryption, but it is more secure (Mircosoft, 2007). The same key cannot be used to reverse the encryption (Hirsch). By contrast, asymmetrical encryption is often used in the exchange of symmetrical keys (The SANS Institue, 2013).

The term 'PKI' is intended to be an inclusive term…one that includes all of the major parts required to create assurance or a chain of trust. PKI is designed with the intention to create, manage, distribute, store, and revoke digital certificates through a set of hardware, software, user roles, policies, and procedures (Hirsch). The primary uses of a PKI are to provide a chain of trust that can be used to authenticate a server or user, construct a secure connection between two end points, validate the integrity of software, data, or a document, or to encrypt/decrypt/sign email messages (Hirsch).

A certificate differs from a PKI in that a certificate is a digitally signed electronic document bound to a publically accessible key. It contains information regarding the origin of issuance (Microsoft, 2005). Information contained within the certificate allows a user to know the name of the entity that issued the certificate and their contact information, as well as a being able to validate the signatures of the Certificate Authorities within the chain of trust (Microsoft, 2005). The certificate provides validation to the end user that the computer or person with whom they are communicating can be trusted (Microsoft, 2005).

Certificates are issued to be valid for specific lengths of time (Microsoft, 2005). The validity period can range from a few days to many years and is dependent on the certificate template configuration. Once the validity period expires, the certificate is no longer valid and is revoked by the Issuing Certificate Authority (Microsoft, 2005). A Certificate Revocation List (CRL) is published by the Certificate Authority to provide an

accessible list of revoked certificates (R. Housley, 2002). CRLs also have a validity period defined by the Certificate Authority and are a necessary part of the chain of trust (R. Housley, 2002).

PKIs can be described in terms of hierarchical roles and levels of assurance. The predominant hierarchical roles of Certificate Authorities are Root Certificate Authority (Root CA) and Subordinate Certificate Authority (Intermediate or Issuing CA) (Pyle, Designign and Implementing a PKI: Part I Design and Planning, 2009). Each role has varying configuration options, dependencies, and requirements to ensure that confidentiality, integrity, and availability are maintained (Microsoft).

Assurance indicates a specific level of trust and can be described as Level 1 to Level 4, in terms of consequence to the CA (William E. Burr, 2011). The definitions applied to assurance levels directly correlate to the sensitivity of environment that is to be secured. Highly sensitive environments (Level 4; production, externally facing) would have a high assurance level and correspondingly rigorous practices that maintain a high level of confidentiality and integrity (William E. Burr, 2011). Low assurance environments (Level 1; non-production, internal customers only) require less rigor and assurance as a result of that which they are in place to secure (William E. Burr, 2011).

Root CAs are the first and most important role within a PKI. Root CAs are the trusted foundation upon which a PKI is built. A Root CA will be trusted by all other Certificate Authorities within the same PKI instance (Pyle, Designign and Implementing a PKI: Part I Design and Planning, 2009). This makes the security practices and procedures used to manage Root CAs critically important to the trustworthiness of certificates issued by the PKI.

Root CAs are often recommended to be built as standalone and offline (Microsoft, 2014). The best practice is to use a hardware security module (HSM) to store the private keys, as this results in enhanced security and logging surrounding the private keys of a CA (Microsoft, 2014). This prevents unauthorized access to the private keys, provides logging for key access, and allows them to be stored online for easy retrieval (Roginsky, 2011). This is most often seen in a large enterprise installation due to high capital expenditure. Small to medium organizations might employ an alternative combination of

hardware and physical controls to provide similar assurance provided by an HSM. Another best practice is to never allow the Root CAs to participate on any network (Microsoft, 2014). This is to ensure that they are not exposed to any threat or compromise.

If an HSM is not used, many creative alternatives can be established to prevent unauthorized access, log key access, and log key retrieval. One such combination of alternative components to build the Root CA can be an offline laptop with an external USB drive that contains the Root CA. These are to be stored in a location to which none of the builders have access. A trusted 3rd party within the organization might possess the ability to retrieve the components from a safe or secured area. When stored, it is advised to seal the components in separate tamper-evident envelopes to ensure that they have not been compromised since their return to storage. Signatures from those who last used the components along all sealed edges are also advised. Each signature must be validated prior to breaking the seal in order to retrieve the component to boot the virtualized guest to make necessary changes.

I recommend that Root CAs are built by 2 or more people, each possessing insufficient information to make changes by themselves to the Root CA (Microsoft, 2003). For example, one individual may possess an encryption password or key for an external drive on which the Root CA resides. The other may know the password to login to the Root CA server itself. This separation of duty provides additional assurance to the integrity of the PKI.

Issuing or Intermediate Certificate Authorities are the online subordinate to the Root CA within the chain of trust (Pyle, Designign and Implementing a PKI: Part I Design and Planning, 2009). The Root CA signs the certificate issued to the Issuing CA to create the chain of trust (Microsoft). The Issuing CA now has authority to issue (approve or reject) the majority of the certificate requests for the PKI (compared to the Root CA).The Issuing CA publishes certificate templates that govern individual template types to be used in the PKI (Microsoft). It also sets the minimum requirements for key length, hash algorithm, validity and renewal periods, and publishes a list of revoked certificates (Microsoft).

As you can see, a PKI is a complex, highly secure, and vital component for an organization. Ensuring that a well-planned implementation occurs is tantamount to creating a PKI that meets the assurance demands of the organization. The following sections outline critical decisions to make prior to implementation as well as installation guidance.

2. Prerequisite Decisions

Prior to implementation, there are a number of PKI design decisions that are *HIGHLY* advisable to make. Making these decisions on the fly may create an undesirable position in the future. As an example, Microsoft advises that the CA Server Name or domain not change after the CA role has been installed (Microsoft, 2013). Changing this essentially means building a new CA and re-issuing all valid certificates (Microsoft, 2013). Choosing appropriate names is critical to the PKI environment as they must be meaningful for the duration of the CA (up to 20 years or longer).

The critical decisions listed below are not intended to be an exhaustive list of every possible decision to be made. This list was created after multiple Microsoft Windows Server 2012 Certification Authority PKIs were designed and implemented for an example organization.

2.1. Private Enterprise Number

Although not required for private or internal PKIs (not made externally available), a Private Enterprise Number (PEN; assigned by the Internet Assigned Numbers Authority (IANA), American National Standards Institute (ANSI), or British Standards Institute (BSI)) is the first step to generate a unique Object Identifier (OID) for any object referenced within the PKI. The OID provides a hierarchical name for almost every object type within a PKI such as a Certificate Practice Statement or Certificate Policy (OID Info, 2014). IANA provides an initial referential value (1.3.6.1.4.1) to which the PEN is appended at the time of issuance. An example of a PEN referenced by IANA is: 1.3.6.1.4.1.5518 (TDS Telecom, Inc.). IANA provides additional guidance regarding the data structure used to define *network management parameters* for use with SNMP and TCP/IP (Internet Assigned Numbers Authority, 2014).

A PEN can be requested from IANA by going to this registration page. The contents of the required form fields will be made available publically with the assigned PEN (Internet Assigned Numbers Authority). A single PEN is normally granted to an organization. An organization can search the PEN registry to determine if a PEN has been issued to them already (Internet Assigned Numbers Authority). This process can also take up to 30 days to complete (Internet Assigned Numbers Authority). The OID Repository also offers a location where information about many OIDs can be found; however it does not (and cannot) contain all OIDs (OID Info, 2014).

Once the PEN is obtained, the organization can append any series of numbers to the end of the OID to identify any object within the PKI (Alvestrand, 1997). Suggestions such as the following have been used to represent additional aspects of an organization via the OID:

[Subsidiary]	1=Corp 2=Subsidiary A 3= Subsidiary B
[Department]	1=IT
[Environment]	1=Production 2=Development
[Technology]	5=PKI
[General Policy]	1=General Purpose Issuance Policy

An example OID for a production PKI implementation for the corporate office using the suggestions would be: 1.3.6.1.4.1.5518.1.1.1.5.1. The numbers 1.1.1.5.1 were appended to the PEN to create the complete OID that refers to the General Purpose Issuance Policy.

One final decision left to make regarding the PEN/OID is: on which Certificate Authority to add the OID? The OID will be added to the 'CAPolicy.inf' file used in the configuration of the Certificate Authority during the installation of the Server 2012 role. This is done to reference the location of the Certificate Practice Statement and Certificate Policy, in the previous example, that govern the CA. Adding the OID to the Root CA means that subsequent CAs in the PKI will be bound to that OID; perhaps better stated that subordinate CAs cannot have a completely unique OID. There may be cases where this may be desirable or undesirable. Root CAs can be built without an OID (remember: they are offline and are not to be added to any network). A single Root CA without a

defined OID can sign certificates for many Issuing CAs easily; managing multiple Root CAs can be cumbersome.

2.2. Certificate Validity Periods

One of a CA's primary responsibilities is to issue certificates (Microsoft, 2012). Certificates issued for and by a CA have a limited life span. The life cycle of a certificate issued by or for a CA should be relative to an organization's requirements and necessary assurance level (Microsoft, 2009). A Certificate Policy (CP) and a Certificate Practice Statement (CPS) are generally used to define the PKI's parameters which notify the consumers what level of assurance to expect (Microsoft, 2009). Create a Certificate Policy and a Certificate Practice Statement prior to implementation (S. Chokhani, 2003). Microsoft offers recommendations regarding the validity period for various CA types (Microsoft, 2009). This guidance includes key length and a maximum number of years for the life of the certificate (Microsoft, 2009). The actual validity used by an organization could be dictated by contractual obligations.

A common length of time for a Root CA to be valid is 20 years. Issuing CAs are generally configured for one-half of the life of its parent/Root CA (in this example, 10 years). This value can be configured to any desired time period; however, it is worth considering a length of time that is shorter than the time expected to break the hash algorithm used within the PKI.

2.2.1. Renewal Validity

A Renewal Validity period is the length of time during which a certificate can be renewed (Microsoft, 2005). Once this time period expires, the certificate will be revoked (unless it is renewed prior to expiring). Validity periods for individual certificates can vary, by template type, from a few days (development, testing) to multiple years, depending, on the use case.

2.3. CRL Renewal Periods

The second responsibility of a certificate authority is to publish a list of certificates that are no longer valid (Delay, 2012). This is done by publishing a Certificate Revocation List (CRL). Clients that want to check the revocation status of a given

certificate will connect to a published CRL distribution point (CDP) to find a copy of the CRL. The Client then parses the CRL for the certificate in question as well as its revocation status (Microsoft, 2005).

The CRL renewal period defines how long the CRL is valid. Shorter validation periods lessen the time to recover in the event of a disaster (Delay, 2012). Also, many clients cache a CRL and won't check back until the validation period expires (Delay, 2012). If a certificate is revoked during this period, a client may be unaware until their cached copy expires and forces them to download a new CRL (Delay, 2012).

CRL renewal periods for Root and Issuing CAs are different as their roles are different. A Root CA is offline (Microsoft, 2014) and not even powered on save for a few times a year (Microsoft, 2012). A Root CA will issue (and by nature revoke) a relatively low number of certificates (Microsoft, 2012). Updating CRLs will be less of a necessity for Root CAs. Thus, a Root CA's CRL Period can easily be configured to be at least 30 days (Microsoft, 2012) or even a length of time up to its renewal validity to avoid powering up the CA unnecessarily.

An Issuing CA, on the other hand, will be issuing and revoking an exponentially higher number of certificates. Thus, publishing a CRL more often is necessary. An example CRL Period for an Issuing CA could be 7 days. This will ensure that revoked certificates are made known publically in a timely fashion as well as forcing clients to check back somewhat frequently (Delay, 2012). This can easily be configured to be shorter or longer depending on the volume and type of certificates issued (higher numbers of issued certificates may likely result in a higher number of revocations).

2.3.1. Delta CRLs

Given that offline Root CAs will not be issuing or revoking many certificates, Delta CRLs are not a necessity root CAs (Microsoft, 2012). For Issuing CAs, the Delta CRL contains a list of revoked certificates and defines the 'delta overlap' period, which is the acceptable length of time that a CRL Period is valid when the publication of a new CRL is delayed or fails to publish timely (Delay, 2012). This extends the life of the existing Delta CRL to allow for the next CRL to be published. The recommended best practice by Microsoft is 10% of the CRL

Period (Microsoft, 2012). The default setting, if not configured, is 12 hours (Microsoft, 2012). This setting also cannot exceed the CRL publishing period (Microsoft, 2012).

2.3.2. CRL Distribution Points

CRL Distribution Points (CDPs) can and will take many different forms within the PKI environment. The primary CDP locations are described below, but the description is not intended to be exhaustive or inclusive. It contains the most common types of CDPs.

Given that Windows Server 2012 is being discussed, you are undoubtedly aware that Certification Authorization roles are tightly integrated within Active Directory. Thus, LDAP can be a location where CRLs and Delta CRLs will be published and made available to domain members (Microsoft, 2009). It is *recommended* but technically not a requirement.

Windows Server 2012 Certificate Services leverages a network share (SMB, if not already running on a Windows server) as another target for publishing CRLs (Microsoft, 2009). In most cases, only the Issuing CA's machine or system account needs access to the share. Two (2) servers minimally are advised to function as CDPs for a given PKI to provide a highly available CDP share. The server names and share name (often CRL$) are used later in the configuration of the Issuing CA (Microsoft, 2009).

Windows Server 2012 Certificate Services also requires a URL (embedded in all issued certificates) that provides access for CRL checking by internal AND external clients (Microsoft, 2009). You will want 2 sets of servers with corresponding shares (Microsoft, 2011): one pair services external or DMZ clients, and one pair services internal clients; both load-balanced. This is generally accomplished by installing Internet Information Services (IIS). Double-escaping is required to be enabled in 'Request Filtering' as the delta CRL contains a plus sign '+' in the file name. Microsoft also offers a PowerShell command (*appcmd set config /section:requestfiltering /allowdoubleescaping:true*) to enable double

escaping (Micrososft, 2012). Also configure the CRL$ share as a virtual directory on the default web site (Microsoft, 2009).

The CDPs also contain a copy of the Root and Issuing CAs public certificates and CRLs, as this is necessary during CRL checking to establish a trust chain (Microsoft, 2012). For the Root CA, this is manually exported and copied into the share, as the Root CA is offline. It is also manually published into Active Directory (Pyle, Designing and Implementing a PKI: Part II Implemntation Phases and Certificate Authority Installation, 2009). During the configuration of Issuing CA, the certificate will be published to Active Directory and copied to the CDP (either via a script or manually) (Pyle, Designing and Implementing a PKI: Part II Implemntation Phases and Certificate Authority Installation, 2009).

A few words of advice about external CDPs: depending how your Active Directory is configured (extended into the DMZ, or the DMZ has a separate Windows domain), the process by which CRLs and Root/Issuing CA public certificates are published could vary. If separate domains for internal and DMZ environments exist, a file copy job (robocopy works well) running daily to move the files is recommended (read: a rule for a single firewall port is needed). If your internal domain is extended into your DMZ, a plethora of Windows ports on your firewall will be required (Microsoft, 2010). This is not advised as there are many, many open ports required (Microsoft, 2010). A file copy job is always preferred over an extremely permissive firewall rule.

2.3.3. Online Certificate Status Protocol

Online Certificate Status Protocol, or OCSP, is an IP protocol used to obtain the revocation status of an individual digital certificate (M. Myers, 1999). It was created as an alternative to certificate revocation list checking to determine the validity of an individual certificate. Communications with OCSP occur over HTTP (M. Myers, 1999). A URL is required for OCSP (Patel, 2012). Thus, it is dependent on the installation of IIS. HTTPS is not mandated (M. Myers, 1999), and thus a 3rd party could intercept unencrypted traffic (M. Myers, 1999).

OCSP uses far fewer resources as the communications contain only information about a single certificate (M. Myers, 1999). Clients do not need to parse the CRL themselves. Instead, OCSP contains a cached copy of the CRL and responds to requests about individual certificates (M. Myers, 1999). A common URL and name that is hosted by a load balancer or DNS is preferred over a server-specific name for the URL.

2.4. Cryptographic Service Provider and Key Length

Microsoft offers a number of Cryptographic Service Providers within the Windows Server 2012 Certification Authorization role. A full list can be found online (Microsoft). Choose the one that best suits your needs. The default in the role installation is **Microsoft RSA Signature Cryptographic Provider** and is likely adequate for many organizations implementing this specific PKI.

When choosing a Key Length, there are a number of factors to consider. Generally longer key lengths are considered more secure as they require more time to brute force the hash algorithm (The SANS Institue, 2013). Choosing a short key length could create a situation where the validity period of the CA is longer than the time required breaking the hash algorithm. Another thing to consider is the age of the operating systems for which certificates will be issued. Older operating system may have limitations regarding supported key lengths. Understand your environment prior to choosing a key length.

2.5. Certificate Templates

Certificate Templates are used to define the properties of certificate issued by a CA and have many attributes that control certificate behavior (Stephens, 2010). A template can limit the number of users who have access to request a certificate, or allow anyone to request a certificate from that template. Templates also contain the validity and renewal periods, backward compatibility settings, enrollees, and minimum key length (among many other things).

Choosing which templates to use for specific applications can be tricky. It is up to each organization to define the types of templates to use for specific applications in their

individual environments. Typical applications are server (HTTP, URL), user (workstation, Wifi networks), and email signing. Microsoft provides guidance regarding how to plan for and choose specific templates to use (Stephens, 2010). It is highly advisable to perform this research and make decisions prior to the start of implementation about which templates best meet specific needs. It is also advisable to duplicate a template rather than edit the default templates provided (Microsoft, 2013). This allows for full customization without losing the original settings.

2.6. Windows Active Directory

If you have an older Active Directory environment, you may have both a forest root and a domain root. You may or may not recall, but the forest root will function as the default certificate store (Baker, 2013). I unfortunately remembered this after I implemented and had some problems with things not working like I expected. However, do not despair! This is a configuration change that can be accomplished without starting over from scratch.

It is highly advisable to ensure that you have a deep understanding of the Active Directory environment in which you are installing a PKI. Does the domain in which you are installing the PKI have an existing PKI? If it does, that is not technical a problem. A given Windows domain can support multiple Issuing CAs (Microsoft). It is good to remember that the trust chain from the new PKI will be inherited by any machine in the domain (Microsoft). It is advisable to avoid a lower assurance PKI in the same domain as a medium or high assurance PKI (William E. Burr, 2011).

Does the domain in which the PKI will be installed have both development and production servers within it? This is not necessarily a problem, if the intention is to issue certificates from the same PKI instance to servers in all environments (prod and non-prod). This could become a problem if the intention is to issue certificates from a non-production PKI to only non-production servers that are managed by a single production domain. Again, any domain member machine will receive the trust chain from any PKI installed in the domain (Microsoft). This could expose production servers to a non-production trust chain, which is undesirable in many cases (William E. Burr, 2011).

Again, it is advisable to avoid a lower assurance PKI in the same domain as a medium or high assurance PKI (William E. Burr, 2011).

2.7. Permissions

Given this process includes Active Directory and Microsoft Windows Server, there are numerous ways to grant the necessary permissions for administration purposes. The permissions described below are intended to cover installation only (Patel, 2012). The section on Administrative Roles makes recommendations regarding separation of duties and appropriate permissions for individual roles.

- **Certificate Services** role installation: local administrator for Root CA; enterprise administrator for Issuing CA. The permissions to administer the Issuing CA long term can be reduce to be less than enterprise administrator.
- **Web Enrollment** server role installation: enterprise administrator
- Internal CDP share
    - NTFS permissions: enterprise administrator with full control during installation; AD group named Certificate Publishers with modify access during and after the installation
    - Share permissions: enterprise administrators with full control during the installation and AD group named Certificate Publishers with modify access during and after the installation
- External CDP share
    - NTFS /Share Permissions: must allow the Internal CDP servers to publish the contents of the Internal CDP shares here. These permissions could vary depending on the type of method uses to populate the share contents.
- **Internet Information Services** role installation: enterprise administrator.

2.8. Legal Notification

Some organizations are required to populate lengthy legal statements in their certificates, but doing so creates additional bloat in the size of the certificate. Default certificate sizes for Server 2012 are around 17KB in the database and 15KB in the log (Arwine, 2012). Error on the side of caution and use a higher value (64KB) to estimate how much local storage will be required in the certificate store for your environment (# of certs * 64KB = X mega/giga bytes).

Some organizations add the majority of their *legal-ease* to the Certificate Policy (CP) and Certificate Practice Statement (CPS) documents and use a simple legal statement such as: "*Legal Policy Statement - This PKI is for the <Company> <production/non-production> environment. Refer to the associated Certificate Practice Statement (CPS) for more information.*" It is advised to so something similar to avoid unnecessary bloat in the CAs storage environment. Guidance to create a Certificate Policy or a Certificate Practice Statement can be found in RFC3647 (S. Chokhani, 2003), as there are standards regarding what the documents contain as well as the order in which these items are displayed.

2.9. Administrative Roles

Microsoft defines the following roles and aligns them closely to roles defined by Common Criteria classifications (Microsoft). While additional roles could be defined, it is advised to determine which individuals and groups within an organization would own each of these roles prior to implementation.

[CA Administrator]	Manages CA
[CA Manager]	Issues and Manages Certificates
[Backup Operator]	Backup / Restore Files and Directories
[Auditor]	Manages Auditing and Security Log
[Enrollees]	Requests Certificates

It is also advised to maintain separation of duties when implementing this security model: no one group would be both a CA administrator AND a CA manager (Microsoft). These roles are recommended to be deployed as groups rather than granting permissions to individual users (Microsoft).

CA Administrators can be added to the local admins group on the Issuing CA server, as well as granted with **Manage CA** permissions defined on the CA itself (Microsoft). *CA Managers* are granted **Issue and Manages Certificates** permissions defined on the CA itself (via Certification Authority (certsrv.mmc) MMC console; right click on the CA object, and choose **Security**) but not added to any local administrative group (Microsoft).

Backup Operator is also a local admin but receives no permissions on the CA itself (Microsoft).

Auditors can be given **Read** permissions to the CA itself (again, via the Certification Authority MMC) in order to audit the CA's configuration. Auditors also are provided permissions to review local audit logs (Microsoft).

Enrollees can be given permissions to **Request Certificates** on the CA itself as well as to various individual templates with **Read** and **Enroll** permissions. A process that describes how to set permissions on templates is described in a later section. This same process is used to add *Enrollee* permissions on templates. *Enrollee* is not considered to be a CA role, however (Microsoft).

3. Installation

The following section summarizes the steps to perform the Root CA installation and configuration as well as the online Issuing CA installation and configuration. The Root CA installation was performed on an offline Windows 7 (base install; no hot fixes) laptop that has all network interfaces disabled. This laptop was installed with VMware Workstation. The Online Issuing CA was built on Server 2012.

For the Root CA install, these instructions assume that one has a VMware guest on an encrypted USB drive that can be booted on a laptop that is 100% offline.

Again, please be advised that all environments are unique, and this is intended to describe the steps used to build a PKI for an example company. No guarantees, either written or implied, are provided.

3.1. CRL Distribution Points (CDP)

Prior to installing the Root or Issuing CA, the CDP URL locations and shares are recommended to be configured. An existing CDP could be used also. Performing this step early in the process ensures that there is an appropriate location in which to store necessary files as they are created by each CA. In order to configure the URLs and shares, the names and networks of the CDPs and servers running the CDP must be determined.

The *external CDP* is an externally accessible location (HTTP; fully qualified domain name) load-balanced between at least two (2) servers. Thus, its name is not expected to reference an individual server. This is the location where CRLs are checked by external entities (Example: *certrev.dmzprod.company.com*). Select two servers to host the External CDP and document their names. Each will require a web server (IIS is used in this example) to host the external-facing URL as well as a network share to which the contents of the internal CDP will be published.

The *internal CDP* is accessible to internal clients only (HTTP; fully qualified domain name) and is also expected to be load-balanced. Thus, its name is not expected to reference an individual server. This is the location where CRLs are checked be clients on the private, internal network of the organization (Example: *certrev.prod.company.com*). Select two servers to host the Internal CDP and document their names. Each will require IIS to host the internal-facing URL. The network share is published via IIS and contains CRLs, Delta CRLs, and public certs for the Root and Issuing CAs.

As previously stated, shares are required to contain public certificates, CRLs, and Delta CRLs for the Certificate Authorities. The creation of two types of shares, external and internal, is described below. Each has a slightly different configuration as the files served by the share are published to the share via different methods.

The internal share will contain the public certificate for the Root and Issuing CAs. Also, the Issuing CA will publish its CRL and Delta CRL to this location. Therefore, specific share and NTFS permissions are required. This section outlines how to create and ACL the share and NTFS permissions.

Create the Internal Shares:

1. Create a directory using the Internal CDP name
    a. Example: mkdir d:\websites\certrev.prod.company.com
        i. This location is suggested as it will be used in the IIS configuration later.
2. Inside this directory, create another directory named **CDP**
    a. Example: mkdir d:\websites\certrev.prod.company.com \CDP
3. Share the CDP folder (d:\websites\certrev.prod.company.com \CDP) as **CRL$**
4. Change the share permissions to only contain **PROD\Cert Publishers** with **CHANGE** and **READ** permissions
5. For the NTFS file permissions, retain all existing entries and add **PROD\Cert Publishers** with **MODIFY** permissions.
6. Repeat steps 1 – 5 on the 2nd internal CDP server

A 'blind' or invisible Windows share (ending with a **$**) has now been created and is only accessible by members of the **PROD\Cert Publishers** group.

Create the External Shares:

1. Create a directory that uses the Internal CDP name
    a. Example: mkdir d:\websites\certrev.organization.net
        i. This location is suggested as it will be used in the IIS configuration later.
2. Inside this directory, create another directory named **CDP**
    a. Example: mkdir d:\websites\certrev.organization.net\CDP
3. Share the CDP folder (d:\websites\certrev.organization.net\CDP) as **CRL$**
    a. The share and NTFS permissions required to facilitate a file copy from the internal CDP servers are required here. See additional comments below.
4. Repeat steps 1 – 5 on the 2nd external CDP server

Rather than publish directly from the Issuing CA to the external CDP, it is advised to copy the contents of the Internal Share to the External Shares. In order to publish directly to a share, RPC traffic must be allowed to pass between your internal and external networks (read: Windows file copy). This is seldom advised due to the high number of ports/protocols required (Microsoft, 2010).

Thus, it is advised to create a script that will copy the contents of the internal CDP share to the external CDPs. Robocopy.exe or SCP.exe are a perfectly suitable tools to do this. Then, you can restrict the firewall rules to allow a single port from an internal CDP server to the external CDP servers. Therefore, the external share must be configured to allow an internal CDP server to write the contents of the Internal CDP to it.

3.2. Internet Information Services (IIS) Configuration

IIS is required for CRL checking via the CDPs, as this is performed via HTTP methods for many legacy applications and operating systems. Online Certificate Status Protocol (OCSP) is used by newer applications and operating systems and will be installed as well. It is also dependent on IIS.

The following section provides *guidance* regarding IIS configuration. IIS *installation* is not covered in this section as this can be specific to a given organization. However, advice is provided regarding some of the configuration options. It is recommended that this be configured identically across all CDP servers.

IIS Installation and Configuration:

1. Install IIS in accordance to organizational procedures.
2. Change the **Default Web Site** settings to point to the first directory you created in the CDP configuration section (example: d:\websites\certrev.prod.company.com)
    a. This ensures that the CDP shared directory becomes part of the hosted web site necessary for CRL checking.
3. Move log files to the same location found in #1 (directly above)
4. Edit the **Request Filtering** settings to **Allow Double Escaping**
    a. This is required as the Delta CRL file contains a plus sign ('+'). Without this setting, the Delta CRL file is not visible.
5. Repeat on all CDP servers using the network-specific URL information to create the directory for the default web site.

3.3. Root Certificate Authority Installation

Prior to installing the Root CA, a custom CAPolicy.inf file was created and placed in the c:\windows directory. This file is parsed during installation and makes some basic configuration settings (rather than after the install has been completed). Please refer

to the example file provided in the Appendix. Items in brackets < > are organization-specific. Microsoft has a well-documented procedure (Microsoft; Microsoft) that covers what is summarized below.

1. Open Server Manager and add a **New Role**.
2. Select **Active Directory Certificate Services**
3. Choose the role labeled **Certification Authority**
4. Select the setup type of **Standalone** for the offline Root CA
5. Create a **New Private Key**
6. Configure the minimum **Cryptographic Service Provider**, **Key Length**, and **Hash Algorithm** that you want the CA to support.
7. Name the Certificate Authority. WARNING: this name will persist for the life of the CA, and it is not recommended to change this in the future.
8. Set the **Validity Period** in the number of **Years** or **Months** that the Root CA's certificate will be valid. See previous guidance regarding an appropriate time frame.
9. Review all configuration settings. Save/apply all changes.

3.4. Root Certificate Authority Configuration

Once the Root CA has been installed, there are items to be configured. This can be done manually via the Certificate Authority MMC, or via a script. The example script in the Appendix describes the configuration settings.

1. Directory Store Configuration Distinguished Name: the location in Active Directory where the configuration information about your PKI is stored.
    a. Example string: CN=Configuration,DC=PROD,DC=Company,DC=Com
2. CRL Period: defines the life of the CRL and is a measure of time (days, weeks, months, years) as a numerical value.
    a. CRLPeriod: Years
    b. CRLPeriodUnits: 19
3. CRL Overlap Period: the amount of time at the end of a published CRL's lifetime that a client can use to obtain a new CRL before the old CRL is considered unusable. This is also a measure of time (days, weeks, months, years) and a numerical value.
    a. CRLOverlapPeriod: Weeks
    b. CRLOverlapUnits: 52

4. Validity Period: defines, in terms of days, weeks, months, or years, how long certificates issued by the CA are valid (example: for the online Issuing CA to be built/configured in a later step)
    a. ValidityPeriod: Years
    b. ValidityPeriodUnits: 10
5. CA Auditing: defines the audit flags that are enabled on a specific CA
        i. CAAuditing: 127
            1. 0 = all auditing disabled
            2. 127 = all auditing enabled (recommended)

Given that a Windows-based PKI is discussed, there is heavy reliance on Active Directory. The Root CA's public certificate is published in Active Directory, as well as in all CDP locations. Without these, a trust chain cannot be established.

A script was used to programmatically configure all items necessary using the information determined in the CDP configuration step. An example script is provided in the appendix, and the locations to edit have been highlighted. Please review the entire script prior to execution or implementation. The items to add to the script are:

1. External CDP URL
2. Internal CDP URL
3. Internal CDP servers (for CRL/Delta CRL publishing)

Adding this information to the example script sets the registry settings on the Root CA to reference these locations. It also copies the *.CR? files (Root CA public cert and CRL) to c:\. These files are to be copied into AD as well as the CDPs (in a later step).

3.5. Issuing Certificate Authority Installation

Prior to the installation of an Issuing CA, it is advised to configure a CAPolicy.inf and copy it into the c:\windows directory on the server that will become the Issuing CA. This file is read as the CA is installed and makes some basic configuration settings. Please refer to the example provided in the Appendix. Items in brackets < > are organization-specific.

Once c:\windows\CAPolicy.inf exists with the correct parameters, the public certificate for the Root CA must be installed into the local certificate store on the Issuing CA and published into Active Directory. This was done via a script for the example

organization but could be done manually. This was accomplished by the following process. This is essential to creating the trust chain between the Root and Issuing CA.

1. *.CRT and *.CRL were copied from the Root CA to c:\ on the Issuing CA
    a. The highlighted text in the example script reflects that which was changed for the example organization.
2. Run the script as **PROD\Enterprise Administrator** to publish the cert and CRL locally and in Active Directory. Note any errors and resolve as necessary prior to moving on.

    After publishing the cert and CRL files, the Issuing CA can be installed.

Microsoft has provided a detailed guide to install an Intermediate or Issuing CA (Microsoft), and this has been summarized below.

1. Open Server Manager and add a **New Role**.
2. Select **Active Directory Certificate Services**
3. Select the role labeled **Certification Authority**
4. Select the setup type of **Enterprise** for the online Issuing CA
5. Select the CA type labeled **Subordinate CA** for the Issuing CA
6. Create a new **Private Key**
7. Select the appropriate **Cryptographic Service Provider**, **Key Length**, and **Hash Algorithm**
8. Since the Root CA is offline, choose to save the certificate request to a file for processing later.
9. Enter an appropriate name for the Issuing CA
10. Enter an appropriate **Validity Period** for the number of **Years/Months** to define the length of time a certificate issues by this CA will be valid.
11. Select appropriate locations for the **Certificate Databases**.
    a. For the example organization, the defaults were unchanged.
12. Confirm installation options and configure.

3.6. Issuing Certificate Authority Configuration

Now that the Issuing CA has been installed, there are still a number of outstanding tasks to accomplish prior to certificate issuance. The following tasks, in the order in which they appear, are recommended:

1. Sign Issuing CA certificate with the Root CA
2. Install CA certificate into local certificate store

3. Configure CRL settings (validity, overlap, and delta periods) and certificate validity settings
4. Configure AIA/CDP configuration settings

During the installation of the Issuing CA, a certificate request was saved to c:\ on the Issuing CA. This file (requestName.req) is to be copied to the Root CA and signed. After the file is copied to the Root CA, the following example command can be used to sign the certificate: **Certreq –submit <path>\requestName.req**

Open the Certificate Authority MMC (certsrv.mmc) console and navigate to 'Issued'. You can now export the signed certificate in a binary format. This export is to be copied back to the Issuing CA for installation. Perform the following steps on the Issuing CA (Patel, 2012):

1. Copy and save the binary export to the Issuing CA (**c:**).
2. Open the Certificate Authority MMC (**certsrv.mmc**) console. Right click on the CA itself (left-hand window), choose **All Tasks**, and select **Install CA Certificate**.
3. Follow the prompts to locate the Issuing CA's signed certificate on **c:** and import it. This will copy the certificate to the correct location in Active Directory.
4. This will require a restart of the **Certificate Authority** services.

With the Issuing CA's certificate signed and installed, the Issuing CA is nearly complete. Much like the Root CA, the CRL and Certificate validity settings are to be configured prior to issuing certificates from the newly minted Issuing CA. These were configured for the example company via a script that edits the registry on the Issuing CA.

1. CRL Period: defines the life of the CRL and is a measure of time (days, weeks, months, years) as a numerical value.
    a. CRLPeriod: Weeks
    b. CRLPeriodUnits: 1
2. CRL Overlap Period: amount of time at the end of a published CRL's lifetime that a client can use to obtain a new CRL before the old CRL is considered unusable. This is also a measure of time (days, weeks, months, years) and a numerical value.
    a. CRLOverlapPeriod: Hours
    b. CRLOverlapUnits: 48
3. CRL Delta Period: defined by a measure of time (days, weeks, months, years) and a numerical value and measures the life of the Delta CRL.

Michael Naish, mnaishjr@gmail.com

   a. CRLDeltaPeriod: Days
   b. CRLDeltaUnits: 1
4. CRL Delta Overlap Period: amount of time at the end of a published CRL's lifetime that a client can use to obtain a new CRL before the old CRL is considered unusable.
   a. CRLDeltaOverlapPeriod: Hours
   b. CRLDeltaOverlapUnits: 6
5. Validity Period: defines, in terms of days, weeks, months, or years, how long certificates issued by the CA are valid
   a. ValidityPeriod: Years
   b. ValidityPeriodUnits: 2
6. CA Auditing: defines what auditing is enabled on a specific CA
   a. CAAuditing: 127
      i. 0 = all auditing disabled
      ii. 127 = all auditing enabled (recommended)

Given that a Windows-based PKI is being discussed, there is heavy reliance on Active Directory. The Issuing CA's public certificate and CRL are published in Active Directory, as well as in all CDP locations. Without these, a trust chain cannot be established. A script was used to configure all items necessary using the information determined in the CDP configuration step. An example script is provided in the appendix, and the locations to edit have been highlighted. Please review the entire script prior to execution or implementation. The items to add to the script are:

1. External CDP URL
2. Internal CDP URL
3. Internal CDP servers (for CRL/Delta CRL publishing)

Adding this information to the example script will set the registry settings on the Issuing CA to reference these locations. It will also copy the *.CR? files (Issuing CA public cert and CRL) to c:\. These files are required to be manually copied one time to all CDP locations.

3.7. Web Enrollment Server and Online Responder Installation

For the example organization, the Web Enrollment Server (WES) and Online Responder (OCSP) were installed on the same server for the example organization. This

was done to consolidate server roles as neither role was expected to be used heavily enough to necessitate physical separation. The following numbered list is a consolidated summary of guidance provided by Microsoft regarding WES (Microsoft) and Online Responder installation (Microsoft).

1. Open Server Manager and add a new role.
2. Select **Active Directory Certificate Services**
3. Select the roles **Certification Authority Web Enrollment** and **Online Responder**
    a. IIS will be installed by default if it is not already installed on the server to be used for WES/Online Responder
4. Click '**Install** to complete the installation

In addition to this configuration, HTTPS binding is to be configured on WES. WES will only request certificates from the Issuing CA if HTTPS bindings are enabled (Microsoft, 2013). Microsoft provides guidance (Microsoft) how to configure HTTPS bindings, and this will not be described at length in this paper. It is advised to issue a certificate to the WES from the Issuing CA previously installed via a template specifically created for the WES (Microsoft).

Due to the fact that the Issuing CA and WES are installed on separate nodes in the example, it is required to configure delegation for the WES to submit certificate requests on behalf of other users. Microsoft provides guidance regarding this process, and it has been summarized below (Microsoft).

1. Open **Active Directory Users and Computers**
2. Navigate to the server object for the WES, right click, and choose **Properties**.
3. Choose the **Delegation** tab
4. Choose **Trust this computer for delegation to specified services only**
    a. Also, choose **Use any authentication protocol**
5. Add the **HOST** and **RPCSS** services for the **Issuing CA's computer object** from Active Directory.
6. Save/Apply all settings; close all open dialog boxes

3.8. OCSP Configuration

To configure OCSP for the example company's PKI, a **Revocation Configuration** is required on the WES server where the **Online Responder** is installed. This requires a renewable certificate using the template type **OCSP Response Signing** (Patel, 2012). This must be published as an available template type on the Issuing CA as well as be ACL'd to allow only the WES to request this type of certificate (Patel, 2012).

Prior to configuring the **Revocation Configuration**, set the permissions on the template, and add the template to the Issuing CA. The following is a summary of how to accomplish this (Patel, 2012):

1. Login to the Issuing CA as an **Enterprise Administrator**
2. Launch the **Certification Authority** MMC (certsrv.mmc)
3. Add the Snap-In for **Certificate Templates**
4. Navigate to **OCSP Response Signing**
5. Choose the **Security Tab**
6. Add the computer account for the WES with **Read**, **Enroll**, and **Autoenroll** permissions
7. Save/Apply all settings; close all open dialog boxes

The final step is to create the Revocation Configuration. This will enable OCSP CRL checking within the example company's environment. The following is a summary of guidance provided by Microsoft (Microsoft) to create the Revocation Configuration.

1. Login to the WES as an enterprise administrator
2. Expand **Online Responder**, choose **Revocation Configuration**, and choose **Add Revocation Configuration** in the upper right hand corner
3. Provide an appropriate name for the Revocation Configuration
    a. Example: *Example Company Production Revocation Configuration*
4. Choose **Select A Certificate for an Existing Enterprise CA**
5. Choose the radio button **Browse CA Certificates Published in Active Directory**, and browse to the Issuing CA
6. Choose the radio button for **Automatically Select a Signing Certificate**, and select the checkbox for **Auto-Enroll for an OCSP Signing Certificate**.
    a. The Issuing CA's name will be populated in the **Certification Authority** text box

b. The name of the OCSP Response Signing template will be populated in the **Certificate Template** drop-down list

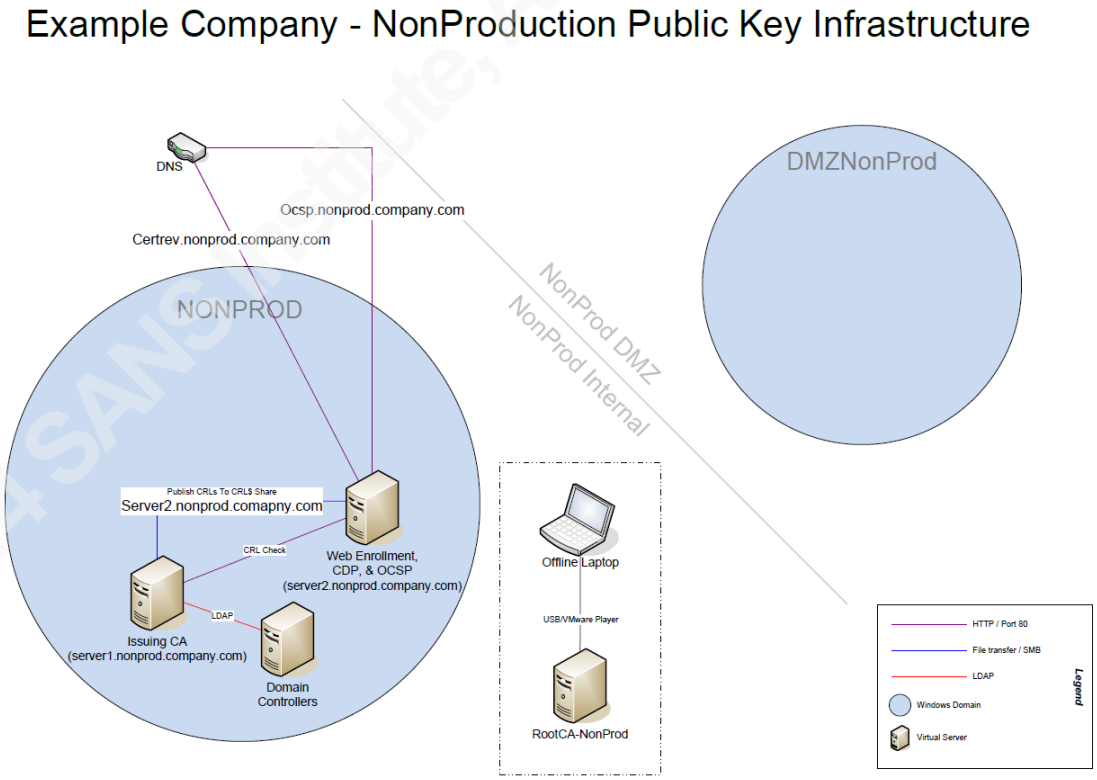
7. Click the provider button and ensure that the checkbox for **Refresh CRLS Based on Their Validity Periods** is selected.

This completes the installation and configuration of the Web Enrollment Server and Online Responder. The PKI installation is now complete and is ready to issue certificates.

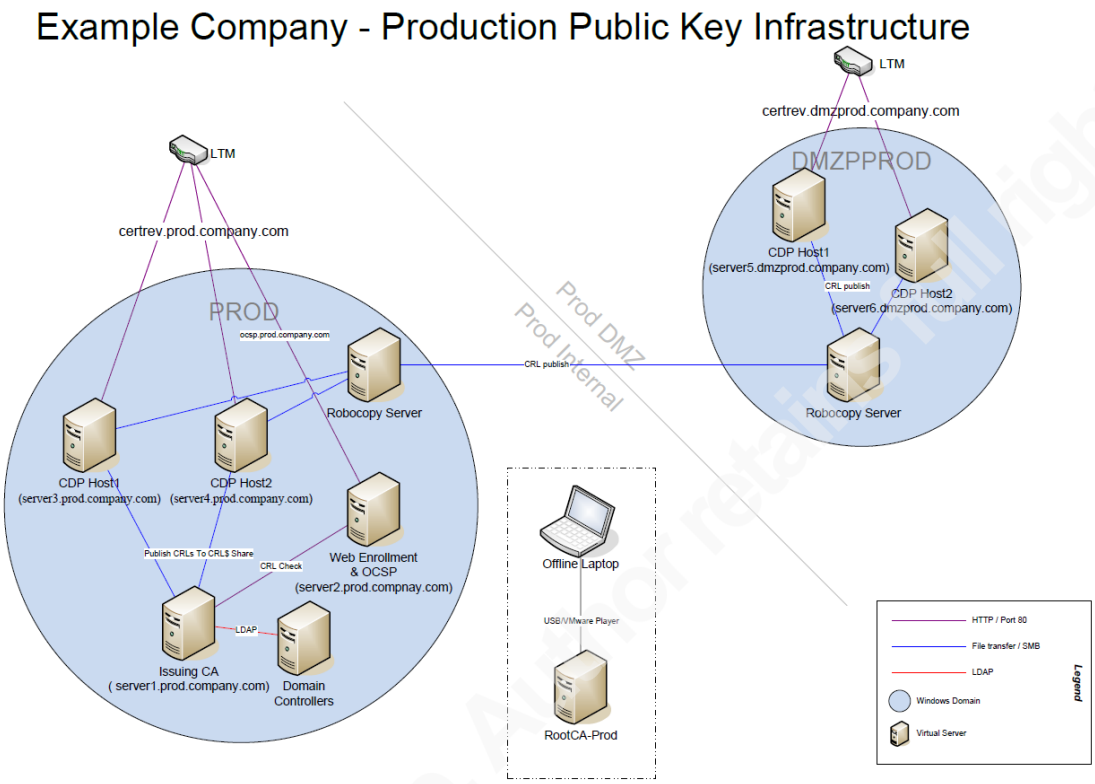
4. Diagrams

The following diagrams are provided as examples of the infrastructure, role location, and network locations for the design described in this paper. Please note that this is one possible example design and that other configurations are possible and viable, depending on environment variables, required assurance levels, and budget.

4.1. Non-Production



4.2. Production



5. Conclusion

A PKI is both a critical application within the Enterprise as well as a complex undertaking that requires intense planning prior to implementation. An understanding of the requirements, dependencies, and use cases helps an organization focus on critical decisions. Focusing on these decisions will ensure a timely deployment that is free of short-sightedness common to rushed implementations.

Each decision is dependent on those that have occurred previously and affects subsequent and future decisions. A focused, methodical implementation approach for Microsoft Windows Server 2012 Certificate Services has been described in this paper. This can be used to create a deployment strategy to rapidly deploy a PKI for any assurance level required.

Michael Naish, mnaishjr@gmail.com

This paper has also described how to use the decisions during the implementation and configuration of Microsoft Windows Server 2012 Certificate Services. A description and configuration guidance for each component has been provided. The intention is to practically apply the outcome of each decision to its corresponding element within the PKI. The resulting methodology helps to develop strategy than can be promptly and accurately implemented.

Michael Naish, mnaishjr@gmail.com

6. References

Alvestrand, H. (1997, February 10). *Object Identifiers*. Retrieved August 6, 2014, from Alevestrand.No: http://www.alvestrand.no/objectid/

Arwine, T. (2012, February 10). *Active Directory Certificate Services (AD CS) Public Key Infrastructure (PKI) Design Guide*. (E. Price, Editor) Retrieved August 11, 2014, from Microsoft TechNet Wiki: http://social.technet.microsoft.com/wiki/contents/articles/7421.ad-cs-pki-design.aspx#Plan_for_CA_Capacity_Performance_and_Scalability

Baker, D. (2013, October 18). *Understanding and Managing the Certificate Stores Used for Smart Card Logon*. Retrieved August 11, 2014, from MSDN Blogs: http://blogs.msdn.com/b/muaddib/archive/2013/10/18/understanding-certificate-stores-and-publishing-certificates-for-smart-card-logon.aspx

Delay, C. H. (2012, November 26). *PKI Design Considerations: Certificate Revocation and CRL Publishing Strategies*. (Microsoft) Retrieved August 6, 2014, from TechNet Blogs: http://blogs.technet.com/b/xdot509/archive/2012/11/26/pki-design-considerations-certificate-revocation-and-crl-publishing-strategies.aspx

Hirsch, F. J. (n.d.). *SSL/TLS Strong Encryption: An Introduction*. Retrieved August 11, 2014, from Apache.org: http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html#cryptographictech

Internet Assigned Numbers Authority. (2014, July 23). *Network Management Parameters*. Retrieved August 6, 204, from Internet Assigned Numbers Authority: http://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml

Internet Assigned Numbers Authority. (n.d.). *Private Enterprise Number (PEN) Request Template*. Retrieved August 6, 2014, from Internet Assigned Numbers Authority (IANA): http://pen.iana.org/pen/PenApplication.page

M. Myers, R. A. (1999, June). *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. Retrieved August 11, 2014, from The Internet Engineering Task Force (IETF): http://tools.ietf.org/html/rfc2560

Microsoft. (2003, March 28). *Defining PKI Management and Delegation*. Retrieved August 6, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc755614(v=ws.10).aspx

Microsoft. (2005, January 21). *Revoking certificates and publishing CRLs*. Retrieved August 23, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc782162(v=ws.10).aspx

Microsoft. (2005, May 19). *Understanding Digital Certificates*. Retrieved August 6, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/bb123848(v=exchg.65).aspx

Microsoft. (2005, January 21). *Validity and renewal periods*. Retrieved August 6, 2014, from Microsoft Technet: http://technet.microsoft.com/en-us/library/cc787132(v=ws.10).aspx

Microsoft. (2009, October 7). *Configure a CRL Distribution Point for Certificates*. Retrieved August 7, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/ee649168(v=ws.10).aspx

Michael Naish, mnaishjr@gmail.com

Microsoft. (2009, August 13). *Creating Certificate Polices and Certificate Practice Statements*. Retrieved August 7, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc780454(v=ws.10).aspx

Microsoft. (2010, June 25). *Firewall Rules for Active Directory Certificate Services*. Retrieved August 7, 2014, from Windows PKI Blog: http://blogs.technet.com/b/pki/archive/2010/06/25/firewall-roles-for-active-directory-certificate-services.aspx

Microsoft. (2011, April 12). *Where to Place the CRL Distribution Points*. Retrieved August 22, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/ee382302(WS.10).aspx

Microsoft. (2012, August 31). *AD CS: The CRL publication for a stand-alone root CA should be at least 30 days*. Retrieved August 6, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/dd379541(v=ws.10).aspx

Microsoft. (2012, April 11). *Configure CRL and Delta CRL Overlap Periods*. Retrieved August 6, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc731104.aspx

Microsoft. (2012, March 16). *How Certificate Revocation Wroks*. Retrieved August 7, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/ee619754(v=ws.10).aspx

Microsoft. (2012, November 20). *Renewing a certification authority*. Retrieved August 6, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc740209(v=ws.10).aspx

Microsoft. (2013, June 24). *Certificate Enrollment Web Service Guidance*. Retrieved August 23, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/hh831822.aspx

Microsoft. (2013, April 1). *Certification Authority Naming*. Retrieved August 6, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc770402.aspx

Microsoft. (2013, November 30). *Windows Server 2012: Certificate Template Versions and Options*. Retrieved August 7, 2014, from Microsoft TechNet: http://social.technet.microsoft.com/wiki/contents/articles/13303.windows-server-2012-certificate-template-versions-and-options.aspx

Microsoft. (2014, July 1). *Certification Authority Guidance*. Retrieved August 6, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/hh831574.aspx

Microsoft. (2014, June 18). *Public Key Infrastructure Design Guidance*. (H. A. Disi, Editor) Retrieved August 6, 2014, from Microsoft TechNet: http://social.technet.microsoft.com/wiki/contents/articles/2901.public-key-infrastructure-design-guidance.aspx#Links_to_Detailed_Design_Guidance

Microsoft. (n.d.). *Add a Certificate Template to a Certification Authority*. Retrieved August 18, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc771937.aspx

Michael Naish, mnaishjr@gmail.com

Microsoft. (n.d.). *Configuring Delegation Settings for the Certificate Enrollment Web Service Account*. Retrieved August 18, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/dd759201.aspx

Microsoft. (n.d.). *Configuring Server Certificates for Certification Enrollment Web Services*. Retrieved August 18, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/dd759140.aspx

Microsoft. (n.d.). *Creating a Revocation Configuration*. Retrieved August 18, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc731099.aspx

Microsoft. (n.d.). *Define Certification Authority Trust Strategies*. Retrieved August 6, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc977803.aspx

Microsoft. (n.d.). *Implement Role-Based Administration*. Retrieved August 11, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc732590.aspx

Microsoft. (n.d.). *Install a Root Certification Authority*. Retrieved August 18, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc731183.aspx

Microsoft. (n.d.). *Install a Subordinate Certification Authority*. Retrieved August 18, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc772192.aspx

Microsoft. (n.d.). *Installing the Certificate Enrollment Web Service*. Retrieved August 18, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/dd759241.aspx

Microsoft. (n.d.). *Microsoft Cryptographic Service Providers*. Retrieved August 6, 2014, from Microsoft Developer Network (MSDN): http://msdn.microsoft.com/en-us/library/windows/desktop/aa386983(v=vs.85).aspx

Microsoft. (n.d.). *Setup Up an Online Responder*. Retrieved August 18, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc725937.aspx

Microsoft. (n.d.). *Use Policy to Distribute Certificates*. Retrieved August 11, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/cc772491.aspx

Micrososft. (2012, February 29). *Configure Request Filtering in IIS*. Retrieved August 10, 2014, from Microsoft TechNet: http://technet.microsoft.com/en-us/library/hh831621.aspx

Mircosoft. (2007, October 26). *Description of Symmetric and Asymmetric Encryption*. Retrieved August 6, 2014, from Microsoft Support: http://support.microsoft.com/kb/246071

OID Info. (2014, July 3). *Frequently Asked Questions*. Retrieved August 6, 2014, from OID Repository: http://www.oid-info.com/faq.htm#2

OID Info. (2014, Februrary 16). *OID Repository*. (Orange S.A.) Retrieved August 6, 2014, from http://www.oid-info.com/

Patel, N. (2012, December 17). *AD CS Step by Step Guide: Two Tier PKI Hierarchy Deployment*. (J. Brew, Editor) Retrieved August 11, 2014, from Microsoft TechNet Wiki: http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx#Configure_the_CDP_and_AIA

Pyle, N. (2009, September 1). *Designign and Implementing a PKI: Part I Design and Planning*. (N. Pyle, Editor, and Microsoft) Retrieved August 6, 2014, from Microsoft TechNet: http://blogs.technet.com/b/askds/archive/2009/09/01/designing-and-implementing-a-pki-part-i-design-and-planning.aspx

Pyle, N. (2009, October 13). *Designing and Implementing a PKI: Part II Implemntation Phases and Certificate Authority Installation*. Retrieved August 7, 2014, from Ask the Directory Services Team blog: http://blogs.technet.com/b/askds/archive/2009/10/13/designing-and-implementing-a-pki-part-ii.aspx

R. Housley, W. P. (2002, April). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Retrieved August 11, 2014, from IETF.org: http://tools.ietf.org/html/rfc3280

Roginsky, E. B. (2011, January). *Transitions: Recommendation for Transitioning the User of Cryptographic Algorithms and Key Lengths*. Retrieved August 22, 2014, from NIST Special Publication 800-131A: http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

S. Chokhani, W. F. (2003, November). *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. Retrieved August 11, 2014, from IETF.org: https://www.ietf.org/rfc/rfc3647.txt

Stephens, J. (2010, May 27). *Designing and Implentation a PKI: Part III Certificate Templates*. Retrieved August 7, 2014, from Ask the Directory Services Team: http://blogs.technet.com/b/askds/archive/2010/05/27/designing-and-implementing-a-pki-part-iii-certificate-templates.aspx

The SANS Institue. (2013). In D. E. Cole, *Security 401: SANS Security Essentials* (pp. 401.4; 1-10, 1-31). The SANS Institue.

William E. Burr, D. F. (2011, December). NIST Special Publication 800-63-1: Electronic Authentication Guideline. Gaithersburg, MD, United States. Retrieved August 6, 2014, from http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

7. Appendix

7.1. Example CAPolicy.INF file

```
                                CAPolicy.inf
;
; CAPolicy.inf File for:  Root CA (<ORGANIZATION_NAME>)
;
; Created:  <DATE>
; By:  <AUTHOR>
; Built from example at http://social.technet.microsoft.com/wiki/contents
;      /articles/15037.step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx
;
[Version]
Signature="$Windows NT$"
[PolicyStatementExtension]
Policies=InternalPolicy

[InternalPolicy]
; OID is unique to the PKI and was registered with ANSI or other standards body
(IANA).
;
; DOMAIN:  PROD  (internal production domain)
;
; The URL is an ALIAS that points to the CPS server (alias configured in the DNS
service of DC).  EDIT OID, NOTICE, and URL BELOW
;OID= <NOT USED IN THIS EXAMPLE; OID ADDED TO ISSUNG/INTERMEDIATE CA>
;
;Notice="Legal Policy Statement - This PKI is for the <ORGANIZATION>'s production
environment.  Refer to the associated Certificate Practice Statement (CPS) for more
information"
;URL=http://<externally_available_URL>/cps
;OID, Notice, and URL commented out due to design choice to support multiple
IssuingCA OIDs

[Certsrv_Server]
; Renewal information for this Root CA certificate.
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=19

; Since this is an OFFLINE root, the CRL publication period has been extended to the
lifetime of the Root CA.
; If a CRL needs to be updated from the root, then the root need to be brought back
online and a new CRL needs
; to be published, replacing the prior CRL for the root.

; The CRL publication period for the root CA should be set to the lifetime of the
Root CA.
CRLPeriod="Years"
CRLPeriodUnits=19

; The two CRL lines disable the publishing of Delta CRLs, which is something you
should not
; need to do for a root CA.  However, base CRLs are still published.
CRLDeltaPeriod=Days
CRLDeltaPeriodUnits=0
```

7.2. Root CA Post Install Script

```
                            PostInstallScript-RootCA.bat
echo off
REM
REM PostInstallConfig-RootCA
REM Created:  <DATE>
REM By:  <AUTHOR>
REM
REM This is a post-installation script (run after the Root CA was created) to
configure the Root CA.
REM
REM Note that this information is redundant with the information in the
c:\Windows\CAPolicy.inf file
REM
REM It is recommended that you are logged in as Administrator to run this script.
REM
REM
echo on

Echo Define Active Directory Configuration Partition Distinguished Name.  EDIT
DOMAIN INFORMATION BELOW
Certutil -setreg CA\DSConfigDN CN=Configuration,DC=PROD,DC=Company,DC=com

Echo Define CRL Period Units and CRL Period
Certutil -setreg CA\CRLPeriod "Years"
Certutil -setreg CA\CRLPeriodUnits 19

Echo Define CRL Overlap Period Units and CRL Overlap Period
Certutil -setreg CA\CRLOverlapPeriod "Weeks"
Certutil -setreg CA\CRLOverlapUnits 52

Echo Define Validity Period Units for all certificates issued by this Root CA.
Echo The Issuing CA should receive a 10 year lifetime for its CA certificate.
Certutil -setreg CA\ValidityPeriod "Years"
Certutil -setreg CA\ValidityPeriodUnits 10

Echo Enable Auditing on Root CA
Certutil -setreg CA\AuditFilter 127

Echo Get Reg Information
certutil -getreg CA > CAConfigInfo.txt

pause
```

Michael Naish, mnaishjr@gmail.com

7.3. Root CA AIA CDP Configuration Script

PostInstallScript-AIACDPConfig-RootCA.bat

```
echo off
REM
REM PostInstall-AIACDPConfig-RootCA
REM Created:  <DATE>
REM By:  <AUTHOR>
REM
REM This is a post-installation script (run after the Root CA was created) to
configure the AIA and CDP for this CA.
REM
REM It is recommended that you are logged in as Enterprise Administrator to run this
script.
REM
REM SYNTAX NOTE:  When using variables, TWO apersands need to be used instead of one
(this is not clear in the book or examples)
REM The % variables have specific meanings:
REM %1 = <serverDNSName>
REM %3 = COMPANY_PKI
REM %4 = RootCA
REM %8 = <CRLNameSuffix>
REM %9 = <DeltaCRLAllowed>
REM %7 = <CATruncatedName>
REM %6 = <ConfigurationContainer>
REM %10 = <CDPObjectClass>
REM %11 = <CAObjectClass>
REM
REM Publication Options (leading value in each string)
REM 1 - Publish CRLs to this location. Identifies locations to which the CA should
automatically publish the physical CRL files. ServerPublish.
REM 2 - Include in all issued certificates. Place a URL for the base CRL in all
certificates issued by the CA. AddtoCertCDP.
REM 4 - Include in CRLs. Clients use this to find delta CRL locations. Places a URL
for delta CRL retrieval in a base CRL. This publication point is stored in the
freshest CRL extension of a CRL and is retrieved only during the CRL

checking process. AddtoFreshestCRL.
REM 8 - Include in the CDP extension of CRLs. Places a URL in the CDP extension of a
CRL issued by the CA to allow the relying party certificate chaining engine to
download the latest CRL version if the current version has expired.

AddtoCRLCDP.
REM 64 - Publish delta CRLs to this location. Specifies where to publish in AD DS
when publishing to LDAP URLs. If the CA is configured to enable delta CRLs, the
delta CRL files are automatically published to this location.

ServerPublishDelta.
REM 128 - Include in the IDP extension of issued CRLs Used by non-Windows clients to
determine the scope of the CRL. The scope can include end-entity certificates only,
CA certificates only, attribute certificate only, or a limited set

of reason codes. IssuingDistributionPoint.

REM Reference: Komar, Brian (2010-03-23). Windows Server® 2008 PKI and Certificate
Security (Pro Other) (p. 115). Microsoft Press. Kindle Edition.

echo on

REM define CDP_Servers and CDP Server Alias.  EDIT CDP INFORMATION BELOW
set "CDP_Server_Alias1=certrev.dmzprod.company.com"
set "CDP_Server_Alias2=certrev.prod.company.com"
set "CDP_Server1=server3.prod.company.com"
set "CDP_Server2=server4.prod.company.com"

Echo Configure AIA...
```


PostInstallScript-AIACDPConfig-RootCA.bat

```
set "AIA_LOCAL=1:C:\Windows\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n"
set "AIA_LDAP=2:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services,%%6%%11\n"
set "AIA_HTTP1=2:http://%CDP_Server_Alias1%/CRL/%%1_%%3%%4.crt\n"
set "AIA_HTTP2=2:http://%CDP_Server_Alias2%/CRL/%%1_%%3%%4.crt\n"
set "AIA_SHARE1=1:file://%CDP_Server1%/CRL$/%%1_%%3%%4.crt\n"
set "AIA_SHARE2=1:file://%CDP_Server2%/CRL$/%%1_%%3%%4.crt\n"
set "AIA_STR=%AIA_LOCAL%%AIA_LDAP%%AIA_HTTP1%%AIA_HTTP2%%AIA_Share1%%AIA_SHARE2%
certutil -setreg CA\CACertPublicationURLs "%AIA_STR%"
echo "%AIA_STR%"

Echo Configure CDP...
set "CDP_LOCAL=1:C:\Windows\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n"
set "CDP_LDAP=10:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key
Services,CN=Services,%%6%%10\n"
set "CDP_HTTP1=2:http://%CDP_Server_Alias1%/CRL/%%3%%8%%9.crl\n"
set "CDP_HTTP2=2:http://%CDP_Server_Alias2%/CRL/%%3%%8%%9.crl\n"
set "CDP_SHARE1=1:file://%CDP_Server1%/CRL$/%%3%%8%%9.crl\n"
set "CDP_SHARE2=1:file://%CDP_Server2%/CRL$/%%3%%8%%9.crl\n"
set "CDP_STR=%CDP_LOCAL%%CDP_LDAP%%CDP_HTTP1%%CDP_HTTP2%%CDP_SHARE1%%CDP_SHARE2%
certutil -setreg CA\CRLPublicationURLs "%CDP_STR%"
echo "%CDP_STR%"

Echo Confirm AIA and CDP Settings...

certutil -getreg CA\CACertPublicationURLs > CRLConfigInfo.txt
certutil -getreg CA\CRLPublicationURLs >> CRLConfigInfo.txt
certutil -getreg CA > CAConfigInfo.txt

Echo Copy Root CA certificate and CRL to C:\ for ease of transport
copy /Y c:\Windows\System32\certsrv\certenroll\*.cr? c:\


pause
```


7.4. Issuing CA Example CA Policy.INF

CAPolicy.inf

```
;
; CAPolicy.inf File for: Issuing CA (<ORGANIZATION>)
;
; Created:  <DATE>
; By:  <AUTHOR>
; Built from example at
http://social.technet.microsoft.com/wiki/contents/articles/15037.step-by-step-guide-
two-tier-pki-hierarchy-deployment.aspx
;
[Version]
Signature="$Windows NT$"

[PolicyStatementExtension]
Policies=InternalPolicy

[InternalPolicy]
; OID is unique to the PKI and is registered with ANSI or other standards body
(IANA).
; DOMAIN:  PROD (internal production domain)
;
; The URL is an ALIAS that points to the CPS server (alias configured in the DNS
service of DC).  EDIT OID, NOTICE, and URL BELOW
OID=<OID>.<ADDITIONAL_INFO>
;
Notice="Legal Policy Statement - This PKI is for the <ORGANIZATION> production
environment.  Refer to the associated Certificate Practice Statement (CPS) for more
information"
URL=http://<internally_available_URL>/cps

[Certsrv_Server]
; Renewal information for this CA certificate.
RenewalKeyLength=4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=10

; The CRL publication period for the issuing CA.
CRLPeriod=Days
CRLPeriodUnits=7

; The Delta CRL publication period for the issuing CA.
CRLDeltaPeriod=Days
CRLDeltaPeriodUnits=1

; Do not install any templates by default
LoadDefaultTemplates=0
```

Michael Naish, mnaishjr@gmail.com

7.5. Issuing CA Pre-Install Configuration Script

PreInstallScript-DomainIssuingCA.bat

```
echo off
REM
REM PreInstallConfig-Issuing CA
REM Created:  <DATE>
REM By:  <AUTHOR>
REM
REM This is a Publication script (run before the Issuing CA is created) to ensure
the root CA CRT and CRL are in the domain controller and CDP.
REM
REM Note that this information is redundant with the information in the
c:\Windows\CAPolicy.inf file
REM
REM It is recommended that you are logged in as Enterprise Administrator to run this
script.
REM
echo on

REM EDIT CDP SERVER INFORMATION and CERTIFICATE FILE INFORMATION BELOW
set "CDP_Server1=server3.prod.company.com"
set "CDP_Server2=server4.prod.company.com"
set "Root_Cert=<ExportedRootCertFileName>"
set "Root_CRL=<ExportedRootCRLFileName>"

REM This published the cert in AIA of the DS, but pushes the CRL into a sub-folder
called CA01 of the CDP.
REM Review these locations in the Domain Controller
REM certutil -f -dspublish "\\%CDP_Server%\c$\certenroll\%Root_Cert%" RootCA
REM certutil -f -dspublish "\\%CDP_Server%\c$\certenroll\%Root_CRL%" CA01
certutil -f -dspublish "c:\%Root_Cert%" RootCA
certutil -f -dspublish "c:\%Root_CRL%"


REM Publish the local Certificate Store for this information on the Issuing CA
server.  These cmds expedite
REM publishing the certs to the local system
REM certutil -addstore -f root "\\%CDP_Server%\c$\certenroll\%Root_Cert%"
REM certutil -addstore -f root "\\%CDP_Server%\c$\certenroll\%Root_CRL%"
certutil -addstore -f root "c:\%Root_Cert%"
certutil -addstore -f root "c:\%Root_CRL%"

pause
```

7.6. Issuing CA Post Install Configuration Script

PostInstallScript-DomainIssuingCA.bat

```
echo off
REM
REM
REM PostInstallConfig-IssuingCA
REM Created:  <DATE>
REM By:  <AUTHOR>
REM
REM This is a post-installation script (run after the Issuing CA was created) to
configure the Issuing CA.
REM
REM Note that this information is redundant with the information in the
c:\Windows\CAPolicy.inf file
REM
REM It is recommended that you are logged in as Enterprise Administrator to run this
script.
REM
echo on

Echo Define CRL Period Units and CRL Period
Certutil -setreg CA\CRLPeriod "Weeks"
Certutil -setreg CA\CRLPeriodUnits 1

Echo Define CRL Overlap Period Units and CRL Overlap Period
Certutil -setreg CA\CRLOverlapPeriod "Hours"
Certutil -setreg CA\CRLOverlapUnits 48

Echo Define CRL Delta Period Units and Delta CRL Period
Certutil -setreg CA\CRLDeltaPeriod "Days"
Certutil -setreg CA\CRLDeltaUnits 1

Echo Define CRL Delta Overlap Period Units and CRL Overlap Period
Certutil -setreg CA\CRLDeltaOverlapPeriod "Hours"
Certutil -setreg CA\CRLDeltaOverlapUnits 6

Echo Define the Maximum Validity Period Units for all certificates ISSUED by this
CA.
Certutil -setreg CA\ValidityPeriodUnits 2
Certutil -setreg CA\ValidityPeriod "Years"

Echo Enable Auditing on the Issuing CA
certutil -setreg CA\AuditFilter 127

Echo Allow OCSP Response Signing certificates to be renewed by using existing CA
keys on the CA computer
certutil -setreg ca\UseDefinedCACertInRequest 1

Echo Get Reg Information
certutil -getreg CA > CAConfigInfo.txt

pause
```

7.7. Issuing CA AIA CDP Configuration Script

PostInstallScript-AIACDPConfig-DomainIssuingCA.bat

```
echo off
REM
REM PostInstall-AIACDPConfig-IssuingCA1
REM Created:  <DATE>
REM By:  <AUTHOR>
REM
REM This is a post-installation script (run after the Issuing CA was created) to
configure the AIA and CDP for this CA.
REM
REM It is recommended that you are logged in as Enterprise Administrator to run this
script. REM
REM SYNTAX NOTE:  When using variables, TWO apersands need to be used instead of one
(this is not clear in the book or examples)
REM The % variables have specific meanings:
REM %1 = <serverDNSName>
REM %3 = <CaName>
REM %4 = <certificateName>
REM %8 = <CRLNameSuffix>
REM %9 = <DeltaCRLAllowed>
REM %7 = <CATruncatedName>
REM %6 = <ConfigurationContainer>
REM %10 = <CDPObjectClass>
REM %11 = <CAObjectClass>
REM
REM Publication Options (leading value in each string)
REM 1 - Publish CRLs to this location. Identifies locations to which the CA should
automatically publish the physical CRL files. ServerPublish.
REM 2 - Include in all issued certificates. Place a URL for the base CRL in all
certificates issued by the CA. AddtoCertCDP.
REM 4 - Include in CRLs. Clients use this to find delta CRL locations. Places a URL
for delta CRL retrieval in a base CRL. This publication point is stored in the
freshest CRL extension of a CRL and is retrieved only during the CRL checking
process. AddtoFreshestCRL.
REM 8 - Include in the CDP extension of CRLs. Places a URL in the CDP extension of a
CRL issued by the CA to allow the relying party certificate chaining engine to
download the latest CRL version if the current version has expired. AddtoCRLCDP.
REM 64 - Publish delta CRLs to this location. Specifies where to publish in AD DS
when publishing to LDAP URLs. If the CA is configured to enable delta CRLs, the
delta CRL files are automatically published to this location. ServerPublishDelta.
REM 128 - Include in the IDP extension of issued CRLs Used by non-Windows clients to
determine the scope of the CRL. The scope can include end-entity certificates only,
CA certificates only, attribute certificate only, or a limited set of reason codes.
IssuingDistributionPoint.

REM Reference: Komar, Brian (2010-03-23). Windows Server® 2008 PKI and Certificate
Security (Pro Other) (p. 115). Microsoft Press. Kindle Edition.


echo on

REM EDIT CDP SERVER INFORMATION

set "CDP_Server_Alias1=certrev.dmzprod.company.com"
set "CDP_Server_Alias2=certrev.prod.company.com"
set "CDP_Server1=server3.prod.company.com"
set "CDP_Server2=server4.prod.company.com"

Echo Configure AIA...
set "AIA_LOCAL=1:C:\Windows\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n"
set "AIA_LDAP=2:ldap:///CN=%%7,CN=AIA,CN=Public Key Services,CN=Services,%%6%%11\n"
set "AIA_HTTP1=2:http://%CDP_Server_Alias1%/crl$/%%1_%%3%%4.crt\n"
set "AIA_HTTP2=2:http://%CDP_Server_Alias2%/crl$/%%1_%%3%%4.crt\n"
set "AIA_SHARE1=1:file://%CDP_Server1%/crl$/%%1_%%3%%4.crt\n"
```


PostInstallScript-AIACDPConfig-DomainIssuingCA.bat

```
set "AIA_SHARE2=1:file://%CDP_Server2%/crl$/%%1_%%3%%4.crt\n"
set "AIA_OCSP=32:http://%CDP_Server_Alias2%/ocsp
set
"AIA_STR=%AIA_LOCAL%%AIA_LDAP%%AIA_HTTP1%%AIA_HTTP2%%AIA_SHARE1%%AIA_SHARE2%%AIA_OCS
P%
certutil -setreg CA\CACertPublicationURLs "%AIA_STR%"
echo "%AIA_STR%"

Echo Configure CDP...
set "CDP_LOCAL=65:C:\Windows\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n"
set "CDP_LDAP=11:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key
Services,CN=Services,%%6%%10\n"
set "CDP_HTTP1=6:http://%CDP_Server_Alias1%/crl$/%%3%%8%%9.crl\n"
set "CDP_HTTP2=6:http://%CDP_Server_Alias2%/crl$/%%3%%8%%9.crl\n"
set "CDP_SHARE1=65:file://%CDP_Server1%/crl$/%%3%%8%%9.crl"
set "CDP_SHARE1=65:file://%CDP_Server1%/crl$/%%3%%8%%9.crl"
set "CDP_OCSP"=32:http://%CDP_Server_Alias2%/ocsp
set
"CDP_STR=%CDP_LOCAL%%CDP_LDAP%%CDP_HTTP1%%CDP_HTTP2%%CDP_SHARE1%%CDP_SHARE2%%CDP_OCS
P%
certutil -setreg CA\CRLPublicationURLs "%CDP_STR%"
echo "%CDP_STR%"

Echo Copy Issuing CA Certificate and CRL to c:\. these are to be copied to the CDP
manually.
copy /Y c:\Windows\System32\certsrv\certenroll\*.cr? c:\


Echo Confirm AIA and CDP Settings...

certutil -getreg CA\CACertPublicationURLs > CRLConfigInfo.txt
certutil -getreg CA\CRLPublicationURLs >> CRLConfigInfo.txt
certutil -getreg CA > CAConfigInfo.txt

pause
```


Michael Naish, mnaishjr@gmail.com