Secure CDP publishing with Forefront TMG and the HTTP-filter

# Abstract

In this article we will first cover some basic information about a Public Key infrastructure which uses CRL, OCSP, CDP and AIA information to keep ensure that revoked or not more valid certificates cannot be used to provide secure access to applications. Next I will show you how to securely publish the CDP with Forefront TMG and the help of the HTTP-filter.

## Let's begin

A Public Key Infrastructure (PKI) is a combination of certificates, services, policies, software and hardware to manage the complete lifecycle of certificates. This lifecycle includes the creation of certificates, issuing, managing and revoking of certificates. The primary part of a PKI is a Certification Authority which is responsible for issuing and revoking certificates for services, clients, Server, people, Smartcards and many more.

Certification Authorities will be distinguished between private and commercial Certificate Authorities. Each of this CA types has pros and cons. If you are using a private CA, you can use the built in Certificate Authority of the Windows Server 200x Operating System. The following screenshot shows the UI of a Windows Server 2008 R2 Enterprise CA.



Figure 1: Certification Authority MMC

As mentioned above, a CA is also responsible for revoking certificates, if issued certificates are out of lifetime or if they must be revoked due to certificate compromise, certificate lost and some more reasons.

Depending on the application or service, not all application checks a certificate for revocation but if a revocation check is required the application must know from where it can download the list of revoked certificates.

The path for revoked certificates is defined in the CDP (Certificate Distribution Point). The CDP contains the Certificate Revocation List (CRL) which must be downloaded by the client or application to get informed about the certificate status during a certificate trust check. A Windows Server 2008 R2 CA publishes the CRL to different locations, containing LDAP, Windows file system and HTTP as you can see in the following screenshot.

General						
	Policy Mo	odule	Exit	t Module		
Extensions	Storage		Certificate I	Managers		
Select extension:						
CRL Distribution Point	(CDP)			•		
CRL Distribution Point	(CDP)					
(Children Authority Information Au	ccess (AIA)					
C:\Windows\svstem32	CertSrv\Cert	Enroll\ <ca< td=""><td>Name&gt;<crln< td=""><td>lameSuffix&gt;&lt;</td></crln<></td></ca<>	Name> <crln< td=""><td>lameSuffix&gt;&lt;</td></crln<>	lameSuffix><		
Idap:///CN= <catrunc< td=""><td>atedName&gt;<c< td=""><td>RLNameS</td><td>uffix&gt;,CN=<s< td=""><td>erverShortNa</td></s<></td></c<></td></catrunc<>	atedName> <c< td=""><td>RLNameS</td><td>uffix&gt;,CN=<s< td=""><td>erverShortNa</td></s<></td></c<>	RLNameS	uffix>,CN= <s< td=""><td>erverShortNa</td></s<>	erverShortNa		
file:// <serverdnsnam< td=""><td>me&gt;/CertEnroll. 1e&gt;/CertEnroll/</td><td>/<caname <caname< td=""><td>e&gt;<crlname &gt;<crlnames< td=""><td>Suffix&gt;<delta Suffix&gt;<delta< td=""></delta<></delta </td></crlnames<></crlname </td></caname<></caname </td></serverdnsnam<>	me>/CertEnroll. 1e>/CertEnroll/	/ <caname <caname< td=""><td>e&gt;<crlname &gt;<crlnames< td=""><td>Suffix&gt;<delta Suffix&gt;<delta< td=""></delta<></delta </td></crlnames<></crlname </td></caname<></caname 	e> <crlname &gt;<crlnames< td=""><td>Suffix&gt;<delta Suffix&gt;<delta< td=""></delta<></delta </td></crlnames<></crlname 	Suffix> <delta Suffix&gt;<delta< td=""></delta<></delta 		
•				•		
		ŀ	\dd	Remove		
Publish CRLs to this	location					
Include in all CRLs.	Specifies whe	re to publis	h in the Activ	e Directory		
when publishing ma	mually.					
🔲 Include in CRLs. Cli	Include in CRLs. Clients use this to find Delta CRL locations.					
Include in the CDP extension of issued certificates						
Publish Delta CRLs to this location						
Include in the IDP extension of issued CBLs.						
	ensentitionen tel 199	9999 WI 169				

Figure 2: CRL Distribution point

The problem begins when there are domain joined clients such Notebooks, which are connected to the Internet and must check certificates for revocation. Because by default the CDP only contains the internal URL of the issuing CA, a certificate revocation check cannot be done. To overcome this limitation you can modify the CDP with a HTTP location which contains a public URL. With the help of Forefront TMG it is possible to publish the CRL to the Internet. A CRL publishing is a Standard Webserver publishing rule with Forefront TMG. Later in this article I will show you the high level steps how to publish the CRL wit Forefront TMG.

As the next step we must extend the CDP of the CA with a public URL which must be reachable from the Internet with the HTTP protocol. There are many ways to extend the CA with a new HTTP CDP but in my opinion one of the best ways is to use a script to modify the CDP. The next screenshot will show you the content of the script

ite Advanced in the iteration is a service of the EAS-CA
certutil -setreg CA\understand CALE Advanced in the EAS-CA
certutil -setreg CA\understand for the

You have to change the script with your internal Active Directory Configuration Partition information and the CRL and AIA location. Thanks to Carsten Zuege how gave me access to this script.

#### OCSP

A detailed description of the OCSP (Online Certificate Status Protocol) is out of the scope of this article but I like to give you some basic informations about the OCSP protocol which can be used as a alternative to the classic CRL publication. The OCSP protocol allows a client to query the status of revoked certificates online against a CA. The CRL must be downloaded by the client as part of a full or delta CRL download. Windows Server 2008 R2 contains a OCSP Responder, as shown in the following screenshot.

File       Action       View       Actions         Image: Signing Certificate Selection       Enrollment Template       Actions     <	🖪 ocsp - [Online Responder: UAG.trai	ner.intern\Revocation Configuration]			_ & ×
Image: Signing Certificate Selection       Enrollment Template         Image: Signing Certificate Selection       Configuration         Image: Signing Certificate Selection       Enrollment Template         Image: Signing Certificate Selection       Configuration         Image: Signing Certificate Selection	File Action View Help				
Image: Signing Certificate Selection       Enrollment Template       Actions         Revocation Configuration       Image: Signing Certificate Selection       Enrollment Template       Actions         Image: Properties for Revocation Configuration:       Image: Signing Certificate Selection       CSPResponseSigning       Revocation Configuration         Image: Properties for Revocation Configuration:       Image: Signing Certificate Selection       Image: Signing Certificate Selection       Revocation Configuration         Image: Certificate Selection       Image: Signing Certificate Selection       OCSPResponseSigning       Revocation Configuration         Image: Certificate Selection       Image: Signing Certificate Selection       OCSPResponseSigning       Revocation Configuration         Image: Certificate Selection       Image: Signing Certificate Selection       OCSPResponseSigning       Revocation Configuration         Image: Certificate Selection       Image: Signing Certificate Selection       Image: Signing Certificate Selection       Configuration         Image: Certificate Selection       Image: Signing Certificate Selection       Image: Signing Certificate Selection       Certificate Selection         Image: Certificate Selection       Image: Signing Certificate Selection       Image: Signing Certificate Selection       Certificate Selection       Certificate Selection         Image: Certificate Selection       Image: Signing Certificate S	🗢 🔿 🖄 🗟 🗟				
Revocation Configuration Array Configuration UAG. trainer.intern Properties for Revocation Configuration: ISASERVER.ORG Add Revocation Configuration: ISASERVER.ORG View ORefresh	Inline Responder: UAG.trainer.intern	Name	Signing Certificate Selection	Actions	
Add Revocation Configuration: ISASERVER.ORG	Revocation Configuration	JSASERVER.ORG	Automatically enrolled	OCSPResponseSigning	Revocation Configuration 🔺
Properties for Revocation Configuration: ISASERVER.ORG View View	UAG.trainer.intern				Add Revocation Configur
Local CRL Revocation Provider Staning		<b>Properties for Revocation Conf</b>	iguration: ISASERVER.ORG	×	View
		Local CRL Revocation Provider	Signing		Q Refresh
Type:		Type:			Export List
Microsoft CRL-based revocation status provider		Microsoft CRL-based revocation s	tatus provider		P Help
Provider description:		Provider description:	antificate based on a CPI insued by	CA	ISASERVER.ORG
Veines the revocation status of a central based of the tasked by CA		Venines the revocation status of a	Revocation Provider Properties		X w CA Certificate
Properties					Properties
based on CRL issued by the CA.			based on CRLs issued by the CA.	s the revocation status of certific	ates ate
Identify the locations for the CRLs.			Identify the locations for the CRLs	•	etc
Base CRLs:			Base CRLs:		lanc
Idap:///CN=RootCA,CN=TRAINER-DC,CN=CDP,CN=Pu A Move up P			<pre>ldap:///CN=RootCA,CN=TRAINER http://crl.trainer.de/certenroll/Root</pre>	otCA.crl	ve up
Move down				Mov	re down
Add Edit Delete			Add Ed	it Delete	
Delta CRLs:			Delta CRLs:		
Move up				in Ma	ive up
Maye down				- Mov	re down
			<b>T</b>		
Add Edit Delete			Add Ed	it,,, Delete	
✓ Refresh CRLs based on their validity periods			Refresh CRLs based on their va	alidity periods	
Update CRLs at this refresh interval (min):			Update CRLs at this refresh int	erval (min):	
				,	
OK Cancel		1		ОК С	ancel

Figure 4: OCSP configuration

## **CRL** publishing with Forefront TMG

Now we can start configuring Forefront TMG to publish the internal CRL to the Internet. We are using the Website Publishing rule wizard. I will only show you the most important steps in the publishing wizard.

First, we must give the publishing rule a name and allow the connection. We are publishing a single website or load balancer. Because a CRL is accessed via a non-encrypted HTTP connection, we only use HTTP.

New Web Publishing Rule Wizard	X
Server Connection Security Choose the type of connections Forefront TMG will establish w Web server or server farm.	with the published
Use SSL to connect to the published Web server or server farm Forefront TMG will connect to the published Web server or server farm using HTTPS (recommended).	HTTPS://
<ul> <li>Use non-secured connections to connect the published Web server or server farm</li> <li>Forefront TMG will connect to the published Web server or server farm using HTTP.</li> </ul>	HTTP://
When Forefront TMG authenticates to the published ser dient, user credentials may be sent over the network in using SSL will help protect dient credentials.	ver on behalf of the clear text. Authentication
< Back	Next > Cancel

Figure 5: HTTP Webserver publishing

Next, enter the FQDN of the internal CA Server in the wizard. The path to publish is the /Certenroll directory on the IIS of the CA server.

New Web Publishing Rule W	lizard	×
Internal Publishing Deta Specify the internal pat can publish the entire V	ails th and publishing options of the published Web site. You Web site, or limit access to a specified folder.	
Enter the name of the file or within a folder use /*. Examp	folder you want to publish. To include all files and subfolde ole: folder/*.	rs
Path (optional):	/certenroll/*	
Based on your selection, the	following Web site will be published:	
Web site:	http://trainer-dc.trainer.intern/certenroll/*	
Forward the original host name field on the previou	: header instead of the actual one specified in the Internal	site
	< <u>B</u> ack <u>N</u> ext >	Cancel

Figure 6: CRL publishing path

**Please note**: We will restrict access to the required path after the wizard has been finished.

We will accept requests for the public name which you entered previously as a CRL path in the CDP location of your CA server. In this example the CRL will be published to CRL.TRAINER.DE.

New Web Publishing Rule Wizard		×
Public Name Details Specify the public domain name (F published site.	FQDN) or IP address users will type to reach the	
<u>A</u> ccept requests for: Only requests for this public name or IF	This domain name (type below): P address will be forwarded to the published site.	•
Public name:	crl.trainer.de	
	Example: www.contoso.com	
Path (optional):	/certenroll/*	
Based on your selections, requests sen	nt to this site (host header value) will be accepted	d:
Site: http://crl.trai	iner.de/certenroll/*	
	< <u>B</u> ack <u>N</u> ext > 0	Cancel

Figure 7: Public name

Next we must create a new weblistener which accepts HTTP connections.

New Web Listener Definition Wizard
Client Connection Security Select what type of connections this Web Listener will establish with clients.
C Require SSL secured connections with clients Forefront TMG will publish servers only over HTTPS to the clients (recommended).
Do not require SSL secured connections with clients     Forefront TMG will publish servers over HTTP. Client     credentials will be sent unencrypted to the Forefront TMG     computer.
If client authentication is required, user credentials may be sent over the network in clear text, depending on the selected client authentication method. Authentication using SSL will help protect client credentials.
< Back Next > Cancel

Figure 8: Connect via HTTP

Select the network EXTERNAL or a specific IP address of the external network and select *No authentication*.

Because no authentication is required we select *No delegation, and client cannot authenticate directly* in the authentication delegation window.

New Web Publishing Rule Wizard
Authentication Delegation Authentication delegation is the method Forefront TMG uses to authenticate the session it opens with the published site.
Select the method used by Forefront TMG to authenticate to the published Web server:
No delegation, and client cannot authenticate directly
Description If the published Web server requests HTTP authentication, Forefront TMG will not pass the authentication request to the user. The user will not be able to authenticate to the published Web server. The client request will be denied.
< <u>B</u> ack <u>N</u> ext > Cancel

Figure 9: No Authentication delegation

The rule accepts access for *All Users*. Click *Finish* to end the publishing wizard and after that click *Apply* to save the configuration.

After the publishing rule has been created, open the publishing rule, navigate to the *Path* tab and restrict the path to the full path for downloading the CRL as shown in the following screenshot.

**Attention**: You have to change the path to your current CA configuration. In my example the CA has the name RootCA, so the CRL file is called RootCA.CRL and RootCA+.CRL.

Attention: If your clients need access to download the RootCA+.CRL file, it might be necessary to allow double byte encoding in the web.config file on the IIS Server of the CA.

CRL Publish Properties	>
Bridging       Users       Schedule         Authentication Delegation       Applic         General       Action       From       To       Traffic       Listener       H         This rule applies to requests for these external paths. E forwarding a request, Forefront TMG modifies the exter maps it to the corresponding internal path on the Web	Link Translation ation Settings Public Name Paths Before mal path and server.
External Path         Internal Path <same as="" internal="">         /certenroll/RootCA+.crl           <same as="" internal="">         /certenroll/RootCA.crl</same></same>	Add
, Paths must be distinct from each other. A path cannot another path. This is true for external and internal path Example: /pathA/* and /pathB/* are distinct external paths.	be a prefix of s. and internal
Test Rule OK Cance	el <u>A</u> pply

Figure 10: Restrict the path to the CRL

Test the CRL download from an Internet client. Enter the path to the CRL into your Web browser and now it should be possible to download the CRL.

						0 444					
(F)	🕑 🥭 http	o://crl.train	er.de/certen	roll/Root	CA.crl	D + C X	🥭 Leere Seite		×		<u> </u>
Datei	Bearbeiten	Ansicht	Favoriten	Extras	7						
											-
		Möchten S	Sie "RootCA.	crl" (712	Bytes) von " <b>crl.trainer.de</b> "	öffnen oder spe	eichern?	Öffnen	Speichern	<ul> <li>Abbrechen</li> </ul>	×
Figur	e 11: CRI	downl	oad test								

## **HTTP-filter**

You can use the HTTP-filter in Forefront TMG to provide some additional security for the CRL publishing rule. For this example I restricted the maximum URL and URL query length to 256 Byte and the maximum header length to 513 bytes.

Attention: These settings will depend on your current environment, so you have to play with these settings.

## Important:

The HTTP Filter in Forefront TMG is rule specific except the Maximum Header length setting. The maximum Header length in Forefront TMG is the same for all Firewall rules with HTTP protocol definitions.

**Please note**: The maximum header length must be greater than the sum of the maximum URL and URL query length.

Configure HTTP policy for rule						
General Methods Extensions Headers Signatures						
- Request Headers						
Maximum headers length (bytes):	513					
Request Payload						
Allow any payload length						
Maximum payload length (bytes):	64					
URL Protection						
Maximum URL length (bytes):	256					
Maximum query length (bytes):	256					
Verify normalization	· · · · · · · · · · · · · · · · · · ·					
Block high bit characters						
Je block responses containing windows executable (	Jorneant					
	Ápolu.					
	ALAH					

Figure 12: HTTP-filter URL length settings

I also instructed Forefront TMG to block Windows executable content and allowed a maximum payload length of 64 bytes.

If you configure the HTTP-filter to restrictive, you will get an error message like the following.



Figure 13: HTTP-filter error message

Because clients will only download the CRL we will allow only the HTTP GET extension.

Configure HTT	P policy for rule	? ×
General Met	hods Extensions Headers Signatures	5
Specify the	action taken for HTTP methods:	
Allow only	specified methods	
Method	Description	Add
GET		Edit
		Remove
	OK Cano	cel Apply

Figure 14: Restrict access to HTTP GET

Next, we configure the HTTP-filter to only allow the .CRL extension to be downloaded.

Configure HTTP policy for rule	? ×				
General Methods Extensions Headers Signatures	,				
Specify the action taken for file extensions:					
Allow only specified extensions					
Extension Description	Add				
CRL	Edit				
	Remove				
Block requests containing ambiguous extensions					
OK Cancel	Apply				

Figure 15: Allow only the .CRL extension for downloads

#### Conclusion

In this article I tried to give you an overview about Windows certificate services and the process of Certificate revocation with CRL and OCSP. We also had a look how to securely publish a CRL to the Internet with Forefront TMG and the HTTP-filter.

#### **Related links**

Microsoft Active Directory Certificate Services http://www.microsoft.com/PKI/ Configure CDP and AIA Extensions http://technet.microsoft.com/en-us/library/cc776904(WS.10).aspx Publishing Certificate Revocation Lists with ISA Server 2006 - Part 1: Creating the **Publishing Rule** http://blog.msfirewall.org.uk/2008/06/publishing-certificate-revocation-lists.html How to configure Certificate Services and ISA Server to publish CRLs http://support.microsoft.com/kb/318707 Publishing a Public Key Infrastructure with ISA Server 2004 (Part 1) http://www.isaserver.org/tutorials/Publishing-Public-Key-Infrastructure-ISA-Server-2004-Part1.html How to Configure UAG to Publish Your Private Certificate Revocation List http://blogs.technet.com/b/tomshinder/archive/2010/08/03/how-to-configure-uag-topublish-your-private-certificate-revocation-list.aspx Configure a CA to Support OCSP Responders http://technet.microsoft.com/en-us/library/cc732526.aspx Configuring the Forefront TMG HTTP Filter

http://www.isaserver.org/tutorials/Configuring-Forefront-TMG-HTTP-Filter.html