Web server certificate enrollment with SAN extension

PKI pkisolutions.com/web-server-certificate-enrollment-with-san-extension

January 24, 2024

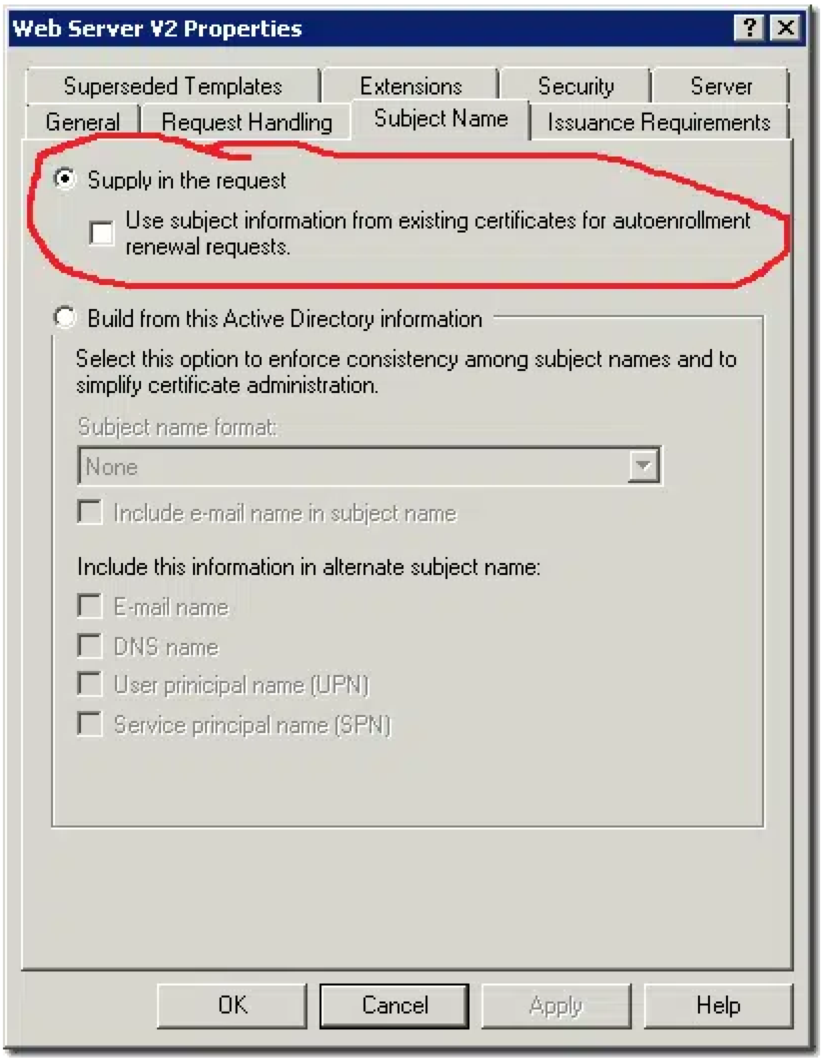
As part of joining PKI Solutions, several blog posts from my old site are re-posted here for visibility and thoroughness.

Many of windows administrators requires to setup SSL on their web servers and mostly they wish to use certificates with the Subject Alternative Name extension that allows to map a single certificate to a multiple web sites. For example, you want to use a single certificate for and . In that case you need to have multiple subjects in the certificate. However X.509 certificates don’t support multiple subject fields. To resolve this issue, Subject Alternate Name extension is used. You can add multiple (even wildcard) subjects to a certificate.

Some time ago (in the case of Windows 2000 and Windows Server 2003), administrators had to use Enrollment Web Pages or use certreq.exe utility in conjunction with a custom INF file (not user-friendly way) because there is no way to generate a custom request from Certificates MMC snap-in. The life was beautiful until Windows Vista and Windows Server 2008 were released. Administrators tried to use a web enrollment to enroll computer certificates for a new OSs. And heck, this hadn’t worked! Yes, old XEnroll ActiveX control is not supported by Windows Vista and higher. Administrators had to install update: KB922706 that adds CertEnroll (native for Windows Vista and higher) ActiveX control. And another heck, there is no option to enroll computer certificates at all! Many administrators overlooked extremely powerful updated Certificates MMC snap-in. Now it is very-very easy to enroll a certificate with a custom SAN extension.

Prepare certificate template

Most certificate templates are configured to build a subject from Active Directory. However this is not common for SSL certificates, because they usually use custom subject name instead of computer’s FQDN. Therefore it is necessary to configure certificate template, that allows subject name supplying within certificate request. If you use default **WebServer** template, no additional steps are required. If you use custom certificate template you must ensure if the subject name is constructed from certificate request as shown:



● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests.

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name

□ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

In addition you must assign **Read** and **Enroll** permissions in the Security tab for your web server ***computer*** account or a custom global or universal group that contains required computer accounts.

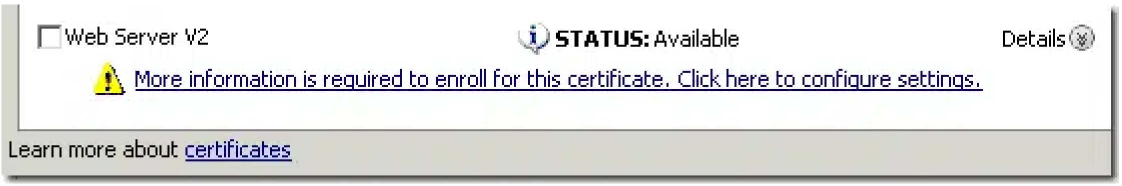
Prepare Certification Authority

Make sure if certificate template is supported by issuing CA. Run **CertSrv.msc** MMC snap-in, expand your CA name and select **Certificate Templates** node. If required template is listed in the window, no additional steps are required. Otherwise right-click on the node, click **New –> Certificate Template to Issue**. In the list select required template and click **Add**.

Certificate enrollment

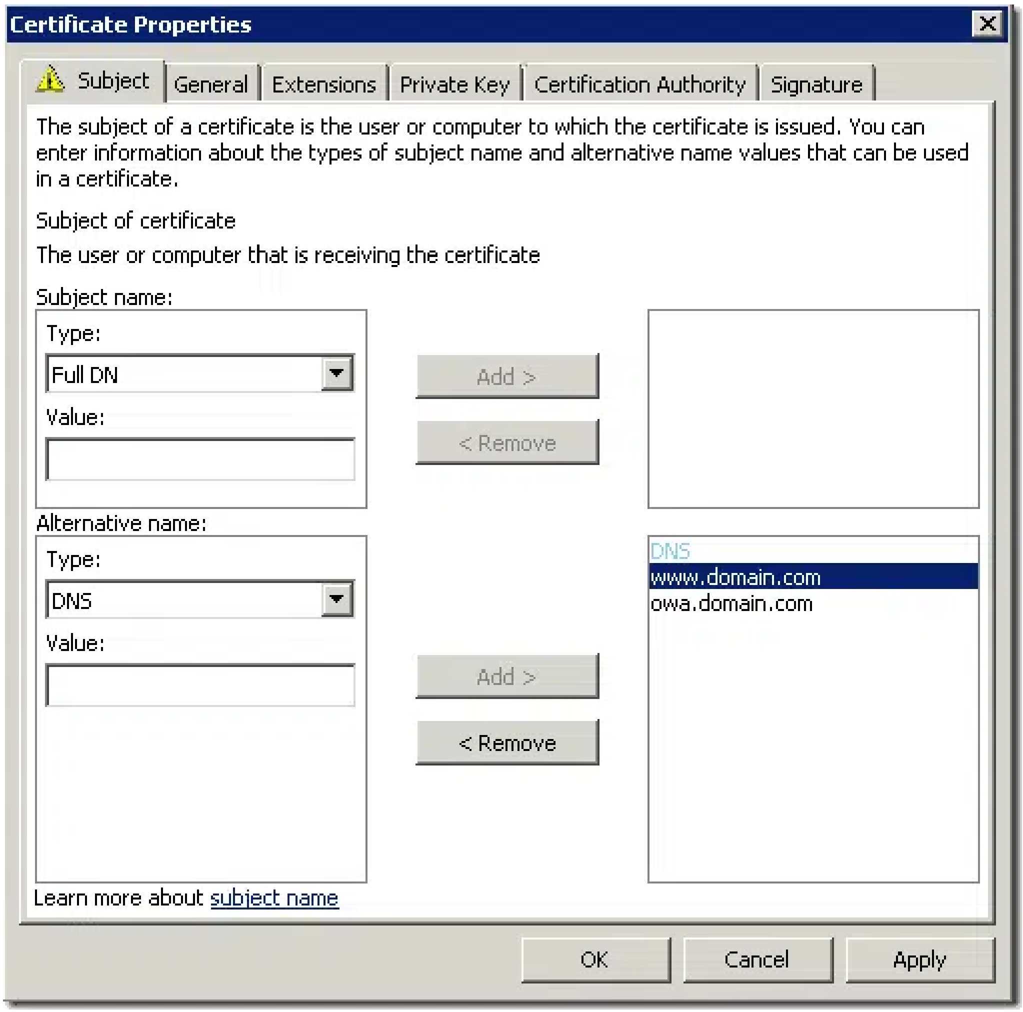
;

- Log on to the web server using domain account with local administrator permissions.
- On the Windows desktop~~,~~ click **Start**, and then click **Run**.
- In the **Run** dialog box type **mmc**, and then click **OK**. If **User Account Control** is enabled, enter required account credentials or just click **Yes** on consent window.

- In the **Console1** window, click **File**, and then click **Add/Remove Snap-in**.
- In the **Add/Remove Snap-in** dialog box, click **Add**.
- In the **Add Standalone Snap-in** dialog box, click **Certificates** and switch radiobutton to **Computer account** and click **Next**.
- In the **Select computer** dialog box use **Local computer** option (default value), click **Finish** and click **Ok**.
- Right-click on **Personal** node, click **All Tasks** and click **Request new certificate**.
- In the **Before you begin** page you can learn about certificate enrollment wizard. Click **Next**.
- If **Select Enrollment Policy** dialog box appear, select appropriate enrollment policy and click **Next**. You should see something like this:
- 

  □ Web Server V2 STATUS: Available

  More information is required to enroll for this certificate. Click here to configure settings.

- Select certificate template, and click the warning message and you will see the following dialog box:
- 

  Certificate Properties

  The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

  Subject of certificate

  The user or computer that is receiving the certificate

  Subject name:

  Type: Full DN

  Value:

  Alternative name:

  Type: DNS

  Value:

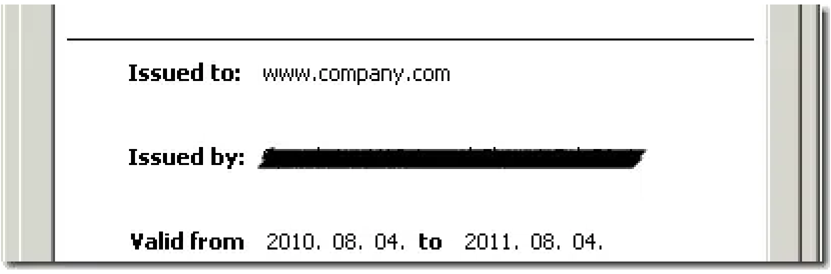
  DNS
  www.domain.com
  owa.domain.com

- You may leave Subject field as empty if you decide to use subject alternative name extension. Expand drop-down **Type** listand select proper SAN format. For SSL certificates **DNS** type is common. In the value edit box type a name in the corresponding format and click **Add**. Repeat the procedure so mush times as it is necessary and click **Ok** when all SAN fields are complete.
- You will be returned to **Certificate Enrollment** wizard. You may notice that warning message is disappeared.
- Click **Enroll** to enroll a certificate.

> **Note:** I recommend to leave Subject field as empty in the case when you use multiple SAN fields. In that case Subject filed will be empty and one of the SANs will be used by clients. In addition, SAN extension will be marked as critical, because this will the only extension that will allow to identify server name.
>
> **Tip:** what means "extension is marked as critical"? Perhaps you remember one cool Slade song:
>
> *"You know what my freedom means to me*
> *What it means, what it means to me*
> *Just exactly what my freedom means to me"*
>
> This means that if an application see any critical extension, the application MUST process this extension. If critical extension is empty or unclear for that application (cannot recognize extension contained value), application MUST reject the certificate.

Here are some issued certificate screenshots:

Certificate view:

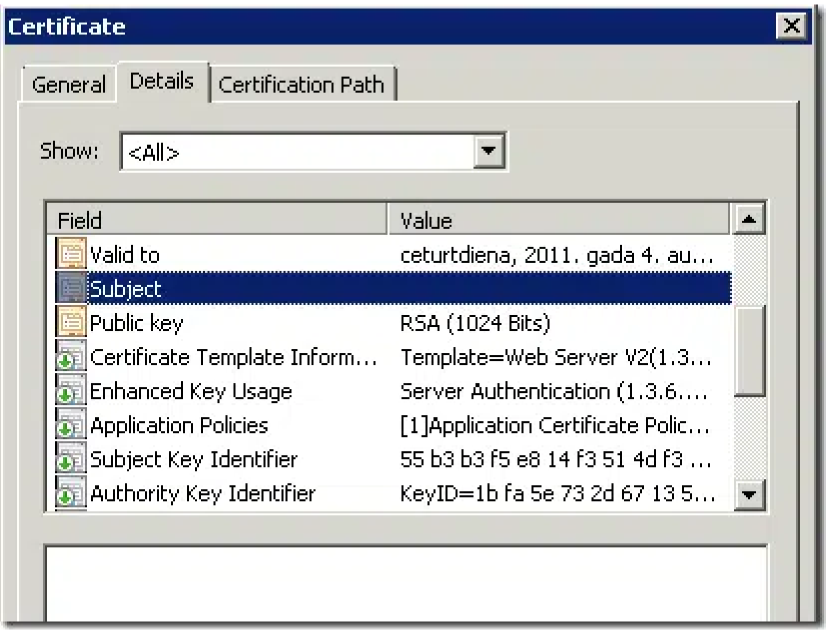


Issued to: www.company.com

Issued by: [redacted]

Valid from 2010. 08. 04. **to** 2011. 08. 04.

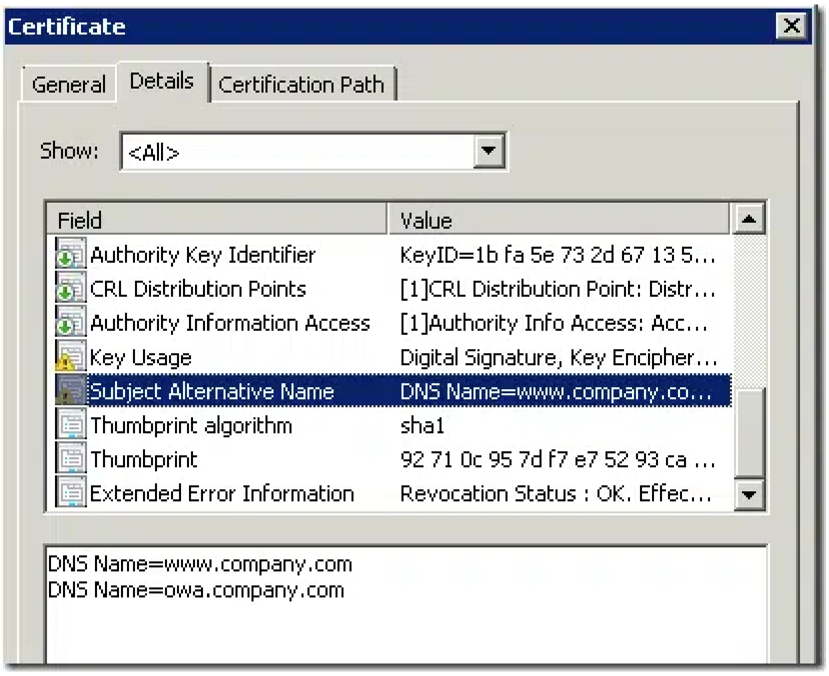
Empty Subject field



Show: <All>

Field	Value
Valid to	ceturtdiena, 2011. gada 4. au...
Subject	
Public key	RSA (1024 Bits)
Certificate Template Inform...	Template=Web Server V2(1.3...
Enhanced Key Usage	Server Authentication (1.3.6....
Application Policies	[1]Application Certificate Polic...
Subject Key Identifier	55 b3 b3 f5 e8 14 f3 51 4d f3 ...
Authority Key Identifier	KeyID=1b fa 5e 73 2d 67 13 5...

SAN extension:



Show: <All>

Field	Value
Authority Key Identifier	KeyID=1b fa 5e 73 2d 67 13 5...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature, Key Encipher...
Subject Alternative Name	DNS Name=www.company.co...
Thumbprint algorithm	sha1
Thumbprint	92 71 0c 95 7d f7 e7 52 93 ca ...
Extended Error Information	Revocation Status : OK. Effec...

```
DNS Name=www.company.com
DNS Name=owa.company.com
```

See that SAN extension is marked as critical (yellow sign on the extension icon), as said this is because we have empty Subject field. There are no addition configuration steps required, because SAN critical flag is automatically determined by CA policy module.