Adding SAN (Subject Alternative Name” into “Additional Attributes” field on a Microsoft Certificate Authority certificate request form does not generate a certificate with a SAN entry

terenceluk.blogspot.com/2017/09/adding-san-subject-alternative-name.html

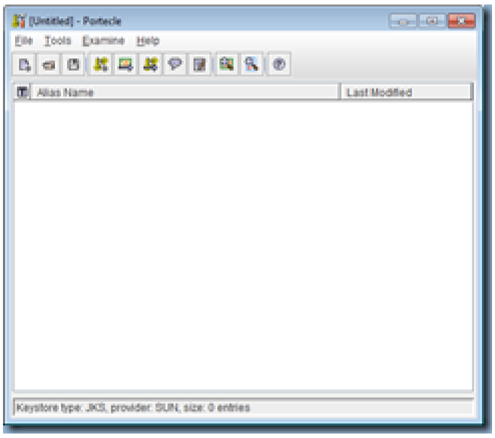
Problem

You’ve completed the process of creating a new keystore with a CSR from the Portecle utility:

http://portecle.sourceforge.net/

Since the Portecle utility does not provide the feature to include SAN entries:

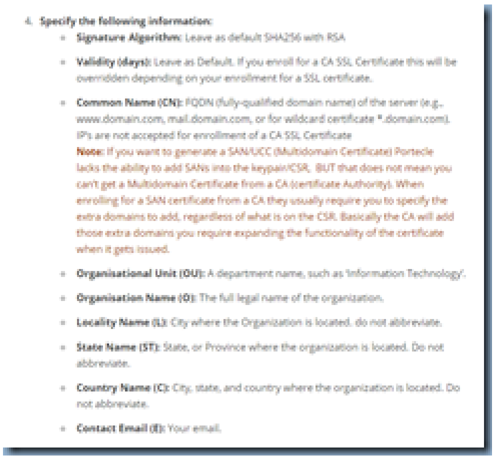
https://www.sslsupportdesk.com/portecle-advanced-keystore-creation-and-manipulation-tool/



Keystore type: JKS, provider: SUN, size: 0 entries

This isn’t usually a problem because it is possible to add SAN entries in the **Additional Attributes** field when submitting the CSR to a Microsoft Certificate Authority server as described here:

How to add a subject alternative name to a secure LDAP certificate
https://support.microsoft.com/en-us/help/931351/how-to-add-a-subject-alternative-name-to-a-secure-ldap-certificate



4. **Specify the following information:**
    - **Signature Algorithm:** Leave as default SHA256 with RSA
    - **Validity (days):** Leave as Default. If you enroll for a CA SSL Certificate this will be overridden depending on your enrollment for a SSL certificate.
    - **Common Name (CN):** FQDN (fully-qualified domain name) of the server (e.g., www.domain.com, mail.domain.com, or for wildcard certificate *.domain.com). IP's are not accepted for enrollment of a CA SSL Certificate
      Note: If you want to generate a SAN/UCC (Multidomain Certificate) Portecle lacks the ability to add SANs into the keypair/CSR. BUT that does not mean you can't get a Multidomain Certificate from a CA (certificate Authority). When enrolling for a SAN certificate from a CA they usually require you to specify the extra domains to add, regardless of what is on the CSR. Basically the CA will add those extra domains you require expanding the functionality of the certificate when it gets issued.
    - **Organisational Unit (OU):** A department name, such as 'Information Technology'.
    - **Organisation Name (O):** The full legal name of the organization.
    - **Locality Name (L):** City where the Organization is located. do not abbreviate.
    - **State Name (ST):** State, or Province where the organization is located. Do not abbreviate.
    - **Country Name (C):** City, state, and country where the organization is located. Do not abbreviate.
    - **Contact Email (E):** Your email.

An example of the format of the string to include is:

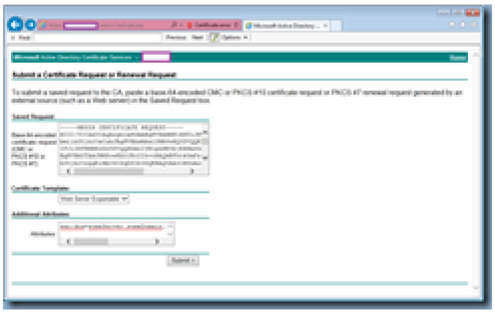
san:dns=corpdc1.fabrikam.com&dns=ldap.fabrikam.com

You proceed to submit the request:

… but notice that the generated certificate does not include a SAN entry.

Solution

One of the reasons why performing the above would not generate a certificate that includes a SAN entry is if the issuance policy of the Microsoft CA is not configured to accept the Subject Alternative Name(s) attribute via the CA Web enrollment page. To correct this, execute the following command:



Microsoft Active Directory Certificate Services -- [redacted]

Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server Exportable

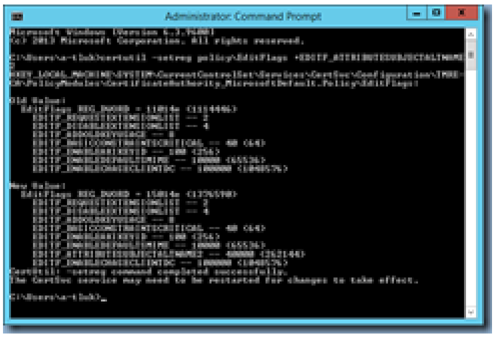
Additional Attributes:

Attributes:

Submit >

certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2

Once the above command is executed, stop and start the certificate authority with:



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\a-tlok>certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\TMRE-
CA\PolicyModules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

Old Value:
  EditFlags REG_DWORD = 11014e (1114446)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)

New Value:
  EditFlags REG_DWORD = 15014e (1376590)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Users\a-tlok>_
```

net stop certsvc
net start certsvc

Proceed to use the CA web enrollment page to generate the certificate with the SAN entry.

Security Concerns:

Note that as per the following Microsoft article:

https://technet.microsoft.com/en-us/library/ff625722(v=ws.10).aspx

It is not recommended to enable the acceptance of the SAN attribute for the CA Web enrollment page so please review the **Security best practices for allowing SANs in certificates** section in the article above to be aware of the security concerns.