Including SANs (Subject Alternative Names) in a Certificate Signing Request

Environment

NetGovern Secure 6.x

Synopsis

When creating SSL certificates for Netgovern Secure, it may be required to work with more than the default hostname. Using a certificate with Subject Alternatives Names (SANs) helps to fulfill this requirement. This article will provide a short reference to creating a certificate with SANs using Openssl.

For more in-depth information, please visit https://www.openssl.org/docs/man1.0.2/apps/x509v3_config.html

The article makes the assumption that the person creating the CSR has some basic working knowledge of Linux, and using command lines such as cp, mv, and text editors (eg. vim or vi).

Solution

This KB will be have two (2) parts:

- Creating a Certificate Signing Request (CSR) with Subject Alternate Names (SANs).
- Verifying the resulting SANs Certificate Signing Request (CSR).

• Creating a Certificate Signing Request (CSR) with Subject Alternate Names (SANs).

One option to create the CSR with SANs is to type one command including all the options and arguments for the Subject Alternative Names. This option is prone to errors, although may have many followers.

Another option is the openssl.cnf file (it comes with openssl) and it provides a section to include the use of x.509 extensions version 3 (RFC 2459), including the Subject Alternatives Names (subjectAltName).

Openssl.cnf default's folder location in Netgorverns Secure appliance is: /etc/pki/tls/

As a good practice, Netgovern recommends creating a backup copy of the original file and working on the copy.

Edit Openssl.cnf

To include multiple SANs into the CSR, edit your copy of openssl.cnf and modify/add these three (3) sections in the file:

```
[ req ]
req_extensions = v3_req (Make sure it is NOT commented)


[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE

keyUsage = nonRepudiation, digitalSignature, keyEncipherment

subjectAltName = @alt_names
```

[alt_names] -->These are the Alternative names added to the CSR

DNS.1 = secure.domain.com

DNS.2 = quarantine.domain.com

DNS.3 = secure-email.domain.com
IP.1 = 192.168.1.1

IP.2 = 192.168.69.14

Save the file with all modifications.

Create the CSR

It is a good practice to generate a new private key along with the CSR when using an input configuration file.

From the console, as a superuser, type the following commands:

openssl genrsa -out osslpriv.pem 2048

openssl req -new -out csr-with-sans.csr -key osslpriv.pem -config openssl.cnf

- ## Verifying the resulting SANs Certificate Signing Request (CSR).

The resulting CSR file should include the names added above. Verifying the CSR is rather simple using the following commands from the console:

openssl req -text -noout -verify -in csr-with-sans.csr

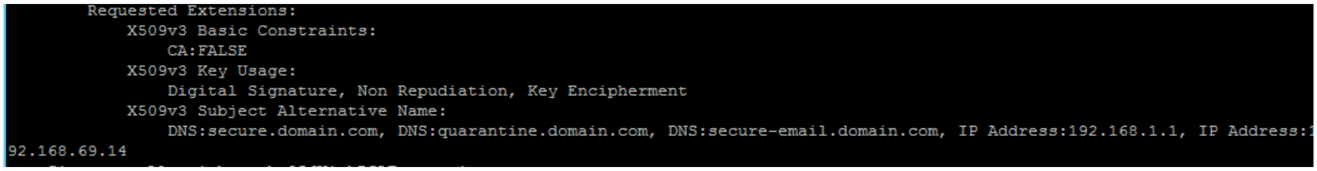
OR

openssl req -text -noout -verify -in csr-with-sans.csr | grep DNS

Both commands should return a Verify OK for the CSR and you will see a Section in the display:

X509v3 Subject Alternative Name:

DNS:secure.domain.com, DNS:quarantine.domain.com, DNS:secure-email.domain.com, IP Address:192.168.1.1, IP Address:192.168.69.14



```
        Requested Extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Subject Alternative Name:
                DNS:secure.domain.com, DNS:quarantine.domain.com, DNS:secure-email.domain.com, IP Address:1
92.168.69.14
```

Once you have finished all of the above and have the expected results, a CSR with Subject Alternative Names, you may copy the file out of netgorven Secure using any file transfer client and upload it to your Certificate Authority in order to create the corresponding certificate.