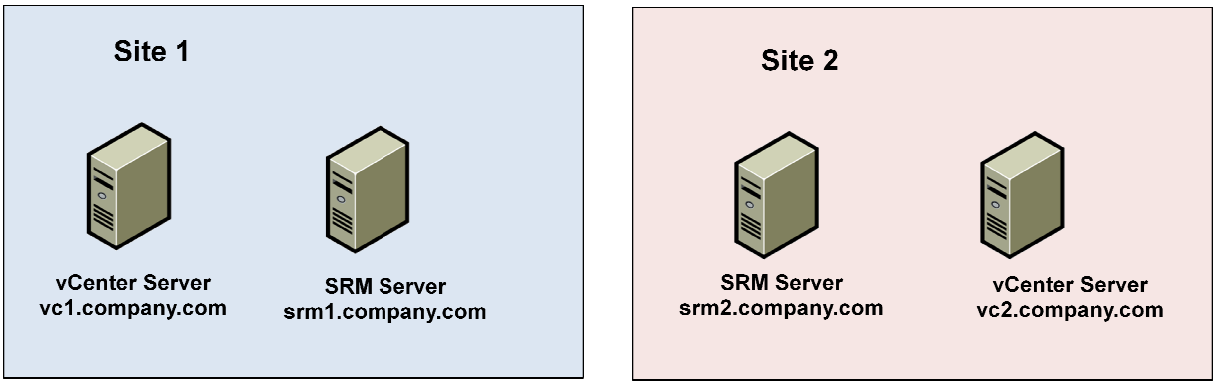
How to use trusted Certificates with VMware vCenter Site Recovery Manager

What's it all about?

In a typical setup you have two VMware vCenter servers - one on your protected site, one on your recovery site. You will also install two VMware vCenter Site Recovery Manager (SRM) servers, like shown below.



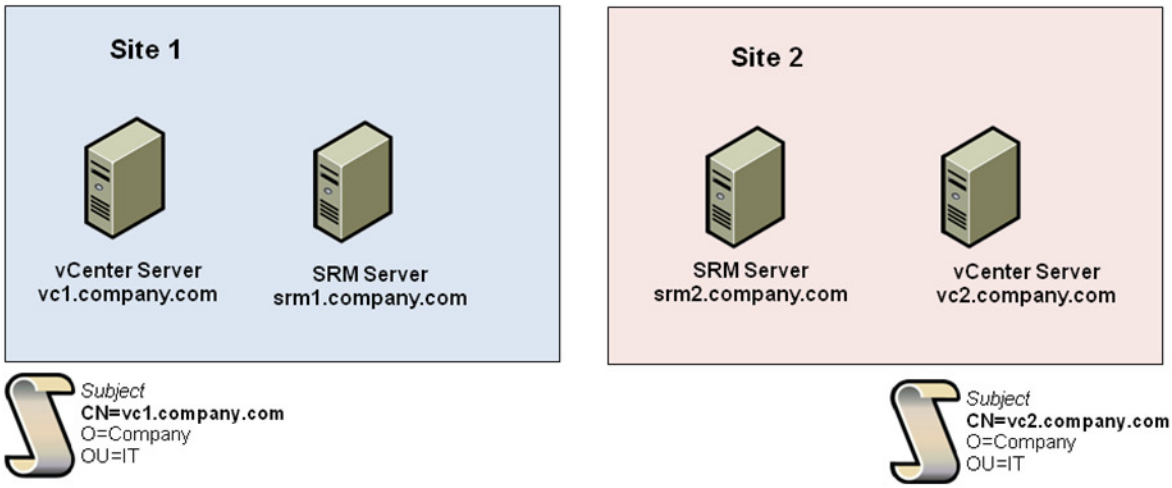
SRM establishes a secure connection between the protected and the recovery site. There are two options for authentication: **Credential based** or **certificate based**. If you install SRM into an existing environment, make sure to choose the method that is appropriate for your environment.

If you have not changed the default certificates that were installed by the VMware vCenter server setup then go for credential based authentication. You do not need to read the remainder of this document.

If you have installed SSL certificates issued by a trusted CA on your VMware vCenter servers then go for certificate based authentication.

In this case you, the Common Name (CN) on the certificates for your vCenter servers should match the respective server's DNS name, like shown below.

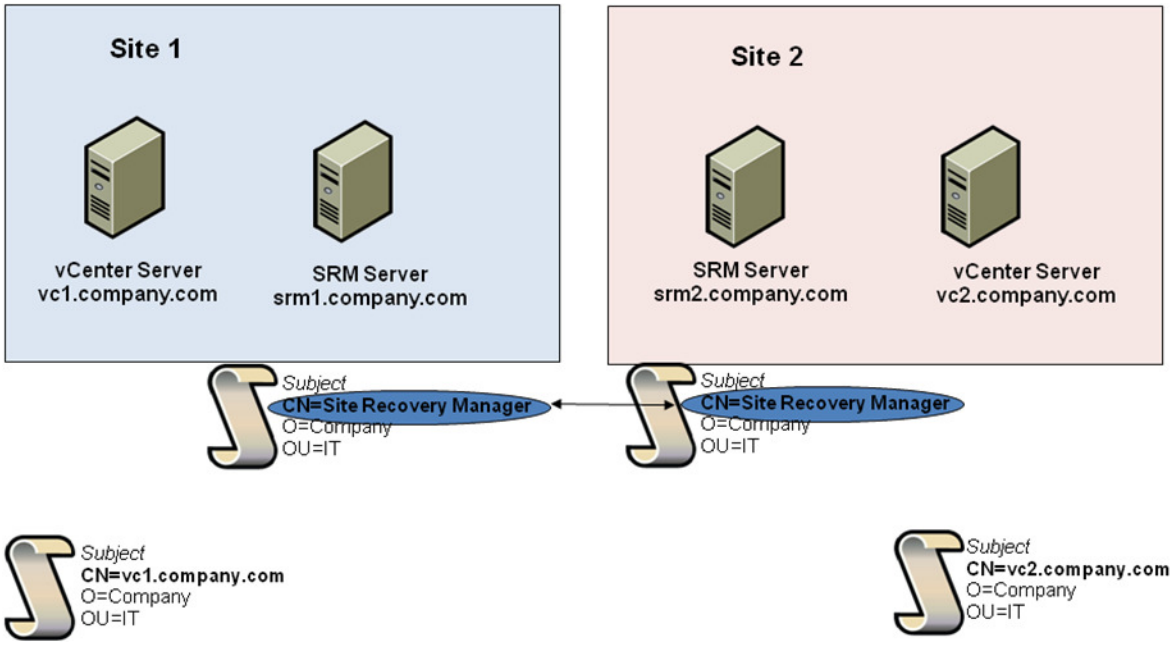
Horst Mundt, Technical Account Manager



Generate SRM server certificates

You will need to generate certificates for your SRM servers using your trusted CA before you install SRM. The certificates need to be in PKCS#12 format. It is assumed that you know how to do this in general, since you did the same for your vCenter servers.

However, the certificates that you need to generate for your SRM servers look slightly different. Namely, the certificates for **both** SRM servers need to have the **same** subject. This includes the Common Name (CN). This should **not** be the DNS name of either of your SRM servers. Choose something generic instead ("Site Recovery Manager" for example). The "Organization" and "Organizational Unit" must match, too:



But this is not enough yet. Your SRM server certificates also need an additional attribute called "Subject Alternative Name". This attribute is designed to hold email addresses, URIs, or DNS

names. In our case it will hold a DNS name – the DNS name of the vCenter server of the respective site.

If you are using an openssl CA, you will need to modify your openssl configuration to include a line like

```
subjectAltName   =     DNS: vc1.company.com
```

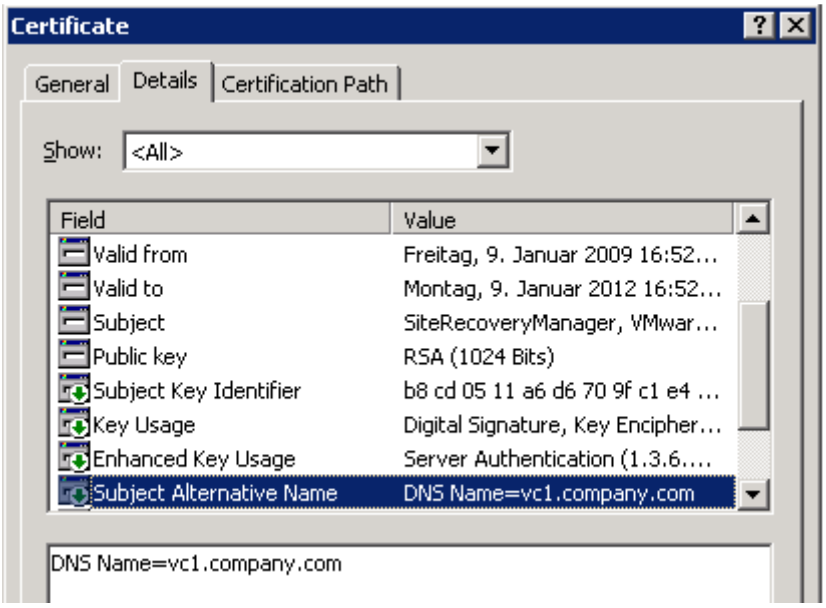
or

```
subjectAltName   =     DNS: vc2.company.com,
```

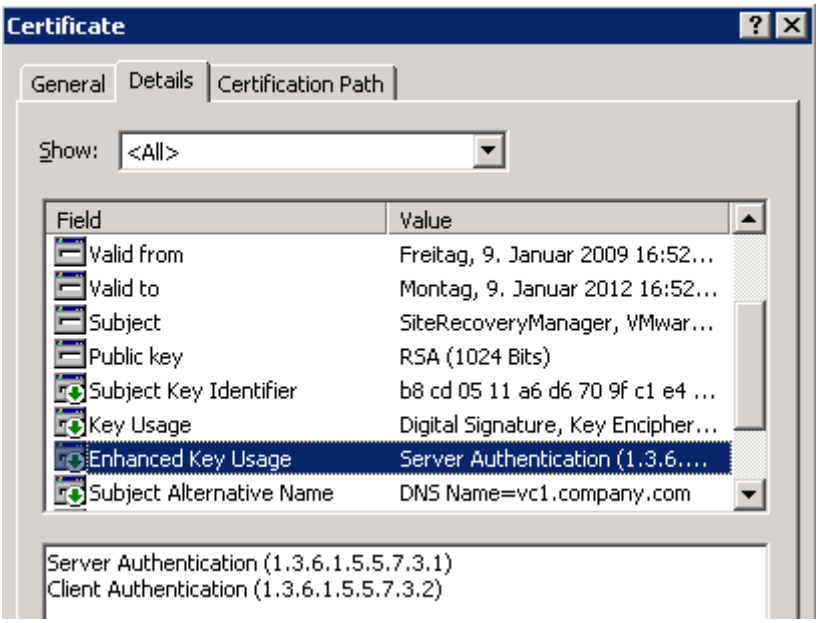
respectively. I'm not aware of a possibility of passing this as a parameter.

If you are using a Microsoft CA refer to http://support.microsoft.com/kb/931351 for information on how to set the Subject Alternative Name.

In the certificates, this looks like this:



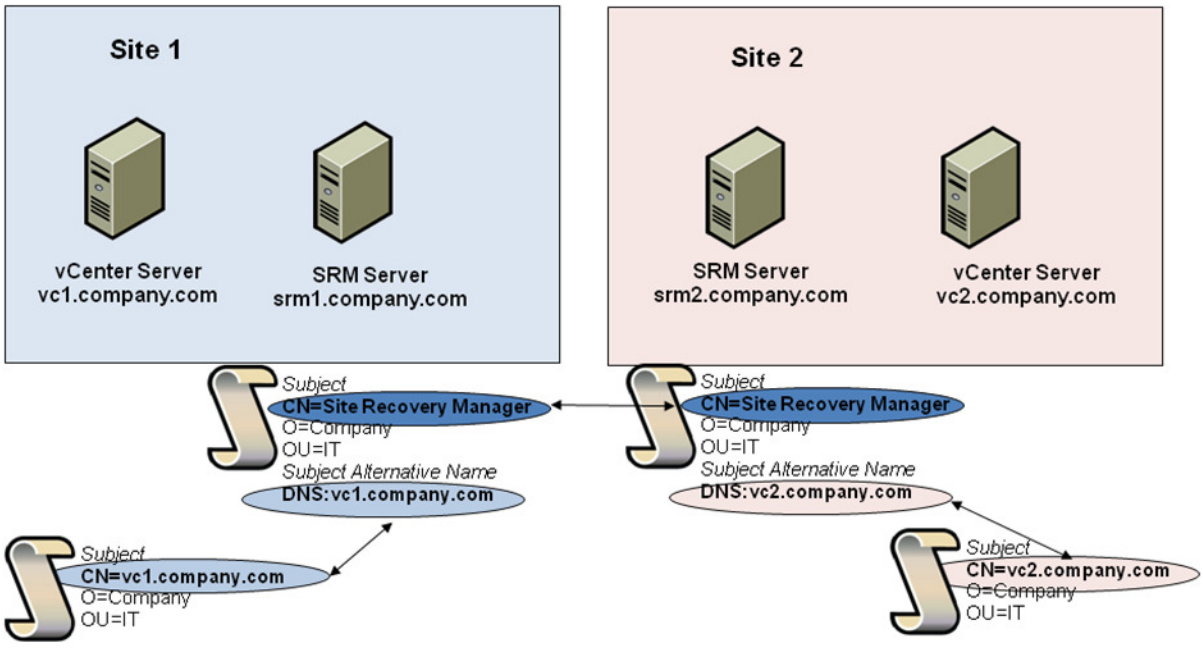
Also make sure that the SRM server certificates have an "Enhanced Key Usage"-attribute for both server and client authentication, like this:



(Note that "Enhanced Key Usage" is how Windows calls it, in openssl it's called "Extended Key Usage", and you need to add the below line to the extensions section of your openssl config file.

```
extendedKeyUsage = serverAuth, clientAuth
```

So here's the complete picture:



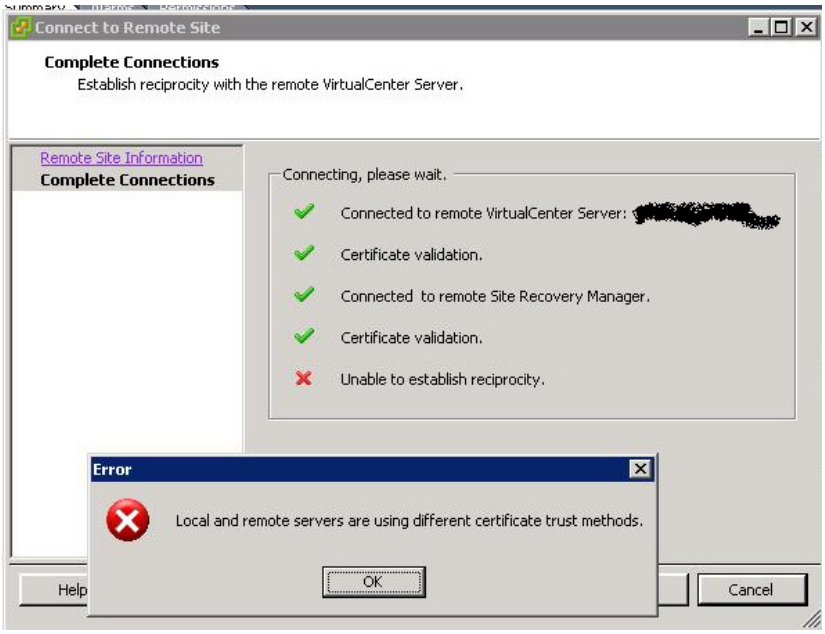
That's the way you need to setup your SRM server certificates.

Installing SRM

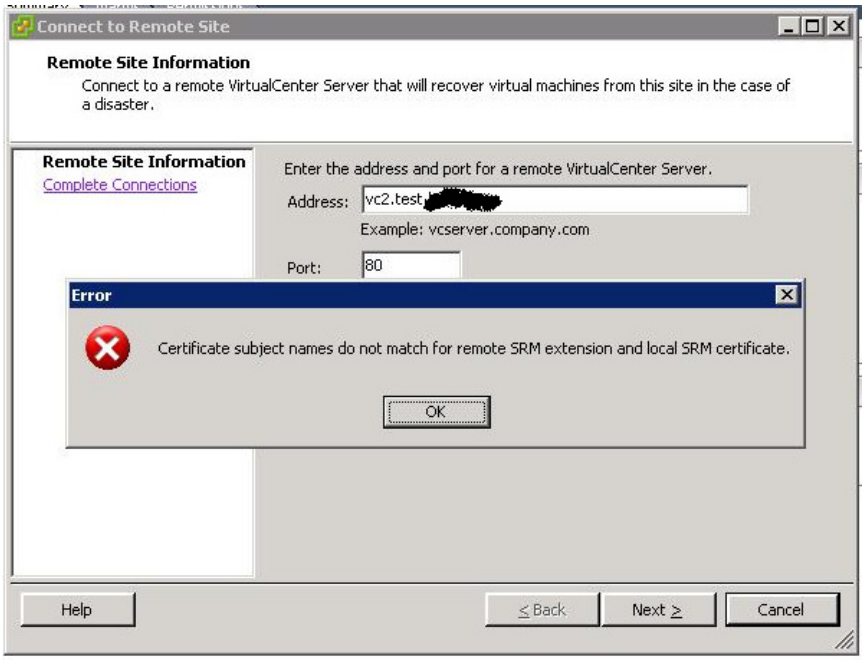
When you install SRM, it will ask you if it should automatically generate a certificate or if you want to provide a PCKS#12 certificate file. Obviously, you choose the latter option and provide the certificate that was generated by your trusted CA.

Troubleshooting

Note that the installation will work if your certificates are not set up correctly, but you will not be able to pair your sites later. You will get messages like the one below, if you are using trusted certificates on your vCenter servers but not for SRM or vice versa. You will get the same message if the "Subject Alternative Name" attribute in the SRM server certificates is not set correctly.



If the "Subject" entries in your SRM server certificates are not identical, you will get messages like below. Make sure that the "Subject" entries in both SRM server certificates are the same.



Disclaimer

This document is provided “as is”. It is not part of official VMware product documentation.

Credits

Special Thanks to Andrei Maier from Swedbank and Dian Nikolov for extensive testing and valuable input.