The usage of PKI Certification (Certificates) within the SVM configuration.

The subject of PKI Certification is quite extensive and the cryptography behind it is the realms of mathematics and science and can seem like a mystical black art to most, but to make use of certification and understand how it applies and how to use it within your environments does not require an understanding of cryptography or a computer science degree, this article aims to provide some general understanding of the of where certificates apply to Software Vulnerability Manager.

So what is certification used for?

Certification is used to ensure a level of trust between one point and another and is used for encryption of data traffic between two points, you will be familiar with SSL/TLS and the lock in your browser when you access a trusted website. Most modern browsers will not let you access websites that are not secured with a valid certificate.

Certification is also used as a proof of trusted identity, most commercial software will be code signed so that your PC can guarantee the software has come from a trusted source, and also software such as hardware devices drivers, in Windows 10 these have to be signed or you cannot install them.

Certification Authorities

A certificate authority is the holder of the "root certificate" by which all certificates generated by the authority is based upon, and by which all certificates that have been issued can be verified against. It is also where you request and obtain a certificate. The certification authority also maintains the "Certificate Revocation List" which as it states is a list of certificates that have been revoked by the authority for whatever reason.

There are public certificate authorities that exist on the internet, and there are private certificate authorities that exist on a corporate enterprise network.

Public Certification Authority needs to be used when you want a certificate to secure a connection to a publicly accessible website. These authorities verify the identity of the certificates applicant (you or me, or the company) and issue a certificate that is publicly verifiable, which means that the third party accessing your website can check that the certificate is valid and has not been revoked. The verification process is automatically done by your browser before the website loads. Software developers will also request Code Signing Certificates from these public authorities for signing their installer packages that it intends to make available to the public.

A private Certification Authority usually exists within a corporate enterprise network, it is responsible for the issuance of certificates for various purposes, such as securing internal intranet sites, securing access to internal web-based devices, client authentication, and lots of other purposes where an encrypted secure connection is required between one to one and one to many scenarios, or where a trusted identity is required.

Within a corporate network it is quite common to find a certificate authority hierarchy, meaning there is a Root Certification Authority (Root CA), and Subordinate Certificate Authority (Intermediate) the subordinate certificate authority issues certificates on behalf of the Root Certification Authority. In Windows-based domain networks, the Root Authority is generally shutdown with the subordinate issuing all of the certificates.

If a Certificate Authority exists on your corporate network, copies of any root certificates and intermediate certificates are generally distributed to all the computers on the network by a group policy, the reason for distributing the root and intermediate certificates is so that computers on your network know to trust any certificates issued by the root or intermediate authority. These certificates will exist in the Trusted Root Authority & Intermediate Certificate Authority containers in the certificate store for the local computer account on all of the corporate machines.

What is the difference between a PKI Certificate and a Self Signed Certificate

You will come across the term self-signed certificates within the documentation so to help you understand the main differences.

Self-Signed Certificates

Self Signed certificates are generated on the computer that you are intending to secure, there is no certification authority issuing the certificate, they cannot be renewed, they cannot be revoked, Self-signed certificates must be distributed to all the other computers Trusted Root Certification Authority stores in order for them to be trusted by any other computer or device. They are fine to use and where a Certificate Authority does not exist and is indeed required.

PKI Issued Certificates

These are issued by your enterprise Certificate Authority, they can be renewed when they expire, they can be revoked by your administrator if required, and provided the RootCA Certificate and any intermediate CA certificates have been distributed to devices are automatically trusted. So no need to separately distribute the certificates. The only caveat in Windows networks that if you have a Code Signing Certificate issued by your PKI Certificate Authority the public key certificate must be distributed to the client computers "Trusted Publishers" store for the local computer account.

So how does all this apply to Software Vulnerability Manager?

In SVM we use certificates in 3 ways:-

- SSL Certificate for the SVM Console (On-Premises SVM Server) to secure the browser connection between the SVM Server and the console operators computer
- Code Signing Certificate, used for signing packages delivered to WSUS from SVM so the packages can be trusted by the client PC's and are allowed to be installed.
- Certificate Authority Root Certificate, so that the SVM Server can trust certificates on the local domain, required when configuring LDAPS

SSL Certificate for SVM Console (On-Prem Only)

To secure access to the SVM Web Console and your PC, you will need to acquire and install a Web Server SSL Certificate that has been issued by your internal certificate authority to the web address that you intend to use for your SVM Server, the web address (*svmservername.domain.local*) is applied to the certificates common name field in the certificate request.

The certificate will need to be supplied to you by your certificate administrator in PFX format (PKCS#12) which is a file that contains both the Private and Public Keys.

To install the certificate on your on-premises SVM Server please see our current product documentation

This document tells you how to import your PKF File into your Linux Server

https://docs.flexera.com/csionpremredhat/Content/helplibrary/Import_Your_Own_SSL_Certificate.htm#rhel_ssl_ldap_2379745888_1047666

This document covers how to configure SVM to use SSL

https://docs.flexera.com/csionpremredhat/Content/helplibrary/RHEL_7_2.htm#rhel_ssl_ldap_2379745888_1048375

Code Signing Certificates

As mentioned earlier in this article, Code Signing Certificates are used to sign software installation packages so that they can be trusted by the computers to which the software packages are to be installed.

When a patching package becomes available within the SVM console to fix and patch discovered software vulnerabilities these packages must be published to your local WSUS Server so that they become available within your System Centre Software Update Point, so they can be subsequently deployed to computers.

Part of the publishing process is to sign the packages using a code signing certificate before the package is delivered to the WSUS Content Store and appears in the WSUS Database.

I have covered creating an installing a Windows Certificate Authority Code Signing Certificate in another KB article, which gives you guidance on how to successfully create and install a Code Signing Certificate for your WSUS Server.

https://community.flexera.com/t5/Software-Vulnerability-Manager/Creating-Windows-CA-Code-Signing-Certificate-for-WSUS/ta-p/149698

Although the above article mainly covers creating the Code Signing certificate, it contains the information on how to successfully install the certificate even if this has been obtained from a non-Windows CA

Root Certificate for LDAPS

The SVM Console can be set up to verify logins using your Windows Active Directory or another type of LDAP server, as this is the exchange of login information between your AD and the SVM Server it is recommended that you configure LDAPS (LDAP Secure). For LDAPS to work you will need to copy your Root Certificate Authority Certificates and if applicable any Intermediate Certificate Authority Certificates to your on-premises SVM Server.

These need to be copied to the directory *"/etc/pki/ca-trust/source/anchors"* on your SVM Server, then you need to run the command *"update-ca-trust"* which will update the CA Trust bundle and this will allow the SVM server to trust the LDAPS server on your local network the SVM Server is querying for logon information.