What is Microsoft Windows Code Signing Certificate?

A Detailed Guide on Microsoft Windows Code Signing Certificate

In today's time, using software and applications is inevitable. A Code signing certificate ensures that the code or software being distributed is legitimate and has not been tampered with by a third party. It provides authenticity and integrity for the code. One form code signing Certificate is Microsoft Windows Code Signing Certificate.

Let us talk about the Windows Code Signing certificate and its importance to the Microsoft community.

What is Microsoft Windows Code Signing?

Windows Code Signing certificate is a type of code signing certificate that is specifically designed for signing code for Windows operating systems. This type of certificate is issued by a trusted Certificate Authority such as Comodo and Sectigo and is used to sign the code, ensuring that it is authentic and has not been modified.

This certificate also ensures that the code is from a trusted publisher and that it is safe to download and install. This makes the Windows Code Signing certificate a must-have for any software developer or publisher who wants to distribute their code to the Windows community. It helps to establish trust and credibility with users, making it more likely that they will download and use the code.

Now that you understand the Code Signing Certificate Microsoft, let us discuss how to obtain one.

How to Obtain a Windows Code Signing Certificate?

To obtain a Microsoft Windows Code Signing certificate, you will need to follow these steps:

Step-1: Generate Certificate Signing Request (CSR)

First, you need to generate a certificate signing request (CSR) on your computer. To generate a CSR for a Windows code signing certificate, you will need to follow these steps:

Open the Microsoft Management Console (MMC) on your computer.

Click on File, and then Add/Remove Snap-in.

Select Certificates from the list and click Add.

Select Computer account and click Next.

Select Local computer and click Finish.

Click OK to close the Add or Remove Snap-ins window.

In the MMC, expand the Certificates (Local Computer) folder and select Personal.

Right-click on Personal and select All Tasks, and then Advanced Operations.

Select Create Custom Request.

Select Code Signing as the certificate template and click Next.

Fill in the necessary information, including the Common Name (your domain name), organization name, and location.

Select the key size and then click Next.

Click Browse and select a location to save the CSR file.

Click Finish to complete the CSR generation process.

After completing the CSR generation process, the CA will verify your identity and issue the certificate to you. The next step is installing it on the system with the corresponding private key.

Step-2: Install CSR on the System

Once you have the certificate, you will need to install it on your computer along with the corresponding private key.

In the Certificates snap-in, navigate to the Personal folder.

Right-click on the Personal folder and select All Tasks > Import.

Follow the prompts to import the certificate and private key files into the Personal folder of the Certificates snap-in.

After importing the certificate, you will see it in the Personal folder. You can now use it for code signing.

After installation, you can use your code signing certificate to sign your software, ensuring that users trust it.

Note: Microsoft has specific requirements for code signing certificates, and not all CAs are able to provide them. As such, you should check with the CA of your choice to see if they offer Microsoft code signing certificates and if so if they meet Microsoft's requirements.

What Types of Windows Code Signing Certificates Are Available?

There are two main types of windows code signing certificates:

Authenticode Code Signing Certificates

Windows Store Code Signing Certificates

Let's explain both types of certificates:

● Authenticode Code Signing Certificate

These certificates digitally sign Windows executables, drivers, and scripts. It provides a secure way of ensuring that the software is safe and has been published by a trusted source.

When a user downloads and runs software signed with an Authenticode Code Signing Certificate, the operating system checks the signature against the certificate's chain of trust. The software will run without displaying any warnings or errors if the signature is valid and the certificate is from a trusted source.

● Windows Store Code Signing Certificates

These certificates ensure that the code of the applications is authentic and has served the same purpose as a regular code signing certificate. Developers who want to distribute their

applications through the Microsoft Store specifically use Windows Store Code Signing Certificates.

The Microsoft Store verifies the signed application before making it available for download. This measure ensures that users are protected from downloading any tampered code. It also helps to maintain the integrity of the Microsoft Store as a secure platform for downloading applications. It is used for Windows 8 and later operating systems.

These are the types of Windows CA Code Signing certificates.

But do you want to know where you will get some of the best Windows Code Signing Certificates?

Where to Find the Best Windows Code Signing Certificate?

There are trusted CA's like Sectigo and Comodo to provide cheap code signing certificates to ensure the digital security shield for software and web application by signing them through digital signature and timestamp. Some of them are:

Sectigo Code Signing Certificate

Sectigo Code Signing Certificate is trusted by Microsoft and its platform there used for code signing Microsoft Office and VBA, Microsoft Authenticode, Microsoft Windows hardware Dev Center, Microsoft Office 365, Microsoft Kernel Mode Code Signing, and Microsoft IoT.

Sectigo also provides a multi-purpose code signing certificate that allows users to sign code for multiple Microsoft platforms, offering a potentially cost-effective solution based on individual requirements.

Comodo Code Signing Certificate

By using Comodo Code Signing Certificate, customers could ensure that Microsoft and its platforms trust their code, and that it has not been tampered with. Comodo's code signing certificates also come with timestamping, which adds an additional layer of security by ensuring the code was signed at a specific date and time.

Your specific certificate will depend on your use case and your target platform. Considering which certificate will be trusted by the target audience and platform is essential.

Code Signing Vs. SSL Certificate: Differences Explained

Concluding Words

Windows codesigning certificates allow the creation of more secure and reliable software applications, which can help to boost a developer's reputation and increase their credibility in the industry.