Digital Signing and Security for Windows Vista Certification

All executable files (including .exe, .dll, .ocx, .sys, .cpl, .drv, and .scr files) in an installation must be digitally signed for the Certified for Windows Vista program.

You can digitally sign your installation and your application to assure end users that neither your installation nor the code within your application has been tampered with or altered since publication. When you digitally sign your application, end users are presented with a digital certificate when they run your installation.

The Signing tab is where you specify the digital signature information—including the digital signature files granted to you by a certification authority—that InstallShield should use to sign your files.

The Signing tab is also where you specify which files in your installation should be digitally signed by InstallShield at build time. InstallShield enables you to sign any and all of the following files in a release, depending on what type of project you are using:

- Windows Installer package (.msi file) for Basic MSI, InstallScript MSI, and Web projects
- Merge module package (.msm file) for Merge Module projects
- Setup.exe file for Basic MSI, InstallScript MSI, and Web projects
- Media header file for InstallScript projects
- Package (self-extracting single-executable file) for InstallScript projects
- Any files in your release, including your application files

Certification Authorities

A certification authority is an organization such as VeriSign that issues and manages digital certificates (also known as digital IDs). The certification authority validates the requester's identity according to prescribed criteria and issues a digital certificate. Obtaining a digital certificate requires providing the certificate authority with specific information about your company and your product.

For a list of certification authorities, see Microsoft Root Certificate Program Members on the MSDN Web site.

Digital Certificate Files

When you sign your installation and your application, you must use one or more digital certificate files. These files are used to generate the digital signature. Two options are available:

Option 1—.spc and .pvk Files

When a certification authority issues you a digital certificate, they provide two files:

- Private key file (.pvk)
- Software publishing credentials file (.spc)

The .pvk file is typically associated with a password.
InstallShield uses Signcode.exe to digitally sign your files with your .pvk and .spc files according to the settings that you configure on the Signing tab in the Releases view. The Signcode.exe file is a Microsoft tool that is installed with InstallShield in the following directory:

InstallShield Program Files Folder\Flexera\IS2008\System

To learn more about Signcode.exe, including its command-line parameters, see the Microsoft Web site.

Option 2—.pfx File

As an alternative to using the .pvk and .spc files to digitally sign your installation and your application, you can use a personal information exchange file (.pfx). You can use PVK2PFX.exe to create a .pfx file from a .pvk file and .spc file; PVK2PFX.exe is part of the Windows Platform SDK, and it is also included with Microsoft Visual Studio 2005.

The .pfx file is typically associated with a password.

InstallShield uses SignTool.exe to digitally sign your files with your .pfx file according to the settings that you configure on the Signing tab in the Releases view. The SignTool.exe file is a Microsoft tool that is installed with InstallShield in the following directory:

InstallShield Program Files Folder\Flexera\IS2008\System

Tip

Using a .pfx file is often the preferred method for digitally signing files, since it is more likely to work in many different environments (such as locked build machines). Since the *SignTool.exe* utility accepts the password as a command-line parameter, it can be automatically provided even in scenarios where *Signcode.exe* cannot accept the password. Therefore, if you specify the digital signature password in InstallShield, you will never see a password prompt if you are using a .pfx file.

Important

InstallShield does not support using .pfx files to sign media header files (.hdr files), which are used for the One-Click Install type of installation for InstallScript projects. For this type of installation, consider one of the following alternatives:

- *Use .spc and .pvk files instead of a .pfx file for your digital signature.*
- *Build a compressed installation, which would enable you to sign with a .pfx file.*

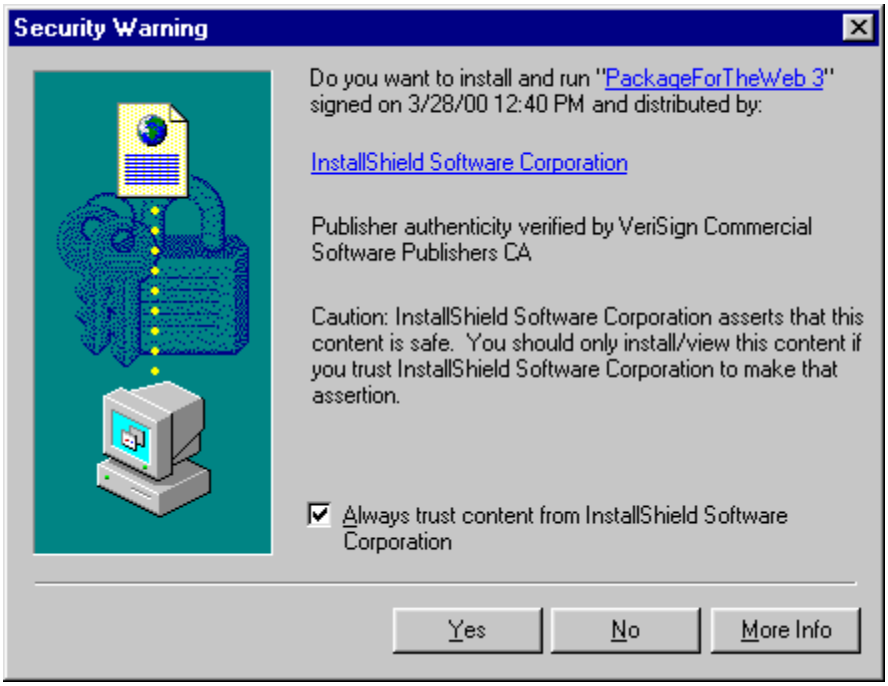
To learn more about SignTool.exe, including its command-line parameters, see the Microsoft Web site. Contact a certification authority for more details about digital certificate files.

Digital Certificate

A digital certificate identifies you, your company, or both to end users and assures them the data they are about to receive has not been altered during its transfer over the Web. Certification authorities issue and manage digital certificates.

When end users download your application, a digital certificate is displayed. The digital certificate is a panel that informs end users when your application was signed and asks if they want to download and run your application. End users click OK to accept your application package.

Below is an example of a digital certificate. The appearance of digital certificates may vary among browsers and browser versions.



Sample Digital Certificate