What is Code Signing?

When customers buy software in a store, the source of that software is obvious.

Customers can tell who published the software, and they can see whether the package has been opened. These factors enable customers to make decisions about what software to purchase and how much to "trust" those products. Customers who download digitally signed Active X controls, dynamic link libraries, .cab files or HTML content from your site can be confident that code really comes from you and hasn't been altered or corrupted since it was created and signed. Digital IDs serve as virtual "shrink-wrap" for your software: after you sign your code, if it is tampered with in any way, the digital signature will break and alert customers that the code has been altered and is not trustworthy.

The solution to these issues is Microsoft's Authenticode technology coupled with Digital IDs from Comodo. Code Signing, through the use of digital signatures, enables software developers to include information about themselves and their code with their software.

When customers download software signed with a Code Signing Certificate issued by Comodo, they can be assured of:

Content Source: End users can confirm that the software really comes from the publisher who signed it.
Content Integrity: End users can verify that the software has not been altered or corrupted since it was signed.
Users benefit from this software accountability because they know who published the software and that the code hasn't been tampered with. In the extreme case that software performs unacceptable or malicious activity on their computers; users can also pursue recourse against the publisher. This accountability and potential recourse serve as a strong deterrent to the distribution of harmful code. Developers and Web masters benefit from Code Signing because it builds trust in their names and makes it more difficult to falsify their products. By signing their code, developers build a trusted relationship with users, who learn they can download software signed by that publisher or Web site with confidence. With Code Signing Certificates, developers can create exciting Web pages using signed ActiveX controls, or other signed executables. And users can make educated decisions about what software they want to download, knowing who published the software and that it hasn't

been tampered with.

Code signing is widely used to protect software that is distributed over the Internet. Code signing does not alter it; it simply appends a digital signature to the executable code itself. Use digital signatures when you want to distribute data, and you want to assure recipients that it does indeed come from you. This digital signature provides enough information to authenticate the signer as well as to ensure that the code has not been subsequently modified. Code signing digital IDs (or certificates) allow content publishers including software developers to sign their content that includes software objects, macros, device drivers, firmware images, virus updates, configuration files or other types of content for secure delivery over the Internet.

Digital signatures are created using a public-key signature algorithm such as the RSA public-key cipher. A public-key algorithm actually uses two different keys: the public key and the private key (called a key pair). The private key is known only to its owner, while the public key can be available to anyone. Public-key algorithms are designed so that if one key is used for encryption, the other is necessary for decryption. Furthermore, the decryption key cannot be reasonably calculated from the encryption key. In digital signatures, the private key generates the signature, and the corresponding public key validates it.