



BUSINESS GUIDE



---

VeriSign® Code Signing for Netscape®  
Object Signing  
Realizing the Possibilities of Internet  
Software Distribution



Where it all comes together.™



**CONTENTS**

+ What Is Netscape Object Signing?	3
+ Who Needs a Code Signing Digital Certificate?	3
+ What Does Object Signing Look Like to Consumers?	4
+ Technical Overview: (Optional Reading)	5
What is a Digital Certificate?	5
CAs	6
How Does Object Signing Work with VeriSign Digital Certificates?	6
The Four Steps to Signing Code	7
+ Conclusion	9



## What Is Netscape Object 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 which software to purchase and how much to trust that software.

When customers download software from the Internet, the most they see is a message warning them about the dangers of using the software. The Internet lacks the subtle information provided by packaging, shelf space, shrink wrap, and the like. Without any assurance of the software's integrity, and without knowing who published the software, it is difficult for customers to know how much to trust software. It is difficult to choose whether to download the software from the Internet.

The solution to these issues is Netscape® Object Signing coupled with a VeriSign® Digital Certificate. VeriSign is Netscape's preferred vendor of digital certificate services. Object signing, through the use of digital signatures, enables software developers to include information about themselves and their code with their programs.

When customers download software signed with Netscape Object Signing and verified by VeriSign, they can be assured of

- **Content Source**—The software really comes from the publisher who signed it.
- **Content Integrity**—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 has not been tampered with. In the extreme case, where 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 Object Signing because it puts trust in their name and makes their products harder to falsify. By signing code, developers build a trusted relationship with users, who then learn to confidently download signed software from that publisher or Web site. With Netscape Object Signing, developers can create exciting Web pages using signed Java™ applets, plug-ins, or other executables. And users can make educated decisions about which software to download, knowing who published the software and that it has not been tampered with.

## Who Needs a Code Signing Digital Certificate?

---

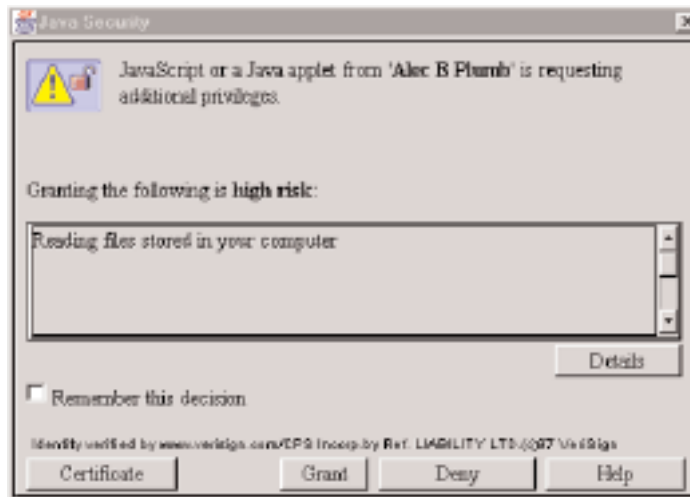
Any publisher who plans to distribute code or content over the Internet or over corporate extranets risks impersonation and tampering. VeriSign® Code Signing Digital Certificate for Netscape Object Signing protects against these hazards.

VeriSign offers a Class 3 digital certificate designed for commercial software developers. This class of digital certificate provides assurance regarding an organization's identity and legitimacy, much like a business license, and is designed to represent the level of assurance provided today by retail channels for software.

## What Does Object Signing Look Like to Consumers?

Netscape Communicator and other popular client applications come with security features that recognize Object Signing. These applications are often used to obtain other pieces of software from networks, sometimes without the end user requesting it. For example, when a user visits a Web page that uses executable files to provide animation or sound, code is often downloaded to the end user's machine to achieve the effects. While this may provide substantial value, users risk downloading viruses or other unwanted code.

When Communicator encounters a software component that is trying to gain access to the user's machine, it automatically checks to see if there is a recognized digital signature with that software. If the code is signed with Netscape Object Signing, the following dialog box will appear:



Through Object Signing, the user is informed

- Of the true identity of the publisher
- Of the type of access requested by the software
- That the authenticity of the above information is provided by VeriSign

The end user can choose to grant or deny the requested privileges or to view the certificate used to sign the code. Communicator provides an estimated level of risk (i.e., high, medium, or low) associated with the privileges requested, and the user can learn more about this risk by clicking "Details."

By selecting “Remember this decision,” the user saves the digital signature of that software publisher so that Communicator will recognize it in the future.

When the end-user’s Netscape browser encounters a signed applet or other code with a recognized signature, the browser automatically allows that code, per the privileges it has previously been granted, without interrupting the user.

Users can add, delete, or edit the privileges they want to grant to publishers at any time. By clicking the security icon in the main Communicator toolbar, users display the following screen:



## Technical Overview: (Optional Reading)

### + What Is a Digital Certificate?

A digital certificate is a form of electronic credential for the Internet. Similar to a driver’s license, employee ID card, or business license, a digital certificate is issued by a trusted third party to establish the identity of the certificate holder. The third party who issues certificates is known as a certification authority (CA).

Digital-certification technology is based on the theory of public key cryptography. In public key cryptography systems, every entity has two complementary keys—a public key and private key—which function only when they are held together. Public keys are widely distributed to users, while private keys are kept safe and only used by their owner. Any code digitally signed with the publisher’s private key, can only be successfully verified using the complementary public key. Another way to look at this is that code that is successfully verified using the publisher’s public key (which is sent along with the digital signature) can only have been digitally signed using the publisher’s private key (thus authenticating the

source of the code), and has not been tampered with. For more information on public keys and private keys, please see the VeriSign White Paper, Introduction to Public Key Cryptography.

The purpose of a digital certificate is to reliably link a public/private key pair with its owner. When a CA, such as VeriSign, issues a digital certificate, it verifies that the owner is not claiming a false identity. Just as when a government issues you a passport, it is officially vouching for the fact that you are who you say you are, when a CA issues you a digital certificate, it is putting its name behind the statement that you are the rightful owner of your public/private key pair.

A VeriSign Digital Certificate is valid only for the period of time specified by VeriSign. The certificate contains information about its beginning and expiration dates. VeriSign can also revoke (cancel) any certificate it has issued and maintains a list of revoked certificates. This list of revoked certificates, called a certificate revocation list (CRL), is published by VeriSign so that anyone can determine the validity of any VeriSign Digital Certificate.

#### + CAs

CAs, such as VeriSign, are organizations that issue digital certificates to applicants whose identity they are willing to vouch for. Each certificate is linked to the certificate of the CA that signed it.

As the Internet's leading CA, VeriSign has the following responsibilities:

- Publishing the criteria for granting, revoking, and managing certificates
- Granting certificates to applicants who meet the published criteria
- Managing certificates (e.g., enrolling, renewing, and revoking them)
- Storing VeriSign root keys in an exceptionally secure manner
- Verifying evidence submitted by applicants
- Providing tools for enrollment
- Accepting the liability associated with these responsibilities

#### + How Does Object Signing Work with VeriSign Digital Certificates?

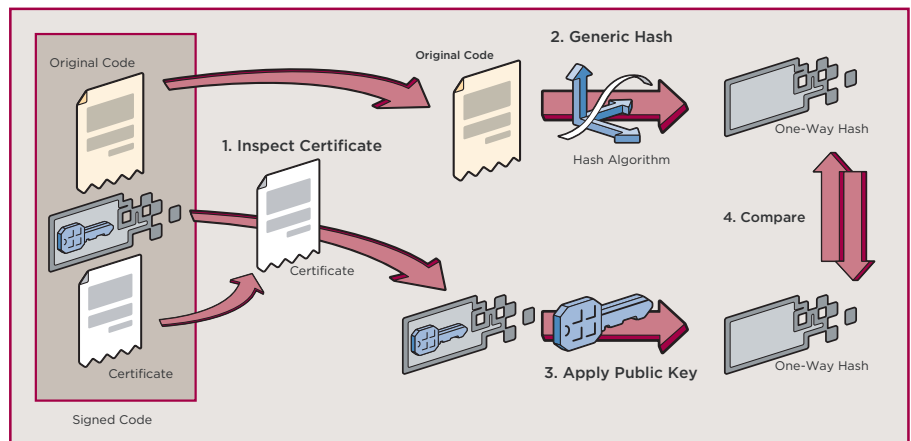
Netscape Object Signing relies on industry standard cryptography techniques such as X.509v3 certificates and Public Key Cryptography Standard (PKCS) #7 and #10. These are well-proven cryptography protocols, which ensure a robust implementation of code signing technology.

Object signing uses digital signature technology to assure users of the origin and integrity of software. In digital signatures, the private key generates the signature, and the corresponding public key validates it. To save time, the object signing protocols use a cryptographic digest, which is a one-way hash of the document.

The process is outlined below:

1. The publisher obtains a VeriSign Code Signing Digital Certificate.
2. The publisher creates code.
3. Using the Netscape Signing Tool, the publisher:
  - Creates a hash of the code, using an algorithm such as message digest 5 (MD5) or secure hash algorithm (SHA).

- Encrypts the hash using his or her private key.
  - Creates a package containing the code, the encrypted hash, and the publisher's certificate.
4. The end user's Netscape browser encounters the package.
  5. The end user's Netscape browser examines the publisher's digital certificate. Using the VeriSign root Public Key that is already embedded in Netscape Communicator, the end user's Netscape browser verifies the authenticity of the Code Signing Digital Certificate (which is itself signed by the VeriSign root Private Key).
  6. Using the publisher's public key contained within the publisher's digital certificate, the end user's Netscape browser decrypts the signed hash.
  7. The end user's Netscape browser runs the code through the same hashing algorithm as the publisher, creating a new hash.
  8. The end user's Netscape browser compares the two hashes. If they are identical, the browser delivers the message that VeriSign has verified the content. The end user then has assurance that the code was signed by the publisher identified in the certificate, and that the code has not been altered since it was signed.



The entire process is seamless and transparent to end users, who see only a message that the content was signed by its publisher and verified by VeriSign.

### + The Four Steps to Signing Code

These instructions will give you an overview of getting and using Netscape Object Signing and a Code Signing Digital Certificate from VeriSign.

#### Step 1: Obtain the Netscape Signing Tool

A variety of tools for different platforms and purposes are available free of charge from Netscape.

#### Step 2: Apply for a VeriSign Code Signing Digital Certificate for Netscape Object Signing

Go to VeriSign enrollment for instructions on obtaining a Code Signing Digital Certificate.

In the process of applying for a VeriSign Code Signing Digital Certificate, your browser will generate a private key, which is stored in your Netscape browser to be used for Netscape

Object Signing. This key is never sent to VeriSign, so if you lose this private key, you will be unable to sign code. If this key is lost or stolen, please contact VeriSign immediately to revoke it.

### Step 3: Pick up Your Digital Certificate

Once you have completed the application process, VeriSign will take a number of steps to verify your identity. For commercial publishers, VeriSign does a considerable amount of background checking. As a result, it will take approximately three to five business days to verify your information and issue a digital certificate.

At the end of this process, VeriSign will send you an email containing a personal identification number (PIN). Follow the instructions in this email to pick up your Digital Certificate. As part of the installation process, Netscape will prompt you to download a .p12 file, which contains both the private key file (key3.db) and the certificate (cert7.db). You now have a backup copy of the private key. This should be stored on a floppy disk in a safety deposit box or other secure location.

Please note that you must use the same machine and browser to apply for and obtain your digital certificate. Once you've completed the installation and backup process, you can use the private key and digital certificate to sign files on a different machine.

### Step 4: Sign Your Files

If you are building any Windows® Preinstallation Environment (PE) file (.exe, .ocx, .dll, or other), you need not do anything special. For .cab files, you need to add the following entry to your .ddf file before creating the .cab file: Set ReservePerCabinetSize=6144

These instructions are for the Netscape Signing Tool version 1.1

1. Create an empty directory.  
% mkdir signdir
2. Put some file into it.  
% echo boo > signdir/test.
3. Specify the name of your object-signing certificate and sign the directory.  
% signtool -k MySignCert -Z testjar.jar signdir
4. Signtool responds with:  
using key "MySignCert"  
using certificate directory: /u/jsmith/.netscape  
Generating signdir/META-INF/manifest.mf file..  
--> test.f  
adding signdir/test.f to testjar.jar  
Generating signtool.sf file..  
Enter Password or Pin for "Communicator Certificate DB":
5. At the prompt, type the password to your private-key database. If it accepts the password, signtool responds as follows:  
adding signdir/META-INF/manifest.mf to testjar.jar  
adding signdir/META-INF/signtool.sf to testjar.jar  
adding signdir/META-INF/signtool.rsa to testjar.jar  
tree "signdir" signed successfully



6. Test your signature.

```
% signtool -v testjar.jar
```

7. Signtool responds with:

```
using certificate directory: /u/jsmith/.netscape
```

```
archive "testjar.jar" has passed crypto verification.
```

```
status: verifired
```

```
path: test.f
```

When a Communicator user downloads your signed file from a Web site, Communicator will display your VeriSign Digital Certificate to the user. If the file is tampered with in any way after it has been signed, the user will be notified and given the option of refusing installation.

For more in-depth instructions on the use of Netscape Signing Tool version 1.1, please see the Netscape Developer's Manual.

## Conclusion

---

Netscape and VeriSign are committed to making the Internet a secure and viable platform for commerce and the distribution of content. With Object Signing and a VeriSign Code Signing Digital Certificate, your code will be as safe and trustworthy to your customers as it would be if you shrink-wrapped it and sold it off a store shelf.

**Visit us at [www.VeriSign.com](http://www.VeriSign.com) for more information.**