



Code Signing Digital IDs

VeriSign Code Signing Digital IDs enable software developers to add a **digital signature** to software and macros including Microsoft Authenticode, Microsoft Office and VBA Signing, Sun Java Signing, Netscape Object Signing, Macromedia Shockwave, and Marimba Castanet Channel Digital IDs for secure delivery over the Internet. Digital IDs are virtual "shrinkwrap" for your software; if your code is tampered with in any way after it is signed, the digital signature will break and alert customers that the code is not trustworthy.

Features & Benefits

Customer Confidence

Signing your software with a VeriSign Code Signing Digital ID protects your customers by assuring them that the integrity of the code they download from your site is intact - that it has not been tampered with or altered in transit.

Authenticity

After downloading, end users can be sure that the code they obtained really came from you, helping you preserve your business reputation and intellectual property. Digital IDs allow customers to identify the author of digitally signed code and contact them should an issue or query arise.

Seamless Integration with Industry-Standard Technology

Most browsers will not accept action commands from downloaded code unless the code is signed by a certificate from a trusted Certificate Authority, such as VeriSign.

Ease of Use

Code signing certificates are easy to use in conjunction with the vendor software tools that developers use to create products, macro's and objects.

Cost Savings

With multi-year certificates, you not only save on the annual cost of ownership of the certificate, but also enjoy the benefits and cost savings from the following:

- **reduced time to market**
- **no need to re-sign code every year and re-distribute**
- **time spent in certificate lifecycle management**

How It Works

Software and macro signing is based on the same public key cryptography system used in Web site and personal digital certificates. Here's an overview of the VeriSign Code Signing process.

1. **First, generate a private/public key pair according to your software instructions.**
2. **Then, enroll for a Code Signing Digital ID with VeriSign by submitting the public portion of the key for certification, along with documentation to prove your identity. (The online enrollment process will provide you with complete instructions.)**
3. **Once VeriSign has verified your identity by checking your documentation, you will be issued a Digital ID, including your full organizational name and your public key. When your certificate is approved and issued, you will be alerted by e-mail either containing the certificate or directing you to a URL where you will be able to access your ID online.**
4. **Use the tools supplied by your software vendor to sign applets, plug-ins, or macros with your Digital ID [see your software documentation]. When your signed object and files are downloaded, they contain a copy of your certificate so that recipients are able to identify you as the author.**
5. **Post your signed code or software on your site so that customers can purchase and download them as normal.**
6. **Customers download your applet, code object or macro. Their browser verifies the signature on the code.**
7. **The customer is able to view the certificate in order to identify the developer who wrote the code. This increases consumer confidence and, if need be, gives the customer the appropriate ability to contact the developer.**

Validation Plan:

1. Once we receive the order from the client, we issue him a Token number similar to TRN number, this will be issued by Validation team Bangalore to the concerned Account manager who can forward this to respective Partner/client.
2. After this the customer / partner has to do the enrolment in our reseller portal URL (details of which will be circulated shortly) and finish the enrolment
3. Documentation to be submitted to VeriSign:
 - **Company Registration document**
 - **Telephone bill in name of company (If client don't have phone bill under company's name, they will need to provide us a verification letter, attested by Notary Public)**
4. VeriSign will check/phone verification and validate the cert in 3-4 business days.
5. Customer receives a email confirmation once validated, needs to download the certificate in his browser/system. **The whole process ideally will take a week – 10 days time.**