How do you know where information came from ?

In the ordinary world of the Internet you don't really know where information comes from. Information may come from the web site that you first linked to, or it may come from a completely different site without you being aware of any change. In the same way, hackers can alter information, and whilst the web site provider might notice, it is difficult for the person receiving the information to be aware that anything is wrong.

Now, cryptography (originally used by the military in machines like the Enigma to protect secrets) can be used to allow users to verify the source of information they receive over the web.

The method used is called 'digital signatures', and it works in the following way.

A web site publisher signs a page, by attaching a digital signature (a unique number directly related to the page) together with a certificate. The certificate tells the person receiving the page and signature who the signer claims to be and where to find the authority that proves the identity of the signer has been checked and is correct.

When a web page is received, a program in the browser is able to check the unique value. If it does not match the original then the signature has failed because the page information has been altered. The certificate is also checked, and if it is found to be incorrect by checking against the reference signature list, the signature has also failed.

Thus the person receiving the page is able to be certain that the page is as published by the original author. They can also tell who the publisher is, and, in the event of a dispute, the publisher cannot deny that they published the information.

The same system can be used when you want to send information to other people. When that happens you sign the information to send (the program carrying out the signing calculates the number and adds your certificate for you) so that the recipient is able to check it.

Now, of course, it matters how you got your certificate, because the recipient can only be sure it's you if they can check the certificate. If you created your own keys and certificate (some products will let you do that) then you may be the person guaranteeing your identity. These are called self-signed certificates.

Unfortunately, if the recipient does not know you personally or did not get a copy of your certificate independently from you, they might find it difficult to believe the certificate on its own. (This is like accepting a cheque without seeing a cheque guarantee card.) You can go to a Certification Authority (CA) to obtain a certificate. (A sample list of CAs is given elsewhere on the ArticSoft site.) They will, for a fee, issue a certificate that gives authenticity to the identity. Otherwise your bank or employer may issue you with a certificate that you can also use.

Many companies that want to prove web identities will go to one of the major CAs and obtain a fully checked certificate that will validate with the default certificates stored on most browsers. In that way you can be confident that their web identity is also their true one.

Articsoft products make use of these features when verifying web pages. They are able to check the mathematics of any certificates using the RSA algorithm that is used to sign web pages. They can also check that the master certificate list has the certificate of the CA claimed and that it too is correct.

ArticSoft products use the same techniques when creating a digital signature for you when you sign something. They add the certificate to the signed data so that the verification program is able to carry out full checking of the certificate.

Naturally, if you are using a certificate that was not signed by one of the major CAs the check against the master list will fail, unless the people receiving your information (customers, suppliers, members and so on) already have your certificate stored in their master list. For most organizations this can be achieved by sending certificates out to people who need to have them, probably by e-mail or otherwise on floppy discs, so that they can be added to the master lists.

Adding certificates to a master list is very easy. The ArticSoft verifier allows the user to add certificates that they have decided to accept (or trust). Once added, anything signed that refers back to that certificate will be accepted as valid by the verifier. If at any time in the future the user decides that a certificate (or are advised of a change to the certificate by the original provider) should no longer be accepted they just delete it from the master list and the verification program will no longer recognize it.