

Digital Signatures 3

Frequently Asked Questions (FAQs)

What is a digital certificate?

It is a collection of electronic information, usually containing a statement of the identity of the owner and some additional data. This is generated using cryptography, not to conceal the statement, but to make it hard for anyone other than the owner to forge it. Digital certificates are usually stored as files, either on a computer disk or a smartcard.

What is a certification authority (CA)?

It is a company, or other trusted organisation, that vouches for the truth of statements contained in digital certificates. After verifying the statement the CA 'signs' the certificate using similar cryptographic techniques to make it hard to forge the signature. The signature then becomes part of the certificate. CAs may create certificates for clients, or may sign certificates generated by clients themselves.

Why are they needed?

For many transactions on the Internet you need to be confident of the physical identity of the person or organisation with whom you are dealing, not just their e-mail or web address. A signed digital certificate is evidence that a third party has performed some identity check: you must decide whether the third party and their checking procedures are adequate for your requirement.

Can I use a certificate on my web server?

Yes, though to be effective in a global community it should be signed by a global certification authority.

At the request of the JISC, JANET has arranged for Globalsign, a commercial Certification Authority, to sell server certificates to sites in the .ac.uk domain. For details see:

<http://www.ja.net/CERT/web/globalsign.html>

Can I use certificates instead of passwords?

At present very few services allow the use of digital certificates in place of traditional usernames and passwords. In any case, unless you have your own computer or smartcard it may be hard to keep your certificate secure while using it on a shared computer.

Should I sign my programs?

Some programming systems allow authors to attach a digital certificate to their code as proof of origin. If you plan to do this, check whether you will be taking on any legal liability for the consequences of running the code.

How can I sign my e-mail?

PGP (Pretty Good Privacy) is the most widely used system for signing electronic mail messages. PGP uses an informal 'web of trust' instead of Certification Authorities so is best suited to small communities and interest groups.

This Factsheet is one of three on digital signatures. Also available are 1. Certificates and Certification Agencies and 2. Signing electronic e-mail.