

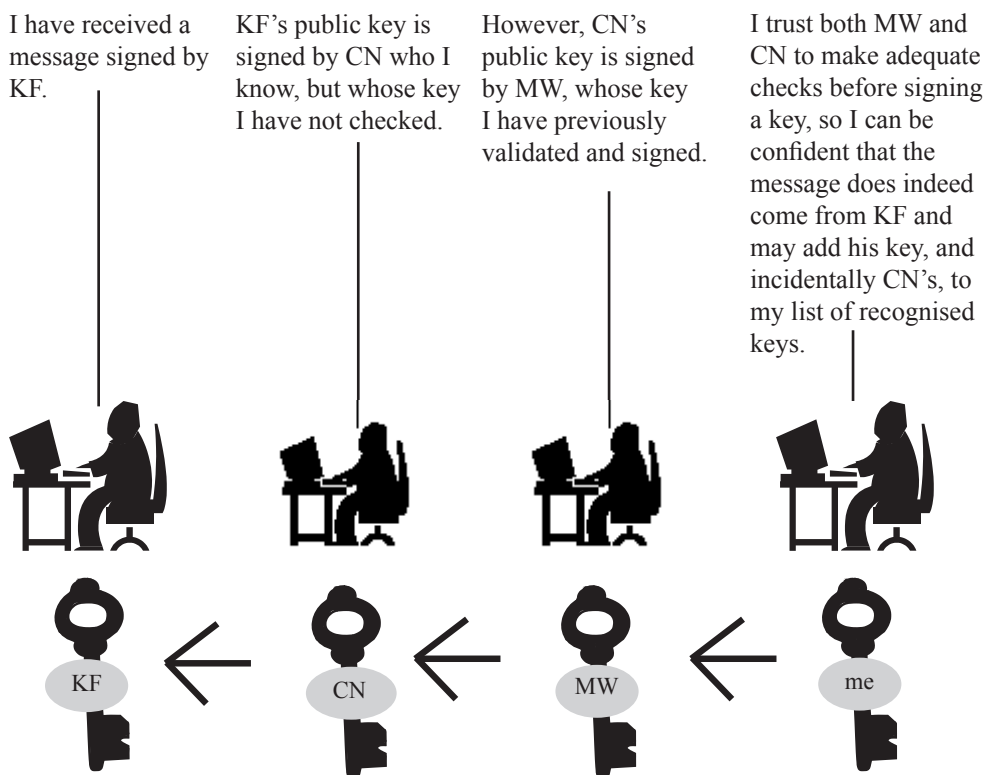
Digital Signatures 2

Signing electronic e-mail

It is relatively easy to create an electronic mail message that appears, superficially at least, to come from someone else. It is therefore useful to be able to 'sign' e-mails, as we use ink signatures on paper documents and letters, to give stronger proof of their origin. There are systems that allow such signatures to be created using certificates and certification agencies, however the most commonly used system, Pretty Good Privacy (PGP), uses a different approach and terminology.

A PGP user signs a message using a private key; the signed message then contains both proof that the message text has not been altered since signing and an assertion of the identity of the signer. The problem, as with any signing system, is to increase the recipient's confidence in that assertion.

PGP keys are generated in pairs. For each private key there is a public key that is mathematically related to, but not feasibly derived from, the private key. Public keys can be signed by other key holders to express their belief in the identity of the key holder. If the recipient of the message accepts the 'word' of one of these signers (and trusts that their signature has not been forged), then they may also believe the identity of the sender. The following example shows how this works in practice.



A PGP pathfinder program (for example <http://www.cs.uu.nl/people/henkp/henkpgp/pathfinder/>) can be used to find links between two keys, but to confirm the identity of the final keyholder I need to know all of the individuals in at least one chain. KF's key is also signed by other people, but since I do not know them their signatures are of little value to me in verifying the ownership of the key. Within existing communities, where there are well-known individuals who sign many keys, this is not usually a problem but without more organisation the system does not scale to diverse user populations. Although PGP has key servers that hold large numbers of signed keys these are passive repositories that, unlike certification authorities, make no statement about the identity of the keys they serve.

This factsheet is one of a series of three on digital signatures. Also available are: 1. Certificates and Certification Authorities and 3. Frequently Asked Questions. Copies of the factsheets are available from service@janet.ac.uk