Glossary of Cryptographic Terms

The following are used as technical terms in this series of documents; each term is italicised on first occurrence in the main text and in cross-references within this glossary:

algorithm

A computational rule; in cryptography, usually a rule for *encrypting* or *decrypting* data. The algorithm itself may be well known; but it is used with a *key,* possessed exclusively by the members of a group who wish to communicate securely, to particularise its effects for their use. See also companion paper *Background to Modern Cryptography* section *Traditional Cryptography.*

asymmetric key

A *key* that is not a *symmetric key*. See also *key pair.*

certificate

Properly called an X.509 certificate; an electronic document that, in PKI applications (including *S/MIME),* associates a *Public Key* with *identity details* of its *owner* and is *digitally signed* to certify the association. Defined in RFC 5280 as updated by RFC 6818; also RFC 5750. See also companion paper *Implementing Cryptography* section *S/MIME.*

certificate owner (also referred to as 'subject' or 'keyholder')

The person or entity that created (and so is presumed to own) the *key pair,* of which the *Public Key* is contained in the *certificate* referred to.

certificate revocation list (CRL)

A list of *certificates* which have been *revoked* by the *certification authority* that originally issued them and which *certificate users* should therefore not rely on. The CA publishes CRLs, with frequent (e.g. daily) updates; users keep their own local caches, which they need to update regularly from the latest CA lists. This has the advantage over the *Online Certificate Status Protocol (OCSP)* system that users can use CRLs even when not online to the internet, but the disadvantage that updating the CRL cache takes much time and internet bandwidth.

Certificate Signing Request (CSR)

An electronic document submitted by a would-be *certificate owner* to a *certification authority,* requesting the CA to issue a signed *certificate.* The CSR is essentially an unsigned draft certificate, which gives the *Public Key* and owner's *identity details* to be included in the certificate (but not the owner's *Private Key,* which never leaves the owner's system). The CA validates the requested certificate content and, if it passes, signs the certificate and returns it to the owner.

certificate user (also referred to as 'user' or 'relying party')

In relation to a *certificate:* a person or entity who, for the purpose of encrypting an outgoing document or verifying an incoming document, uses (and relies on) that certificate as evidence of ownership of the *Public Key* contained in it.

certification authority (CA)

A trusted third party intermediary who validates, signs and issues *certificates* containing *S/MIME* type *Public Keys.* See also companion paper *Implementing Cryptography* section *S/MIME.*

ciphertext

Encrypted data, the result of applying *encryption* to *plaintext* data. Ciphertext can only be interpreted by *decrypting* it using the appropriate *key*. Only authorised people should be allowed to possess copies of the key giving access to the data.

decrypt

Reverse the effect of *encryption* to retrieve the original *plaintext* data, as it was before it was encrypted.

digital signature

Data added to a document to prove the *identity* of the author and assure the reader that the document content is what the author actually wrote. Fulfils the same function as a manuscript signature on a written document.

domain

Part of the naming scheme used on a computer network such as the Internet or a local network. A domain groups together a set of network resources controlled or provided by the domain owner. Domain names on the Internet are issued by authorised registrars: ICANN for generic international domain names and local registrars for country-specific domain names (e.g. Nominet in the UK). These names are unique, constitute valuable property and can be bought and sold. Names of resources such as mail boxes, which form part of the domain, incorporate the domain name – e.g. `'richard@rstonehouse.co.uk'` where `'rstonehouse.co.uk'` is the domain name. A correspondent's e-mail address may be under their own domain name, if they have one, or under that of the Internet Service Provider or Web-mail service (e.g. googlemail) who provides their e-mail facility. See also *WHOIS.*

Elliptic-curve Cryptography (ECC)

A family of modern public-key cryptographic algorithms, based on the properties of mathematical functions known as *elliptic curves.* Provide stronger cryptography, for a given key size, than *RSA.*

e-mail ping

A rough check that the person claiming to own an e-mail address does, at least, have access to it; part of the procedure to generate a *personal certificate* using a web browser. An e-mail is sent to the purported owner at the e-mail address they claim to own, inviting them to enter a particular web address into their browser in order to continue the procedure. If the e-mail address is invalid or the claimant does not have access to it, they will not receive the e-mail and so will be unable to proceed. See also companion paper *Implementing Cryptography,* section *S/MIME* sub-section *Personal Certificates* and *Appendix I* sub-section *CAcert.*

encrypt

Convert a piece of *plaintext* data into unintelligible gibberish, known as *ciphertext*, from which the original data can be retrieved only by *decrypting* it using the correct key.

end-to-end (E2E), end-to-end encryption (E2EE)

Communication in which the cryptographic protections (encryption and/or digital signature) are applied to messages by their original senders and verified by their final recipients, so that an operator of any computer that the messages happen to pass through on their journey between these two end-points cannot read and/or successfully interfere with the contents of the messages. This safeguards messages against malicious attackers who have broken into or compromised the communications network and also against operators acting under instructions from a government or a court order.

enterprise certificate

A *certificate* owned by a company or organisation. See also companion paper *Implementing Cryptography* section *S/MIME* sub-section *Enterprise Certificates.*

extended validation

Additional validation of a *certificate* to prove ownership of the internet *domain,* organisation *identity* and physiA family of modern public-key cryptographic algorithms, based on the properties of mathematical functions known as *elliptic curves.* Provide stronger cryptography, for a given key size, thancal presence of the legal entity who owns the certificate.

fingerprint

A *hash* of the content of a *Public Key,* used to identify the Public Key.

forward secrecy (sometimes referred to as 'perfect forward secrecy', 'disappearing messages' or 'exploding messages')

Encryption that allows the encrypted information to be read for only a specified period of time and then to disappear for ever. See also companion document *Implementing Cryptography* section Forward Secrecy.

hash

A numeric value produced by applying a hashing *algorithm,* which is an advanced form of sum-check, to a piece of data. The hashing algorithm, applied to the same piece of data, will always yield the same hash, which may therefore be considered to identify the data. A hash value is not unique to the piece of data it is derived from; there may be many different pieces of data that will produce the same hash, but the hashing algorithm and the size of the hash are chosen so that such 'collisions' are very rarely encountered in practice and the hash may be treated as, in effect, a unique identifier of the data. The hashing process is non-reversible; the original data cannot be recovered from the hash.

identity, identity details

Details that distinguish a unique individual person or organisation. See also companion paper *Implementing Cryptography,* section *Identity in the Virtual World.*

key

Something, usually a block of digital data, that is used in conjunction with a cryptographic *algorithm* for *encrypting* or *decrypting* data. A key determines the effect of the encryption or decryption performed by an algorithm for a particular group of users. Traditional cryptography uses *symmetric* keys, where the same key that was used to encrypt a piece of data is also used to decrypt it. Public Key cryptography uses *key pairs,* each consisting of a pair of related *asymmetric* keys, where one of the keys is used to encrypt the data and the other to decrypt it. See also companion paper *Background to Modern Cryptography* sections *Traditional Cryptography* and *Public Key Cryptography.*

key owner (also referred to as 'owner')

The person or entity who owns the *Private Key of* the *key pair* referred to.

key pair

A pair of *asymmetric keys* that are related in that, if a piece of data has been *encrypted* using one of the keys, it can only be *decrypted* by using the other key of the same pair. In particular, it cannot be decrypted by using the same key that was used for encryption. One of the keys is designated as the owner's *Private Key* and the other as their *Public Key*.

key server

A public computer from which *OpenPGP* type *keys* can be downloaded.

keyholder

See *certificate owner.*

key user (also referred to as 'user')

In relation to a *Public Key:* a person or entity who uses and relies on it for encrypting an outgoing document or verifying an incoming document.

Man in the Middle (MITM)

An attacker who clandestinely intercepts and falsifies the communication between two legitimate users or their systems, with the aim of impersonating one or both of them to the other.

OCSP Responder

An online server, maintained by a *certification authority,* which provides the revocation status of the *certificates* that the CA has issued and are still within their validity periods. Can be queried using the *Online Certificate Status Protocol (OCSP).*

Online Certificate Status Protocol (OCSP)

A means by which a *certificate user* can determine whether a *certificate* has been *revoked* by its *certification authority* to indicate that it should not be relied on. The CA notifies users of certificates' revocation status through an online *OCSP responder.* This has the advantage over the alternative *Certificate Revocation List (CRL)* system that up-to-date status information is provided to the user instantly, but the disadvantage that it does not work when the user is offline from the internet.

OpenPGP

A cryptographic message format, defined in RFC 4880: *OpenPGP Message Format.* Discussed in companion paper *Implementing Cryptography* section *OpenPGP.*

passphrase

Like a password, only longer; used to protect a *Private Key.* Must be supplied by the user in order to carry out any operation using the Private Key. Usually consists of more than one word. See also companion paper *Background to Modern Cryptography* section *Public Key Cryptography.*

persona

A pseudonym by which an internet user chooses to be known online. It need bear no resemblance to their true *identity* and a single individual may use several different personas, for example when participating in different groups. See also companion paper *Implementing Cryptography,* section *Identity in the Virtual World.*

personal certificate

A *certificate* owned by an individual person. See also companion paper *Implementing Cryptography* section *S/MIME* sub-section *Personal Certificates.*

phishing

An attack using deception to extract secret information from an individual or organisation. The attacker makes contact with the individual victim, or person in the organisation who has access to the information (but of course ought not to disclose it), generally via telephone or electronic messaging. They may gain the victim's trust by, for example, adopting a trusted person's *identity,* impressive-looking (but false) credentials or a fake website. The aim is to trick the victim into either disclosing the information directly to the attacker or installing 'spyware' that, unknown to the victim, will extract the information from their computer system and deliver it to the attacker.

plaintext

Data that is not *encrypted* and is therefore intelligible to anyone, without the need for them to possess a cryptographic *key* in order to *decrypt* it.

platform

A web-site and its associated infrastructure that provides social media facilities to registered users, often via software that is proprietary to the owner of the platform and can only be used on that platform.

Private Key

A *key,* one of a *key pair,* that is kept secret by the person who owns it. The sender of a *digitally signed* message uses their Private Key to *encrypt* the digital signature that they attach to it. The recipient of an *encrypted* message uses their Private Key to *decrypt* it. See also companion paper *Background to Modern Cryptography* section *Public Key Cryptography.*

Public Key

A *key,* one of a *key pair,* that its owner makes available to other people. The sender of an *encrypted* message uses the intended recipient's Public Key to *encrypt* it. The recipient of a *digitally signed* message uses the sender's Public Key to *decrypt* the digital signature attached to it. See also companion paper *Background to Modern Cryptography* section *Public Key Cryptography.*

Public Key Infrastructure (PKI)

A network of *certification authorities* through whom the ownership of *certificates* is authenticated using a centralised trust model. Used by *S/MIME* for secure e-mail, by SSL for secure web-pages and by code-signing. Compare *Web of Trust*. Discussed in companion paper *Implementing Cryptography* section S/MIME sub-section *Public Key Infrastructure.*

relying party

See *certificate user.*

revocation status check

A check, carried out by cryptography software on a *certificate user's* behalf, as to whether a *certificate* has been *revoked.* The user should set up their software to do this, either by searching the *certification authority's Certificate Revocation List* or by querying the CA's OCSP responder using the *Online Certificate Status Protocol.*

revoke

In relation to a *certificate:* give notice, as the *certification authority* who signed the certificate referred to, that it is to be regarded as invalid – for example because it has been compromised or the owner is in breach of the CA's terms.

root certification authority (root CA)

A *certification authority* whose *certificate* is *self-signed,* and which therefore forms the head of a chain or tree structure of *certificates.*

RSA

One of the first public-key cryptographic algorithms, based on the problem of factorising large numbers. Still in widespread use at the time of writing. See Rivest, Shamir and Adleman: *A method for obtaining digital signatures and public-key cryptosystems* <https://people.csail.mit.edu/rivest/Rsapaper.pdf>.

safety number

An array of numbers identifying a user's *Public Key,* to guard against possible alteration of the key by a *Man in the Middle* attacker during transmission from one user's system to another. The user who receives the key checks its safety number against that of the key that was sent. Similar to a *fingerprint* but slightly more user-friendly.

self-signed certificate

A *certificate* in which the *digital signature* is made using this certificate itself rather than the certificate of a higher-level *certification authority.* Used for certification authorities' root certificates and may also be used for the root certificate of a local certificate network within an organisation.

S/MIME

A cryptographic message specification, defined in RFC 8551: *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification.* Discussed in companion paper *Implementing Cryptography* section *S/MIME.*

SMS ping

A rough check that the person claiming to own a mobile telephone or device does, at least, have access to it, by sending an authorisation code to the phone or device via SMS and inviting the recipient to confirm receipt of the code by typing it in. Often used where the telephone number also serves as a user identifier.

subject

See *certificate owner.*

subordinate certification authority (subordinate CA)

A *certification authority* whose *certificate* is signed by a higher-level certification authority.

symmetric key

A single *key* that is used both for *encrypting* data and for *decrypting* the data that was encrypted using it.

Trust on First Use (TOFU)

A trust model, used in the *New Cryptography* and also in SSH and GnuPG, in which a Public Key is provisionally accepted without authentication. "Subsequent communication that is authenticated using the cached key … is secure against an MiTM attack, if such an attack did not succeed during the vulnerable initial communication." See RFC 7435: *Opportunistic Security: Some Protection Most of the Time.*

two-factor authentication (2FA), two-step verification

A method of authentication that requires the candidate to provide two pieces of information drawn from different categories of the set:
(1) something that they *have*; (2) something that they *know;* and
(3) something that they *are.* See also companion paper *Pros and Cons of Cryptography* section *3. Stolen or Counterfeit Credentials.*

two-step verification

See *two-factor authentication (2FA).*

user

See (according to context) *key user, certificate user* or *user interface.*

user interface

The style of interaction between the user of a computer and a system or program running on it. Examples are the traditional Command Line interface and the more modern Graphical User Interface.

Web of Trust (WoT)

A network of third-party intermediaries through whom the ownership of *Public Keys* is authenticated using a decentralised trust model. Used for *OpenPGP* secure e-mail. Compare *Public Key Infrastructure.* Discussed in companion paper *Implementing Cryptography* section *OpenPGP* sub-section *Key Servers and Webs of Trust.*

WHOIS

Services provided by Internet *domain* name registrars, giving limited public access to the registers that they maintain. WHOIS for the top-level register that contains the generic domains ending in .com, .org, .net etc. is provided by ICANN <https://whois.icann.org/en>. WHOIS for the individual country registers is delegated to local registrars; that for UK domains, ending in .uk, .cymru or .wales, is provided by Nominet UK <https://www.nominet.uk/whois/>. The register entries contain contact details for the domain owners, but this information is redacted from the WHOIS output unless the domain owner has consented to its being made public, or the enquirer is a law enforcement agency or has an approved reason for wanting the information.

Richard Stonehouse