Glossary

Cryptography

AEAD

Authenticated Encryption with Associated Data. A modern mode of encryption that provides in-built authenticity, usually via the computation of a MAC that is computed over the message or ciphertext, and additional data that requires protection. Modern algorithms that support this are AES-GCM and ChaCha20.

AES

The Advanced Encryption Standard. The most commonly used block cipher. The Rijndael algorithm was developed by researchers in Belgium as a response to a NIST call for replacements for DES.

Asymmetric Encryption

Encryption that uses two keys, one for encryption and one for decryption. Traditionally only one of the keys is kept private.

ChaCha20

A modern stream cipher, often paired with the Poly1305 MAC. Uses only basic CPU operations, and as such is extremely fast on modern devices, particularly phones. Used as standard on Android phones when connecting to Google servers. It is also an available cipher suite in TLS.

Digital Signature

A message signed (encrypted by) the private key of a key pair. This key is usually associated with a public key certificate.

DSA

Digital Signature Algorithm. An alternative to RSA based on different mathematics. Support for this has waned, and usually only allows for the use of 1024 bit keys, which is not enough. The elliptic curve variant ECDSA is much preferred.

ECDSA

Elliptic curve variant of DSA. Much more efficient and secure, likely to see increased use as it offers more security than RSA for shorter key lengths.

Ed25519

A new elliptic-curve based signature algorithm offering 128 bits of security. Fast and secure, it is seeing increased use. A specific instance of ECDSA.

Ed448

A new elliptic-curve based signature algorithm offering 224 bits of security. A specific instance of ECDSA.

Galois Counter Mode

A modern mode of operation often seen used with AES. GCM is similar to counter mode, but also computes a message authentication code or GMAC over the data, ensuring message authenticity.

Hash Function

A function that takes a message of any length, and returns a message of a fixed size. Used frequently in message authentication codes and digital signatures. Also sometimes used to secure passwords, and to derive keys from shared secrets like Diffie-Hellman output.

HMAC

An improved structure for a MAC, using two derived keys and two applications of a hash function. Used as part of the KDF in TLS.

IV

Initialisation Vector. A random string that is not secret, and used to provide randomness. Usually it is required that IVs may repeat (at random), but should be strongly random and as such, unpredictable.

KDF

Key derivation function. Any (normally hash-based) algorithm for converting a pre-master secret into an actual key.

Key

The secret component of most ciphers. A string of bytes that are used to alter the output of a cipher, such that it cannot be reversed without possessing those same bytes.

Key Exchange

A protocol that allows two parties to generate or share a secret key over an insecure channel.

Message Authentication Code (MAC)

A tag appended to a message that provides authenticity. A shared secret is combined with the message and hashed, to provide a tag that is able to verify whether a message has been changed.

Mode of Operation

A protocol within which a block cipher is used, in order to facilitate the encryption of messages of arbitrary lengths. Modern modes of operation often provide useful features beyond the core block cipher, such as message authentication.

Nonce

A ”number used once”. A string of bytes that are used once in combination with a key, to provide different permutations (e.g. a random keystream) as required. Seen in TLS in any counter mode, including modern AEAD ciphers.

Padding

Additional bytes added to a message as required to bring the message to the required size of a block cipher or hash function.

Poly1305

A modern MAC that is often used with ChaCha20. It's name is derived from the polynomial function used within it, $2^{130} - 5$.

Public-key Cryptography

Another term that is commonly used to refer to asymmetric encryption, but also encompases key exchange mechanisms such as Diffie-Hellman.

RSA

The most commonly used public-key cryptographic system. Provides a public and private key pair, either of which can be used for encryption, with the other reversing this process. RSA is used for encryption and for signing. RSA is based around the difficulty of solving the integer factorisation problem.

SHA-1

A hash function with a 160-bit block size. Still secure within structures like HMAC, but a collision has been found, so security advice is to move toward SHA-2 at this point.

SHA-2

Very similar to SHA-1, but with a 256 or 512-bit block size. This increased block size makes collisions much more difficult, and this function is currently considered secure.

SHA-3

An alternative to SHA-2, should a serious vulnerability with SHA-2 be found. Offers similar hash lengths, but the function itself is very different to SHA-1 and SHA-2.

Symmetric Encryption

Encryption that uses a single key for both encryption and decryption.

Public Key Infrastructure

Baseline Requirements

A set of technical and policy requirements that Cas must adhere to. Most root store programs enfore these in order for a CAs root certificate to be trusted.

Certificate

A file in a standard format that contains, among other things, a public key and identifying information about the owner.

Certificate Chain

A chain of intermediate certificates leading from an end entity (leaf certificats to a trusted root certificate.

Certificate Extension

An optional extension to the standard certificate format. Usually used to add functionality at a later date.

Certificate Revocation List (CRL)

A list of revoked certificates distributed by a CA.

Certificate Signing Request (CSR)

A signed file in a standard format that incudes data required by a CA to issue a certificate. Typically, a public key and subject identifying information. Other information on the resulting certificate will be generated by the CA.

Certificate Store / Trust Store

A list of trusted root certificates. Operating systems manage these trust stores, along with Mozilla, and some browsers. Many other browsers and programs rely on the OS trust stores.

Certification Authority

Commonly called a Certificate Authority (CA). An organisation that issues signed certificates.

Common Name (CN)

The name of the subject of this certificate. For end entity certificates this will usually be a domain name. For intermediate and root certificates this will be a human readable name.

Critical Extension

A certificate extension, but marked such that failure to parse should be grounds to reject this certificate. For example, if a client does not understand this extension.

DER

A binary encoding used for, among other things, certificates and keys. Stands for Distinguished Encoding Rules for ASN.1.

Domain Validated (DV) Certificates

Certificates for which the subject has demonstrated control over the domain in the CN field. This is verified by the CA.

Extended Validation (EV) Certificates

Similar to an OV certificate, but with more stringent checks on the validation of the organisation.

Intermediate Certificate

A certificate that signs end entity certificates or other intermediate certificates. These are used to prevent the root keys being required regularly.

Issuer

A field on a certificate indicating the name of the certificate that signed it.

OCSP

A response signed by a CA indicating that a specific certificate is valid. May be used by a client to verify a certificate has not been revoked.

OCSP Stapling

The process of a server sending an OCSP response with its certificate, such that the client does not have to perform this task themselves. Uses the TLS Certificate Status Request extension.

Organisation Validation (OV) certificates

Certificates where the identification of the organisation in the subject has been verified by the CA.

PEM

An ASCII base 64 encoded file used for storing certificates and private keys.

Pinning

The process of validating a certificate against a known public key or certificate stored in ahead of time. Allows clients to provide additional assurances as to the validity of a certificate, as generally any certificate signed by any CA is valid.

Pinset

A set of pins for multiple end entity, intermediate and root certificates.

Public Key Infrastructure

(PKI) is a standardised set of policies and file formats for the management and use of public key certificate..

Root Certificate

A certificate stored in a trust store, representing the end of a chain. These are usually self-signed, unless signed by another CA.

Self-signed Certificate

A certificate whose signature has been generated by using its own private key.

Subject Alternative Name

An X.509 extension used to hold alternative host names valid for a certificate. Useful for virtual servers and subdomains.

X.509

A standard certificate format widely supported in PKI.

Transport Layer Security

0-RTT

A handshake protocol supported in TLS 1.3. If a pre-shared key is available, the client can send this during the handshake, and immediately begin sending encrypted application data. Note: This doesn't protect against replay attacks, so should be used for read operations from the server only..

Alert

A TLS subprotocol (21). Indicates a notification or fatal error. Contains a byte for the message type, and a byte for the description index.

Application Data

A TLS subprotocol (23). Used to send any standard application data under whatever current encryption has been arranged.

ChangeCipherSpec

A TLS subprotocol (20). Indicates a party is to begin encrypting under a new set of keys and parameters. Used as part of a TLS 1.2 handshake, but not used in TLS1.3.

Cipher Suite

A string representing the selected ciphers and other algorithms used during an encrypted session. An example would be TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. From TLS 1.3, key exchange and authentication suites are separated and passed as extensions.

Client / Server Nonce

Random values passed during the client and server hello messages. They are used to prevent replay attacks, where messages are re-sent later.

Extensions

Optional additional data that may be sent within a TLS message. Originally extensions were optional, but some have become inbuilt into the protocol, particularly in TLS 1.3.

Finished

A handshake message indicating the end of the handshake protocol. Contains a MAC of all previous handshake messages, ensuring both the client and server have seen the same set of messages.

Handshake

A series of defined messages in TLS that establish the security parameters of a session between two parties. Contain, among others, the ClientHello, ServerHello, Certificate, and Finished messages.

Handshake (Message)

A TLS subprotocol (22). A handshake message that contains its own sub header indicating the type of message. Examples are ClientHello, ServerHello, Certificate, Finished.

HTTPS

A common use case for TLS, encrypted web connections using HTTP are known as HTTPS connections. Although this is the primary use case for TLS, it is by no means the only one.

Master Secret

A shared master secret derived from the combination of the pre-master secret, the client and server random values (nonces). These bytes are used to derive all key material required for a session.

OpenSSL

A widely used implementation of SSL/TLS. It forms the backend for many packages that offer TLS, and also provides CA, X509 and other related PKI functionality.

Pre-master Secret

The shared secret derived from the client and server key exchange messages.

Record

The common data structure for transport of any TLS message. Contains a header holding the type of the message, the version number, and the length of the payload. The payload itself is treaded as opaque, with the record unchanged regardless of the contents. Record contents may or may not be encrypted..

Renegotiation

Reestablishment of session parameters such as keys during a session. All TLS sessions will renegotiate from time to time to provide forward secrecy. Renegotiation can also be used to request a client certificate that wasnt required before. In TLS 1.3 renegotiation isnt supported in this way via ClientHello messages. Instead KeyUpdate and CertificateRequest messages.

Secure Socket Layer

(SSL) is a protocol that was a predecessor to TLS. Developed starting in 1994 by Netscape, only SSL3 bears resemblance to modern TLS. It is common for the acronyms TLS and SSL to be used interchangeably, but strictly speaking SSL is deprecated.

Transport Layer Security

(TLS) is a modern version of the SSL3 protocol, that has now undergone significate revisions and improvements. Currently on version 1.3.

Version

Two bytes indicating the major and minor TLS version numbers. TLS was seen as SSL3.1, thus TLS 1.0 had version number 3_1. The later versions are 3_2 (TLS 1.1), 3_3 (TLS 1.2) and 3_4 (TLS 1.3).