University of BRISTOL

Computer System- B Security

Introduction to Internet Security

SSL/TLS

Alma Oracevic

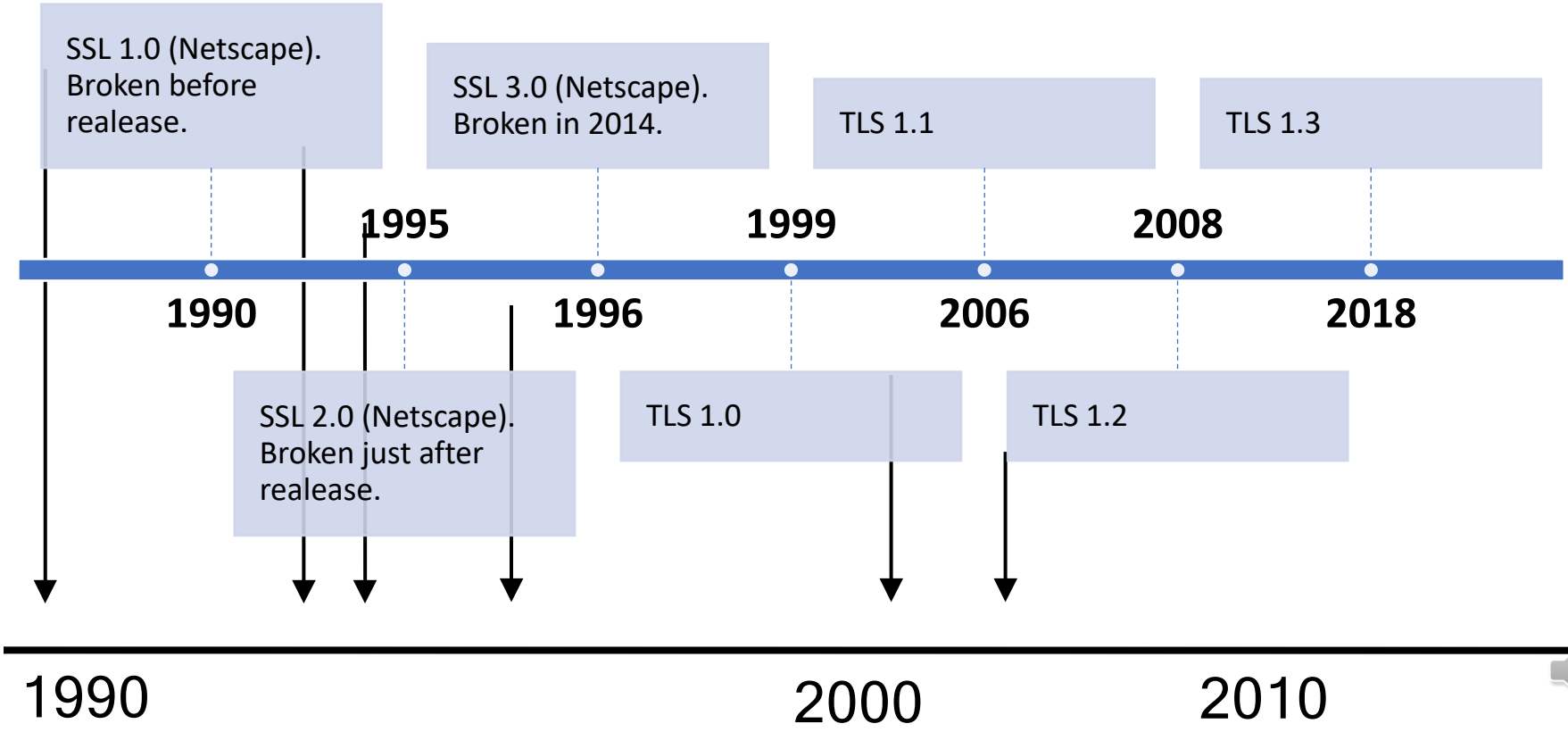
bristol.ac.uk

Recall… HTTPS and VPN across layers

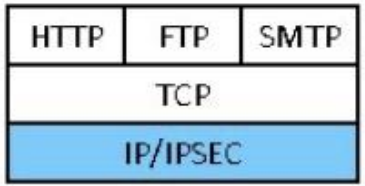
- Transport layer
  - –SSL/TLS
    - Provides encryption and authentication at application layer, which is the most common way to provide CIA security properties over the internet.

SSL/TLS

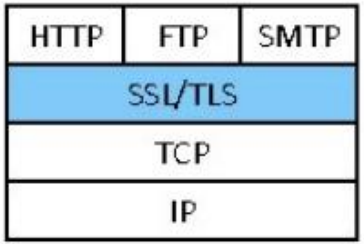
SSL / TLS timeline



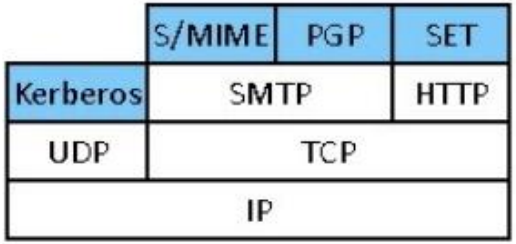
Security at layers



At the Network Level



At the Transport Level



At the Application Level

https://slidetodoc.com/the-internet-layers-tcp-udp-ip-ddo-s/

SSL / TLS Protocol

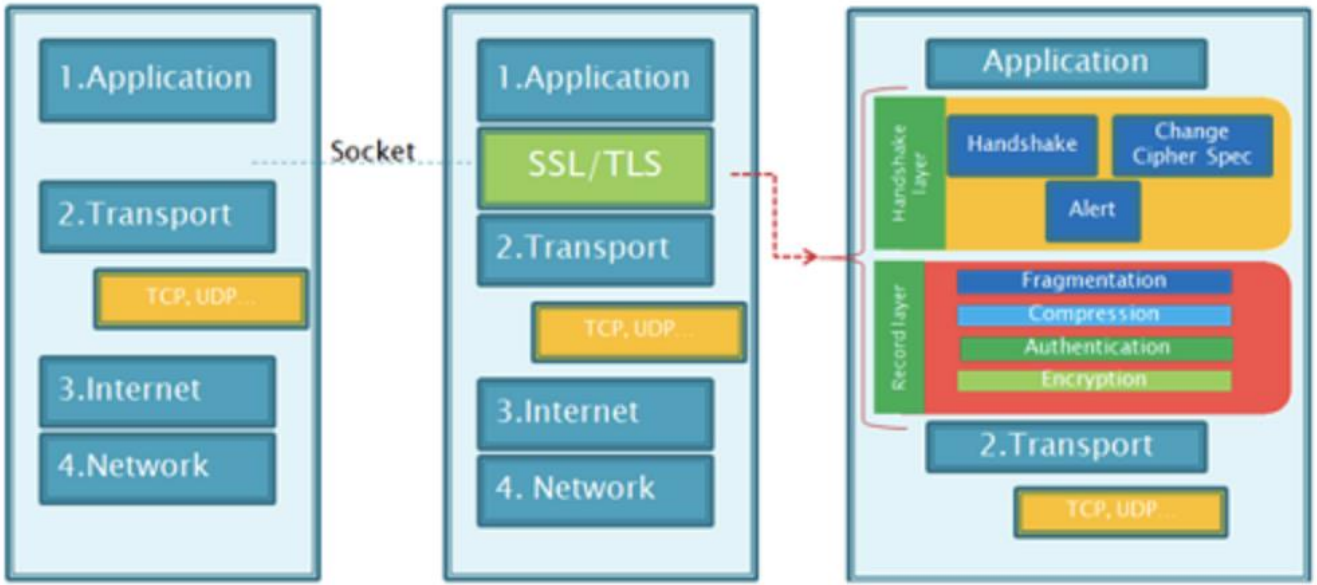


image-1: pic courtesy- google

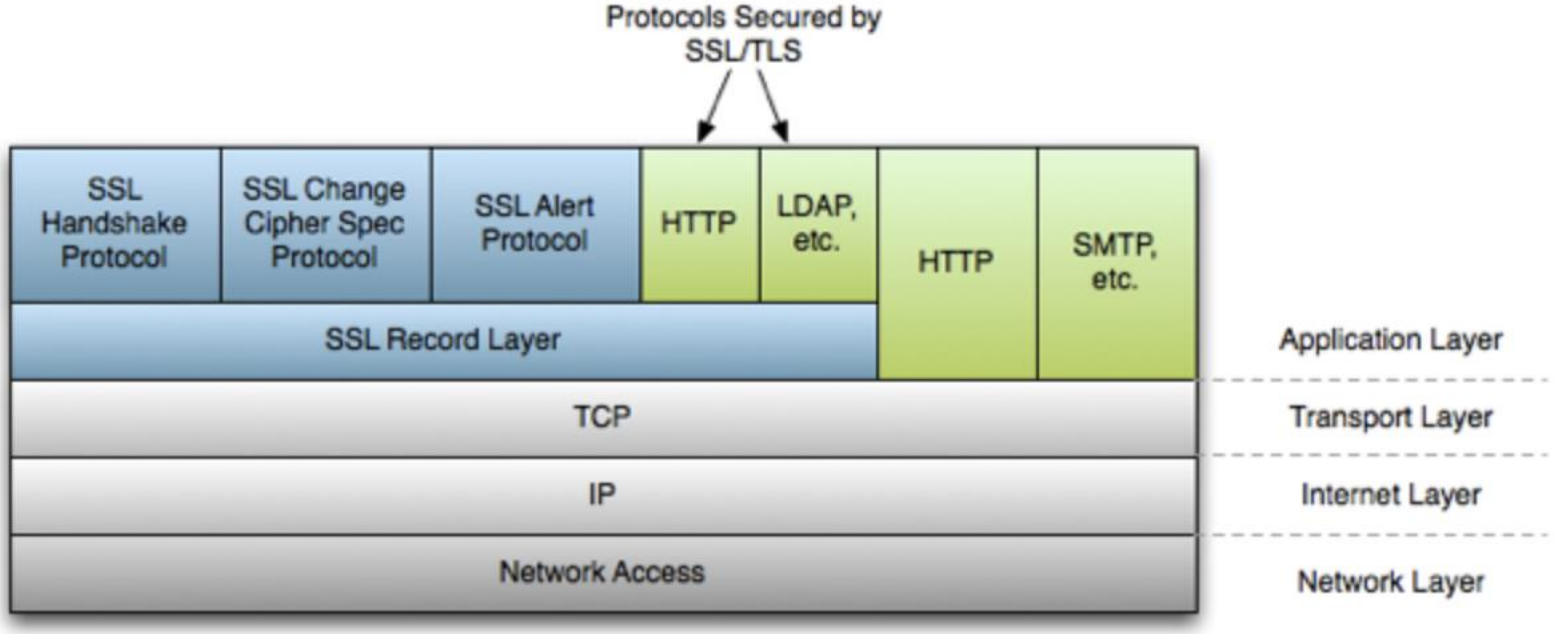
SSL / TLS

- Transport layer security service
- Originally developed by **Netscape**
- Uses TCP to provide a reliable end-to-end service
- Libraries (implementation)

  OpenSSL, BoringSSL, LibreSSL, GnuTLS,...
- Has two layers of protocols
  - L1: SSL Record Protocol
  - L2: Handshake, change cipher, alert

https://systemzone.net/how-to-create-free-ssl-tls-certificate-with-openssl/

SSL / TLS protocol diagram



https://www.wolfssl.com/docs/wolfssl-manual/appendix-a//

SSL / TLS protocol services

message integrity

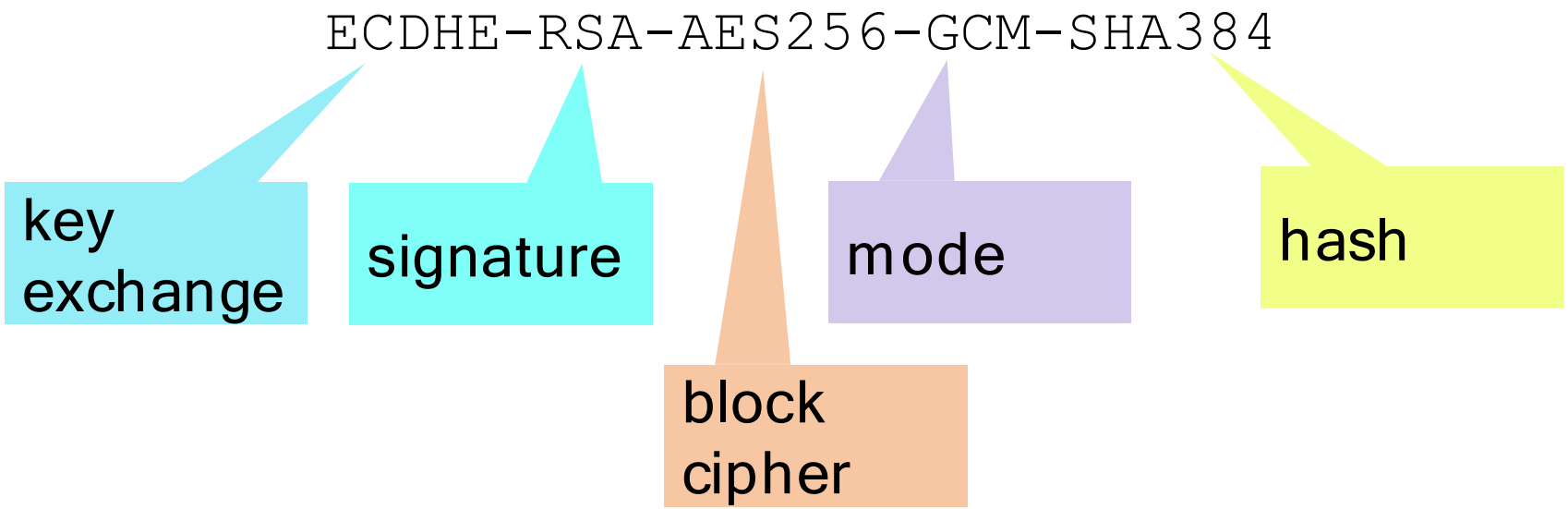
- using a MAC with shared secret key

confidentiality

- using symmetric encryption with a shared secret key defined by Handshake Protocol
- message is compressed (optionally) before encryption

TLS cipher suites

TLS 1.2 using OpenSSL 1.0.1f: 80 cipher suites, e.g.



TLS cipher suites

- Some of the main options:

key ex	sig	cipher	hash
DH	RSA	AES256-GCM	SHA
DHE	DSS	AES256-CBC	SHA384
ECDH	ECDSA	CAMELLIA	SHA256
ECDHE		AES128-GCM	
		AES128-CBC	

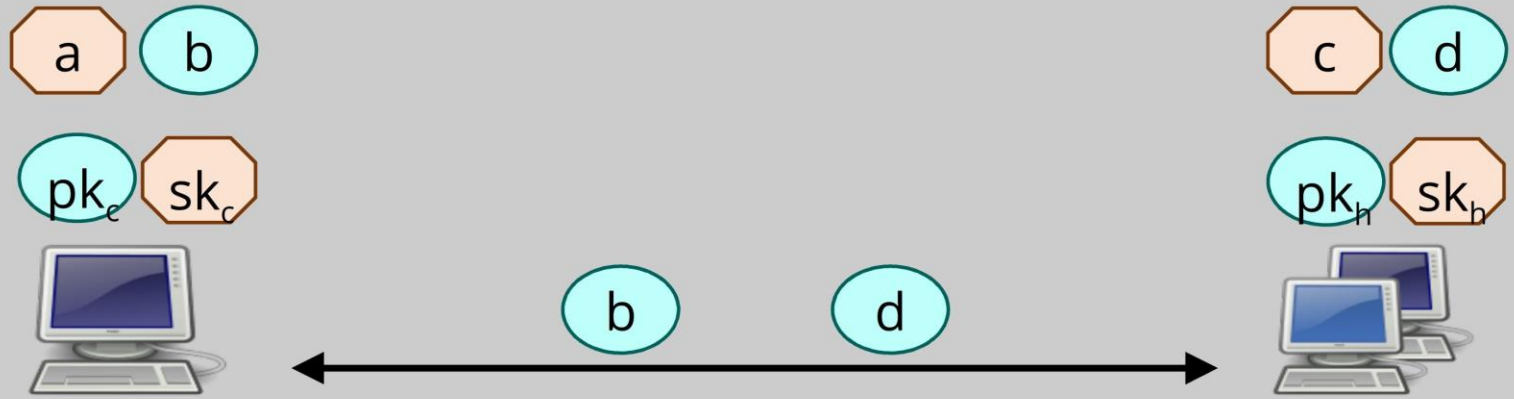
If using PKC, why key Exchange?

- An interactive session has forward secrecy if compromise of the parties, after the session has ended (i.e. in future), does not reveal session's contents.
- The usual way to achieve this is ephemeral key exchange, i.e. do a new key exchange for each session.

- Forward secrecy

Ephemeral key exchange

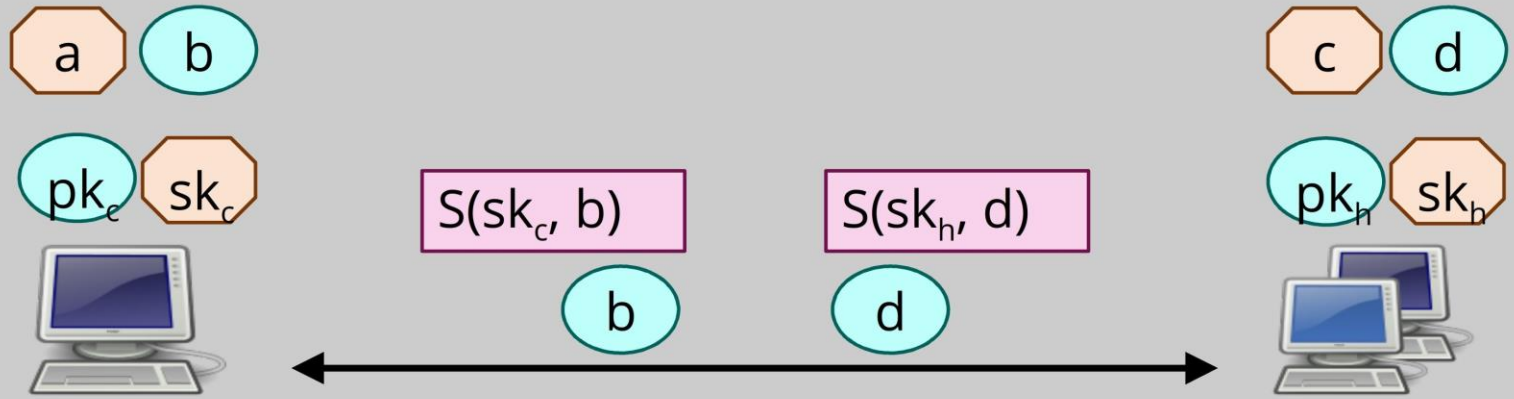
- Solution: create an *ephemeral* (=temporary) key pair for each session, do the key exchange with that. Delete the session keys as soon as the session ends.

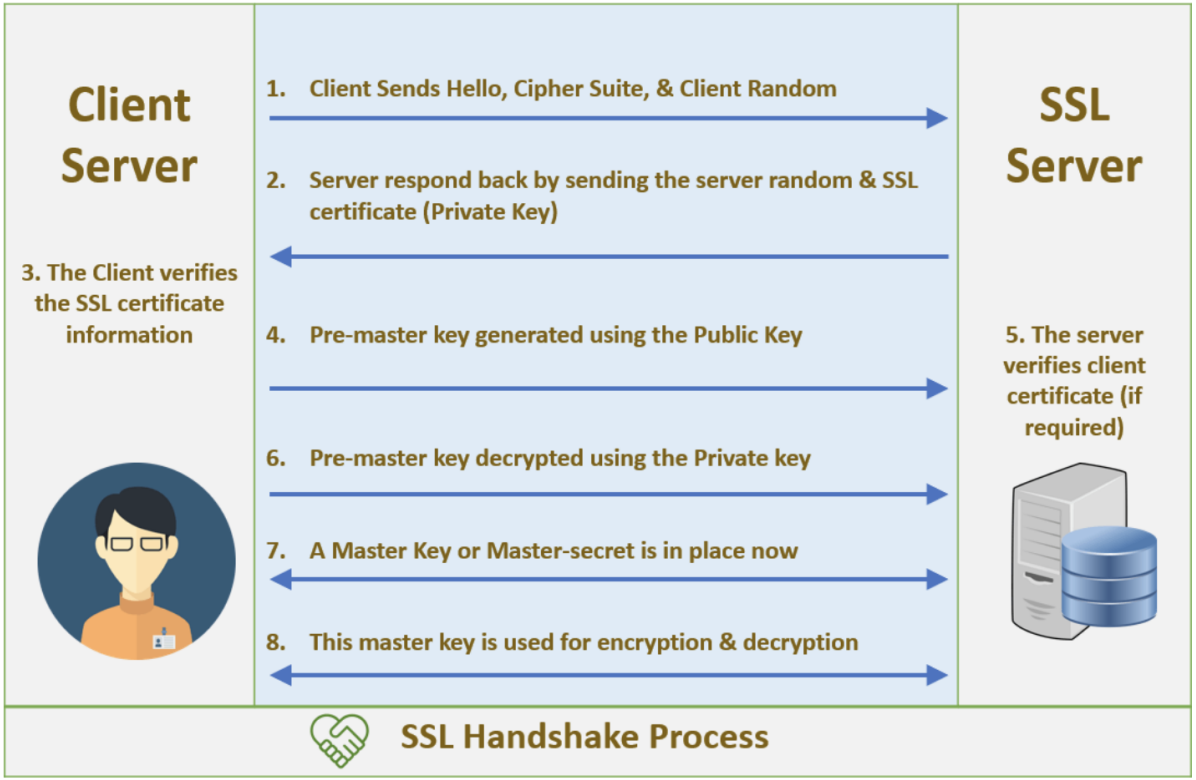


Ephemeral key exchange

Why do we have long-term keys at all then?

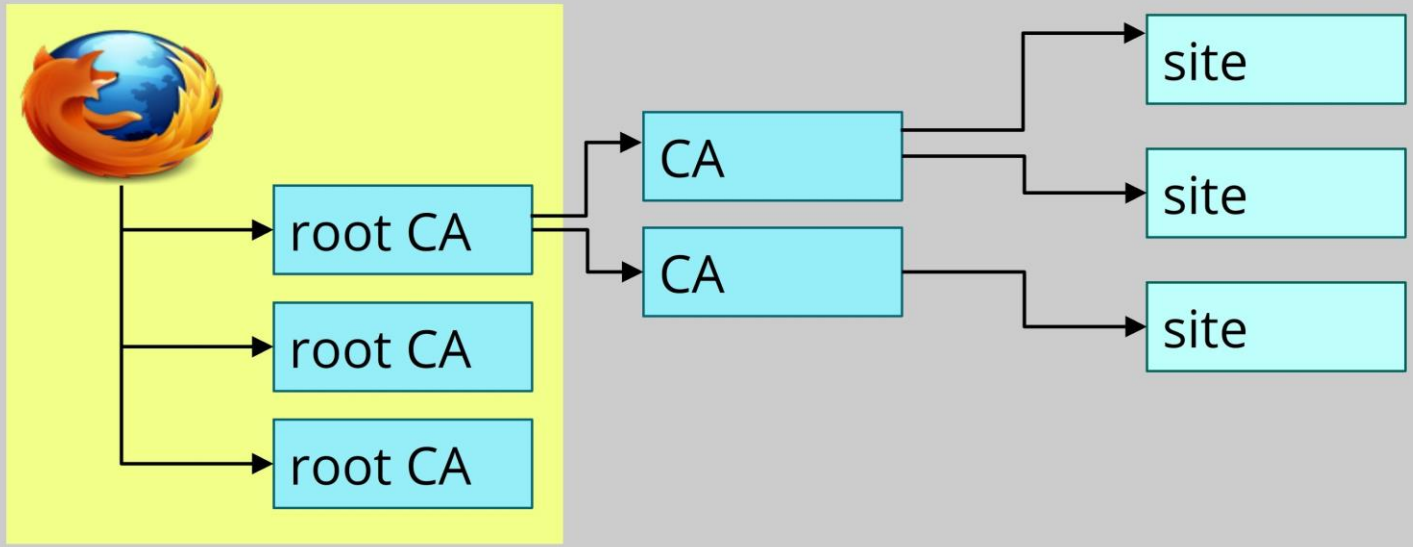
They are for authentication: parties *sign* the key exchange with their long-term keys.





SSL Handshake Protocol

TLS certificates



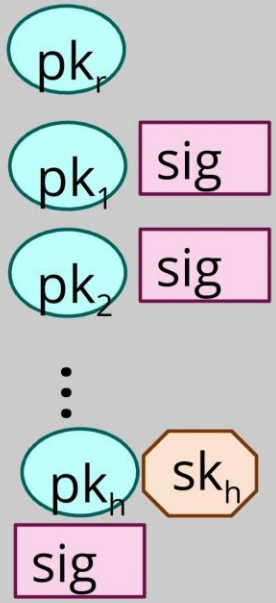
Root CA certificates are shipped with your browser.

TLS protocol layer

root of trust

intermediate CA keys

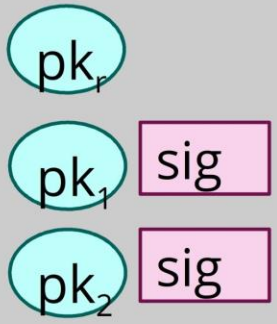
host key



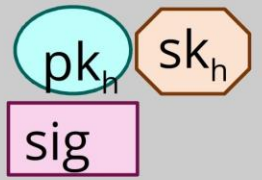
TLS protocol layer

root of trust

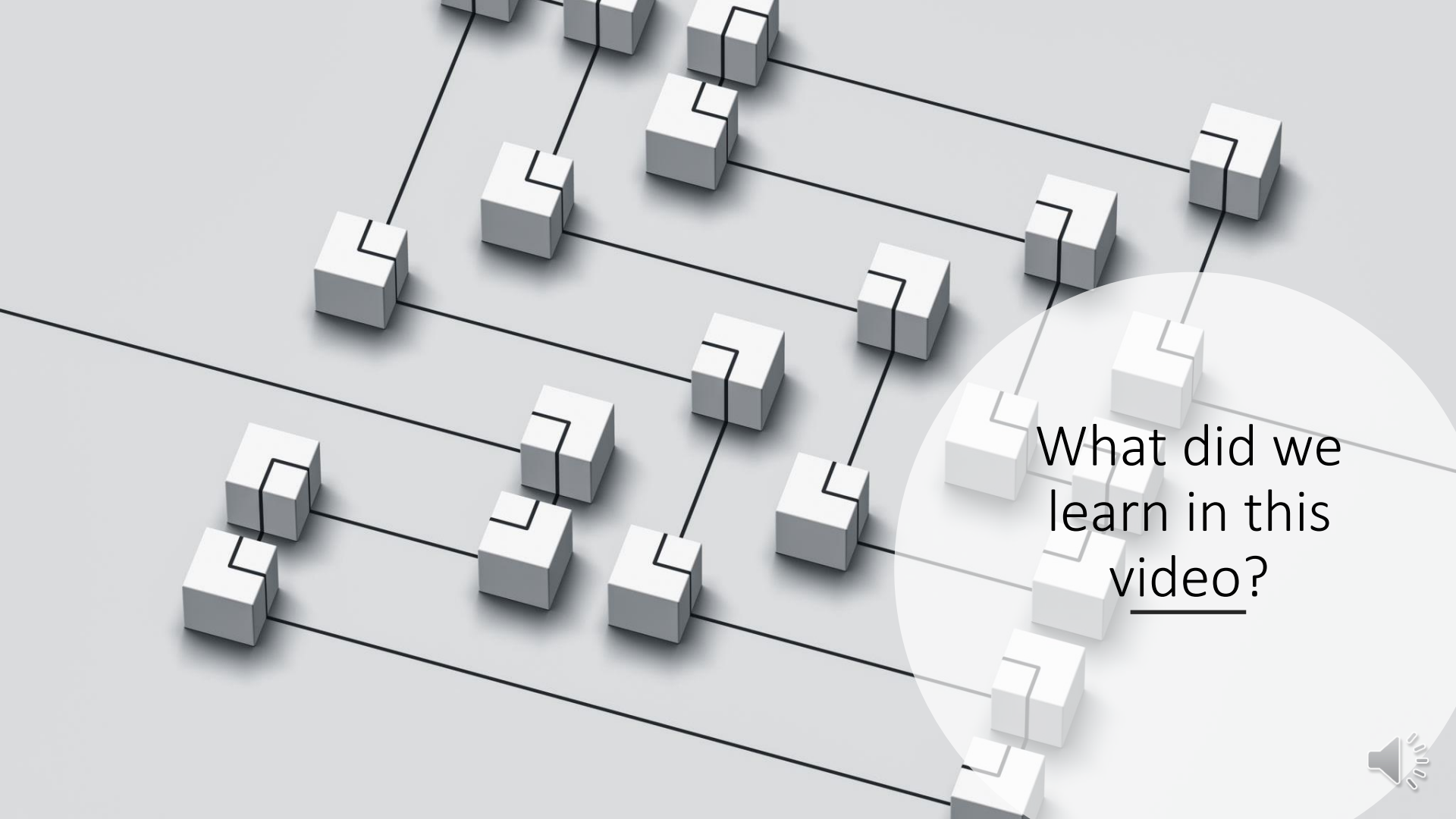
intermediate CA keys



host key



We can check such data from our browser!


What did we learn in this video?