# Security in application layer protocols

2024/25 Q2

***Jaime Delgado***

DAC - UPC

DMAG
DISTRIBUTED MULTIMEDIA APPLICATIONS GROUP

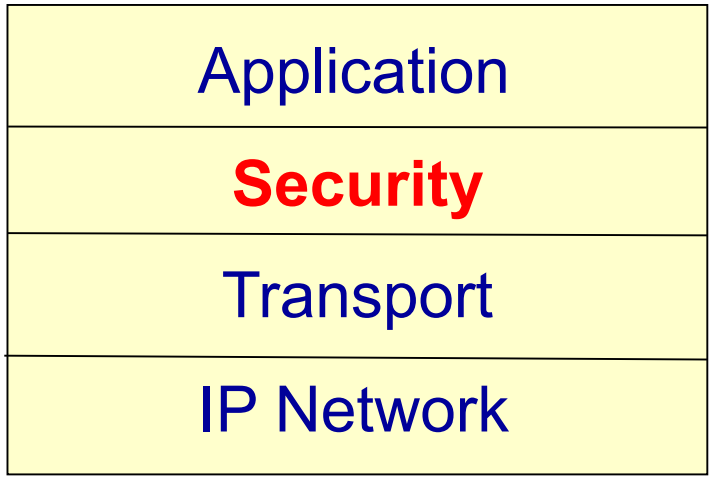
# Security in application layer protocols

Protocols:

- **Web (HTTP)**
  - **TLS**
  - **QUIC**
- **E-mail (S/MIME)**

# Protocols

- Web (HTTP):
  - HTTPS: Secure transport (TCP) connection
    - → Transport Layer Security (TLS) / Secure Sockets Layer (SSL)

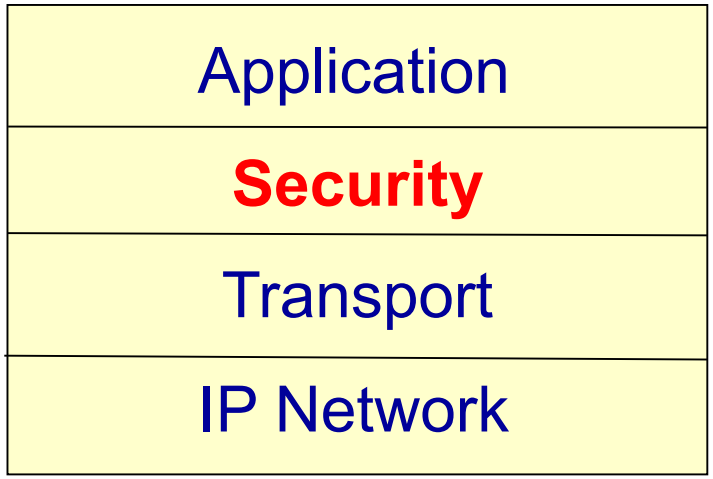



- E-mail

# Protocols

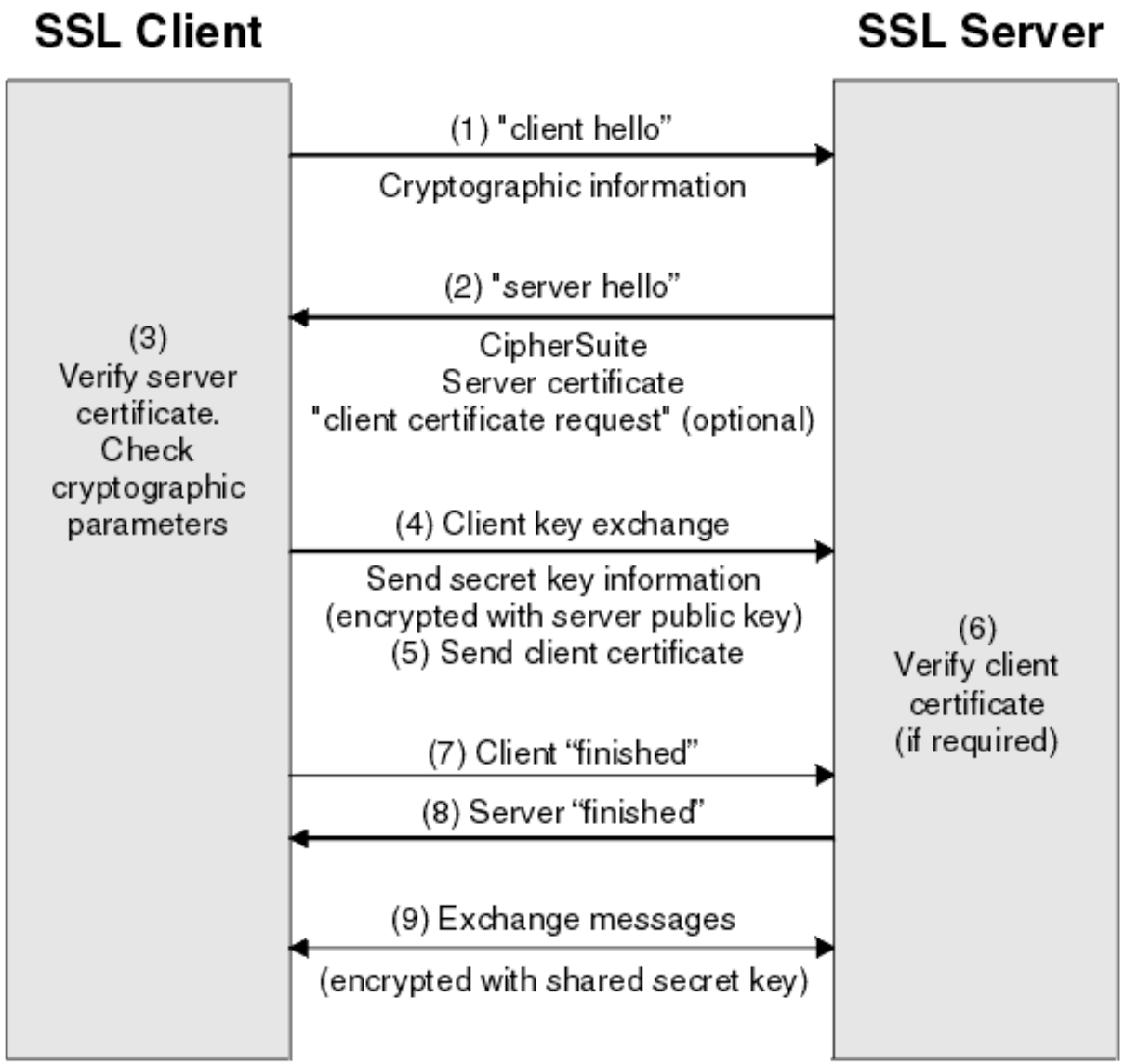
- Web (HTTP):
  - HTTPS: Secure transport (TCP) connection
    - → Transport Layer Security (TLS) / Secure Sockets Layer (SSL)

Application data encrypted?




- E-mail

# HTTPS: TLS/SSL handshake (v1.2)



# TLS (Transport Layer Security) protocol

- Versions:
  Still available: TLSv1.2 (RFC5246, 2008)
  New: **TLSv1.3** (**RFC8446**, Aug. 2018, started 2014)
- *Handshake protocol phase*:
  - Authentication one or both sides (usually the server)
  - Negotiation: “cipher suites” (only Elliptic Curve *Diffie-Hellman* key exchange algorithms, in v1.3)
- *Record protocol phase*:
  - Carries and encapsulates data
  - Adds a MAC, encrypts *application protocol data* and adds a TLS header (5 bytes)

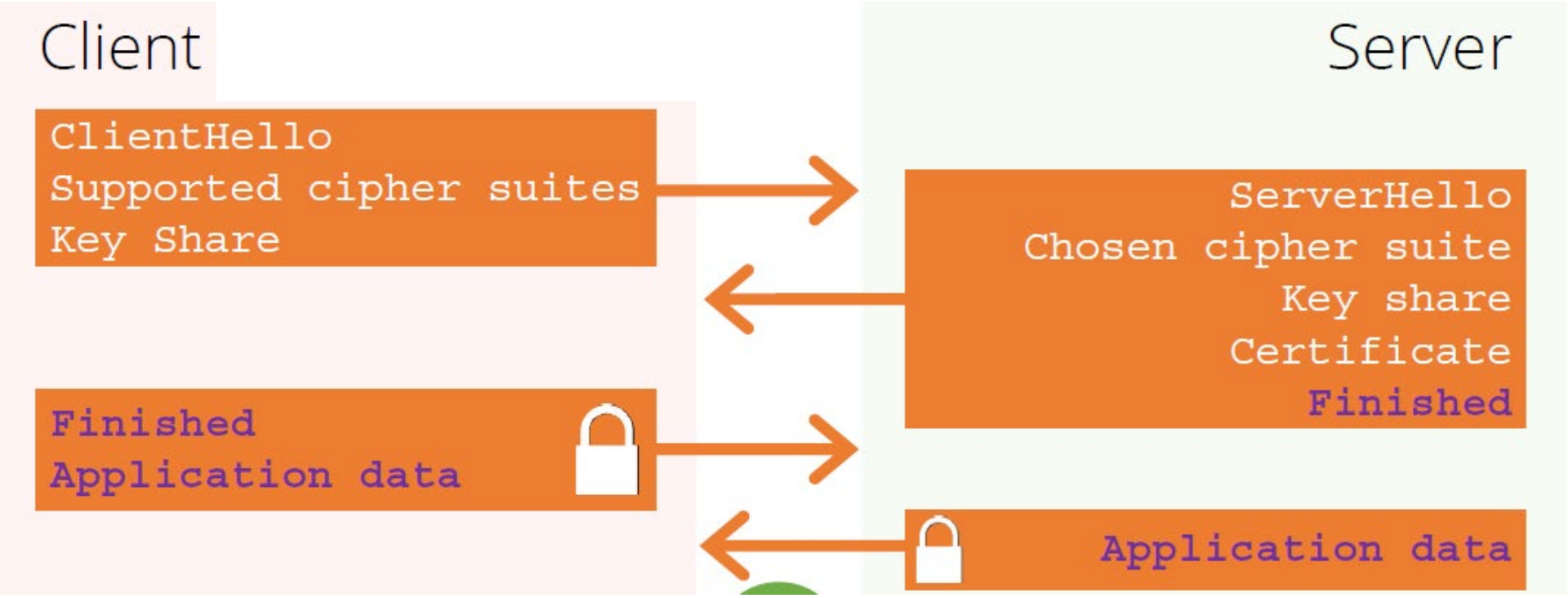
# TLS (Transport Layer Security) protocol

- Versions:
  Still available: TLSv1.2 (RFC5246, 2008)
  New: **TLSv1.3** (**RFC8446**, Aug. 2018, started 2014)
- *Handshake p*
  - Authenticati
  - Negotiation:
    *Hellman* key
- *Record proto*
  - Carries and encapsulates data
  - Adds a MAC, encrypts *application protocol data* and adds a TLS header (5 bytes)

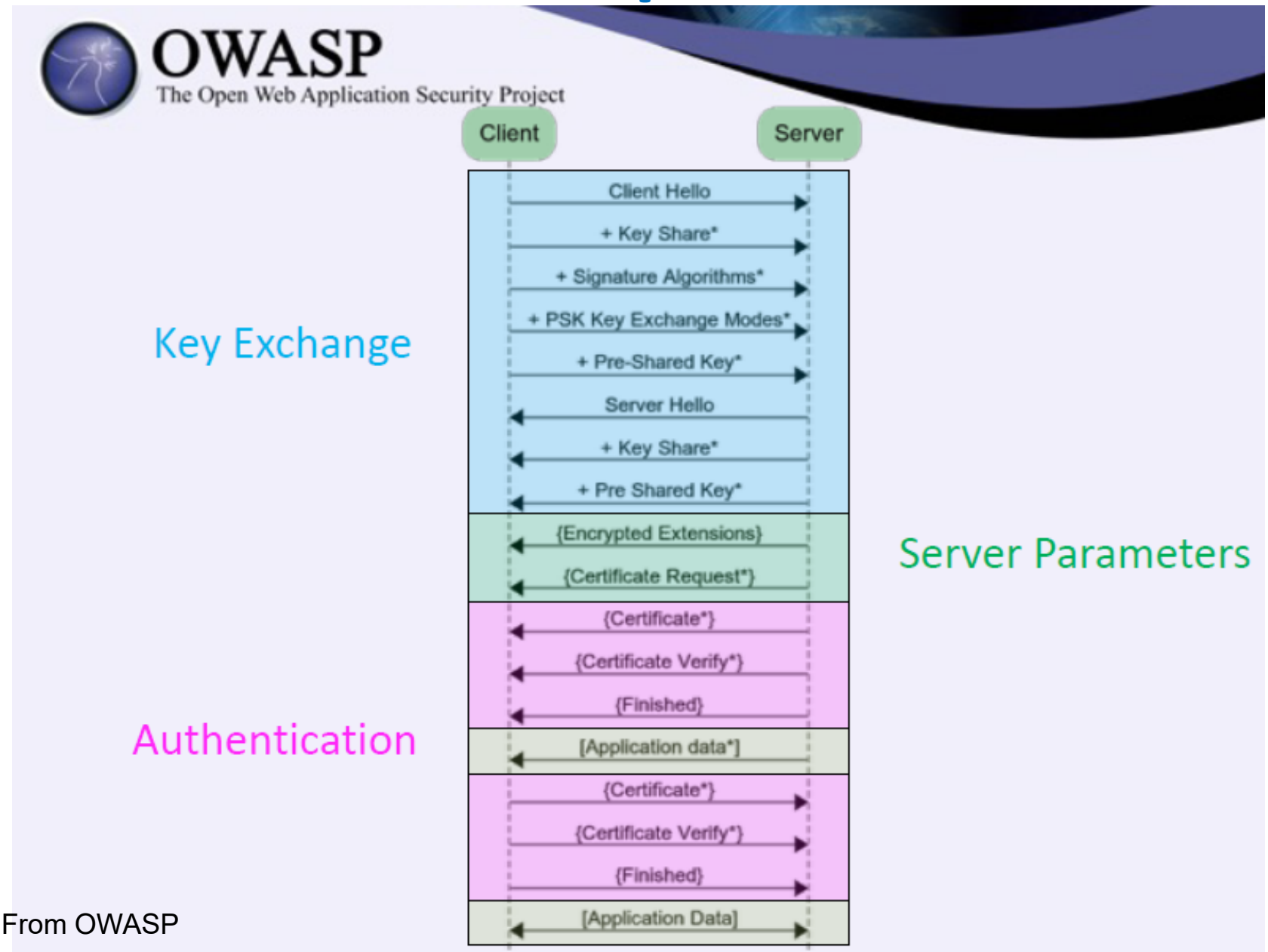
Work going on (since August 2020)
in a replacement: **RFC8446bis**
Current version (12) Febr. 2025

`https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/`

# HTTPS: TLSv1.3 handshake & record



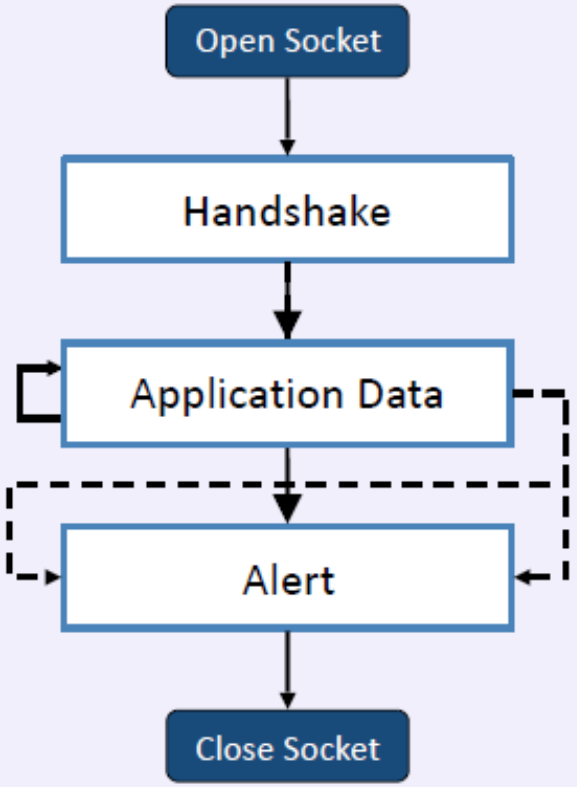
# TLSv1.3 protocol




From OWASP

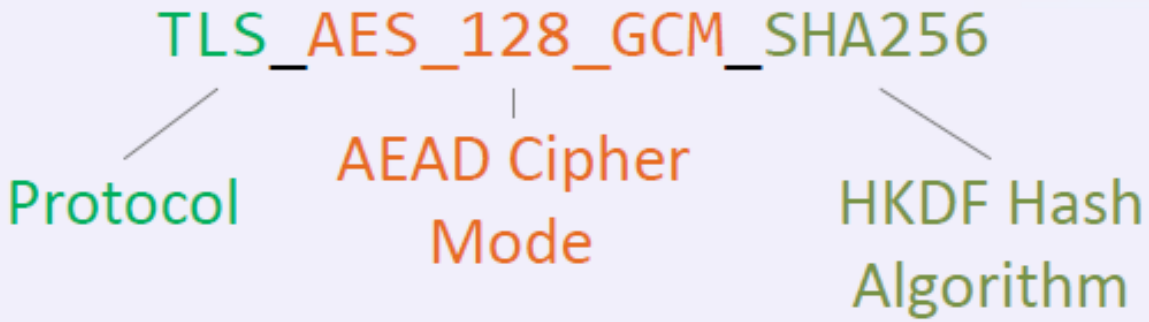
# TLSv1.3 protocols details

- Handshake
  - Agree a cipher suite.
  - Agree a master secret.
  - Authentication using certificate(s).
- Application Data
  - Symmetric key encryption.
  - AEAD cipher modes.
  - Typically HTTP.
- Alerts
  - Graceful closure, or
  - Problem detected.




From OWASP

# TLSv1.3 cipher suites




- TLS v1.3 supports 5 cipher suites.
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_CCM_8_SHA256

From OWASP

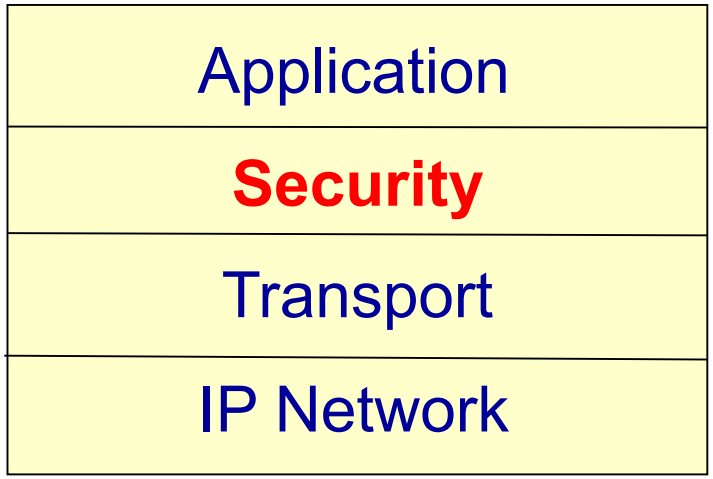
# TLSv1.3 cipher suites

- AEAD: Authenticated Encryption with Associated Data
- HKDF: Key Derivation Function (KDF) based on a *Hash*-based Message Authentication Code (HMAC)
- **AEAD**s:
  - GCM: AES Galois Counter Mode
  - CCM: Counter with CBC (Cipher Block Chaining) - MAC mode
  - ChaCha: a stream cipher
  - Poly1305: cryptographic MAC
    (Message Authentication Code)

# Protocols

- Web (HTTP):
  - HTTPS: Secure transport (TCP) connection
    - → Transport Layer Security (TLS) / Secure Sockets Layer (SSL)

Application data encrypted?




  - Alternative to TLS → QUIC (HTTP/3)

# QUIC

- "Quick UDP Internet Connections"
- Originally (2014): Protocol between Google services and Chrome. HTTP3 = HTTP2 over UDP with integrated security
- Standardization (IETF):
  - IETF QUIC WG October 2016
  - HTTP as initial application

  - *draft-ietf-quic-transport-34 (Jan. 2021);* Expires: July 2021 →
    → **RFC9000 (Proposed Standard) May 2021**
  - `https://www.rfc-editor.org/rfc/rfc9000.html`
- **QUIC:**

  ***A UDP-Based Multiplexed and Secure Transport***

# QUIC features

- New encrypted Internet transport protocol
- Improvements to accelerate HTTP traffic and make it more secure
- Runs on top of UDP !!
- Objective: replacing TCP and TLS on the web?
- **Main goal**: Improve perceived performance of connection-oriented web applications

Los dos están conviviendo, no tiene el objetivo de reemplazarlo.

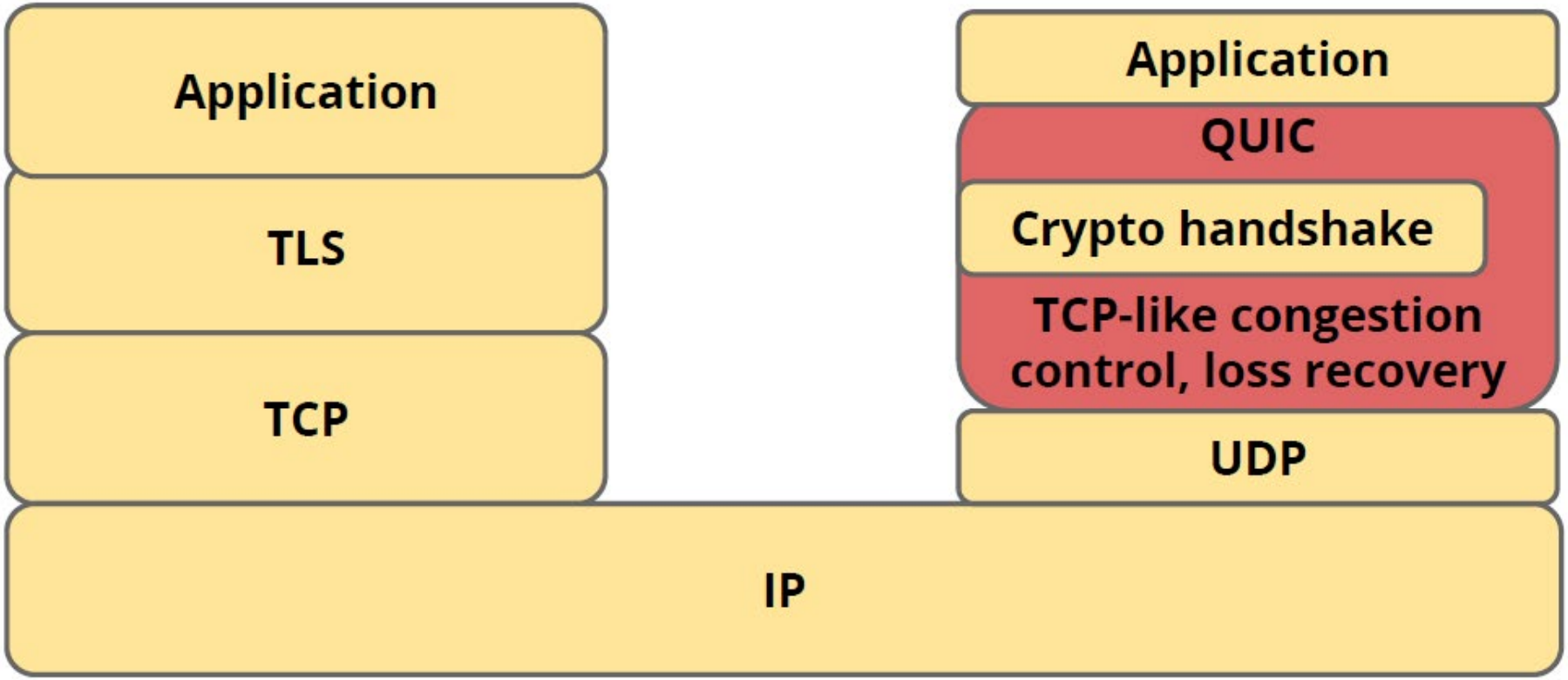
# QUIC “transport”

- https://www.rfc-editor.org/rfc/rfc9000.html
- QUIC, RFC9000 (Proposed Standard) (May 2021)
- **“This document defines the core of the QUIC transport protocol. QUIC provides applications with flow-controlled streams for structured communication, low-latency connection establishment, and network path migration. QUIC includes security measures that ensure confidentiality, integrity, and availability in a range of deployment circumstances. Accompanying documents describe the integration of TLS for key negotiation, loss detection, and an exemplary congestion control algorithm.”**

# QUIC – the standard

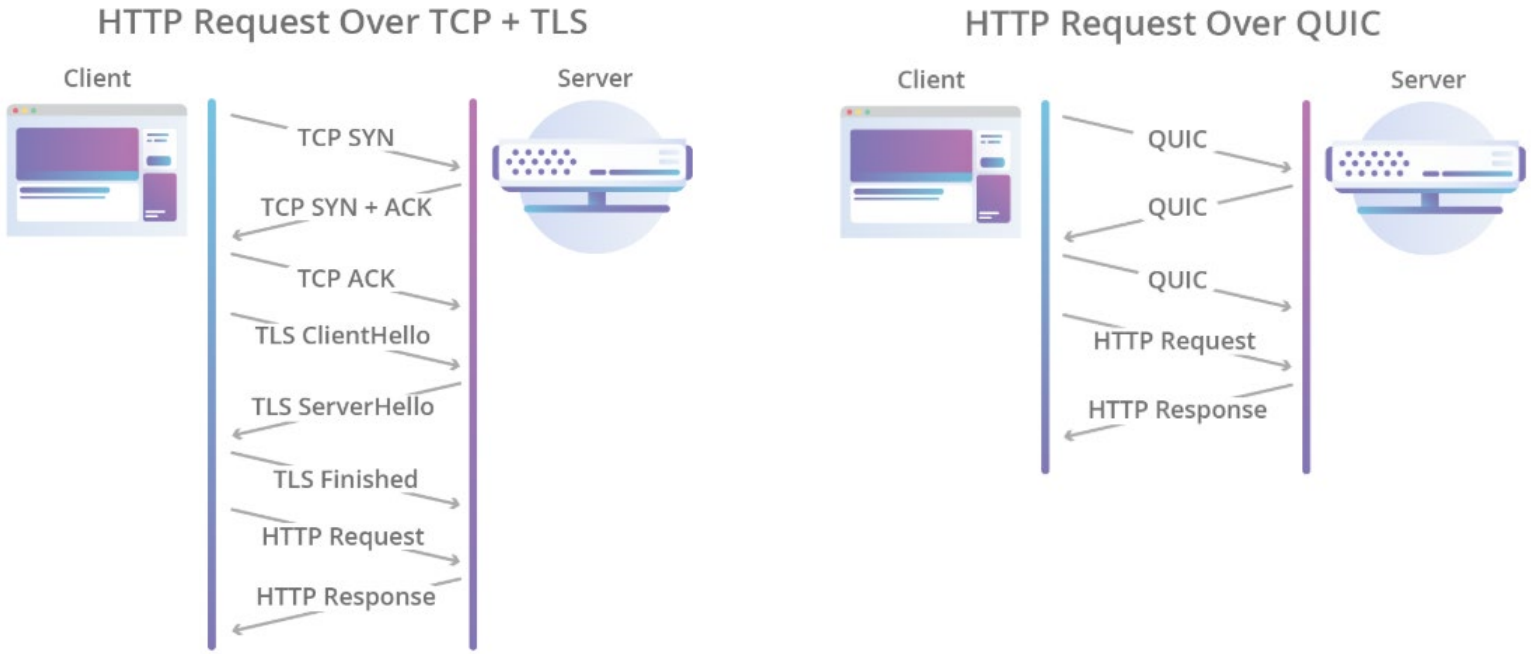
- Multiplexed and secure transport protocol that runs on top of UDP
- Reduced connection and transport latency
- Bandwidth estimation in each direction to avoid congestion
- Mechanisms for connection establishment, stream multiplexing, stream and connection-level flow control, and data reliability
- **Additionally**: loss recovery, congestion control, use of TLS 1.3 for key negotiation

# QUIC architecture



# Authenticated and encrypted header and payload

- Secure-by-default transport protocol
- Authentication and encryption
- TLS 1.3



# HTTP/3 vs. QUIC

- https://datatracker.ietf.org/doc/html/draft-ietf-quic-http-34, Internet-Draft, February 2021

  → *RFC 9114, June 2022*

- **Hypertext Transfer Protocol Version 3 (HTTP/3)**
- **"The QUIC transport protocol has several features that are desirable in a transport for HTTP, such as stream multiplexing, per-stream flow control, and low-latency connection establishment. This document describes a mapping of HTTP semantics over QUIC. This document also identifies HTTP/2 features that are subsumed by QUIC, and describes how HTTP/2 extensions can be ported to HTTP/3."**

# HTTP/3 vs. QUIC

- https://datatracker.ietf.org/doc/html/draft-ietf-quic-http-34, Internet-Draft, February 2021

  → *RFC 9114, June 2022*

- **Hypertext Transfer Protocol Version 3 (HTTP/3)**
- **"The QUIC transport protocol has several features that are desirable in a transport for HTTP, such as stream multiplexing, per-stream flow control, and low-latency connection establishment. This document describes a mapping of HTTP semantics over QUIC. This document also identifies HTTP/2 features that are subsumed by QUIC, and describes how HTTP/2 extensions can be ported to HTTP/3."**

**HTTP/3 is HTTP over QUIC**

# Security in applications

Protocols:

- **Web (HTTP)**
  - **TLS**
  - **QUIC**
- **E-mail (S/MIME)**

# Protocols

- Web (HTTP)

- E-mail:
  - **S/MIME** (Secure / Multipurpose Internet Mail Extensions)
    - MIME over pkcs#7 (enveloped)
    - **IETF RFC 8551 (2019)**: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 - Message Specification"

      (Version 3 (1st for IETF) started in RFC 2633, 1999)

  - PGP: Signature

# Protocols

- Web (HTTP)

- E-mail:
  - **S/MIME** (Secure / Multipurpose Internet Mail Extensions)
    - MIME over pkcs#7 (enveloped)
    - **IETF RFC 8551 (2019)**: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 - Message Specification"

      (Version 3 (1st for IETF) started in RFC 2633, 1999)

  - PGP: Signature

# S/MIME

- **RFC 8551**
  Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 - Message Specification

- Different messages built over pkcs7/CMS:
  - Envelope-Only
  - Authenticated Envelope-Only
  - Signed-Only