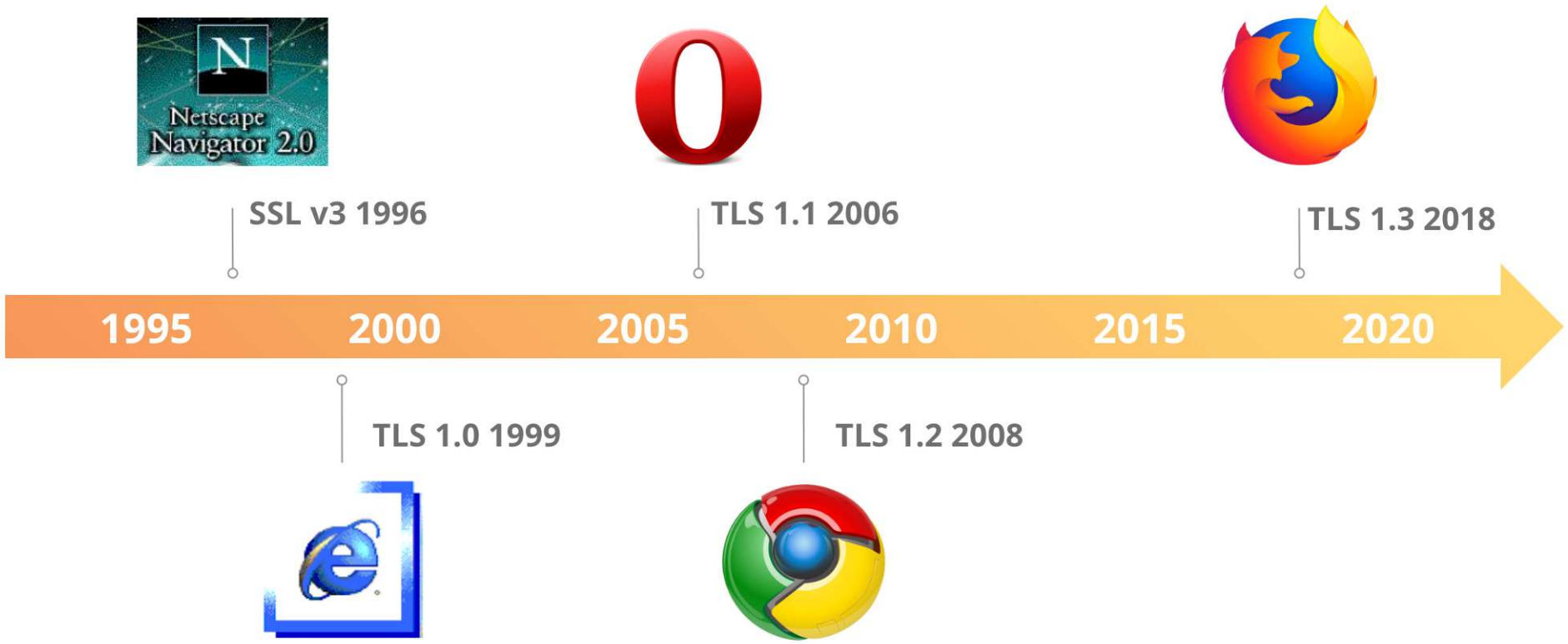
UTN.BA

TLS

Transport Layer Security

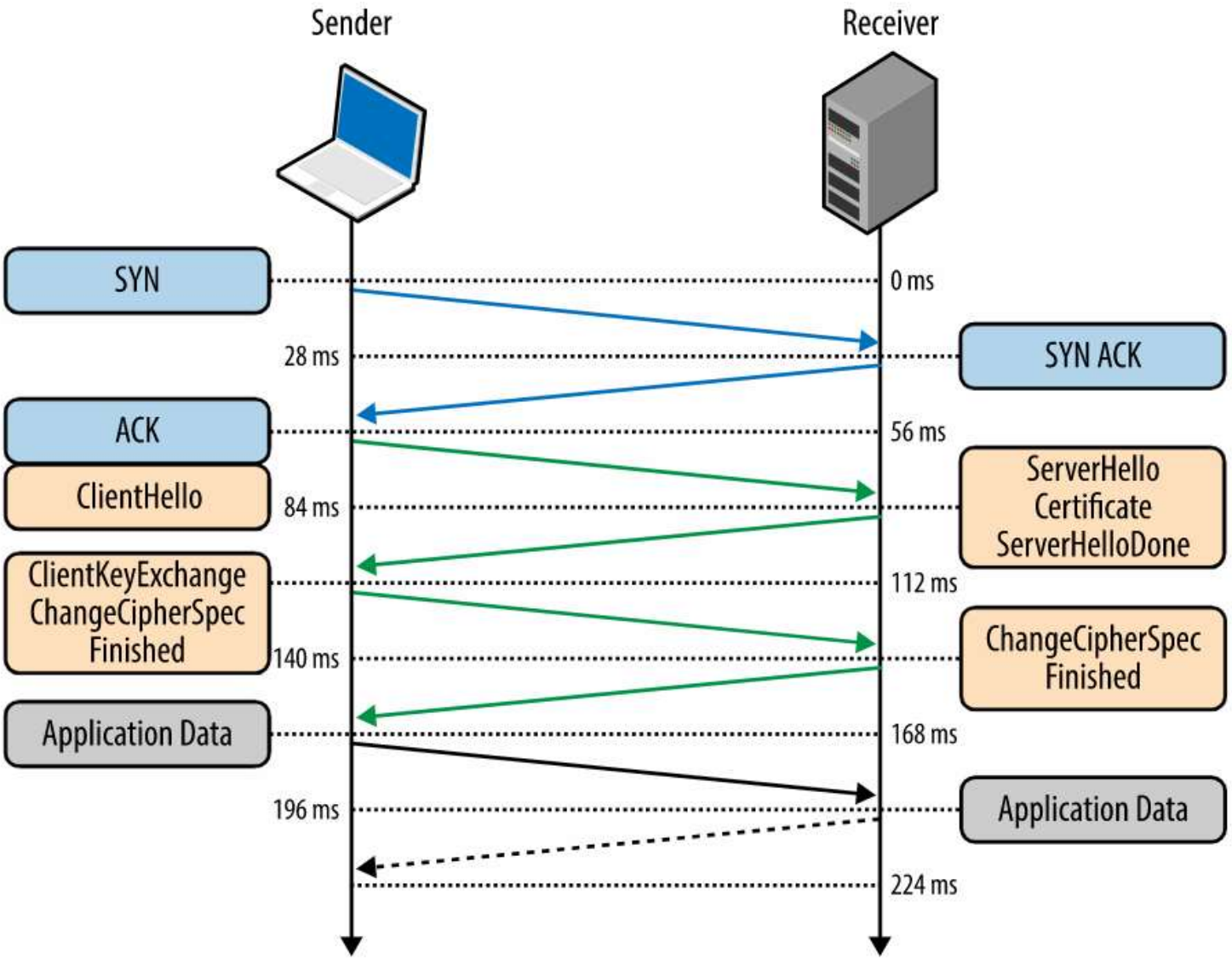
Evolución: SSL -> TLS



TLS (evolución del SSL)

- Evolución del Secure Socket Layer (SSL) creado por Netscape, actualmente obsoleto.
- Ampliamente utilizado para proteger tráfico web entre un servidor HTTP y un browser
- Utiliza encriptación simétrica y asimétrica

Handshake


Sender
Receiver
SYN
0 ms
28 ms
SYN ACK
ACK
56 ms
ClientHello
84 ms
ServerHello
Certificate
ServerHelloDone
ClientKeyExchange
ChangeCipherSpec
Finished
112 ms
140 ms
ChangeCipherSpec
Finished
Application Data
168 ms
196 ms
Application Data
224 ms

Handshake

- **Client HELLO** El cliente abre una conexión TCP y envía el mensaje TLS *Client Hello* indicando la solicitud de una conexión segura. Envía una lista de "Cipher Suites“ soportados

Cipher Suite es una lista de algoritmos criptográficos ordenados por orden de preferencia. El servidor elegirá el mayor que pueda soportar. Contiene:

key exchange algorithm – cómo se intercambiarán las claves simétricas
authentication algorithm – cómo se autenticará
bulk encryption algorithm – algoritmo de clave simétrica a utilizar
Message Authentication Code (MAC) – método para chequear integridad.

TLS_ECDHE_ECDSA_WITH_AES_256_CB C_SHA384

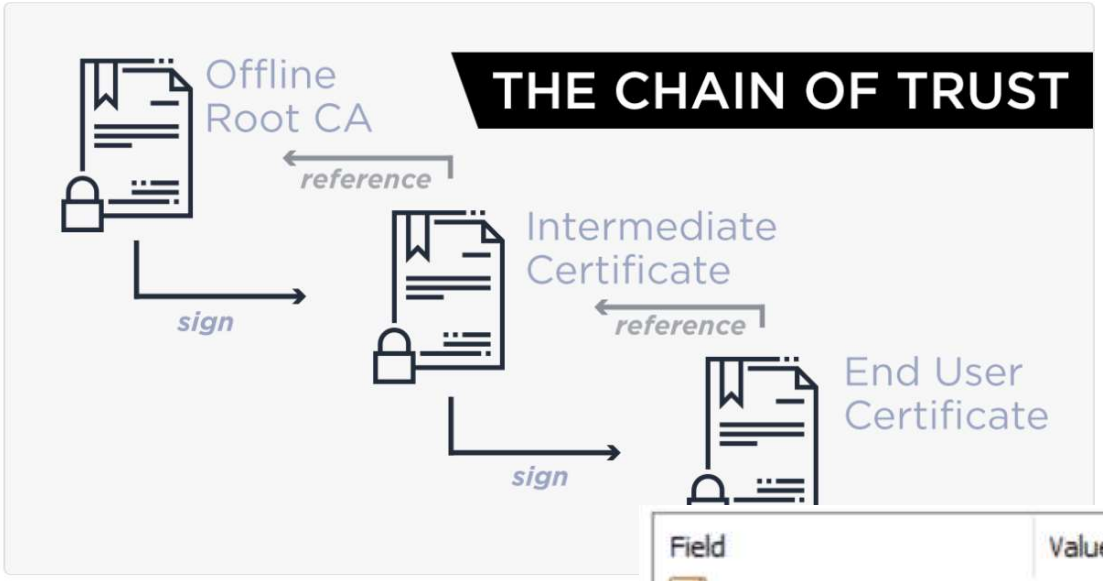
TLS - protocol; ECDHE key exchange algorithm; ECDSA authentication algorithm; AES_256_CBC bulk encryption algorithm; and SHA384 MAC algorithm.

Handshake

- **Server HELLO** El servidor acepta utilizar TLS en esta conexión, informando el Cipher seleccionado.
- **CERTIFICATE** El servidor envía la cadena de certificados
- **Server Key Exchange/Client Key Exchange** Permite a ambos interlocutores encriptar el intercambio de clavesmensajes
- **Change Cipher Spec** Estos mensajes finalizan el handshake.

La autenticación del cliente (TLS mutual authentication) es opcional. El servidor puede solicitarle al cliente su certificado luego del Server Hello.

Certificados



Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	DigiCert Global Root CA, www.digicert.
Valid from	lunes, 6 de noviembre de 2017 09:23::
Valid to	sábado, 6 de noviembre de 2027 09:2:
Subject	RapidSSL RSA CA 2018, www.digicert.
Public key	RSA (2048 Bits)

CN = RapidSSL RSA CA 2018
OU = www.digicert.com
O = DigiCert Inc
C = US