¿En qué momento acepta tu navegador la identidad de un servidor HTTPS?

Cuando accedemos a una página web mediante HTTPS, se produce un proceso llamado *handshake TLS* que permite establecer una comunicación cifrada y verificar que estamos hablando con el servidor legítimo.

Si ejecutamos un comando como:

curl -v https://www.ejemplo.com

podemos observar una línea similar a esta:

TLS handshake, Certificate (11)

Ese es el momento en el que el servidor envía su certificado digital al cliente.

¿Y qué contiene ese certificado?

- La identidad del servidor (dominio).
- La clave pública del servidor.
- La firma digital de una Autoridad de Certificación (CA).

Una vez recibido el certificado, el cliente realiza varias comprobaciones:

 El dominio coincide con el solicitado.

 El certificado no está caducado.

 La entidad emisora es de confianza.

 La cadena de certificación es válida.

Si todo es correcto, aparece un mensaje similar a:

SSL certificate verify ok.

Ese mensaje indica que el cliente ha aceptado la identidad del servidor y confía en la clave pública recibida.

Es importante destacar que en TLS 1.3 la clave pública del certificado no se utiliza para cifrar directamente toda la comunicación. Su función principal es autenticar al servidor. Posteriormente, mediante mecanismos de intercambio de claves como ECDHE, cliente y servidor generan de forma segura unas claves de sesión simétricas que serán las utilizadas para cifrar todo el tráfico.

De forma simplificada, el proceso es:

```
Cliente ------------------> Servidor
          ClientHello

Cliente <------------------ Servidor
          Certificado
          (incluye clave pública)
```

Cliente:
- Verifica el certificado
- Comprueba el dominio
- Comprueba la firma de la CA

Si todo es correcto:

✓ Confía en el servidor
✓ Continúa el handshake

```
Cliente <================> Servidor
      Comunicación cifrada
```

Por tanto, el instante clave en el que el cliente decide si puede confiar o no en el servidor ocurre justo después de recibir el certificado y antes de completar el establecimiento de la conexión TLS.