Wie funktioniert HTTPS?

Ein klitze kleiner Vortrag

über

Wie HTTPS funktioniert!

Wie funktioniert HTTPS?

HTTP ist das

HyperText Transport Protokoll

Wie funktioniert HTTPS?

HTTPS ist das

HyperText Transport Protokoll

eingeschlossen in einen Kryptotunnel.

Wie funktioniert HTTPS?
Der Ablauf

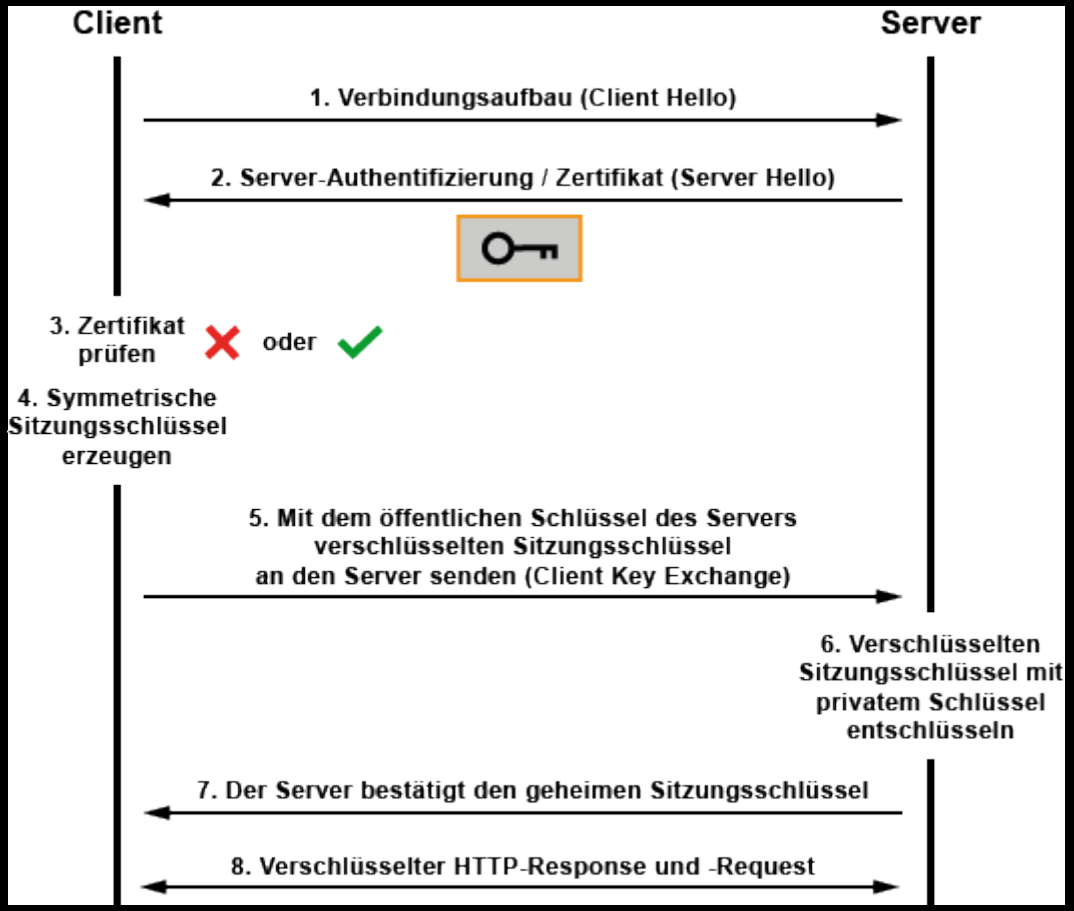
1. Der Browser/Client öffnet eine Verbindung zum Server
2. Der Server schickt seinen Public Key aka Zertifikat, welche Cipher und Protokolle er sprechen kann zum Clienten
3. Der Client prüft, ob der Server der ist, der vorzugeben er scheint *.

Wenn Nein => Abbruch → Userabfrage wie es weiter geht!

5. Client berechnet einen Symetrischen Sitzungsschlüssel (S-Key)
6. Client schickt den S-Key an den Server
7. Der Server bestätigt den S-Key
8. Die Datenübertragung kann anfangen.

*) Prüfung auf gültiges Zertifikat, signiert von einer CA, mit dem passenden Domainnamen

Wie funktioniert HTTPS?
Der Ablauf



Wie funktioniert HTTPS?
Basis

- Asymetrischer Schlüsselaustausch nach Diffi-Hellman

- Zertifikate werden in der Form X509 oder DER gespeichert.

- Das übliche Protokoll ist TLS 1.2 mit einem AES Cipher von 128++ Bits für den Session-Key.

Wie funktioniert HTTPS?
Basis

Gibt es noch andere Cipher / Verschlüsselungsalgorithmen als AES ?

Wie funktioniert HTTPS?
Basis

Gibt es noch andere Cipher /
Verschlüsselungsalgorithmen als AES ?

Ja, aber die sind unüblich
und meistens veraltet/unsicher.

Wie funktioniert HTTPS?

Wo kommt das Zertifikat her?

Das Zertifikat kann selbst erstellt werden, oder von einer Beglaubigungsstelle, einer Certificate Authority (CA), signiert werden.

Wie funktioniert HTTPS?

Wo kommt das Zertifikat her?

Der Ablauf:

1. einen privaten Schlüssel erstellen
2. einen Certificate Signing Request erstellen
3. den CSR selbst signieren, oder
an die CA schicken.

Aus beidem entsteht ein Zertifikat, daß zum Key paßt und Daten des CSR enthält, wie Domainname, Firmenname, Adresse usw.

Wo ist die nächste CA ?

CA's gibt es viele.

Einige wollen Geld für Ihren Dienst sehen, andere, wie Let's Encrypt, machen das kostenlos um HTTPS zu pushen.

Wie funktioniert HTTPS?
Wie ruft man das auf?

Im Browser in die Adresseleiste schreiben:

https://domainname.de

Wie funktioniert HTTPS?

So kann ein Zertifikat aussehen


```
-----BEGIN CERTIFICATE-----
MIIGDTCCBPWgAwIBAgISA+vuRwWL4+8YM6VB6cPUHZWJMA0GCSgGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MSMwIQYDVQQD
ExpMZXQncyBFbmNyeXB0IEF1dGhvcmI0eSBYMzAeFw0xODAxMTAyMjAxMjFaFw0x
ODA0MTAyMjAxMjFaMBcxFTATBgNVBAMTDGJlbmRlcmlyYy5kZTCCAiIwDQYJKoZI
hvcNAQEBBQADggIPADCCAgoCggIBAMXxFQ7FVLVkhiAJG42VwQvUl9Mh9ipaflgl
cH8sv/R+vMoY8vWtYxjdNVX9VAttJsnvHfLDqOsEHEZH4HPrkIuSuk7IM7vihu5g
HPPUafZ8OxUvhil3XHFaofCy++MHJiY79tb7w7kYaS6jIs84b6loUxWNODCf/SDN
Nph6IfQ0VGVlmuhtkTz07WDt9IJ/SVyc4M4dh4N6nlgTwo0ZUn0hosggzmLCdM05
gCSe8K4rpxgYm5HMjx8UfwfYEO7SXKsIzpOtssRsnkp46Dy2B4xuvkmI+4dzDhFO
xrEnK2Hg8+KrN/NSzaOuseIGX54ZfMUnOgayZrEVS4+mOi/ph8kby6Q5abTBKMYA
W2NPnh+vcxBNzZWyVGILttvCZ6qIJhznPdeN5OLTyJvTrcWr4bSOc6xq/NmZjNoy
05epOsG0epGOClhTBn+EtfSZNJNRlsWXnT0pH9estH2Y9/EjimBTCIt3Cmls0J3S
T9i3WkisgD7bsS4nkLuNQOSabB5VO1/m37ouI3I50xI4hMOQLaVxt14CSK1ex7OJ
WDewlST22CAkB+ZWCvCZpNG2tkqNAd3XUpTr0Hv1MiEnqL7t+3fggLeS/4zv6OcX
VDmOxOgz8grJB55CVP06MmWEEAxEfToQ/ElgFPog8DSKHUcNhdyVHGjd0ipABVAB
H2sHy9k3AgMBAAGjggIeMIICGjAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYI
KwYBBQUHAwEGCCsGAQUFBwMCMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFB75fDN4
/MdqdGkEfn4fBrXMxL/lMB8GA1UdIwQYMBaAFKhKamMEfd265tE5t6ZFZe/zqOyh
MG8GCCsGAQUFBwEBBGMwYTAuBggrBgEFBQcwAYYiaHR0cDovL29jc3AuaW50LXgz
LmxldHNlbmNyeXB0Lm9yZzAvBggrBgEFBQcwAoYjaHR0cDovL2N1cnQuaW50LXgz
LmxldHNlbmNyeXB0Lm9yZy8wKQYDVR0RBCIwIIIMYmVuZGVyaXJjLmRlghB3d3cu
YmVuZGVyaXJjLmRlMIH+BgNVHSAEgfYwgfMwCAYGZ4EMAQIBMIHmBgsrBgEEAYLf
EwEBATCB1jAmBggrBgEFBQcCARYaaHR0cDovL2Nwcy5sZXRzZW5jcnlwdC5vcmcw
gasGCCsGAQUFBwICMIGeDIGbVGhpcyBDZXJ0aWZpY2F0ZSBtYXkgb25seSBiZSBy
ZWxpZWQgdXBvbiBieSBSZWx5aW5hIFBhcnRpZXMgYW5kIG9ubHkgaW4gYWNjb3Jk
YW5jZSB3aXRoIHRoZSBDZXJ0aWZpY2F0ZSBQb2xpY3kgZm91bmQgYXQgaHR0cHM6
Ly9sZXRzZW5jcnlwdC5vcmcvcmVwb3NpdG9yeS8wDQYJKoZIhvcNAQELBQADggEB
AAAfdBD+wTefx2mHr1ATrzPWv6G9hwXhI8IWGcyTae4a5rjKsEEdYEhprHyOTrmZ
sG03OAE6MjF4vfwTSrjFD0so1g0X/oLA/ulbSHEMJ0tidG6XjliaWS3FHeSjgnx1
NOOKcxtRJ+zPfYnbKuZNjsrprSAWzcTHuxMFp/K5rWoMUVJJZfacn/vQvnUag5zX
A4tAs090ylLxi+KE76F3mGbLW/B1j9/z+kScowZ+goZXGugxYjYlhisK4UMNYduw
SlDJVQdAdJgvwoU2ZwjgD6jFFj2jgER9gjt+ENp9FcuqAEd9ou3mKq0hCfPLJDDe
FAjDJZBDOhR//4gpCAz4IFA=
-----END CERTIFICATE-----
```

Wie funktioniert HTTPS?

So kann ein Zertifikat aussehen

„Wie kann er nur ein echtes Zertifikat zeigen!?“

Wie funktioniert HTTPS?

So kann ein Zertifikat aussehen

Ist das grade durch Euren Kopf gegangen?

„Wie kann er nur ein echtes Zertifikat zeigen!?“

Wie funktioniert HTTPS?

So kann ein Zertifikat aussehen

Ist das grade durch Euren Kopf gegangen?

„Wie kann er nur ein echtes Zertifikat zeigen!?“

Wenn ja, müssen wir nochmal bei Adam und Eva anfangen! :D

Wie funktioniert HTTPS?
Setup Webserver

Apache Webserver Setup :

```
SSLEngine on
SSLInsecureRenegotiation off
SSLProtocol TLSv1.2
SSLHonorCipherOrder on
SSLCipherSuite
EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA384:EECDH+ECDSA
+SHA256:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:EECDH:EDH+aR
SA:HIGH:!MD5:!aNULL:!EDH:!RC4:!RC4
SSLCertificateKeyFile /etc/httpd/certs/benderirc.de.key
SSLCertificateFile /etc/httpd/certs/benderirc.de.crt
SSLCACertificateFile /etc/httpd/certs/benderirc.de.ca
```

Wie funktioniert HTTPS?

Kann man HTTPS erzwingen?

Ja, sollte man auch.

Hängt aber vom eingesetzten Server ab,
wie man das genau einstellt.

Wie funktioniert HTTPS?
Kann man HTTPS erzwingen?

Apache Beispiel:

```
RewriteCond %{SERVER_PORT}   !^443$
RewriteRule  (.*)  https://%{HTTP_HOST}/$1   [L]
```

Wie funktioniert HTTPS?
Was ist HSTS ?

HTTP Strict Transport Security – HSTS

ist ein Header, der bei der Übertragung vom Server zum Browser eingesetzt wird und im Prinzip sagt, daß der Browser immer gleich HTTPS benutzen soll, auch wenn HTTP eingegeben wird.

Das verhindert, daß jemand dem Benutzer eine unsichere Verbindung unterjubeln kann.

Wie funktioniert HTTPS?
Was ist HSTS ?

Funktioniert HSTS auch, wenn man die Seite zum allerersten mal aufruft ?

Wie funktioniert HTTPS?
Was ist HSTS ?

Funktioniert HSTS auch, wenn man die Seite zum allerersten mal aufruft ?

Nein.

Wie funktioniert HTTPS?
Was ist HSTS ?

Funktioniert HSTS auch, wenn man die Seite zum allerersten mal aufruft ?

Nein.

Das funktioniert nur, wenn man die Seite vorher schon mal besucht hatte.

Diverses

Kann man mit einem Zertifikat für einen Webserver auch etwas anderes machen ?

Diverses

Kann man mit einem Zertifikat für einen Webserver auch etwas anderes machen ?

Ja, seinen Mail-,FTP-,POP3- usw. -Server absichern. Das Zertifikat ist nicht an einen speziellen Dienst gekoppelt.

Wie funktioniert HTTPS?
Links

https://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure

https://tools.ietf.org/html/rfc2818 (May 2000)

https://www.softed.de/blog/wie-funktioniert-https/