

# 11. HTTPS

31 janvier 2024

## Développement web il3

### HTTPS

HE-Arc (DGR) 2022

### Sécuriser un site web

- Authentification du serveur
  - Assurer que le serveur est celui qu'il prétend être
- Intégrité des données
  - Assurer que les données reçues sont celles qui ont été envoyées
- Confidentialité des données
  - Eviter que des tiers ne puissent voir les données
- Authentification du client (optionnelle)
  - Assurer que le client est celui qu'il prétend être
- Pour un site web, ces services sont fournis par https
  - HTTPS : HTTP sécurisé par SSL/TLS, par défaut sur le port 443

## Secure Socket Layer → Transport Layer Security

- Conçu par Netscape (v2.0 en 1994, v3.0 en 1996)
- Brevet racheté par l'IETF : TLS v1.0 en 1999 (SSL 3.1), v1.3 en 2018
- Couche Application :
  - Entre les couches transport et application
  - Pas besoin de modifier la pile TCP/IP
- Possibilité de sécuriser d'autres protocoles :
  - HTTP, SMTP, SIP, ...
- Services offerts :
  - Authentification serveur + intégrité données
  - Confidentialité des données
  - Authentification optionnelle du client
- Certificats (clé publique associée au certificat)

## Rôle d'un certificat

- Garantir le lien entre une entité physique et une entité numérique :
  - Intégrité des données
  - Authentification
  - Confidentialité
- Document contenant une identité et une signature numérique
- Utilisations courantes : https, mails
- Délivré par une autorité de certification
- Certificats clients

## Autorité de Certification

- Tiers de confiance
  - enregistrée et certifiée par des autorités publiques ou de gouvernance de l'Internet
- Rôle :
  - Vérifier et garantir les informations sur l'entité
  - Emettre, délivrer et révoquer les certificats
  - Leur assigner une période de validité
  - Maintenir la liste des certificats valides/révoqués

- Certificats auto-signés :
  - usage interne
  - pas de tiers de confiance

## **Contenu d'un certificat X509**

- version de X.509 (v3, depuis 1996)
- numéro de série du certificat
- algorithme de chiffrement utilisé pour signer le certificat
- nom de l'AC émettrice
- informations sur la clé publique
- dates de début et fin de validité du certificat
- clé publique du propriétaire du certificat
- signature de l'émetteur du certificat (thumbprint)
- ...



## Déploiement

- Installer OpenSSL
- (Créer son autorité de certification si autosigné)
- Obtenir le certificat et la clé privée du serveur
- Configurer httpd. Pour Apache :
  - virtual host (port 443), ssl.conf, (ports.conf)
- Création de l'arborescence sécurisée
- Démarrage serveur
- OU BIEN utiliser Let's encrypt<sup>5</sup>
- OU BIEN utiliser un serveur pré-configuré comme Caddy<sup>6</sup>

## HTTPS Aujourd'hui

- Il n'y a plus de bonne raison d'utiliser HTTP
- TLS toujours utilisé avec HTTP2 et HTTP3
- HTTP2 et 3 minimisent et accélèrent les échanges
- Certificats gratuits
- Mise en place simplifiée

## Ressources

- Security Party 23.10.2009<sup>7</sup>
- SebSauvage<sup>8</sup>
- HTTPS en détails :
  - Diagramme de séquence HTTPS<sup>9</sup>
  - Diagramme de séquence SPDY<sup>10</sup>
  - SSL<sup>11</sup> en détails
- Durée de vie de la Clé Symétrique<sup>12</sup>
- Faux Certificat<sup>13</sup>
- Autorités de certification :

---

<sup>5</sup><https://letsencrypt.org/>

<sup>6</sup><https://caddyserver.com/>

<sup>7</sup><https://wiki.alphanet.ch/Ateliers/PresentationSecurityParty>

<sup>8</sup><http://www.sebsauvage.net/comprendre/ssl/>

<sup>9</sup><https://www.eventhelix.com/networking/SSL.pdf>

<sup>10</sup><https://www.eventhelix.com/networking/ssl-tls/https-ssl-tls-session-for-spdy.pdf>

<sup>11</sup><https://security.stackexchange.com/questions/20803/how-does-ssl-tls-work/20847#20847>

<sup>12</sup><https://security.stackexchange.com/questions/55454/how-long-does-an-https-symmetric-key-last>

<sup>13</sup><https://www.win.tue.nl/hashclash/rogue-ca/>

- Let's Encrypt<sup>14</sup>
- CA Cert<sup>15</sup>
- SSLforFree<sup>16</sup>
- Différences TLS / SSH : Snailbook<sup>17</sup>, StackExchange<sup>18</sup>

## Sources

---

<sup>14</sup><https://letsencrypt.org/>

<sup>15</sup><http://www.cacert.org/>

<sup>16</sup><https://www.sslforfree.com/>

<sup>17</sup><http://www.snailbook.com/faq/ssl.auto.html>

<sup>18</sup><http://security.stackexchange.com/questions/1599/what-is-the-difference-between-ssl-vs-ssh-which-is-more-secure>