Infrastructures à clés publiques

Public Key Infrastructure (PKI)

Romain Tartière <romain@opus-codium.fr>

31 octobre 2017

Romain Tartière

Infâme (Free)BSDiste (romain@)

Je casse des trucs

Expérience PKI :

- Grilles
- CPS
- HDS
- opus-codium/pakotoa
- Puppet

« C’est peut-être évident pour vous, mais ça ne l’est pas pour tout le monde »

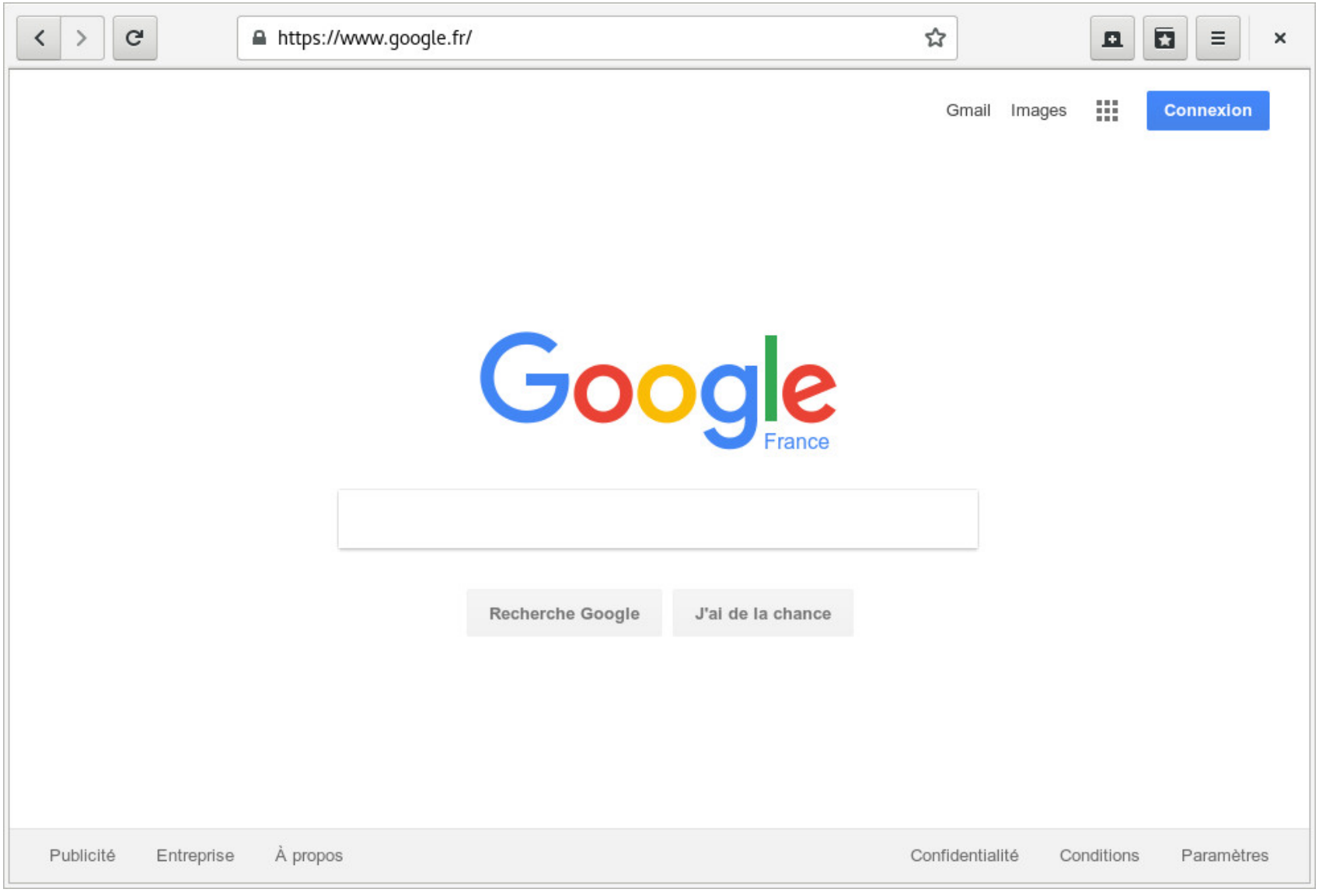
Photo : Ollivier Robert

Plan

1. Vocabulaire
2. Cryptographie
3. X.509
4. PGP
5. En vrac
6. Conclusion

N’attendez pas pour poser vos questions !

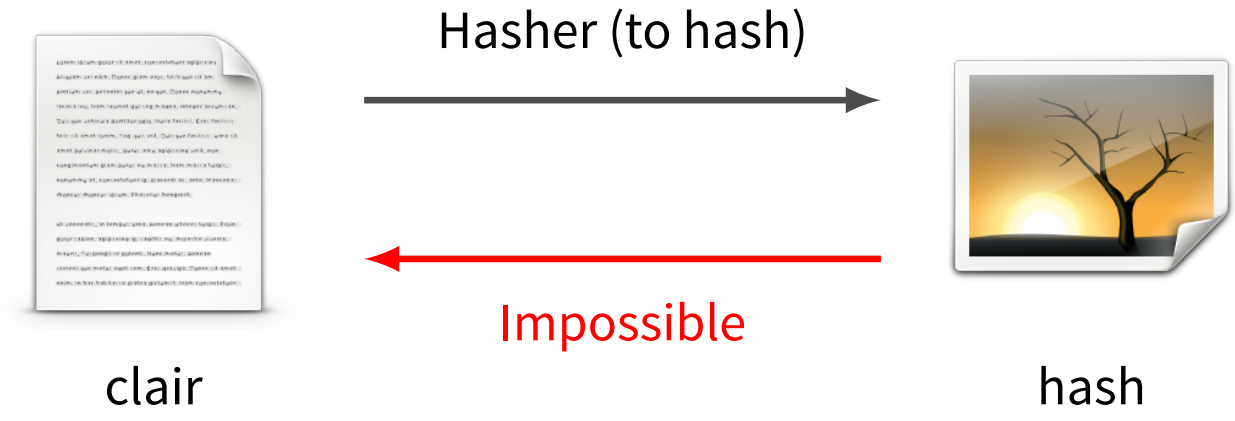
Ceci n’est pas une pipe



I

Vocabulaire

Hasher

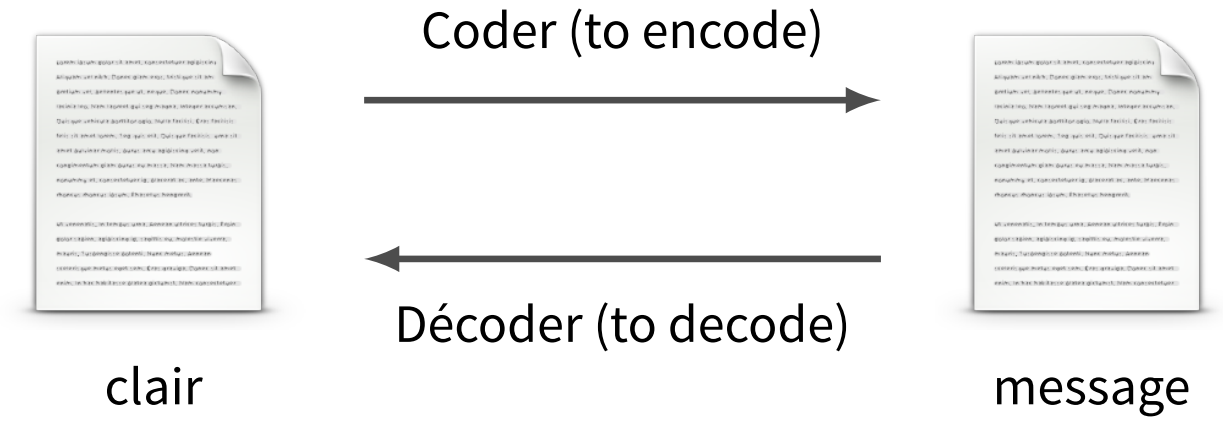


Hash / Empreinte / Condensat

Taille fixe (quelques octets)

Pas d’opération inverse

Coder

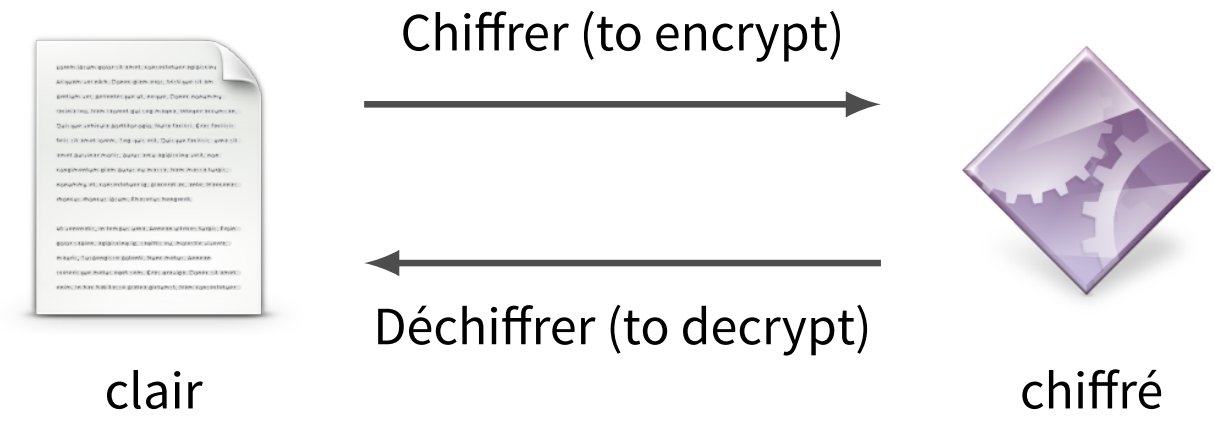


Défini une manière de stocker de l'information

Exemples : a=1, b=2, … ; a=0x61, b=0x62, …

Opération inverse : Décoder

Chiffrer



Utiliser un procédé cryptographique pour rendre la compréhension d'un document impossible sans clé

On obtiens un chiffré

Opération inverse : Déchiffrer

Chiffrage

C’est pour un devis

Cryptage, crypter, encrypter

II

Cryptographie

Pourquoi chiffre-t-on ?

1. Confidentialité
2. Authentification
3. Intégrité
4. Non répudiation

Types de chiffrements

On distingue deux types de chiffrements :

1. Chiffrement *symétrique*
   - Chiffrement à clés privées~~clés privées~~ / *secret partagé*
2. Chiffrement *asymétrique*
   - Chiffrement à *clés publiques*

Chiffrement symétrique

- La même clé sert à chiffrer et à déchiffrer

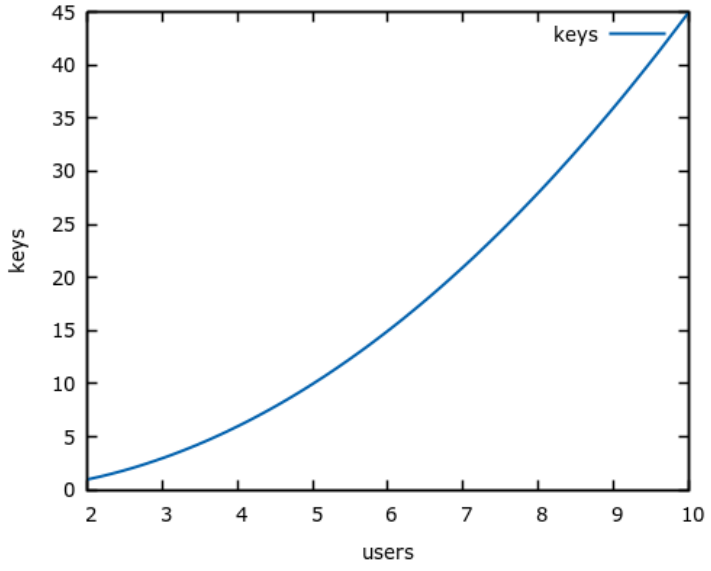
```
encrypt(clair, k)   #=> chiffré
decrypt(chiffré, k) #=> clair
```

- Avantages :
  - Simple à mettre en œuvre
  - Peu gourmand en ressources
- Inconvénients :
  - Difficulté de distribution de la clé
  - Une clé à gérer par destinataire
- Exemples :
  - DES, 3DES, **AES**, Blowfish…

Problème du partage de la clé secrète

- Risque d'interception
- Une clé par lien chiffré
  - Croissance du nombre de clés

$$\frac{n \times (n-1)}{2}$$



  - Destinataires multiples ?

Chiffrement asymétrique

- Deux clés distinctes :
  - Une clé privée
  - Une clé publique

```
encrypt(clair, k1)   #=> chiffré
decrypt(chiffré, k2) #=> clair
```

- Inconvénients :
  - Plus complexe à mettre en place
  - Plus consommateur de ressources
- Avantage :
  - Distribution de la clé publique facilitée
    - Elle est publique
    - Il faut vérifier que c'est la bonne
- Exemples :
  - DSA, **RSA**, ECDSA, EdDSA…

Usage du chiffrement asymétrique

Prérequis :

- Alice et Bob on chacun générés une paire de clés
- Ils ont échangé leurs clés publiques

Usage du chiffrement asymétrique

Signature d'un message

Alice chiffre le message avec sa clé privée

Tout le monde peut déchiffrer le message avec la clé publique d'Alice

Peu pratique : sans la clé publique d'Alice, on ne peut pas lire son message

Plutôt que chiffrer le message complet, Alice calcule l'empreinte du message (H) et chiffre celle-ci

Bob calcule l'empreinte du message reçu (H'), déchiffre l'empreinte d'Alice (H) et compare les deux

Les clés de Bob n'ont jamais été utilisées

Usage du chiffrement asymétrique

Chiffrement d’un message

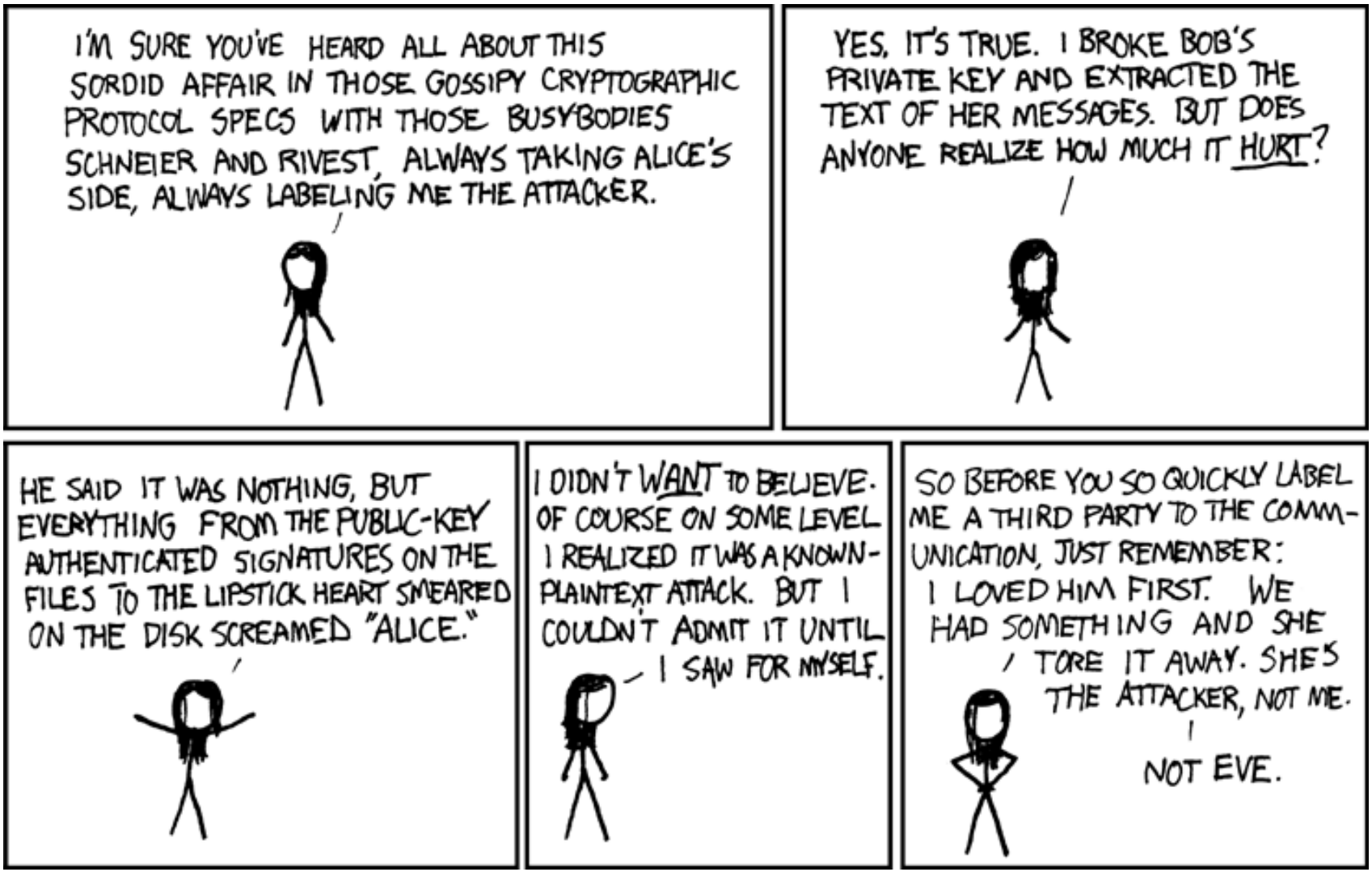
Alice chiffre le message avec la clé publique de Bob

Seul le possesseur de la clé privée de Bob peut déchiffrer le message

Les clés d’Alice n’ont jamais été utilisées

Usage du chiffrement asymétrique

Ève a pu se faire passer pour Alice



Yet one more reason I'm barred from speaking at crypto conferences.

xkcd 177 — Alice and Bob : Randall Munroe

Usage du chiffrement asymétrique

Signer et chiffrer ses messages

Dans la pratique, pour que des échanges soient sûrs :

- il faut signer **et** chiffrer les messages
- il faut être certain de l'identité du possesseur de la clé
- il faut protéger sa clé (passphrase)

Comment faire confiance à des gens qu'on ne connait pas ?

Concept de certificats électroniques

Une clé c'est :

- un nombre

Un certificat c'est :

- une clé (publique)
- des informations (identité)
- une signature

Infrastructure à clés publiques

Deux approches

- X.509
- PGP

III

X.509

Anatomie d’une clé RSA

```
% openssl genrsa -out KEY
Generating RSA private key, 2048 bit long modulus
.....................................+++
.+++
e is 65537 (0x10001)
```

Anatomie d'une clé RSA

```
% cat KEY
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAr1qwBc8sIIOqVpnfubgnQyEkØDEYM7NyRG2RG3Qkqfo5OLG7
DBNcQ4Ay9sIpy1CrQAQØQ7J8wSU1MwbNkhzJXj/RX/2+hp8ouPgFp+wjØqo3ZbvX
LRDMJ7kN8GexZmE45+kxKHBbowZ4/LCPD2in7jeUVØI89/C8oWPnEfbyqco7wGHw
lTEkKyURUlscqw4u3v2S4AjFhEN34e3q6ABHbA1SAd7psFk+vFzpYF1SYmgy2kwF
XQApk6+dmSvZdNVwUAsxCrN8dOWfRazr1vW2K+dYoAn+dYhtYØl43Sc522M4Cdq0
ttbØd9tY3CgoYQ4Ir/aJ5+VgDRoywlA1RkT2/QIDAQABAoIBAE+BHKHlpqovSEHv
jkJUPmjvVBOYztJSIBLqYopCBIWUz/DmlFoLRR/Ntk2vBugJ8TsbLN8sw+eGiTJT
eUØwBBTZdoLBN2suKnaC7X2PUUaoqmlT22GxZf7Øpl9DhGlY1ØY+smØVVFb8Dkrz
ekmQN+OIC5fsjlwUKFI8S34XqzpTmHOmRcB4RB+uer6mXx6YdYwx/C68n2eW8qrl
hYeXancUsOr+zk7avkØPI67CFHmd9YuDlJOy/bdN4Ooz3p7IØtjisW2cØU7ZgfmØ
U2IKBg7k7Ahx4hXt8ykDSPgnt4nØuClBlgØBv3RP3TSyt6HZViIENThzjqXsYt5E
/7y8LAECgYEA4cmgFir3U4HSwHLpv5fHBSf5xVgbQd1/u6OXJJMMqKbbHA+absGF
EhNJ+BoPXqMvNgYLOgiTN5OngWuJOyAohd/Dj6HgFw4gZ+hxP6TsvØlxt3qC+Py2
+WGFlzmDOK8ØsSouF8qcoDHPGxsrvgBXdYo+ØOIxLNrdRvsDXaAOWnØCgYEAxtF2
l/dQBUj+1A8273ptDXNV9Oonh5QIEizvIIJLmdIcAAQn1McndXZ9IV328UkZzoØm
CKkwMa7godIZBbpcKFWpdw2ezKKFLdM18U463UWC/iFS5Kp1zØVXTzcu5+FhScXl
/MR+u2Z3D1iaBihk5ntRaXqF366wJ5lCn9cvNoECgYAc6JrVm8SØ7W9VcqEZBc7W
iyrAqKo8waZkGOr2JNm/EjYFnr3QJnjqOowC9xs2q8AUs6tmT8jBmecde+5DIrft
```

Anatomie d’une clé RSA

```
hBve3QP7D7T4eNtfIbeqOjYUHtx8Eqc+wMzA8v0pGc2uTU8/fpKVNCtnNhBgsFyC
USP/zKYtLwyb1PG2YBLWZQKBgQCFAjTYzbdXEdKJg/Q4mirCyNpEkzIG3d3Yav8/
PGvfaFUbHayYCPQ4/SARZo+CNGlzabJ8MNPxKRFWsPvUfSySP1y0LQSD2mZGlfqM
iM2QoqRT529RU0ildbpHYJ+cuYcgl6iZRcuTC6Wz0o8wd22pU+7PJgzR7Egk9b9A
t/D6AQKBgGw/ZbFm8wqRhI0HBzBU8zsDX5NG7e026hZ1bUWhHeuHOoDvCSMPth/m
F58q+rWTX/ITo/Lyhf7HGioJG0aEnhuJZHJgtYaWTrgyMubN8s4UFQM1Gc3iW6El
Pmx7b1COsy8MP8cUDuMO7d+pmN21/9ec/NjDALKklGINudpQWu7h
-----END RSA PRIVATE KEY-----
```

Anatomie d’une clé RSA

Chiffrement asymétrique, donc partie publique **et** privée

```
% openssl rsa -in KEY -pubout
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr1qwBc8sII0qVpnfubgn
QyEk0DEYM7NyRG2RG3Qkqfo50LG7DBNcQ4Ay9sIpy1CrQAQ0Q7J8wSU1MwbNkhzJ
Xj/RX/2+hp8ouPgFp+wj0qo3ZbvXLRDMJ7kN8GexZmE45+kxKHBbowZ4/LCPD2in
7jeUV0I89/C8oWPnEfbyqco7wGHwlTEkKyURUlscqw4u3v2S4AjFhEN34e3q6ABH
bA1SAd7psFk+vFzpYF1SYmgy2kwFXQApk6+dmSvZdNVwUAsxCrN8d0WfRazr1vW2
K+dYoAn+dYhtY0l43Sc522M4Cdq0ttb0d9tY3CgoYQ4Ir/aJ5+VgDRoywlA1RkT2
/QIDAQAB
-----END PUBLIC KEY-----
```

Certificats X.509

Attributs :

- Version
- Serial
- **Subject**
- Issuer
- Public Key
- **Not Before**
- **Not After**
- Extensions
  - Key Usage
  - Subject Key Identifier

Le tout signé… par qui ?

Les attributs Subject et Issuer

Permet d'identifier un certificat

- Country (countryName, C)
- Organization (organizationName, O)
- Organizational Unit (organizationalUnitName, OU)
- State or Province Name (stateOrProvinceName, ST)
- Common Name (commonName, CN)
- …

Exemple :

- `/CN=example.com`
- `/C=FR/L=PARIS/O=DIRECTION GENERALE DES FINANCES PUBLIQUES/OU=0002 13000495500014/2.5.4.97=NTRFR-13000495500014/CN=www.impots.gouv.fr/serialNumber=S4706005`

Anatomie d’un certificat X.509

```
% openssl req -x509 -key KEY -subj /CN=example.com -out CERTIFICATE
```

```
% cat CERTIFICATE
-----BEGIN CERTIFICATE-----
MIIC/zCCAeegAwIBAgIJAM4FANszQweWMA0GCSqGSIb3DQEBCwUAMBYxFDASBgNV
BAMMC2V4YW1wbGUuY29tMB4XDTE3MTAzMTExMzEzNFoXDTE3MTEzMDExMzEzNFow
FjEUMBIGA1UEAwwLZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCvWrAFzywgg6pWmd+5uCdDISTQMRgzs3JEbZEbdCSp+jk4sbsME1xD
gDL2winLUKtABDRDsnzBJTUzBs2SHMleP9Ff/b6Gnyi4+AWn7CPSqjdlu9ctEMwn
uQ3wZ7FmYTjn6TEocFujBnj8sI8PaKfuN5RXQjz38LyhY+cR9vKpyjvAYfCVMSQr
JRFSWxyrDi7e/ZLgCMWEQ3fh7eroAEdsDVIB3umwWT68XOlgXVJiaDLaTAVdACmT
r52ZK9l01XBQCzEKs3x05Z9FrOvW9bYr51igCf51iG1jSXjdJznbYzgJ2o621vR3
21jcKChhDgiv9onn5WANGjLCUDVGRPb9AgMBAAGjUDBOMB0GA1UdDgQWBBQgg3k1
TLp/fdsAELoix3XfjywcSDAfBgNVHSMEGDAWgBQgg3k1TLp/fdsAELoix3Xfjywc
SDAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQB5BUB5/MhCDMBuFoMl
6YmbkOMiv+RhiiO6ma0og8kwNi30SlERp04uDDgiqqRuNUGWuY5KBfwWu9Lsgd2A
```

Anatomie d’un certificat X.509

```
o1znz7wGFURupqhLgSXjoHThU9v9DP2UA4IalbIqK5XOlkDMhØwv4KB7IcadZa8j
U7wØRhWaXq22ZhjiUVCHai78Un7aK2FiK2gTMzOHjyXLLi9tOtMnuIJ7SxsjQht7
jWNMYaoia8tnWt3COPeY8UMzKkZTVPQØNv9Jsf1r5ZgEzdmNn1DIzMSiEOApfTo+
F4V2jZ+srØph4HEWWNOVL+QxZAWH7Sidh4pAoxpP4C42PrlffcdR9bzyB2yYeYsB
meev
-----END CERTIFICATE-----
```

Anatomie d'un certificat X.509

```
% openssl x509 -text -noout -in CERTIFICATE
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            b0:34:09:01:23:48:b2:64
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=example.com
        Validity
            Not Before: Oct 31 11:26:42 2017 GMT
            Not After : Nov 30 11:26:42 2017 GMT
        Subject: CN=example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:5a:b0:05:cf:2c:20:83:aa:56:99:df:b9:b8:
                    27:43:21:24:d0:31:18:33:b3:72:44:6d:91:1b:74:
                    24:a9:fa:39:38:b1:bb:0c:13:5c:43:80:32:f6:c2:
                    29:cb:50:ab:40:04:34:43:b2:7c:c1:25:35:33:06:
```

Anatomie d’un certificat X.509

```
                cd:92:1c:c9:5e:3f:d1:5f:fd:be:86:9f:28:b8:f8:
                05:a7:ec:23:d2:aa:37:65:bb:d7:2d:10:cc:27:b9:
                0d:f0:67:b1:66:61:38:e7:e9:31:28:70:5b:a3:06:
                78:fc:b0:8f:0f:68:a7:ee:37:94:57:42:3c:f7:f0:
                bc:a1:63:e7:11:f6:f2:a9:ca:3b:c0:61:f0:95:31:
                24:2b:25:11:52:5b:1c:ab:0e:2e:de:fd:92:e0:08:
                31:0a:b3:7c:74:e5:9f:45:ac:eb:d6:f5:b6:2b:e7:
                58:a0:09:fe:75:88:6d:63:49:78:dd:27:39:db:63:
                38:09:da:8e:b6:d6:f4:77:db:58:dc:28:28:61:0e:
                08:af:f6:89:e7:e5:60:0d:1a:32:c2:50:35:46:44:
                f6:fd
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            20:83:79:35:4C:BA:7F:7D:DB:00:10:BA:22:C7:75:DF:
            8F:2C:1C:48
        X509v3 Authority Key Identifier:
            keyid:20:83:79:35:4C:BA:7F:7D:DB:00:10:BA:22:C7:
            75:DF:8F:2C:1C:48
```

Anatomie d’un certificat X.509

```
            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         91:18:86:f9:39:98:3b:15:ec:28:f1:38:58:26:79:c4:b9:df:
         50:25:12:7b:83:f1:2e:58:1f:c5:20:f2:aa:02:51:32:02:91:
         7d:3d:c6:8c:43:73:3e:4b:61:ea:c2:02:fa:49:b6:80:b1:78:
         e8:0f:4c:dc:39:27:2c:e4:30:67:da:23:04:ce:10:1f:56:58:
         48:5c:ab:b5:c5:32:77:44:22:9a:8e:6d:8d:6c:c7:cd:76:b7:
         c3:3c:f9:d1:b2:a7:e9:5a:25:dc:50:d9:0d:cc:0d:ad:d6:21:
         24:7e:31:8f:7d:0e:e0:1e:32:4d:48:06:df:34:8f:58:4d:d2:
         4f:59:e9:62:68:2f:5f:2e:08:07:4e:f8:6e:e7:f7:f5:2c:07:
         a0:3c:d8:b9:de:80:ed:b4:04:de:da:73:b8:de:d9:b2:48:a5:
         14:d4:7b:55:9a:32:b0:16:3c:46:b6:d3:4b:99:86:df:a5:c8:
         b5:11:6d:e5:b5:70:7d:18:b2:fb:1a:91:a1:14:aa:e3:2a:8b:
         95:e2:b1:e4:5e:39:c1:c2:84:99:ad:ba:e4:c2:74:48:86:4f:
         56:25:a2:6d:af:aa:20:cf:8a:dd:4c:29:b5:aa:6e:e4:1f:50:
         c9:33:68:09:7e:41:e6:e4:14:55:36:7d:b8:40:67:65:fb:0b:
         d1:c8:ea:3d
```

Vérification de la validité d’une signature

```
% openssl verify -CAfile CERTIFICATE CERTIFICATE
CERTIFICATE: OK
```

Certificat auto-signé

Issuer et Subject identiques

Tout le monde peut en fabriquer

Rejeté par défaut

Autorités de certification (CA)

Tiers de confiance

Rôles :

- Gèrent les demandes de certificats
- Vérifient les identités
- **Signent les certificats**
- Gèrent les révocations

Certificats des CA dans les navigateurs

Anatomie d’un Certificate Sign Request (CSR)

```
% openssl req -new -subj /CN=example.com -key KEY -out CSR
% cat CSR
-----BEGIN CERTIFICATE REQUEST-----
MIICWzCCAUMCAQAwFjEUMBIGA1UEAwwLZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCvWrAFzywgg6pWmd+5uCdDISTQMRgzs3JEbZEb
dCSp+jk4sbsME1xDgDL2winLUKtABDRDsnzBJTUzBs2SHMleP9Ff/b6Gnyi4+AWn
7CPSqjdlu9ctEMwnuQ3wZ7FmYTjn6TEocFujBnj8sI8PaKfuN5RXQjz38LyhY+cR
9vKpyjvAYfCVMSQrJRFSWxyrDi7e/ZLgCMWEQ3fh7eroAEdsDVIB3umwWT68XOlg
XVJiaDLaTAVdACmTr52ZK9l01XBQCzEKs3x05Z9FrOvW9bYr51igCf51iG1jSXjd
JznbYzgJ2o621vR321jcKChhDgiv9onn5WANGjLCUDVGRPb9AgMBAAGgADANBgkq
hkiG9w0BAQsFAAOCAQEAqU0fmzFkcUzzQDyn5yPJHQBY8ru+bPxHhLShoOXahdtu
s1h1pe/WWgkWk1pk/h5dpQD6O+4l/8cxDm8/pbzKKf/Wo79PTFywO9eDffg4S+qN
wzUzqI0B1BT4e8IUHVE5oAeNefHeCz7kx4+g4YBnh/7duRUpf8aCZ67wLScy9INB
xIe7QSDRGjuLRIVmVTGeYInxRtBLM3UGDjIX9d9+lAxPhg4XSInL9hx3qhvTjjy3
Q2b85t1aOEwVun6Fvsqk6ACaQb9K34GlhzttOB9kWdYwdmEazka4F7EVvVJrag7E
TSRtxREHr6nJmfX+nPArTbANHeitno46CIqKlPOihg==
-----END CERTIFICATE REQUEST-----
```

Anatomie d'un Certificate Sign Request (CSR)

```
% openssl req -in CSR -text -noout
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: CN=example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:5a:b0:05:cf:2c:20:83:aa:56:99:df:b9:b8:
                    27:43:21:24:d0:31:18:33:b3:72:44:6d:91:1b:74:
                    24:a9:fa:39:38:b1:bb:0c:13:5c:43:80:32:f6:c2:
                    29:cb:50:ab:40:04:34:43:b2:7c:c1:25:35:33:06:
                    cd:92:1c:c9:5e:3f:d1:5f:fd:be:86:9f:28:b8:f8:
                    05:a7:ec:23:d2:aa:37:65:bb:d7:2d:10:cc:27:b9:
                    0d:f0:67:b1:66:61:38:e7:e9:31:28:70:5b:a3:06:
                    78:fc:b0:8f:0f:68:a7:ee:37:94:57:42:3c:f7:f0:
                    bc:a1:63:e7:11:f6:f2:a9:ca:3b:c0:61:f0:95:31:
                    24:2b:25:11:52:5b:1c:ab:0e:2e:de:fd:92:e0:08:
                    c5:84:43:77:e1:ed:ea:e8:00:47:6c:0d:52:01:de:
```

Anatomie d’un Certificate Sign Request (CSR)

```
                    e9:b0:59:3e:bc:5c:e9:60:5d:52:62:68:32:da:4c:
                    05:5d:00:29:93:af:9d:99:2b:d9:74:d5:70:50:0b:
                    31:0a:b3:7c:74:e5:9f:45:ac:eb:d6:f5:b6:2b:e7:
                    58:a0:09:fe:75:88:6d:63:49:78:dd:27:39:db:63:
                    38:09:da:8e:b6:d6:f4:77:db:58:dc:28:28:61:0e:
                    08:af:f6:89:e7:e5:60:0d:1a:32:c2:50:35:46:44:
                    f6:fd
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         a9:4d:1f:9b:31:64:71:4c:f3:40:3c:a7:e7:23:c9:1d:00:58:
         f2:bb:be:6c:fc:47:84:b4:a1:a0:e5:da:85:db:6e:b3:58:75:
         a5:ef:d6:5a:09:16:93:5a:64:fe:1e:5d:a5:00:fa:3b:ee:25:
         ff:c7:31:0e:6f:3f:a5:bc:ca:29:ff:d6:a3:bf:4f:4c:5c:b0:
         3b:d7:83:7d:f8:38:4b:ea:8d:c3:35:33:a8:8d:01:d4:14:f8:
         7b:c2:14:1d:51:39:a0:07:8d:79:f1:de:0b:3e:e4:c7:8f:a0:
         e1:80:67:87:fe:dd:b9:15:29:7f:c6:82:67:ae:f0:2d:27:32:
         f4:83:41:c4:87:bb:41:20:d1:1a:3b:8b:44:85:66:55:31:9e:
         60:89:f1:46:d0:4b:33:75:06:0e:32:17:f5:df:7e:94:0c:4f:
```

Anatomie d’un Certificate Sign Request (CSR)

```
86:0e:17:48:89:cb:f6:1c:77:aa:1b:d3:8e:3c:b7:43:66:fc:
e6:dd:5a:38:4c:15:ba:7e:85:be:ca:a4:e8:00:9a:41:bf:4a:
df:81:a5:87:3b:6d:38:1f:64:59:d6:30:76:61:1a:ce:46:b8:
17:b1:15:bd:52:6b:6a:0e:c4:4d:24:6d:c5:11:07:af:a9:c9:
99:f5:fe:9c:f0:2b:4d:b0:0d:1d:e8:ad:9e:8e:3a:08:8a:8a:
94:f3:a2:86
```

Un CSR peut être vu comme un mini certificat auto-signé

Émission d’un certificat par une CA

- CSR envoyé à une CA
- La CA vérifie que c’est OK (signature, CN)
- La CA créé un certificat avec les infos du CSR :
  - Une partie copiée
  - Une partie générée
- La CA signe le certificat avec sa clé privée

La CA peut modifier la demande

Émission d'un certificat par une CA

```
req #=> #<OpenSSL::X509::Request>

cert = OpenSSL::X509::Certificate.new

cert.version    = 2
cert.serial     = self.next_serial!
cert.issuer     = self.certificate.subject
cert.not_before = Time.now
cert.not_after  = Time.now + 1.year

cert.subject    = req.subject
cert.public_key = req.public_key

cert.sign(self.key, OpenSSL::Digest::SHA256.new)
```

Révocation de certificats

Certificate Revocation List (CRL)

Mécanisme nécessaire en cas de compromission / décommissionnement

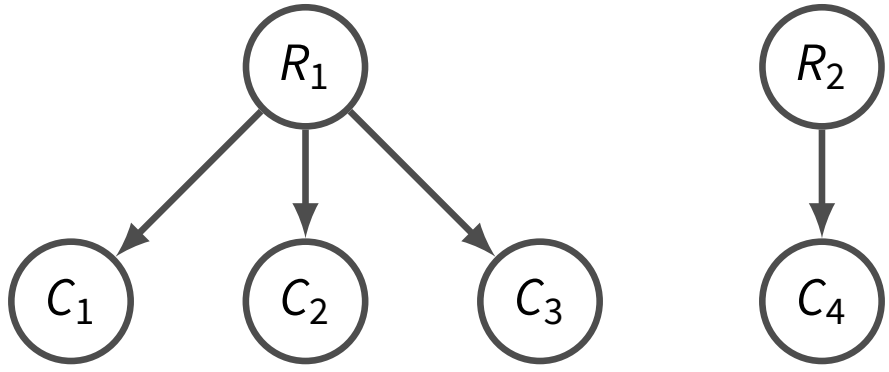
- On informe la CA
- La CA ajoute le certificat a sa liste de certificats révoqués
- Cette liste est signée par la CA

Habituellement c'est la même clé qui signe les certificats et les CRL

Quand-est-ce que le navigateur l'actualise ?

Synthèse X.509

Centralisation de la confiance auprès des CA



IV

PGP

Historique

PGP 1.0 le 5 juin 1991

Philip Zimmermann

GNU Privacy Guard (aka GnuPG aka GPG)

Photo : Philip Zimmermann

Création d'une clé PGP

```
% gpg --gen-key
```

- Créé la paire de clés de l'utilisateur
- Créé un « certificat » avec la clé publique et l'identité de l'utilisateur (clé publique)
- Signe la clé publique avec la clé privée

C'est grosso-modo un certificat X.509 auto-signé

Signature d'une clé PGP

Une clé PGP peut avoir *plusieurs signatures*

- Alice fourni à Bob l'empreinte de sa clé publique
- Bob vérifie que l'empreinte correspond
- Bob signe la clé publique avec sa clé privée
- Bob envoie à Alice sa clé publique signée

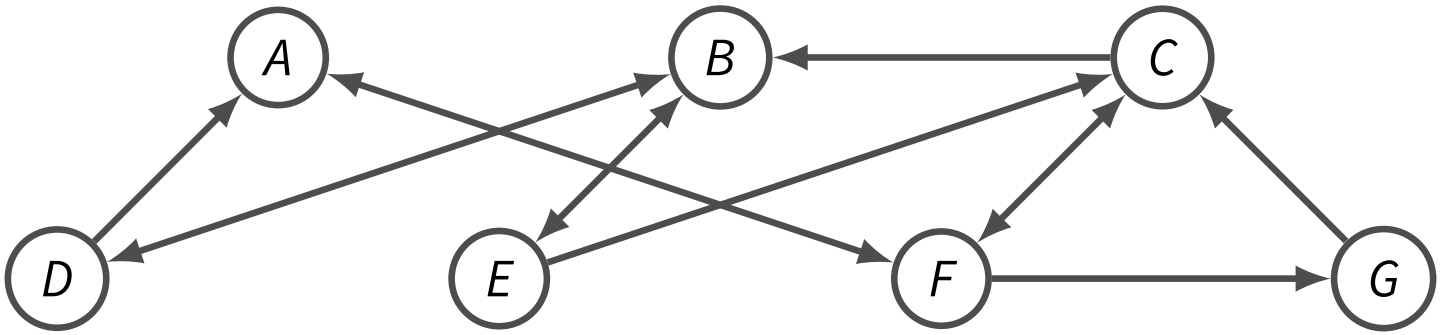
- Alice importe sa clé dans son trousseau
- La clé existe déjà, seule la nouvelle signature est ajoutée

Bob peut aussi publier la clé d'Alice sur Internet… mais c'est mal vu

Réseau de confiance

Les signatures sont publiques : on sait qui à signé la clé de qui (donc qui fait confiance à qui)

« Les amis de mes amis sont mes amis »



On est en moyenne à 5.5 clés d'un autre utilisateur de PGP

Synthèse X.509 vs. PGP

X.509	**PGP**
Certificat créé par la CA	Certificat créé par l'utilisateur
1 seule signature : celle de la CA	Plusieurs signatures
Chiffre le tuyau (TLS/SSL)	Chiffre les messages
Confiance centralisée	Confiance distribuée
Forêt d'arbres de confiance	*Graph orienté* de confiance

V

En vrac

Connexion SSL/TLS (exemple : HTTPS)

1. Le serveur
   - Envoie son certificat au client
2. Le client
   - Reçoit un certificat
   - Vérifie sa validité (domaine, date, émetteur, révocation)
   - Génère une clé de chiffrement symétrique (secret partagée)
   - Chiffre le secret partagée avec la clé publique du serveur
   - Envoie la clé chiffrée au serveur (`ClientKeyExchange`)
3. Le serveur
   - Reçoit la clé partagée chiffrée générée par le client
   - Déchiffre la clé partagée avec sa clé privée

La suite de la communication est chiffrée symétriquement

Connexion SSL/TLS (exemple : HTTPS)

Remarques :

- Le client a authentifié le serveur, mais le serveur n'a aucune information sur le client
- Les paramètres de chiffrements sont négociés et « jetables »

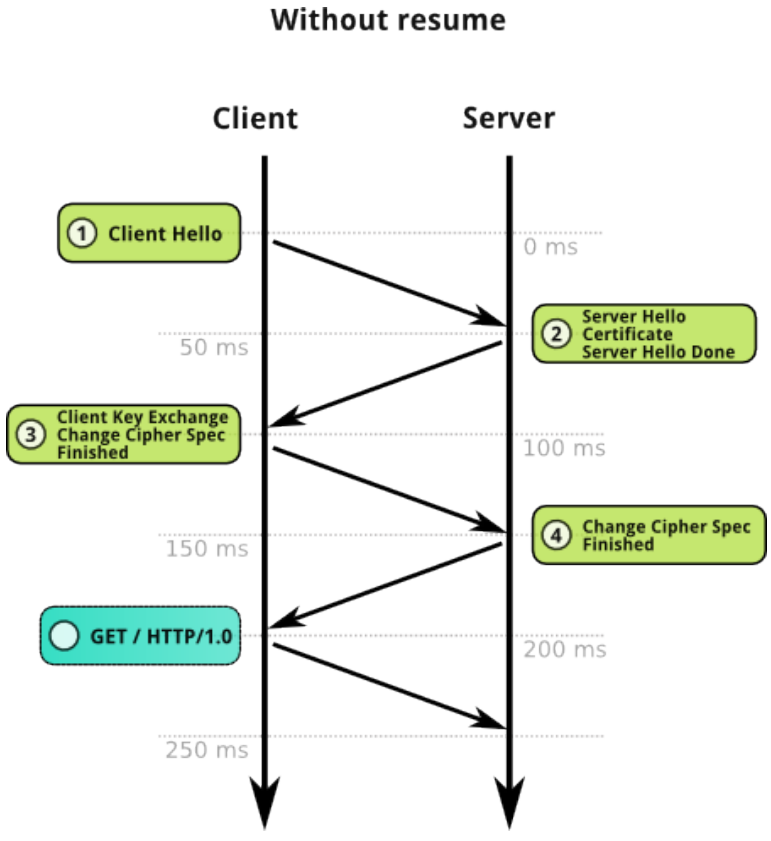


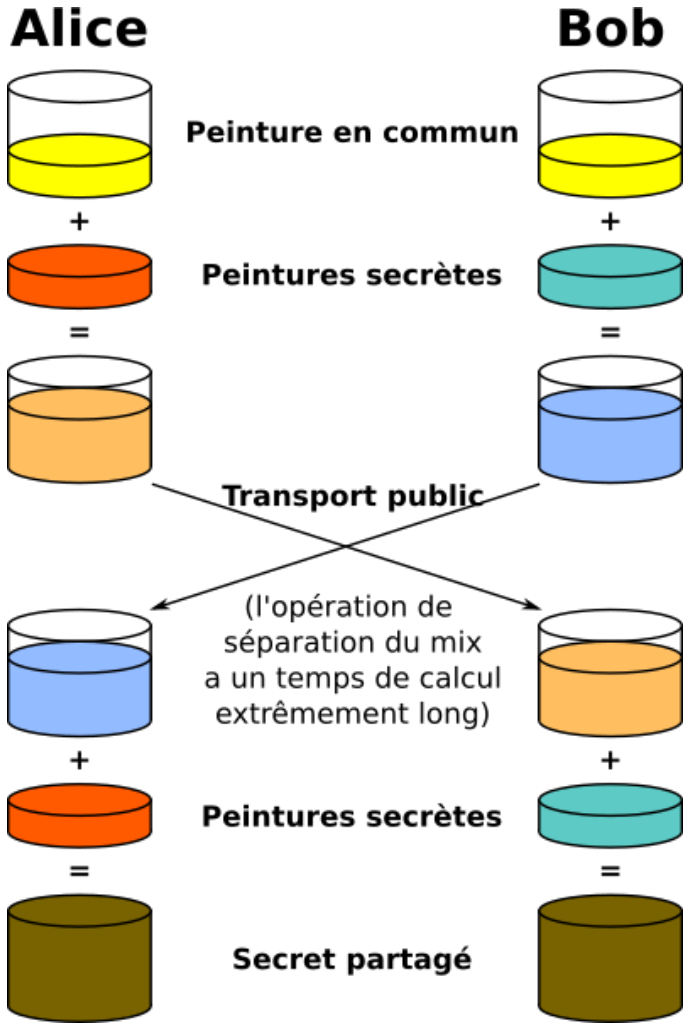
Image : Vincent Bernat

Perfect Forward Secrecy (PFS)

En français : *confidentialité persistante*

Si la clé privée du serveur est compromise, qu'en est-il des transactions passées ?

La PFS introduit un `ServerKeyExchange`



Infographie : A.J. Han Vinck, Flugaal, Dereckson

Chiffrer pour plusieurs destinataires

On ne veut pas envoyer *n* messages distincts, ni un message chiffré avec *n* clés différentes

1. On chiffre le message avec un algorithme symétrique et une clé aléatoire
2. On chiffre cette clé *n* fois pour les *n* destinataires
3. On envoie le message chiffré symétriquement et la clé partagée chiffrée pour chaque destinataire

Chaque destinataire peut déchiffrer la clé partagée avec sa clé privée et déchiffrer le message

Chaînes de certification

Que se passe-t-il si la clé privée d’une CA est compromise ?

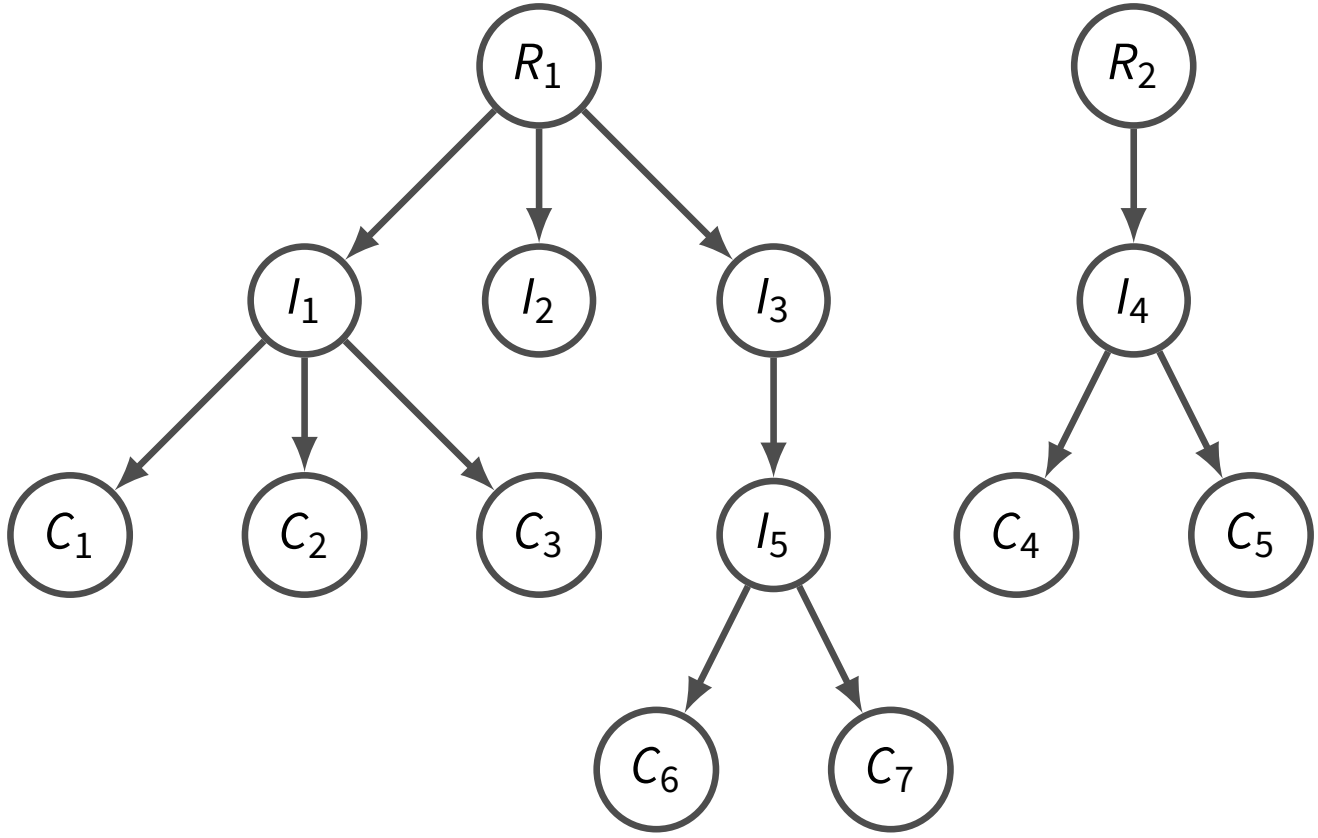
Chaînes de certification

Un certificat est rarement signé par une CA racine

La CA racine créé plusieurs CA intermédiaires

Les CA intermédiaires signent les certificats des clients

Chaînes de certification



Le serveur droit fournir la chaîne de certification en plus de son certificat

Online Certificate Status Protocol (OCSP)

Protocole d'interogation de la validité d'un certificat

But : palier à la faiblesse de mise à jour des CRL par les clients

Certificats clients

Un client peut présenter un certificat au serveur

Le serveur vérifie si le certificat est signé par une CA de confiance

Le serveur peut utiliser ces informations pour authentifier l'utilisateur

Le certificat peut être stocké dans un périphérique (e.g. Yubikey), une carte à puce (e.g. CPS), …

Certification Authority Authorization (CAA)

Une CA peut vérifier si elle est autorisée à émettre un certificat pour un domaine via le DNS (enregistrement CAA)

Devenu obligatoire le 8 septembre 2017

Le 9 septembre 2017, Comodo s'est fait pincer pour ne pas le respecter : Comodo Caught Breaking New CAA Standard One Day After It Went Into Effect

Validation par les CA

DNS-Based Authentication of Named Entities (DANE)

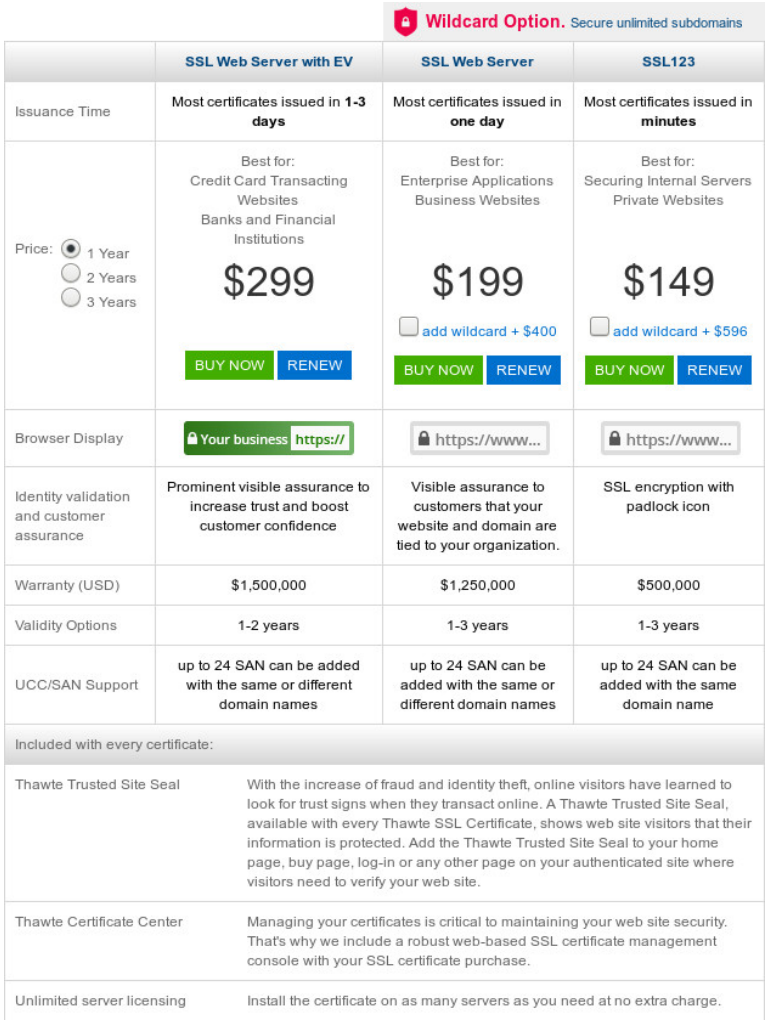
Publication du certificat dans un enregistrement `TLSA` du DNS, protégé par DNSSEC

Validation par les clients

On peut se passer des CA

Types de certificats : DV, OV et EV

- Domain Validation (DV)
  - $ 149
- Oraganization Validation (OV)
  - $ 199
- Extended Validation (EV)
  - $ 299



Wildcard Option. Secure unlimited subdomains

	SSL Web Server with EV	SSL Web Server	SSL123
Issuance Time	Most certificates issued in **1-3 days**	Most certificates issued in **one day**	Most certificates issued in **minutes**
Price: 1 Year / 2 Years / 3 Years	Best for: Credit Card Transacting Websites, Banks and Financial Institutions $299 BUY NOW RENEW	Best for: Enterprise Applications, Business Websites $199 add wildcard + $400 BUY NOW RENEW	Best for: Securing Internal Servers, Private Websites $149 add wildcard + $596 BUY NOW RENEW
Browser Display	Your business https://	https://www...	https://www...
Identity validation and customer assurance	Prominent visible assurance to increase trust and boost customer confidence	Visible assurance to customers that your website and domain are tied to your organization.	SSL encryption with padlock icon
Warranty (USD)	$1,500,000	$1,250,000	$500,000
Validity Options	1-2 years	1-3 years	1-3 years
UCC/SAN Support	up to 24 SAN can be added with the same or different domain names	up to 24 SAN can be added with the same or different domain names	up to 24 SAN can be added with the same domain name

Included with every certificate:

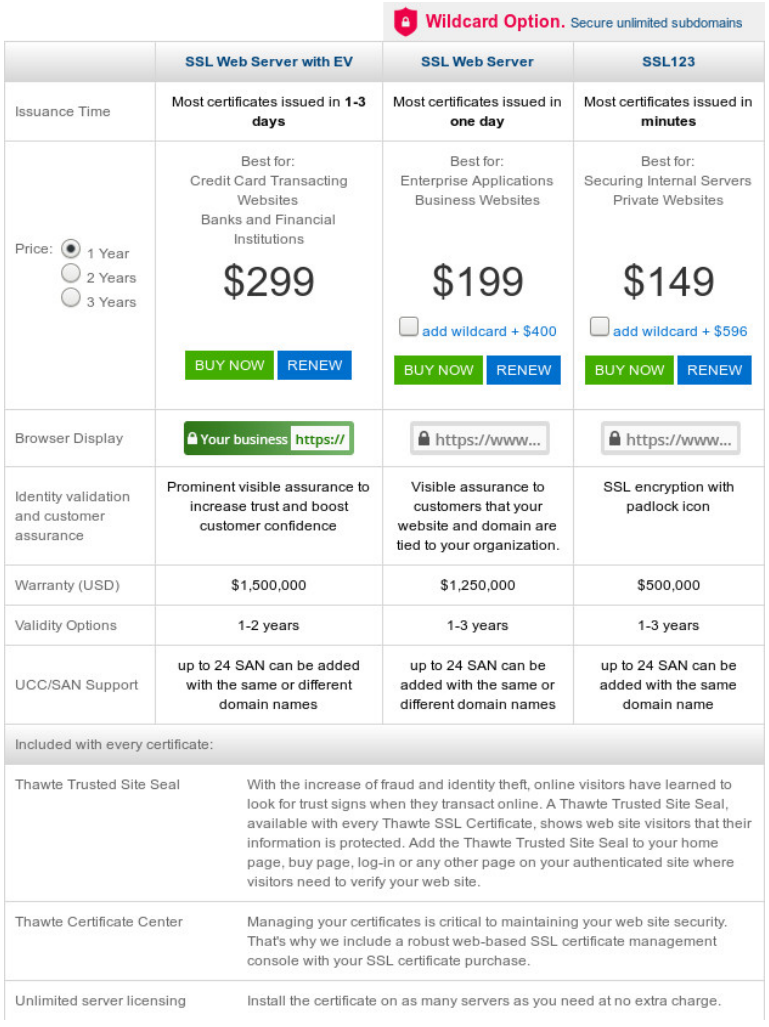
Thawte Trusted Site Seal	With the increase of fraud and identity theft, online visitors have learned to look for trust signs when they transact online. A Thawte Trusted Site Seal, available with every Thawte SSL Certificate, shows web site visitors that their information is protected. Add the Thawte Trusted Site Seal to your home page, buy page, log-in or any other page on your authenticated site where visitors need to verify your web site.
Thawte Certificate Center	Managing your certificates is critical to maintaining your web site security. That's why we include a robust web-based SSL certificate management console with your SSL certificate purchase.
Unlimited server licensing	Install the certificate on as many servers as you need at no extra charge.

Source : https://www.thawte.com/ssl/

Certificats wildcard

Valide pour un ensemble de noms de domaines :

- `/CN=*.example.com`
  - + $ 596 (DV)
  - + $ 400 (OV)



Wildcard Option. Secure unlimited subdomains

	SSL Web Server with EV	SSL Web Server	SSL123
Issuance Time	Most certificates issued in **1-3 days**	Most certificates issued in **one day**	Most certificates issued in **minutes**
Price: 1 Year / 2 Years / 3 Years	Best for: Credit Card Transacting Websites, Banks and Financial Institutions $299 BUY NOW RENEW	Best for: Enterprise Applications, Business Websites $199 add wildcard + $400 BUY NOW RENEW	Best for: Securing Internal Servers, Private Websites $149 add wildcard + $596 BUY NOW RENEW
Browser Display	Your business https://	https://www...	https://www...
Identity validation and customer assurance	Prominent visible assurance to increase trust and boost customer confidence	Visible assurance to customers that your website and domain are tied to your organization.	SSL encryption with padlock icon
Warranty (USD)	$1,500,000	$1,250,000	$500,000
Validity Options	1-2 years	1-3 years	1-3 years
UCC/SAN Support	up to 24 SAN can be added with the same or different domain names	up to 24 SAN can be added with the same or different domain names	up to 24 SAN can be added with the same domain name

Included with every certificate:

Thawte Trusted Site Seal	With the increase of fraud and identity theft, online visitors have learned to look for trust signs when they transact online. A Thawte Trusted Site Seal, available with every Thawte SSL Certificate, shows web site visitors that their information is protected. Add the Thawte Trusted Site Seal to your home page, buy page, log-in or any other page on your authenticated site where visitors need to verify your web site.
Thawte Certificate Center	Managing your certificates is critical to maintaining your web site security. That's why we include a robust web-based SSL certificate management console with your SSL certificate purchase.
Unlimited server licensing	Install the certificate on as many servers as you need at no extra charge.

Source : https://www.thawte.com/ssl/

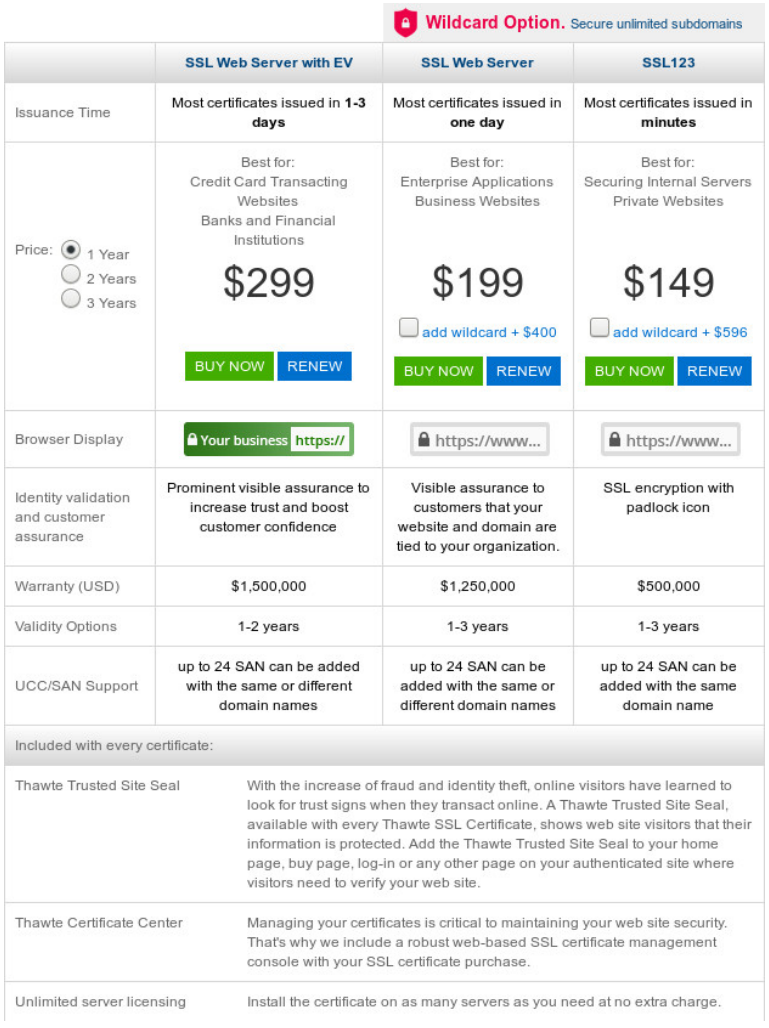
Subject Alternative Name (SAN)

Extension X.509

Permet à un certificat d'être valide pour plusieurs noms de domaines distincts :

- `example.com`
- `www.example.com`
- `example.net`
- `*.example.net`

Nécessite un navigateur qui supporte le *Server Name Indication* (SNI)



Wildcard Option. Secure unlimited subdomains

	SSL Web Server with EV	SSL Web Server	SSL123
Issuance Time	Most certificates issued in **1-3 days**	Most certificates issued in **one day**	Most certificates issued in **minutes**
Price: 1 Year / 2 Years / 3 Years	Best for: Credit Card Transacting Websites, Banks and Financial Institutions $299 BUY NOW RENEW	Best for: Enterprise Applications, Business Websites $199 add wildcard + $400 BUY NOW RENEW	Best for: Securing Internal Servers, Private Websites $149 add wildcard + $596 BUY NOW RENEW
Browser Display	Your business https://	https://www...	https://www...
Identity validation and customer assurance	Prominent visible assurance to increase trust and boost customer confidence	Visible assurance to customers that your website and domain are tied to your organization.	SSL encryption with padlock icon
Warranty (USD)	$1,500,000	$1,250,000	$500,000
Validity Options	1-2 years	1-3 years	1-3 years
UCC/SAN Support	up to 24 SAN can be added with the same or different domain names	up to 24 SAN can be added with the same or different domain names	up to 24 SAN can be added with the same domain name

Included with every certificate:

Thawte Trusted Site Seal	With the increase of fraud and identity theft, online visitors have learned to look for trust signs when they transact online. A Thawte Trusted Site Seal, available with every Thawte SSL Certificate, shows web site visitors that their information is protected. Add the Thawte Trusted Site Seal to your home page, buy page, log-in or any other page on your authenticated site where visitors need to verify your web site.
Thawte Certificate Center	Managing your certificates is critical to maintaining your web site security. That's why we include a robust web-based SSL certificate management console with your SSL certificate purchase.
Unlimited server licensing	Install the certificate on as many servers as you need at no extra charge.

Source : https://www.thawte.com/ssl/

Let’s Encrypt / CAcert

	Let’s Encrypt	**CAcert**
Lancement	2015	2002-2004 (?)
Réseau de confiance		✔
Dans les navigateurs	✔	
Certificats wildcard		✔
Subject Alternative Name	✔	✔
Validité des certificats	3 mois	2 ans
Coût	0 €	0 €

Extensions des fichiers

Nombreuses extensions : `.pem`, `.key`, `.crt`, `.cer`, `.cert`, `.csr`, `.crl`, `.der`

PEM	DER
Privacy Enhancement Mail	Distinguished Encoding Rules
Texte	Binaire
Concaténables	Non concaténables

Mon usage :

- Clé : `common_name.key`
- Certificat : `common_name.crt`

OpenSSL

156 vulnérabilités au cours des 12 dernières années

https://www.openssl.org/news/vulnerabilities.html

Website security : Use OpenSSL.

> OpenSSL has a horrible track record for security ; but it has the saving grace that because it is so widely used, vendors tend to be very good at making sure that OpenSSL vulnerabilities get fixed promptly. I wish there was a better alternative, but for now at least OpenSSL is the best option available.

Source : http://www.daemonology.net/blog/2009-06-11-cryptographic-right-answers.html

OpenSSL

- Supporte des architectures jamais inventées (e.g. i386 / amd64 big-endian)
- À une API particulièrement pénible à utiliser
- La documentation de la commande `openssl(1)` est dans `genrsa(1)`, `x509(1)`

Patch `mod_ssl` Apache de l'ASIP Santé

- Les certificats X.509 des CPS des médecins sont signés par une CA
- Les CRL sont signées par une CA distincte
- Ces deux CA ont le même Subject

L'ASIP Santé fourni des patch pour Apache 2.1.17 et 2.2.26 (uniquement) :

- ne sont pas publics
- ne semblent pas à jour (On en est à 2.4.29)
- ne sont pas triviaux (800 lignes environ)
- causent des memory leaks

Un contournement simple reste possible (patch de 2 lignes)

Temps qu'on cause de l'ASIP Santé

18 Dec 2014	un commit dans OpenSSL rends ~40% des cartes CPS inopérantes
20 Mar 2015	Découverte du problème. Développement de sante-link/test-cps-certificate (un outil de test)
28 Mar 2015	Échanges avec l'auteur du commit, contact de l'ASIP Santé
31 Mar 2015	L'ASIP nous réponds : le problème est connu, leur plan a deux axes : - Côté serveur, fournir un patch pour OpenSSL - Coté client, modifier leur bibliothèque pour modifier le certificat à la volée En attendant, ils nous demandent d'être discret…

Error 502

Ray ID: 3b5dd26334a50920 • 2017-10-30 10:51:52 UTC

Bad gateway

You	Paris	[redacted]
Browser	Cloudflare	Host
Working	Working	Error

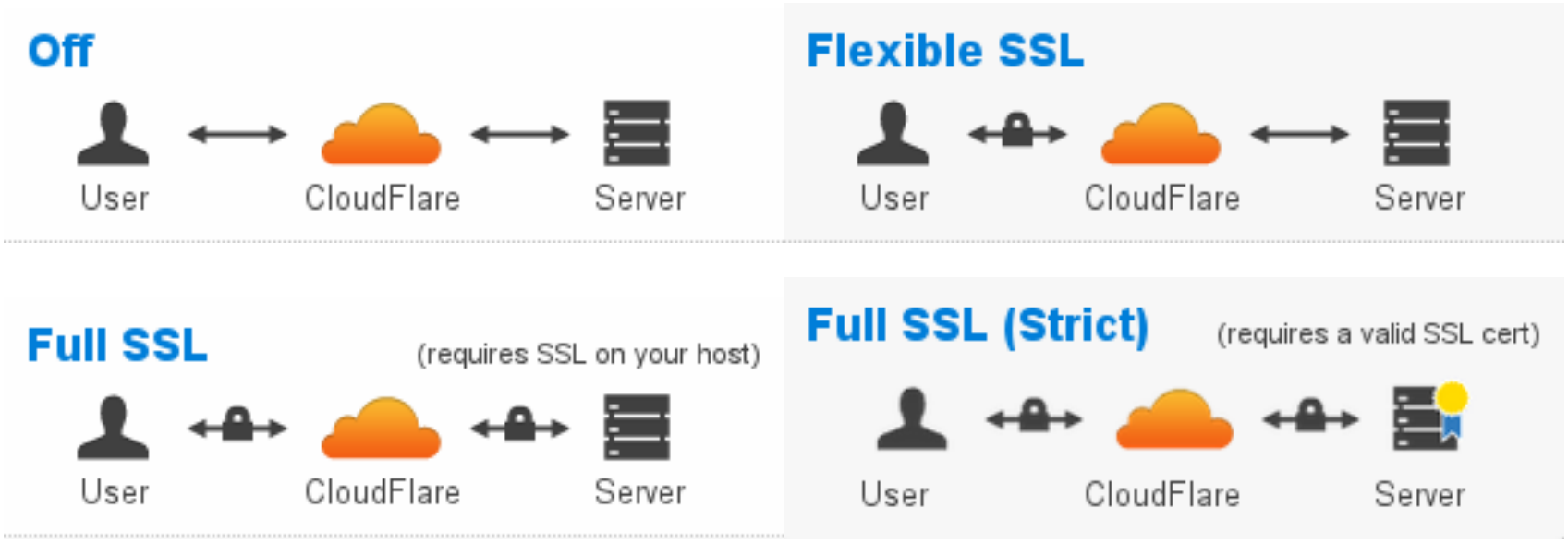
What happened?

The web server reported a bad gateway error.

What can I do?

Please try again in a few minutes.

Au delà des Content Delivery Networks (CDN) ?



Images : https://support.cloudflare.com/hc/en-us/articles/200170416

Un CDN est généralement un *reverse proxy*, donc il est en position de *Man In The Middle* (MITM)

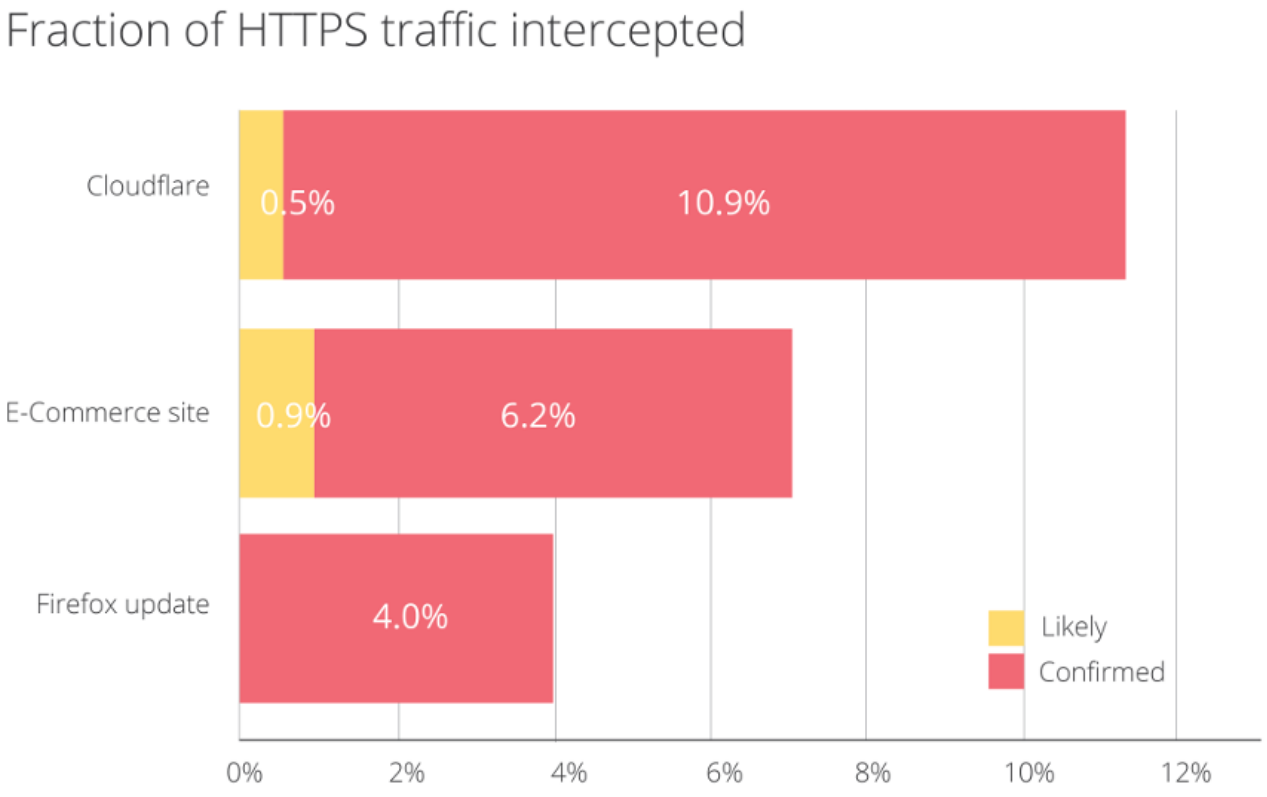
- Peut altérer le contenu qu'il fait transiter
- Peut collecter des informations sur le visiteur

Interception

Les connexions passent par un proxy qui intercepte le trafic

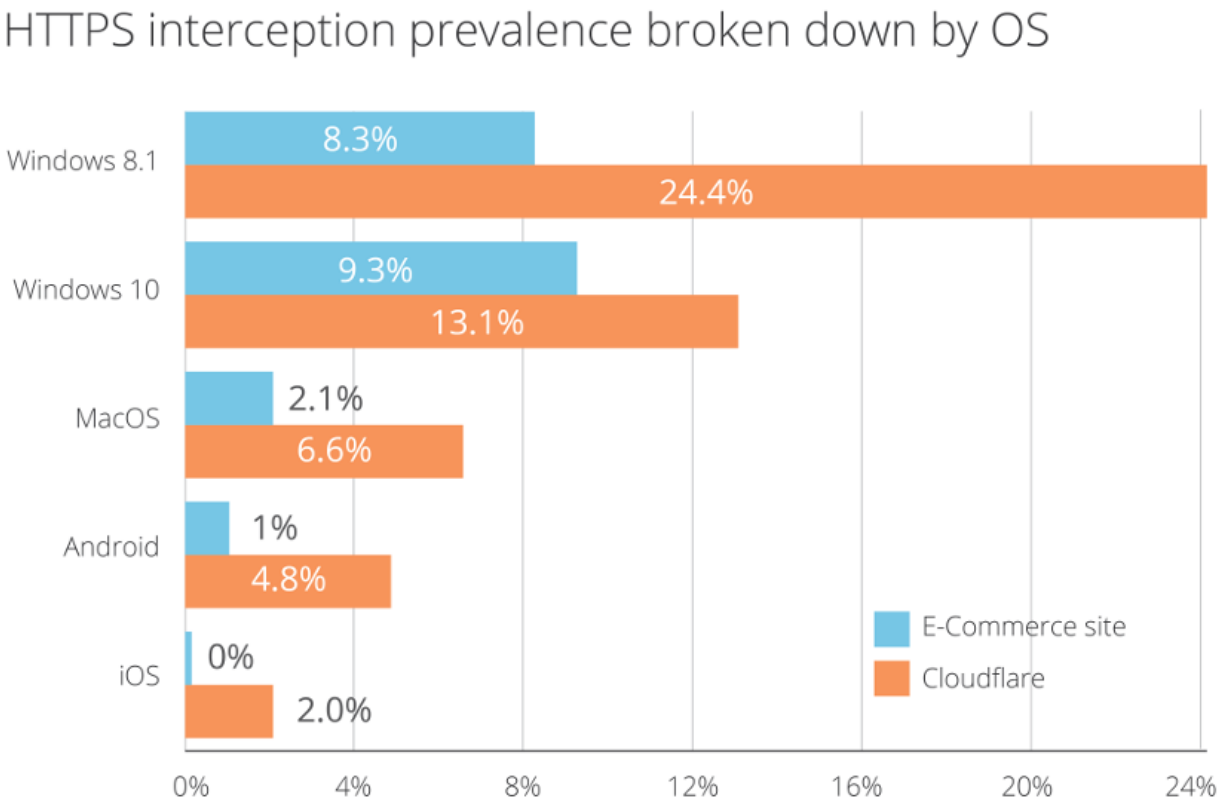
- Bonjour l'antivirus
- Les sysadmins peuvent ajoutent une CA de confiance et un proxy (risk management)

Interception



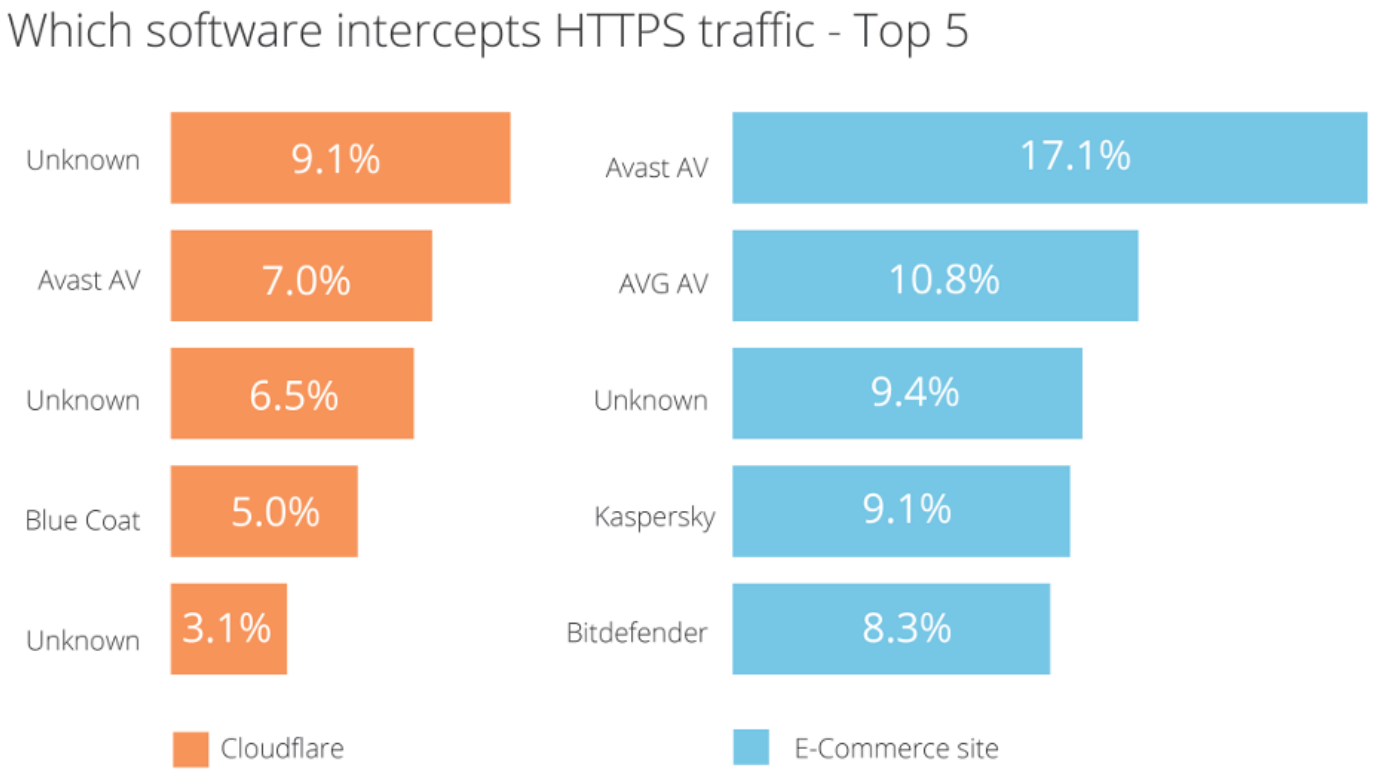
Source : https://blog.cloudflare.com/understanding-the-prevalence-of-web-traffic-interception/

Interception



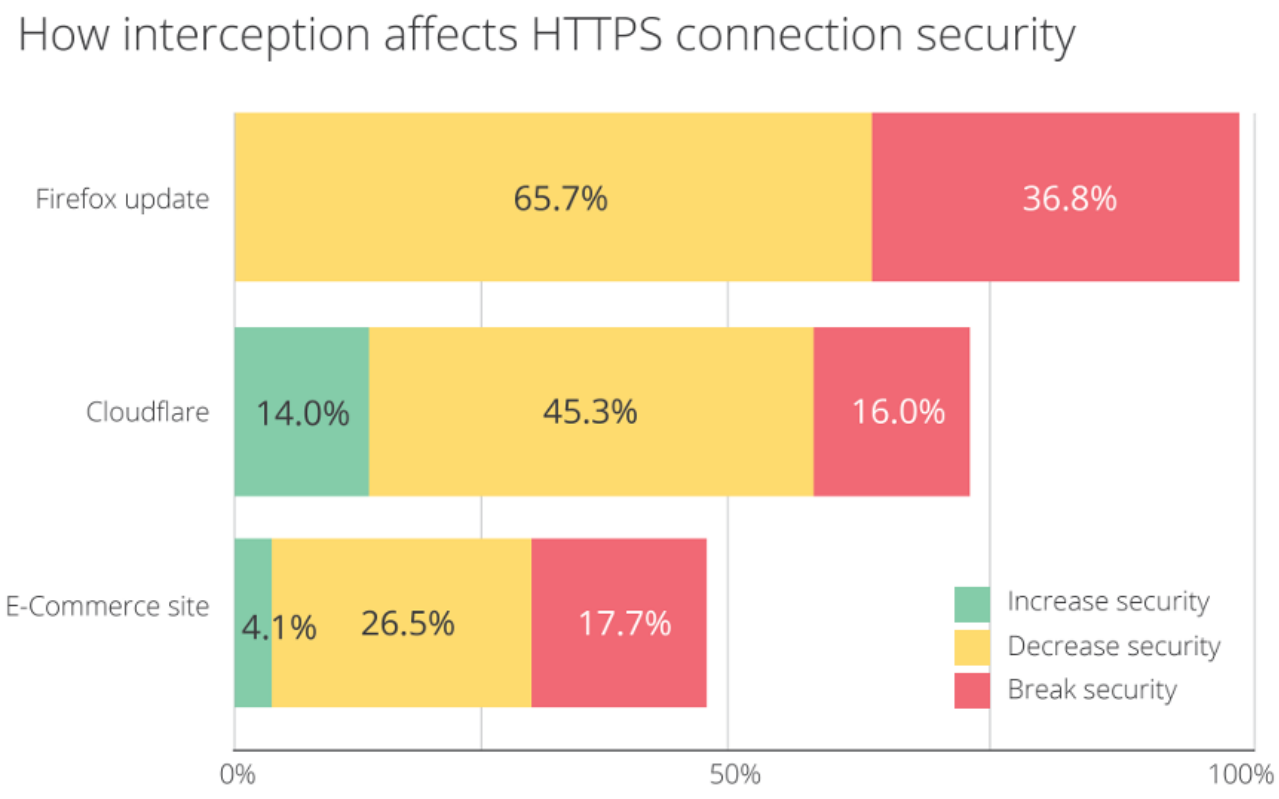
Source : https://blog.cloudflare.com/understanding-the-prevalence-of-web-traffic-interception/

Interception



Source : https://blog.cloudflare.com/understanding-the-prevalence-of-web-traffic-interception/

Interception



Source : https://blog.cloudflare.com/understanding-the-prevalence-of-web-traffic-interception/

Publicité, Trackers et ressources distantes

https://ivg.gouv.fr/ : 71 ressources

- 28 JavaScript
  - 16 facebook.com
  - 12 gouv.fr
- 13 CSS
  - 9 gouv.fr
  - 2 facebook.com
  - 1 cloudflare.com
  - 1 googleapis.com
- 12 Images
  - 11 gouv.fr
  - 1 facebook.com
- 3 HTML
  - 2 facebook.com
  - 1 gouv.fr
- 15 Médias
  - 15 facebook.com

L’avenir du World Wide Web

2014-10-28 *HTML5*, W3C
https://www.w3.org/TR/html5/

2015-02-15 *Web Security - “HTTPS Everywhere” harmful*, Tim Berners-Lee
https://www.w3.org/DesignIssues/Security-NotTheS.html

2015-04-30 *Deprecating Non-Secure HTTP*, Mozilla
https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/

2017-09-18 *An open letter to the W3C Director, CEO, team and membership*, EFF
https://www.eff.org/deeplinks/2017/09/open-letter-w3c-director-ceo-team-and-membership

VI

Conclusion

Quelques liens

Cryptographic Right Answers

http://www.daemonology.net/blog/2009-06-11-cryptographic-right-answers.html

Recommandations de sécurité relatives à TLS

https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls/

SSL Server Test

https://www.ssllabs.com/ssltest/

Version script shell

https://testssl.sh/

Plus complet

https://observatory.mozilla.org/