Autorité de Certification et Certificats SSL

Sami Taktak

sami.taktak@cnam.fr

Centre d'Étude et De Recherche en Informatique et Communications
Conservatoire National des Arts et Métiers

juin 2014

le cnam

Confidentialité

- Chiffrement symétrique :
  - clé de chiffrement connue des 2 parties
  - clé utilisée pour chiffrer et déchiffrer
- Chiffrement asymétrique :
  - Chaque partie possède une clé privée et une clé publique
  - La clé privée doit rester secrète
  - La clé publique doit être connue
  - Un message est chiffrer avec la clé publique du destinataire
  - Un message est déchiffrer avec la clé privée du destinataire

$\Rightarrow$ Seul le destinataire peut décoder le message

Authentification

- Utilise le chiffrement asymétrique
- L'émetteur chiffre un message avec sa clé privé
- Toute personne possédant la clé publique de l'émetteur peut déchiffrer le message
- Si le message déchiffrer correspond au message initial alors l'émetteur est authentifier

Comment être sur que l'émetteur est bien celui qu'il prétend être ?

- Chaîne de confiance (*Web of Trust*)
- Autorité de certification (CA : *Certificate Authority*)

Certificats

- Clé publique
- Information spécifiques au certificat
- Signature par une CA

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 12103226332656409189 (0xa7f74c3952239a65)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, ST=IdF, L=Paris, O=NFA083, OU=CA, CN=localhost
        Validity
            Not Before: Jun 12 14:19:55 2014 GMT
            Not After : Jul 12 14:19:55 2014 GMT
        Subject: C=FR, ST=IdF, L=Paris, O=NFA083, OU=TP, CN=localhost
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:ae:8d:ac:57:76:14:5b:c3:23:17:dd:c4:be:57:
                    c1:da:07:45:c5:aa:1f:64:c9:38:82:5f:23:6f:6f:
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
         52:91:2e:a4:70:19:e8:8f:8d:db:5d:e4:5b:fd:79:82:12:31:
         af:f1:80:a1:86:ed:10:25:0d:e1:4b:df:ba:97:b5:4a:b8:6d:
```

Autorité de Certification (CA)

- Doit être de confiance
- Signe les demandes de certificats
- Possède aussi une clé privée et un certificat
- Possibilité de certificat autosigné

OpenSSL

- Implémentation des protocoles SSL et TLS
- Fournit les protocoles de chiffrement et authentification
- Permet de créer des clés publiques/privées, des certificats
- Permet de créer sa propre autorité de certification
- Possède un module Apache

Activation du module `ssl` d'Apache :

```
a2enmod ssl
```

Création d'un Certificat

- Génération d'une clé privé :

```
openssl genrsa 1024 > serveur.key
```

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC9FNacrVW8vwmvJWCyHEhpBzcoszCW
vMe4j8P27EW3ZHaTJLMCQQDo/cH6EQUS2z5GZlVFdtZS
bUwmbp4ByihybVwHhoipF6GnVJvfSgRSo16nHBezpNud
-----END RSA PRIVATE KEY-----
```

Création d'un Certificat

- Création de la demande de signature du certificat associé :

```
openssl req -new -key serveur.key > serveur.csr
```

```
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:IdF
Locality Name (eg, city) []:Paris
Organization Name (eg, company) []:NFA083
Organizational Unit Name (eg, section) []:TP
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Création d'un Certificat

- Envoie de la demande à une CA
- Signature du certificat par la CA

```
openssl x509 -req -in serveur.csr -out serveur.crt

Signature ok
subject=/C=FR/ST=IdF/L=Paris/O=NFA083/OU=TP/CN=localhost
Getting CA Private Key
Enter pass phrase for ca.key:
```

Configuration d'un Serveur Virtuel Sécurisé

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
ServerAdmin webmaster@localhost

DocumentRoot /var/www
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
<Directory /var/www/>
Options Indexes FollowSymLinks MultiViews
AllowOverride None
Order allow,deny
allow from all
</Directory>

#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

SSLCertificateFile    /etc/ssl/certs/ssl-cert.crt
SSLCertificateKeyFile /etc/ssl/private/ssl-cert.key
</VirtualHost>
</IfModule>
```

Certificat non vérifiable

This Connection is Untrusted

You have asked Iceweasel to connect securely to **127.0.0.1:2443**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

Technical Details

127.0.0.1:2443 uses an invalid security certificate.

The certificate is not trusted because no issuer chain was provided.
The certificate is only valid for localhost

(Error code: sec_error_unknown_issuer)

I Understand the Risks

Certificat non valide

This Connection is Untrusted

You have asked Iceweasel to connect securely to **127.0.0.1:2443**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

Technical Details

127.0.0.1:2443 uses an invalid security certificate.

The certificate is only valid for localhost

(Error code: ssl_error_bad_cert_domain)

I Understand the Risks