# Connexion sécurisée HTTPs et répondeur OCSP

Ludovic Fontaine
Département Réseaux et Télécommunications, IUT de Blois
Blois, France
ludovic.fontaine@univ-tours.fr

## RESUME

Dans cet article, je décrirai les bases de la cryptographie afin de comprendre le contenu et le fonctionnement d'un certificat numérique signé par une autorité de certification et intégré dans un serveur web. La finalité résidera dans la mise en place d'un répondeur OCSP associé à l'autorité de certification permettant au client navigateur de vérifier la validité du certificat qu'il a reçu du serveur, et assurant la confiance que le client aura à utiliser le certificat.

## Mots clés

Chiffrement symétrique ; chiffrement asymétrique ; hachage ; signature ; autorité de certification ; certificat numérique ; HTTPs ; répondeur OCSP.

## 1. INTRODUCTION

Bien souvent, les enseignants spécialisés en réseaux informatiques connaissent et enseignent les principes du chiffrement et des certificats, utilisent OpenSSL pour générer les clés et certificats, bien souvent auto-signés, intègrent le certificat dans un serveur web Apache, mais mettent très rarement en œuvre la vérification de la validité du certificat. Cet article s'adresse à la fois, à un lecteur débutant désireux de connaitre les bases du chiffrement assurant la confidentialité et l'authenticité d'une transmission d'informations, un lecteur averti désireux de connaitre le contenu, l'utilité et le fonctionnement d'un certificat numérique, et un lecteur expérimenté désireux de comprendre comment le client vérifie la véracité du certificat envoyé par le serveur. Ainsi, les enseignants non spécialisés dans le domaine des réseaux informatiques pourront découvrir le fonctionnement d'une transmission sécurisée via le protocole HTTPs, et les enseignants spécialisés finaliseront la transmission HTTPs avec la vérification de la validité du certificat via le protocole OCSP. Il va de soi qu'en fonction de la réceptivité et des compétences des étudiants de DUT ou de LP, l'enseignant adaptera le degré d'avancement dans cette mise en œuvre.

L'article final contiendra les parties suivantes : dans un premier temps, l'architecture de travail sera détaillée permettant ensuite de mettre en œuvre les diverses fonctionnalités de cette article. Dans une seconde partie, les bases de la cryptographie seront énoncées avec la confidentialité assurée par les chiffrements symétriques et asymétriques, l'intégrité par le hachage, et l'authentification par la signature, ces 2 dernières fonctionnalités assurant l'authenticité. Dans une troisième partie, le certificat numérique et le rôle de l'autorité de certification seront détaillés, le protocole TLS sera introduit permettant la mise en œuvre d'une connexion sécurisée HTTPs. Enfin, la dernière partie introduira le protocole OCSP permettant de vérifier la validité du certificat numérique détenu par le serveur web auprès de son autorité de certification munie d'un répondeur OCSP. Enfin, une conclusion viendra synthétiser l'essentiel des notions et fonctionnalités étudiées.

Dans ce résumé, on se limitera à énumérer les prérequis, les fonctionnalités théoriques étudiées, le matériel à disposition, et les fonctionnalités pratiques mises en oeuvre. Tous les détails de la découverte à la mise en pratique seront décrits dans l'article final. Le diagramme de transfert HTTPs est ici mis en évidence et sera davantage explicité dans l'article final.

## 2. ENVIRONNEMENT DE TRAVAIL

Dans cette partie, l'architecture du réseau, les fonctionnalités et les services prérequis seront présentés afin de préparer le lecteur à la mise en œuvre de la transmission sécurisée HTTPs et la vérification de la véracité du certificat auprès du répondeur OCSP.

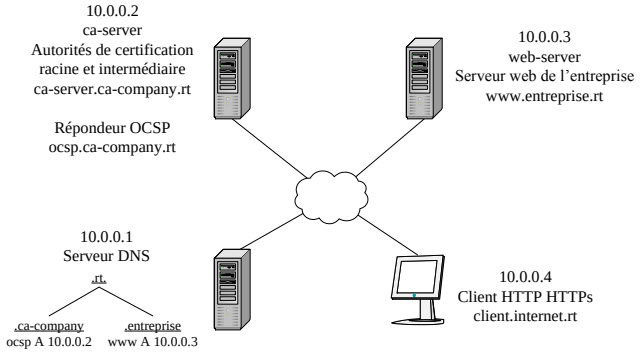


**Figure 1. Infrastructure réseau**

L'architecture réseau (Fig. 1) comporte un serveur DNS résolvant les noms ocsp.ca-company.rt et www.entreprise.rt, une autorité de certification racine/intermédiaire et son répondeur OCSP, un serveur web d'une entreprise et un client sur Internet. Tous les équipements sont clients du serveur DNS.

OpenSSL est un logiciel open source qui permet de générer des clés, créer des certificats, signer des certificats, chiffrer/déchiffrer de données, mettre en place un répondeur OCSP,… Il est installé sur ca-server et sur web-server.

Apache est un logiciel open source de serveur web. Il est installé sur web-server.

L'installation et la configuration du serveur DNS ne seront pas abordées dans cet article.

## 3. BASES DE LA CRYPTOGRAPHIE

Dans cette partie, les bases de la cryptographie seront énoncées afin que tout lecteur comprenne le principe d'un chiffrement symétrique à clé secrète et d'un chiffrement asymétrique à clés privée et publique, ainsi que leurs avantages et inconvénients. La vérification des données transférées par hachage, l'authentification par signature et l'authenticité par signature de l'empreinte seront ensuite explicitées.

Des schémas comme celui de la figure 2 – très connus du lecteur averti, mais inconnus du lecteur néophyte – illustreront ces principes.

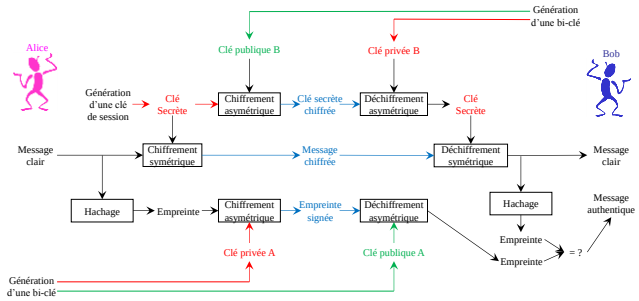


**Figure 2. Transfert confidentiel avec authenticité**

# 4. CERTIFICAT NUMERIQUE

Dans cette partie, je commencerai par décrire l'utilité d'une autorité racine de certification, d'une autorité intermédiaire de certification et du contenu du certificat numérique. La couche de sécurité TLS sera ensuite décrite afin de faire le lien entre les protocoles de service en clair et leur version sécurisée (HTTP et HTTPs seront pris en exemple).

OpenSSL permettra la mise en œuvre complète du certificat qui sera intégré au serveur web Apache. Les fichiers de configuration et les commandes OpenSSL seront décrites afin de mettre en place les autorités de certifications racine et intermédiaire avec leurs certificats racines et intermédiaires, ainsi que la demande de certificat du serveur web qui sera signée par l'autorité de certification, dont un extrait est présenté figure 3.

```
root@ca-server#openssl ca -config intermediate/openssl-inter.cnf \
  -extensions server_cert -days 365 -notext -md sha256 \
  -in intermediate/csr/www.entreprise.rt.csr.pem \
  -out intermediate/newcerts/www.entreprise.rt.cert.pem
```

**Figure 3. Signature du certificat par l'autorité de certification**

L'intégration du certificat dans Apache sera ensuite décrite afin que le lecteur puisse mettre en œuvre une connexion sécurisée HTTPs. Un extrait est présenté figure 4.

```
<VirtualHost *:443>
  ServerName www.entreprise.rt
  SSLEngine On
  SSLCertificateFile /etc/apache2/ssl/www.entreprise.rt.cert.pem
  SSLCertificateKeyFile /etc/apache2/ssl/www.entreprise.rt.key.pem
</VirtualHost>
```

**Figure 4. Extraits du fichier de configuration d'Apache**

# 5. REPONDEUR OCSP

Dans cette dernière partie, après avoir énoncé le rôle d'un répondeur OCSP (Online Certificate Status Protocol), je décrirai la mise en place de ce répondeur, ainsi que le lien entre le certificat numérique et le répondeur OCSP permettant au client navigateur de vérifier la validité du certificat auprès de l'autorité de certification en lien avec son répondeur OCSP.

Le répondeur OCSP basique sera mise en œuvre par OpenSSL.

L'analyse des trames résultantes de l'interrogation du serveur web par un client navigateur via HTTPs permettra d'établir le diagramme de la figure 5, les différentes étapes suivantes seront mises en évidence et explicitées avec davantage de détails :

- Le client établit une connexion TCP sur le port 443 du serveur web dont il vient de récupérer l'adresse IP après interrogation du serveur DNS.
- CLIENT-HELLO cipher suites : le client envoie au serveur sa liste d'algorithmes de chiffrement et de hachage.
- SERVER-HELLO cipher suite : parmi les algorithmes envoyés par le client, le serveur choisit le meilleur algorithme de chiffrement et de hachage en commun, et l'envoie au client.
- CERTIFICATE : le serveur envoie au client son certificat contenant, entre autres, la clé publique et l'URI du répondeur OCSP.
- Le client ayant obtenu dans le certificat l'URI du répondeur OCSP, il s'y connecte alors après avoir obtenu l'adresse IP auprès de son serveur DNS.
- OCSP request : le client envoie au répondeur OCSP une requête concernant le certificat à vérifier.
- OCSP response : le répondeur envoie au client le statut du certificat (Good, Revoked, Unknown).
- Après vérification de la signature de la réponse, le client sait que le certificat est valide (Good), que le hachage de la clé publique du certificat est identique entre le serveur web et le répondeur OCSP et qu'il peut donc faire confiance au certificat.
- SERVER-KEY-EXCHANGE / SERVER-KEY-EXCHANGE SESSION-TICKET : en utilisant la clé publique du certificat, le client entame ensuite un échange avec le serveur web pour s'échanger la clé de session.
- TLSv1.2 Application Data : après l'information SERVER-HELLO-DONE, les échanges sont tous chiffrés/déchiffrés via l'algorithme de chiffrement/déchiffrement symétrique et la clé de session. Les mêmes commandes de base HTTP sont maintenant chiffrées dans la connexion HTTPs.

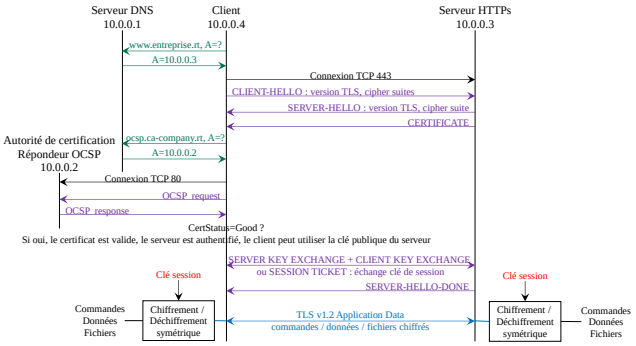


**Figure 5. Diagramme d'un transfert HTTPs**

# 6. CONCLUSION

Dans cet article a été décrite une vue de l'article final qui comprendra la théorie sur la cryptographie puis la mise en place d'une autorité de certification et de son répondeur OCSP et l'élaboration d'un certificat numérique venant s'intégrer à un serveur web. Les transmissions sous-jacentes mettent en évidence le transfert du certificat du serveur web au client navigateur, puis l'interrogation du répondeur OCSP pour vérifier la véracité du certificat, avant de poursuivre par le transfert chiffré des données entre le navigateur et le serveur web.

L'aspect didactique et pédagogique de la progression permet au lecteur de découvrir les principes du chiffrement, le contenu d'un certificat numérique, le rôle de l'autorité de certification et de son répondeur OCSP, l'intégration du certificat dans le serveur web et l'enchainement des diverses trames entre le navigateur client et les serveurs. Le lecteur peut alors comprendre le fonctionnement d'une transaction HTTPs qu'il a déjà effectué à maintes reprises sur Internet.

# 7. REFERENCES

L'article final comportera une bibliographie / webographie.