

Autorité de certification

Le besoin

Les accès aux ressources en lignes (à l'intérieur de l'entreprise ou sur une connexion extérieure) exposent les informations échangées à un **risque d'altération ou d'interception**.

Pour empêcher ce risque de modification ou d'écoute, la mise en place d'une **connexion chiffrée assurant la confidentialité des échanges** est aujourd'hui assurée par [SSL/TLS](#).

Toutefois, avoir une connexion chiffrée ne suffit pas pour garantir la sécurité : il faut aussi avoir la **garantie que la connexion est de confiance**, sinon, bien que l'échange soit **confidentiel**, les données sont envoyées vers un serveur éventuellement malveillant.

C'est là qu'intervient l'[autorité de certification](#).

Le rôle de l'autorité

L'autorité de certification est une des méthodes de mise en place d'**infrastructure à clé publique** (ICP) ou de **public key infrastructure** (PKI). C'est la technique qui s'applique pour les **certificats normalisés au format X.509**.

Comme son nom l'indique, l'autorité de certification est un **organisme qui fait autorité et dont la fiabilité ne peut être discutée**. Elle a donc la possibilité de garantir l'identité d'une organisation en procédant à des contrôles divers. On parle d'un **tiers de confiance**.

Une **autorité de certification** est un **service** chargé de :

- **délivrer des éléments de sécurité** (clé privée, certificat public) dont l'**authenticité** est contrôlée (vérification de la détention du nom de domaine, de l'existence réelle de l'entreprise, etc), aussi bien pour des individus, des matériels ou des services
- **vérifier** si un **certificat** reçu par un utilisateur, un matériel ou un service dans le cadre d'un échange chiffré est fiable et donc si la **communication est de confiance**.

Fonctionnement

La garantie réalisée par l'autorité se déroule en deux étapes :

1. production et distribution des éléments de sécurité
2. exécution d'une demande de vérification sur une identité (certificat)

1 Production et distribution des éléments de sécurité

Pour garantir l'identité d'une organisation, l'AC s'appuie sur trois phases :

- **Enregistrement de la demande** : un **rôle d'autorité d'enregistrement** (ou RA Registry Authority) reçoit des demandes de validation au format CSR (Certificate Signing request) émise par une entreprise (ou depuis un serveur/machine interne). Il s'agit d'un fichier numérique **.csr** généré à partir de la clé privée de l'entreprise demandeuse.
- **Validation** : un **rôle d'autorité de validation** est chargé de contrôler l'identité de l'émetteur par divers moyens (vérification d'une adresse mail, d'un nom de domaine, d'un numéro de SIRET/SIREN, du KBis de l'entreprise, etc). En fonction de l'étude, cette validation peut être acceptée ou rejetée
- **Certification** : c'est l'étape finale, faites par le **rôle autorité de certification** : le fichier au format CSR soumis par l'entreprise demandeuse est signé **par la clé privée de l'AC**, ce qui garantit son authenticité (seule l'AC dispose de cette clé privée et peut créer le fichier de sortie). Le fichier ainsi produit est un certificat public.

A la fin du processus, l'organisme certificateur retourne à l'entreprise demandeuse le certificat garanti qu'il a généré. L'entreprise peut alors l'intégrer au service ou serveur ou le fournir à l'individu pour lequel elle a fait la demande.

2 Vérification d'un certificat

Lorsque les individus naviguent sur un site sécurisé, ils reçoivent de la part de ce site le certificat public qu'il héberge.

Grâce à un **magasin d'autorités** connu par le navigateur, ce dernier va demander à l'AC déclarée dans le certificat public si le document est authentique.

L'AC va vérifier dans la liste des certificats qu'elle a généré si le document est conforme :

- toujours valide ou expiré
- le FQDN est celui enregistré initialement
- l'utilisation prévue (par exemple HTTPS) est conforme
- l'**empreinte du certificat** est la même que celle enregistrée lors de la génération (contrôle de l'**intégrité**)

Amélioration du fonctionnement : Protocole OCSP

Le trafic généré par les validations de certificats est important : demande à chaque connexion pour chaque ordinateur du réseau, récupération des dernières versions des certificats publics connus par chaque autorité, etc.

Pour alléger l'activité des serveurs autorité, le protocole **OCSP** (Online Certificate Status Protocol) ajoute un niveau intermédiaire. Les serveurs OCSP gardent une information actualisée pour la mettre à disposition des navigateurs des utilisateurs. Ils font donc un travail commun à l'ensemble des postes à la façon d'un relais.

From:

<https://wiki.sio.bts/> - **WIKI SIO : DEPUIS 2017**

Permanent link:

<https://wiki.sio.bts/doku.php?id=autoritecertif&rev=1664380013>

Last update: **2022/09/28 15:46**

