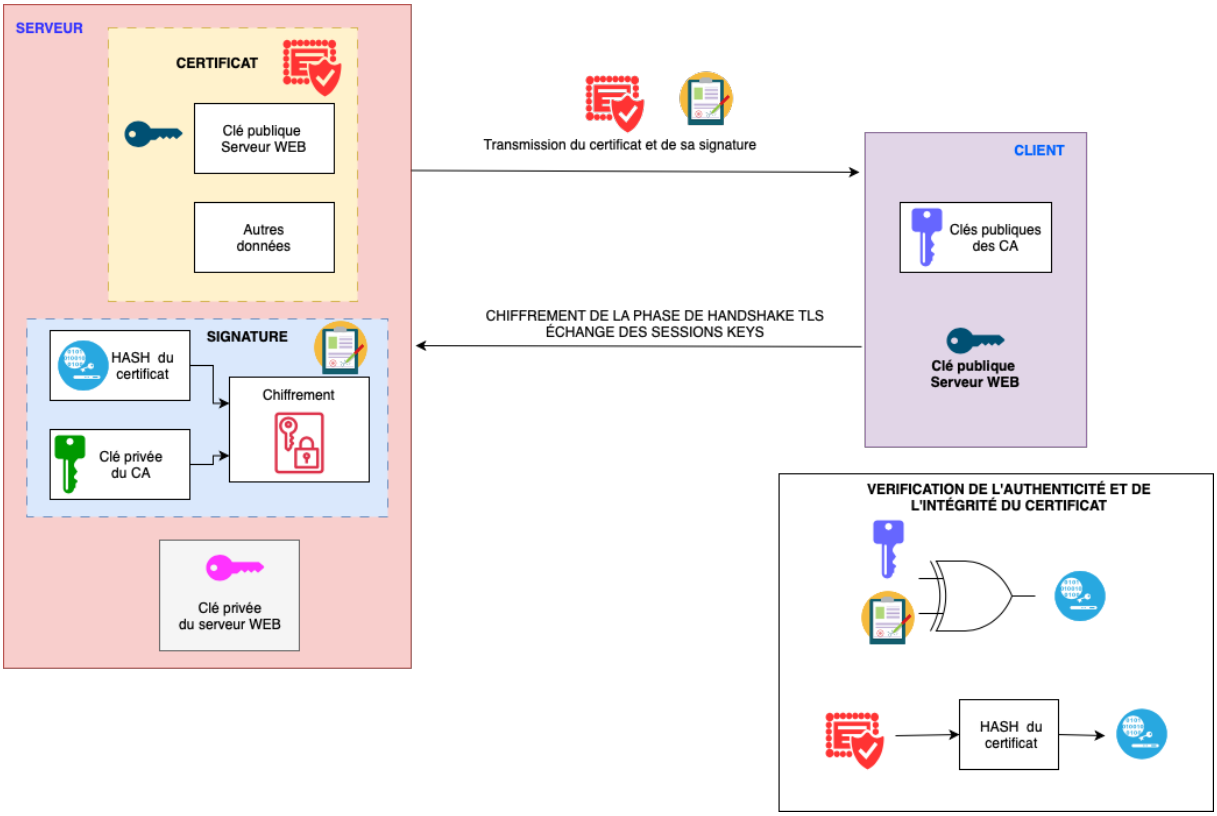
CERTIFICATS SSL



Constitution d'un certificat :

Un certificat SSL est constitué de plusieurs éléments clés qui assurent son fonctionnement et sa sécurité :

- **Nom de Domaine** : Le certificat spécifie le nom de domaine pour lequel il est valide. Cela peut être un nom de domaine spécifique (par exemple, www.exemple.com) ou un nom de domaine à caractère générique (par exemple, *.exemple.com pour tous les sous-domaines de exemple.com).
- **Détails de l'Organisation** : Il contient des informations sur l'organisation ou l'individu à qui le certificat a été émis. Cela comprend généralement le nom et l'adresse.
- **Autorité de Certification (CA)** : Le certificat indique l'Autorité de Certification qui l'a émis. Les navigateurs et les systèmes d'exploitation ont une liste des CA de confiance, et ils utilisent cette liste pour vérifier l'authenticité des certificats.
- **Clé Publique** : Le certificat contient la clé publique du serveur. Cette clé est utilisée par les clients pour chiffrer les données envoyées au serveur, qui les déchiffre ensuite avec sa clé privée correspondante.
- **Période de Validité** : Chaque certificat a une période de validité. Il indique la date de début et de fin de cette période. Après la date d'expiration, le certificat n'est plus considéré comme valide.
- **Numéro de Série** : Un identifiant unique attribué au certificat par l'Autorité de Certification.

- **Signature de l'Autorité de Certification** : Le certificat est signé numériquement par l'Autorité de Certification. Cette signature est utilisée pour vérifier que le certificat n'a pas été altéré et qu'il est authentique.
- **Algorithmes de Chiffrement** : Le certificat spécifie les algorithmes de chiffrement utilisés pour la signature et peut également inclure des informations sur les types de chiffrement supportés pour le chiffrement des données.
- **Extensions** : Des informations supplémentaires peuvent être incluses dans les extensions du certificat, telles que les contraintes d'utilisation du certificat, les politiques de certification, etc.

Signature de l'Autorité de Certification :

La signature d'un certificat SSL est un processus crucial qui assure son authenticité et son intégrité. Voici comment cela se passe :

1. **Création d'une Demande de Signature de Certificat (CSR)** : Tout d'abord, l'entité qui souhaite obtenir un certificat SSL (comme une entreprise ou un individu) génère une Demande de Signature de Certificat (Certificate Signing Request - CSR). Cette demande comprend la clé publique du demandeur ainsi que des informations d'identification, comme le nom de l'organisation et le nom de domaine.
2. **Envoi du CSR à l'Autorité de Certification (CA)** : Le CSR est ensuite envoyé à une Autorité de Certification de confiance. La CA vérifie l'identité et les informations fournies par le demandeur. Cette vérification peut inclure la confirmation de l'existence et de la légitimité de l'entreprise, la correspondance du nom de domaine, etc.
3. **Génération de la Signature Numérique** : Une fois le CSR vérifié, l'Autorité de Certification utilise son propre algorithme de signature numérique pour signer le certificat. La signature est réalisée en utilisant la clé privée de la CA. Cela implique généralement un processus de hachage des informations du certificat, puis de chiffrement du hash avec la clé privée de la CA.
   - Hachage : Le contenu du certificat (y compris la clé publique du demandeur) est d'abord haché, c'est-à-dire transformé en une chaîne de caractères de longueur fixe (le hash). Ce hash représente de manière unique le contenu du certificat.
   - Chiffrement du Hash : Le hash est ensuite chiffré avec la clé privée de la CA. Ce chiffrement du hash constitue la "signature numérique".
4. **Émission du Certificat Signé** : La CA ajoute ensuite cette signature numérique au certificat et l'émet au demandeur. Le certificat signé contient donc la clé publique du demandeur, ses informations d'identification, ainsi que la signature numérique de la CA.
5. **Vérification de la Signature** : Lorsqu'un client (comme un navigateur web) reçoit le certificat SSL d'un serveur, il peut vérifier la signature numérique. Pour ce faire, le client utilise la clé publique de l'Autorité de Certification (qui est préinstallée dans le navigateur ou le système d'exploitation) pour déchiffrer la signature numérique, récupérant ainsi le hash. Le client génère alors son propre hash à partir des informations du certificat et compare les deux. Si les hashes correspondent, cela signifie que le certificat est authentique et n'a pas été altéré.