# Mieux comprendre les certificats SSL

**THAWTE EST L'UN DES PRINCIPAUX FOURNISSEURS DE CERTIFICATS SSL DANS LE MONDE**

thawte

# sommaire

# mieux comprendre les certificats SSL

Les certificats SSL (Secure Socket Layer) sont couramment utilisés pour sécuriser et authentifier les communications sur Internet et au sein des intranets d'entreprise. Thawte s'affirme comme l'un des principaux fournisseurs de ces certificats SSL dans le monde. L'utilisation de certificats Thawte SSL sur vos serveurs Web d'entreprise vous permet de reicueillir en toute sécurité des informations sensibles transmises en ligne afin de garantir à vos clients et utilisateurs la protection de leurs communications.

Dans ce guide d'initiation à la sécurité SSL, nous aborderons les principes de base du fonctionnement du protocole SSL. Nous y évoquerons les diverses applications des certificats SSL et vous livrerons les conseils d'un déploiement en bonne et due forme, avant de conclure sur les moyens à votre disposition pour tester des certificats SSL sur votre serveur Web.

## SSL et certificats SSL : définition

Développé par Netscape en 1995, le protocole SSL s'est rapidement imposé comme le mode de sécurisation privilégié des transmissions de données sur Internet.

Intégré aux principaux navigateurs et serveurs Web, SSL utilise des techniques de cryptage qui s'appuient sur un système de clé publique/privée initialement développé par RSA. L›établissement d'une connexion SSL nécessite l'installation d'un certificat numérique sur le serveur Web. Ce certificat utilise alors les clés publiques et privées pour le cryptage, et identifie le serveur de manière unique et définitive. Les certificats numériques s'apparentent à une forme de carte d'identité électronique qui permet au client d'authentifier le serveur avant l'établissement d'un canal de communication crypté.

Généralement, les certificats numériques sont délivrés par un organisme de confiance indépendant – condition sine qua non à leur validité et leur acceptation à grande échelle. L'organisme émetteur de certificats est appelé Autorité de certification (AC), dont Thawte constitue un exemple à l'échelle mondiale.

## Les fonctionnalités SSL

On associe généralement SSL au cryptage. Or un certificat SSL remplit quatre fonctions bien distinctes, toutes indispensables à la protection de la confidentialité et de la sécurité des clients et utilisateurs : cryptage, intégrité, authentification et non-répudiation.

### CRYPTAGE

Le cryptage utilise des algorithmes mathématiques pour transformer les données et les rendre exclusivement lisibles par les parties concernées. Dans le cadre d'une transaction sécurisée par SSL, les clés privées et publiques fournies avec le certificat numérique du serveur jouent un rôle déterminant dans la sécurisation des données envoyées et reçues par le navigateur Web.

### INTÉGRITÉ

En cryptant les données pour les rendre exclusivement lisibles par les parties concernées, les certificats SSL assurent également leur intégrité. En d'autres termes, ces données ne pouvant être lues par aucun tiers, leur modification en cours de transit s'avère par conséquent impossible. Si les données cryptées étaient modifiées, elles seraient de fait rendues inutilisables – ce qui ne saurait échapper aux parties concernées. La moindre tentative d'interférence est donc automatiquement repérée.

### AUTHENTIFICATION

L'émission d'un certificat numérique par une autorité de certification permet essentiellement de valider l'identité de l'organisme – ou de la personne – à l'origine de la demande de certificat. Les certificats SSL sont associés à un nom de domaine Internet. La vérification par l'AC de l'identité du propriétaire du domaine en question permet aux utilisateurs de savoir dans un premier temps à qui ils ont affaire. Ainsi, lorsque vous vous connectez sur un site sécurisé par SSL comme Amazon.fr, le certificat identifie le propriétaire comme étant la société Amazon, Inc. Vous avez ainsi l'assurance d›être sur le véritable site exploité par Amazon.

### NON-RÉPUDIATION

La non-répudiation se caractérise par l'association de fonctions de cryptage, de protection de l'intégrité et d'authentification. En clair, aucune partie prenante à une transaction sécurisée ne peut légitimement affirmer que ses échanges/communications provenaient d'une autre personne ou entité. Cette caractéristique supprime toute possibilité pour l'une des parties de répudier ou de « se rétracter » par rapport à des informations communiquées en ligne.

## Champs d'application du SSL

Le protocole SSL peut être utilisé de diverses façons et à des fins différentes :

- Communications « de navigateur à serveur » : la plupart du temps le SSL sert à sécuriser les communications entre un serveur Web et un navigateur, notamment dans le cadre de transmissions d'informations sensibles (achats en ligne, dossiers médicaux ou transactions bancaires). La technologie SSL permet de confirmer à l'utilisateur l'identité du destinataire de ses informations personnelles, tout en assurant que seule cette entité autorisée y aura accès.
- Communications « de serveur à serveur » : le protocole SSL peut également être utilisé pour sécuriser les communications entre deux serveurs, telles que les transactions entre deux entreprises. Dans ce scénario, les deux serveurs possèdent généralement un certificat qui leur permet de s'authentifier mutuellement et de sécuriser leurs communications bilatérales.
- Respect des obligations réglementaires : de nombreuses réglementations juridiques et sectorielles exigent des niveaux d'authentification et de confidentialité que les certificats SSL permettent d'obtenir. Le standard PCI DSS (*Payment Card Industry Data Security Standard*) exige par exemple l'utilisation de technologies d'authentification et de cryptage pour tout paiement en ligne.

## SSL côté utilisateur

Lors de sa visite sur un site Web sécurisé par un certificat SSL, l›utilisateur voit s'afficher dans son navigateur Web plusieurs indices visuels attestant de l'activation du protocole SSL. Par exemple, l'adresse dans la barre d'adresse du navigateur commencera par **https://** pour les connexions sécurisées par SSL, et par **http://** pour les connexions non sécurisées.

La plupart des navigateurs affichent également un cadenas (voir figure 1), dont l'emplacement et l'aspect varient d'un navigateur à un autre.


*Figure 1 : cadenas affiché par un navigateur Web*

Sur certains navigateurs, l'utilisateur peut également cliquer sur le cadenas pour consulter des informations complémentaires sur le certificat. Ainsi, Firefox™ affiche une boîte de dialogue semblable à celle reproduite à la figure 2, avec diverses informations sur le certificat, son propriétaire et l'autorité émettrice.

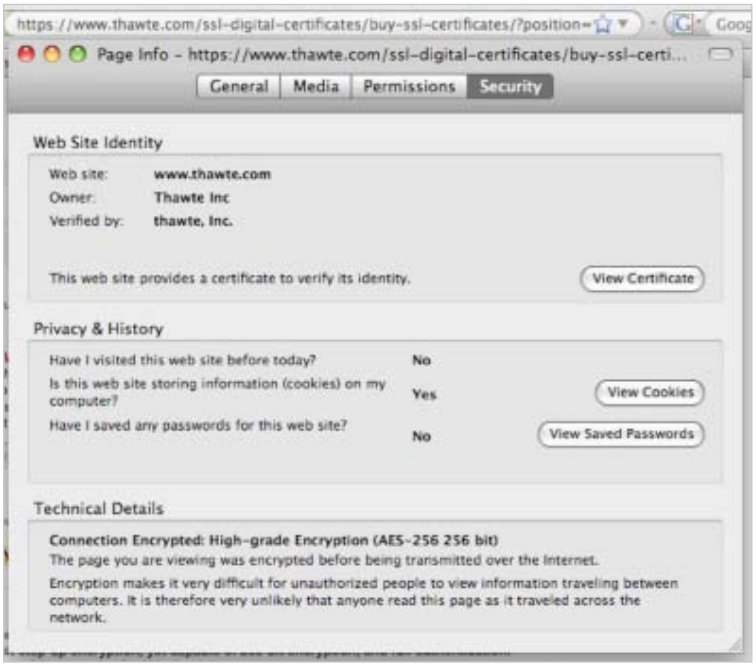


*Figure 2 : renseignements sur un certificat, y compris son propriétaire et l'autorité émettrice.*

Pour obtenir d'autres informations comme la date d'expiration, les empreintes de vérification etc., il suffit de cliquer sur « Afficher le certificat » (figure 3).

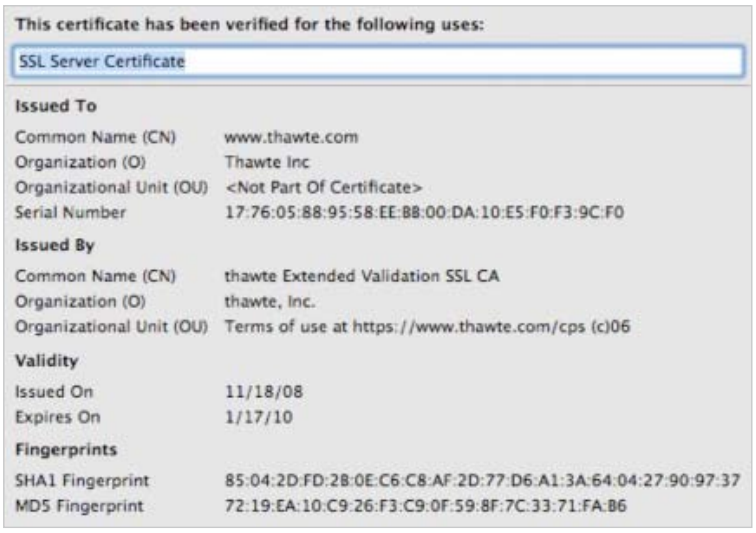


*Figure 3 : renseignements complémentaires sur un certificat.*

Plusieurs éléments d'informations essentiels sont proposés :

- Nom du domaine pour lequel le certificat est délivré. Le certificat n'est valide que s'il est utilisé avec ce domaine. Toute demande associée à un autre nom de domaine fait l'objet d'un refus systématique par le navigateur.
- Propriétaire du certificat : les utilisateurs peuvent ainsi voir le nom de l'entité détentrice du site.
- Période de validité du certificat : correspond à la date de début et de fin de validité du certificat. À l'instar d'autres formes d'identification, les certificats numériques ont une date d'expiration et doivent être renouvelés. Objectif : permettre à l'AC de vérifier à nouveau l'identité du propriétaire du certificat.

## Certificats SSL et certificats SSL Extended Validation (EV)

Le maintien du processus rigoureux de vérification des identités préalable à l'émission de certificats SSL représente un coût conséquent pour les autorités de certification. À l'origine, le prix des premiers certificats SSL reflétait donc la qualité de ce processus de vérification. Or, sous la pression du marché, les AC ont commencé à proposer des certificats plus abordables avec « validation de domaine uniquement ». Dépourvus de toute vérification poussée de l'identité de la société propriétaire du domaine, ces certificats à bas prix ne vérifient que le nom de domaine pour lequel ils sont émis. Moins coûteux, ils offrent inévitablement moins de garanties à l'utilisateur final. Ces certificats conviennent généralement à des usages à faible niveau de sécurité qui ne nécessitent pas la validation détaillée d'un certificat SSL classique.

Cette segmentation a toutefois fini par entraîner une certaine confusion entre les différents types de certificats SSL. Les utilisateurs ont donc exigé la mise en place de moyens de distinction entre certificats économiques et certificats renforcés soumis à une vérification plus poussée des identités. Le CA Browser Forum – un regroupement professionnel indépendant – n'a pas tardé à répondre à cette demande avec une série de principes directeurs pour l'élaboration d'un certificat à validation renforcée ou certificat Extended Validation (EV).

Un certificat EV est un certificat SSL pour lequel l'autorité de certification émettrice valide l'identité du demandeur du certificat à travers un processus encore plus détaillé et rigoureux. Les AC doivent également soumettre leurs procédures de validation à un audit indépendant pour conserver leurs droits d'émission de certificats EV. Résultat : les certificats EV ne sont généralement proposés que par des autorités de certification de premier plan comme Thawte.

La présence de certificats EV sur les sites Web est signalée visuellement de différentes manières par les navigateurs Web, qui proposent également des informations d'identité plus complètes et plus facilement accessibles (voir figure 4).


*Figure 4 : indices visuels indiquant la présence d'un certificat EV.*

Ces indices visuels spécifiques (comme la barre de navigation verte) renforcent la distinction entre certificats ultra fiables pour les applications haute sécurité, et les autres. Les utilisateurs ont ainsi tous les éléments en main pour s'assurer avec certitude de l'identité de l'entité avec laquelle ils communiquent (voir figure 5).

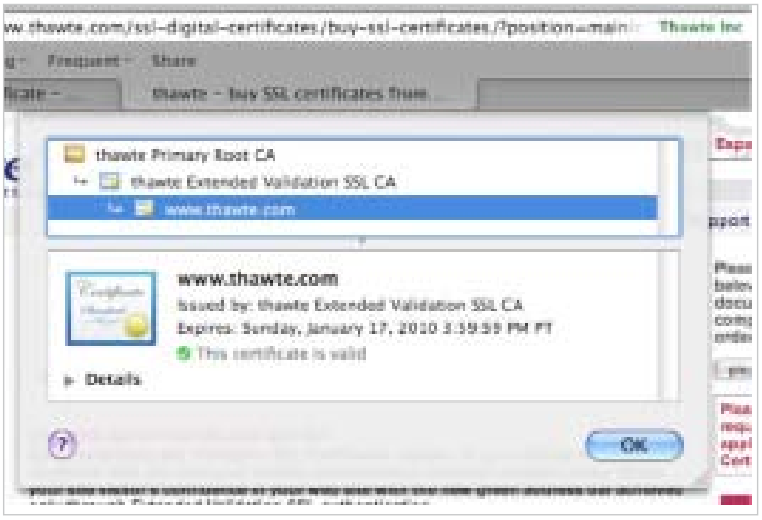


*Figure 5 : accès aux informations d'un certificat EV.*

## Fonctionnement du protocole SSL

Le protocole SSL est relativement simple... malgré la complexité de ses algorithmes.

### CLÉS PUBLIQUES ET PRIVÉES

Le protocole SSL utilise des clés de cryptage publiques et privées. Lors de l'émission d'un certificat numérique pour un serveur Web, ce certificat contient deux clés : l'une, détenue de manière privée par le serveur Web (« clé privée »), et l'autre, rendue publique à toute personne en faisant la demande (« clé publique »).
Ces deux clés sont asymétriques :

- Les données cryptées par la clé privée ne peuvent être décryptées que par la clé publique
- Les données cryptées par la clé publique ne peuvent être décryptées que par la clé privée

Ainsi, pour garantir la confidentialité des échanges, le navigateur Web s'adresse à la clé publique du serveur. Le navigateur l'utilise ensuite pour crypter les informations à transmettre – informations qui pourront ensuite être décryptées par le serveur Web à l'aide de sa propre clé privée. Dans la pratique, le processus de cryptage fait parfois intervenir des clés de session aléatoires, valables pour une courte durée entre le navigateur et le serveur. Ces clés de session sont utilisées car bien souvent, le navigateur ne possède pas son propre certificat numérique et sa propre paire de clés.

## CRÉATION D'UNE SESSION SSL

Le début d'une session SSL est marqué par l'envoi d'une requête par le navigateur au serveur Web à l'aide du protocole **https://** (voir figure 6).

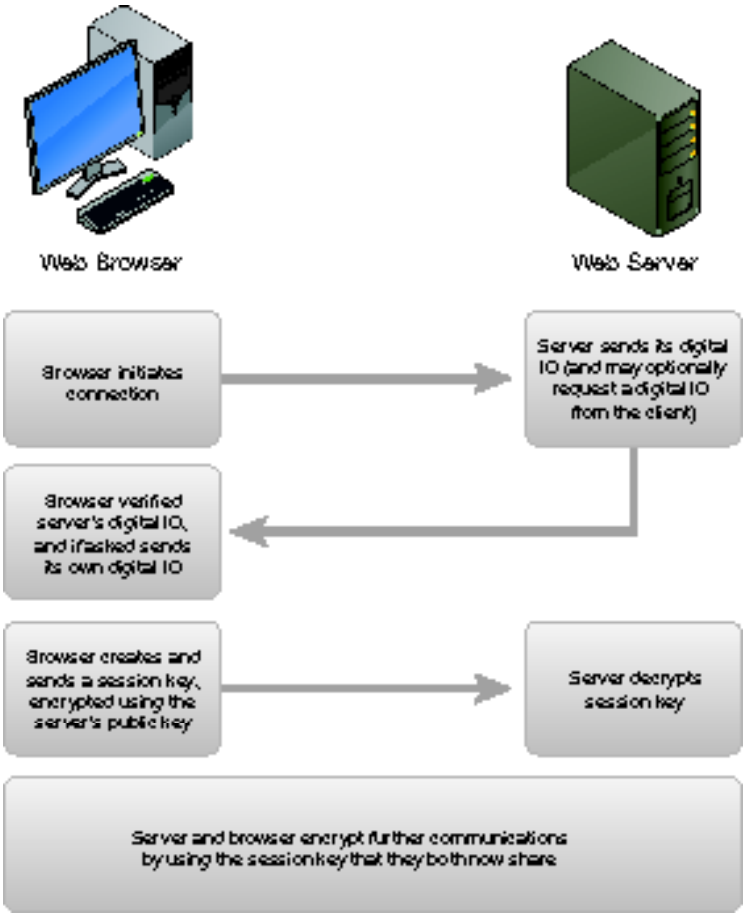


*Figure 6 : création d'une session SSL.*

Le serveur Web répond avec son identifiant numérique qui comprend sa clé de cryptage publique. Le navigateur vérifie l'identifiant numérique, en consultant par exemple l'autorité de certification pour une vérification en ligne, et en contrôlant également les dates de validité et d'autres informations relatives au certificat lui-même. Une fois ces vérifications terminées, le navigateur génère une clé de session qu'il crypte à l'aide de la clé publique du serveur, avant de renvoyer l'ensemble au serveur.

Le serveur décrypte alors la clé de session à l'aide de sa clé de cryptage privée qu'il est le seul à posséder. La clé de session n'appartient qu'au navigateur et au serveur qui peuvent alors utiliser cette clé commune pour crypter leurs échanges. Généralement, les serveurs rejettent les clés de session après quelques minutes d'inactivité.

## Les solutions SSL signées de Thawte

Thawte propose plusieurs types de certificats SSL. Chacun de ces produits est conçu pour des besoins bien ciblés :

- **Le certificat SSL EV pour serveur Web** est un certificat à validation étendue (Extended Validation) doté d'un algorithme de cryptage fort (256 bits). Ce type de certificat implique des procédures de vérification d'identité très détaillées pour garantir un niveau de confiance maximal sur les sites et applications Web haute sécurité.
- **Le SGC SuperCert** est un certificat SSL haut de gamme avec cryptage SSL jusqu'à 256 bits et authentification complète. Ces certificats règlent automatiquement le niveau de cryptage à 128 bits sur certains navigateurs Web plus anciens.
- **Le certificat SSL pour serveur Web** est un certificat SSL standard avec authentification et cryptage jusqu'à 256 bits.
- **Le certificat SSL123** est un certificat validant uniquement le nom de domaine. Émis en quelques minutes seulement, ce type de certificat offre un niveau de cryptage jusqu'à 256 bits.
- **Les certificats SSL Wildcard** peuvent être utilisés pour sécuriser plusieurs sous-domaines appartenant à un domaine unique entièrement validé, à l'aide d'un seul certificat. Ces certificats offrent un niveau de cryptage jusqu'à 256 bits.

Pour plus d'informations sur ces produits, et nos autres certificats, n'hésitez pas à interroger les conseillers commerciaux Thawte.

### LE SCEAU DE CONFIANCE THAWTE

Tous nos clients de certificats SSL pour serveur Web, certificats SGC SuperCert et certificats SSL EV pour serveur Web peuvent afficher le sceau de confiance Thawte sur leur site Web (voir figure 7). Ce sceau est une image sécurisée générée par Thawte qui atteste du niveau de confiance dont bénéficie votre site. Disponible en plusieurs langues et formats, il s'intègre harmonieusement au design de votre site.


*Figure 7 : le sceau de confiance Thawte.*

## Test d'un certificat SSL sur votre serveur Web

Pour vous faire une meilleure idée de nos produits, nous vous invitons à tester et évaluer par vous-même un certificat SSL. Il vous suffit pour cela de télécharger notre version d'évaluation d'un certificat Thawte SSL. Valides pendant 21 jours, ces certificats vous permettent de vous familiariser avec le processus d'installation et les questions de compatibilité avec le logiciel de votre serveur Web. Pour demander votre version d'évaluation gratuite de notre certificat SSL, rendez-vous sur :
https://ssl-certificate-center.thawte.com/process/retail/thawte_trial_initial?application_locale=THAWTE_US

## Liens utiles

Nous vous invitons à consulter nos liens utiles :

- Renseignements complémentaires sur les certificats Thawte SSL pour serveur Web disponibles sur : http://www.thawte.fr/ssl/web-server-ssl-certificates/index.html
- Base de connaissances Thawte recensant des exemples des principaux problèmes et solutions inhérents aux certificats SSL : https://search.thawte.fr
- Pour vos achats de certificats Thawte SSL en ligne : http://www.thawte.fr/ssl/index.html

## La société Thawte

Thawte est une autorité de certification habilitée à émettre des certificats SSL et des certificats numériques code signing aux entreprises et particuliers à travers le monde. Thawte procède à plusieurs niveaux de vérification et d'authentification en fonction du type de certificat requis. Réputés pour leur interopérabilité avec les principaux serveurs Web, navigateurs et autres applications Web, les certificats numériques Thawte garantissent et améliorent l'intégrité de vos transactions et communications en ligne.

## Nous contacter

Pour tout complément d'information ou pour vous entretenir avec un conseiller commercial Thawte, n'hésitez pas à nous contacter :

- Adresse électronique : sales@thawte.com
- France : +33 157 32 42 68
- Amérique du Nord : +1 888 484 2983
- International : +27 21 819 2800
- Fax : +27 21 819 2960
- Chat en direct : https://www.thawte.fr/chat/chat_retail_new.html




27-01-2011
AL100685