Guide d'initiation aux certificats TLS/SSL

Faire le bon choix parmi les options de sécurité en ligne disponibles

digicert®

Sommaire

Introduction

Pour les particuliers comme pour les entreprises, la sécurité en ligne devrait être abordée comme n'importe quelle question de sécurité physique. Outre son effet rassurant, une démarche de cybersécurisation fondée sur des principes de sécurité universels permet de protéger l'ensemble de vos visiteurs – amis, collègues, partenaires professionnels ou internautes. Mais pour une protection optimale, il est indispensable de bien cerner les risques en présence – un objectif qui tient souvent de la gageure tant l'environnement technologique ne cesse d'évoluer. D'où l'intérêt de contracter les services d'un prestataire de sécurité en ligne réputé et respecté.

Ce guide de découverte des certificats TLS/SSL vous livre toutes les clés d'un choix éclairé. N'hésitez pas à vous reporter au glossaire des termes techniques proposé au chapitre « Mini-glossaire de la cybersécurité » à la fin de ce document.

Qu'est-ce qu'un certificat TLS/SSL ?

Le TLS (Transport Layer Security) et son prédécesseur le SSL (Secure Sockets Layer) sont les protocoles de sécurité les plus répandus à l'heure actuelle. Ils remplissent avant tout deux fonctions :

1. **Authentification et vérification –** Le certificat TLS/SSL authentifie les éléments d'identification d'une personne, d'une entreprise ou d'un site web, préalablement validés par son Autorité de certification (AC) émettrice. Pour consulter ces informations, les internautes doivent cliquer sur le cadenas ou la marque de confiance (comme le sceau DigiCert® Secured ou le sceau Norton Secured powered by DigiCert) qui s'affiche dans leur navigateur. Plus loin, nous passerons en revue les différents niveaux de validation existants.
2. **Chiffrement des données –** Le certificat TLS/SSL permet également de chiffrer les données sensibles échangées via le site web pour éviter toute interception ou exploitation par toute autre personne que le destinataire visé.

À l'image des cartes d'identité ou des passeports délivrés par les autorités officielles d'un pays, les certificats TLS/SSL n'ont de valeur que s'ils sont émis par une AC de confiance. L'AC doit en effet obéir à un ensemble de règles particulièrement strictes pour octroyer, ou non, un certificat TLS/SSL au demandeur. La possession d'un certificat TLS/SSL valide, émis par une AC de confiance, constitue par conséquent un gage de sérieux pour vos clients et partenaires.

Fonctionnement du chiffrement TLS/SSL

À l'instar d'une clé qui permet de fermer et d'ouvrir une porte, le chiffrement utilise une clé pour verrouiller et déverrouiller vos données. Sans la bonne clé, impossible d'y accéder.

Chaque session TLS/SSL comprend deux clés :

- La clé publique, qui permet de chiffrer (crypter) les informations.
- La clé privée, qui sert à déchiffrer (décrypter) ces mêmes informations et à les restituer dans leur format d'origine.

TLS et SSL sont les abréviations respectives de Transport Layer Security et Secure Socket Layer. Ces technologies permettent d'établir une connexion sécurisée entre le navigateur de l'internaute et votre site web. Ainsi, tous les échanges effectués dans le cadre de cette session sont chiffrés, et donc protégés.

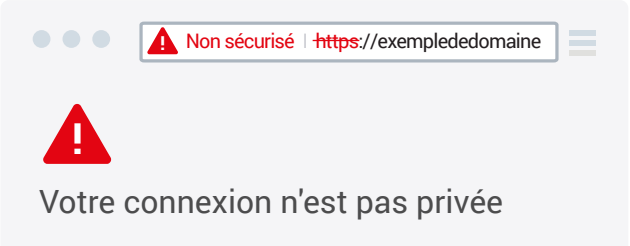
Vous viendrait-il à l'idée de noter vos données confidentielles ou votre code de carte bleue au dos d'une carte postale ? Il en va de même pour vos communications sur Internet.

C'est pourquoi le TLS/SSL crée un canal parfaitement privé et sécurisé pour vos communications.

Description du processus : un certificat TLS/SSL émis par une AC n'est valable que pour un serveur et un domaine de site web (adresse du site) spécifiques. Ainsi, lorsqu'un internaute utilise son navigateur pour accéder à un site web protégé par un certificat TLS/SSL, la session débute par un échange de messages appelé « négociation TLS/SSL » (ou handshake en anglais) entre le navigateur et le serveur. Le serveur est enjoint de fournir certaines informations qui s'affichent alors dans le navigateur de l'internaute. L'ouverture d'une session sécurisée se reconnaît à certains signes – par exemple l'apparition d'une marque de confiance sur laquelle il suffit de cliquer pour afficher des informations telles que la période de validité du certificat TLS/SSL, le domaine sécurisé, le type de certificat et l'AC émettrice. Une liaison sécurisée est ainsi établie à l'aide d'une clé de session unique. Les transactions peuvent alors être effectuées en toute sécurité.

Identification de la présence d'un certificat TLS/SSL valide sur un site web

1. Sur un site web standard dépourvu de certificat TLS/SSL, la mention « http:// » précède l'URL du site affichée dans la barre d'adresse du navigateur. Ce préfixe désigne le protocole de transfert hypertexte (de l'anglais « Hypertext Transfer Protocol »), mode de transmission d'informations non sécurisé sur Internet. À l'ouverture de tels sites, la plupart des navigateurs affichent un message d'avertissement qui produit un véritable effet d'épouvantail sur les internautes.



Sur un site web sécurisé par un certificat TLS/SSL, l'adresse est précédée du préfixe « https:// » qui désigne un protocole HTTP sécurisé.

2. Vous remarquerez également l'icône d'un cadenas fermé en haut ou en bas du navigateur (varie selon les navigateurs).

3. Souvent, vous verrez s'afficher une marque de confiance sur le site web lui-même. Les clients DigiCert affichent par exemple le sceau DigiCert® Secured ou Norton Secured powered by DigiCert sur leur site. Lorsque l'on clique sur le sceau DigiCert ou n'importe quelle marque de confiance estampillée « powered by DigiCert », ou encore sur l'icône du cadenas de la page, on obtient tous les renseignements sur le certificat, ainsi que les coordonnées de l'entreprise vérifiées et authentifiées par l'AC.

4. Pour afficher le nom de la société authentifiée, l'internaute peut cliquer sur le cadenas fermé dans la fenêtre du navigateur, ou sur certaines marques de confiance TLS/SSL (dont le sceau DigiCert® Secured ou Norton Secured). Dans les navigateurs plus sécurisés, le nom de la société authentifiée apparaît bien en évidence et le texte ou la barre de navigation peut s'afficher en vert dès qu'un certificat TLS/SSL Extended Validation (EV) est détecté. En revanche, si les données ne concordent pas, ou si le certificat a dépassé sa date d'expiration, un message d'erreur ou d'alerte s'affiche.

Champs d'application des certificats TLS/SSL

Un certificat TLS/SSL sert à sécuriser la transmission d'informations sur Internet.

Quelques exemples d'utilisation :

- Pour sécuriser les échanges entre votre site web et le navigateur Internet d'un de vos clients
- Pour sécuriser les échanges internes sur l'intranet de votre entreprise
- Pour sécuriser les informations entre serveurs (internes et externes)
- Pour sécuriser les informations reçues et envoyées à partir de terminaux mobiles

Les différents types de certificats TLS/SSL

Plusieurs types de certificats TLS/SSL sont aujourd'hui disponibles sur le marché.

- Le premier type est connu sous le nom de certificat auto-signé. Comme son nom l'indique, ce certificat n'est pas émis par une AC, ce qui le voue généralement à un usage interne. Dans la mesure où le propriétaire du site web génère lui-même son certificat, celui-ci n'a pas la même crédibilité qu'un certificat TLS/SSL émis par une AC au terme d'un processus rigoureux de vérification et d'authentification.
- Certificat TLS/SSL de base, le certificat de validation de domaine (DV) peut être émis rapidement. La seule vérification effectuée consiste à s'assurer que le domaine (adresse du site web) de rattachement du certificat appartient bien au demandeur. Aucun contrôle supplémentaire n'est réalisé pour vérifier l'authenticité de l'entité détentrice du domaine.
- Le certificat TLS/SSL avec authentification intégrale représente la première étape d'une stratégie de renforcement de la sécurité et de développement de votre capital confiance en ligne. Ces certificats ne sont accordés qu'une fois les contrôles et les validations d'usage effectués (confirmation de l'existence de l'entreprise, nom du propriétaire du domaine, habilitation de l'utilisateur à formuler une demande d'émission de certificat), d'où des délais d'émission légèrement plus longs.

Tous les certificats TLS/SSL de la marque DigiCert font l'objet d'une authentification intégrale.

- Bien souvent, plusieurs suffixes sont associés à un même nom de domaine. C'est pourquoi un certificat Wildcard vous permet de sécuriser par TLS/SSL l'ensemble des hôtes de votre domaine. Par exemple, dans l'adresse host.votre-domaine.com, « host » correspond à une variable, tandis que le nom de domaine reste constant.
- Malgré de nombreuses similitudes avec un certificat Wildcard, le certificat TLS/SSL SAN (Subject Alternative Name) offre davantage de polyvalence et permet de couvrir plusieurs domaines avec un seul et même certificat TLS/SSL.
- Les certificats TLS/SSL Extended Validation (EV) constituent la référence absolue en matière d'authentification et de mise en confiance du client. Lorsqu'un client surfe sur un site web sécurisé par un certificat TLS/SSL EV, la barre d'adresse s'affiche en vert (dans certains navigateurs) et un champ fait apparaître le nom du propriétaire officiel du site et celui de l'autorité émettrice. Les noms du détenteur du certificat et de l'AC émettrice s'affichent également dans la barre d'adresse. Ces témoins visuels représentent un excellent levier de mise en confiance du consommateur.

Mini-glossaire de la cybersécurité

Chiffrement : processus permettant de chiffrer les données pour les rendre inexploitables par toute personne autre que le destinataire visé.

Déchiffrement : processus permettant de déchiffrer les données pour les restituer dans leur format d'origine.

Clé : formule mathématique, ou algorithme, utilisée pour chiffrer ou déchiffrer vos données. À l'image des cadenas à combinaison multi-chiffres, plus la clé de chiffrement est longue (en nombre de bits), plus le cryptage est fort.

Navigateur : logiciel utilisé pour accéder à Internet. Les navigateurs les plus courants sont Microsoft Edge, Mozilla Firefox, Apple Safari et Google Chrome.

Conclusion

La confiance est devenue un enjeu majeur et un facteur clé de compétitivité pour les acteurs de l'économie numérique. De fait, toute entreprise active sur le Net se doit d'investir dans des technologies capables de protéger ses clients et de gagner leur confiance. Pour ce faire, rien ne vaut un certificat TLS/SSL d'une AC réputée et une marque de confiance bien positionnée.

DigiCert s'impose aujourd'hui comme le leader de la sécurité TLS/SSL. Des moteurs de recherche à l'acte d'achat, en passant par la navigation sur votre site, DigiCert reste ainsi à vos côtés pour renforcer la confiance de vos clients*. DigiCert sécurise plus d'un million de serveurs web dans le monde, soit plus que toute autre Autorité de certification.* Nous émettons également plus des deux-tiers du parc mondial de certificats TLS/SSL EV, y compris pour les plus grands noms du commerce en ligne et du secteur bancaire.* Avec DigiCert, vous faites le choix de la sérénité : votre site web et votre image sont protégés par un partenaire de sécurité au parcours et à la réputation irréprochables.

Pour plus d'informations, retrouvez-nous sur : https://resources.digicert.com/ssl-tls.

* DigiCert ainsi que ses filiales et ses revendeurs.

Pour plus d'informations, écrivez à nos experts en sécurité à contactus@digicert.com

Amériques

Lehi, Utah, États-Unis
2801 North Thanksgiving Way, Lehi, Utah 84043, États-Unis

Mountain View, Californie, États-Unis
485 Clyde Ave., Mountain View, Californie 94043, États-Unis

Asie-Pacifique, Japon

Bangalore, Inde
RMZ Eco World, 10th Floor, 8B Campus, Marathalli Outer Ring Road, Bangalore - 560103, Inde

Melbourne, Australie
437 St Kilda Road, Melbourne, 3004, Australie

Tokyo, Japon
Ginza Six 8F, 6-10-1 Ginza Chuo-Ku, Tokyo, 104-0061, Japon

Europe, Moyen-Orient, Afrique

Nieuwegein, Pays-Bas
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein, Pays-Bas

Le Cap, Afrique du Sud
Gateway Building, Century Blvd & Century Way 1, Century City, 7441, Le Cap, Afrique du Sud

Dublin, Irlande
Block 21 Beckett Way, Park West Business Park, Dublin 12, D12 C9YE, Irlande

Saint-Gall, Suisse
Poststrasse 17, Saint-Gall, Suisse, 9000

Londres, Angleterre
7th Floor, Exchange Tower, 2 Harbour Exchange Square, Londres, E14 9GE, Angleterre

Malines, Belgique
Schaliënhoevedreef 20T, 2800 Malines, Belgique

Munich, Allemagne
Ismaninger Strasse 52, 81675 Munich, Allemagne

digicert®