

Installation et utilisation de vos certificats SSL

Le guide des bonnes pratiques





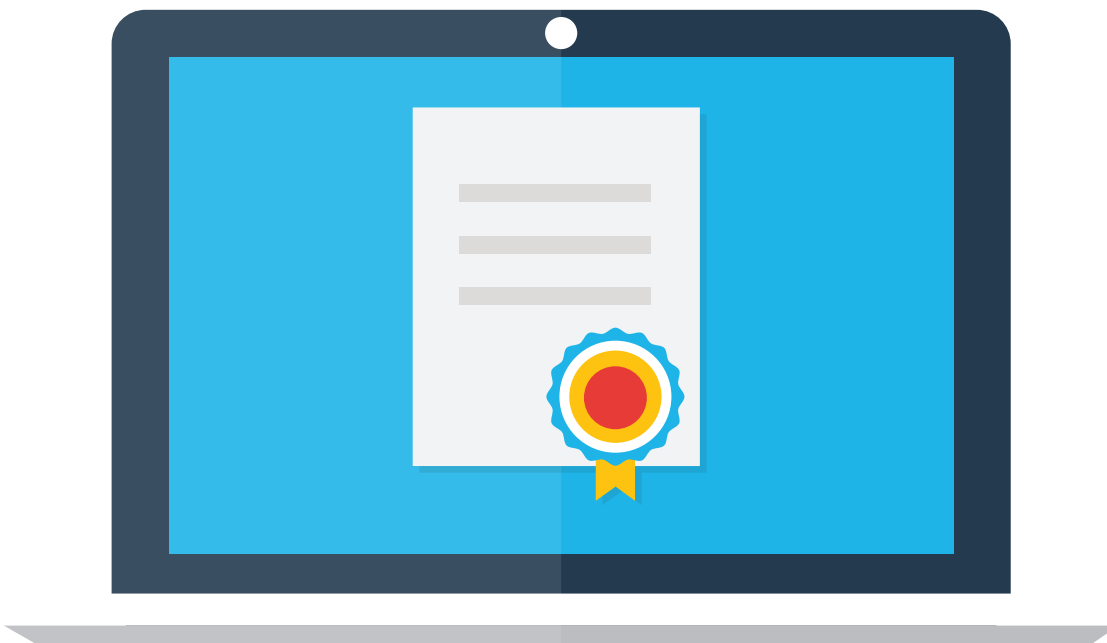
En achetant un certificat Symantec SSL, vous avez fait le bon choix.

Mais l'achat d'un certificat ne constitue que la première des nombreuses étapes à suivre pour sécuriser votre site Web. Trop souvent, les certificats ne sont pas correctement installés, des pages à risque restent non sécurisées et les informations saisies dans les formulaires sont transmises sans cryptage, laissant ainsi de nombreux sites Web vulnérables aux attaques.

Pour toutes ces raisons, Symantec a élaboré ce guide de recommandations destinées à sécuriser rigoureusement votre site Web dès le départ. Pour tenir le cap dans les eaux troubles du Web, nous y dressons un état des lieux des méthodes utilisées par les hackers pour saper la protection SSL, mais aussi et surtout des parades disponibles. Car un certificat SSL est et reste un élément indispensable de la sécurisation de votre site – pour vous-même, vos collaborateurs et vos clients.

Une seule méthode d'installation : la bonne

À l'instar de nombreuses entreprises, vous avez identifié la nécessité d'acquérir un certificat SSL et entrepris de franchir cette étape essentielle. À présent, vous devez veiller à l'installer correctement. Car si vos clients ne se sentent pas totalement protégés sur votre site, ils ne feront pas affaire avec vous. Tout simplement.





CONSEIL N°1 : préparez la clé privée et la requête CSR



Pour installer un certificat SSL, vous devez en premier lieu créer la clé privée, puis la requête de signature de certificat (CSR, *Certificate Signing Request*) à partir de cette clé privée, pour le serveur sur lequel le certificat sera installé. Ensuite, il ne vous reste qu'à envoyer la CSR pour inscrire le certificat en question. Suivez le guide...

Si vous exploitez des serveurs IIS 6 (et versions supérieures) ou des serveurs Linux Redhat, vous pouvez télécharger notre utilitaire [Assistant SSL Symantec](#) et suivre les instructions à l'écran. Pour consulter les modes de création d'une CSR (*Certificate Signing Request*) sur d'autres serveurs, visitez la page [Génération d'une CSR Symantec](#). Pour vous inscrire à un des services de certificat Symantec SSL, vous devrez communiquer les informations suivantes :

- La durée ou période de validité du certificat : 1, 2 ou 3 ans
- Le nombre de serveurs hébergeant un même domaine (jusqu'à cinq serveurs)
- La plate-forme serveur
- L'entité, l'unité organisationnelle et l'adresse
- Les coordonnées de paiement et de contact pour la facturation
- Le nom commun, composé du nom d'hôte et du nom de domaine, par exemple « `www.mondomaine.com` » ou « `webmail.mondomaine.com` »
- L'adresse e-mail à laquelle Symantec peut vous contacter pour valider les informations
- Une CSR générée à partir du serveur à sécuriser

Une fois que vous avez reçu votre certificat, suivez les instructions du Conseil n°3.

Si votre serveur n'est pas répertorié ou si vous souhaitez des informations supplémentaires, reportez-vous à la documentation de votre serveur ou prenez contact avec le constructeur. Si vous ignorez la configuration logicielle de votre serveur, contactez vos administrateurs informatiques.

Pendant le processus d'inscription, veillez à envoyer la CSR accompagnée des séparateurs de début et de fin :

-----BEGIN CERTIFICATE SIGNING REQUEST-----

XXXXXXX

-----END CERTIFICATE SIGNING REQUEST-----



CONSEIL N°2 : suivez la bonne méthode d'installation de votre certificat SSL



Vous installez un certificat SSL pour la première fois et l'idée vous intimide ? Pas d'inquiétude : l'opération est beaucoup plus simple qu'il n'y paraît. Découvrons ensemble comment installer un certificat sur un serveur.

Tous les serveurs suivent la même logique :

Étape 1 : enregistrement du certificat

Suivez les instructions indiquées dans votre e-mail de confirmation pour enregistrer le certificat SSL sur votre poste de travail à partir de l'URL fournie. Cette procédure vous permettra d'obtenir votre certificat et les certificats d'AC intermédiaires nécessaires.

Étape 2 : installation ou déplacement dans un dossier de certificat

Étape 3 : configuration du certificat sur le site Web

Étape 4 : référencement du certificat

Pour obtenir des informations détaillées et des instructions pas à pas pour chaque type de serveur, [cliquez ici](#).

Pour exploiter tous les avantages de votre certificat SSL, veillez à bien afficher le sceau Norton Secured sur votre site Web. Sa présence rassurera vos clients quant au niveau de sécurité que vous leur proposez.

Pour ce faire, il vous suffit de copier-coller les lignes de code de la page Norton Secured sur votre site. Tous les détails sont disponibles sur le lien fourni plus bas. Vous y découvrirez également comment tester votre certificat à l'aide de notre outil Certificate Installation Checker, en saisissant le nom de votre domaine lorsque vous y êtes invité.

Votre certificat SSL est désormais installé et opérationnel.

En cas de problème

Symantec propose une série de tutoriels vidéos pour divers serveurs : [Visionner les tutoriels](#)

Vérification de votre installation

Il vous suffit d'entrer l'URL du serveur à vérifier : [Vérifier l'installation](#)

Génération du sceau pour votre site

Instructions d'installation du sceau Norton Secured : [Générer le sceau](#)

Dépannage

Visitez le site de support Symantec : [Accéder au support technique](#)



CONSEIL N°3 : optez pour la meilleure méthode de protection de vos clés privées



Les clés publiques et privées sont les chevilles ouvrières du protocole SSL. La clé privée, qui reste secrète sur votre serveur, sert à crypter tout le contenu du site Web. Quant à la clé publique, elle est placée au sein même du certificat et contient d'autres éléments de l'identité de votre site Web, notamment le nom du domaine et les coordonnées de votre société.

Vos clés privées doivent être considérées comme des informations ultra sensibles, connues seulement d'un nombre restreint de collaborateurs ou d'associés de confiance. Imaginez-vous un instant directeur d'agence bancaire : donneriez-vous les clés du coffre à n'importe qui ? Bien sûr que non. Voici donc quelques bonnes pratiques à appliquer :

- **Générez vos clés privées sur un serveur de confiance.** Ne délégez jamais cette opération à un tiers !
- **Protégez les clés privées par mot de passe** afin d'éviter toute compromission lors de leur stockage sur vos systèmes de sauvegarde.
- **Renouvelez vos certificats chaque année** et profitez de cette occasion pour créer de nouvelles clés privées.

La longueur de la clé privée influe considérablement sur la négociation cryptographique servant à établir les connexions sécurisées. L'utilisation d'une clé trop courte réduit le niveau de protection, mais une clé trop longue peut ralentir considérablement le trafic.

Le cryptage ECC (*Elliptic Curve Cryptography*) gagne actuellement du terrain, car il assure un niveau de protection élevé malgré des clés moins longues. Symantec propose donc un cryptage ECC associé à des clés beaucoup plus courtes que celles imposées par les technologies RSA et DSA, mais pourtant plus de 10 000 fois plus difficiles à décoder (la sécurité cryptographique d'une clé ECC 256 bits équivaut à celle d'une clé RSA de 3072 bits). ECC permet donc de gagner en sécurité tout en sollicitant moins les ressources du serveur et en réduisant le nombre de cycles processeurs nécessaires aux opérations cryptographiques.

Un complément d'information sur le cryptage ECC est disponible à la page 7.



CONSEIL N°4 : éliminez les éventuels maillons faibles de la chaîne



Dans la majorité des déploiements SSL, le certificat serveur à lui seul ne suffit pas : trois certificats au moins sont nécessaires pour former une chaîne de confiance complète. Une chaîne de certification est composée de tous les certificats nécessaires à l'authentification de l'entité identifiée par le certificat final.

En pratique, cette chaîne contient le certificat de l'entité finale, les certificats d'AC intermédiaires et le certificat d'AC racine.

Le processus permettant de vérifier l'authenticité et la validité d'un nouveau certificat suppose la vérification de tous les certificats d'une AC racine unanimement reconnue et des AC intermédiaires, jusqu'au certificat nouvellement reçu, à savoir le certificat de l'entité finale. Un certificat n'est réputé fiable que lorsque tous les certificats de cette chaîne ont été émis et validés dans les règles.

Or, l'une des erreurs courantes consiste à bien configurer le certificat pour l'entité finale, mais à oublier d'y inclure les certificats d'AC intermédiaires. Pour vérifier la bonne installation des certificats intermédiaires, utilisez le [Certificate Installation Checker](#).



CONSEIL N°5 : réfléchissez à l'importance des longueurs de clés dans RSA et ECC



Le cryptage ECC (*Elliptic Curve Cryptography*) offre à votre entreprise une protection renforcée, avec en prime des gains de performance par rapport au cryptage actuel.

Homologuée par la NSA et les pouvoirs publics américains, la méthode de cryptage ECC crée des paires de clés publique/privée en se basant sur les points d'une courbe elliptique. Difficile à décoder via les attaques par force brute privilégiées des hackers, cette méthode est aussi plus performante et moins gourmande en ressources informatiques que le cryptage RSA.

RSA est un algorithme de cryptage et de signature numérique au cœur de la sécurité Internet depuis presque deux décennies. Toujours en vigueur actuellement, la longueur minimale acceptable de sa clé a progressivement augmenté pour neutraliser des attaques cryptographiques de plus en plus puissantes. Avec ECC, vous renforcez à la fois la sécurité et la performance grâce à des clés plus courtes. Ainsi, une clé ECC de 256 bits procure une protection équivalente à une clé RSA de 3072 bits. Résultat : vous bénéficiez de la sécurité recherchée, sans aucun compromis sur la performance.

De même, la compacité des clés ECC réduit la consommation de bande passante. À l'heure où vos clients sont de plus en plus nombreux à réaliser leurs transactions en ligne sur des appareils mobiles, ECC contribue à fluidifier l'expérience utilisateur.

Les racines ECC de Symantec sont disponibles dans les trois grands navigateurs Internet depuis 2007. Par conséquent, les certificats ECC de Symantec seront compatibles avec votre infrastructure existante – sans aucun surcoût pour vous –, dès lors que vous utilisez des navigateurs à jour.

Plus d'infos sur [ECC et les options d'algorithme possibles](#).



CONSEIL N°6 : optez pour une protection intégrale « Always-On SSL »



Vous devez systématiquement chercher à crypter par SSL l'intégralité de votre site Web. Et Always-On SSL est le meilleur moyen d'y parvenir. Ce dispositif de sécurité protège l'intégralité de l'expérience utilisateur, de la connexion à la déconnexion. Les internautes peuvent ainsi effectuer des recherches, faire des achats et partager des informations en toute sécurité.

Always-On SSL s'impose comme une évidence aux entreprises soucieuses de protéger leurs clients et leur réputation au moyen des certificats SSL d'une AC de confiance comme Symantec. Facile à déployer, Always-On SSL authentifie l'identité d'un site Web et crypte toutes les informations échangées entre ce site et les internautes (y compris les cookies). Résultat : ces informations sont protégées contre toute visualisation, modification ou utilisation non autorisée.

À cet égard, l'Online Trust Alliance incite les sites Web à adopter le dispositif Always-On SSL. L'organisme précise : « Always-On SSL est une mesure de sécurité pratique et éprouvée qui devrait être mise en œuvre sur tous les sites Web où les visiteurs partagent ou consultent des informations sensibles ».

De nombreux sites parmi les plus visités au monde ont déjà pris conscience de l'intérêt d'une mise en œuvre d'Always-On SSL. Ils se protègent ainsi contre les détournements de session (« *sidejacking* ») et les attaques de type Firesheep ou par injection de code malveillant.

Avec Always-On SSL, vous envoyez un message de confiance fort aux internautes en leur prouvant votre sérieux sur les questions de sécurité et de confidentialité, ainsi que votre engagement à prendre toutes les dispositions nécessaires pour garantir leur protection sur Internet.



CONSEIL N°7 : jouez la carte de la confiance avec le Public Key Pinning



L'extension Public Key Pinning pour HTTP est un mécanisme de vérification permettant aux exploitants de sites Web de définir les autorités de certification autorisées à émettre des certificats pour leurs serveurs.

Essentiellement, l'extension *Public Key Pinning* (PKP) associe un hôte à son certificat ou sa clé publique attendue. Dès lors qu'une clé publique est connue ou visible pour un hôte, elle est associée, ou « épinglée », à cet hôte (d'où le terme anglais de « pinning »).

D'après le CA Security Council, le PKP permet au propriétaire du site Web d'imposer une ou plusieurs règles à ses certificats SSL :

- Clé publique spécifiée
- Signature du certificat par une AC au moyen de cette clé publique
- Vérification en cascade jusqu'à une AC avec cette clé publique

Lorsqu'un certificat est émis par une AC non répertoriée (c'est-à-dire non épinglée) pour le domaine en question, tout navigateur compatible avec l'extension PKP le signale par un avertissement de sécurité. Les propriétaires de sites Web peuvent également épingler plusieurs clés issues de plusieurs AC, que les navigateurs considéreront alors toutes comme valides.

En recourant au PKP, le propriétaire d'un site Web s'assure que les AC n'émettront pas par erreur un certificat pour son domaine. En outre, ces AC limitent souvent le nombre d'utilisateurs habilités à demander l'émission d'un certificat pour les domaines concernés. Cette restriction supplémentaire renforce de fait le dispositif de prévention de toute émission de certificat à des tiers non habilités.

Malheureusement, le CA Security Council stipule que le mécanisme PKP mis en place par Google en 2011 manque d'évolutivité, car il impose d'ajouter les clés publiques pour chaque domaine au navigateur. Une nouvelle solution PKP plus évolutive est actuellement en cours d'élaboration par l'intermédiaire d'un document IETF RFC (*Internet Engineering Task Force Request for Comments*).

Dans cette version préliminaire, les associations ou « épingles » PKP sont définies dans un en-tête HTTP du serveur au navigateur. Les options de l'en-tête peuvent par exemple contenir un algorithme à clé SHA-1 et/ou SHA-256, la durée maximale de l'association, l'éventuelle prise en charge de sous-domaines et le degré de rigueur de l'association.



CONSEIL N°8 : lutez contre les interceptions avec la confidentialité persistante



Que diriez-vous si un espion interceptait votre trafic Web d'aujourd'hui pour mieux le déchiffrer demain ? Vous seriez évidemment inquiet. C'est pourtant bien ce qui pourrait vous arriver à votre insu.

Prenez le cas du cryptage RSA. Il génère des clés publiques et privées pour le cryptage et le décryptage des messages. Or, l'utilisation de clés récupérables pourrait exposer les données cryptées stockées en cas de compromission ultérieure des clés. Dans de nombreux cas, un pirate ayant enregistré votre trafic SSL et disposant de votre clé privée pourra utiliser cette dernière pour décrypter toutes les clés de session créées au cours des négociations SSL enregistrées, puis décrypter tous les enregistrements des données de session au moyen de ces clés de session. Un tel scénario n'est naturellement guère rassurant, mais la parade existe. Son nom : « Perfect Forward Secrecy » (PFS), ou confidentialité persistante.

Avec la PFS, des clés de session provisoires et non récupérables sont générées, utilisées puis éliminées. Dès lors qu'elle est correctement mise en œuvre avec ECC (voir Conseil n°5), la PFS s'avère non seulement plus sûre que les algorithmes RSA, mais également plus performante.

La PFS efface tout lien entre la clé privée du serveur et les clés de session. Si le client et le serveur sont tous deux compatibles PFS, ils utilisent la variante d'un protocole dit de Diffie-Hellman (du nom de ses inventeurs) pour échanger en toute sécurité des nombres aléatoires et parvenir au même secret partagé. Grâce à cet algorithme ingénieux, un espion intercepteur ne pourra pas s'immiscer dans ce secret, même s'il a pu intercepter la totalité du trafic.

Pour en savoir plus, reportez-vous à cette infographie Symantec :
[Télécharger l'infographie](#)



CONSEIL N°9 : tendez un filet de protection avec HTTP Strict Transport Security



Sur Internet, la sécurité est en enjeu vital. Parfois, cela suppose de dépasser le simple cadre de la sécurité standard pour parvenir au niveau de protection souhaité.

Les hackers ont les armes pour intercepter les communications sur les réseaux sans fil, notamment par la méthode « *SSL Stripping* » qui consiste à capter les requêtes des navigateurs aux sites HTTPS et à renvoyer les pages demandées par HTTP. La connexion n'étant alors plus cryptée, le hacker n'a plus qu'à intercepter les informations saisies par la victime sur le site Web prétendument sécurisé. D'autant que la victime ne s'apercevra souvent jamais du subterfuge car elle ne prête pas forcément attention à la barre d'adresse de chaque nouvelle page Web visitée. Et comme les navigateurs n'ont aucun moyen de savoir si la page téléchargée est censée être sécurisée, ils ne vous avertissent pas si la connexion n'est pas cryptée.

C'est là que la méthode HSTS (HTTP Strict Transport Security) intervient pour permettre aux serveurs d'envoyer au navigateur un message exigeant le cryptage de la connexion en cours. Le navigateur réagit alors en cryptant chaque page Web visitée par l'internaute, vous protégeant ainsi, vous et vos clients, contre ce type d'attaque.

Pour activer la protection HSTS, il vous suffit de définir un en-tête de réponse sur vos sites Web. Dès lors, les navigateurs qui prennent en charge HSTS (parmi lesquels Chromium, Google Chrome, Firefox, Opera ou Safari) suivront vos instructions. Une fois activé, HSTS interdit toute communication non sécurisée avec votre site Web. Pour ce faire, il convertit automatiquement tous les liens en texte clair en liens sécurisés.

Internet Explorer n'est pas encore compatible avec HSTS, mais Microsoft promet d'y remédier avec Internet Explorer 12.

© 2015 Symantec Corporation. Tous droits réservés.
Symantec, le logo Symantec, le logo en forme de coche et le logo Norton Secured sont des marques commerciales ou des marques déposées de Symantec Corporation ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms peuvent être des marques commerciales de leurs détenteurs respectifs.