# Certificats SSL Extended Validation : un gage de confiance absolue

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

thawte

# certificats SSL Extended Validation : un gage de confiance absolue

Pour de nombreux particuliers, la méfiance reste de mise sur le Net. Cette réserve freine le développement des achats en ligne, des transactions bancaires et autres opérations nécessitant la transmission d'informations sensibles sur Internet. L›explosion des arnaques en ligne, comme le phishing et le pharming (détournement d'URL), entretient un climat d'incertitude anxiogène.

Selon un rapport Gartner publié en 2006, 41 % des adultes américains ont déjà reçu des arnaques par e-mail de type phishing. Inquiets pour leur sécurité, 46 % ont modifié leur comportement sur la Toile et les sites marchands, et 10 % ont divisé par deux leur volume d'achats en ligne. Résultat : les e-commerçants estiment à près de 2 milliards de dollars (environ 1,5 milliards d'euros) le manque à gagner engendré par ce déficit de confiance des cyberconsommateurs.

Lorsque le protocole SSL est apparu, la sécurité sur Internet était une affaire relativement simple : soit un site Web avait besoin du niveau de cryptage et d'authentification fourni par les certificats SSL, soit il n'en avait pas besoin. La démarche s'arrêtait là. Aujourd'hui, la sécurité en ligne recouvre une réalité plus fine. Si certains sites Web ne nécessitent qu'un système de cryptage simple pour protéger les identifiants de leurs utilisateurs, d'autres doivent traiter des informations personnelles extrêmement sensibles et requièrent un cryptage fort assorti d'un système de vérification complète de l'identité des propriétaires des sites Web.

Certaines autorités de certification (AC) comme Thawte ont donc diversifié leur offre pour répondre à ces différents objectifs. Plus économiques et rapides à obtenir, les certificats de validation de domaine **Thawte® SSL123** sont particulièrement adaptés aux sites Web n'exigeant qu'un cryptage simple et un niveau minimum de vérification d'identité. En revanche, pour les sites gérant des données personnelles particulièrement sensibles, Thawte propose ses **certificats SSL Extended Validation (EV)**.

La norme EV a été établie par le CA/Browser Forum, un consortium indépendant également à l'origine des nombreuses directives d'audit destinées à définir et contrôler les procédures de validation et d'émission de ces certificats EV. La présence de certificats EV sur un site se repère à des indices spécifiques affichés par le navigateur. Ces différents signaux ont pour objectif de rassurer les internautes sur l'entité exploitant le site et la sécurité de la connexion. Les dernières versions des principaux navigateurs Web prennent en charge les certificats EV. Quant aux sites marchands et bancaires les plus fréquentés de la Toile, ils utilisent des certificats EV pour renforcer la confiance de leurs clients.

## À qui faites-vous confiance ?

La mission des certificats SSL est double :

- Authentifier le site Web d'une société
- Crypter les échanges entre le serveur Web et le navigateur de l'internaute

N'importe quel certificat numérique – avec son binôme clé publique/clé privée – peut être utilisé pour crypter des données. Toutefois, le niveau de **confiance** que suscite un certificat SSL dépend des procédures de vérification des identités utilisées par l'AC émettrice du certificat. Il appartient à cette autorité de certification d'identifier le propriétaire du domaine auquel le certificat SSL sera associé, mais aussi de s'assurer de la

légitimité et du sérieux de ce même propriétaire. Une connexion SSL doit ensuite permettre de rassurer les internautes : sur un site Web de phishing (site frauduleux se faisant passer pour un site licite), soit les internautes ne pourront tout bonnement pas établir de connexion SSL, soit le certificat SSL en place leur révélera que l'entité sous-jacente ne correspond pas à l'entité censée exploiter le site. Cependant, au fil du temps, les certificats SSL classiques ont commencé, dans certains cas, à faillir à leurs obligations.

## Les problèmes des certificats SSL classiques

Pour les cybercriminels, la contrefaçon de sites marchands n'a jamais posé problème. En 1995, à l'époque des premiers certificats SSL, les arnaques sur la Toile étaient rarissimes. Les certificats SSL classiques offraient un niveau de sécurité suffisant pour rassurer les internautes. Il n'y avait que peu, voire aucune tentative délibérée d'usurpation de site d'e-commerce officiel. Pour la plupart des internautes, la simple présence d'un cadenas dans leur navigateur – confirmant l'établissement d'une connexion SSL – constituait un gage de confiance suffisant.

Les temps ont bien changé. Les arnaques se sont sophistiquées et les cybercriminels parviennent souvent à se procurer des certificats SSL avec validation de nom de domaine, sans validation de leur identité ni de celle de leur société. Résultat : certains sites Web frauduleux établissent parfois une connexion SSL, aussi limitée soit-elle. En apercevant le cadenas, l'internaute pense se trouver sur un site légitime et poursuit sa navigation sur le site frauduleux. Bien entendu, l'internaute lambda pourrait étudier de plus près le certificat depuis son navigateur, mais peu d'utilisateurs sont suffisamment versés dans la technique pour saisir l'importance de cette démarche.

Certains usurpateurs parviennent même à obtenir des certificats SSL complets de la part d'AC moins regardantes. En clair, cela signifie que des cybercriminels peuvent obtenir des certificats numériques attestant d'une identité frauduleuse. Dans ces cas, même l'internaute le plus averti qui étudie le certificat SSL présenté par le site peut être dupé. C'est là que les certificats EV prennent tout leur intérêt.

## Certificats SSL EV

Aboutissement d'une démarche commune entre autorités de certification et éditeurs de navigateurs, les certificats SSL EV présentent deux avantages majeurs par rapport aux certificats SSL classiques :

- Une meilleure visibilité du certificat EV dans l'interface utilisateur du navigateur
- Une vérification plus poussée de l'identité des demandeurs de certificats par les AC habilitées à émettre des certificats SSL EV

Le consortium CA/Browser Forum rassemble plus de 20 éditeurs de navigateurs, autorités de certification et auditeurs WebTrust, ainsi que le comité de sécurité de l'information de l›American Bar Association (ABA-ISC). La norme EV évolue en permanence pour s'adapter et contrer les nouvelles formes de cyberfraude. De fait, les directives d'émission de certificats EV définissent un ensemble de bonnes pratiques et de standards auxquels les AC émettrices de certificats EV doivent se conformer. Les autorités de certification doivent également se soumettre régulièrement à des audits indépendants destinés à valider l'adhésion de leurs processus avec ces directives et d'attester de leur habilitation à émettre des certificats SSL EV.

Sur le plan technique, un certificat EV fonctionne exactement comme un certificat SSL classique, et ce même sur les navigateurs plus anciens ne prenant pas explicitement en charge la norme EV. Les navigateurs récents reconnaissent quant à eux les éléments clés d'un certificat EV et en affichent des indices visuels sur l'interface utilisateur. L›internaute bénéficie ainsi d'un accès immédiat aux informations de sécurité et de confiance.

## Améliorations côté utilisateur

L'un des avantages critiques de la norme EV est de communiquer plus clairement les informations d'identité et de confiance sur les navigateurs Web, une évolution considérable pour l'internaute. Pour ce faire, la norme EV s'articule autour d'un certain nombre de bonnes pratiques.

### VERT COMME CONFIANCE

En tête de ces innovations côté utilisateur, la barre de navigation verte – symbole universel de sécurité – pour indiquer la présence d'un certificat EV valide. Si les indices visuels de sécurité diffèrent selon les navigateurs, le code couleur, lui, reste immuablement vert. Tous affichent le nom de la société – et non le domaine du site Web – à laquelle le certificat EV a été délivré (voir Figure 1). Dans certains navigateurs, le nom de la société s'affiche en alternance avec le nom de l'AC émettrice du certificat EV. Le but : informer clairement les internautes sur l'organisme ayant validé l'identité de l'opérateur du site.

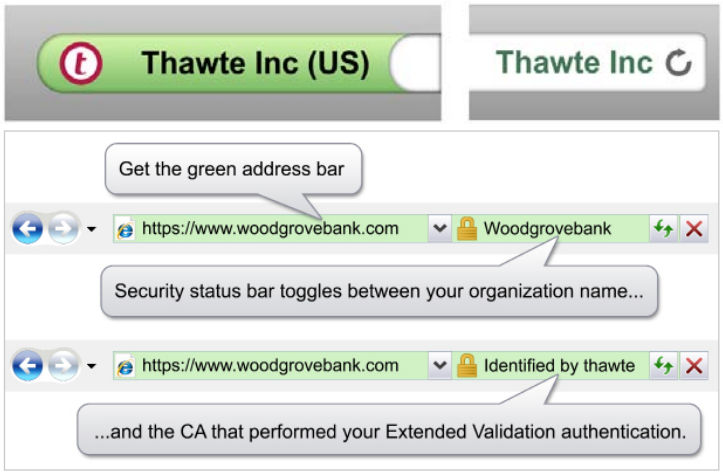


*Figure 1 : indices visuels permettant aux internautes de reconnaître un certificat EV actif.*

Avec un certificat SSL classique, un site frauduleux ne sera pas en mesure d'afficher la barre d'adresse verte. Il est d'ailleurs impossible pour un tel site d'obtenir un certificat EV valide en raison de l'exhaustivité des procédures de vérification d'identité obligatoires. Même s'il essayait de duper les internautes avec un certificat EV au nom de sa propre société, l'internaute verrait apparaître le nom de cette société-là dans la barre d'adresse verte. Conséquence : la discordance entre la barre d'adresse et le nom du site frauduleux mettrait inévitablement la puce à l'oreille des internautes.

### CONTRÔLES DE VALIDITÉ EN TEMPS RÉEL

Les navigateurs Web prennent pratiquement tous en charge le protocole OCSP (Online Certificate Status Protocol) pour la réalisation, en temps réel, de contrôles de validité des certificats EV. Grâce au protocole OCSP, le navigateur vérifie la validité du certificat EV directement auprès de l'AC émettrice de ce certificat. L'opération s'effectue entièrement en ligne et quasiment instantanément dès la première présentation du certificat EV au navigateur. Ces contrôles en temps réel permettent de s'assurer que le certificat EV n'a pas été révoqué entre temps, offrant ainsi un niveau de sécurité supplémentaire. La barre verte n'apparaît dans le navigateur qu'une fois ces contrôles de validité en temps réel effectués. Cette fonctionnalité est automatiquement activée dans la plupart des navigateurs récents avec les options de filtre anti-phishing.

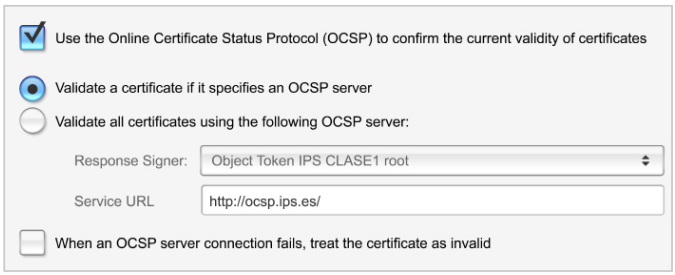


*Figure 2 : activation du protocole OCSP pour des contrôles en temps réel de la validité des certificats EV.*

### EV UPGRADER™ POUR WINDOWS XP

Une quantité phénoménale d'ordinateurs continuent de fonctionner sous Microsoft Windows XP avec Internet Explorer 7 (IE7). Pour profiter des avantages et de tous les indices visuels des certificats EV sous IE7 (ou versions ultérieures), les utilisateurs devront probablement effectuer une mise à niveau de leur magasin de certificats racine. Pour faciliter l'opération, Thawte met gratuitement à disposition son EV Upgrader™ qui permet d'effectuer une mise à niveau automatique d'IE7 sur les clients Windows XP.

Il vous faut pour cela installer EV Upgrader sur votre site Web, avec votre certificat EV. L'outil de mise à niveau déclenche des fonctions Windows XP intégrées en toute transparence pour l'internaute. Il suffit ensuite d'une première visite sur un site intégrant EV Upgrader pour que s'affichent automatiquement les conventions d'interface EV dans le navigateur IE7, dès lors que l'utilisateur visite un site protégé par un certificat Thawte SSL EV.

En intégrant EV Upgrader au sceau de confiance Thawte®, Thawte facilite son installation sur votre site Web. Il vous suffit d'insérer le sceau sur votre page Web pour permettre à chaque client Windows XP exécutant IE7 de mettre automatiquement à niveau ses fonctions EV à chacune de ses visites sur votre site.

## Les solutions SSL EV signées de Thawte

Compatibles avec un large éventail de navigateurs Web, les certificats Thawte SSL EV proposent plusieurs niveaux de cryptage : 256 bits, 128 bits, 56 bits et 40 bits. Les navigateurs sélectionnent automatiquement le niveau de cryptage le plus élevé qu'ils puissent prendre en charge. Les certificats Thawte SSL EV sont entièrement conformes aux directives et obligations du CA/Browser Forum. Thawte se soumet par ailleurs régulièrement à des audits de conformité.

## Liens utiles

Nous vous invitons à consulter nos liens utiles :

- Pour plus d'infos sur les certificats Thawte SSL EV et pour acheter votre certificat EV en ligne : http://www.thawte.fr/ssl/extended-validation-ssl-certificates/index.html
- Pour consulter la rubrique Foire Aux Questions de Thawte : http://www.thawte.fr/resources/ssl-information-center/inspire-trust-online/extended-validation-ssl-faq/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