



DOCUMENT TECHNIQUE

Maximiser la confiance des
internautes au moyen de SSL
Extended Validation





SOMMAIRE

+ L'érosion de la garantie d'identité SSL	3
+ Présenter une identité qui met en confiance les visiteurs	4
Internet Explorer 7 : feu vert	4
+ Comment fonctionne Extended Validation ?	7
+ EV Upgrader élargit la protection aux clients Windows XP	8



Le commerce électronique est confronté à une crise de confiance. La confiance que les utilisateurs témoignent à la sécurité des sites est en berne. Les consommateurs sont toujours plus nombreux à modérer la fréquence de leurs achats en ligne, voire à y renoncer complètement. Selon une étude réalisée par Forrester Research le 8 décembre 2005, pas moins de 24 % des internautes avaient déclaré leur intention de renoncer au cybershopping pour les fêtes de fin d'année, se disant peu rassurés à cette idée. 61 % avaient confié avoir au moins restreint leurs achats en ligne pour la même raison. Bien que ce phénomène ait été masqué par la hausse généralisée des activités en ligne (banque, négoce de titres et déclarations fiscales), le fait est que de nombreuses entreprises de détail actives sur la Toile sont moins performantes que ce qu'elles pourraient être et perdent de l'argent dans l'aventure.

Début 2007, les cyberentreprises seront en mesure d'apporter définitivement la preuve de leur identité à leurs clients. Ces derniers auront à leur tour l'occasion de confirmer cette dernière auprès de sites de confiance. Cette possibilité est le fruit de l'évolution la plus importante que le réseau fédérateur de sécurisation du Web ait connu en dix ans. Il s'agit du lancement d'un certificat SSL d'un nouveau genre, le premier à faire son apparition depuis les premiers pas de cette technologie il y a plus de dix ans.

Ces nouveaux certificats, appelés certificats SSL Extended Validation (Validation étendue, EV), représentent plus d'une année d'efforts consentis par le CA/Browser Forum, un consortium sectoriel réunissant les principaux éditeurs de navigateurs Web et les autorités de certification SSL (AC) telles que VeriSign. Fin 2006, les membres du CA/Browser Forum ont mis ces nouveaux certificats à disposition dans l'intérêt tant des cyberentreprises que des internautes. Ces certificats peuvent faciliter le commerce en ligne sous toutes ses formes, en renforçant la confiance des visiteurs dans des sites légitimes et en endiguant nettement l'efficacité des attaques de phishing.

L'érosion de la garantie d'identité SSL

Demandez à un cyberacheteur lambda de vous dire à quoi sert ce petit verrou qui s'affiche dans son navigateur Internet et il vous répondra qu'il assure le chiffrement des transmissions pour les mettre à l'abri des regards indiscrets. Même si l'explication est correcte d'un point de vue technique, ce n'est qu'une infime partie de ce que les premiers pionniers du commerce électronique entendaient lui donner comme signification.

L'objectif premier des certificats SSL était de valider l'identité d'un site lors de la connexion d'un utilisateur. Bien qu'il soit difficile de plagier physiquement l'identité d'une entreprise, il est en revanche aisé de s'y substituer en ligne. Le secteur l'a bien compris dès 1995 et a donc inventé les certificats SSL. Ses créateurs voulaient que le certificat se porte garant de l'identité du site et protège ainsi les cyberacheteurs des arnaques potentielles. Au début, la garantie d'identité d'un certificat SSL standard suffisait amplement. Ce n'est plus le cas de nos jours. L'usage généralisé de la Toile par des novices dépourvus de formation spéciale en informatique, associé au manque de visibilité du verrou sur les navigateurs les plus courants, ont en effet permis au phishing (hameçonnage) de devenir le phénomène qu'il est aujourd'hui.

En dépit de leurs intentions initiales, les certificats SSL classiques ne suffisent plus. Certaines autorités de certification sont passées maîtres dans l'art de l'authentification ; d'autres se ménagent ou mettent en œuvre des pratiques qu'il est facile de contourner. Un site peut même utiliser un certificat SSL auto-signé totalement dénué d'authentification de l'identité. Au second semestre 2005, la Toile a ainsi été le théâtre d'attaques de phishing de grande ampleur, tirant parti du faible niveau d'authentification (certificats SSL de type « cible molle ») pour donner l'illusion de la légitimité.

Présenter une identité qui met en confiance les visiteurs

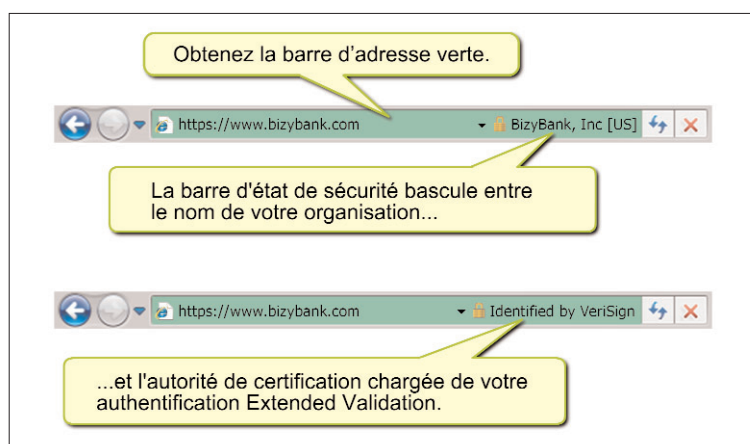
Dans le but de redorer le blason des certificats SSL comme source d'information sur l'identité du site vis-à-vis des visiteurs, les leaders du secteur ont dû remédier à deux points faibles au sein du système existant. D'abord, le secteur avait besoin d'une nouvelle catégorie de certificats SSL porteuse d'un niveau élevé de garantie en ce qui concerne l'identité du propriétaire du site. Il fallait donc disposer d'une interface navigateur qui permette aux utilisateurs de visualiser l'identité quand celle-ci était connue et d'être avertis quand elle ne l'était pas. Ces nouveaux certificats sont les certificats SSL EV susmentionnés. Certains utilisateurs les désignent par leur fonction, à savoir certificats SSL hautement sécurisés. Ceux-ci se distinguent d'ailleurs des « certificats hautement sécurisés » génériques dénués de fonction EV.

Constitué de plus de 20 éditeurs de navigateurs Web de premier plan, de fournisseurs de certificats SSL et d'auditeurs WebTrust, le CA/Browser Forum a collaboré pendant plus d'un an avec le American Bar Association Information Security Committee (ABA-ISC) en vue de donner naissance à une procédure d'authentification standardisée à laquelle chaque autorité de certification est tenue de se conformer lors de l'émission de certificats EV. Ces autorités doivent se soumettre à des audits indépendants en vue d'attester leur conformité à la procédure en question. Le CA/Browser Forum a basé cette procédure sur les pratiques de vérification existantes qui ont fait leurs preuves au fil de plusieurs années de mise en oeuvre dans l'authentification de millions de certificats SSL.

Dès qu'une autorité de certification a effectué l'authentification conformément à cette procédure, elle peut émettre un certificat dit « EV ». Ce dernier fonctionne exactement comme un certificat SSL classique. En fait, les navigateurs qui n'étaient pas conçus pour identifier les certificats EV (dont Windows® Internet Explorer® 6, Mozilla® Firefox® 2.0 et leurs prédécesseurs) se comportent exactement comme s'il s'agissait d'un certificat non EV. Cependant, les nouveaux navigateurs compatibles EV affichent ces certificats de manière bien visible et plus indicative. Le premier du genre est Internet Explorer 7 (IE7).

+ Internet Explorer 7 : feu vert

IE7 a intégré plusieurs conventions d'interface en vue d'optimiser l'identification du propriétaire du site. La plus évidente est la « barre d'adresse verte ». Lorsqu'un navigateur IE7 accède à une page dotée d'un certificat EV valide, l'arrière-plan de la barre d'adresse vire au vert. Cette simple modification indique de manière très visible que le site a fait l'objet d'une authentification d'identité de haut niveau. Le choix de la couleur répond à des conventions d'interface qui ont fait leurs preuves. Dans le jargon de la conception d'interface bureau, le vert signifie « la voie est libre », tout comme le rouge est synonyme de danger ou d'avertissement.



Des études menées auprès des consommateurs ont démontré la grande efficacité de ces conventions d'interface. À l'automne 2006, VeriSign a étudié les modalités d'utilisation et le comportement de cyberconsommateurs américains. Les résultats ont été les suivants :

- 100 % des participants ont remarqué si un site affichait ou non la barre d'adresse verte Extended Validation.
- 100 % des participants étaient plus enclins à communiquer les données de leur carte de crédit à des sites affichant la barre d'adresse verte.
- 98 % des participants ont préféré faire leurs achats sur des sites affichant la barre d'adresse verte Extended Validation.
- 80 % des participants ont déclaré qu'ils hésiteraient à effectuer leurs achats sur un site qui affichait auparavant la barre d'adresse verte Extended Validation et qui ne l'affiche plus.

IE7 comporte aussi une zone complémentaire située à droite de la barre d'adresse, appelée « Barre d'état de sécurité ». Cette zone s'affiche quand le navigateur est en mesure de fournir des informations utiles aux visiteurs du site en vue d'évaluer ce dernier. Sur les pages dotées de certificats SSL EV, la barre d'état de sécurité affiche le nom de l'entreprise. Cette chaîne de texte est directement issue du certificat, de l'endroit où l'autorité de certification l'a placée. L'autorité de certification a vérifié ce nom et le navigateur l'affiche sur son interface. Le visiteur peut donc se fier à l'authenticité de cette chaîne.

Imaginons une banque en ligne appelée BizyBank. Le nom de l'institution s'affichera directement sur l'interface du navigateur. Les consommateurs finaux pourront vérifier l'identité du site en recherchant la barre d'adresse verte et le nom BizyBank, qui, ensemble, constituent un nouvel obstacle significatif pour les hameçonneurs désireux de violer les comptes de BizyBank. De nos jours, il suffit au hameçonneur de plagier le site original et de trouver une URL convaincante pour être opérationnel. Si les clients de BizyBank prennent l'habitude de rechercher le nom de l'institution et la barre d'adresse verte avant de communiquer des informations confidentielles, le candidat hameçonneur sera dans l'impossibilité de plagier l'interface. Même si le hameçonneur venait à acheter des certificats EV par l'intermédiaire d'une entreprise existante et à les installer sur son site de phishing, l'interface du navigateur n'afficherait quand même pas le nom de BizyBank.

La barre d'état de sécurité comporte aussi le nom de l'autorité de certification ayant authentifié le certificat, ce qui permet aux clients de s'assurer de la sécurité mise en oeuvre par les sites avant d'y effectuer des transactions. S'ils n'ont pas confiance dans le fournisseur du certificat SSL approuvé, les visiteurs du site ont le loisir d'effectuer leurs achats ailleurs. Inversement, si une autorité de certification émet des certificats EV défectueux, le public apprendra à ne pas faire confiance aux sites ayant recours à cette marque de certificat SSL.

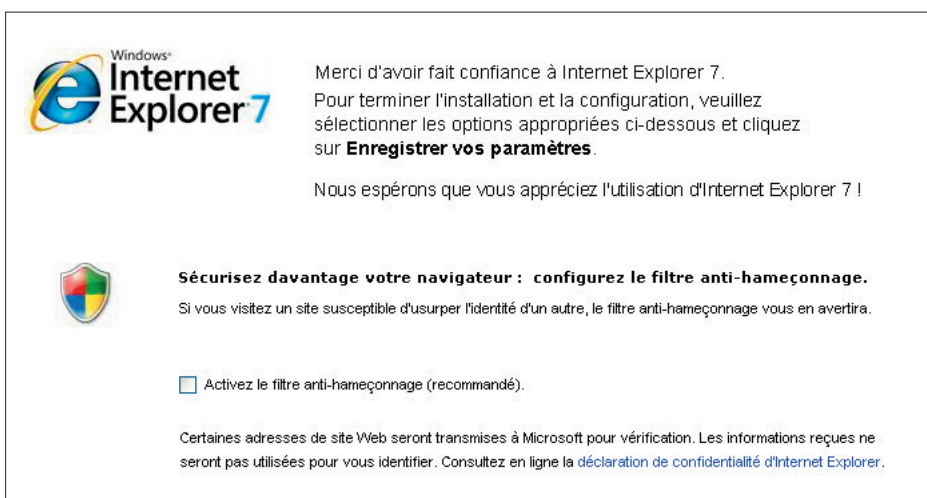
Des études indiquent que le choix de la marque du certificat SSL peut influencer la propension du visiteur à effectuer des transactions. Ainsi, le premier voyageur européen Opodo a testé une série de pages de commande identiques, avec ou sans sceau VeriSign Secured Seal™, et s'est rendu compte que les pages assorties du sceau enregistraient 10 % de ventes en plus que celles en étant dépourvues. Selon Warren Jonas, responsable de gestion de service chez Opodo : « Nous avons d'emblée mesuré l'impact que le capital confiance peut avoir sur les taux d'abandon des paniers. Depuis, nous publions le sceau VeriSign sur toutes les pages de règlement, sur l'ensemble de notre réseau de sites européens. »

En outre, en été 2006, TNS, un bureau d'études de marché de premier plan, s'est penché sur les réactions des cyberacheteurs confrontés à une série de sceaux de sécurité en ligne et a conclu que le sceau VeriSign Secured Seal était de loin la marque de confiance en ligne la plus connue au monde. L'étude indique que 56 % des cyberacheteurs du monde entier reconnaissent le sceau VeriSign Secured Seal, soit huit fois plus que pour la deuxième marque de certificat SSL la plus connue.

Ces résultats soulignent l'importance de la marque de sécurité des certificats SSL que les détaillants en ligne choisissent d'afficher sur leurs sites. Le choix délibéré d'afficher la marque de sécurité la plus célèbre sur la toile est susceptible d'accroître le volume transactionnel et donc l'efficacité globale d'un site de vente en ligne de l'ordre de 10 %, voire davantage.

Certains paramètres d'IE7 peuvent conditionner l'affichage de ces conventions d'interface. Pour que l'interface adopte ces comportements, il faut activer la fonction OCSP (Online Certificate Status Protocol) du navigateur. OCSP permet à un navigateur de vérifier en temps réel que les certificats SSL n'ont pas été révoqués. Les versions les plus récentes des navigateurs prennent en charge le protocole OCSP. Leur interface comporte aussi une commande qui permet de le désactiver. Vu la garantie de haute assurance des certificats EV, le protocole OCSP doit être activé sur IE7 pour permettre l'affichage des barres d'adresse vertes et autres conventions d'interface EV associées à tout certificat EV. Non content de savoir que le site qu'il consulte a fait l'objet d'une authentification d'identité renforcée, l'utilisateur sait aussi qu'aucun incident ne s'est produit ultérieurement, susceptible d'entraîner la révocation dudit certificat.

En plus de mettre directement en œuvre OCSP, IE7 peut aussi prendre automatiquement en charge cette fonction lorsque l'utilisateur active une autre fonctionnalité du produit qui repose sur ce protocole. Appelée « filtre anti-hameçonnage », cette fonction renforce la fonctionnalité EV en affichant les barres d'adresse en rouge ou en vert sur les sites qui répondent à certaines conditions d'activation les classant dans la catégorie des sites à risque. IE7 permet d'activer cette fonction dès l'installation et recommande même à l'utilisateur de le faire. La configuration du filtre anti-hameçonnage active aussi l'interface EV.



L'activation du filtre anti-hameçonnage (recommandée durant l'installation) active aussi automatiquement SSL EV.

Le système d'exploitation Windows Vista™ va même encore plus loin. Dans IE7 sous Windows Vista, la fonctionnalité OCSP et le filtre anti-hameçonnage sont configurés par défaut. L'utilisateur du navigateur doit les désactiver manuellement s'il ne souhaite pas y avoir recours.

Il est impossible de mesurer le pourcentage de systèmes clients IE7 qui ont activé le protocole OCSP. Étant donné la grande utilité des barres d'adresse vertes EV et du filtre anti-hameçonnage pour les utilisateurs finaux, la visibilité de ces fonctionnalités au niveau de l'interface et la recommandation du filtre anti-hameçonnage pendant l'installation, VeriSign estime que ce pourcentage pourrait être très élevé. Les administrateurs de sites qui évaluent les certificats SSL EV devraient d'ailleurs s'assurer que ces fonctionnalités sont activées sur leurs systèmes. Les barres d'adresse vertes ne s'afficheront jamais sur un exemplaire d'IE7 où ces fonctionnalités sont désactivées.

Comment fonctionne Extended Validation ?

L'architecture EV a été conçue pour offrir aux utilisateurs finaux des informations fiables sur l'identité des sites Web afin qu'ils puissent accorder, en connaissance de cause, leur confiance à ces derniers. La réussite de cette mission a nécessité de modifier chaque composant de l'architecture de protection du Web. Parallèlement aux nouvelles conventions d'interface très compréhensibles, les certificats EV doivent leur fiabilité aux 1) modifications intervenues au niveau des procédures d'authentification et 2) à la validation du certificat en temps réel.

- 1) La première étape est l'authentification. Le CA/Browser Forum a consacré plus d'un an à élaborer avec soin des directives d'authentification EV, et ce afin de garantir la fiabilité des résultats d'authentification. Ces directives exigent que les AC utilisent les informations primaires ou authentifiées en lieu et place des données communiquées par les demandeurs de certificats proprement dits. Ces dernières mettent en oeuvre des techniques éprouvées qui ont permis d'authentifier des millions de certificats pendant plus d'une décennie. Cette procédure garantit que toutes les informations figurant dans le certificat sont correctes et que le demandeur du certificat est autorisé à l'obtenir pour l'entreprise en question. Ces procédures d'authentification sont mises à la disposition du public sur www.cabforum.org. Chaque AC est tenue de se soumettre à un audit annuel réalisé par un cabinet d'audit agréé WebTrust en vue de garantir le respect scrupuleux des directives EV.
- 2) Dès que le certificat est émis, l'étape suivante consiste à faire en sorte que le certificat soumis au client soit fidèle aux données détectées par l'AC et que les certificats censés être conformes à la norme d'authentification EV le sont effectivement. L'intégrité du certificat est garantie, étant donné que les certificats SSL intègrent des fonctions de hachage sécurisées et ne fonctionneront pas correctement s'ils sont falsifiés, de quelque manière que ce soit. L'infrastructure EV s'assure du bon fonctionnement du certificat en recourant à une validation en temps réel. Cette validation dépend de deux infrastructures parallèles. La première est le protocole OCSP susmentionné. Pour chaque certificat, OCSP vérifie en temps réel si le certificat a été révoqué. S'il est compromis ou doit être révoqué pour quelque raison que ce soit, le certificat EV incriminé ne s'affichera plus comme valide dans les navigateurs compatibles EV.

Le second service en temps réel réside dans le magasin de racines de Microsoft®. Un marqueur de métadonnées très simple indique l'état de chaque certificat EV comme tel. Pour éviter qu'une AC non conforme ou incompétente n'émette de manière erronée des certificats EV marqués comme tels même si ceux-ci n'ont pas fait l'objet d'une authentification EV correcte, le navigateur IE7 effectue une vérification en temps réel par rapport au magasin de racines de Microsoft afin de garantir que la racine SSL en question est admise pour les certificats EV. Grâce à cette vérification, si une AC venait à émettre des certificats assortis du marqueur EV sans avoir été agréée pour l'émission de certificats EV, ces derniers n'activeraient pas la barre d'adresse verte et les autres optimisations d'interface EV. De même, si une AC existante venait à rater son audit annuel ou à émettre à plusieurs reprises des certificats incorrects sous la bannière EV, Microsoft serait en mesure de supprimer la racine en question de la liste des racines approuvées. Cette mesure désactive les barres d'adresse vertes et les autres éléments d'interface EV pour tous les certificats adossés à cette racine suspecte.

EV Upgrader élargit la protection aux clients Windows XP

Les éléments d'interface EV s'affichent automatiquement chez les clients Windows Vista qui naviguent sur un site. En revanche, IE7 sous Windows XP exige une mise à jour des racines SSL pour pouvoir afficher les certificats EV en tant que tels. VeriSign a donc créé VeriSign® EV Upgrader™, la première solution qui permet à tous les navigateurs IE7 de détecter des certificats SSL EV et de les afficher correctement. EV Upgrader tire parti des fonctionnalités existantes de mise à jour des racines du système d'exploitation Windows pour télécharger et installer automatiquement et discrètement la nouvelle racine EV sur le système client. Pour optimiser la convivialité de EV Upgrader pour les administrateurs de sites Web, VeriSign l'a intégré au cœur du sceau VeriSign Secured Seal, y compris dans celui que vous avez probablement déjà installé sur votre site.

Pour obtenir une description complète de EV Upgrader et ses modalités de fonctionnement au sein du sceau VeriSign Secured Seal, veuillez consulter le document technique de VeriSign, *EV Upgrader : Extended Validation désormais accessible aux clients Windows XP*. Pour en savoir plus sur les certificats VeriSign EV ou pour en faire l'acquisition pour votre site, rendez-vous sur <http://www.verisign.fr/ssl/index.html>.