



GUIDE COMMERCIAL

ÉTABLIR UNE RELATION DE CONFIANCE
POUR PROTÉGER ET DÉVELOPPER VOTRE
ACTIVITÉ EN LIGNE

Authentification et cryptage - Les pierres
angulaires de la sécurité en ligne



TABLE DES MATIÈRES

+ Sommaire	4
+ Présentation	4
+ Pourquoi l'authentification SSL est-elle nécessaire ?	5
Cryptage	5
Authentification	5
Certificats numériques	5
+ Comment les certificats SSL authentifiés fonctionnent-ils ?	6
+ Les risques des certificats SSL non authentifiés	7
Cas de figure n°1 : Pas d'authentification de l'organisation par l'autorité de certification (AC)	8
Cas de figure n°2 : Pas de vérification de l'existence de l'organisation par l'autorité de certification (AC)	8
+ Comment vérifier qu'un site Web est authentique ?	9
+ Processus d'authentification de VeriSign	10
Étape 1	10
Étape 2	10
Étape 3	10
Étape 4	10

(Suite)





GUIDE COMMERCIAL

TABLE DES MATIÈRES

+ Pourquoi les procédures authentifiées de VeriSign sont-elles plus fiables ?	10
+ Avantages pour votre société	11
Attrait pour les clients	11
Authentification	11
Confidentialité des messages	11
Intégrité des messages	11
+ Conclusion	12
+ Pour plus d'informations	12



Where it all comes together.™

Sommaire

Au vu des risques associés au commerce électronique et aux communications en ligne, il est impératif d'utiliser une technologie de cryptage sécurisée lors de toute activité commerciale en ligne, mais également de justifier son identité et d'établir des relations de confiance avec les clients et les partenaires.

L'établissement de relations de confiance avec les partenaires et les clients en ligne implique d'être authentifié par un tiers fiable et de recevoir un certificat SSL (Secure Sockets Layer) authentifié et signé par ce tiers de confiance. L'intégrité et la confidentialité des données nécessaires au commerce électronique sont fondées sur le cryptage, qui est un processus de transformation des informations permettant de les rendre inintelligibles à quiconque excepté le destinataire désigné. Sans authentification, cependant, la technologie de cryptage n'est pas suffisante pour protéger les internautes. Il est impératif d'utiliser conjointement l'authentification et le cryptage pour obtenir :

- La confirmation que l'organisation désignée dans le certificat a le droit d'utiliser le nom de domaine indiqué
- La confirmation que l'organisation désignée dans le certificat est une entreprise légitime
- La confirmation que l'individu qui a demandé le certificat SSL au nom de l'organisation a été autorisé à le faire.

Certaines autorités de certification (AC) estiment que le cryptage seul est suffisant pour sécuriser un site Web et établir la confiance entre vos clients et vous. En réalité, toutefois, il existe une distinction certaine entre les certificats authentifiés, qui fournissent un haut niveau de fiabilité et de sécurité, et les certificats non authentifiés, qui représentent une menace pour la confiance des clients et la sécurité en ligne. Outre l'utilisation d'une technologie de cryptage, il est essentiel que votre site Web soit authentifié, ce qui augmente la confiance des visiteurs envers votre site et votre commerce.

Lorsque vous sécurisez votre site Web avec VeriSign®, vous pouvez profiter des nombreuses options proposées pour améliorer le fonctionnement de votre commerce électronique. Avec le sceau Secured Seal de VeriSign, inclus dans chaque service Secure Site, vous affichez la marque numéro un en matière de sécurité sur Internet, pour que vos clients sachent qu'ils communiquent et effectuent des transactions en toute confiance, sur votre site. Ce sceau permet à vos visiteurs de vérifier en temps réel les informations et le statut de votre certificat SSL, ce qui augmente leur confiance dans vos activités en ligne et développe vos ventes et donc votre chiffre d'affaires.



Les services Secure Site de VeriSign vous donnent les moyens de sécuriser et d'activer le commerce en ligne sur votre site, en offrant à vos clients le plus haut niveau de fiabilité disponible sur Internet. La confiance accrue dans la sécurité des transactions en ligne permet, entre autres avantages, l'augmentation des revenus et de la rentabilité. Le commerce en ligne est synonyme de risques importants et d'opportunités exceptionnelles pour ceux qui seront capables de fournir le même niveau de fiabilité et de personnalisation sur Internet que les magasins traditionnels.

Présentation

Jusqu'à récemment encore, la majorité des certificats SSL pouvaient être classés dans les catégories fiabilité moyenne et fiabilité élevée, en fournissant trois services de sécurité distincts : la confidentialité, l'authentification et l'intégrité. Les certificats numériques identifient de manière unique les individus et les sites Web et permettent des communications confidentielles et sécurisées. Malheureusement, certains fournisseurs de certificats SSL ont choisi de ne fournir que des certificats non authentifiés, à la fiabilité peu élevée, pour pouvoir baisser leurs coûts et accélérer le processus de commande. Ceci est en contradiction avec les pratiques normales du secteur, affaiblit la confiance des clients et entraîne une certaine confusion pour les utilisateurs de sites Web.

Les certificats SSL « faible fiabilité » offrent bien la confidentialité et l'intégrité, mais manquent d'authentification. Par le passé, l'icône de cadenas des navigateurs Web était perçue comme une marque fiable du degré d'authentification. Aujourd'hui, les utilisateurs sont obligés d'examiner le certificat SSL lui-même pour savoir s'il est authentifié et donc d'une fiabilité élevée ou non.

Si, par exemple, un utilisateur tente de communiquer de manière sécurisée avec un site Web arborant un certificat SSL de l'organisation « ABC Inc. », l'utilisateur est contraint de vérifier si ce certificat est authentifié par un tiers. Le certificat SSL est supposé fournir aux visiteurs l'assurance que le site Web qu'ils visitent (par exemple, www.abc-incorporated.com) est bien un site de l'organisation « ABC Inc. » et qu'il ne s'agit pas d'une autre entité prétendant être l'organisation ABC Inc, pour inciter les internautes à faire des achats sur son site. Seule une authentification rigoureuse permet à une société de prouver à ses clients et partenaires que son site Web est authentique et qu'elle a le droit d'utiliser le nom de domaine indiqué sur le certificat.

Pourquoi l'authentification SSL est-elle nécessaire ?

Les notions d'identité et d'authentification sont des concepts fondamentaux dans tous les secteurs d'activité. Les particuliers et les institutions doivent apprendre à se connaître et à se faire confiance avant de faire des affaires. Dans le commerce traditionnel, les gens se fient à des critères physiques, tels qu'une licence commerciale ou une lettre de crédit, pour prouver leur identité et assurer l'autre partie concernée de leur capacité à effectuer une transaction commerciale.

À l'âge du commerce électronique, les certificats SSL authentifiés offrent des fonctions cruciales de sécurité et d'identification en ligne, qui aident à établir une relation de confiance entre les deux parties impliquées dans des transactions sur des réseaux numérique. Qu'il s'agisse d'un commerce traditionnel ou électronique, les parties concernées doivent être à même de répondre aux questions suivantes :

- Qui êtes-vous ? (Justificatif d'identité)
- À quelle communauté appartenez-vous ? Êtes-vous agréé ? (Agréé par une association)
- De quelle manière pouvez-vous justifier votre identité ? (Confirmation de l'identité)

Les clients doivent pouvoir être sûrs que le site Web qu'ils visitent est authentique et que les informations qu'ils envoient via leur navigateur Web resteront privées et confidentielles.

+ Cryptage

Internet pose des problèmes de fiabilité bien particuliers, que les entreprises doivent résoudre dès le départ afin de réduire les risques pour la sécurité. Les clients transmettent des informations et achètent des biens ou des services via Internet uniquement lorsqu'ils sont certains que leurs informations personnelles, telles que les numéros de carte de crédit et les données bancaires, sont sécurisées. La solution, pour les sociétés qui envisagent le commerce électronique de manière sérieuse, consiste à mettre en place une infrastructure de commerce électronique fiable et complète basée sur la technologie de cryptage. L'intégrité et la confidentialité des données nécessaires au commerce électronique sont fondées sur le cryptage, qui est un processus de transformation des informations permettant de les rendre inintelligibles à quiconque excepté le destinataire désigné.

+ Authentification

Certaines autorités de certification (AC) estiment que le cryptage seul est suffisant pour sécuriser un site Web et établir la confiance entre vos clients et vous. Elles ont tort. Il est impératif que votre site Web soit également authentifié, ce qui permettra d'améliorer la confiance que les internautes ont en vous et en votre site. Cela signifie qu'une autorité certifiée doit prouver que vous êtes bien qui vous prétendez être. Pour prouver que votre société possède une existence légale, votre site Web doit être sécurisé par le biais d'une technologie de cryptage et d'une procédure d'authentification d'une fiabilité optimale.

+ Certificats numériques

Un certificat numérique est un fichier électronique qui identifie de manière unique des personnes et des sites Web, sur Internet, et permet d'établir des communications sécurisées et confidentielles. Les certificats numériques servent de passeport ou de document d'identification numérique.

En règle générale, le « signataire » d'un certificat numérique est une autorité de certification (AC), telle que VeriSign. Certains certificats numériques correspondent à des autorités fiables et authentifiées, mais malheureusement certaines d'entre elles fournissent des certificats SSL non authentifiés. Cette pratique expose les internautes à des risques d'usurpation (faux sites). Leader du marché des services sécurisés, VeriSign fournit des certificats SSL qui scellent des relations de confiance entre vous et vos clients.

Les certificats SSL authentifiés permettent à un visiteur de site Web de :

- Communiquer en toute sécurité sur un site Web, de manière à ce que les informations fournies par le visiteur ne puissent être interceptées lors de leur transfert (confidentialité) ni modifiées sans qu'il le sache (intégrité)
- Vérifier que le site qu'il visite est bien celui de la société indiquée et non d'un imposteur (authentification)

VeriSign garantit cette confiance en alliant son service d'authentification à une technologie de cryptage de pointe, dans ses certificats numériques. Le certificat SSL de VeriSign de votre commerce en ligne ne sera émis qu'une fois les procédures suivantes complétées :

- Vérification de votre identité et confirmation que votre organisation est une entité légale
- Confirmation que vous avez le droit d'utiliser le nom de domaine inscrit dans le certificat
- Vérification que l'individu qui a demandé le certificat SSL au nom de l'organisation a été autorisé à le faire.

Comment les certificats SSL authentifiés fonctionnent-ils ?

Un certificat SSL authentifié permet au destinataire d'un message numérique d'être certain de l'identité de l'expéditeur et de l'intégrité du message. Voici trois étapes d'authentification et de vérification indispensables à la procédure d'émission de certificats SSL haute fiabilité pour le site Web d'une organisation :

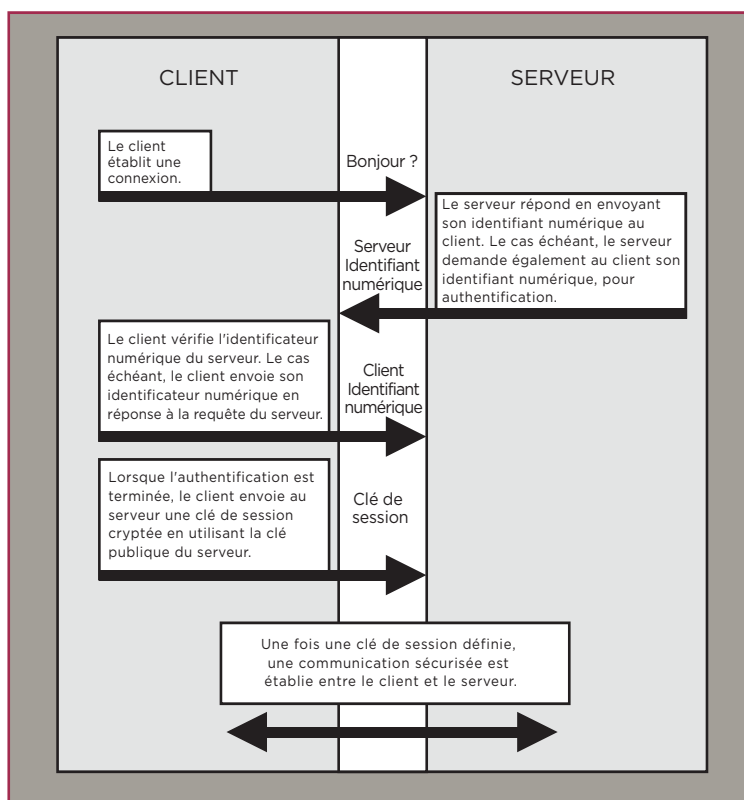
- La confirmation que l'organisation désignée dans le certificat a le droit d'utiliser le nom de domaine indiqué
- La confirmation que l'organisation désignée dans le certificat est une entreprise légitime
- La confirmation que l'individu qui a demandé le certificat SSL au nom de l'organisation a été autorisé à le faire

Lorsque des visiteurs se connectent à un site Web, ils peuvent utiliser deux types de serveur. S'ils utilisent un serveur sécurisé,

des messages de confirmation s'affichent. De même, des avertissements s'affichent s'ils accèdent à des serveurs non sécurisés. Un serveur Web véritablement sécurisé possède un certificat SSL authentifié. Ce certificat authentifié indique aux utilisateurs qu'une société indépendante et fiable a vérifié que le serveur appartenait bien à la société qui le prétendait. Un certificat authentifié valide signifie que les utilisateurs peuvent être sûrs qu'ils envoient leurs données confidentielles au destinataire souhaité.

Le Webmaster génère une demande de certificat, qui crée deux clés cryptées : une clé privée et une clé publique. Il envoie ensuite la clé publique à une autorité de certification, telle que VeriSign. Celle-ci doit alors s'assurer que les certificats sont émis pour la société appropriée. Elle doit notamment vérifier que :

- La société faisant l'objet d'un certificat est bien propriétaire du nom de domaine certifié
- Cette société a une existence légale, dans un ou plusieurs pays
- Le nom enregistré est le même que celui figurant sur le certificat que l'AC doit signer
- La personne demandant le certificat est bien employée par cette société



Une fois les vérifications effectuées, l'autorité de certification (AC) signe la clé publique. Celle-ci est renvoyée au Webmaster, qui la charge sur le serveur. Dès que la clé publique et la clé privée s'alignent parfaitement, la technologie SSL est activée. Cette fonction SSL garantit que les informations envoyées par le serveur sont identiques à celles reçues par le visiteur du site Web et qu'aucune modification n'a été effectuée.

Les risques des certificats SSL non authentifiés

Actuellement, les navigateurs ne savent pas distinguer un certificat SSL authentifié (haute fiabilité) d'un certificat SSL non authentifié (faible fiabilité). Dans la mesure où le certificat SSL a été émis par une autorité de certification agréée et que le nom de domaine du certificat correspond à celui du site Web, l'utilisateur fait automatiquement confiance au certificat SSL.

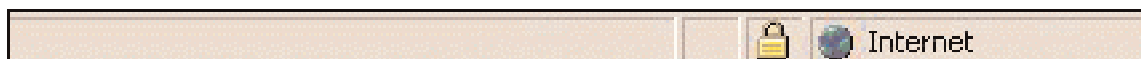
L'icône de cadenas affichée dans le navigateur de l'utilisateur ne varie pas si celui-ci visite un site possédant un certificat SSL authentifié ou un certificat SSL non authentifié.

Jusqu'à récemment, cette approche simple fonctionnait

Quelles sont les autres raisons de l'importance de l'authentification ? Les fraudes sur Internet restent aujourd'hui un obstacle majeur à la consommation en ligne et une source de fraudes importante, face à des acheteurs imprudents faisant affaires avec des sociétés qu'ils ne connaissent que peu ou pas du tout.

Voici quelques chiffres concernant la fraude sur Internet:

- La fraude a entraîné la perte de plus de 700 millions de dollars US de recettes en ligne en 2001, ce qui représente 1,14 % du chiffre d'affaires annuel total qui se monte à 61,8 milliards de dollars, selon GartnerG2. Les pertes (en dollars) dues à la fraude en 2001 étaient 19 fois plus élevées pour les ventes en ligne que pour tous les autres types de vente.
- Selon le groupe Gartner, la fraude sur Internet revient cher aux commerçants en ligne. En interrogeant plus de 160 entreprises, Gartner a découvert que le nombre de transactions frauduleuses sur Internet était 12 fois plus élevé que pour la vente au détail traditionnelle. En outre, les commerçants en ligne supportent les frais et la responsabilité en cas de fraude, alors que les fraudes relatives aux commerces traditionnels sont généralement prises en charge par les compagnies d'assurance, dans la mesure où le détaillant respecte la procédure requise et conserve un reçu signé.
- Des recherches menées par Jupiter Media Metrix ont démontré que la crainte de la fraude en ligne était plus courante que la fraude même.



parfaitement et a permis l'expansion du commerce en ligne. Cependant, de récents changements survenus sur le marché des certificats SSL ont engendré une menace potentielle pour la sécurité des clients et de l'utilisation des sites de commerce électronique. L'un des principaux risques associés à un certificat SSL non authentifié est l'« usurpation de sites ». Le coût peu élevé de la création d'un site Web, ainsi que la facilité avec laquelle il est possible de copier des pages existantes rendent extrêmement aisée la création de sites illégitimes, qui semblent avoir été publiés par des organisations existantes. En réalité, des imposteurs ont obtenu de manière illégale des numéros de cartes de crédit en créant des sites d'apparence professionnelle imitant des entreprises légitimes ; ils se servent pour cela d'un nom de domaine similaire au nom légitime et présentent un contenu trompeur pour piéger les internautes et leur faire prendre une décision dangereuse.

« L'achat en ligne a mauvaise presse, mais la plupart des histoires rapportées sont anecdotiques et concernent des entreprises qui n'avaient pas mis des mesures de défense efficace en place. » affirme Harry Wolhandler, vice-président du département Étude de marché chez ActivMedia. « Les commerçants en ligne qui protègent correctement les informations de leurs clients sont très peu concernés par ce problème, avec des pertes moyennes dues à la fraude qui dépassent à peine les 1 %. Le contrôle de la fraude est parfaitement possible en ligne, même si de nombreuses entreprises ne mettent pas en place une protection rigoureuse ni des mesures de prévention. »

La section suivante décrit quelques risques dus à une authentification insuffisante, avec deux cas de figure où des commerces en ligne sécurisés sont menacés.

	Option 1	Option 2	Option 3	Option 4
Organisation (O) =	ABC Global Bank	abcbankonline.com	abcbankonline.com	
Nom commun (CN) =	abcbankonline.com	abcbankonline.com	abcbankonline.com	abcbankonline.com
Réclamation	Organisation non authentifiée	Organisation non authentifiée		

+ Cas de figure 1 : Pas d'authentification de l'organisation par l'autorité de certification (AC)

M. Impostor s'enregistre sous le nom de domaine www.abcbankonline.com, usurpant ainsi l'identité du site de l'ABC Global Bank pour attirer des clients imprudents, et obtient un certificat SSL non authentifié. Ce certificat inclut l'un des éléments du tableau ci-dessus dans le champ du nom.

Lorsqu'un client visite le « faux site » de M. Impostor, il n'a à sa disposition aucun moyen facile de savoir que ce site n'est pas légitime. Si le client voit s'afficher l'icône de cadenas, il peut avoir une fausse impression de sécurité. Il croira certainement être connecté au site Web de l'ABC Global Bank, ce qui n'est absolument pas le cas. L'affichage de cette icône de cadenas incite l'utilisateur à saisir son ID utilisateur et son mot de passe. M. Impostor peut alors capturer l'ID utilisateur et le mot de passe, puis transférer l'utilisateur sur le site légitime.

Si le client examine le certificat SSL et voit s'afficher « organisation non authentifiée » ou que le nom ABC Global Bank n'apparaît pas sur le certificat, les plans de M. Impostor seront contrecarrés. Ceci suppose toutefois que l'utilisateur prenne quelques précautions avant de saisir son ID utilisateur et son mot de passe ou même des informations personnelles ou confidentielles. Imaginons que l'ABC Global Bank enregistre le nom de domaine www.abcbank.com et crée un site Web de services bancaires en ligne légitimes en utilisant un certificat SSL. Ce certificat inclut la mention suivante dans le champ du nom :

Organisation (O) =	ABC Global Bank
Nom commun (CN) =	abcbank.com

La procédure d'authentification permet d'éviter qu'une personne ou une entité malveillante n'obtienne un certificat contenant le nom d'une autre organisation. L'utilisation d'un nom d'organisation authentifié dans le certificat SSL garantit aux utilisateurs que l'organisation qui a acheté le certificat pour ce site Web est une organisation légitime.

+ Cas de figure : Pas de vérification de l'existence de l'organisation par l'autorité de certification (AC)

M. Impostor enregistre un nom de domaine au nom de la société Internet Bank Corp. (qui n'existe pas), en utilisant une carte de crédit volée comme moyen de paiement. M. Impostor crée un site Web et obtient un certificat SSL non authentifié donnant une apparence de légitimité à son site. Un internaute voit s'afficher l'icône de cadenas dans son navigateur et pense que ses données sont en sécurité. Si M. Impostor propose des taux d'intérêt plus élevés que la moyenne sur l'épargne ou un financement intéressant, cela incitera les utilisateurs à fournir leurs données personnelles.

Une vérification préalable de l'existence de l'organisation permet d'éviter qu'un individu malveillant prétende être une organisation légitime.

Comment vérifier qu'un site Web est authentique ?

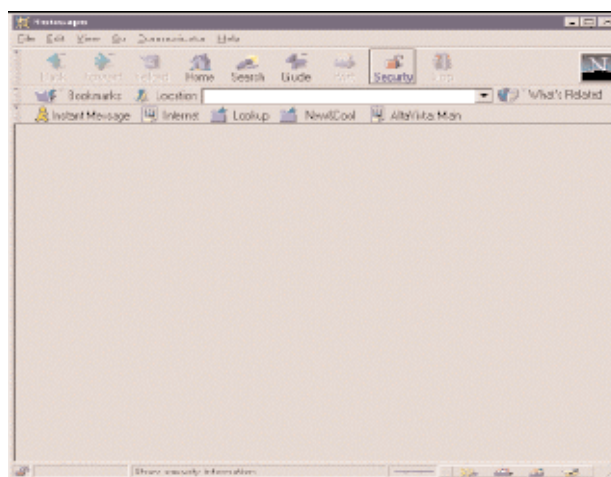
Avant d'envoyer des informations ou d'acheter des biens sur un site de commerce en ligne, vous devez vous assurer que la société commerciale est bien celle qu'elle prétend être. Alors que les sites Web peuvent acheter des certificats de serveur auprès de nombreuses autorités de certification différentes, les navigateurs Internet sont configurés pour faire confiance uniquement aux certificats de serveur provenant d'un cercle restreint de sociétés très réputées. Lorsque vous visitez un commerce en ligne sécurisé par VeriSign, par exemple, vous pouvez être certain que ce site est authentique.

Bien que la plupart des clients et des commerçants ne connaissent pas entièrement les procédures détaillées sous-jacentes aux services d'authentification de VeriSign, ils savent que le sceau Verisign Secured Seal est la preuve qu'une société est réelle et que le site est sécurisé. Chaque commerce en ligne authentifié obtient un sceau avec son certificat, afin d'améliorer la confiance de ses clients.

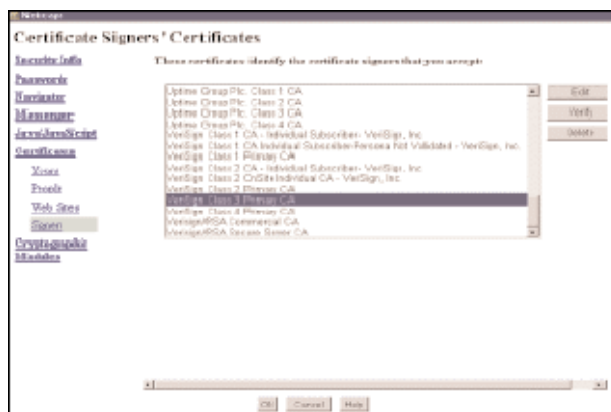


Les navigateurs Netscape Navigator et Microsoft Internet Explorer disposent de mécanismes de sécurité intégrés pour empêcher les utilisateurs d'envoyer à leur insu des informations personnelles à travers des canaux non sécurisés. Si un utilisateur tente d'envoyer des informations vers un site non sécurisé (ne possédant pas de certificat SSL authentifié), les navigateurs affichent, par défaut, un avertissement qui peut dissuader les utilisateurs de faire des achats sur ce site.

Les certificats VeriSign prouvent votre identité lors du traitement des transactions électroniques de la même manière qu'une pièce d'identité lors des transactions traditionnelles. Avec un certificat SSL de VeriSign, vous pouvez assurer à vos clients que les données électroniques qu'ils reçoivent de vous sont authentiques.



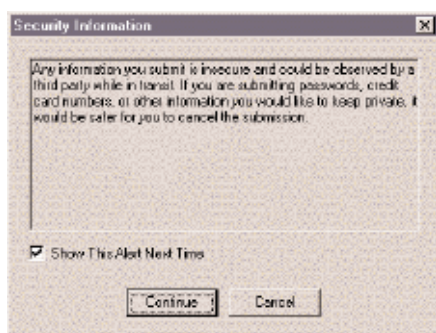
Vous trouverez ci-dessus un exemple de certificat SSL, affiché dans Netscape Communicator v4.0.



Commencez par cliquer sur l'icône « Sécurité » de la barre d'outils.



Sélectionnez les signataires du certificat et affichez la liste des certificats.



Procédure d'authentification de VeriSign

Les procédures d'authentification et de vérification établies par VeriSign aident les commerçants à développer leur activité en ligne et réduisent les risques de fraude. Les commerçants gagnent ainsi la confiance de leurs clients en leur offrant la possibilité de vérifier leur identité. Ces procédures sont le résultat d'années d'expérience dans l'utilisation d'une infrastructure sécurisée sur Internet et de l'authentification de plus d'un demi-million de sociétés. Pour vous permettre d'apprécier l'efficacité et la fiabilité de cette procédure, ainsi que les avantages qu'elle représente pour la croissance de votre activité de commerce en ligne, la procédure d'authentification de VeriSign est décomposée ci-dessous :

+ Étape 1

L'authentification commence lorsque les particuliers et les entreprises fournissent des informations à VeriSign pour acheter en ligne leurs certificats numériques, de façon rapide et pratique.

+ Étape 2

VeriSign vérifie alors que :

- Ni les employés de l'organisation ni le contact de l'organisation ne figurent sur l'une des trois listes noires du gouvernement des États-Unis : « Denied Persons List », « Denied Entities List » et « US Treasury Department List »
- L'organisation dispose d'informations d'identification émises par l'administration, comme des statuts ou une patente, qui l'autorisent à effectuer des transactions commerciales
- L'organisation est propriétaire du nom de domaine pour lequel le certificat est délivré OU le propriétaire du nom de domaine a autorisé l'organisation à utiliser légalement son nom de domaine
- Le contact de l'organisation peut être identifié comme faisant partie du personnel de l'organisation qui commande le certificat, en appelant le numéro de téléphone d'un tiers

+ Étape 3

VeriSign délivre alors le certificat conformément à sa politique d'exploitation (Operations Policies), qui prévoit les procédures suivantes :

- Répartition des tâches : deux employés différents de VeriSign doivent effectuer les procédures d'authentification de l'organisation d'où émane la

demande de certificat, ainsi que les procédures de vérification de la validité du contact au sein de l'entreprise

- Tous les employés de VeriSign chargés de traiter les certificats numériques doivent subir un contrôle approfondi de leurs antécédents pénaux et financiers
- Une infrastructure de sécurité par biométrie, de type militaire, est requise pour tous les locaux où sont traités des certificats numériques
- Toutes les informations relatives aux clients sont strictement confidentielles et les centres de données où elles se trouvent sont hébergés dans des endroits hautement sécurisés par biométrie

+ Étape 4



Une fois que VeriSign a émis le certificat SSL et que le commerçant en ligne authentifié l'a installé sur son site Web, les visiteurs du site peuvent à tout moment accéder aux données d'authentification. Ces données leur garantissent que le site est bien ce qu'il paraît être et appartient à une société légitime ; pour vérifier ces informations, il leur suffit de cliquer sur l'icône de cadenas ou sur le sceau VeriSign Secured Seal, fourni pour chaque site Web équipé d'un certificat SSL.

Pourquoi les procédures authentifiées de VeriSign sont-elles plus fiables ?

La procédure d'authentification de VeriSign est parfaitement sécurisée et efficace : nous offrons le temps de réponse le plus court possible pour les demandes de certificat SANS compromettre la fiabilité de la procédure.

Avant de délivrer un certificat SSL, VeriSign passe en revue vos pièces justificatives et effectue une vérification complète et approfondie de votre organisation, pour garantir qu'elle est bien ce qu'elle prétend être. VeriSign émet ensuite un certificat SSL authentifié ; il s'agit d'une pièce justificative électronique que votre organisation peut afficher pour prouver son identité ou ses droits d'accès à des informations.

Avantages pour votre société

Lorsque vous avez installé votre certificat VeriSign, votre serveur active automatiquement la technologie SSL, créant un canal de communication sécurisé et authentifié entre votre serveur et le navigateur de vos clients. Votre site peut communiquer en toute sécurité avec les clients utilisant Netscape Navigator, Microsoft Internet Explorer et les autres systèmes de messagerie courants. Une fois activée par votre certificat de serveur, la technologie SSL démarre automatiquement et vous procure tous les avantages de transactions en ligne sécurisées :

+ Attrait pour les clients

Lorsque vous sécurisez votre site Web, vous pouvez profiter des nombreuses options proposées par VeriSign pour améliorer le fonctionnement de votre commerce électronique. Avec le sceau Verisign Secured Seal, inclus dans chaque service Secure Site, vous affichez la marque numéro un sur Internet en matière de sécurité, pour que vos clients communiquent et effectuent des transactions en toute confiance, sur votre site. Le sceau permet à vos visiteurs de vérifier les informations et le statut de votre certificat SSL en temps réel et vous apporte une protection supplémentaire contre l'usage abusif de certificats révoqués ou périmés.

VeriSign a effectué la sécurisation de plus de sites Web que n'importe quelle autre société du marché, avec plus de 500 000 sites sécurisés. Sa clientèle variée inclue la plupart des sociétés Fortune 500 et les principaux sites mondiaux de commerce électronique, mais également de nombreuses PME débutant sur Internet.

Le nombre de sites sécurisés par VeriSign est si important, et la confiance dans le sceau Verisign Secured Seal si forte, que le nombre de clients ayant cliqué sur un sceau Secure Site était de près de 1 million au cours du seul mois d'avril 2002. Le sceau fournit aux internautes la preuve que le site Web qu'ils visitent a été authentifié, qu'il s'agit d'une société légitime et que le site est sécurisé à l'aide de la technologie de cryptage SSL.

Quelle est la conséquence la plus importante d'un certificat de serveur VeriSign sur votre site ? Il permet de garantir des transactions électroniques sécurisées à la fois pour vos clients et pour votre société. Les clients peuvent avoir confiance en votre prestation de service et savent que leurs données personnelles sont envoyées à une société légitime et non à un imposteur. En retour, vous savez que votre société reçoit des informations exactes, que le client ne peut contester ultérieurement.

Les services Secure Site de VeriSign vous donnent les moyens de sécuriser et d'activer le commerce en ligne sur votre site, en offrant à vos clients le plus haut niveau de fiabilité disponible sur Internet. La confiance accrue dans la sécurité des transactions en ligne permet, entre autres avantages, l'augmentation des revenus et de la rentabilité.

+ Authentification

En consultant votre certificat VeriSign, vos clients peuvent vérifier que le site Web vous appartient bien et qu'il ne s'agit pas d'une usurpation. Cela permet de forger la confiance nécessaire à l'envoi d'informations confidentielles.

+ Confidentialité des messages.

La technologie SSL crypte toutes les données échangées entre votre serveur Web et vos clients, notamment les numéros de cartes de crédit et autres données personnelles, à l'aide d'une clé de session unique. Pour transmettre la clé de session au client, de manière sécurisée, votre serveur la crypte à l'aide de votre clé publique. Chaque clé de session n'est utilisée qu'une fois, au cours d'une seule session (qui peut inclure une ou plusieurs transactions), avec un seul client. Ces différents niveaux de protection de la confidentialité garantissent que les données ne peuvent être affichées si un tiers non autorisé les intercepte.

+ Intégrité des messages

Lors de l'envoi d'un message, l'ordinateur émetteur et l'ordinateur récepteur génèrent chacun un code basé sur le contenu du message. Si le contenu du message est altéré en cours de route, même d'un seul caractère, l'ordinateur récepteur génère un code différent et alerte le destinataire que le message n'est pas sûr. Grâce à la fonctionnalité d'intégrité des messages, les deux parties concernées dans la transaction savent que le message reçu est strictement identique au message envoyé.

Conclusion

Certaines autorités de certification (AC) estiment que le cryptage sans authentification est suffisant pour sécuriser un site Web et établir la confiance entre vos clients et vous. Toutefois, le cryptage seul n'est pas suffisant.

Les certificats SSL non authentifiés offrent la confidentialité et l'intégrité, mais pas l'authentification indépendante nécessaire pour :

- Vérifier que le site visité par l'utilisateur est bien celui de la société indiquée et non celui d'un imposteur
- Permettre au destinataire d'un message numérique d'être certain de l'identité de l'expéditeur et de l'intégrité du message
- Garantir des transactions électroniques sécurisées à la fois pour vos clients et pour votre société.

Pour toutes ces raisons, il est essentiel que votre site Web soit authentifié, ce qui améliorera la confiance de vos clients. En outre, si des certificats peuvent être délivrés par des tiers non autorisés, la fiabilité des certificats légitimes en sera diminuée. Une vérification de la légitimité de la demande de certificat d'une organisation (par exemple, une preuve d'emploi dans l'organisation indiquée sur le certificat), permet d'éviter qu'un certificat ne soit délivré à des individus malveillants n'ayant aucun rapport avec cette organisation.

Un certificat SSL VeriSign authentifié fournit la dernière technologie en matière de crédibilité pour votre commerce en ligne. Nos rigoureuses procédures d'authentification sont les plus fiables du marché et garantissent que :

- Les demandeurs sont correctement identifiés et authentifiés
- Les demandes de certificat sont exactes, autorisées et complètes

De plus, en affichant le sceau Verisign Secured Seal, vous offrez à vos clients la garantie qu'ils effectuent des communications et des transactions en toute sécurité sur votre site. Le sceau Verisign Secured Seal permet à vos visiteurs de vérifier en temps réel les informations et le statut de votre certificat SSL et vous apporte une protection supplémentaire contre l'usage abusif de certificats révoqués ou périmés.

Les procédures d'authentification rigoureuses de VeriSign, les techniques de cryptographie avancées et les locaux ultra sécurisés ont été conçus pour augmenter la confiance que vous et vos clients nous portez. Ces procédures, en termes de technologie et d'infrastructure sont la base sur laquelle s'appuient les certificats de serveur pour sécuriser les transactions, en fonctionnant conjointement avec votre serveur Web.

Pour plus d'informations

Pour contacter un expert sécurité de VeriSign, appelez le 0800 90 43 51. Vous pouvez également contacter un représentant VeriSign par courrier électronique, à l'adresse : ventes@verisign.fr.

Pour plus d'informations, visitez notre site à l'adresse www.verisign.fr.