



LIVRE BLANC

Gestion de SSL Security dans des environnements multiserveurs

Réduction des coûts de sécurité et accélération de la gestion des certificats SSL grâce aux services Web faciles à utiliser de VeriSign





LIVRE BLANC

DOCUMENTATION TECHNIQUE

- + Une stratégie intelligente pour la gestion de SSL Security sur des serveurs multiples 3
- + La gestion au cas par cas des Certificats : un processus fastidieux 5
- + La simplification de la gestion SSL grâce à la solution Web de VeriSign 7
 - Un contrôle centralisé grâce à l'interface Web 7
- + Des rapports automatisés pour un meilleur contrôle 9
- + Un service de niveau professionnel avec l'expertise SSL à votre disposition 11
- + Découvrez et testez les avantages de MPKI pour SSL 12



Where it all comes together.™

Une stratégie intelligente pour la gestion de SSL Security sur des serveurs multiples

Protéger la confidentialité et l'intégrité des informations confidentielles transmises sur le réseau de votre organisation est un facteur crucial pour forger la confiance de vos clients, établir des relations sécurisées avec vos partenaires commerciaux et assurer la conformité aux nouvelles réglementations en matière de confidentialité. Votre société a le devoir de sécuriser les échanges d'informations entre les serveurs et les clients Web, entre différents serveurs et entre d'autres équipements réseau, tels que les équilibreurs de charge serveur ou les accélérateurs SSL. Pour obtenir une sécurité optimale, le système de sécurité inter-réseau doit protéger les serveurs en liaison à la fois avec Internet et avec des Intranets privés.

La technologie Secure Sockets Layer (SSL) est la première norme mondiale utilisée pour la protection des données transmises sur Internet à l'aide du très répandu protocole HTTP. SSL protège votre système contre l'usurpation de sites, l'interception et l'utilisation frauduleuse de données. La majorité des systèmes d'exploitation, des applications Web et des serveurs matériels prennent en charge le protocole SSL en natif. Grâce au puissant cryptage SSL et à la confiance découlant des procédures d'authentification de VeriSign®, votre société peut immédiatement protéger les données confidentielles transférées entre vos serveurs et vos clients, employés et partenaires commerciaux.

La solution Managed PKI pour SSL (MPKI pour SSL) est un service Web flexible et facile à utiliser signé VeriSign, qui permet de déployer et de gérer plusieurs certificats SSL au sein de votre organisation. Basée sur l'infrastructure évolutive et hautement sécurisée de VeriSign, la solution professionnelle Managed PKI pour SSL vous permet de réduire de manière significative les coûts associés au déploiement des certificats SSL, tout en conservant un contrôle maximum au niveau local.

MPKI pour SSL de VeriSign

Simple : Service Web de gestion de tous vos certificats SSL ; aucune installation directe de matériel ou de logiciels n'est requise.

Efficace : Inscription, validation, émission, refus, révocation et renouvellement en quelques clics.

Rapide : Émission de certificats SSL à la demande.

Sûr : Accès sécurisé aux Certificats par compte administrateur.

Complet : Gestion de tous les hôtes en liaison avec Internet ou des Intranets (en option.)

Valeur ajoutée : Achat par lots de certificats SSL à tarif dégressif.

Managed PKI pour Intranet SSL (MPKI pour Intranet SSL) est le service Web connexe de VeriSign utilisé pour le déploiement et la gestion des certificats SSL sur des hôtes ; cette solution est destinée aux Intranets privés uniquement. Managed PKI pour Intranet SSL fournit aux hôtes internes les fonctionnalités et les avantages de la solution Managed PKI pour SSL.

¹ L'équipe d'ingénierie Internet a rebaptisé la technologie SSL en TLS (Transport Layer Security) et travaille actuellement sur l'adoption globale du protocole TLS. La nomenclature SSL reste cependant très répandue aujourd'hui.

+ Une sécurité optimale pour les transactions Web grâce aux certificats SSL

La transmission sur Internet ou sur un Intranet de données confidentielles, telles qu'un numéro de carte de crédit ou un dossier médical, requiert un processus d'authentification pour garantir que le destinataire des données est légitime, un processus de cryptage pour protéger les données contre toute interception ou altération et l'intégrité du message pour garantir que les informations ne sont pas modifiées durant la transmission. Les certificats numériques de VeriSign utilisent la technologie SSL (Secure Sockets Layer) pour traiter ces différents problèmes. SSL est aujourd'hui devenue la norme mondiale en matière de protection des données confidentielles transmises en HTTP sur Internet ou sur des Intranets. .

En tant que composant de l'infrastructure à clé publique (PKI, Public Key Infrastructure) pour la sécurité Web, les certificats numériques activent la fonctionnalité de SSL Security intégrée à tous les navigateurs et autres applications Web. Les certificats SSL de VeriSign offrent trois avantages clés :

Authentification de l'identité d'une société

VeriSign utilise des procédures complètes destinées à vérifier l'identité des entreprises et l'autorisation du demandeur avant d'émettre un certificat SSL. Les principaux navigateurs Web acceptent par défaut les certificats SSL signés par l'autorité de certification souche de VeriSign, ce qui donne aux visiteurs du site Web l'assurance que leurs informations seront transmises à une entreprise légitime, et non à un imposteur.

VeriSign est le leader du marché en matière d'authentification de l'identité des entreprises, grâce à sa procédure de contrôle en trois étapes, la plus approfondie du marché. Celle-ci vérifie si :

- L'entreprise citée dans le certificat a le droit d'utiliser le nom de domaine indiqué
- L'entreprise citée dans le certificat est une entreprise légitime
- L'individu qui a demandé le certificat SSL au nom de l'entreprise a été dûment autorisé à le faire

Cryptage

Toutes les données transmises par SSL entre les navigateurs Web (clients) et les serveurs sont cryptées à l'aide de techniques cryptographiques sophistiquées qui rendent pratiquement impossible une interception des données. Chaque connexion sécurisée située entre le client et le serveur est dotée d'une « clé de session SSL » ; la longueur de la clé indique le degré de cryptage.

Le degré de cryptage utilisé pour une session SSL spécifique dépend de la version du navigateur et du type de certificat SSL installé sur le serveur Web. Le cryptage SSL le plus puissant disponible pour les navigateurs actuels est le cryptage 128 bits, ce qui signifie que la clé de session SSL a une longueur de 128 bits. Cependant, les versions de navigateur exportées hors États-Unis avant janvier 2000 ne prennent généralement en charge que des sessions SSL 40 bits, à moins que le certificat SSL du serveur Web n'inclue la cryptographie SGC (Server Gated Cryptography), également appelée technologie de « mise à niveau ».

Intégrité des messages

Le contenu de toutes les communications entre le client et le serveur est protégé contre toute altération. Chacune des parties engagées dans la transaction sait que les informations qu'elle a reçues sont exactement identiques à celles émises à l'origine par l'autre partie de la connexion SSL.

ÉTUDE DE CAS SSL : Finance

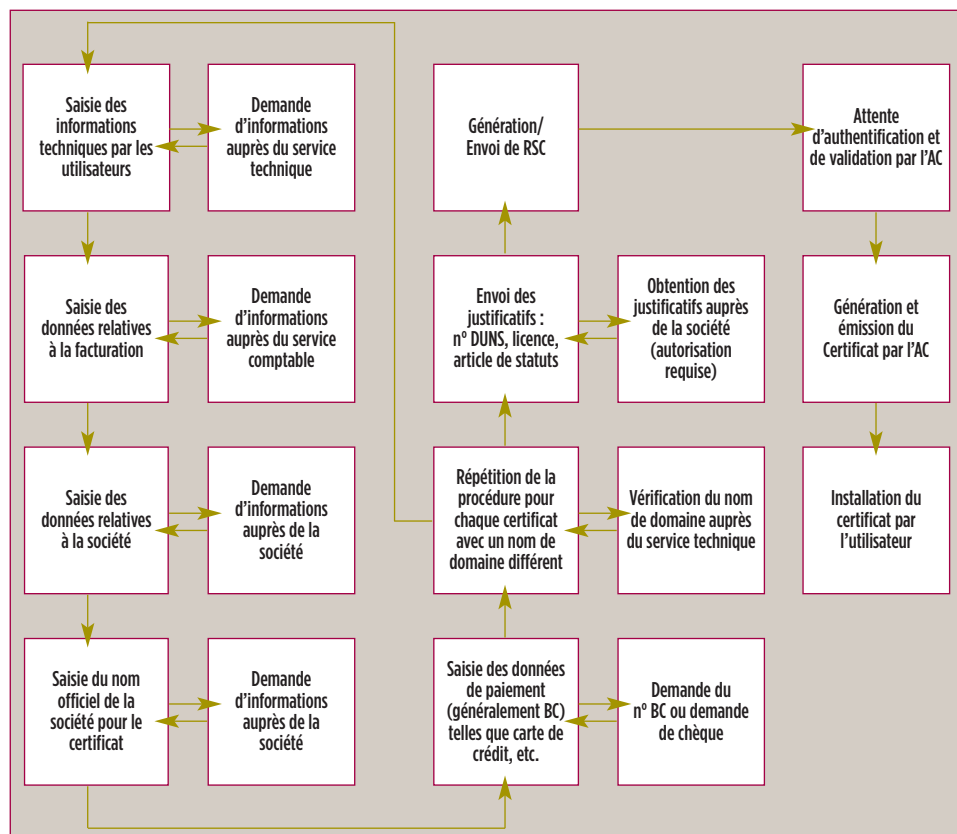
Un important établissement financier utilise plus de 700 certificats : 500 unités achetées avec MPKI pour SSL de VeriSign et environ 200 de manière individuelle. Le regroupement de tous les certificats sous MPKI pour SSL a permis à cette société de réduire de plus de 70 000 \$ ses coûts annuels de renouvellement et de gestion des certificats individuels et elle contrôle à présent les abonnés-demandeurs à l'aide d'une procédure rigoureuse d'autorisation et d'authentification.

La gestion au cas par cas des certificats : un processus fastidieux

Le choix de votre organisation d'utiliser de nombreux certificats SSL implique une décision de gestion pratique : Allez-vous effectuer cette opération manuellement ou utiliser un service Web évolutif, tel que MPKI pour SSL ou MPKI pour Intranet SSL de VeriSign, qui permet d'automatiser la gestion des certificats multiples ? La gestion des certificats SSL au cas par cas est appropriée pour les organisations de petite taille, dans lesquelles une seule personne est responsable du déploiement et de la gestion d'un ou deux certificats SSL. Cependant, le déploiement de certificats SSL multiples sur plusieurs services et sites géographiquement distincts est un problème beaucoup plus complexe.

Au premier abord, la stratégie de déploiement au cas par cas paraît relativement simple. Certaines sociétés décentralisées profitent des tarifs dégressifs proposés par d'autres fournisseurs de certificats SSL, mais elles ne se rendent souvent pas compte des « coûts cachés » qu'impliquent la gestion de nombreux certificats SSL au sein d'une organisation. Le prix du certificat SSL lui-même n'est pas le seul coût à prendre en compte, tout particulièrement dans les organisations possédant plusieurs types de serveur, plusieurs sites géographiques et plusieurs administrateurs de serveur.

Consultez le schéma ci-dessous pour découvrir chaque étape type de la procédure de demande d'un certificat SSL.



Service de gestion des certificats SSL pour les hôtes internes

Managed PKI pour Intranet SSL sécurise les communications au sein de votre Intranet ou de votre réseau privé.

- Fonctions et avantages identiques à Managed PKI pour SSL
- Simple, efficace, rapide, sûr et à haute valeur ajoutée
- Utile pour sécuriser les opérations internes, les portails d'entreprise, ainsi que les environnements de test et de développement

La procédure indiquée ci-dessus inclut de nombreuses étapes de collecte et de vérification des informations requises par l'autorité de certification (AC), chargée d'autoriser de délivrer les certificats SSL. Certaines informations requises lors de la procédure de demande sont difficiles à trouver, tout particulièrement lorsque le responsable informatique doit aller frapper à la porte des cadres concernés pour leur demander une documentation spécifique, des articles de statuts et autres documents justificatifs. En outre, une autorisation d'achat individuelle est généralement demandée pour chaque certificat SSL, ce qui peut reporter l'attribution du certificat, car l'AC applique une procédure complète d'authentification et de vérification pour chaque demande de certificat SSL. En conséquence, le coût total d'un certificat SSL acheté individuellement est bien plus élevé que le simple prix d'achat initial.

Le travail et les frais découlant du déploiement du certificat représentent simplement une partie du coût de gestion du certificat SSL sur l'ensemble de sa période de validité, également appelée « cycle de vie du certificat ». Six opérations différentes peuvent être effectuées dans le cadre du cycle de vie d'un certificat SSL :

+ Composantes du cycle de vie d'un certificat SSL

- **Demande**—procédure d'inscription complète pour l'achat d'un certificat SSL, incluant l'envoi des données administratives et relatives à l'éligibilité de l'organisation.
- **Validation**—interface avec une autorité de certification indépendante, qui vérifie l'éligibilité de l'organisation et valide l'octroi du certificat ; procédure concernant uniquement les produits MPKI pour SSL et MPKI pour Intranet SSL de VeriSign.
- **Émission**—l'autorité de certification émet le certificat ; l'acheteur installe ce dernier sur le serveur ou le périphérique désigné pour activer les services SSL.
- **Refus**—rejet administratif immédiat de toute demande de certificat non autorisée ; procédure concernant uniquement MPKI pour SSL de VeriSign.
- **Révocation**—révocation administrative immédiate d'un certificat ; procédure concernant uniquement les produits MPKI pour SSL et MPKI pour Intranet SSL de VeriSign.
- **Renouvellement**—garantit que chaque certificat est renouvelé de manière appropriée par l'autorité de certification.

La procédure manuelle au cas par cas est adaptée à la gestion d'un nombre peu élevé de certificats. La gestion d'un nombre élevé de certificats est un processus long, fastidieux et onéreux, tout particulièrement pour les grandes organisations. L'automatisation de ce processus à l'aide des outils MPKI pour SSL et MPKI pour Intranet SSL de VeriSign est la solution logique pour une gestion efficace de SSL Security.

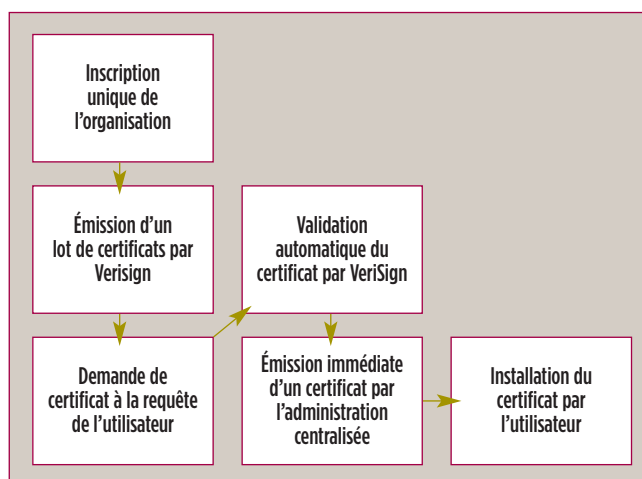
ÉTUDE DE CAS SSL : Assurances

Une grande compagnie d'assurance utilise des certificats SSL individuels pour assurer la sécurité de ses systèmes de transaction Web. Le développement du projet se faisant le week-end et pendant les horaires de fermeture, cette compagnie a besoin de pouvoir émettre instantanément des certificats pour tester et implémenter l'infrastructure de sécurité sur ses nouveaux serveurs de production. L'émission de certificats individuels demande quatre jours, la compagnie décide donc d'utiliser la solution MPKI pour SSL de VeriSign. Aujourd'hui, cette compagnie d'assurance est à même d'atteindre ses objectifs de performances et a réduit ses coûts de gestion et d'acquisition des certificats.

La simplification de la gestion SSL grâce à la solution Web de VeriSign

Les sociétés souhaitant implémenter cinq certificats SSL ou plus peuvent grandement simplifier le processus de gestion en utilisant les fonctions d'automatisation, MPKI pour SSL et MPKI pour Intranet SSL de VeriSign. La gestion Web des certificats SSL offre à votre organisation une vue globale des certificats utilisés, un contrôle financier et opérationnel centralisé et l'assurance d'une protection SSL complète pour les transactions de serveur.

Le schéma ci-dessous illustre comment MPKI pour SSL et MPKI pour Intranet SSL de VeriSign simplifient le processus complexe de demande de certificat, permettant une émission rapide et à la demande de certificats SSL.

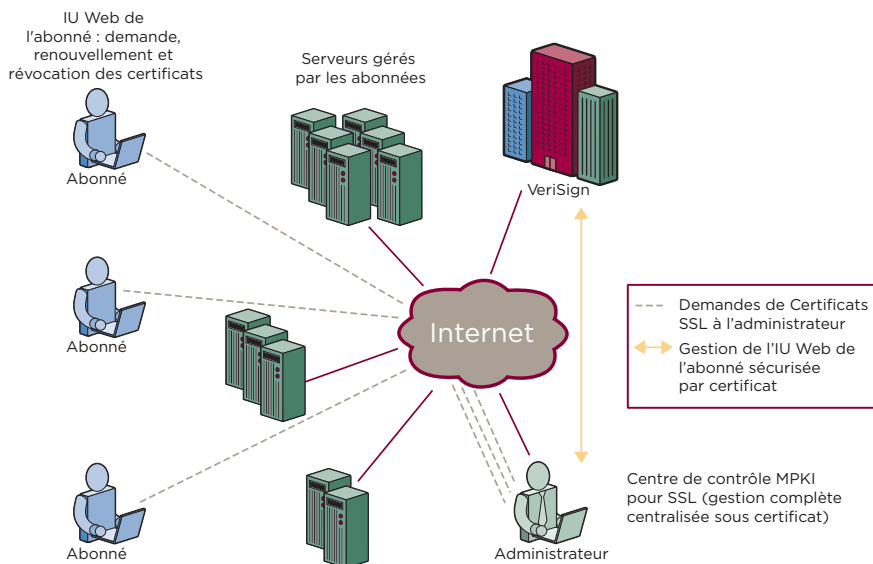


Un contrôle centralisé grâce à l'interface Web locale

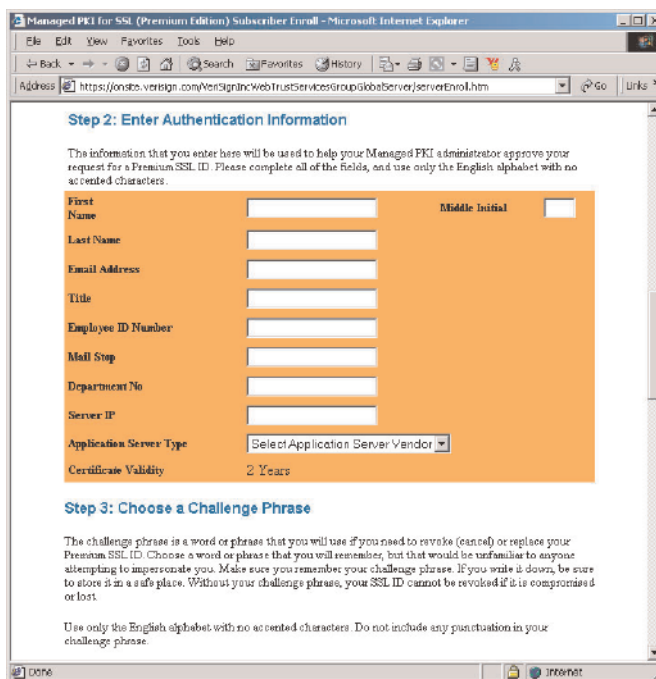
La clé de l'automatisation de processus proposé par les solutions MPKI pour SSL et MPKI pour Intranet SSL de VeriSign est l'infrastructure Web hébergée. L'administrateur local de votre organisation peut ainsi gérer de manière centralisée toutes les étapes du cycle de vie d'un certificat SSL, à l'aide des outils de gestion de l'interface Web appelée Centre de contrôle (Control Center). Les administrateurs authentifiés se servent de ce Centre de contrôle pour gérer et surveiller les procédures de demande, de validation, d'émission, de refus, de révocation et de renouvellement des certificats. Le Centre de contrôle propose les fonctions suivantes :

- Gestion PKI complète
- Contrôle et administration centralisés
- Accès à des rapports spécifiques pour la recherche des détails d'un certificat
- Journal de vérification de tous les certificats émis et de toutes les actions administrateur
- Alertes par courrier électronique
- Téléchargement de CRL
- Aide en ligne interactive

Les outils de gestion incluent également le composant « Outils abonnés », qui permet la délégation des tâches sur la base de rôles, pour une administration partagée. Les abonnés d'un certificat communiquent avec le système par le biais d'écrans personnalisés. Toutes les données sont automatiquement traitées au niveau du centre de données fournisseur hébergé par VeriSign, qui joue le rôle de relais masqué entre l'administrateur et les utilisateurs ; le schéma ci-dessous représente les flux de travail entre ces différentes entités :



Les écrans de l'interface Web personnalisable permettent aux utilisateurs de demander des certificats et d'effectuer d'autres tâches sans qu'une intervention humaine ne soit nécessaire. Par exemple, l'illustration ci-dessous présente l'écran de navigateur type de l'outil MPKI pour SSL ou MPKI pour Intranet SSL de VeriSign, qui permet la saisie des informations relatives à une demande de certificat.



Ce que disent les détenteurs d'une solution MPKI pour SSL de VeriSign:

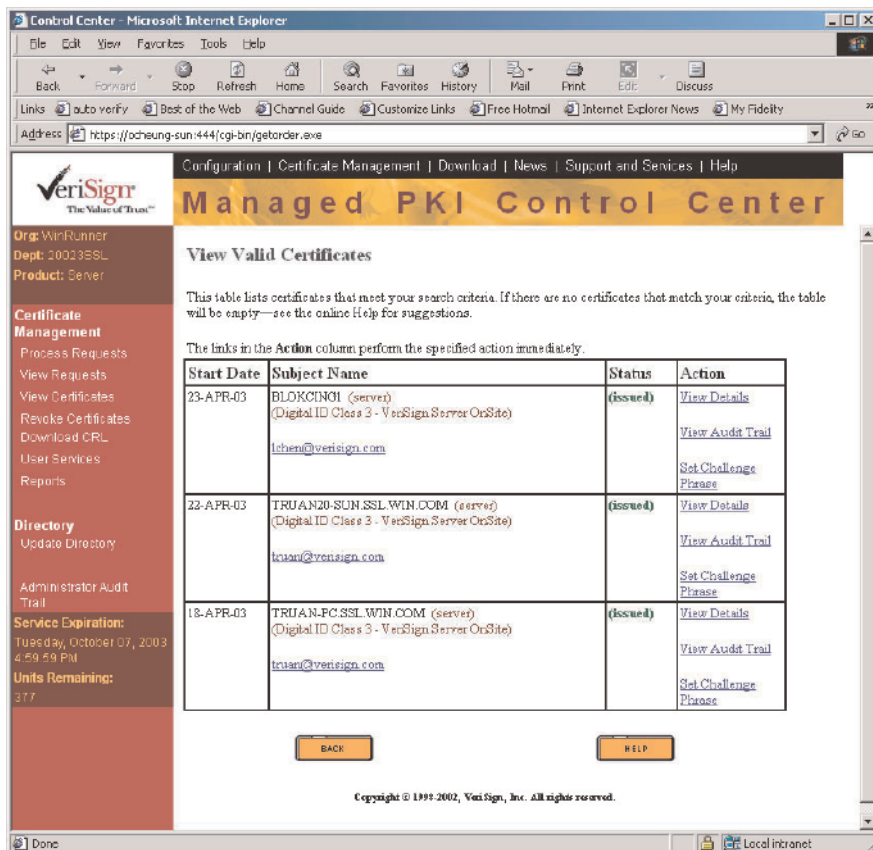
- 94 % contrôlent de manière centralisée la gestion et les coûts de certification
- 59 % utilisent un seul administrateur; 27 % en utilisent deux
- 53 % estiment que les coûts internes sont inférieurs à 5 % du prix du certificat ; 41 % les estiment entre 5 et 25 %
- 64 % utilisent certains certificats pour des applications internes, derrière le pare-feu (d'après une étude datant de 2003 ; 76 % de ces sociétés comptaient plus de 1 000 employés)

Des rapports automatisés pour un meilleur contrôle

Le Centre de contrôle contient un historique complet de toutes les activités relatives au certificat. Les rapports Web automatiquement générés par MPKI pour SSL et MPKI pour Intranet SSL de VeriSign donnent un point de vue précis et en temps réel des certificats sur l'ensemble de la société. Les rapports servent également de support de vérification tiers sur l'activité des certificats.

Les rapports répertorient les certificats demandés, validés, émis, refusés et révoqués. L'illustration ci-dessous présente un rapport type indiquant les certificats valides.

Grâce au Centre de contrôle, votre administrateur peut également filtrer les rapports en fonction de la date et afficher toutes les données, ou encore rechercher des détails granulaires spécifiques. Les administrateurs peuvent afficher les résultats d'une recherche quand ils le souhaitent, en téléchargeant un fichier de rapport CSV, généré par VeriSign, qu'ils peuvent ensuite importer dans une application de tableur.



Solutions de certificats Managed PKI pour SSL de VeriSign

VeriSign a créé les solutions Managed PKI pour SSL et Managed PKI pour Intranet SSL afin de faire face à vos besoins en matière de sécurité SSL, à l'intérieur et à l'extérieur du pare-feu :

Premium Edition—SSL Security 128 bits utilisée pour la protection des données les plus confidentielles de votre réseau. Les certificats Managed PKI pour SSL Premium Edition de VeriSign utilisent la technologie de cryptographie SGC (Server Gated Cryptography) qui permet la prise en charge du cryptage SSL 128 bits sur la majorité des ordinateurs actuels, y compris les anciens navigateurs et tous les systèmes Windows 2000.

- Les certificats SSL Premium Edition garantissent une session SSL 128 bits avec tous les navigateurs actuels. D'autres autorités de certification proposent leurs propres certificats SSL « 128 bits », mais ceux-ci n'utilisent pas la technologie SGC et ne peuvent donc garantir ce niveau de cryptage sur tous les systèmes. Les anciennes versions et certaines versions exportées de navigateur, ainsi que de nombreux systèmes Windows 2000 (quelle que soit la version d'Internet Explorer installée) doivent donc se contenter d'un degré de cryptage inférieur.
- VeriSign est la seule autorité de certification agréée par le Ministère américain du commerce (U.S. Department of Commerce) à fournir des certificats SSL 128 bits SGC hors des États-Unis.

Standard Edition. Protection des données confidentielles sur les Intranets et les sites Web publics. Les certificats SSL Standard Edition de VeriSign offrent :

- Un cryptage SSL 128 bits pour la communication avec des navigateurs Microsoft et Netscape récents
- Un cryptage SSL 40 bits pour la communication avec les anciennes versions et les versions exportées des navigateurs Microsoft et Netscape, ainsi que de nombreux systèmes Windows 2000

Prise en charge étendue de la plate-forme serveur. Les certificats Managed PKI pour SSL Standard et Premium Edition de VeriSign sont compatibles avec presque toutes les plates-formes serveur existantes. (Pour plus de détails, visitez le site <http://www.verisign.fr/products/site/secure/index.html>)

Processus de cryptage optimal. VeriSign protège les entreprises grâce au processus de cryptage de certificat le plus fiable du marché, composé de trois niveaux. Ainsi, nous vérifions et garantissons l'existence légale de l'organisation et son nom de domaine, par un processus de double vérification impliquant des recherches et des appels individuels réalisés par le personnel de VeriSign.

Garantie maximum. Chaque Certificat Managed PKI pour SSL est pris en charge par le programme d'assurance NetSure® de VeriSign, qui protège les détenteurs de certificats SSL de VeriSign contre toute perte financière découlant du vol, de l'altération, de l'usurpation ou de la perte d'un certificat. La garantie est limitée à un montant de 250 000 \$ pour les certificats MPKI pour SSL Premium et de 100 000 \$ pour les certificats Standard.

La solution hébergée MPKI pour SSL de VeriSign offre l'infrastructure intégrée suivante :

- Expertise PKI
- Personnel informatique qualifié
- Personnel de sécurité qualifié
- Serveurs redondants
- Mise en réseau redondante
- Sauvegarde/Récupération sur sinistre
- Centre de données renforcé
- Centre de contrôle réseau renforcé
- Alimentation redondante, système CVCA
- Commandes d'accès physiques et numériques
- Commandes d'accès physiques et numériques
- Authentification numérique
- Gestion des clés souches
- Audits de sécurité tiers
- Assurance responsabilité civile

Un service de niveau professionnel avec l'expertise SSL à votre disposition

L'un des principaux avantages des solutions hébergées de Verisign MPKI pour SSL et MPKI pour Intranet SSL est que votre société a accès en permanence à une expertise unique en matière de sécurité. VeriSign, leader du marché mondial, a déjà émis plus de 430 000 certificats SSL. Dans le cadre de ces solutions, le client a accès à une large palette de services d'assistance pour les entreprises, notamment :

- Un centre de données de niveau mondial, disponible 24 heures sur 24 et 7 jours sur 7
- Un service d'assistance disponible 24 heures sur 24 et 7 jours sur 7
- Des ressources Web exhaustives
 - Des séminaires techniques en ligne
 - Une base de connaissances
 - Des conseils de dépannage
 - Des didacticiels
 - Des foires aux questions (FAQ)
- Niveaux d'assistance : Standard, Gold, Platinum
- Temps de réponse : Contrats de niveau de service pour chaque niveau d'assistance et de gravité
- Une sécurité physique AC maximum
 - Infrastructure de sécurité de niveau 7
 - Aucun point faible ni problème en salle de secours
 - Structure de récupération
 - Niveaux de performances garantis et capacité évolutive

Outre les options d'assistance disponibles, un interlocuteur VeriSign particulier est affecté à votre dossier. Aucune autre autorité de certification ne vous proposera une expérience et des services aussi complets que VeriSign.

Découvrez et testez les avantages de MPKI pour SSL

Les solutions MPKI pour SSL et MPKI pour Intranet SSL de VeriSign vous aideront à simplifier la gestion des certificats SSL de votre organisation, sans nécessiter d'installation ou d'utilisation directe de matériel ou de logiciels. En quelques clics, vous pourrez facilement demander, valider, émettre, refuser, révoquer et renouveler les certificats SSL de toute votre entreprise, à partir d'un point d'administration central unique. Grâce à VeriSign, vous gagnez du temps en effectuant toutes ces opérations à la demande, quand vous le souhaitez. Toutes les activités de gestion sont sécurisées grâce aux processus d'authentification et de cryptage. Des tarifs dégressifs sont proposés pour l'achat en gros de certificats SSL.

+ Offre d'essai

VeriSign vous invite à découvrir et tester les avantages d'un service Web hébergé et automatisé pour la gestion de vos certificats SSL. Pour demander une version de démonstration gratuite de MPKI pour SSL de VeriSign ou en savoir plus sur MPKI pour Intranet SSL, contactez l'un de nos experts en sécurité SSL au 0800 90 43 51, option 2.

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