



FICHE TECHNIQUE

AVANTAGES CLÉS

Complet

VeriSign® Identity Protection (VIP) inclut des moyens invisibles (VeriSign® Identity Protection Fraud Detection Service) et plus visibles (VeriSign® Identity Protection Authentication Service) de sécurisation des identités en ligne.

Simple

VIP permet à l'utilisateur de vivre une expérience extrêmement sécurisée et parfaitement adaptée à son style de fonctionnement sur le Web. L'approche unique orientée service de VIP permet à l'entreprise d'en déléguer la complexité.

Intelligent

VIP Shared Authentication Network (Réseau d'authentification partagé pour la protection d'identité de VeriSign) et VIP Fraud Intelligence Network (Réseau de renseignements sur les fraudes pour la protection d'identité de VeriSign) permettent à une entreprise d'y voir mieux et plus clairement. Grâce à l'exploitation de l'infrastructure DNS/ internet et à son infrastructure d'authentification partagée, VeriSign dispose d'une vision unique et complète de l'intelligence Internet non accessible aux autres solutions logicielles.

Éprouvée

VeriSign est, de longue date, le fournisseur de services d'authentification de plus de 500 000 sites Web : pour 93 % des entreprises du Fortune 500, 40 des plus grandes banques du monde et 47 sites de commerce électronique sur les 50 plus importants. Au final, le sceau VeriSign Secure Site Seal signifie vraiment quelque chose pour les consommateurs et est depuis longtemps associé au commerce sécurisé.

VeriSign® Identity Protection

L'usurpation d'identité sur Internet, le « phishing » et la fraude financière en ligne sont des motifs forts de déploiement de systèmes puissants d'authentification pour les applications orientées utilisateurs. Avec le développement d'initiatives nouvelles de la part des établissements financiers et des sites de commerce électronique pour proposer des services en ligne supplémentaires, les organismes gouvernementaux recommandent désormais des principes de protection d'identité. Par exemple, le récent guide concernant l'authentification dans un environnement bancaire sur Internet (FFIEC-AUTH), publié par le Federal Financial Institutions Examination Council (FFIEC), recommande que les établissements financiers offrant des produits et des services sur Internet emploient des méthodes efficaces d'authentification des clients utilisant ces produits et services. Plus particulièrement, le FFIEC-AUTH considère que l'authentification à un seul facteur comme seul mécanisme de contrôle est inadapté dans le cas de transactions à risque élevé impliquant l'accès aux informations des clients ou le mouvement de fonds vers d'autres destinataires.¹

Chez VeriSign, nous pensons qu'il faut une approche entièrement nouvelle de la protection des identités numériques. Cette nouvelle approche doit comprendre une défense complète et intégrer des services et une approche réseau. Cette nouvelle approche doit également être cohérente avec le style de fonctionnement sur le Web des consommateurs en fournissant une solution flexible basée sur le risque avec un impact minimum sur l'expérience utilisateur.

Présentation de VeriSign® Identity Protection (Protection d'Identité de Verisign, VIP) - VeriSign Identity Protection est la suite la plus complète de services de protection et d'authentification d'identité conçue pour renforcer et protéger les identités numériques des consommateurs. Proposé sur un réseau partagé sécurisé, VIP aide à gérer le risque pour la réputation des services financiers, des entreprises de commerce électronique ou des entreprises qui traitent numériquement les données personnelles de leurs clients.

Pourquoi VeriSign est-il en mesure de proposer la meilleure solution de protection d'identité ?

- 80 % des utilisateurs en ligne reconnaissent le sceau VeriSign Secured Seal comme la marque de confiance pour les transactions en ligne sécurisées.
- VeriSign propose déjà des services d'authentification à presque 500 000 sites Web : à plus de 93 % des entreprises du Fortune 500, aux 40 plus grandes banques du monde et à 47 sites de commerce électronique sur les 50 plus importants.
- Avec ses résultats éprouvés qui font fonctionner l'infrastructure critique pour Internet, VeriSign est le seul fournisseur d'authentification à utiliser une infrastructure de réseau globale et disposant d'une fiabilité et d'un temps de fonctionnement reconnus.

¹ Authentification dans un environnement bancaire sur Internet, http://www.ffiec.gov/pdf/authentication_guidance.pdf



Where it all comes together.™

+ Protection des identités numériques avec une identité visible et invisible et des services d'authentification

VeriSign Identity Protection fournit une protection de l'identité invisible et visible, ou proactive, et consolidée par des services réseau afin de permettre le partage des références et de proposer une intelligence au niveau d'Internet.

+ VeriSign® Identity Protection Fraud Detection Service

La détection de fraude est essentielle pour permettre une authentification basée sur le risque, avec laquelle une entreprise peut mettre en œuvre une authentification basée sur le risque proportionné d'une transaction donnée. Le Service VIP Fraud Detection (Service de détection de fraude pour la protection d'identité de VeriSign) fournit un moyen invisible de protéger proactivement les consommateurs. Grâce à l'utilisation d'une technologie avancée de détection d'anomalies, le service détecte les connexions et transactions frauduleuses en temps réel sans affecter l'expérience Web de l'utilisateur légitime. La solution adopte une approche de la détection de fraude basée sur l'auto-apprentissage, en s'adaptant aux habitudes d'utilisation de chaque consommateur. Grâce à l'utilisation de cette technologie de reconnaissance de règles et de schémas d'utilisation, le service identifie les activités potentiellement frauduleuses sur la base de types connus de fraude et de comportements non associés à l'utilisateur. Le service apprend automatiquement, il peut s'adapter en fonction des modifications des comportements criminels, et ce sans intervention manuelle. Cette approche non intrusive ne nécessite aucune modification des sites Web et reste invisible pour les consommateurs tant qu'aucune fraude n'est détectée.

Le VIP Fraud Detection Service offre quatre avantages clés

- **Invisible pour le consommateur.** VIP Fraud Detection Service ne modifie en rien l'expérience des utilisateurs : ils se connectent au site Web comme d'habitude.
- **Simple à mettre en œuvre.** VIP Fraud Detection Service est une solution côté serveur uniquement, qui n'exige aucun changement pour l'utilisateur final.
- **Intelligent.** VIP Fraud Detection Service inclut à la fois des systèmes reposant sur des règles et un moteur basé sur l'auto-apprentissage pour identifier la fraude. En outre, VIP Fraud Detection Service s'intègre au VIP Fraud Intelligence Network (Réseau de renseignements sur les fraudes pour la protection d'identité de VeriSign).
- **Conformité à bas coût.** VIP Fraud Detection Service est un moyen économique de se conformer aux normes gouvernementales.

+ VeriSign® Identity Protection Authentication Service

Le « VeriSign® Identity Protection Authentication Service » (Service d'authentification pour la protection d'identité de VeriSign) fournit une sécurité solide et visible pour les applications de commerce en ligne. VIP Authentication Service permet à une entreprise d'émettre et/ou d'accepter facilement plusieurs références pour chaque utilisateur. Le service d'authentification VIP fournit la meilleure sécurité actuellement disponible pour les transactions des consommateurs. L'idéal pour les transactions à valeur et à risque élevés.

VIP Authentication Service adopte des standards ouverts et permet d'utiliser tout périphérique compatible OATH (Open Authentication, Authentification ouverte) pour l'authentification. VIP Authentication Service inclut un certain nombre d'options pour des facteurs supplémentaires, dont des périphériques autonomes tels que des jetons à mot de passe à usage unique (One Time Password, OTP) ainsi que des périphériques « logiciels » tels que l'OTP à commande vocale et question/ réponse. À l'avenir, VIP Authentication prendra également en charge les OTP sur SMS et les téléphones cellulaires OTP.

VIP Authentication Service utilise une infrastructure de validation partagée exploitée par VeriSign qui permet aux entreprises de déployer une authentification forte sans avoir à supporter le poids de la gestion et du fonctionnement de leur propre infrastructure d'authentification.

+ VeriSign® Identity Protection Portal

Le portail « VeriSign Identity Protection Portal » (Portail de protection de l'identité de VeriSign) est un système de gestion complet du cycle de vie des références, incluant l'approvisionnement, la distribution et la prise en charge externalisés des consommateurs finaux. Au niveau du VIP Portal, les utilisateurs finaux pourront se procurer des références à deux facteurs et pourront également les gérer et les mettre à jour centralement.

En se servant de la fonctionnalité du VeriSign Identity Protection Portal, les entreprises peuvent proposer de façon économique et rapide une authentification forte à leurs clients, et ce pour un coût nettement inférieur à celui de la mise au point et de la gestion de leur propre solution complète. Les entreprises peuvent ainsi se concentrer sur leurs activités principales tout en mettant en œuvre la marque réputée de sécurité de VeriSign.

+ VeriSign® Identity Protection Fraud Intelligence Network

Le réseau « VIP Fraud Intelligence Network » (Réseau de renseignements sur les fraudes pour la protection d'identité de VeriSign, VIP FIN), qui sera mis à disposition des clients au deuxième semestre 2006, est un mécanisme permettant le partage des renseignements sur les fraudes entre les sociétés et sur Internet et constituera une option à valeur ajoutée supplémentaire du VIP Fraud Detection Service. Il englobe deux niveaux de partage des renseignements. Le premier inclut l'extension du service VIP Fraud Detection Service afin de comparer les modèles de comportement des sites Web participant en temps réel. VIP FIN peut aider à détecter et à stopper des attaques qui n'auraient pas pu être détectées avec les données d'un seul site. VIP FIN ne nécessite aucune information d'identification personnelle pour détecter une fraude, mais il peut utiliser des pseudonymes uniques pour identifier les utilisateurs finaux des sites Web.

Le deuxième niveau de partage de renseignements est l'ajout du niveau d'intelligence Internet dérivé de l'exploitation par VeriSign de l'infrastructure Internet critique.

+ VeriSign® Identity Protection Shared Authentication Network

Il peut être onéreux d'ajouter l'authentification multifactorielle à une application en ligne orientée utilisateur.

- Le système doit permettre l'émission simple de seconds facteurs à des millions et des millions d'utilisateurs.
- Entretien plusieurs périphériques et utilisateurs exige un programme de service clients et de maintenance coûteux.

La façon la moins onéreuse d'ajouter une authentification multifactorielle est de passer par le réseau « VIP Shared Authentication Network » (Réseau d'authentification partagé pour la protection d'identité de VeriSign). Dans le VIP Shared Authentication Network, un site n'a pas à supporter le poids du développement, de l'assistance aux clients et de la maintenance du système. Au contraire, un site peut rejoindre le réseau VIP Network en tant que partie utilisatrice, simplement utiliser les références VIP déjà émises et payer seulement une participation modeste par utilisateur pour les validations. Un site Web peut ajouter une authentification forte sans coûts d'expédition ni de relation client supplémentaires.

Si votre activité exige une authentification forte, vous pouvez émettre des jetons utilisables sur le réseau VIP Network. Les émetteurs profitent de tous les avantages des parties utilisatrices, avec des coûts de transaction moindres, la possibilité de promouvoir leur marque via le jeton et un meilleur contrôle des expériences Web de leurs clients finaux.

Pour que l'authentification des consommateurs soit largement adoptée, les clients doivent être en mesure d'utiliser un périphérique unique de second facteur d'authentification qui répond à tous leurs besoins de sécurité dans les domaines de la banque en ligne, du courtage, des soins de santé et du commerce électronique. Sans cette flexibilité, les clients risquent de finir avec un « collier de jetons », une chaîne de jetons uniques émis par différents fournisseurs, qui sécurisent des transactions ou des sites Web uniques. Avec le Shared Authentication Network, VeriSign Identity Protection (Protection d'identité de VeriSign) adopte une approche entièrement nouvelle pour relever ce défi. Les utilisateurs pourront utiliser le même périphérique d'authentification à deux facteurs partout où est apposé le logo VIP.

eBay® et PayPal® sont des partenaires de fond du réseau VIP Token Sharing Network (Réseau à partage de jetons pour la protection d'identité de Verisign). Dès 2006, les clients eBay utiliseront un jeton VIP pour sécuriser leurs achats en ligne.

+ Pour en savoir plus

Les services de sécurité de VeriSign protègent les interactions en ligne, permettant aux entreprises de gérer les risques liés à l'image, à l'exploitation et à la conformité de la façon la plus simple et rentable possible.

Pour plus d'informations sur les solutions VeriSign Identity Protection, veuillez composer le 0800 90 43 51 ou envoyer un courrier électronique à l'adresse suivante : unifiedauthentication@verisign.fr.

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