SECURITY BOX®

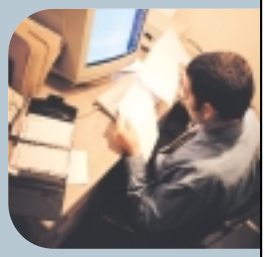
Security BOX® Business Solutions

Finmatica

The Value of Innovation.

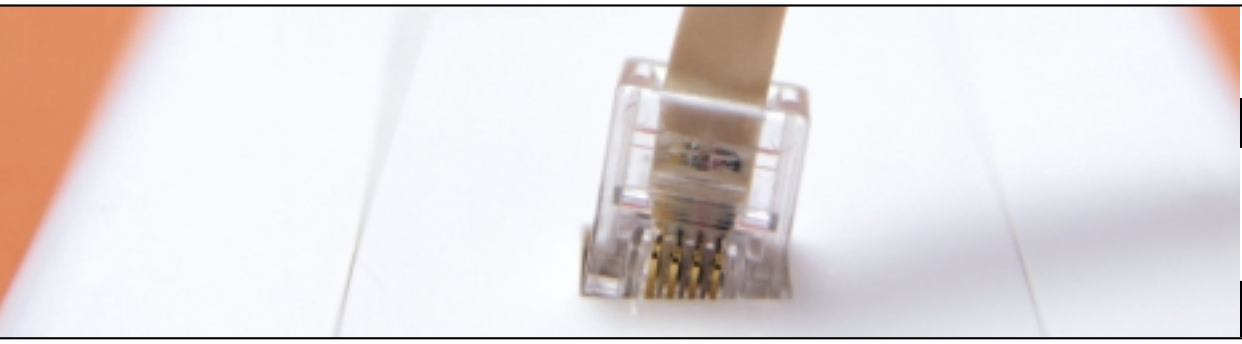
Les usages professionnels des réseaux locaux, d'Intranet, d'Internet, et des messageries électroniques sont de plus en plus courants...

Au sein des **Entreprises**, l'utilisation des réseaux locaux et d'Intranet rend chaque jour les collaborateurs de plus en plus "en ligne" avec le système d'information.
Le réseau Internet "ouvert" à l'ensemble de la planète, voit son usage s'amplifier tous les jours pour des échanges d'informations de partenaire à partenaire ou de client à fournisseur.



Pour les **Communautés Professionnelles** (notaires, avocats, professionnels de la Santé,...), les communications via Internet et les messageries ne cessent de se développer et véhiculent de plus en plus souvent des informations sensibles.

Les **Administrations**, tout comme les Entreprises, font aussi un grand usage des réseaux Intranet et de la messagerie pour accéder aux données de leur système d'information.
Par ailleurs, pour faciliter les relations avec les administrations, nous assistons à la mise en place sur Internet de "télé-procédures" utilisables par les Entreprises et les Particuliers.



SECURITY BOX®

...ils induisent de forts besoins de protection des données et des communications...

La **confidentialité** et **l'intégrité** des données, **l'authentification** des correspondants lors d'une communication, et la signature de fichiers, de documents et d'emails sont au premier plan des préoccupations des professionnels pour lutter contre les malveillances de l'intelligence économique, pour garantir les transactions commerciales ou plus simplement pour protéger la vie privée des individus.
On constate aujourd'hui que les sites centraux des systèmes d'information des entreprises sont généralement protégés. Cependant, de larges besoins de sécurité subsistent au niveau des **stations de travail** et des **serveurs Web sensibles.**
A ce niveau, la protection des données et des communications peut se faire par la mise en place de **logiciels cryptographiques** associés ou non à des composants matériels (par exemple cartes à microprocesseur, clés USB...).

La protection des fichiers

Assurer la **confidentialité** des fichiers sur le poste de travail par un logiciel cryptographique permet de lutter contre la consultation de ces données par une personne non autorisée. Cette fonction est particulièrement importante pour les ordinateurs portables souvent exposés à des risques de vol ou de consultation pirate, mais reste également nécessaire dans le cadre bureautique (surtout pour un ordinateur en réseau).

La protection des messageries

La messagerie est devenue un outil de travail courant et efficace, il complète (voir remplace souvent) l'usage du téléphone et apporte en plus la transmission de pièces jointes (informations qui auparavant circulaient par courrier ou par télécopie). En ce sens, la messagerie est doublement porteuse d'informations précieuses qu'il est plus que jamais nécessaire de chercher à protéger quelque soit le parcours emprunté, lors de leur acheminement. Signer les messages, pour garantir au récepteur leur origine et leur intégrité (voir chercher à constituer une preuve ou un élément de preuve), et les crypter, pour en assurer la confidentialité, constituent aujourd'hui le meilleur moyen de protéger ce mode de communication très apprécié et utilisé dans le monde professionnel.

La protection des communications Internet

Les fonctions d'authentification réciproques garantissent à l'utilisateur d'un navigateur Internet qu'il est en communication avec le bon serveur Web (et pas avec un serveur pirate), et au serveur Web qu'il a en ligne un utilisateur autorisé. La confidentialité et l'intégrité des données transmises sur le réseau sont des solutions couramment proposées pour sécuriser les communications avec les serveurs Web sensibles.

Une solution... la cryptographie

En l'absence de protection intrinsèque des systèmes d'exploitation et des réseaux, la seule solution consiste à sécuriser les données elles-mêmes tout au long de leur cycle de vie. Cette sécurisation doit cependant utiliser des moyens incontournables même pour le plus doué des hackers.

La cryptographie est en ce sens une approche mathématique du problème qui permet de quantifier l'effort d'attaque et donc de mesurer le niveau de protection effectif.
Les protections habituelles (droit d'accès, firewall, ...) sont des barrières chaque jour franchies et rehaussées, alors que la cryptographie porte sur les données elles-mêmes et apporte un coût de franchissement qui se chiffre généralement en années, voire en siècles de calcul de milliers d'ordinateurs, tant les probabilités nécessaires au "cassage" d'un code sont importantes.

La cryptographie permet de remplir la plupart des fonctions évoquées plus haut (authentification, confidentialité, intégrité, signature).
La mise en œuvre de cette technologie passe alors par le déploiement de solutions logicielles, adaptées à chaque besoin fonctionnel, comme peuvent l'être Security BOX® Mail pour la messagerie, Security BOX® File pour la protection des fichiers, Security BOX® SHL pour la protection des communications Internet.

Comment déployer des logiciels cryptographiques ?

Distribuer les logiciels sur chaque poste de travail

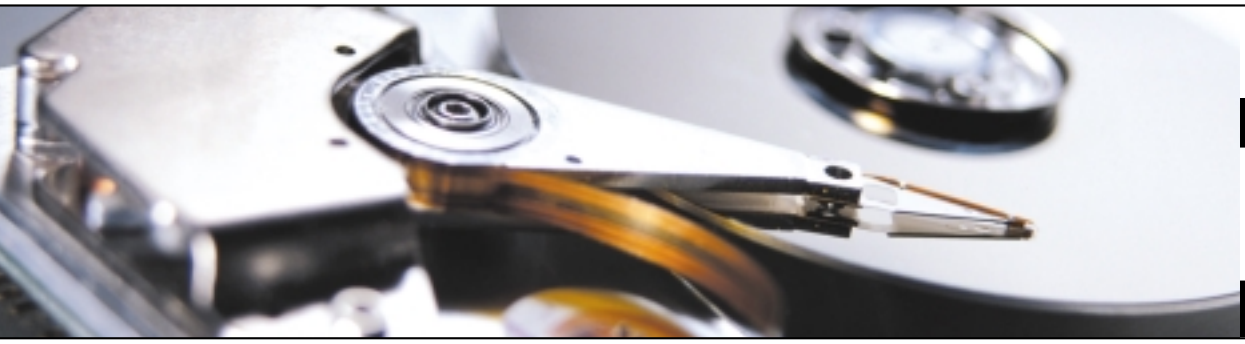
Comme pour tout logiciel standard cette opération peut être réalisée par une installation locale (sur chaque poste) ou peut être prise en charge par des mécanismes d'installation automatisés (master logiciels, distribution automatisée via un serveur, ...).

Doter chaque utilisateur de clés et de certificats

Deux approches sont possibles :
Décentralisée : l'utilisateur crée ses clés sur son poste de travail, puis effectue une demande de certification de sa clé publique auprès de l'Autorité de certification que lui a désigné son administrateur (voir encart Technologie et État de l'art).
Centralisée : l'administrateur de la sécurité procède aux opérations de création de clés et de certificats pour l'ensemble des utilisateurs ; il distribue ensuite les clés et les certificats via un moyen sécurisé (par exemple en les plaçant dans une carte à microprocesseur ou une clé USB).

Définir les options d'utilisation des logiciels cryptographiques

Définir à l'avance, pour les utilisateurs, le niveau de cryptage et la puissance des clés à utiliser, imposer ou présélectionner les options de configuration relèvent également des règles de sécurité propre à chaque entreprise.



SECURITY BOX®

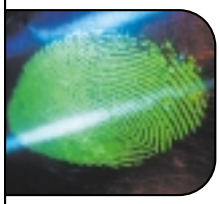
Technologie et État de l'art

Les fonctions de confidentialité, d'authentification et de signature font appel à des processus cryptographiques dits "à clés asymétriques" qui constituent aujourd'hui l'état de l'art en la matière.

En voici les principes :

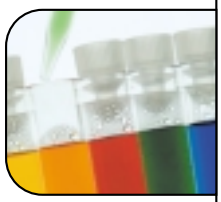
Les clés de l'utilisateur

Chaque utilisateur se dote d'une clé en deux parties : la première partie est la "clé privée" de l'utilisateur ; sa protection doit être assurée soit en l'inscrivant dans un composant matériel (carte à microprocesseur, clé USB), soit en la conservant cryptée par un mot de passe.
La deuxième partie est la "clé publique" de l'utilisateur qui comme son nom l'indique peut être publiée.
Les clés de l'utilisateur peuvent être générées par l'utilisateur lui-même ou produites de façon centralisée par un administrateur de la sécurité.



Le certificat de l'utilisateur

Pour éviter toute usurpation d'identité, avant d'être publiée, la "clé publique" d'un utilisateur doit être certifiée par une Autorité reconnue qui peut être publique (opérateur de certification) ou interne à l'entreprise.
Le rôle de l'Autorité consiste à certifier l'identité du porteur d'une clé publique donnée, en procédant à une identification formelle de cette personne. Elle assure également le contrôle de possession de la clé privée correspondante.
L'Autorité délivre alors un certificat signé, qui permettra à un tiers de s'assurer que la clé publique qu'il va utiliser appartient bien à la personne avec laquelle il veut effectuer un échange sécurisé.
L'Autorité peut également se charger de la publication des certificats dans un annuaire.

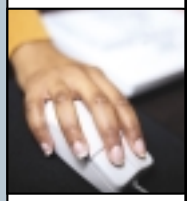


Le principe de fonctionnement

Pour envoyer un message de façon confidentielle à un correspondant :
(X) chiffre un message avec la "clé publique" de son correspondant (Y).
(X) connaît cette clé puisqu'elle est publiée et certifiée par l'Autorité.
(X) transmet ce message crypté sur le réseau sans aucun risque car seul (Y) détient la "clé privée" permettant de décrypter le message.

Pour signer un message, (X) utilise sa "clé privée" qui l'identifie totalement (il est le seul à la posséder). Ses correspondants pourront contrôler la signature du message en utilisant la "clé publique" de (X) qui a été publiée et certifiée par l'Autorité.

Security BOX® **Business Solutions**



Poste utilisateur

FILE
DISK
SHREDDER

INTERNET
OUTLOOK
LOTUS NOTES

SHL PROXY

LOGON -SSO
Mot de passe
Carte à puce
Token

Administration Gestion de clés

ANNUAIRE LDAP

CRLS

Security BOX® Manager

PKI

Offres externes
Certplus, GIP-CPS, Verisign...

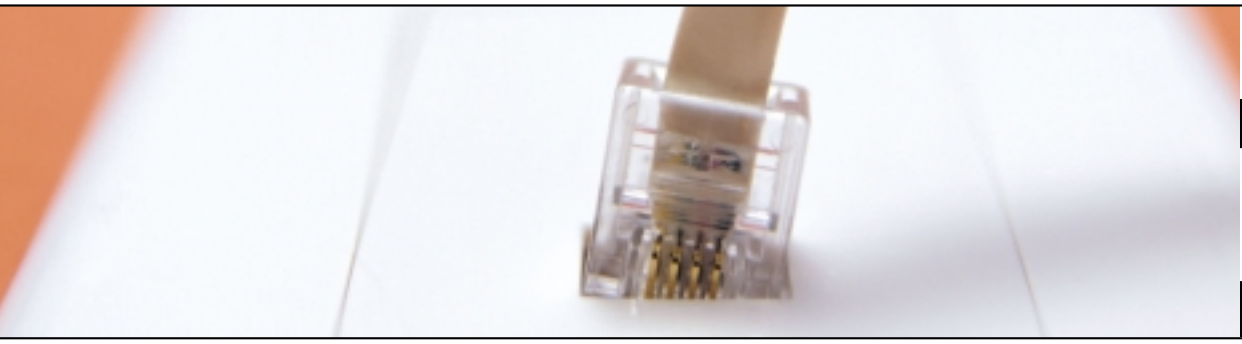
Offres internes
Iplanet, Microsoft...

Une suite logicielle pour sécuriser les stations de travail

Security BOX® Business Solutions n'est pas un produit en tant que tel, mais une "suite" logicielle (ensemble de plusieurs logiciels complémentaires). Cette "suite" regroupe plusieurs produits qui peuvent être achetés et installés ensemble ou séparément. La "suite" comprend notamment :
Security BOX® File pour le cryptage des fichiers, **Security BOX® Mail** pour le cryptage et la signature d'email, **Security BOX® SHL** pour l'authentification et le cryptage des communications Internet.
L'architecture modulaire et évolutive de la "suite" permet d'équiper progressivement les stations de travail, de tout ou partie des produits, sans pour autant remettre en cause ni les habitudes de travail des utilisateurs, ni la configuration des comptes de sécurité et encore moins l'infrastructure de gestion de clés (PKI) si elle existe déjà.

L'administration et le déploiement peuvent être gérés par un logiciel complémentaire **Security BOX® Manager**. Cette solution permet à l'Administrateur de gérer les "comptes" de chaque utilisateur.

On appelle compte, la structure de données sécurisées, propre à chaque utilisateur, qui regroupe les informations le concernant : ses clés, ses certificats, les paramètres de configuration et les options de fonctionnement de Security BOX®.



Security BOX® **Business Solutions**

Les fonctions communes

Tous les produits de la "suite" **Security BOX® Business Solutions** disposent d'un certain nombre de fonctions de gestion qui sont automatiquement installées lorsqu'on utilise un produit.
La "suite" bénéficie en outre d'une approche intelligente visant à ne pas installer deux fois les mêmes composants, mais à les partager dynamiquement, lorsqu'au moins deux produits sont installés sur le même ordinateur.
On parlera alors de fonctions communes, dont les principales sont détaillées ci-après :

Identification unique (Single log-on)

Cette fonction permet à l'utilisateur de s'identifier une fois pour toutes. A partir du moment où l'identification a eu lieu une fois (par exemple le matin au démarrage de l'ordinateur), l'utilisateur n'aura plus besoin de ressaisir ni son mot de passe ni son code PIN pour accéder aux différentes fonctions des produits de la suite Security BOX® (File, Mail, SHL).

Cartes à microprocesseur et clés USB

L'identification des utilisateurs peut être effectuée au choix au moyen d'un mot de passe, d'une carte à microprocesseur ou d'une clé USB.
Ce choix est déterminé à l'installation du logiciel mais peut être modifié par la suite.
Plusieurs marques de cartes à microprocesseur et de clés USB sont supportées, notamment les produits des compagnies suivantes : Eutron, Schlumberger, Oberthur, Gemplus, Rainbow, et cartes CPS pour le secteur de la Santé.

Annuaire local

L'annuaire local permet aux utilisateurs d'avoir accès aux clés publiques de leurs interlocuteurs et aux autorités de certification déclarées comme étant de confiance.
Cette fonction apporte un réel avantage fonctionnel dans le cas d'ordinateurs non connectés ou portables.
Par contre, si les clés d'un interlocuteur ne figurent pas dans l'annuaire local et que l'ordinateur est de nouveau connecté au système d'information de l'entreprise, la recherche est alors basculée de manière automatique et transparente vers les annuaires LDAP accessibles.

Annuaires LDAP

Security BOX® Business Solutions supporte la recherche et la consultation sur plusieurs annuaires LDAP internes ou externes (annuaires d'entreprises / annuaires publics). La grande souplesse d'administration et la vitesse de recherche, inhérentes aux annuaires LDAP apportent un grand niveau de confort pour l'utilisateur de Security BOX®. Une fois l'accès à l'annuaire paramétré, la recherche des clés publiques de correspondants est totalement transparente et immédiate.

Gestion des CRLs

Security BOX® Business Solutions supporte la recherche et la consultation des CRLs.

Security BOX® **Business Solutions**

Respect des standards

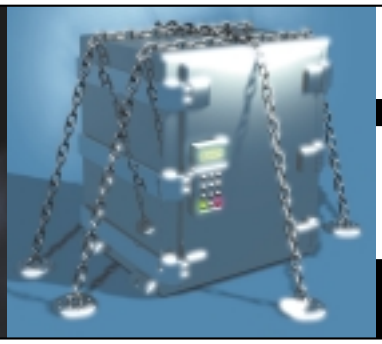
Le respect des standards (certificats X509, PKIx, S/Mime) et la conception des produits Security BOX® apportent la garantie d'un fonctionnement optimum pour les besoins de sécurité d'aujourd'hui comme de demain.
Cette notion apporte une totale compatibilité avec d'autres produits de sécurité (par exemple : échange de mails entre Security BOX® Mail et une autre solution également compatible S/Mime) ainsi qu'avec les logiciels de PKI (Public Key Infrastructure) déployés en entreprise, que ce soit sous une forme internalisée ou externalisée, apportant ainsi une complète flexibilité quant au choix de l'opérateur ou du système de certification.

Gestion et administration des comptes Security BOX®

Security BOX® Manager est l'outil d'administration et de déploiement de la "suite" Security BOX®.
Il peut fonctionner de manière autonome ou être interfacé à une PKI, permettant alors la certification et la publication dans un annuaire de clés des utilisateurs.
Security BOX® Manager assure également le paramétrage des différentes options de sécurité : le cryptage, la signature, le compte des utilisateurs, l'automatisation du cryptage.

Ergonomie

Les solutions Security BOX® sont faciles à utiliser. Elles proposent des interfaces simples et permettent l'usage du clic droit de la souris et du glisser-déposer (drag&drop).
Les options de sécurité sont riches mais néanmoins aisément accessibles et toujours accompagnées de guides et d'explications commentées (wizards).



SECURITY BOX® FILE

Security BOX® **File**

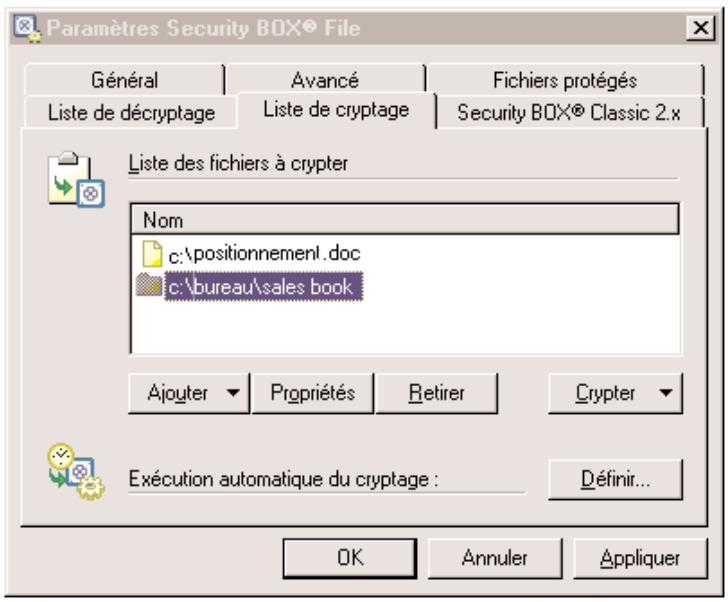
Security BOX® File est un logiciel de cryptage des données. Il protège les fichiers et les répertoires pour les ordinateurs portables et les ordinateurs bureautiques connectés au réseau. Il offre également des fonctions d'effacement irréversible des données.

Security BOX® File est un logiciel d'une grande facilité d'utilisation fonctionnant sous Microsoft Windows.

Security BOX® File assure la sécurité de vos données de plusieurs manières :

Cryptage à la demande ou automatique
Security BOX® crypte les fichiers et les répertoires par un simple clic droit de souris ou par glisser-déplacer (drag & drop) depuis la fenêtre active du logiciel.

Security BOX® File permet de créer des listes de cryptage (et décryptage) automatiques afin de faciliter la gestion quotidienne des données sensibles. Le cryptage d'un répertoire ou des fichiers *.doc peut être, par exemple, lancé automatiquement tous les soirs à 19h30 ou déclenché automatiquement à la fermeture de Windows.
Security BOX® File permet d'interdire le cryptage de certains fichiers tels que les fichiers systèmes afin de prévenir les risques de mauvaise utilisation ou d'erreur d'inattention.

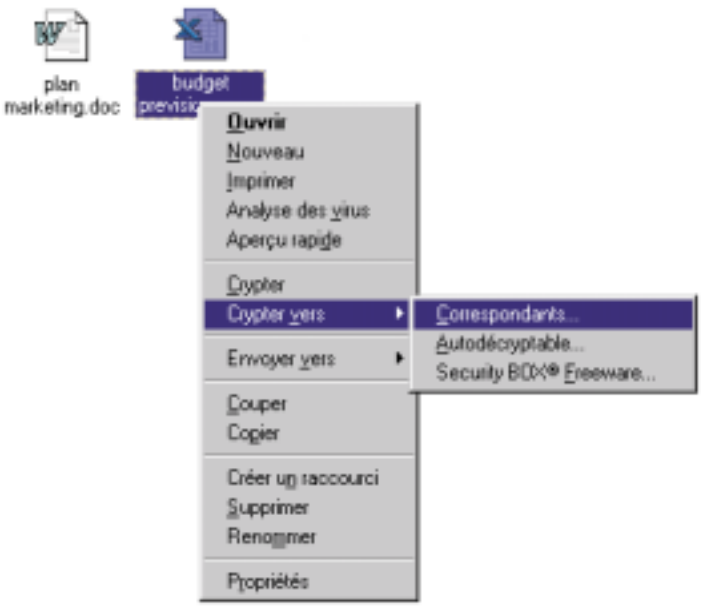


Security BOX® **File**

Echange de fichiers cryptés

• Crypter pour un correspondant

L'utilisation du système de cryptage à clés publiques supporté par Security BOX® File permet de crypter des fichiers pour un ou plusieurs correspondants, sans avoir besoin de leur communiquer de mot de passe. Les fichiers sont cryptés à l'aide des clés publiques des destinataires et seuls ceux-ci pourront avoir connaissance de l'information, puisqu'ils sont les uniques détenteurs de la clé privée (voir paragraphe "Technologie et état de l'art").



• Crypter pour un correspondant qui ne possède pas Security BOX® File

Deux options sont possibles dans ce cas :

Auto-décryptable

La fonction auto-décryptable permet de transformer un fichier normal en un fichier auto-exécutable, contenant le fichier crypté et le programme nécessaire à son décryptage. Il suffit de choisir un mot de passe pour ce fichier, de le communiquer à son correspondant (par téléphone, courrier, email...) puis de transmettre le fichier auto-décryptable.

Crypter au format Security BOX® Freeware

Security BOX® File permet également de crypter des fichiers pour des correspondants disposant de Security BOX® Freeware (Security BOX® Freeware est téléchargeable gratuitement sur Internet www.securitybox.net).
Pour communiquer de manière sécurisée, il suffit d'envoyer le fichier (en pièce jointe par exemple) et de communiquer le mot de passe ayant servi au cryptage. Cette technique à l'avantage de permettre le transfert d'un fichier crypté sans passer par un programme auto-décryptable (fichier.exe).
En effet, récupérer sans vigilance depuis Internet et utiliser sur son ordinateur des fichiers.exe, dont on ne connaît pas forcément la provenance (comme ceux reçus en pièce jointe d'email), peut représenter une source potentielle de risque. De nombreux virus existent sous la forme de fichiers.exe et la confusion pour un utilisateur distrait peut être facile.

SECURITY BOX® FILE

Security BOX® **File**

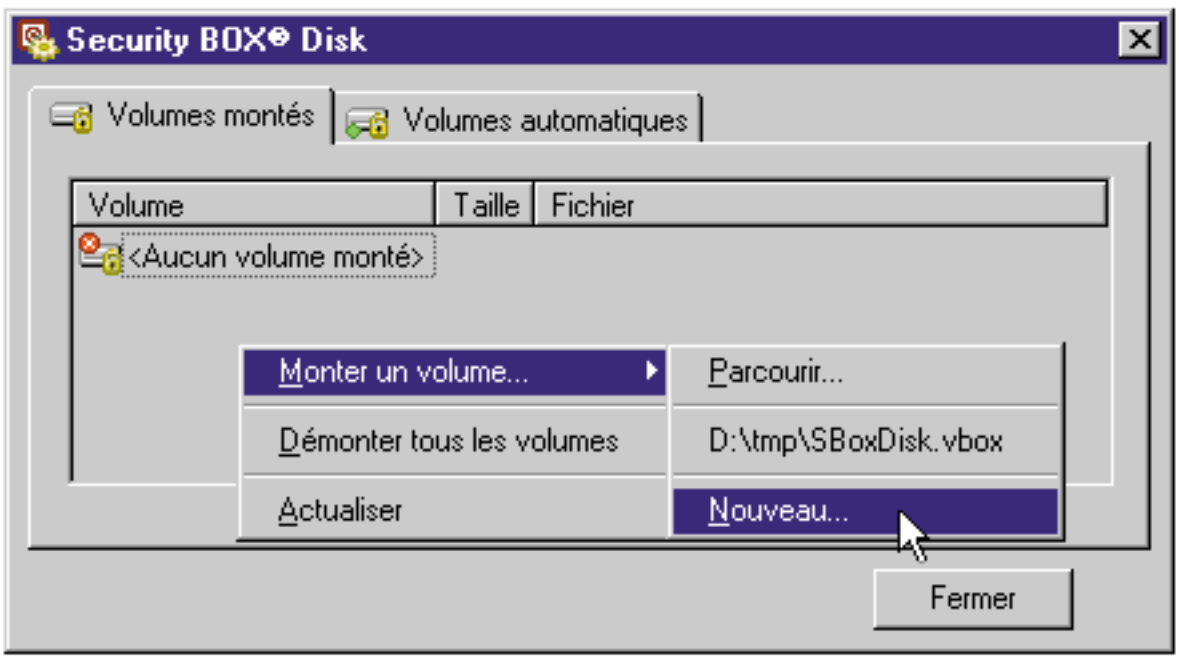
Security BOX®File dispose d'outils complémentaires et optionnels (appelés extensions) qui renforcent la sécurité active du poste de travail.

• **Security BOX® Disk Extension :** Security BOX® Disk Extension sécurise les fichiers créés ou déposés sur un volume disque virtuel. La mise en œuvre de cette option ne modifie aucunement l'utilisation du produit, l'utilisateur aura juste l'impression de disposer d'un nouveau disque dur sur sa machine.

Ressemblant en tous points à un disque dur normal, celui-ci apporte néanmoins :

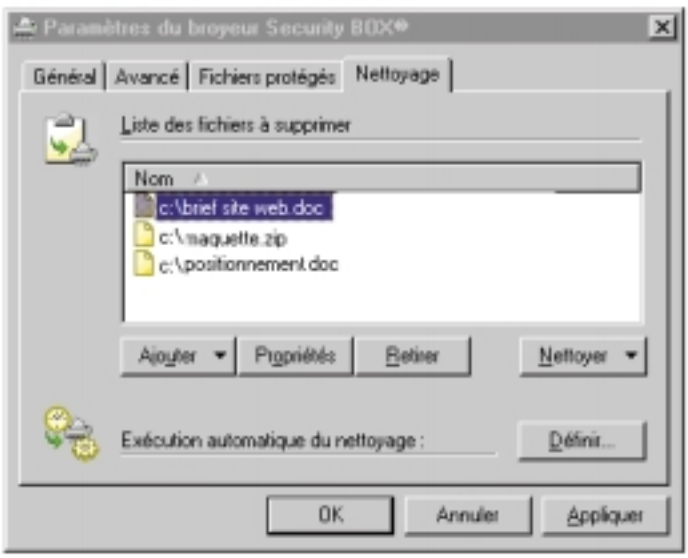
- une sécurisation permanente et à la volée (toutes les informations qui y sont déposées sont automatiquement cryptées).
- une accessibilité inégalée, le disque virtuel apparaît automatiquement une fois que l'utilisateur est connecté et disparaît dès que l'utilisateur se déconnecte de Security BOX®.

Le fort niveau de sécurité induit par ce mécanisme (les données restent cryptées en permanence sur le disque dur et seule l'information consultée à un moment donné est décryptée en mémoire) associé au très grand confort d'utilisation font de Security BOX® Disk Extension une réelle avancée en terme de sécurité et de simplicité d'utilisation.



Security BOX® **File**

• **Security BOX® Shredder Extension :** Cette seconde extension de Security BOX® File efface de manière irréversible les traces résiduelles des fichiers effacés par Windows afin d'éviter leur possible recouvrement.
Le mécanisme consiste à ré-écrire sur un fichier anciennement effacé et donc d'écraser son contenu. Le nombre de passes de ré-écriture ainsi que leurs attributs est paramétrable afin de garantir un bon niveau de sécurité.
Il est possible d'effacer irréversiblement (ou de broyer) des fichiers par un simple glisser-déplacer (drag & drop) ou en utilisant la fonction "envoyer vers"

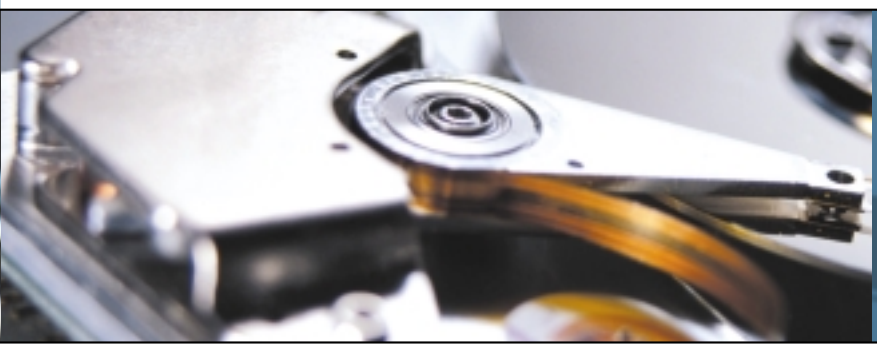


de Windows. Il est également possible d'automatiser cette tâche en créant une " liste de nettoyage ". Cette fonction peut se déclencher dans le temps pour une plus grande facilité d'usage : à heures fixes, toutes les X minutes ou à la déconnexion de Security BOX®.

Administration et déploiement

Security BOX® File et ses extensions sont conçus pour être installés simplement en mode "autonome" sur un ordinateur PC individuel. Cependant le logiciel est également prévu pour être déployé automatiquement et à grande échelle par des automates d'installation.
Il est possible de paramétrer à l'avance toutes les options du logiciel afin de :

- Restreindre le choix des algorithmes de cryptage,
- Choisir la longueur des clés utilisées,
- Sélectionner le niveau de renouvellement des mots de passe et des listes de fichiers,
- Protéger certains fichiers système contre un cryptage ou un broyage accidentel...



SECURITY BOX® MAIL

Security BOX® **Mail**

Security BOX® Mail est un logiciel de sécurité pour la messagerie, il assure la signature électronique et le cryptage des emails émis et reçus.

Facile à installer et sans impact sur les habitudes de travail, Security BOX® Mail apporte un fort niveau de sécurité pour tout échange d'email interne comme externe à l'entreprise.

Respectant les standards S/MIME et X 509, Security BOX® Mail permet, non seulement d'assurer le plus fort niveau de sécurité aujourd'hui disponible pour vos emails, mais reste également interopérable avec toute autre solution respectant S/Mime.

Une utilisation transparente

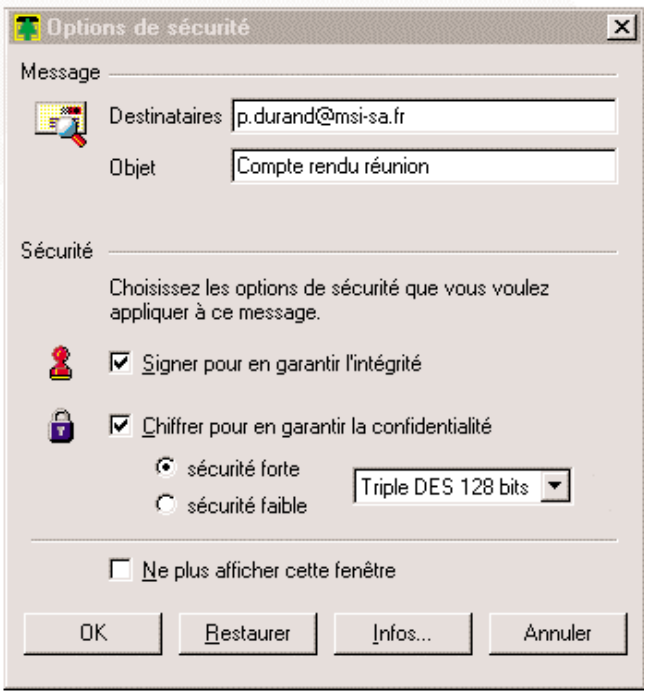
Complètement intégré à votre logiciel de messagerie (mailer), Security BOX® Mail s'utilise de manière intuitive au travers de deux boutons qui permettent à l'utilisateur de protéger ses courriers électroniques en les signant, en les cryptant ou les deux simultanément.

La conservation des messages cryptés

Security BOX® crypte les messages envoyés et les conserve cryptés dans la boîte de réception de votre outil de messagerie. Ainsi, et tant que vous n'êtes pas connecté à Security BOX®, personne ne pourra lire les emails cryptés que vous avez reçu, même après que vous les avez déjà lus.

L'émission d'un message crypté et/ou signé

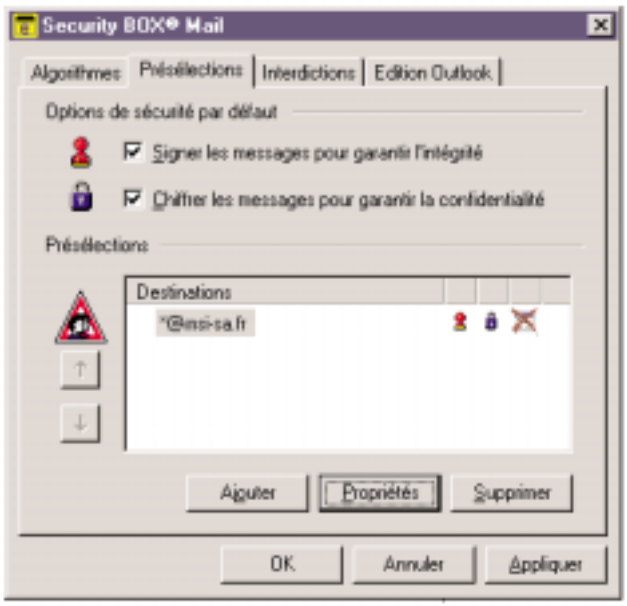
A chaque émission d'un message (et si l'on n'a pas utilisé les boutons) Security BOX® propose le cryptage ou la signature de l'email.
Il est également possible d'éviter cette question en automatisant les options de sécurité pour les destinataires (par exemple tous les emails envoyés à XXXXX@msi-sa.fr seront systématiquement signés et cryptés).



Security BOX® **Mail**

Présélections et interdictions

Security BOX®Mail permet de présélectionner les options de sécurité d'un message en fonction de ses destinataires. Par exemple, vous pouvez souhaiter : signer et chiffrer automatiquement vos messages destinés à votre siège social, ce qui automatisera le cryptage pour ces destinations et assurera une sécurité automatique.
De la même manière, il sera possible d'interdire des destinations.



La délégation de déchiffrement

Cette option consiste à permettre à une autre personne (par exemple votre secrétaire) de décrypter et lire vos messages en votre absence. Il faut pour cela lui déléguer votre clé personnelle (si vous ne possédez qu'une seule clé) ou votre clé de cryptage (si vous possédez deux clés différentes pour signer et crypter).

La gestion des CRLs (Certificate Revocation List)

Un certificat est valide durant une période définie. A l'expiration de cette période, il devient naturellement invalide. Il est parfois également nécessaire de révoquer un certificat (le rendre invalide) avant sa date d'expiration (notamment en cas de vol du PC ou de la carte à microprocesseur, de corruption du mot de passe ou du code PIN). Pour savoir si le certificat de votre correspondant est révoqué (et donc ne pas lui envoyer de message crypté avec cette clé), il suffit de disposer d'un logiciel supportant la fonction CRL, c'est notamment le cas de Security BOX® Mail.

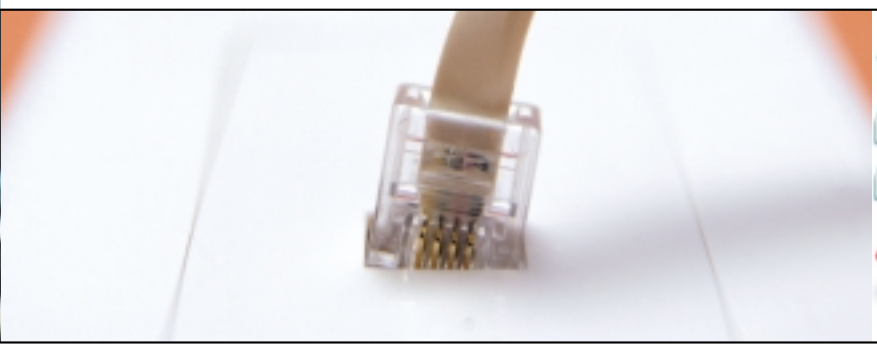
Administration

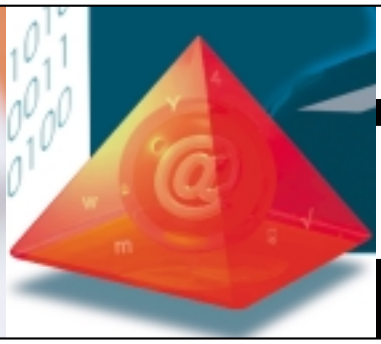
Pour faciliter la gestion en entreprise, Security BOX® Mail est administrable. Il est donc possible de paramétrer différentes options de sécurité telles que :

- Forcer le cryptage et/ou la signature d'emails vers un correspondant ou un domaine,
- Interdire tout envoi d'emails vers un correspondant ou un domaine,
- Paramétrer le profil de sécurité de l'utilisateur (compte de messagerie sécurisé, algorithme de cryptage, clés de l'utilisateur...).

Interopérabilité

- Plug-in pour messagerie SMTP/Pop 3 (Microsoft Outlook Express, Netscape, Messenger, Eudora light...),
- Plug-in pour Microsoft Outlook 98, 2000, XP,
- Plug-in pour Lotus Notes 5.x,
- Interopérable avec tous les produits S/MIME.





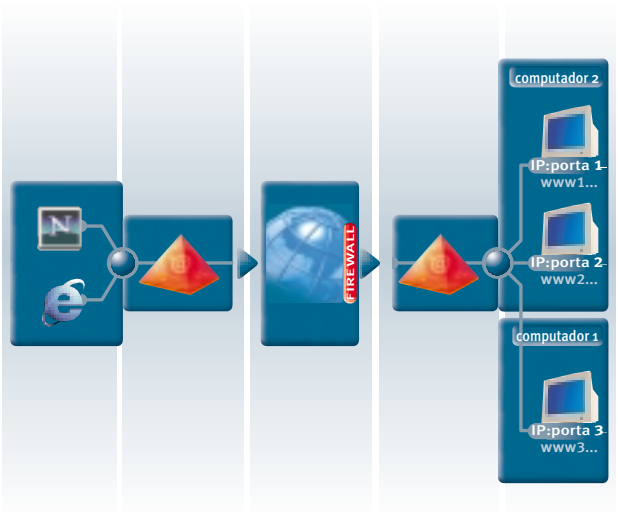
SECURITY BOX® SHL

Security BOX® **SHL**

La solution SHL est composée d'un logiciel serveur de sécurité fonctionnant en frontal d'un serveur Web : SHL Gateway et d'un logiciel client fonctionnant en plug-in d'un navigateur Internet : SHL Proxy.
Ces deux logiciels s'intercalent de part et d'autre de la liaison " navigateur / serveur Web " afin d'y appliquer des services de sécurité cryptographiques (authentification, intégrité, confidentialité).

Security BOX® SHL est le logiciel de sécurité, permettant de sécuriser les communications de type Web sur Internet ou Intranet par des dispositifs de sécurité cryptographiques éprouvés. Cette solution est particulièrement bien adaptée aux besoins de protection pour :

- **L'Intranet**
- **Les serveurs de formulaires administratifs, commandes, abonnements, inscriptions...**
- **Les Extranets d'entreprises**

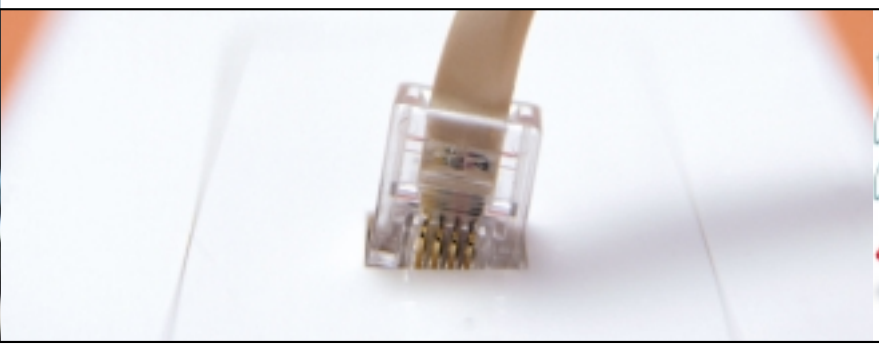


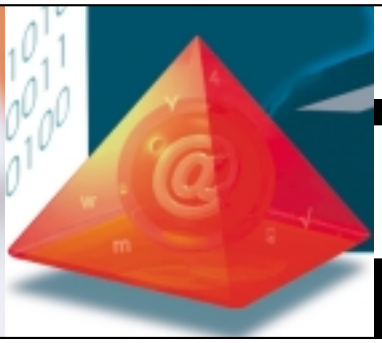
Security BOX® **SHL**

Solution pour serveur

SHL Gateway est une " passerelle " de sécurité intervenant sur le contenu des données transférées entre un serveur et un navigateur Internet. Elle mutualise la gestion de la sécurité pour plusieurs sites (chaque site pouvant néanmoins être configuré de manière particulière), déchargeant les serveurs Web de lourds calculs algorithmiques et simplifiant la gestion par la mise en œuvre de règles de sécurité plus homogènes. Elle permet également d'externaliser la sécurité en la dissociant du développement des pages Web.

Paramétrée de manière externe par un professionnel de la sécurité, SHL Gateway garantit un fort niveau de sécurité par des fonctions d'authentification, de scellement de cryptage, imputables de manière générique (*.html, *gif, *.*), sans impact sur les évolutions futures du site.





SECURITY BOX® SHL

Security BOX® **SHL**

Un logiciel conçu pour assumer de fortes charges

SHL Gateway a été conçue pour traiter un très grand nombre de sessions de sécurité; des requêtes simultanées, des requêtes en cours (de réception, d'acheminement vers le serveur Web, d'attente de réponse du serveur Web, de réception de réponse du serveur Web, d'acheminement de réponse...), sur plusieurs serveurs Web à la fois.
Architecturée autour d'une conception Multi-thread (threads systems) qui permet de tirer pleinement partie des machines multi-processeurs ; les traitements des flux de connexions et requêtes sont alors effectués sans contention ou rétention grâce à un acheminement à la volée.
SHL Gateway est composée d'un seul processus "demon Unix ou service NT", mais il est possible d'en lancer plusieurs sur la même machine (sous réserve des droits de licence acquis).

Compatibilité avec les standards de l'Internet

SHL Gateway est compatible avec tous les serveurs Web du marché (Microsoft IIS, Netscape Server, Lotus Domino, Apache, ...) et les différentes technologies de contenu en vigueur (Javascript, Java-Server, ActiveX, ASP, etc.).
Respectant la norme Http, SHL est entièrement compatible avec tous les types de Firewall, routeurs, proxies utilisés dans le monde Internet.
SHL s'installe et s'utilise sans nécessiter aucune modification des sites web côté Gateway, ni aucun paramétrage côté Proxy.

Security BOX® **SHL**

Solution pour poste client

• Security BOX® SHL Proxy

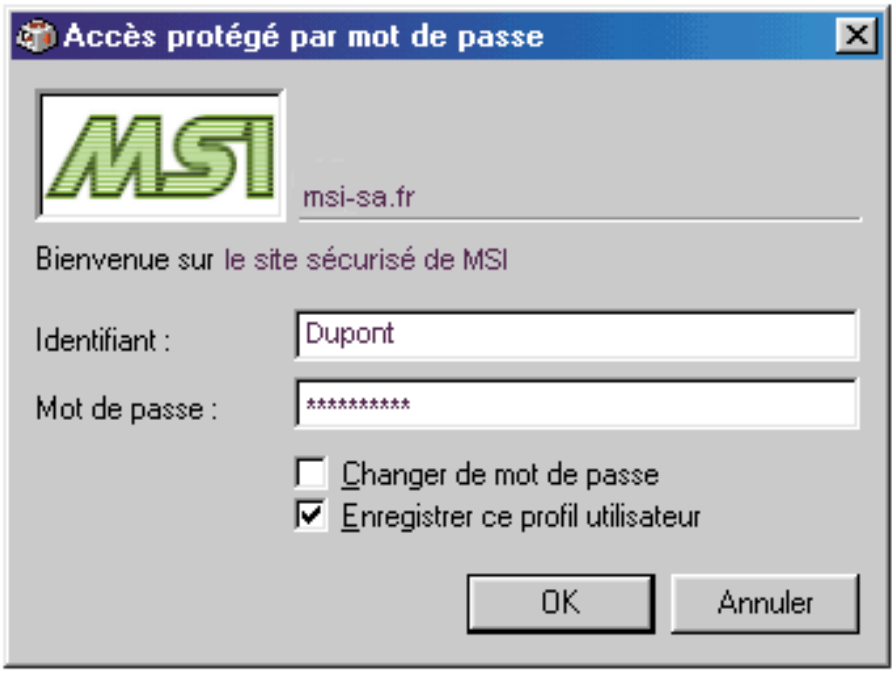
Security BOX® SHL Proxy se télécharge et se paramètre automatiquement avec le ou les navigateur(s) présent(s) sur le poste lors de son installation. Il entre ensuite automatiquement en action lorsqu'il détecte une communication sécurisée avec un serveur SHL Gateway. Le logiciel met alors en œuvre les services de sécurité requis par le serveur (demande d'authentification, intégrité/scellement des données, cryptage automatique et à la volée des données échangées).

Ce logiciel gratuit et téléchargeable fonctionne sur systèmes PC et MAC et permet une authentification forte par "mot de passe" utilisant une technologie de mot de passe dynamique ou "pass ticket" afin d'assurer une authentification non-re-jouable sur le réseau.

Security BOX® SHL Proxy fonctionne avec tous les navigateurs Internet du marché (Microsoft, Netscape, ...).

• Security BOX® SHL Pro

Security BOX®SHL Pro est une version plus évoluée de Security BOX®SHL proxy permettant une authentification forte par certificat RSA en cohérence avec la gamme Security BOX® Business Solutions.
Security BOX®SHL Pro permet de bénéficier de l'identification unique (Single log-on) de l'ensemble de la gamme Security BOX® Business Solutions.
Ainsi l'utilisateur s'identifie une seule fois (par mot de passe ou carte à microprocesseur).



SECURITY BOX® MANAGER

Security BOX® **Manager**

Security BOX® Manager est l'outil d'administration de la gamme Security BOX® Business Solutions. Il permet la création, la gestion et le paramétrage des comptes utilisateurs. Cette gestion des comptes utilisateurs assure la garantie de l'application des mesures et des politiques de sécurité mises en place par la société.

Gestion des utilisateurs

- Création de bases utilisateurs,
- Importation de listes d'utilisateurs,
- Création, suppression, modification d'utilisateurs,
- Création des comptes Security BOX® Business Solutions.

Gestion du porte-clés

- Tirage ou importation des clés (clé publique/clé privée),
- Génération des clés de chiffrement, de signature, de déchiffrement, de recouvrement,
- Demande de certificats,
- Import / Export de certificats,
- Export au format P12.

Paramétrage des annuaires

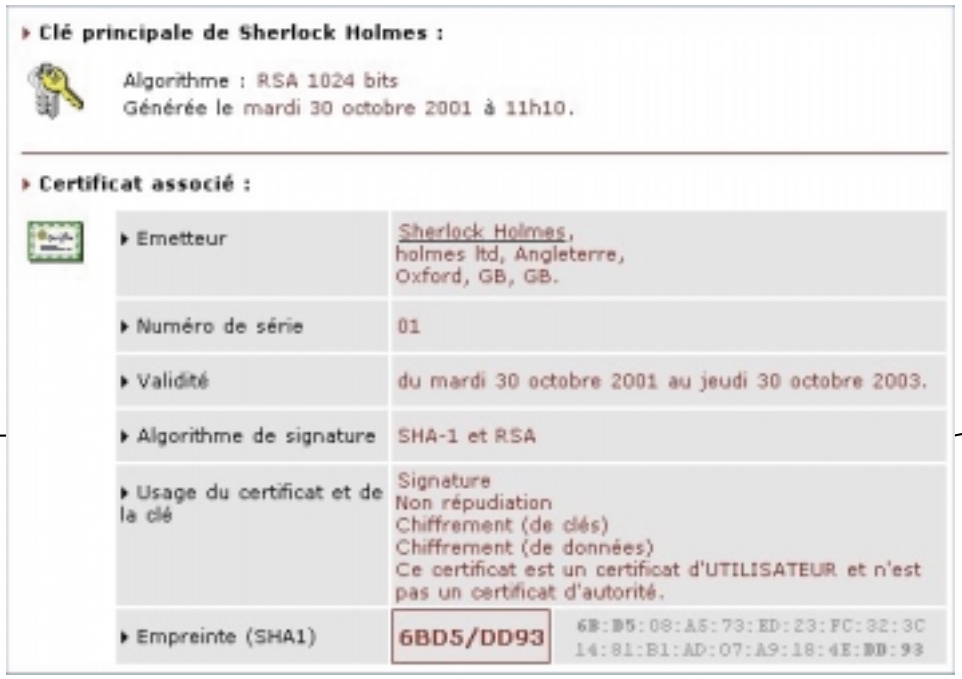
- Annuaire local de l'utilisateur,
- Lien vers les annuaires LDAP.

Personnalisation des cartes et clés USB

- Ecriture des secrets (clés) dans la carte ou la clé USB,
- Tirage des clés dans la carte (inboard key generation) puis écriture des certificats dans la carte.

Liaison avec un logiciel de PKI

- Emission/Réception de demandes de certification vers la PKI,
- Liaison vers les annuaires LDAP.



Security BOX® **Manager**

Paramétrage des logiciels Security BOX®

Security BOX® Manager permet d'industrialiser le déploiement des logiciels Security BOX® en présélectionnant à la place des utilisateurs toutes les options des produits.
L'administrateur peut définir outil par outil les options qu'il souhaite proposer (modifiables par l'utilisateur), imposer (non modifiables par l'utilisateur) ou imposer de manière cachée (non modifiables et non visibles par l'utilisateur).
L'administrateur peut à tout moment modifier ces paramètres en publiant de nouveaux profils (fichiers .urs et .usd).

Toutes les options présentes dans les produits et visibles par l'utilisateur sont paramétrables :

Paramétrage de connexion

- Connexion par carte à puce ou mot de passe,
- Demande du code secret : à la connexion, à chaque opération, toutes les x minutes,
- Verrouillage de Security BOX® : au déclenchement de l'écran de veille, à l'arrachage de la carte,
- Changement de mot de passe : tous les x jours/mois.

Paramétrage pour Security BOX® File

- Choix des algorithmes et des longueurs de clés,
- Liste de fichiers à protéger contre le cryptage (ex : fichiers système),
- Liste de cryptage automatique,
- Liste de décryptage automatique,
- Importation des anciens comptes Security BOX® Classic.

Paramétrage pour Security BOX® Disk Extension

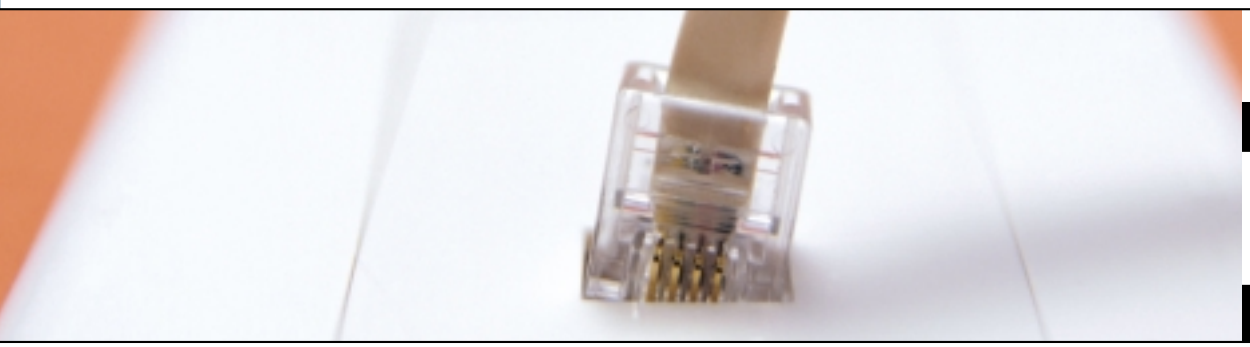
- Lancement automatique d'un volume virtuel crypté.

Paramétrage pour Security BOX® Shredder Extension

- Liste de fichiers à broyer automatiquement (ex : fichiers, répertoires ou *.*...),
- Liste de fichiers interdits au broyage (ex : fichiers, répertoires ou *.*...),
- Choix des caractéristiques d'effacement (nombre de passes, valeurs héxadécimales).

Paramétrage pour Security BOX® Mail

- Choix des algorithmes et des longueurs de clés,
- Présélection des options de sécurité par défaut en fonction des adresses email (chiffrer + signer pour *@msi-sa.fr),
- Interdiction d'envoi d'e-mail sécurisé en fonction des adresses,
- Présélection des options de confort (message de confirmation, affichage des comptes rendus de sécurité...) en fonction de l'outil de messagerie utilisé.



SECURITY BOX®

Security BOX® **Business Solutions**

Services d'accompagnement pour la mise en place d'une infrastructure pour clés publiques

Intégrateur spécialisé dans la mise en service d'infrastructure pour clés publiques (PKI), MSI intervient sur des projets de toutes tailles, du projet pilote de quelques dizaines d'utilisateurs jusqu'aux systèmes complets couvrant l'ensemble des établissements d'une entreprise.

MSI fournit des solutions clés en main en intégrant les différents composants nécessaires ; le logiciel de PKI, le composant de sécurité hardware (HSM) associé, l'annuaire LDAP, les logiciels cryptographiques sur les postes de travail (Security BOX® Business Solutions), le produit d'aide au déploiement (Security BOX® Manager), les cartes à microprocesseur ou les clés USB, le cas échéant.

Prestations type

- Rédaction de la PC (politique de certification) et de la DPC (déclaration des procédures de certification),
- Définition de l'architecture de la PKI (centralisée, répartie, redondante, etc...),
- Sélection d'un produit de PKI. Installation et configuration,
- Réalisation des travaux de personnalisation (habillage graphique, tuning,...),
- Réalisation de composants spécifiques si nécessaire (par exemple outils de personnalisation de cartes par lots),
- Qualification du système (fonctionnel, tenue en charge, endurance, volumétrie, exploitabilité,..),
- Manuels d'exploitation - formation des exploitants,
- Aide à la définition du déploiement des produits Security BOX® sur les postes de travail.

Security BOX® **Business Solutions**

Produits de PKI

MSI propose le logiciel PKI le plus adapté aux besoins et aux contraintes exprimées (fonctionnalités, architecture, volumétrie, pérennité, coûts). MSI dispose d'ingénieurs spécialisés sur l'installation et la mise en œuvre des principaux logiciels de PKI du marché (iPlanet, Microsoft, Baltimore).

HSM (hardware Security Module)

Le HSM, composant matériel de sécurité, est un dispositif additionnel à l'Autorité de certification qui renforce les opérations de certification en protégeant la clé de signature de l'Autorité.
Ce dispositif peut selon les cas prendre la forme, soit d'une carte cryptographique sur bus PCI, soit d'une boîte noire, soit plus simplement d'une carte à microprocesseur.

Aide au paramétrage

Security BOX® Manager est l'outil d'administration et d'aide au déploiement des logiciels de la gamme Security BOX® Business Solutions. Sa mise en œuvre, en complément d'une PKI, assure la centralisation des règles de sécurité définies par l'administrateur.

Cartes à microprocesseur et clés USB

MSI fournit et intègre les cartes à microprocesseur et les clés USB supportées en standard par les produits Security BOX® Business Solutions.
Les cartes à microprocesseur des constructeurs suivants sont aujourd'hui supportées :

- Eutron,
- Gemplus,
- OberthurCS,
- Rainbow,
- Schlumberger

Nota : cette liste non exhaustive est susceptible d'évoluer sans préavis

Caractéristiques techniques de la suite Security BOX® Business Solutions

Normes et standards supportés

- CMS (Cryptographic Message Syntax),
- S/Mime (Secure / Multipurpose Internet Mail Extensions) versions 2 et 3,
- LDAP (Lightweight Directory Access Protocol).
- X509 versions 1, 2, 3,
- CRLs (Certificate Revocation List),
- PKCS (Public-Key Cryptography Standards) PKCS# 1 / PKCS# 5 / PKCS# 7 / PKCS# 10 / PKCS# 11 / PKCS# 12.

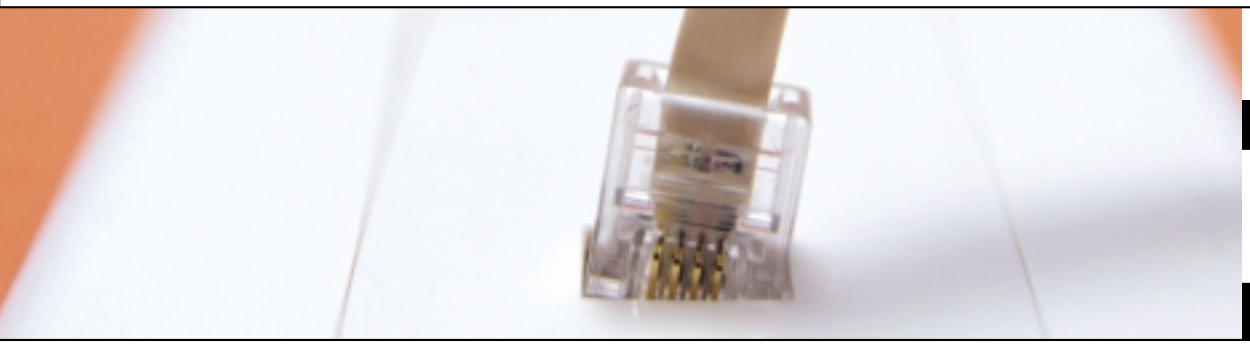
Algorithmes supportés*

*Clés variant de 40 à 256 bits en fonction des algorithmes

- RSA
- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- Triple DES
- RC2
- RC4
- RC5
- MD5
- SHA-1

Plates-formes supportées

- Microsoft Windows 98
- Microsoft Windows 98 SE
- Microsoft Windows Me
- Microsoft Windows NT
- Microsoft Windows 2000
- Microsoft Windows XP



SECURITY BOX®

Security BOX® **Business Solutions**

CATALOGUE

Security BOX® Business Solutions/Client

Désignation	Référence	Plate-forme
Security BOX® File Chiffrement - déchiffrement de fichiers + compression	SBF-10	Win32
Security BOX® Disk Extension *Extension de Security BOX ®File pour le chiffrement à la volée (disques virtuels cryptés)*	SBF-Disk-10	Win32
Security BOX® Shredder Extension *Extension de Security BOX® File pour broyer les fichiers (suppression et effacement sécurisé)*	SBF-Shredder-10	Win32
Security BOX® Mail – Edition Internet Chiffrement - signature de messages Mail au format S/Mime	SBM-I22	Win32
Security BOX® Mail – Edition Notes Chiffrement - signature de messages Mail au format S/Mime	SBM-N22	Win32
Security BOX® Mail – Edition Outlook Chiffrement - signature de messages Mail au format S/Mime	SBM-022	Win32
Security BOX® SHL Pro Authentification Web et chiffrement de trames Http Single login gamme Security BOX® Gestion avancée des cartes à microprocesseur	PSHLP-21	Win32
Security BOX® SHL Client Windows Authentification Web et chiffrement de trames Http	PSHLW-21	Win32
Security BOX® SHL Client Mac Authentification Web et chiffrement de trames Http	PSHLM-21	Mac/OS
Security BOX® Extension carte *Schlumberger : Cryptoflex / Cyberflex / E-gate* *OberthurCS : AuthentIC* *Gemplus : GPK / GemSafe*	KITCARD-10	Win32
Security BOX® Extension carte CPS *Middleware de raccordement pour cartes CPS*	KITCPS-24	Win32
Security BOX® Premium Package intégrant : • 1 licence Security BOX® File + Disk +Shredder • 1 licence Security BOX® Mail • 1 licence Security BOX® SHL Pro • 1 licence middleware extension carte (au Choix Gemplus, Oberthur, Schlumberger, CPS)	SBP	Win32

***WIN 32** : Windows 98, 98Se, Me, NT, 2000, XP / **MAC/OS** : Mac/OS 7.5.3 jusqu'à Mac/OS 9x

Security BOX® Business Solutions/Serveur

Désignation	Référence	Plate-forme
Security BOX® SHL Gateway Edition de base (500 utilisateurs / 3 destinations / 25 accès)	XPSHLB/2X	NT 2000 - XP - UNIX AIX - SOLARIS
Security BOX® SHL Gateway Edition Entreprise (500 utilisateurs / destinations illimitées / accès illimités)	XPSHLE/2X	NT 2000 - XP - UNIX AIX - SOLARIS

IMP-Teasing

Siège social
Http://www.msi-sa.fr
Http://www.securitybox.net
7, rue Jean Mermoz
78000 Versailles
Tel : +33 (1) 39 07 27 27
Fax : +33 (1) 39 07 27 20

RCS Versailles B 343 947 834
Code APE 722 Z

Agence de Brest
5, rue Benjamin Delessert
29200 Brest
Tel : +33 (2) 98 46 22 66
Fax : +33 (2) 98 46 95 46

Agence de Lyon
3, place Renaudel
69003 Lyon
Tel : +33 (4) 78 14 01 10
Fax : +33 (4) 78 14 04 11