

Token GIGA-PASS

Transformez vos clés USB en Tokens d'authentification

La clé USB Multifonction

La technologie GIGA-PASS permet d'accroître les possibilités des clés de stockage USB traditionnelles et de les utiliser pour authentifier les utilisateurs au système d'information de l'entreprise.

- ⇒ Ouvrir une session sur une station de travail
- ⇒ Chiffrer des données
- ⇒ Signer électroniquement une transaction
- ⇒ Etablir une liaison distante sécurisée (VPN)
- ⇒ Automatiser la connexion à de nombreuses applications (Single Sign On)

La clé USB conserve par ailleurs sa mission initiale de transport et de stockage des données personnelles de l'utilisateur.

Principe de fonctionnement

La technologie GIGA-PASS associe une clé USB mémoire à un émulateur. Celui-ci permet à toutes les applications de sécurité de voir la clé comme une carte à puce. Les données "carte" sont stockées dans la clé sous la forme d'une partition cachée. Elles ne peuvent être détruites ou modifiées directement par l'utilisateur. Ces données sont protégées par un chiffrement AES assurant la confidentialité des données en cas d'attaque extérieure.

L'accès par les applications au contenu de la partition chiffrée est conditionné à la validation d'un code PIN par l'utilisateur. L'itération de trois saisies erronées bloque la clé. Elle devient inutilisable sans le support d'un administrateur habilité.

Le Token GIGA-PASS offre toutes les fonctionnalités d'une carte à puce d'authentification, tout en conservant celles d'une clé USB mémoire. Plus de 99 % de la capacité mémoire reste disponible pour le stockage de données. Selon le type de clé retenue, les données personnelles des utilisateurs peuvent être automatiquement chiffrées sur le support (domaine de la santé ou de la finance...).

Un coût défiant toute concurrence

La production en volume de clés USB de stockage est le gage pour le client d'un prix d'achat optimisé. Le Token GIGA-PASS est commercialisé sous la forme d'une clé USB 1 ou 2 Go de mémoire.

Pour des clients disposant d'un parc existant de clé USB la technologie GIGA-PASS peut être acquise sous licence.

Une solution plébiscitée par les utilisateurs

La fourniture d'une clé USB mémoire est perçue comme un acte positif par l'utilisateur. De plus, la clé peut être personnalisée aux couleurs de l'entreprise. L'association de données personnelles à la fonction d'authentification renforce l'appropriation de l'outil de sécurité et minimise les situations de perte ou d'oubli du Token.

L'exploitation de clés USB de stockage est devenue un acte familier. Associer un service supplémentaire à ces clés simplifie significativement les procédures de conduite du changement. L'authentification forte devient un acte naturel ...



Points clés et bénéfices

Un seul support pour 2 usages : clé USB mémoire standard (de 64Mo à plusieurs Go) et token de sécurité offrant les mêmes fonctions d'authentification, chiffrement et signature qu'une carte à puce.

Token de sécurité le plus économique du marché : les prix des clés USB ne cessent de baisser (moins de 5 € pour 100 unités). Le logiciel Scrypto CMS permet de personnaliser toute clé USB mémoire en token USB GIGA-PASS.

Evolutivité : hébergement de certificats et de credentials SSO en grand nombre ; permet le déploiement progressif des applications sans remise en cause de l'existant.

Compatibilité : associé au logiciel client Scrypto, les tokens sont exploitables par tous les logiciels compatibles CryptoAPI ou PKCS#11.

Sécurité : protection par PINcode (blocage après présentation de 3 codes faux), utilisation de secrets propres à l'entreprise.

Personnalisation : marquage possible au logo de l'entreprise.



Support de haute sécurité

Les données « cartes » sont protégées par plusieurs niveaux de chiffrement. Le premier niveau de chiffrement interdit la copie des données sur une autre clé. Le second interdit l'utilisation des clés d'une entreprise dans une autre entreprise. Enfin, le code PIN est utilisé pour chiffrer une nouvelle fois les données sensibles (clé privée, identifiant et mot de passe SSO...)

Le logiciel client associé permet d'interdire si souhaité l'utilisation de toute autre clé USB sur le poste de travail. Le formatage de la clé par l'utilisateur n'a aucune incidence sur le contenu de la partition chiffrée hébergeant les données « carte », la partition n'est pas visible du gestionnaire de fichiers Microsoft.

Identification et traçabilité renforcée

La solution GIGA-PASS permet de remplacer l'identification par mot de passe par l'insertion du token et la saisie du code PIN. Elle peut être généralisée ou limitée aux accès ou utilisateurs spécifiques (VPN, Extranet, administrateurs, VIP...)

Seule la possession du Token permet d'initialiser une procédure d'authentification de la personne. Les failles de sécurités associées aux mots de passe inscrit sur des supports de type « post it[®] » sont éliminées...

L'utilisation par des collègues de l'identité d'un autre employé à son insu pour accomplir des tâches critiques devient impossible. L'authentification forte optimise la traçabilité des échanges numériques et facilite l'atteinte des objectifs fixés par les nouvelles réglementations en la matière. La traçabilité des transactions devient un acquis pour l'entreprise pour les utilisateurs fixes et mobiles.

Une solution souple à administrer

Espace mémoire « on demand »

L'évolution des usages de la sécurité est propice à une intégration progressive de nombreux certificats numériques ou de nombreux couples identifiant / mot de passe.

La procédure de personnalisation des Token GIGA-PASS permet de faire évoluer la taille de la partition consacrée au stockage de l'identité de l'utilisateur en fonction des besoins de la politique de sécurité de l'entreprise.

Gestion des stocks optimisée

La gestion des stocks est simplifiée, la clé USB contrairement à une carte à Puce ou token de sécurité dédié est un bien courant, disponible sans délais. La distribution des clés USB à une population significative d'utilisateurs n'est plus une contrainte. L'utilisation de plusieurs générations de clés, de tailles mémoire différentes, issus de constructeurs variés n'a aucun impact sur le déploiement et le support de la solution.

Gestion des Exceptions simplifiée

Le remplacement d'un token de sécurité oublié ou perdu pose de sérieux problèmes de délais et de coût lorsqu'il est basé sur un média propriétaire.

Avec la technologie GIGA-PASS, une clé temporaire peut-être créée à distance, en liaison avec le service habilité. En cas de perte, la banalisation du support permet de mettre en œuvre la procédure de remplacement dans les meilleurs délais.

Interopérabilité

Les Tokens USB GIGA-PASS sont compatibles avec toutes les solutions de sécurité Conforme au standard MS Capi et PKCS#11.

Ex: Authentification forte, chiffrement de fichiers et de disque dur, email chiffrés et signature électronique, Single Sign On.

Les Tokens GIGA-PASS permettent en particulier de sécuriser les **accès distants** :

- Ouverture de session VPN/SSL ou IPSec
- Authentification SSL sur accès Web

Le token GIGA-PASS est compatible avec tous les logiciels de la gamme CYBER-PASS de SCRYPTO :

CYBER-PASS CMS :

Le logiciel CYBER.PASS CMS, outil de card management offre toutes les fonctions de personnalisation et de gestion du cycle de vie des token GIGA-PASS et des credentials qu'ils abritent :

(Code PIN, clés et certificats d'authentification ou de chiffrement, ou mots de passe d'accès aux applications).

CYBER-PASS DynamiD :

DynamiD remplace le mot de passe demandé à l'ouverture de session Windows par une authentification par carte à puce ou token. Le logiciel s'appuie sur la technologie Microsoft du « Smart Card Logon » :

- Verrouillage de session par retrait du token
- Déblocage à distance des tokens par code ou défi/réponse
- Gestion du mode multi domaines
- Compatible client léger CITRIX, MS Terminal Serveur

A PROPOS DE SCRYPTO

Société française créée en 1989.

SCRYPTO conçoit et commercialise des solutions à bas de carte à puce ou de token USB permettant à tout type d'organisation de déployer, gérer et mettre en œuvre des supports d'authentification pour sécuriser les accès aux Systèmes d'information, sécuriser les communications, protéger les documents confidentiels ou authentifier les transactions électroniques.