CRYHOD

FOR DISKS AND LAPTOPS

CHIFFREMENT DES ORDINATEURS ET DES DISQUES
CONTRE LE VOL OU LA PERTE

CRYHOD, solution Certifiée de Full Disk Encryption (FDE), permet le chiffrement intégral des dispositifs de stockages physiques et virtuels pour protéger la mobilité, le télétravail et sécuriser le recyclage.

Les risques

Pour une entreprise, le préjudice lié au vol ou à la perte d'un ordinateur va bien au-delà de la valeur du matériel. La récupération, puis la divulgation ou l'utilisation des informations présentes sur le disque de l'équipement peuvent entraîner notamment une perte d'image, des dégâts industriels et financiers ou des infractions à des réglementations (RGPD, Diffusion Restreinte).

Pour prévenir ces risques, accentués avec le développement du travail hors les murs, il est impératif de ne pas laisser reposer la sécurité des postes sur le 'login' classique et de garantir que seuls les utilisateurs dûment authentifiés et autorisés aient accès à leur contenu et ce dès le branchement ou le démarrage du matériel.

C'est ce qu'apporte le Pre-Boot Authentication (PBA) associé au Full Disk Encryption (FDE) que propose **CRYHOD**, une solution Européenne Certifiée pour la protection des postes de travail, adoptée par tous les grands Ministères Français.

Sécurisation du télétravail et de la mobilité

CRYHOD permet à l'Entreprise de protéger les équipements des collaborateurs qui sortent des locaux suivant une stratégie globale et administrée. Ces outils peuvent être un ordinateur portable, des clés USB, des disques externes, des machines virtuelles locales ou dans le Cloud.

Protection intégrale des terminaux et des disques

CRYHOD peut chiffrer une ou toutes les partitions des ordinateurs et des dispositifs externes, il apporte ainsi un chiffrement des données permanent, ce qui protège ces matériels contre la perte et le vol pendant tout leur cycle de vie y compris après leur mise au rebut.

Sécurité transparente pour l'utilisateur, peu contraignante

L'utilisateur fournit son 'secret' au démarrage de la machine et travaille ensuite comme d'habitude. L'ouverture de session peut ensuite être effectuée automatiquement (Single Sign On). Les secteurs des partitions sont chiffrés et déchiffrés à la volée et ainsi l'utilisateur n'a aucune interaction avec le produit. Lorsqu'il referme ou éteint son poste, son contenu reste chiffré et donc protégé.

Solution 'encrypt and forget'

Une fois déployé, **CRYHOD** se fait oublier. La politique de sécurité de l'Entreprise est garantie, les utilisateurs l'oublient, et tous les matériels sont protégés.

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu - Tél.: +33 (0)1 40 95 24 80
Siège social : 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Direction commerciale : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu

CHIFFREMENT

- **Chiffrement des partitions (système et données)**
- **Chiffrement à la volée, transparent pour l'utilisateur**
- **Chiffrement initial en arrière-plan; reprise sur coupure; mode rapide (ne traitant que les secteurs utilisés) ou complet (pour l'ensemble des secteurs)**
- **Hibernation sécurisée**

AUTHENTIFICATION

- **Authentification pré-boot** *(avant démarrage ou au branchement)*
- **Authentification par mot de passe, carte à puce ou token**
- **Ouverture de session manuelle ou automatique** *(Single Sign On)*
- **Poste de travail mono-utilisateur ou multi-accès** *(poste partagé/en libre-service)*

ADMINISTRATION - IT

- **Déploiement via les infrastructures IT courantes** *(SCCM, AD, ...)*
- **Gestion IT minimale 'Encrypt and Forget'**
- **Tous types de disques et d'ordinateurs** *(BIOS ou UEFI)*

ADMINISTRATION - SÉCURITÉ

- **Politiques de Sécurité définies par le responsable de la sécurité**
- **Mécanisme de recouvrement des données configurable**
- **Secours utilisateurs** *(perte de clé ou de mot de passe)*

CARACTÉRISTIQUES TECHNIQUES

+ **Windows** 11+
+ Firmware BIOS ou UEFI
+ Chiffrement **AES 256**
+ Accès par **certificats/clés RSA** *(jusqu'à 4096 bits)* **et/ou mots de passe** *(de force configurable)*
+ Compatible avec les principaux **badges à crypto-processeurs** **PKCS#11** *(format carte ou USB)*
+ Compatible avec la plupart des **PKI** *(IGC)* du marché

CERTIFICATIONS

Certification critères communs EAL3+

Visa de sécurité et qualification ANSSI

Protection des données marquées : diffusion restreinte OTAN et UE

2025.07

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu - Tél.: +33 (0)1 40 95 24 80
Siège social : 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Direction commerciale : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu