USE CASE

CRYHOD ZONECENTRAL



ADMINISTRATION

SÉCURISER L'ENSEMBLE DES TERMINAUX D'UN MINISTÈRE

Cas du Ministère de l'Intérieur français*

« Le Ministère de l'Intérieur assure au quotidien la sécurité des Français face aux divers risques. Les moyens des services doivent constamment s'adapter aux menaces qui évoluent très rapidement, aux nouvelles formes de criminalité et de terrorisme, mais également aux évolutions technologiques. »

EXIGENCES

Le Ministère mène un ambitieux projet de sécurisation de son système d'information sur 3 ans, avec un objectif : **la protection de ses données bureautiques jusqu'au niveau Diffusion Restreinte.** « Pour les systèmes d'information et de communication, les projets portés [...] s'articulent autour de plusieurs priorités [...] **dont le renforcement et la sécurisation des infrastructures informatiques via le chiffrement des réseaux et des postes de travail.** »

Est prévu en première vague, le chiffrement de l'ensemble des postes de travail équipés d'un système d'exploitation Windows (plus de 110 000 ordinateurs). En second temps, les postes de travail équipés d'un système d'exploitation Linux seront à leur tour chiffrés.

SOLUTION

À cet effet, l'Agence Nationale de la Sécurité des Systèmes d'Information en France (ANSSI) a acquis pour le compte du Ministère de l'Intérieur les **solutions CRYHOD et ZONECENTRAL, déployées sur l'ensemble de son parc informatique :**

+ CRYHOD pour garantir la confidentialité des informations **en cas de vol de données ou de tentative d'espionnage ;**

+ ZONECENTRAL pour protéger les informations stockées dans les dossiers locaux, sur des espaces partagés, ainsi que celles qui sont envoyées vers l'extérieur ;

+ ZED! et **ZEDMAIL**, pour sécuriser les données vers des destinataires externes (e-mails, clés USB, disques externes, partages en ligne, etc.).

La définition des politiques de sécurité permet de s'assurer que **le chiffrement des données soit automatique et incontournable.**

EXPÉRIENCE

Côté utilisateur, le code PIN de la carte à puce est à renseigner au démarrage du poste de travail, permettant à l'utilisateur de déchiffrer son disque, d'accéder à sa session et de consommer les données chiffrées par **ZONECENTRAL.**

AVANTAGES

CRYHOD, ZONECENTRAL et ZED! sont Certifiés CC EAL3+, Qualifiés au niveau Standard par l'ANSSI et permettent donc de protéger des informations marquées NATO Restricted / EU Restricted.

Lors d'un accès sur un serveur via le réseau, les données transitent chiffrées. Le chiffrement/déchiffrement des fichiers se fait directement sur le poste de travail de l'utilisateur.

Enfin, CRYHOD et ZONECENTRAL réservent l'accès à l'information aux utilisateurs autorisés et identifiés via leur carte agent (badge à microprocesseur du Ministère).

2023.06

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