Trustway Proteccio netHSM

Le HSM qualifié, la racine de votre sécurité

Trustway Proteccio est un module matériel de sécurité (Hardware Security Module – HSM) mettant à disposition des solutions logicielles dans un environnement performant et hautement sécurisé pour la réalisation de leurs opérations cryptographiques les plus sensibles.

La combinaison de ses dispositifs de sécurité physique et d'un cœur cryptographique soumis aux exigences de sécurité les plus strictes apporte aux systèmes d'information d'entreprise et aux services du cloud l'un des modules cryptographiques les plus certifiés au monde.

Sa mise en œuvre simplifiée, pensée pour un déploiement autonome, propose aux environnements critiques une réponse optimale et à moindre coût pour une sécurité inconditionnelle de leurs données sensibles.

Cryptographie certifiée

Trustway Proteccio prend en charge l'ensemble des opérations cryptographiques sensibles des applications de sécurité (PKI, signature, eID, chiffrement, etc.)

Son architecture 100% européenne apporte les implémentations cryptographiques les plus sûres, issues de plus de 20 ans de Recherche et Développement en France et soumis aux certifications internationales les plus exigeantes.

Déjà déployé dans les environnements les plus critiques (OIV, défense, énergie, télécommunications), Trustway Proteccio apporte aux organismes nationaux et aux entreprises la fiabilité d'une architecture de pointe et la robustesse d'un produit conçu au plus près des exigences de sécurité les plus strictes au monde.

Optimisation des ressources

Le partitionnement fort proposé par Trustway Proteccio permet l'utilisation d'un même équipement par plusieurs applications distinctes en toute sécurité.

Un même HSM peut ainsi être utilisé par différentes applications de sécurité indépendamment les unes des autres, en apportant le même niveau de sécurité et de conformité que l'exploitation.

Haute disponibilité et optimisation des performances

La mutualisation des HSM Trustway Proteccio en clusters réseau permet la constitution de pools cryptographiques sécurisés bénéficiant d'une répartition de charge native et d'une réplication automatique des clés.

Chaque pool est accessible de façon transparente par les applications logicielles, sans aucune modification de leur code source.

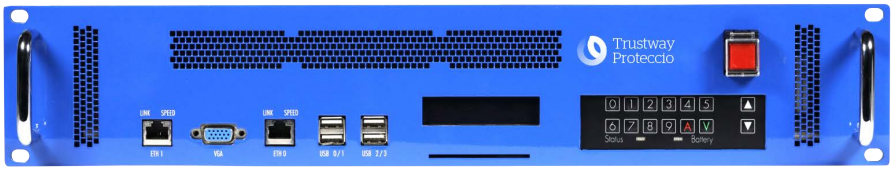
La conjugaison du partitionnement fort et du clustering natif donne aux architectes et aux administrateurs une marge de manœuvre inédite, permettant un dimensionnement sur mesure et une réponse optimale aux cahiers des charges d'infrastructure et de performances.

Simplicité d'installation et d'administration

Les HSM Trustway Proteccio prennent en charge l'ensemble des modalités techniques et sécuritaires inhérentes au déploiement et à l'utilisation de la cryptographie matérielle.

Ils font l'objet de procédures d'administration simplifiées, réduisant de façon significative les risques liés au déploiement de la cryptographie et à son exploitation à très long terme par des équipes hétérogènes.

Les HSM Trustway Proteccio, leurs partitions et les politiques de sécurité dont ils font l'objet sont administrés de façon centralisée par une application unique, conçue pour garantir une indépendance technique et une simplicité d'utilisation uniques sur le marché.



Trusted partner for your **Digital Journey**

Le HSM Trustway Proteccio en un coup d'oeil

Sécurité certifiée

Le HSM Trustway Proteccio est entièrement conçu, développé et fabriqué par Bull en France. Il satisfait les évaluations sécuritaires des processus de certification les plus exigeants.

La certification CC EAL4+, la qualification renforcée (ANSSI QR), l'agrément EU RESTRICTED et l'agrément NATO SECRET couvrent l'ensemble de l'architecture matérielle et logicielle.

HSM virtuel

Huit HSM virtuels peuvent être utilisés de façon simultanés dans un même HSM Trustway Proteccio.

Chaque HSM virtuel est une partition sécurisée indépendante (contrôle d'accès, utilisateurs, opérations cryptographiques, journaux, auditeurs et administration). Ce partitionnement fort permet la mutualisation d'un même HSM physique parmi différentes applications, tout en bénéficiant d'un niveau de sécurité identique au déploiement de plusieurs équipements.

Haute disponibilité, failover, backup

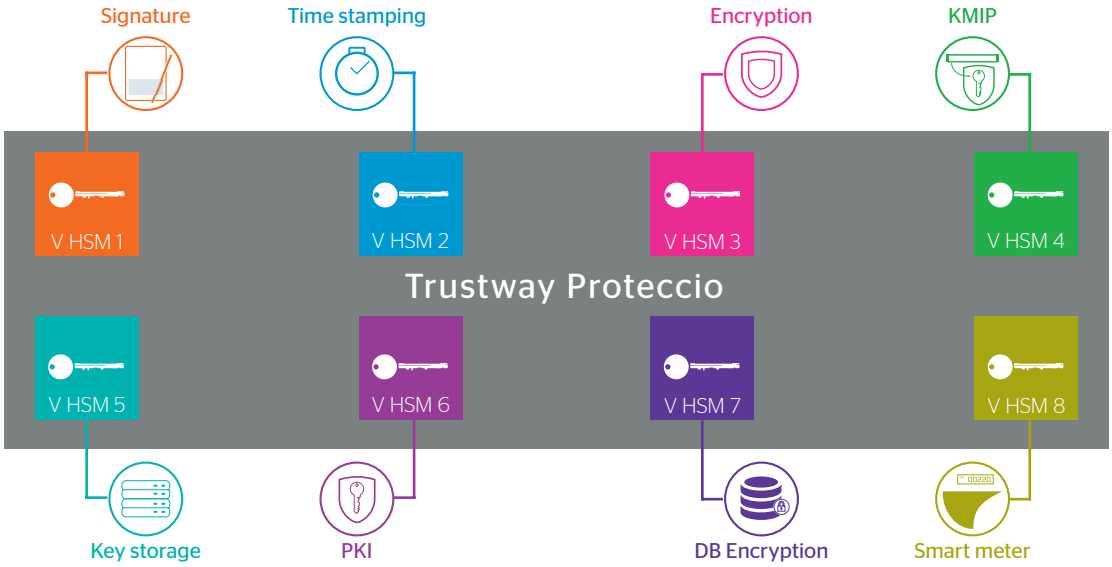
Associés au sein de clusters, les HSM Trustway Proteccio bénéficient de mécanismes de Haute Disponibilité et de failover natifs, incluant une réplication automatique et sécurisée des clés sur l'ensemble des membres du cluster.

Les fonctionnalités de backup et de restauration permettent par ailleurs la mise en œuvre simplifiée de plans de reprise d'activité.

Administration

Trustway Proteccio est entièrement administré depuis une application graphique simple et ergonomique.

La centralisation des opérations de déploiement, d'administration et d'audit au sein d'une application reconnue pour sa simplicité, permet une gestion fiable, sécurisée et à très long terme sans compétence technique spécifique.



Caractéristiques

Certifications

- EU RESTRICTED
- Critères communs EAL4+ conformes au CWA 14167-2-PP
- NATO SECRET
- Conforme eIDAS
- Qualification renforcée (ANSSI)
- FIPS 140-2 niveau 3 (en cours)

Algorithmes

- Chiffrement asymétrique : RSA
- Chiffrement symétrique : AES 128 à 256, 3DES
- Signature électronique : RSA PSS, PKCS v1.5, ECDSA
- Hachage : MD5, SHA-1, SHA 256, SHA 384, SHA 512
- Courbes nommées prises en charge : ANSI, NIST, ANSSI et toutes les courbes jusqu'à 521 bits, courbes Brainpool comprises

Administration

- Définition de profils cryptographiques
- Mises à jour sécurisées des logiciels intégrés
- Répartition de charge

API

- PKCS#11
- OpenSSL
- Java Cryptography Architecture/Extension (JCA/JCE)
- Microsoft Crypto API (CSP), Cryptography Next Generation (CNG)

Interfaces

- 2 ports Ethernet 10/100/1000BASE-T
- 4 ports USB2
- 1 port VGA
- Clavier et lecteur de carte à puce intégrés
- Alimentation électrique redondante
- Bouton de réinitialisation en façade
- Lien RPC sécurité par SSL vers serveurs Windows, Linux et AIX 32/64

Performances

- Asymétrique : jusqu'à 1 600 sign/s
- Symétrique : jusqu'à 200 Mbits chiffrés par seconde

Veuillez trouver plus d'information sur
atos.net/fr/produits/cybersecurite/chiffrement-donnees/hsm-trustway-proteccio-nethsm

CT_180917_LPM_Fs-Trustway_Proteccio_netHSM_fr4