Trustway Key Management Centre

Gestion de clé pour les banques et grandes organisations

Dans toutes les industries les exigences de gestion des clés cryptographiques sont de plus en plus complexes. S'assurer que chaque clé est au bon endroit au bon moment pour le bon usage est une contrainte pour de nombreuses organisations, telles que les banques émettrices de cartes, les infrastructures de transport ou les émetteurs de cartes d'identité ou de passeports. La prolifération des applications et des modules de sécurité nécessite la création d'outils centralisés et l'harmonisation des procédures de gestion des clés. La solution KMC d'Atos a été conçue pour gérer les clés pour les banques et les grandes organisations.

Cérémonies de clés

Le KMC permet de réaliser des Cérémonies de Clés dans un environnement sécurisé, indépendant des systèmes de production. L'interface graphique du KMC facilite la conduite des cérémonies de clés. La gestion de clés centralisée sur le KMC assure le plus haut niveau de sécurité, limite les coûts associés et élimine le besoin de gestion des clés sur les serveurs de production. L'utilisation de cartes à puce offre plus de sécurité et de commodité pour la sauvegarde et le transfert sécurisé des clés cryptographiques.

Une approche intégrée

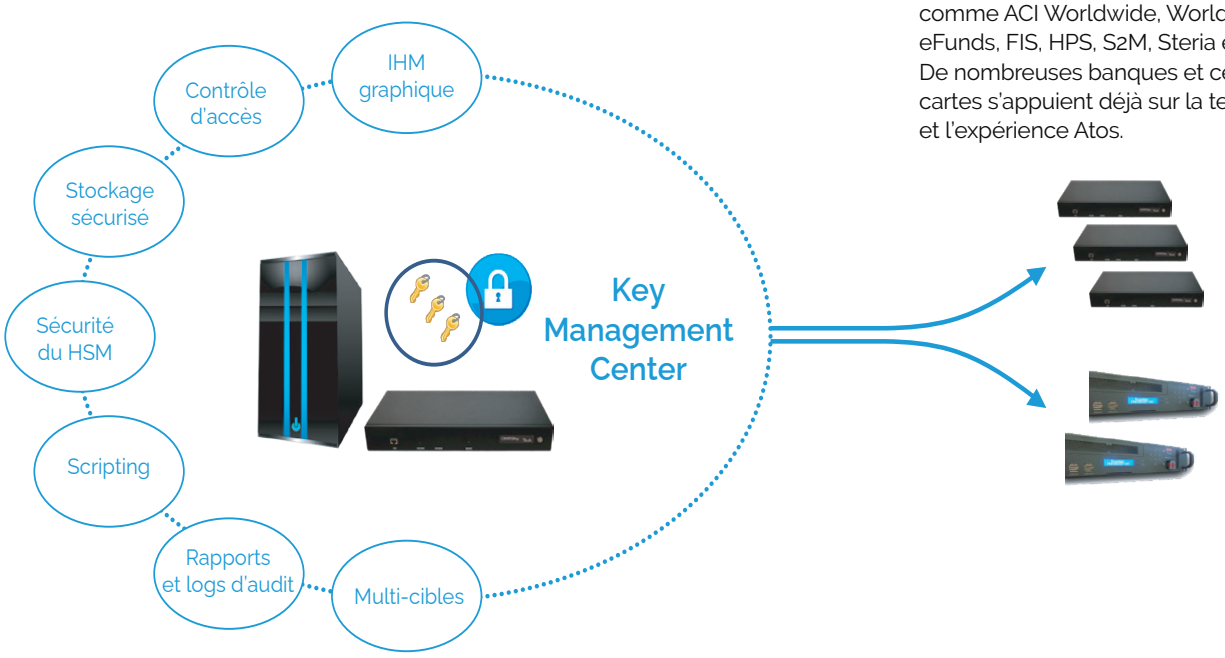
Le KMC s'appuie sur le HSM crypt2pay™ pour une protection permanente des clés. Un PIN PAD est connecté directement au HSM pour la saisie des PIN et des composantes de clés, offrant un chemin de confiance pour l'introduction des secrets. La solution KMC offre plusieurs formats pour les échanges de clés avec des partenaires et permet la distribution des clés vers des HSM cibles d'Atos (crypt2pay) et d'autres fournisseurs.

Leader européen de la sécurité intégrée

Atos a développé une expertise unique de la sécurité des systèmes d'information, conjuguant un savoir-faire de conseil et d'intégrateur avec la maîtrise des technologies de souveraineté.

Avec plus de 30 ans de présence dans la sécurité, Atos a acquis une grande expérience professionnelle des réseaux bancaires.

Grâce à un réseau de partenaires reconnus, Atos prend une part active à la mise en oeuvre de systèmes de paiement s complet s avec des éditeurs de renom comme ACI Worldwide, Worldline, eFunds, FIS, HPS, S2M, Steria et d'autres. De nombreuses banques et centres cartes s'appuient déjà sur la technologie et l'expérience Atos.



Les fonctionnalités du KMC

Stockage sécurisé

Le KMC permet la création et le stockage sécurisé de clés secrètes, de clés privées et de clés publiques certifiées. Les attributs des clés sont définis par l'interface graphique et enregistrés dans la base de données, cloisonnée en différentes hiérarchies de clés.

Contrôle d'accès

La connexion de l'application KMC au HSM crypt2pay est sécurisée par SSL, avec authentification de l'opérateur par carte à puce.

Autorité de certification

Le KMC est une solution complète qui intègre une autorité de certification (AC) avec des fonctions pour la signature des certificats SSL.

Partage de Secrets

Les clés racines doivent être recouvrées à partir de composantes introduites par les dépositaires de secrets pour déverrouiller l'accès aux clés. L'utilisation de cartes à puce offre plus de commodité et de sécurité.

Chemin de confiance

L'introduction des secrets dans la mémoire sécurisée du HSM est effectuée grâce à un PIN PAD avec connexion directe et sécurisée au HSM. Une imprimante peut être connectée au port série du HSM pour imprimer les composantes de clés à des fins de sauvegarde.

Import / Export de clés

Les clés secrètes peuvent être importées ou exportées sur le PAD PIN (composantes de clés) ou sous forme chiffrée dans des fichiers XML. Plusieurs mécanismes de chiffrement sont pris en charge pour l'export des clés secrètes ou privées utilisant la cryptographie symétrique ou asymétrique.

Une fonction de scripting

Une fonction de scripting permet d'automatiser la génération de clés et de demander des certificats d'émetteur EMV pour améliorer la productivité des cérémonies des clés.

Magasins de clés cibles

Des règles de distribution sont définies pour les HSM ou des groupes de HSM cibles. A chaque cible est affectée une liste de clés parmi toutes celles stockées dans la base.

Les magasins de clés, protégés en confidentialité et en intégrité, sont produits pour chaque cible. Ainsi chaque HSM cible reçoit toutes les clés dont il a besoin pour sa production, et seulement ces clés. Plusieurs formats de magasins de clés sont supportés selon le fournisseur du HSM et de l'application cible.

Rapport et journaux d'audit

Chaque opération est enregistrée dans un fichier journal protégé en intégrité. Des rapports personnalisés des Cérémonies de clés peuvent être produits pour assurer la traçabilité des opérations de gestion des clés.

Méta-données

Des méta-données peuvent être définies et associées aux clés pour adapter la gestion des clés au contexte de l'établissement.

Sécurité classes de clés principales fonctions

- HSM crypt2pay
- Certifications : MEPS, FIPS 140-2 niveau 3+, PCI HSM et qualification ANSSI
- Chemin de confiance pour l'introduction des clés (XOR, SHAMIR)
- Authentification forte des opérateurs

Classes de clés

- DES : DES, 2DES, 3DES
- Mifare : DES Fire
- RSA : Jusqu'à 4096 bits
- Clés publiques certifiées
- HMAC : 20 à 64 bit
- AES : 128, 192 et 256 bits
- ECDSA : ANSI X9.62-2005
- Secrets Génériques

Principales fonctions

- Génération de clés
- Génération de demandes de certificats EMV (MASTERCARD & VISA)
- Import/export de clés
- Sauvegarde et restauration de clés
- Distribution de clés à des HSMs cibles (crypt2pay, SafeNET KMU, ATALLA, IBM, TR31)
- Gestion des droits des applications clientes

Mécanismes d'import/ export types de clés

- DES & AES en mode ECB CBC et CBC PAD
- RSA PKCS et OAEP
- Blocs de clés TR31 (versions A à D)

Types de clés

- Clés du domaine du paiement
- Clés du domaine des compteurs intelligents
- Clés PKCS#11
- Clés Secrets Génériques

Environnement technique

- Java Runtime Environment 1.8

For more information: atos.net/en/solutions/cyber-security-products/data-protection-governance/hsm-trustway-crypt2pay

CT-221123-AR-BC-Trustway-KMC for banks and large organisations-Fr-V2