Trustway Key Management Centre

KMC for banks and large organisations

In all industries the requirements of cryptographic key management are becoming increasingly complex. Ensure that each key is in the right place at the right time for the right use is a constraint for many organizations, such as card issuing banks, transport infrastructure or identity cards or passports issuers. The proliferation of applications and HSMs requires the establishment of centralized tools for key management and harmonization of procedures for key management. Atos KMC solution has been designed to manage keys for banks and large organizations.

Perform Key ceremonies

KMC offers key management functions to perform Key Ceremonies in a secure environment, independent from production systems. The GUI of KMC application facilitates the conduct of key ceremonies. The centralized key management on the KMC ensures the highest level of security, limits related costs and eliminates the need for key management on production servers. The use of smart cards offers greater security and convenience for secure backup, recovery and transfer of cryptographic keys.

Atos KMC solution, an integrated approach

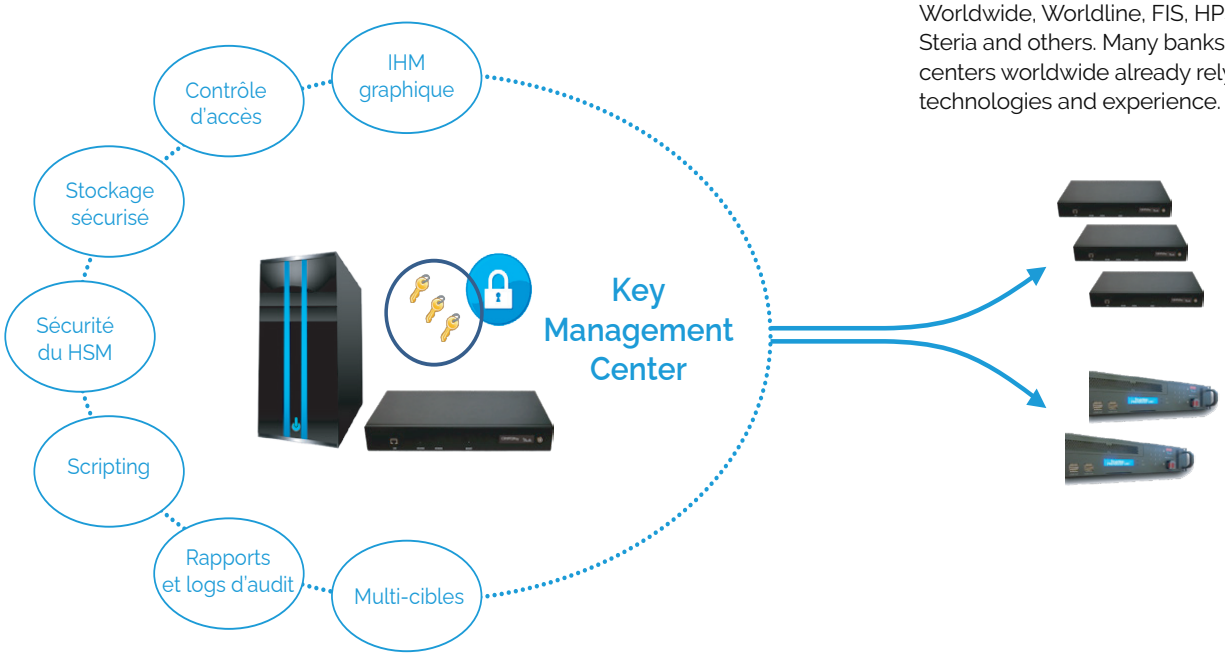
Atos KMC solution offers several import/ export formats to exchange keys with partners and includes key distribution to target HSM from Atos (crypt2payTM) and other vendors. KMC relies on crypt2pay HSM to ensure a permanent protection of keys. The key introduction device is connected directly to the HSM of the KMC for entering PINs and key components, in order to provide a trusted path for the introduction of secrets.

A European leader in integrated security

Atos has built up a unique body of expertise in information systems security, bringing together consulting and systems integration expertise and an in-depth understanding of corporate security technologies.

With more than 30 years in financial security, Atos has gained considerable professional experience in securing banking networks.

Thanks to a network of recognized partners, Atos takes an active part in implementing comprehensive payment systems with renowned software publishers such as ACI Worldwide, Worldline, FIS, HPS, S2M, Steria and others. Many banks and card centers worldwide already rely on our technologies and experience.



KMC feature

Secure storage

The core function is to create and store securely secret keys, private keys are certified public keys. Identifiers and other key attributes are defined through the GUI and saved in the database with encrypted key values. Key partitioning is achieved through the definition of key hierarchies.

Access Control

The connection of KMC application to crypt2pay HSM is secured by TLS. The KMC operator is authenticated by crypt2pay HSM through the presentation of a user certificate on a smart card.

Certification Authority

KMC integrates Certification Authority (CA) functions for signing the SSL certificates. This integrated CA can be used to avoid the need of an external PKI solution.

Secret Share

Root keys shall be recovered from key shares introduced by key custodians to unlock access to the lower level keys in the hierarchy. Key shares can be stored on smart cards for convenience and security.

Trusted path

Introduction of key share values inside the HSM's secured memory can only be performed through a PIN PAD with direct and secured connection to the HSM. A printer can be connected to the HSM's serial port to print key shares for backup purposes.

Key Import/Export

Secret keys can be imported or exported through the PIN PAD (key shares) or in encrypted form in XML files. Several encryption mechanisms are supported to import or export secret or private keys using symmetric or asymmetric cryptography.

Scripting feature

Scripting feature can be used to automate key generation and EMV Issuer Certificate Request generation. As a result, productivity of key ceremonies is improved.

Meta data

Meta data may be defined and associated with keys to customize the key management to the target environment.

Target key stores

Key distribution scheme is defined through the HSM management function. Each target is assigned a list of keys among all keys stored in the database in order to ensure that each target has all the keys it needs for its production, and only the keys it needs. Distribution rules can be defined for single HSMs or groups of HSMs.

Key stores are produced for each target with integrity and confidentiality protections. Several key stores format are supported depending on the target HSM vendor and target application.

Report & Audit logs

Each operation is recorded in an audit log file protected in integrity. Customized Key Ceremony reports can be issued to ensure traceability of key management operations.

Why use

- Crypt2pay HSM
- Tamper resistant design: MEPS approved, FIPS 140-2 level 3+, PCI HSM and ANSSI (National Agency for the security of information systems) qualification
- Trusted path for key shares input/output (XOR, SHAMIR)
- User strong authentication

Key classes

- DES: DES, 2DES, 3DES
- Mifare: DES Fire
- RSA: Keys up to 4096 bits
- Certified public keys
- HMAC: 20 to 64 bits
- AES: 128, 192 and 256 bits
- ECDSA: ANSI X9.62-2005, recommended domain parameters
- Generic secret keys

Main feature

- Key generation
- EMV certificate request generation (MASTERCARD & VISA)
- Key import/export
- Key backup & recovery
- Key distribution to target HSMs (crypt2pay, SafeNET KMU, ATALLA, IBM, TR31)
- Management of rights on client applications

Import/export mechanisms

- DES & AES in ECB, CBC and CBC_PAD modes
- RSA PKCS and OAEP
- TR31 key blocks (version A to D)

Key types

- Payment Industry keys
- Smart metering Industry keys
- PKCS#11 keys
- Generic secret keys

Technical environment

- Java Runtime Environment 1.8

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