CRYPTOMATHIC

Solution Brief

CKMS z/OS Integration

Key Management for IBM z/OS Mainframe Applications

Mainframe key management

Large Banks and Financial Institutions typically run critical applications on the IBM's z/OS ('mainframe') platform. While there is extensive support for cryptography, the platform lacks a modern, independent and comprehensive solution for the management of key material. Importing keys to the z/OS platform is typically a manual process; sharing keys with other platforms can be complex and time consuming.

Modern banking requires agility of business processes, and this extends to cryptography; siloed key-stores and proprietary protocols are being replaced with flexible and standards-based systems that can grow and flex to the demands of the business. Mainframe systems are subject to the same calls for openness, transparency and efficiency.

Client benefits

- ✓ **Securely share keys between mainframe, on-premise and cloud applications**
- ✓ **Centrally manages the life-cycle of cryptographic keys at large scale**
- ✓ **Automates key management activities and on-line key distribution**
- ✓ **Reduces the risk of key compromise and human errors**
- ✓ **Provides tamper-evident audit and usage logs for compliance**
- ✓ **Based on industry-standard APIs and key-formats**

Automate the key life-cycle and distribution with CKMS

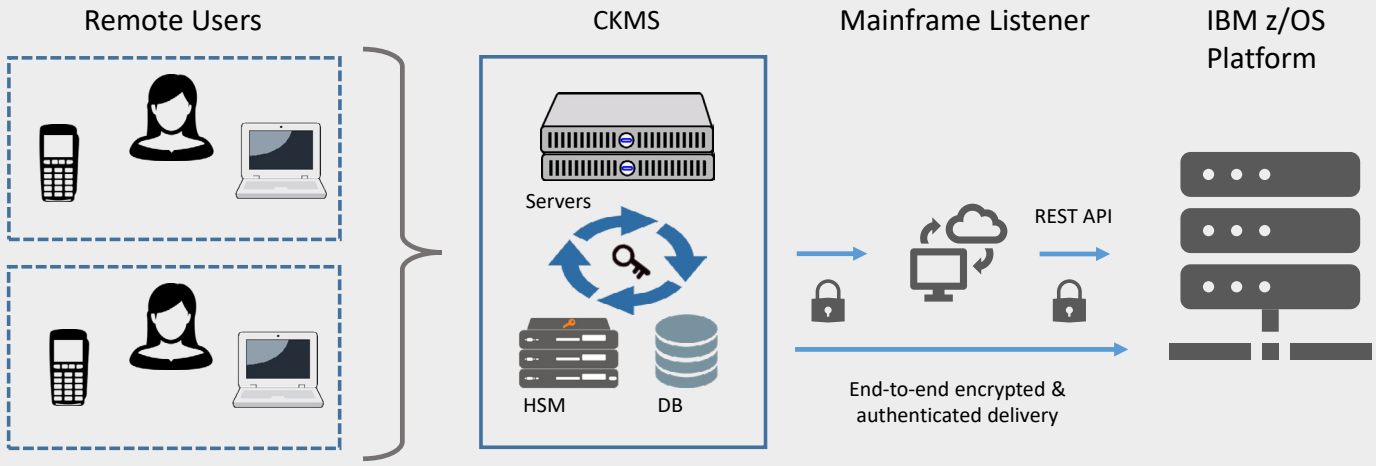
Cryptomathic's CKMS offers centralized and automated key management, with comprehensive support of financial cryptography primitives. CKMS orchestrates the delivery of keys to a wide range of applications, ensuring the appropriate keys are available at the right time and place.

The z/OS integration extends the benefits of CKMS to a new class of applications: for the first time an independent and well-trusted KMS can programmatically deliver keys to applications running on a mainframe, without altering the application. Using IBM's standard REST API, CKMS securely updates keys in a data-set, using an industry-standard (IBM CCA) key-format.

CKMS allows for key material to be easily shared between mainframe, conventional servers and even cloud-based services. CKMS provides a central and canonical repository of critical high-value keys (e.g. Payment keys), highly available for applications throughout the bank or enterprise.

High level architecture

CKMS is built on a resilient client-server architecture. Administrators securely access the remote key management server via the easy-to-use CKMS client GUI - supported by secure PIN entry devices (PEDs) and ICCs for strong authentication. CKMS uses Hardware Security Modules (HSMs) to ensure high quality key material and strong protection of encrypted keys that are stored in a database. High availability is ensured through clustering of the server, database and HSMs. The PEDs also support remote key import/export and key share printing. Keys are distributed to applications and HSMs in a wide range of formats (key-blocks). Integration with the mainframe and other 3rd party systems is achieved with a 'Listener' that provides a consistent interface to CKMS while conforming to the protocol and cryptographic needs of the target system.



- ✓ Mainframe listener implemented as .NET Core service
- ✓ Channel from CKMS Server to Mainframe Listener is protected by TLS and CKMS Target Authentication Key
- ✓ Mainframe Listener protects credentials to operate Mainframe REST API
- ✓ Channel from Mainframe Listener to Mainframe is protected by TLS and REST API credentials
- ✓ Application keys are end-to-end encrypted from CKMS Server to Mainframe (under KEK)

Mainframe integration

- Supports DES, 3DES, AES, HMAC keys
- Keys are delivered in IBM CCA or TR-31 format
- Key are delivered encrypted & integrity-checked from end-to-end
- Supports sequential and partitioned data sets
- Requires z/OS REST API 2.4.0 enabled

CKMS features

- Key Block support includes: IBM CCA (v4.2 and v6), TR-31, TR-31 2018, Atalla Key Block
- HSM support: nCipher, Utimaco; Gemalto / SafeNet
- DB support: MS SQL, Oracle
- Supported key types include: AES, DES, 3DES, ECC, RSA, HMAC, X509 and EMV certificates

Learn more at cryptomathic.com/CKMS

About Cryptomathic

Contact us: enquiry@Cryptomathic.com

Cryptomathic is a global provider of secure server solutions to businesses across a wide range of industry sectors, including banking, government, technology manufacturing, cloud and mobile. With over 30 years' experience, we provide systems for Authentication & Signing, EMV, Mobile App Security and Crypto & Key Management through best-of-breed security solutions and services.

We pride ourselves on strong technical expertise and unique market knowledge, with two-thirds of employees working in R&D, including an international team of security experts and a number of world-renowned cryptographers. At the leading edge of security provision within its key markets, Cryptomathic closely supports its global customer base with many multinationals as longstanding clients.

v1.1