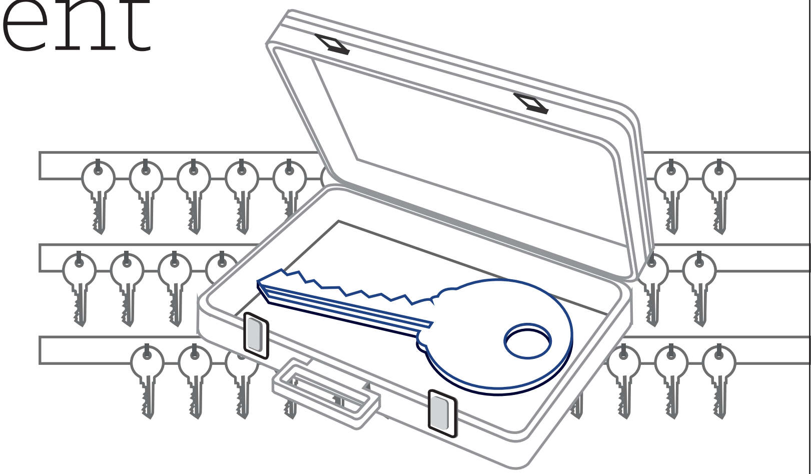
CRYPTOMAThIC SECURE METRIC TECHNOLOGY

SecureMetric Technology
Key Management Solution



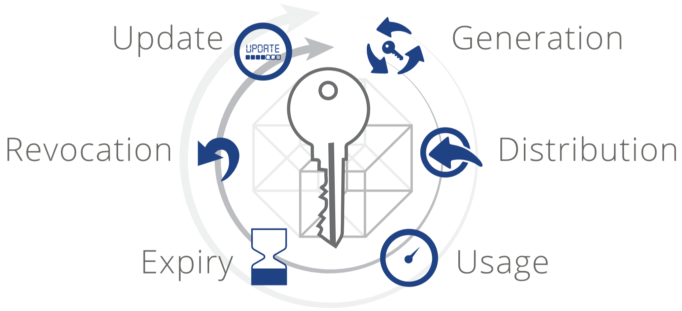
About Key Management

Across all industries the requirements for managing cryptographic keys are becoming ever-more complex. Ensuring that the right key is in the right place at the right time is mandated by many organisations, i.e. major card payment scheme providers. This is a complicated requirement as most businesses need to manage an ever-increasing number of keys, while reducing the risk of internal and external fraud, as well as keeping costs at a minimum.

The Key Management System (KMS) streamlines administration and reduces costs associated with traditional key management. Through its flexible and automated protocols, KMS gives users the flexibility to manage a very large number of keys - throughout their entire life cycle - without drowning in work. Using KMS, administrators can uniformly and centrally manage the life cycle of all cryptographic keys across a range of encryption platforms.

Basic Key Management?

End-to-end lifecycle key management includes generation, distribution, usage, expiry, revocation and update of keys. It is about having the right key, in the right place, at the right time.



TRADITIONALLY KEY MANAGEMENT DISADVANTAGES

Paper-based procedures

Extremely resource-intensive

Multi-party key ceremonies

3-4 staff members

Problems face by Organisations

No central surveillance of their Key

No central surveillance of their use

No central surveillance of their Location

When will they expire

Who is responsible

Increase in workload

Increase in cost

Why Key Management?

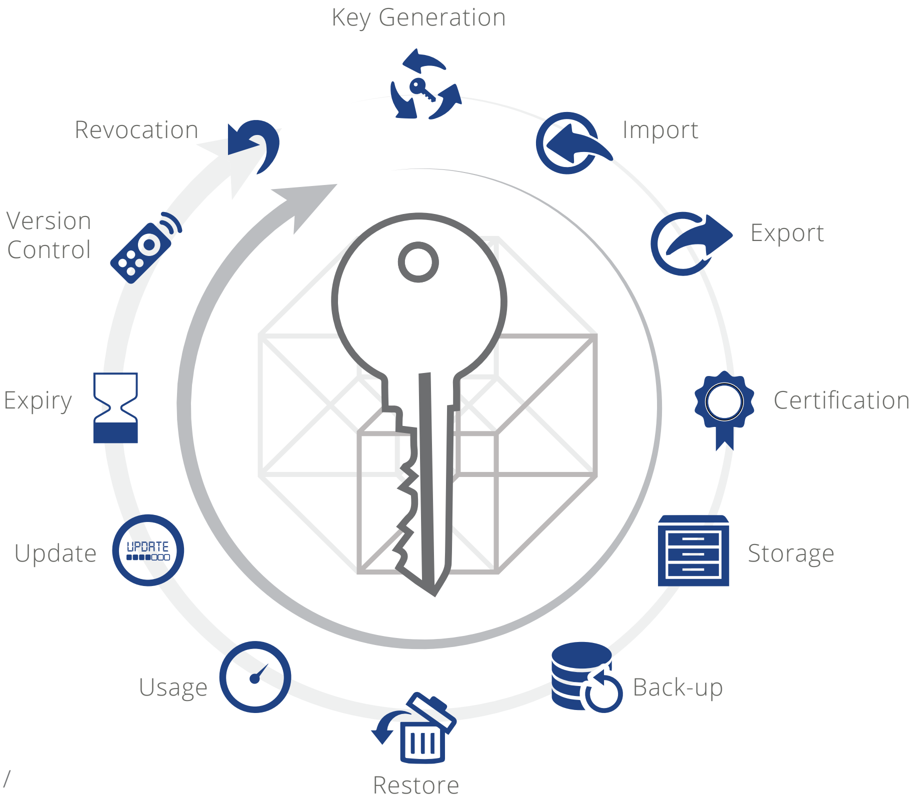
Technology trends point towards greater systems connectivity, larger data volumes and higher electronic transaction values. To secure these increasingly complex systems requires the management of ever larger numbers of cryptographic keys – from the tens towards the thousands, for medium to large organisations. Increasingly, such organisations, in particular in the financial sector, deploy secure key management systems dedicated to this task.

In addition to rising volumes of cryptographic keys, many financial institutions are facing an increasing regulatory burden imposed by creditand debit-card payment schemes and the Payment Card Industry (PCI) standards. Information security, and thus key management, is central to compliance.

Key Management System

Key Management Functions:

- Generation / back up / restore / update
- Distribution - automated or in key shares
- Import or export in key shares
- Enforce security controls
- Encryption using Key Encryption Keys (KEKs) / Zone Master Keys (ZMKs)
- Certification (e.g. using X.509 or EMV certificates)



KMS manages all aspects of cryptographic keys during their life cycle

The Key Management System (KMS) uses a client-server based architecture, with shared HSMs, to provide a centralised key management solution. The system is accessed by operators using desktop computers equipped with secure PIN pads for key component entry. An extremely flexible 'key-push' protocol allows the KMS server to securely connect with practically any secure host system that supports exchange of cryptographic keys.

Both symmetric keys and asymmetric key pairs (and their corresponding certificates) are easily managed using KMS. Each key is assigned its current state and specific set of attributes, including its history and general lifecycle management. KMS facilitates efficient operation through the ability to automate and optimise the working processes while adhering to the strictest set of security standards.

Needless to say, full compliance with all relevant industry and government regulations and best business practice is maintained throughout, with the added benefit of automated key management across multiple sub-systems and a central view of all cryptographic keys within the business as a whole.

Benefit Highlights

Consolidated Management
security officers can set up key projects to manage logical sets of keys as a single entity. It also allows for other security officers to review and execute the key projects, once complete.

Automated
securely push keys to any key distribution target as and when required.

Mobility
allows security officers and custodians to manage keys over a network. Operators no longer need to be monitored using physical room security mechanisms such as video surveillance, physical room access control and hard-copy-logging, due to the KMS desktop terminals which have hardware security mechanisms, smartcard access and local printing of key components

Reduced Dependency
asynchronous log-on allows for key custodians to add components securely as they are available, reducing the need for key ceremonies.

Centralised
securely manage keys across multiple parties/zones, i.e. banks, personalization bureaus, payment schemes, etc

Lifecycle Management
Automated and tamper-evident audit logs are maintained for all keys, allowing for complete accountability and the restoration of keys to a given state at any point in time.

Management Of Key Lifecycles

The concept of working with key projects is central to using KMS. It allows an organisation to enforce its procedures related to its various staff groups, e.g. key custodians, security officers and even security auditors if required, and lets each group perform their task – while
no other person or group is left idle.

Keys can be generated, installed, backed up, restored, disabled, reenabled, updated or – at the end of life - deleted. A central view allows for an easy overview of keys and their status. Additionally, interactive flags and reminders let the system operators know that action may be required in the near future e.g. related to key- or certificates updates. Keys and any information related thereto (version control, certificates, etc.) are managed in such a way that reports on all key-related events throughout the systems history may be viewed at a later stage if required.

Additionally, the dynamic definition and set-up of key types and targets in KMS allows for organisations to set up secure communication with practically any system.

Key Advantages

- **Streamline Processes**
- **Cost Saving – Eliminate Custodians**
- **Centrally Managed Upgrades**
- **Avoid Human Error**
- **Fewer HSMs**

TECHNICAL SPECIFICATION

System Architecture

- Client-server architecture
- Support of internal or network HSMs
- Simple integration and automated production through a dedicated API
- Flexible integration with existing cryptographic sub-systems

Keys

- Multiple algorithms (DES, 3DES, AES, RSA, ECC)
- Multiple key types (Master Key, Zone Key, Key Encryption Key, Certificates)
- Support for groups of keys (EMV key sets, etc.)

Security Architecture

- AES protected network communication
- Access control via smart cards
- Secure environment using HSMs
- HSM programming for key and certificate management
- Secure audit log of all events (in HSM)
- Secure PIN pad for secure key custodian work

Secret Sharing Schemes

- Key shares on PIN-pad
- Key shares on file
- XOR key shares
- Encrypted key to file

Standards & Evaluation Criteria

- ANSI: X9.17, X9.24, X9 TR-31
- ISO/IEC: 11568, 11770
- OASIS KMIP
- NIST: FIPS 140-2, SP800 57
- PCI DSS, PCI PIN

Syntax, Certificate Formats and Requests

- X.509v3, PKCS#7, PKCS#10
- EMV certificate for Visa, MasterCard, Amex, Interac
- DES, 3DES, AES, RSA (PKCS#1, PKCS#8), ECC, SHA-1

Operating Environment

- Microsoft Windows

Database

- Microsoft SQL Server
- Oracle

Hardware Security Modules

- IBM
- Thales / nCipher
- SafeNet
- Utimaco
- Other HSMs upon request

Appliance

- Customised KMS appliance available with multiple HSMs

Key Targets

- Authorisation system (e.g. ACI/Base 24 with Atalla Key Block)
- IBM Mainframe ICSF/CCA
- Data-preparation and card personalisation systems
- Database system
- Storage/Disk encryption system
- Application-level encryption
- Crypto-Service-Gateway
- Any other HSM or target upon request.

Protocols

- Web services for key Request and Key Push
- Support of synchronous and asynchronous targets

KUALA LUMPUR (HQ)
SecureMetric Technology Sdn. Bhd.
2-2, Incubator 2, Technology Park Malaysia,
Lebuhraya Sg Besi-Puchong, Bukit Jalil,
57000 Kuala Lumpur, Malaysia
T +603 8996 8225 F +603 8996 7225

SINGAPORE
(Sales Representative Office)
105, Cecil Street, #06-01, The Octagon,
Singapore 069534
T +65 6827 4451 F +65 6827 9601

JAKARTA
PT SecureMetric Technology
Komp. Ruko ITC Roxy Mas, Block C2, No. 42,
Jl. KH. Hasyim Ashari, 10150 Jakarta, Indonesia
T +62 21 6386 1282 F +62 21 6386 1283

MANILA
SecureMetric Technology, Inc.
Office 27, 7F BA Lepanto Building, 8747 Paseo de Roxas,
Makati CBD, Makati City 1226 Philippines
T +63 2 267 6797 +63 2 463 5634 M +63 9328 739046

HANOI
SecureMetric Technology Co., Ltd
203B, TDL Office Building, No. 22, Lang Ha Street,
Dong Da District, Hanoi, Vietnam
T +84 4 3776 5410 F +84 4 3776 5416

HO CHI MINH CITY
SecureMetric Technology Co., Ltd
L14-08B, 14th floor, Vincom Tower, 72 Le Thanh Ton,
Ben Thanh Ward, District 1, Ho Chi Minh City, Vietnam
T +84 8 6287 8544 F +84 8 6268 8188

YANGON
(Sales Representative Office)
3rd Floor, Building (8), Junction Square, Pyay Road,
Kamaryut Township, Yangon, Myanmar
T +951 2304155 F +951 2304155

sales@securemetric.com www.securemetric.com