CRYPTOMATHiC

CRYSTALKEY 360 PRODUCT SHEET

KEY MANAGEMENT AND DATA SECURITY PLATFORM

Cryptomathic not only secures your digital assets—with CrystalKey 360 we empower your team to centralize all cryptographic security decisions, delivering cost-effective compliance, business resilience and future readiness.

Whether you need a low-friction, secure way for your organization to adopt cryptography or you already have a large existing cryptographic project portfolio, we have a platform that will make your security and compliance simpler and more efficient to manage.

CRYSTALKEY 360 PRODUCT SHEET

WE CREATE VALUE ACROSS YOUR ORGANIZATION:

Security, risk and compliance
Effortlessly align with regulatory standards and pioneer adaptability to stay ahead of emerging threats. We ensure compliance and business continuity with business-wide adoption of cryptographic controls while future-proofing your operations in a cost effective manner.

Development
We empower your team to supercharge efficiency and streamline operations with best-in-class security tech, industry-leading support, cutting-edge tech expertise, seamless integration with legacy systems, and comprehensive training.

Tech Leadership
We provide a world-class security solution to manage cryptographic keys across your business. Our key management platform allows a seamless integration with your existing infrastructure, enabling you to harmonize every aspect of your cryptographic hardware operations. We offer rapid and flexible deployment models, on-premises, in the cloud or hybrid.

HOW OUR CUSTOMERS USE CRYSTALKEY 360

Optimization of HSM resources

- CrystalKey 360 enables your business to consolidate and streamline your HSM resources across your entire business and across different HSM brands offering HSM-as-a-Service.

Get your applications secured and to market faster

- CrystalKey 360 enables you to accelerate your application development by removing the need for special libraries and the overhead of hardware sourcing and integration.

Opening the cloud for regulated industries

- CrystalKey 360 enables the use of Enclave Security Modules (ESMs). ESMs are a cloud alternative to traditional HSMs. Operate HSMs for FIPS compliance mode and ESMs as confidential computing in the cloud for data privacy requirements and everything else.

Provide integrity to your software with remote code signing

- A flexible remote code signing setup with the ability to bring your own certificate authority and key storage.

CRYSTALKEY 360 PRODUCT SHEET

CRYPTOMATHiC

WHY USE CRYSTALKEY 360

A crypto agile platform for future-proofing your business
CrystalKey 360 provides the foundation for a future-proof security infrastructure by enabling true crypto-agility: the ability to change all cryptographic security decisions centrally. This makes it possible to update digest, signing, or encryption algorithms and even key types without requiring changes to the individual applications.

A streamlined user interface for ease of use
CrystalKey 360 makes it easier to adopt cryptography with a great user experience that enables you to quickly solve the simpler use cases and give you the full cockpit to master the advanced setups.

Hybrid deployment – Fully customizable deployments in the cloud and/or On-Premises

- Private / public / hybrid cloud
- Ability to keep key management on-premises, while enabling cryptographic services in the cloud

Data Sovereignty, Security and Privacy by design
Operate in the cloud, on-premises or hybrid infrastructure without sacrificing compliance with privacy laws (CCPA, GDPR, Privacy Act, etc.)

HSM-as-a-Service & Confidential Computing

- FIPS 140-2/3 Level 3 HSMs - vendor agnostic
- FIPS 140-3 Level 1 compliant Enclave Security Module for integration in the cloud

Compliance

- For compliance with FIPS 140-2, FIPS 140-3 and PCI-DSS 4.0 · Immutable logging
- Tamper evident audit and usage logs for all keys and cryptographic operations

Policy Enforcement

- Tailored to your needs
- Least privilege with RBAC
- Dual Control
- Multi-factor authentication
- Simplify internal and external compliance audits (e.g. PCI-DSS)
- Key usage policy

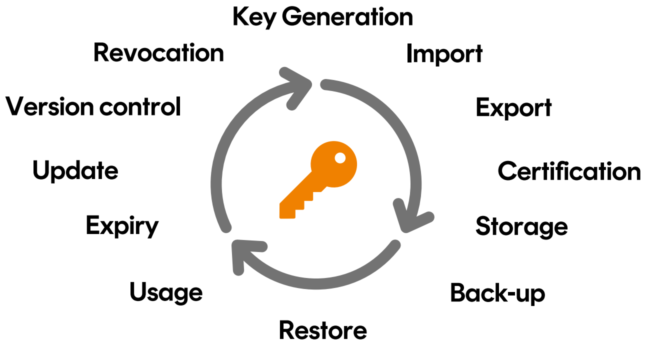
REST APIs

- OpenAPI 3.0 to automate workflows and integrations with homegrown and 3rd party systems, empowering businesses to effortlessly integrate key management into their organization

CRYSTALKEY 360 PRODUCT SHEET

CRYPTOMATHiC

FEATURES HIGHLIGHTS



Multi-Cloud Enterprise Key Management

- Centralize and automated key life-cycle management
- Ultimate control and visibility of your cryptographic keys on-premises or in the cloud
- Make keys available at the right time and place

Data Masking and Tokenization

- Protect sensitive data, ensure data privacy compliance, prevent data breaches, and maintain data usability, all while adhering to company policies and regional legislation

Code Signing

- Manage keys and certificates for code signing of drivers, software, etc.
- Support for quorum approval through Endorsed Signing to further protect your signing key

Crypto-Agility / Post-Quantum Cryptography

- Seamless switch to quantum-safe cryptography or other emerging requirements & standards

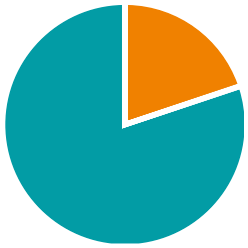
Confidential Computing

- Deploy Enclave Security Modules within secure enclaves to provide a trusted execution environment in the cloud, as an alternative to traditional HSMs

Data protection-as-a-Service

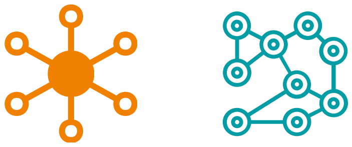
- Simplifies application integration for securing the digital assets of a business
- Implements key usage policy enforcement
- Reduces costs through shared infrastructure and increased HSM utilization

Time to market for a new project



80% quicker

Centralized trust center vs decentralized project siloes



1 silo vs. multiple

Cost of ownership per application

<1/5 of the cost

For more information visit our website

www.cryptomathic.com

CRYSTALKEY 360 PRODUCT SHEET

CRYPTOMATHiC

TECHNICAL SPECIFICATIONS

Operating Systems
- Windows
- Red Hat Enterprise Linux
- CentOS
- DBs
- MS SQL
- Oracle
- Maria DB
- PostGres

Security Modules
- HSMs
  - Entrust
  - Thales
  - Utimaco
- ESM - Confidential Computing
  - Cryptomathic Enclave Security Module

· **APIs**
- REST APIs - OpenAPI 3.0
- Libraries: Java, C++, C#/.NET
- JCA
- CNG
- PKCS#11

Supported Key types:
- AES
- 3DES
- RSA
- EC
- HMAC
- And more

Algorithms/Modes
- Hashing: SHA256, SHA384, SHA512
- Symmetric: ECB, CBC, IBMIPS, GCM, HMAC
- Asymmetric: PKCS#1v1.5, OAEP, PSS, ECDSA

Financial functionality
- PIN validation and translation
- CVV/CVC validation
- ARQC validation
- EMV issuer scripting

Integrations
- PKI
  - Smart ID Certificate Manager (formerly Nexus)
  - PrimeKey EJBCA
  - Entrust CA
  - and more…

- Multi-Cloud
  - GCP Cloud KMS
  - Azure Key Vault
  - AWS

- IdP Providers
  - Okta
  - Entra ID
  - KeyCloak
  - ForgeRock

- Key Listeners
  - Mainframe Listener
  - Atalla Listener
  - PayShield Listener
  - and more…

- Others
  - Microsoft Authenticode
  - CyberArk
  - Tomcat
  - and more…

For more information visit our website **www.cryptomathic.com**