CRYPTOMATHIC

KEY MANAGEMENT SYSTEM

A BUYERS GUIDE WITH SUPPLIER AND SYSTEM CHECK LIST

CRYPTOMATHIC

THE PRINCIPLES

A Key Management Platform is the backbone function of a mature security and compliance setup.

However, the scope of such a platform can vary a lot. This can add a costly, and potentially disruptive nature to the decision of implementing or replacing a key management system. Therefore, you want to ask the right questions to any potential suppliers!

In this guide, you will find a list of fitting questions to ask. One list is designed to vet the supplier, and another to qualify the product.

All questions are defined as yes/no questions, and you are looking for 'Yes's'!

This is a list of general questions and may vary slightly depending on the use case, however, keep in mind that a vendor who ticks all these boxes will have the tools to help future proof your operations and help your business scale in the long run. Some potential use cases for this list could include:

- Code signing
- Data protection and privacy
- Data masking and tokenization
- Consolidation through HSM as a service
- Future Proofing through Crypto Agility
- Streamline integration through Crypto as a service
- Or other...

SO HERE IT GOES...

CRYPTOMATHIC

KEY MANAGEMENT SYSTEM

SUPPLIER

PEDIGREE OF THE VENDOR

Do they have a strong reputation and long track record within the cryptographic security industry?

SECURITY ARCHITECTURE

Can the vendor provide a detailed security architecture that shows how various threats are mitigated?

FUTURE-PROOFING

Is the product being actively maintained and updated in line with market trends, e.g., cloud computing, regulation, post-quantum algorithms?

SUPPORT

Can the vendor provide professional services to help with design and implementation, and a high quality of ongoing maintenance and support (on a 24/7 basis if required)?

COMPLIANCE

Can the vendor prove how they address compliance with relevant regulations?

CREDIBILITY

Is the product proven? and is it backed up by high-profile references or case studies?

CRYPTOMATHIC

KEY MANAGEMENT SYSTEM

CAPABILITY CRITERIA

USER AUTHENTICATION
Does the solution provide strong user authentication?

POLICY CONTROL
Does the solution enforce user-defined policy, including user-defined roles and privileges and two-person operations?

AUDIT
Does the solution provide an integrity-protected audit log?

RESILIENCE
Does the solution provide for high-availability, backup and disaster-recovery?

INTEGRATION
Does the solution provide an 'out-of-the-box' integration with your applications?

CUSTOMIZATION
If required, can the vendor offer custom integrations?

EASE-OF-USE
Does the product make life easier for operations staff, e.g., context-sensitive GUI, asynchronous workflow and task automation?

CRYPTOMATHIC

CAPABILITY CRITERIA

APPLICATION AGNOSTICISM
Can the solution manage keys for alternative applications (other than the vendor's own applications)?

HSM VENDOR INDEPENDENCE
Does the solution support multiple HSM brands for vendor independence?

SECURITY MODULE OPTIMIZATION
Does the solution support Hardware Security Modules, Cloud Enclave Security Modules and Software Security Modules to optimize cost and security requirements for different use cases?

SUPPORTED KEY TYPES
Does the solution support a wide range of symmetric and asymmetric key types, lengths and formats (including any specific to your applications or industry)?

KEY IMPORT/EXPORT
Does the solution allow key import and export (wrapped under suitable key encryption keys)?

PHYSICAL PROTECTION
Are keys secured to the FIPS 140-2 standard (ideally Level 3)?

CRYPTOMATHiC

CONTACT US

Website

www.cryptomathic.com

Email

enquiry@cryptomathic.com

LinkedIn

www.linkedin.com/company/cryptomathic