"best" solution, we recommend a systematic approach based on the following sequential steps:

- Specify the different use cases for which cryptographic keys are used.
- Derive the relevant functional and non-functional requirements from these use cases.
- Compare and extend the derived requirements based on the list provided in this article, or any other relevant, internal and external guideline.
- Identify which of the existing solution fits best in regard to the extended requirements.
- Implement a Proof of Concept to ensure that the identified solution does indeed meet the requirements. Remember that Usability is Key!

Sources:

- 1. Suetonius, Vita Divi Julii, http://thelatinlibrary.com/suetonius/suet.caesar.html#56
- 2. Kerckhoffs, Auguste (January 1883). "La cryptographie militaire". Journal des sciences militaires. IX: 5–83, https://www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf
- 3. Kerckhoffs, Auguste (February 1883). "La cryptographie militaire". Journal des sciences militaires. IX: 161–191, https://www.petitcolas.net/kerckhoffs/crypto_militaire_2.pdf
- 4. https://www.youtube.com/watch?v=y2PM7Uox8Pc https://www.youtube.com/watch?v=nBljbb-nPY4
- 5. PKCS #11 Cryptographic Token Interface Base Specification Version 2.40
- 6. Key Management Interoperability Protocol Profiles Version 2.0
- 7. NIST SP 800-57 Part 1 Rev. 5: Recommendation for Key Management: Part 1 – General
- 8. NIST SP 800-152 A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)
- 9. FIPS 140-2 Security Requirements for Cryptographic Modules
- 10. NIST Validated Modules, https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search
- 11. Known KMIP Implementations, https://wiki.oasis-open.org/kmip/KnownKMIPImplementations

Dr. Julind Budurushi - Chief cyber Security Officer at Cloudical
Jurlind is working on security challenges in the cloud native approach, focusing on Kubernetes. He is a passionate engineer and trainer, and aims to enable and establish an holistic security mindset. In addition, he is a lecturer on Cyber Security

Table 1: CKMS findings of the research survey

Company	Solution	Reference
Cavium Inc.	LiquidSecurity & NITROX HSM	https://www.marvell.com/products/security-solutions/nitrox-hs-adapters.html
WISKey Semiconductors	VAULTIC Series	https://www.wisekey.com/products-services/secure-semiconductors/secure-elements/
securosys	HSM E-Series	https://www.securosys.com/en/product/pci-card-replacement-network-hsm
securosys	HSM X-Series	https://www.securosys.com/en/product/high-availability-high-performance-hardware-security-module
securosys	HSM Primus S500	https://www.securosys.com/en/product/primus-hsm-s500
securosys	Decanus	https://www.securosys.com/en/product/decanus-remote-control-terminal
Engage Communication Inc.	BlackVault	https://www.engageblack.com/products/black-vault/hardware-security-module
Hancome Secure	Enterprise Key Management	https://www.hsecure.co.kr/1_1_e.php
Kryptus	KNET	https://kryptus.com/en/network-hsm-knet/
Bloombase	KeyCatel	https://bloombase.com/products/keycastle/specifications.html

Company	Solution	Reference
Thales	CipherTrust Manager	https://cpl.thalesgroup.com/encryption/ciphertrust-manager
Thales	Vormetric Data Security Manager	https://cpl.thalesgroup.com/encryption/vormetric-data-security-manager
Venafi	Trust Protection Platform	https://www.venafi.com/platform/trust-protection-platform
HyTrust	Universal Key Management System for Encrypted Workloads	https://www.hytrust.com/products/keycontrol/
Ultimaco	Key Management	https://hsm.utimaco.com/products-hardware-security-modules/key-management/eskm/
RealSec	Dekaton	https://realsec.com/en/cryptosec-dekaton
IBM	Security Key Guardium Key Lifecycle Manager	https://www.ibm.com/products/ibm-security-key-lifecycle-manager/details
Symantec	Information Centric Encryption	https://help.symantec.com/cs/ICE1.0/ICE/v120281935_v120576779/Components-and-integrations-of-Information-Centric-Encryption?locale=EN_US
VirtuCrypt	Enterprise Key Management	https://www.virtucrypt.com/services/enterprise/enterprise-key-management/
VirtuCrypt	Remote Enterprise Key Management	https://www.virtucrypt.com/services/elements/remote-key-management/
HP	Enterprise Secure Key Management	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=c02907295
Cryptomathic	Crypto-Key-Management-System	https://www.cryptomathic.com/products/key-management/crypto-key-management-system
Cryptomathic	Crypto-Service-Gateway	https://www.cryptomathic.com/products/key-management/crypto-service-gateway
CYSEC	Arca	https://cysec.com/arca/
Fornetix	VaultCore	https://www.fornetix.com/our-products/
Fortanix	Self Defending KMS	https://resources.fortanix.com/fx2200-series2-datasheet/
Unbound	Unbound Key Control	https://www.unboundtech.com/unbound-key-control/
Zettaset	XCrypt – Key Management and Administration	https://www.zettaset.com/products/encryption-key-management/
nCipher	nCipher HSMs	https://www.ncipher.com/products
Cryptsoft	Key Management Products	https://www.cryptsoft.com/products/
Townsend	Alliance Key Manager	https://www.townsendsecurity.com/products/centralized-encryption-key-management
Atos	HSM Trustway	https://atos.net/en/solutions/cyber-security-products/data-protection-governance/data-encryption-hardware-security-module-hsm
Atos	Trustway DataProtect KMS	https://atos.net/en/solutions/cyber-security-products/data-protection-governance/trustway-dataprotect-kms-key-manager#Features
Ultra	KeyperPlus	https://www.ultra-cis.com/capabilities/cryptographic-key-management
sansec	SecKMS	https://en.sansec.com.cn/product/SecKMS-57.html
Yubico	YubiHSM	https://www.yubico.com/products/hardware-security-module/
Futurex	Key Managment Servers	https://www.futurex.com/products/category/key-management-servers
StorMagic	SvKMS	https://stormagic.com/svkms-data-sheet/
P6R	SKC Secure KMIP Client	https://www.p6r.com/software/skc.html#features
QuintessenceLabs	qCrypt 300H	https://www.quintessencelabs.com/products/encryption-key-management/

Table 2: Comparison of selected solutions

Requirements	Vendor	Thales	
	Solution	Cipher Trust Manager	Vormetric Data Security Manager
Functional			
Key Life Cycle		+	+
Key: -Grouping -Segregation -Splitting		 + + -	 + + -
Cryptopgraphy: -RSA -AES		 + +	 + +
Key Types: -Private Signature Key -Public Signature Key -Symmetric Data Encryption/Decryption Key -Symmetric Key Wrapping Key		 - - + +	 + + + +
APIs: -REST -PCKS#11 -KMIP		 + + + (1.1 only)	 + + + (1.1 only)
Integration with existing PK		-	+
Access Control: -Sparation of Duties -MFA -Dual control		 + + -	 + - (optional) -
Backup & Restore		+	+
On-premises		+	+
Policy configuration		+	+
-Accountibility -Auditing -Reporting		+ + +	+ + +
HW features: -Hot swappable RAID -Dual redudnant power supply -Independent network interfaces -N+2 redundancy		 + + + +	 - + + +
Businsess continuity		+	+
Security goals: -Confidentiality -Integrity		 + +	 + +
GUI		+	+
Input validation		n/a	n/a
User assistance		n/a	n/a
Non-Functional			
Design specification		+	+
HA		+	+
FIPS level 3		+	+
Application-agnostic		-(additinal connectors for each application)	- (additinal connectors for each application)
Strategic nature of the product		+	- (the vendor does not support this product in the long term)
Vendor credibility		+	+
Vendor support		+	+

	Cryptomathic	Fortanix	QuintessenceLabs	Unbound
	Crypto-Key-Management-System	Self Defending KMS	qCrypt 300H	Unbound Key Control
	+	+	+	+
	n/a n/a n/a	+ + +	+ + -	+ + +
	+ +	+ +	+ +	+ +
	+ + + +	+ + + +	- - + +	+ + + +
	+ + + (only symmetric profile)	+ + +(up to version 1.4)	+ + +(up to version 1.4)	+ + +(up to version 1.2)
	+	+	-	+
	+ + -	+ + -	+ - -	+ - +
	+	+	+	+
	+	+	+	+
	-	+	+	-
	+ + n/a	+ + +	+ + +	+ + -
	n/a + + +	- + + +	+ + + +	- - - -
	+	+	+	+
	+ +	+ +	+ +	+ +
	+	+	+	+
	n/a	n/a	n/a	n/a
	n/a	n/a	n/a	n/a
	+	+	+	+
	+	+	+	+
	+	+	+	-
	- (additional key listerner)	+	+	+
	+	+	+	+
	+	+	+	+
	+	+	+	+