SOLUTION BRIEF

How Fortanix Can Help Meet NCS-1:2020 Standards

What is NCS-1:2020 standards?

The National Cryptographic Standards (NCS - 1: 2020) defines the minimum cryptography requirements to be met by national entities when using cryptography to protect data (in use, at rest and in transit), systems and networks for civilian or commercial purposes.

Please refer to the detailed guidelines as stipulated by the NCS-1:2020 standards here- https://www.nca.gov.sa/ncs_en.pdf

The NCS defines two strength levels for cryptographic standards: the MODERATE level and the ADVANCED level.

- Having two strength levels provides more flexibility to choose the appropriate level of protection for different classes of data, systems, and networks. Each national entity is required to choose and implement the appropriate cryptographic standard level based on the nature and sensitivity of the data, systems, and networks to be protected. Furthermore, other cybersecurity regulations, issued by the NCA, may mandate the use of a particular cryptographic standard level to protect data, systems, and networks.
- The MODERATE and ADVANCED strength levels are designed to target 128-bit and 256-bit security levels, respectively. Specific requirements for each strength level are specified throughout this document. Any requirement not specifically associated with one of these two strength levels apply equally to both.

Fortanix supports all the capabilities aligned to both the strength levels for cryptographic standards as specified by the guideline.

How Fortanix can help meet NCS-1:2020 standards?

Fortanix Data Security Manager (DSM) offers organizations with all the capabilities for the implementation of the NCS-1:2020 standards related to data security and encryption key lifecycle management.

Encryption Capabilities, Key Lifecycle Management and Policy Enforcement
Fortanix DSM delivers encryption functionalities tailored to specified algorithms, key types, and lengths, ensuring compliance with NCS-1 standards for both moderate and advanced cryptographic strength. Fortanix DSM excels in key lifecycle management and policy enforcement, guaranteeing adherence to regulatory standards.

Random Number Generation, Post Quantum Crypto and Resistance to Side Channel Attacks
Fortanix DSM delivers encryption functionalities tailored to specified algorithms, key types, and lengths, ensuring compliance with NCS-1 standards for both moderate and advanced cryptographic strength. Fortanix DSM excels in key lifecycle management and policy enforcement, guaranteeing adherence to regulatory standards.

How Fortanix Helps?

Section 2.1, Section 2.2, and Section 2.3-
Algorithm support

Support for Symmetric Algorithms

For symmetric keys, the guideline specifically mandates the support for a) Stream Ciphers and b) Block Ciphers.
Fortanix solution supports Stream ciphers which are often used for speed and simplicity of implementation in hardware, and in applications where plaintext comes in quantities of unknowable length like a secure wireless connection.

For block ciphers, Fortanix DSM supports the following:
AES
DES
DES3
ARIA
SEED.

Support for Asymmetric Algorithms

For Asymmetric Keys, Fortanix supports- RSA- Fortanix supports configuration of RSA key exponent to be 65537, this can be enforced as the only accepted standard in Fortanix DSM by the administrator setting a crypto policy for RSA key generation.

X25519- Fortanix DSM support X25519 and Ed25519 depending on the use case. X25519 is typically used for key exchange for producing digital signatures for authentication and data integrity for various protocols and applications.

Support for Hash Functions

Fortanix supports all types of SHA-2 functions 256, 384, 512 and more.

Section 6.2 of the Guideline:
Support for Key Lifecycle Processes

- Fortanix DSM can enforce cryptographic policies at the account and group level to ensure key creation is specific to the approve key types, lengths etc.
- Fortanix DSM can integrate with various CA's such as but not limited to; Microsoft AD CS CA, KeyFactor etc.
  Depending on the integration and support from the external application, Fortanix can securely distribute and store key. If the end application supports BYOE/HYOK, Fortanix DSM will securely store Private keys within TEE's.

Section 7.1 of the Guideline
Support for Key Entropy with Pseudo Random Number Generation (PRNG)

Fortanix effectively addresses the challenge of insufficient entropy in software-based Hardware Security Module (HSM) solutions by employing dedicated FIPS 140-2 Level 3 compliant hardware. In our solution, a True Random Number Generator (TRNG) serves as the entropy source for our Deterministic Random Bit Generator (DRBG).

	It's important to note that the TRNG is not directly involved in key generation; instead, it acts as a reliable source of entropy for our DRBG. The DRBG, in turn, utilizes a Counter mode (CTR) with derivation function and AES-256 encryption, complying with SP 800-90A standards. This combination ensures a secure and unpredictable foundation for cryptographic operations. providing secure solutions that meet the highest industry standards. Furthermore, our hardware-based entropy source undergoes rigorous testing in accordance with SP 800-90C, validating its compliance with established standards. This commitment to robust cryptographic practices aligns with Fortanix's dedication to providing secure solutions that meet the highest industry standards.
Section 7.2 of the Guideline: Support for Post-Quantum Cryptography	The Fortanix Data Security Manager (DSM) platform is a data-first, unified security and privacy platform, powered by Confidential Computing. The Fortanix platform provides organizations with crypto agility, allowing them to rapidly adopt new cryptographic algorithms, without disrupting the organization's operations. With Fortanix, organizations can accelerate their post-quantum readiness journey and implement the latest NSA-recommended quantum-resistant algorithms, such as: · AES-256 · SHA-384 · SHA-512 · LMS Fortanix also closely follows NIST's announcements about new standards in quantum-resistant algorithms and rapidly implements the latest technologies into its SaaS platform.
Section 7.3 of the Guideline: Resistance to Side-Channel Attacks	Fortanix solutions have been designed with various defences, leveraging expertise in hardware-based security and cryptography, to protect against side channel attacks.

Further information can be found here:

Blog: 5 Things you need to know about Side Channels

Whitepaper: Side Channel and Runtime Encryptions solutions with Intel SGX.

Download the Spreadsheet to get detailed information
of specific support as mandated by NCS-1:2020

DOWNLOAD SHEET