****belum fact-check**

ISO/IEC 18033-1 Specify Encryption Systems for Data Confidentiality

Description:

- Establishes general principles for encryption algorithms.
- Provides definitions, classification, and terminology.
- Addresses security objectives, design principles, and application scope.
- Does not prescribe specific algorithms but sets foundational context.
- Supports lifecycle and operational considerations in encryption.

Justification:

- Provides foundational guidance for secure algorithm development.
- Essential for evaluating local/national cryptographic solutions.
- Supports regulatory, technical, and policy decision-making.
- Enhances compliance, security assessment, and procurement.
- Serves as an educational and training resource.

ISO/IEC 18033-6 Homomorphic Encryption

Description:

- Focuses on homomorphic encryption, which allows computations on encrypted data.
- Classifies HE schemes: Partially, Somewhat, and Fully Homomorphic Encryption.
- Defines security objectives (e.g., IND-CPA) and performance requirements.
- Provides evaluation criteria and use-case guidance.
- Relevant to privacy-preserving computation, cloud security, and quantum-resistant design.

Justification:

- Supports secure data processing and privacy-preserving technology.
- Crucial for evaluating HE schemes in government and cloud systems.
- Aids in national cryptographic innovation and post-quantum resilience.
- Provides a benchmark for regulatory frameworks and compliance.
- Enhances research, training, and collaboration in advanced cryptography.

ISO/IEC 14888-3 Digital Signatures

Description:

- Part of the ISO/IEC 14888 series focusing on digital signature mechanisms.
- Specifically defines digital signature algorithms based on discrete logarithm problems.
- Includes widely recognized schemes such as DSA, ECDSA, and other discrete-log-based techniques.
- Establishes algorithm parameters, key generation, signature generation and verification procedures.
- Addresses cryptographic strength, implementation guidelines, and performance considerations.

Justification:

- Essential for secure implementation and governance of digital signature systems.
- Provides formal specifications for widely used signature algorithms in PKI and identity systems.
- Supports the evaluation, certification, and deployment of cryptographic modules.
- Assists in policy development for secure authentication and digital trust services.
- Enables alignment with international standards in cryptographic infrastructure.

ISO/IEC 19790 Security Requirements for Cryptographic Modules

Description:

- Specifies security requirements for the design and implementation of cryptographic modules.
- Covers four security levels for varying degrees of protection.
- Applies to both hardware and software cryptographic modules (e.g., HSMs, smart cards, crypto libraries).
- Addresses areas such as cryptographic key management, physical security, operational environment, and self-tests.
- Harmonized with and foundational to international certification programs like FIPS 140-3 and Common Criteria.

Justification:

- Enables development and certification of secure cryptographic modules in line with international standards.
- Essential for national cryptographic governance and compliance verification.
- Supports critical infrastructure protection, particularly in defense, banking, identity systems, and telecommunications.
- Provides a benchmark for procurement, evaluation, and vendor accountability.
- Strengthens Malaysia's capability to develop a national certification or evaluation lab for crypto modules.

ISO/IEC 20543 Evaluation for Cryptographic Applications

Description:

- Defines test and evaluation methods to assess cryptographic modules against non-invasive attacks.
- Covers threats like timing attacks, power analysis (SPA/DPA), electromagnetic emissions, and fault injection.
- Supports the validation of secure hardware/software without requiring invasive tampering.
- Complements standards such as ISO/IEC 19790 and ISO/IEC 24759.
- Provides methodologies used by evaluation labs, product developers, and national certifiers.

Justification:

- Vital for assessing cryptographic systems in military, financial, and critical infrastructure.
- Enables national evaluation facilities to test real-world resistance against side-channel threats.
- Supports alignment with international certification practices.
- Strengthens local development and export readiness of certified cryptographic modules.
- Aids in policy, procurement, and research for secure device certification.

ISO/IEC 23837 Security of Cryptographic Systems

Description:

- Specifies general security requirements for the end-to-end lifecycle of cryptographic systems.
- Covers system design, implementation, deployment, operation, maintenance, and decommissioning.
- Emphasizes system-level integration, not just algorithm or module-level requirements.
- Addresses requirements such as trust anchors, key lifecycle management, secure system architecture, and interoperability.
- Serves as a foundation standard for building secure and trustworthy cryptographic systems across sectors.

Justification:

- Provides a system-level framework critical for designing secure national cryptographic infrastructure.
- Enhances governance over implementation, operation, and decommissioning of crypto systems.
- Supports compliance with international standards and best practices in system security.
- Crucial for formulating national-level cryptographic policies and architecture standards.
- Empowers local developers, integrators, and evaluators to build end-to-end secure systems.

ISO/IEC 15408 Evaluation criteria for IT security

Description:

- Internationally recognized as the Common Criteria (CC) for Information Technology Security Evaluation.
- Defines a structured framework for evaluating the security properties of IT products and systems.
- Composed of three parts:
    - Part 1: Introduction and general model.
    - Part 2: Security functional requirements (SFRs).
    - Part 3: Security assurance requirements (SARs).

- Enables creation of Protection Profiles (PPs) and Security Targets (STs) for specific system evaluations.
- Widely used for certifying products such as cryptographic modules, operating systems, smart cards, and network devices.
- Forms the basis of international mutual recognition arrangements like the CCRA (Common Criteria Recognition Arrangement).

Justification:

- Provides the international benchmark for evaluating IT product security and trustworthiness.
- Supports government procurement, ensuring only certified and evaluated products are used in critical infrastructure.
- Essential for establishing a national IT security certification scheme in line with global best practices.
- Facilitates mutual recognition of certified Malaysian products under the CCRA framework.
- Equips developers and auditors with a structured approach for developing and certifying secure IT systems.

ISO/IEC JTC 1/SC 27 Cryptographic and Security Mechanisms including PQC.

Description:

- A subcommittee of ISO/IEC JTC 1 responsible for developing international standards in:
- Information security
- Cybersecurity
- Privacy protection
- Maintains key standards such as:
    - ISO/IEC 27000 series (Information Security Management Systems)
    - ISO/IEC 15408 (Common Criteria)
    - ISO/IEC 19790 (Cryptographic modules)
    - ISO/IEC 23837, 20543, and 18033 series (Cryptographic techniques and systems)
- Structured into five Working Groups (WGs):
    - WG 1: Information security management systems

    - WG 2: Cryptography and security mechanisms
    - WG 3: Security evaluation, testing, and specification
    - WG 4: Security controls and services
    - WG 5: Identity management and privacy technologies
- Acts as a global forum for experts and member countries to collaborate on developing and maintaining security standards.
- Supports global harmonization of trust frameworks, compliance regimes, and cross-border cybersecurity initiatives.

Justification:

- Strategic for aligning national security frameworks with international standards.
- Provides early access to drafts and revisions of upcoming global cybersecurity standards.
- Enables active participation in shaping standards relevant to Malaysia's national interest.
- Supports development of national compliance, certification, and evaluation programs.
- Promotes local industry competitiveness by ensuring Malaysian products conform to globally accepted security specifications.
- Facilitates capacity building through exposure to global best practices and expert networks.

ETSI TR 103 619: Quantum-Safe Cryptography (QSC) – Cryptographic Libraries

ETSI GR QSC 001 – 005 (All QSC Reports)

FIPS (Federal Information Processing Standards)

FIPS 140-3 Security Requirements for Cryptographic Modules

Description:

- Specifies security requirements for cryptographic modules protecting sensitive information. It superseeds FIPS 140-2 and harmonized with ISO/IEC 19790:2012
- Key areas covered:
    - Physical security
    - Key management
    - Module interfaces
    - Role-based access control
    - Self-test and lifecycle management
- It defines four security levels (1-4) each providing increased physical and logical security.
- It requires cryptographic modules to undergo rigorous validation through the Cryptographic Module Validation Program (CMVP).

Justification:

- Mandatory for federal agencies and widely adopted across industries for security assurance.
- Ensure trustworthiness and interoperability of cryptographic solutions.
- Essential for deploying any cryptographic technology, including post-quantum algorithms in a validated and secure module

FIPS 203 Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM)

Description:

- Specifies a module-lattice-based key encapsulation mechanism (KEM), based on the CRYSTALS-Kyber algorithm, selected during NIST's post-quantum cryptography standardization process.
- It provides quantum-resistant key exchange capabilities.
- Designed to be efficient and secure even in the presence of quantum computers
- Intended to replace or augment traditional KEMs like RSA or ECC-based ones

Justification:

- Foundational PQC standard - supports quantum-resilient secure key exchange
- FIPS 203 algorithms are performance-efficient and suitable for a wide range of devices.
- Adoption is critical for future-proofing cryptographic infrastructure against quantum threats.

FIPS 204 Module-Lattice-Based Digital Signature Algorithm (ML-DSA)

Description:

- Defines a digital signature algorithm based on CRYSTALS-Dilithium, another winner of the NIST PQC competition.
- Offers strong security based on lattice problems.
- Designed to replace legacy digital signature schemes (like RSA or ECDSA) in a post-quantum world.
- Emphasizes high performance and robustness.

Justification:

- Primary candidate for quantum-safe digital signatures
- Suitable for a broad spectrum of applications - from secure email to firmware validation.

FIPS 205 Stateless Hash-Based Signature Scheme (SLH-DSA_

Description:

- Defines a stateless hash-based digital signature algorithm derived from the SPHINCS+ family
- Stateless design to avoid risk of key reuse errors
- Suitable for high-assurance environments where long-term security is crucial

Justification:

- An alternative or backup to lattice-based schemes with different security assumptions
- Offers conservatism and robustness, useful for long-term digital signatures such as software signing or archival records.
- Diversity in post-quantum approaches helps mitigate risks from unforeseen cryptanalytic advances

FIPS 197 Advanced Encryption Standard (AES)

Description:

- Specifies the Advanced Encryption Standard (AES), a symmetric block cipher used globally to encrypt sensitive data. It supports key sizes of 128, 192, and 256 bits and operates on 128-bit blocks.

Justification:

- AES is the foundation of the modern encryption for data at rest and in transit.
- Strong resistance to classical cryptanalysis

- Still considered quantum-resistant for symmetric encryption when used with larger key sizes (e.g., AES-256)
- Remains critical in hybrid post-quantum encryption systems.

FIPS 180-4 Secure Hash Standard (SHS)

Description:

- Defines the SHA family of cryptographic has functions: SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. SHA-1 is deprecated for many uses due to known weaknesses.

Justification:

- Hash functions are a cornerstone of cryptographic operations (e.g., signatures, HMACs key derivation).
- SHA-2 family is secure against both classical and known quantum attacks (Grover's algorithms gives a quadratic speedup not exponential)
- Continued relevance in both classical and post-quantum cryptography

FIPS 186-5 Digital Signature Standard (DSS)

Description:

- Defines digital signature algorithms including:
    - DSA (Discrete Algorithm)
    - RSA (Rivest-Shamir-Adleman)
    - ECDSA (Elliptic Curve DSA)
- Includes key generation, signature generation and verification procedures

Justification:

- Provides authentication, integrity, and non-repudiation in digital communications
- Classical algorithm are vulnerable to quantum attacks (e.g., Shor's algorithm breaks RSA and ECC
- Necessary during transition periods where hybrid (classical + PQ) signing is required for backward compatibility

FIPS 198-1 HMAC (Keyed-Hash Message Authentication Code)

Description:

- Defines a method for using cryptographic hash function (e.g, SHA-256) to produce a message authentication code (MAC)

Justification:

- Widely used for data integrity and authenticity

- HMACs based on SHA-2 remain resistant to quantum attacks
- Fundamental component in hybrid cryptography systems and secure protocols (e.g., TLS, IPsec)

FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

Description:

- Provides guidance for categorizing systems based on confidentiality, integrity, and availability (CIA) impacts

Justification:

- While not algorithm-specific, it helps organizations identify required cryptographic protections based on risk levels
- Drives the selection and implementation of appropriate cryptographic mechanism

ITU-T (International Telecommunication Union - Telecommunication Standardization Sector)

1. Y.3800 Overview on networks supporting quantum key distribution.
2. H.234 Encryption key management and authentication system for audiovisual services
3. ITU-T QKD Standards

Key Management Interoperability Protocol (KMIP) - a protocol for managing cryptographic keys, with updates to support PQC algorithms

Transition Guidelines and Roadmaps

1. NIST IR 8547 Guidelines for transitioning to PQC standards
2. GSMA PQC guidelines: recommendations for telecom use cases