

4.1.1 Cryptography

Contents

1. Definitions	2
2. Purpose	3
3. Scope	3
4. Policy	3
5. Non-compliance	4
6. References	4

Version	Adjustment Date	Approved By	Approval Date
2.0	4/7/2024	Saud Alsulami	7/7/2024



1. Definitions

For purposes of this "Cryptography" the following definitions apply:

- **Encryption** is the process of converting plain text or any other type of data into an unreadable format called ciphertext, using an algorithm and an encryption key. The primary purpose of encryption is to ensure that the data remains secure and confidential, even if it is intercepted or accessed by unauthorized parties.
- **A hash** is a function that converts an input (or 'message') into a fixed-size string of bytes. The output, commonly known as a hash value or hash code, is typically a unique representation of the input data. Hash functions are widely used in various applications like data integrity checks, password storage, and digital signatures, due to their one-way nature and the difficulty of generating the original input from the hash value.
- **Encryption keys** are secret values used in cryptographic algorithms to perform encryption and decryption of data. In symmetric encryption, the same key is used for both encryption and decryption. In asymmetric encryption, two keys are used: a public key for encryption and a private key for decryption. The security of the encrypted data relies heavily on the protection and management of these keys.
- **RSA (Rivest-Shamir-Adleman)** is a widely used asymmetric cryptographic algorithm named after its inventors. It employs a pair of keys: a public key, which can be freely distributed, and a private key, which must be kept secret. RSA is commonly used for secure data transmission, digital signatures, and key exchange, and is known for its robustness and security when using sufficiently large key sizes (e.g., 2048 bits or higher).
- **AES (Advanced Encryption Standard)** is a symmetric encryption algorithm that encrypts data in fixed block sizes (128 bits) using keys of 128, 192, or 256 bits. Known for its efficiency and security, AES is widely adopted in various security protocols and applications to protect sensitive information both in transit and at rest. AES-256 is favored for its high level of security.



2. Purpose

The purpose of this policy is to establish a framework for the effective use of cryptography to protect the confidentiality, integrity, and availability of sensitive information. By implementing approved cryptographic protocols, algorithms, and key management practices, Taqnyat aims to safeguard its information assets, comply with legal and regulatory requirements, and build trust with its customers, partners, and stakeholders.

3. Scope

This policy outlines the requirements and guidelines for the use of cryptography to protect sensitive information within Taqnyat and its subsidiaries. The scope of this policy covers all information systems, networks, and data handled by Taqnyat, including data at rest, data in transit, and data in use. The policy applies to all employees, contractors, and third parties who have access to or handle sensitive information on behalf of Taqnyat.

4. Policy

- 4.1. All encryption technologies and techniques used by Taqnyat must be approved by Taqnyat Cyber Security department and Technical Advisor.
- 4.2. Taqnyat Technical Advisor is responsible for the distribution and management of all encryption keys, other than those managed by Taqnyat customers.
- 4.3. All use of encryption technology should be managed in a manner that permits properly designated Taqnyat personnel to promptly access all data, including for purposes of investigation and business continuity.
- 4.4. Taqnyat Technical Advisor will create and publish the Taqnyat Encryption Standards, which must include, at a minimum:
 - The type, strength, and quality of the encryption algorithm required for various levels of protection.
 - Key lifecycle management, including generation, storing, archiving, retrieving, distributing, retiring, and destroying keys.



- 4.5. All Taqnyat information classified as confidential must be encrypted when:
 - Transferred electronically over public networks.
 - SMS Content transferred and stored
 - End User Client and Employees Passwords
 - Stored on mobile storage devices.
 - Stored on laptops or other mobile computing devices.
 - At rest.
 - All Encrypted data must use the RSA, AES and Hash encryption methodology.
- 4.6. The use of proprietary encryption algorithms is not permitted, unless approved by Taqnyat Cyber Security and Technical Advisor.
- 4.7. The Cryptographic Techniques List file is considered part of these policies and must be implemented and adhered to.
- 4.8. The Cryptographic Techniques List file is reviewed annually and whenever there is a need to change the encryption techniques due to the discovery of vulnerabilities, for example.

5. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

6. References

- ISO 27002
- National Cybersecurity Authority's (NCA) ECC standards
- SANS v7.0
- NIST

