Cybersecurity Cryptography Standard operating procedure

I. Purpose

1. The purpose of the cryptography SOP is to provide guidance for protecting WHO information while in use, during its transmission (in transit) and while at rest (stored) in accordance with its organizational value and as a result of a risk assessment.

2. This Procedure shall be read in conjunction with the WHO Global Cybersecurity Policy, related Cryptography Rule and WHO asset classification rule.

II. Scope

3. This procedure applies to all WHO employees, contactors and visitors ("users") using the WHO information assets and applicable to all offices of the WHO presence and scope.

Definitions

4. Please refer to the Cybersecurity Definitions document

Procedure

Risk-based approach

5. Cryptography requirements shall be established based on a risk based approach to identify the required level of protection taking into account the type, strength and quality of the encryption algorithm required. Cryptographic systems that have been proven to be weak will not be used to provide cryptographic services. Refer to the Annex 1, for getting further guidance on certain algorithms.

General

6. Cryptographic controls can be used to achieve different Cybersecurity objectives, e.g.:

a. **Confidentiality**: using encryption of information to protect confidential information from unauthorized access, while the information is at rest (stored) or while in transit (transmitted);

b. **Integrity/authenticity**: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted confidential information;

c. **Non-repudiation**: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;

d. **Authentication**: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources

7. Some of the main uses of cryptography are shown below:

a. **Passwords** are usually stored in encrypted or hashed form in the authenticating systems (e.g. Active Directory, Azure AD, etc.). Complex processes such like hashing are also used to protect passwords transmitted over networks.

b. **Databases** may also contain encrypted information to prevent an unauthorised user with direct access to the database from using it.

c. **Network communications** can be secured, either through the use of encrypted protocols (e.g. WPA2) or through the use of encrypted Virtual Private Networks (VPNs) over untrusted networks.

d. **Electronic mails** or transactions may be encrypted and/or digitally signed to guarantee their confidentiality, integrity and authenticity.

e. **Electronic signatures** are used to guarantee the origin and/or content of a message or other data.

f. **Files** stored on computers or media (e.g. backup tapes, disks or USB memory sticks) can be encrypted to protect their confidentiality.

g. A **Digital Fingerprint** is a hash-value of a document that is used to verify the integrity of a signed electronic document.

h. **Whole disk encryption** (e.g. Bitlocker in Synergy10 machines) is used to protect information, particularly on portable devices such as laptops.

i. **Web communications** may be encrypted, often via HTTPS using TSL, to guarantee the identity of either party and/or to protect the data transmitted.

j. **Interactive application sessions** may be encrypted to protect data in transit from the user's workstation to the application server.

k. **Application-to-application** communications can also be encrypted.

l. **File transfers** and remote file services may be encrypted, usually for confidentiality (e.g. SSH or SFTP).

8. Several of these functions are supported by Public Key Infrastructure (PKI) systems, which provide a framework for issuing and using public/private key pairs. See below section on PKI for more details.

9. WHO will use cryptographic systems to provide various cryptographic services:

a. Symmetric cryptography: the involved parties share a common secret (password, passphrase, or key)

b. Asymmetric cryptography: Asymmetric algorithms use two keys, one to encrypt the data, and either key to decrypt. These inter-dependent keys are generated together. One is labelled as Public key and is distributed freely. The other is labelled as Private Key and shall be kept confidential.

c. Hashing: Hash functions take some data of an arbitrary length (and possibly a key or password) and generate a fixed-length hash based on this input.

d. Key exchange algorithms: These allow use to safely exchange encryption keys with an unknown party

10. Information should be secured end-to-end, while in transit as well as in storage, both inside and outside WHO networks.

11. Cryptography controls should be embedded for protecting the information transported by mobile or removable media devices.

Key Management

12. Key management procedures must be documented and implemented for all cryptographic processes. These procedures must cover at least the following:

a. Generation – The private key shall be created using industry best practices on cryptography such that it cannot be practically replicated or guessed by an adversary.

b. Issuing and obtaining public key certificates: Public key certificates must be issued and obtained using a well-established secure method (e.g. Internal PKI or Cloud-based PKI).

c. Distribution – A secure method of delivering the keys to the intended user shall be established, along with instructions for activating the keys.

d. Key Inventory – A current inventory of all <AGENCY NAME> keys with description of their purpose and the person to whom they are entrusted shall be established. The persons or office / division who will be responsible for maintaining the inventory shall be named.

e. Storage and Access – Standards shall be set out describing under what conditions, a user can store both electronic and physical, keys and how they shall be protected. A backup or archive shall be created along with rules for how authorized users can obtain access to the backup and main storage. All such accesses shall be logged with relevant data.

f. Key Lifetime -- All public and private encryption keys shall have a defined lifetime and shall be changed on or before the expiration date. Keys or key components that are no longer required shall be destroyed with the destruction witnessed and documented by a third party.

g. Key Protection – Persons entrusted with a private encryption key shall reasonably safeguard the key from disclosure. The private key itself is considered “Confidential” and access shall be strictly limited. Standards shall be created regarding the strength of passwords that may be used to generate or use encryption keys.

h. Compromised Keys –Standards shall be created to handle an incident where a key is suspected or known to be disclosed or corrupted. Standards shall include notification of parties, when suitable, and destruction of the compromised key.

i. Revoking keys – Standards shall be defined on how keys shall be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys shall also be archived);

j. Recovering keys – Standards shall be defined to recover keys that have been lost or corrupted

k. Backup and archiving of keys – Standards shall be defined on the backup and recovering options for keys

l. Logging and auditing of key management systems – All access to key management systems shall be logged such that it is possible to assess who accessed the system at any given point of time and what actions were taken by the individual during the course of access. The key management system shall be monitored using the "four eyes principle."

Public Key Infrastructure (PKI)

13. PKI is implemented through a system that employs cryptography. As such, PKI implementations must follow the rules contained in the Cryptography Rule as well as in the previous sections of this SOP.

14. WHO systems and applications must only use the Organization's provided PKI infrastructure.

15. Each PKI system must have a Certificate Policy (CP) and a Certificate Practice Statement (CPS) that define the rules and practices governing the security policies and controls of the system. The CP and CPS must be made available to all users of the system. The CPS documents the practices employed in the operations and management of the PKI system.

16. The confidentiality, integrity and availability of the private key that is used to sign the root certificate must be highly protected and the root certificate must be renewed on a timely basis to ensure the continuous validity of all certificates.

17. A Certificate must contain at least the following information:

a. Version
b. Serial number
c. Name or other information that can uniquely identify the requestor
d. Period of validity of the certificate
e. The identification of the CA issuing the certificate
f. The identity code of the certificate
g. The usage scope of the certificate
h. The algorithm used to create the signature
i. The signature of the CA.

18. A certificate must be revoked as soon as possible when the relationship between the requestor and the public key ends or when the certificate is no longer valid. The CA must authenticate each certificate revocation request to the same level as for the issuing of the certificate.

19. Revoked certificates must be included in a Certificate Revocation List (CRL) until the certificate expiration date. The certificate owner must be notified of the revocation of the certificate.

20. A link to the CRL must be included in all certificates. All appropriate measures shall be taken to avoid denial-of-service attacks that may render CRLs unavailable to the verifiers. The CRL must be signed with the private key of the CA. The verifier must be able to verify the integrity and origin of the CRL by checking the electronic signature of the CRL.

21. End users must not use certificates for fraudulent or other illegal purposes or to masquerade as other users.

22. Certificate owners must inform the CA immediately if any of the following conditions is true:

a. identification information in the certificate becomes invalid;
b. the private key of the requestor/owner has been compromised;
c. the owner leaves the WHO (e.g. digital signature and email encryption)

Risks linked with the use of Cryptography

23. Even though cryptography is an effective Cybersecurity control, improper use can lead to a number of risks, due to either inadequate procedures or malicious use, such as:

a. Encryption can introduce technical complications such as problems in establishing secure (encrypted) network connections.

b. Encryption can also cause effective (temporary or permanent) loss of data, if the information only exists in encrypted form but the key is lost.

c. Cryptographic tools could be used for hiding data associated with illegal activities and impeding investigation procedures.

d. Encryption of communications (such as e-mails or Internet traffic) can make it impossible to scan for viruses or other threats at the gateways.

e. Weaknesses in cryptographic algorithms, may introduce vulnerabilities.

f. Deliberate acts, such as unauthorised use of a crypto module for nefarious purposes, can introduce liabilities.

Compliance

24. All individuals referred to within the scope of this procedure are required to adhere to its terms and conditions.

25. All alleged violations of this procedure should be reported to the Global or Regional Service Desk and the appropriate authority responsible for administering this procedure in the WHO location involved (primarily members of the Cybersecurity team, Regional ICT Managers, WHO Representatives in the COs), who will investigate the allegations and if appropriate refer the matter to the relevant WHO authorities.

26. Individual WHO supervisors are responsible for ensuring that this procedure is applied within their own teams. This also extends to any contractors, consultants or visitors who are working within them.

Any queries on the application or interpretation of this procedure must be discussed with the IT Department prior to any action being taken.

ANNEX I

Minimum required encryption algorithms and strength

Algorithm	Recommendation
Symmetric	Key sizes of 128 bits are sufficient for most applications Consider 168 or 256 bits for secure systems such as applications hosting sensitive data Symmetric-key encryption protocols shall include message authentication Always Encrypt then Message Authentication Codes (MACs)
Asymmetric	Key sizes of 1280 bits or 1536 bits are sufficient for most applications in the intranet 2048 bits shall be considered for applications/systems that have been rated as HIGH or VERY HIGH in the Cyber risk classification Tool
Hashing	Hash sizes of 256 bits are sufficient for most applications Consider 512 bits for applications/systems that have been rated as HIGH or VERY HIGH in the Cyber risk classification Tool