NÚKIB

MINIMUM REQUIREMENTS FOR CRYPTOGRAPHIC ALGORITHMS

Cryptographic Security Recommendations

Non-binding EN translation of CZ version 4.0, valid as of February 1, 2025

Contents

Introduction

Pursuant to Section 26, letter d) of Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, cyber security reporting requirements and data disposal (hereinafter referred to as the "Cyber Security Decree"), liable entities under the Act No. 181/2014 Coll., on cyber security and the amendment of related laws (hereinafter referred to as the "Cyber Security Act"), are obliged to take into account cryptographic recommendations issued by the National Cyber and Information Security Agency for the purpose of protecting information and communication system assets. This document contains the aforementioned recommendations.

For questions of a legal nature, please contact the secretariat of the National Cyber and Information Security Agency:

National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky

Phone: +420 541 110 777
E-mail: nckb@nukib.gov.cz

Questions, comments, and suggestions of a cryptological nature can be sent to the e-mail address: kryptoalgoritmy@nukib.gov.cz

Notice:

This document contains the recommendations of the National Cyber and Information Security Agency in the field of cryptographic protection. Liable entities under the Cyber Security Act are obliged, according to Section 26 letter d) of the Cyber Security Degree, to take these recommendations into account to protect information and communication system assets.

This document may be changed based on current knowledge in the field of cryptographic protection.

1 Cryptographic Security Recommendations

The National Cyber and Information Security Agency (NÚKIB) issues the list of approved cryptographic algorithms (*Approved, Recommended*) that it believes to be secure at least in the medium term.

Quantum-vulnerable cryptography and preparation for the transition to quantum-resistant cryptography

For each algorithm group, we indicate below whether they are vulnerable or resistant to quantum algorithms. The consequence of quantum vulnerability of an approved algorithm is the need to replace it by suitable quantum-resistant cryptography in the not-too-distant future.

For the case of classical asymmetric algorithms (Section 3), which are primarily targeted by the quantum threat, these quantum-resistant variants are specifically mentioned in separate Section 4 of this document (Post-Quantum Cryptography).

Cryptographic recommendations for the preparation of the transition from quantum-vulnerable to quantum-resistant cryptography are presented and explained in more detail in the annex “Quantum Threat and Quantum-Resistant Cryptography”.

2 Symmetric Algorithms

a) Block ciphers

1. Advanced Encryption Standard (AES) with key lengths of 128, 192 and 256 bits
2. Twofish with a key length of 128 to 256 bits
3. Camellia with key lengths of 128, 192 and 256 bits
4. Serpent with key lengths of 128, 192 and 256 bits

b) Stream ciphers

1. SNOW 2.0, SNOW 3G with key lengths of 128 and 256 bits
2. ChaCha20 with a key length of 256 bits and a key load[1] of less than 256 GB

We recommend preferring:

- Block ciphers over stream ciphers.
- In the case of block ciphers: AES, Camellia, and Serpent (in this order).
- Key length of 256 bits.

Quantum vulnerability and quantum resistance:

- All ciphers with key lengths of 128 bits and 192 bits are quantum-vulnerable.
- All ciphers with a key length of 256 bits are quantum-resistant.

c) Authenticated encryption modes

1. CCM
2. EAX
3. OCB1 and OCB3, we recommend preferring OCB3 over OCB1
4. GCM with an initialization vector length of 96 bits and a tag length of 128 bits
5. ChaCha20 + Poly1305 with a key load[1] of less than 256 GB
6. Composite Encrypt-then-MAC schemes

Caveats:

- Approved encryption modes must use block ciphers specified in Section 2, point a).
- Composite Encrypt-then-MAC schemes must only use integrity protection modes specified in Section 2, point e) for the MAC calculation, and encryption modes specified in Section 2, point d) for encryption, or, in the case of disk encryption, modes specified in Section 2, point f). Furthermore, these schemes must not use the same key for the encryption and MAC calculation.
- The initialization vector must be part of the input for the MAC calculation.
- When using the GCM mode, the initialization vector value must not be repeated for a given key. In any case, the key must be changed after 2^{32} initialization vector values at the latest.

[1] Key load is the maximum amount of data that can be encrypted with the same key.

d) Encryption modes for composite Encrypt-then-MAC schemes

1. CTR
2. OFB
3. CBC (also CBC-CS)
4. CFB

Caveats:

- CBC and CFB modes must be used with a random, attacker-unpredictable initialization vector.
- When using OFB mode, the initialization vector value must not be repeated for a given key.
- When using CTR mode, the value of the counter must not be repeated for a given key.
- Stand-alone use of these encryption modes, outside the Encrypt-then-MAC schemes, is not approved.

e) Integrity protection modes (Message Authentication Code – MAC)

1. HMAC with a hash function specified in Section 5
2. CMAC
3. KMAC
4. GMAC with an initialization vector length of 96 bits and a tag length of 128 bits
5. EMAC[2]
6. UMAC[2]

Caveats:

- When using GMAC, the initialization vector value must not be repeated for a given key. In any case, the key must be changed after 2^{32} initialization vector values at the latest.
- When using UMAC, the initialization vector value must not be repeated for a given key.
- For all algorithms listed above, the tag length must be at least 96 bits, unless otherwise stated.

f) Disk encryption modes

1. XTS – the length of a data unit (sector) must not exceed 2^{20} blocks of the cipher (for a 128-bit block cipher, it is approximately 16 MB)
2. EME2

Quantum resistance: All approved symmetric cryptography modes are quantum-resistant when used with a quantum-resistant block cipher or a quantum-resistant hash function.

[2] EMAC and UMAC algorithms are rare in practice and we are considering removing them from the list of approved algorithms in the future. In case you are using them, please share this information to kryptoalgoritmy@nukib.gov.cz.

3 Classical Asymmetric Algorithms

a) Classical digital signature algorithms

1. Digital Signature Algorithm (DSA) with a key length of 3072 bits or more and cyclic subgroup parameter length of 256 bits or more
2. Elliptic Curve Digital Signature Algorithm (EC-DSA) with a key length of 256 bits or more
3. Rivest-Shamir-Adleman Probabilistic Signature Scheme[3] (RSA-PSS) with a key length of 3072 bits or more
4. Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) with a key length of 256 bits or more

Quantum vulnerability: All approved classical digital signature algorithms are quantum-vulnerable.

b) Classical key establishment algorithms[4]

1. Diffie-Hellman (DH) with a key length of 3072 bits or more and cyclic subgroup parameter length of 256 bits or more
2. Elliptic Curve Diffie-Hellman (ECDH) with a key length of 256 bits or more
3. Elliptic Curve Integrated Encryption System – Key Encapsulation Mechanism (ECIES-KEM) with a key length of 256 bits or more
4. Provably Secure Elliptic Curve – Key Encapsulation Mechanism (PSEC-KEM) with a key length of 256 bits or more
5. Advanced Cryptographic Engine – Key Encapsulation Mechanism (ACE-KEM) with a key length of 256 bits or more
6. Rivest Shamir Adleman – Optimal Asymmetric Encryption Padding (RSA-OAEP) with a key length of 3072 bits or more
7. Rivest Shamir Adleman – Key Encapsulation Mechanism (RSA-KEM) with a key length of 3072 bits or more

Recommendation: For elliptic-curve cryptography, we recommend preferring a key length of 384 bits or more.

Quantum vulnerability: All approved classical key establishment algorithms are quantum-vulnerable.

[3] The RSA-PSS algorithm is sometimes equivalently referred to as RSASSA-PSS.

[4] We consider *key establishment* to be the most general term which covers all methods in which the communicating parties can obtain a shared key. It encompasses both *key agreement* and *key wrapping/key encapsulation*.

4 Quantum-Resistant Asymmetric Algorithms (Post-Quantum Cryptography)

The process of replacing quantum-vulnerable cryptography will be extremely challenging. Therefore, we recommend that you familiarize yourself with the more detailed explanations and recommendations provided in the annex "Quantum Threat and Quantum-Resistant Cryptography".

a) Stand-alone post-quantum key establishment algorithm

1. ML-KEM-1024

ML-KEM-1024 is the standardized version of the Kyber-1024 algorithm (also referred to as CRYSTALS-Kyber Level 5). For stand-alone use, implementation according to the NIST standard (FIPS 203)[5] is required.

b) Hybrid quantum-resistant cryptography for key establishment

It combines one of the following post-quantum KEM/Encryption algorithms:

1. ML-KEM-1024/Kyber-1024, ML-KEM-768/Kyber-768
2. FrodoKEM-1344, FrodoKEM-976
3. mceliece8192128, mceliece6688128, mceliece460896, mceliece8192128f, mceliece6688128f, mceliece460896f

with one of the classical key establishment algorithms specified in Section 3, point b), in such a way that the security of the hybrid combination is preserved even if one of its components is broken.

Recommendation: In hybrid combination, it is possible to use the standardized ML-KEM algorithm as well as the original Kyber algorithm, however, we recommend preferring ML-KEM over Kyber and in the future, we anticipate approving the standardized version only.

c) Stand-alone post-quantum digital signature algorithm for firmware and software integrity protection

1. LMS
2. XMSS

We only recommend using these algorithms to protect firmware and software integrity.

[5] https://csrc.nist.gov/pubs/fips/203/final

d) Stand-alone post-quantum digital signature algorithm for general use

1. ML-DSA-87
2. SLH-DSA

ML-DSA-87 is the standardized version of the CRYSTALS-Dilithium Level 5 algorithm (see the NIST standard FIPS 204)[6]. SLH-DSA is the standardized version of the SPHINCS+ algorithm.

Caveat: For stand-alone use of the SLH-DSA algorithm, we approve NIST security levels 3 and 5 (see the NIST standard FIPS 205)[7].

e) Hybrid quantum-resistant cryptography for digital signatures

It combines one of the following post-quantum digital signature algorithms:

1. ML-DSA/CRYSTALS-Dilithium
2. SLH-DSA/SPHINCS+
3. Falcon

with one of the classical digital signature algorithms specified in Section 3, point a), in such a way that the security of the hybrid combination is preserved even if one of its components is broken.

Caveat: For ML-DSA in hybrid combination we approve the variants ML-DSA-87 and ML-DSA-65. For SLH-DSA in hybrid combination we approve security levels 3 and 5 according to the NIST standard FIPS 205[5]. Specific variants of Falcon are going to be recommended following the standardization process of this algorithm.

[6] https://csrc.nist.gov/pubs/fips/204/final
[7] https://csrc.nist.gov/pubs/fips/205/final

5 Hash Function Algorithms

a) SHA-2 hash functions

1. SHA-256
2. SHA-384
3. SHA-512
4. SHA-512/256

b) SHA-3 hash functions

1. SHA3-256
2. SHA3-384
3. SHA3-512
4. SHAKE128
5. SHAKE256

c) Other hash functions

1. Whirlpool
2. BLAKE2

Caveat: All approved hash functions must have an output length of at least 256 bits. However, we recommend preferring an output length of at least 384 bits.

Quantum vulnerability and quantum resistance:

- All approved hash functions with an output length of 384 bits or greater are quantum-resistant.
- All approved hash functions with an output length of 256 bits or less are quantum-vulnerable.

6 Algorithms for Secure Password Storage

1. Argon2 with selected function Argon2id and parameters at least
   i) t = 1, m = 2^{21} (2 GiB of RAM), p = 4
   ii) t = 3, m = 2^{16} (64 MiB of RAM), p = 4 for memory-constrained environments
2. scrypt with parameters at least N = 131072 (2^{17}), r = 8 a p = 1
3. PBKDF2
   i) HMAC-SHA-256 with at least 600 000 iterations
   ii) HMAC-SHA-512 with at least 210 000 iterations

Caveats:

- Randomly generated salt must be used for each password.
- The length of the salt must be at least 128 bits (16 B).
- The length of the output (tag) must be at least 256 bits (32 B).

Recommendations:

- It is advisable to choose the parameter size as the maximum possible practically usable for the given application.
- We recommend preferring Argon2 with the above parameters.

Quantum resistance: All approved password storage algorithms are quantum-resistant, provided that the symmetric ciphers and hash functions used in them are quantum-resistant.

Document version

Date (original)	Date (translation)	Version	Changed (name)	Change
Nov. 26, 2018	-	1.0	OBIT, NÚKIB	Document creation
June 8, 2022	-	2.0	OBIT, NÚKIB	Document revision, algorithms for secure password storage
July 1, 2023	Nov. 1, 2023	3.0	OBIT, NÚKIB	Document revision, quantum-resistant cryptography, annex
Feb. 1, 2025	May 20, 2025	4.0	OBIT, NÚKIB	Document revision, NIST post-quantum standards, KMAC, parameter update for secure password storage algorithms, legacy algorithms removal