NÚKIB

MINIMUM REQUIREMENTS FOR CRYPTOGRAPHIC ALGORITHMS

Cryptographic Security Recommendations

Version 1.0, valid as of November 1, 2023

Content

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.cz

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

(1) Categories of Cryptographic Algorithms Based on Their Validity Period

In terms of validity period, we distinguish the following categories of algorithms:

Approved cryptographic algorithms (*Recommended, Future*) are algorithms that we believe are secure at least in the medium term.

Quantum-resistant public-key cryptography (*Quantum Safe Cryptography*) are public-key cryptographic mechanisms that we believe will be suitable to replace quantum-vulnerable cryptography in the near future.

Legacy cryptographic algorithms are algorithms that we recommend abandoning by the end of 2023. Furthermore, we recommend that new cryptographic systems should only contain approved cryptographic algorithms (and not the legacy ones).

(2) 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 that it has to be replaced by suitable quantum-resistant cryptography in the not-too-distant future. This is briefly outlined in Chapter 5 of this document.

Cryptographic recommendations for the preparation of the transition from quantum-vulnerable to quantum-resistant cryptography are presented and explained in the appendix “Kvantová hrozba a kvantově odolná kryptografie” (Quantum Threat and Quantum-Resistant Cryptography), only available in Czech.

(3) Symmetric Algorithms

a) Approved block and stream 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
5. SNOW 2.0, SNOW 3G with key lengths of 128 and 256 bits
6. ChaCha20 with a key length of 256 bits and a key load of less than 256 GB

Note: The key load is the maximum amount of data that can be encrypted with the same key.

We recommend preferring:

- Block ciphers over stream ciphers.
- Among block ciphers: AES, Camellia, and Serpent (in this order).
- A 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.

b) Legacy block and stream ciphers

1. Triple Data Encryption Standard (3DES) with 112-bit key length, limited use only with a key load less than 10 MB, gradually moving to AES. It is recommended to use a unique key for each message.
2. Blowfish with 128-bit key length, limited use only with a key load less than 10 GB
3. Kasumi with 128-bit key length, limited use only with a key load less than 10 GB

Quantum vulnerability:

All legacy ciphers are quantum-vulnerable.

c) Approved authenticated encryption modes

1. CCM
2. EAX
3. OCB1 and OCB3, we recommend preferring OCB3 over OCB1
4. GCM with a nonce length of 96 bits and a tag length of 128 bits, the key must be changed after 2^{32} nonce values at the latest
5. ChaCha20 + Poly1305 with a key load of less than 256 GB
6. Composite Encrypt-then-MAC schemes

Notes:

- Approved encryption modes must use approved block ciphers.
- Encrypt-then-MAC schemes must use only the encryption modes specified in paragraph d) for encryption and only approved integrity protection modes for the MAC calculation.
- The initialization vector (or nonce) must be part of the input for the MAC calculation.

d) Encryption modes

Their stand-alone use is considered legacy, but their use in composite Encrypt-then-MAC schemes is approved.

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

Notes:

- For use within an approved composite Encrypt-then-MAC scheme, these modes must use only approved block ciphers.
- CBC and CFB modes must be used with a random, (for an attacker) unpredictable initialization vector.
- When using the OFB mode, the value of the initialization vector must not repeat for the given key.
- When using the CTR mode, the value of the counter must not repeat for the given key.
- When using the CBC mode for encryption without integrity protection, resistance against the padding attack on the CBC mode must be verified.

e) Approved 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

f) Approved integrity protection modes

1. HMAC with an approved hash function
2. EMAC
3. CMAC
4. UMAC with a tag length of 64 bits

Quantum resistance:

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

g) Legacy integrity protection modes

1. HMAC-SHA1
2. CBC-MAC-X9.19, limited use only with a load of less than 10^9 MACs

Quantum vulnerability and quantum resistance:
Of the modes considered, only CBC-MAC-X9.19 is quantum-resistant, provided that it uses a cipher with a key length of 256 bits (ciphers with key lengths of 128 bits and 192 bits are quantum-vulnerable).

(4) Classical Asymmetric Algorithms

a) Approved 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 (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) Legacy classic digital signature algorithms

1. Digital Signature Algorithm (DSA) with a key length of 2048 bits and cyclic subgroup parameter length of 224 bits
2. Elliptic Curve Digital Signature Algorithm (EC-DSA) with a key length of 224 bits
3. Rivest-Shamir-Adleman Probabilistic Signature Scheme (RSA-PSS) with a key length of 2048 bits
4. Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) with a key length of 224 bits

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

c) Approved classical key agreement and key encryption algorithms

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 an approved hash function and 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 using a key length of 384 bits or more.

Quantum vulnerability:

All approved classical key agreement and key encryption algorithms are quantum-vulnerable.

d) Legacy classical key agreement and key encryption algorithms

1. Diffie-Hellman (DH) with a key length of 2048 bits and cyclic subgroup parameter length of 224 bits
2. Elliptic Curve Diffie-Hellman (ECDH) with a key length of 224 bits
3. Elliptic Curve Integrated Encryption System – Key Encapsulation Mechanism (ECIES-KEM) with a key length of 224 bits
4. Provably Secure Elliptic Curve – Key Encapsulation Mechanism (PSEC-KEM) with a key length of 224 bits
5. Advanced Cryptographic Engine – Key Encapsulation Mechanism (ACE-KEM) with an approved hash function and a key length of 224 bits
6. Rivest-Shamir-Adleman – Optimal Asymmetric Encryption Padding (RSA-OAEP) with a key length of 2048 bits
7. Rivest-Shamir-Adleman – Key Encapsulation Mechanism (RSA-KEM) with a key length of 2048 bits

Quantum vulnerability:

All legacy key agreement and key encryption algorithms are quantum-vulnerable.

(5) Quantum-Resistant Public-Key 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 appendix "Kvantová hrozba a kvantově odolná kryptografie" (Quantum Threat and Quantum-Resistant Cryptography), only available in Czech.

a) Hybrid quantum-resistant cryptography for key establishment

It combines an approved classical key establishment algorithm (paragraph (4)c) with one of the following post-quantum KEM/Encryption algorithms:

Kyber-1024, Kyber-k768, FrodoKEM-1344, FrodoKEM-976, mceliece8192128, mceliece6688128, mceliece460896, mceliece8192128f, mceliece6688128f, mceliece460896f.

These hybrid combinations of classical and post-quantum cryptography can be considered approved.

b) Stand-alone post-quantum key establishment algorithm

CRYSTALS-Kyber Level 5, implemented according to the NIST standard.

Since the NIST standard will not be published until 2024, this solution has not yet been approved. This will only happen for implementations following the NIST standard.

Note: Kyber-1024 is another name for CRYSTALS-Kyber Level 5.

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

1. LMS
2. XMSS

Separate use of these algorithms to protect firmware and software integrity can be considered approved.

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

CRYSTALS-Dilithium Level 5, implemented according to the NIST standard.

Since the NIST standard will not be published until 2024, this solution has not yet been approved. This will only happen for implementations following the NIST standard.

Note: CRYSTALS-Dilithium Level 5 is also called Dilithium 5.

e) Hybrid quantum-resistant cryptography for digital signatures

It combines an approved classical digital signature algorithm (paragraph (4)a) with one of the following post-quantum digital signature algorithms: Dilithium, SPHINCS+, Falcon. Their specific variants will be recommended following the next course of their standardization.

(6) Hash Function Algorithms

a) Approved SHA-2 hash functions

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

b) Approved SHA-3 hash functions

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

c) Other approved hash functions

1. Whirlpool
2. BLAKE2

Recommendation:
For approved hash functions, we recommend an output length of 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.

d) Legacy hash functions

1. SHA-2 with an output length of 224 bits (SHA-224, SHA-512/224)
2. SHA3-224
3. RIPEMD-160

Quantum vulnerability:
All legacy hash functions are quantum-vulnerable.

(7) Algorithms for Secure Password Storage

a) Approved algorithms

1. Argon2 with selected function Argon2id and parameters at least
   i) t=1, m=2^{21} (2 GiB of RAM)
   ii) t=3, m=2^{16} (64 MiB of RAM) for memory-constrained environments
2. Scrypt with parameters at least N=32768 (2^{15}), r=8, and p=1
3. PBKDF2 with at least 100,000 iterations and an approved SHA-2 hash function

Notes:

- A salt randomly generated for each password must be used.
- 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).

Recommendation:

- 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.

Document version

Date	Version	Changed (name)	Change
Nov. 1, 2023	1.0	ICT Security Department	English translation of the original Czech document