NÚKIB

MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY

doporučení v oblasti kryptografických prostředků

Verze 1.0, platná ke dni 28.11.2018

Obsah

Úvod

Podle § 26 písm. d) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“) mají povinné osoby podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti“) povinnost zohlednit doporučení v oblasti kryptografických prostředků vydaná Národním úřadem pro kybernetickou a informační bezpečnost za účelem ochrany aktiv informačního a komunikačního systému. Tento dokument obsahuje zmíněná doporučení.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 777

E-mail: nckb@nukib.cz

Upozornění:

Tento dokument obsahuje doporučení Národního úřadu pro kybernetickou a informační bezpečnost v oblasti kryptografických prostředků. Povinné osoby podle zákona o kybernetické bezpečnosti jsou na základě § 26 písm. d) vyhlášky o kybernetické bezpečnosti povinny tato doporučení zohlednit za účelem ochrany aktiv informačního a komunikačního systému.

Dokument může být měněn na základě aktuálních poznatků z oblasti kryptografických prostředků.

1 Doporučení v oblasti kryptografických prostředků

Kategorie kryptografických algoritmů podle omezení doby své použitelnosti
Níže uvádíme dvě kategorie kryptografických algoritmů, které nazýváme „schválené“ a „dosluhující“.

Schválené kryptografické algoritmy (*Approved, Recommended, Future*) jsou algoritmy, u kterých jsme přesvědčeni, že jsou bezpečné alespoň ve střednědobém horizontu.

Dosluhující kryptografické algoritmy (*Legacy*) jsou algoritmy, u kterých doporučujeme přestat s jejich používáním do r. 2023. A dále doporučujeme nově zavádět pouze takové kryptografické systémy, které obsahují pouze schválené kryptografické algoritmy (a neobsahují dosluhující).

(1) Symetrické algoritmy

a) Schválené blokové a proudové šifry

1. Advanced Encryption Standard (AES) s využitím délky klíčů 128, 192 a 256 bitů
2. Twofish s využitím délky klíčů 128 až 256 bitů
3. Serpent s využitím délky klíčů 128, 192, 256 bitů
4. Camellia s využitím délky klíčů 128, 192 a 256 bitů
5. SNOW 2.0, SNOW 3G s využitím délky klíčů 128, 256 bitů
6. ChaCha20 s délkou klíče 256 bitů a se zatížením klíče menším než 256 GB

Doporučujeme preferovat:

- Použití blokových šifer před proudovými.
- V případě blokových šifer: AES, Camellia a Serpent (v uvedeném pořadí).
- Délku klíče 256 bitů.

b) Dosluhující blokové a proudové šifry

1. Triple Data Encryption Standard (3DES) s využitím délky klíčů 112 bitů, omezené použití jen se zatížením klíče menším než 10 MB, postupně přecházet na AES. Doporučeno použití jedinečného klíče pro každou zprávu
2. Blowfish s využitím minimální délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB
3. Kasumi s využitím délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB

c) Schválené módy šifrování s ochranou integrity

1. CCM
2. EAX
3. OCB1 a OCB3, doporučujeme preferovat OCB3 před OCB1
4. GCM s noncí dlouhou 96 bitů a s tagem dlouhým 128 bitů, nejpozději po 2^{32} hodnotách nonce musí dojít k výměně klíče
5. ChaCha20 + Poly1305 se zatížením klíče menším než 256 GB
6. Složená schémata typu „Encrypt-then-MAC“

Poznámky:

- Schválené módy šifrování musí používat schválené blokové šifry.
- Schémata typu „Encrypt-then-MAC“ musí používat k šifrování pouze šifrovací módy uvedené v odstavci d) a k výpočtu MAC pouze schválené módy pro ochranu integrity.
- Inicializační vektor (nebo nonce) musí být součástí vstupu pro výpočet MAC.

d) Módy šifrování (jejich samostatné použití je dosluhující, ale schválené je jejich použití ve složených schématech typu „Encrypt-then-MAC)

1. CTR
2. OFB
3. CBC
4. CFB

Poznámky:

- Pro použití v rámci schváleného složeného schématu typu Encrypt-then-MAC musí tyto módy používat pouze schválené blokové šifry.
- Módy CBC a CFB musí být použity s náhodným, pro útočníka nepředpověditelným, inicializačním vektorem.
- Při použití módu OFB se pro daný klíč nesmí opakovat hodnota inicializačního vektoru.
- Při použití módu CTR se pro daný klíč nesmí opakovat hodnota čítače.
- V případě použití CBC módu k šifrování bez ochrany integrity je třeba ověřit odolnost proti útoku na padding CBC módu.

e) Schválené módy pro šifrování disků

1. XTS – délka jednotky dat (sektoru) nesmí přesáhnout 2^{20} bloků šifry (v případě šifry se 128-bitovým blokem je to zhruba 16 MB)
2. EME

f) Schválené módy pro ochranu integrity

1. HMAC se schválenou hašovací funkcí
2. EMAC
3. CMAC
4. UMAC s délkou tag 64 bitů

g) Dosluhující módy pro ochranu integrity

1. HMAC-SHA1
2. CBC-MAC-X9.19, omezené použití jen se zatížením menším než 10^9 MAC

(2) Asymetrické algoritmy

a) Schválené algoritmy pro technologii digitálního podpisu

1. Digital Signature Algorithm (DSA) s využitím délky klíčů 3072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více
2. Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 256 bitů a více

3. Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 3072 bitů a více
4. Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s využitím délky klíče 256 bitů a více

b) Dosluhující algoritmy pro technologii digitálního podpisu

1. Digital Signature Algorithm (DSA) s využitím délky klíčů 2048 bitů, délky parametru cyklické podgrupy 224 bitů
2. Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 224 bitů
3. Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 2048 bitů
4. Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s využitím délky klíče 224 bitů

c) Schválené algoritmy pro procesy dohod na klíči a šifrování klíčů

1. Diffie-Hellman (DH) s využitím délky klíčů 3072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více
2. Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 256 bitů a více
3. Elliptic Curve Integrated Encryption System – Key Encapculation Mechanism (ECIES-KEM) s využitím délky klíčů 256 bitů a více
4. Provably Secure Elliptic Curve – Key Encapculation Mechanism (PSEC-KEM) s využitím délky klíčů 256 bitů více
5. Asymetric Ciphers and Key Encapculation Mechanism (ACE-KEM) s využitím délky klíčů 256 bitů a více
6. Rivest Shamir Adleman – Optimal Asymetric Encryption Padding (RSA-OAEP) s využitím délky klíčů 3072 a více
7. Rivest Shamir Adleman – Key Encapsulation Mechanism (RSA-KEM) s využitím délky klíčů 3072 a více

Doporučení:
U kryptografie na bázi eliptických křivek doporučujeme preferovat délku klíčů 384 bitů.

d) Dosluhující algoritmy pro procesy dohod na klíči a šifrování klíčů

1. Diffie-Hellman (DH) s využitím délky klíčů 2048 bitů, délky parametru cyklické podgrupy 224 bitů
2. Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 224 bitů
3. Elliptic Curve Integrated Encryption System - Key Encapculation Mechanism (ECIES-KEM) s využitím délky klíčů 224 bitů
4. Provably Secure Elliptic Curve - Key Encapculation Mechanism (PSEC-KEM) s využitím délky klíčů 224 bitů
5. Asymetric Ciphers and Key Encapculation Mechanism (ACE-KEM) s využitím délky klíčů 224 bitů
6. Rivest Shamir Adleman - Optimal Asymetric Encryption Padding (RSA-OAEP) s využitím délky klíčů 2048 bitů
7. Rivest Shamir Adleman - Key Encapsulation Mechanism (RSA-KEM) s využitím délky klíčů 2048 bitů

(3) Algoritmy hašovacích funkcí

a) Schválené hašovací funkce SHA-2

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

b) Schválené hašovací funkce SHA3

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

c) Ostatní schválené hašovací funkce

1. Whirlpool
2. BLAKE2

Doporučení:
U schválených hašovacích funkcí doporučujeme preferovat délku výstupu 384 bitů.

d) Dosluhující hašovací funkce

1. SHA2 s délkou výstupu 224 bitů (SHA-224, SHA-512/224)
2. SHA3-224
3. RIPEMD-160

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
26.11.2018	1.0	Odbor bezpečnosti informačních a komunikačních technologií	Vytvoření dokumentu