Verze 2.0.1-min, účinnost od 1. 11. 2026

Mapování výsledku skenu na povinnost ke kryptografii

Verze dokumentu 2.0.1-min. Odkazy na předpisy odpovídají stavu ke dni 6. října 2026.

Dokument vysvětluje, k čemu slouží export jednoho skenu a co z něj neplyne. Není to právní posudek, audit ani osvědčení. pqc-ruqa nevydává osvědčení ani certifikát souladu se směrnicí NIS2, se zákonem o kybernetické bezpečnosti ani s doporučeními NÚKIB.

1. K čemu výstup je

Export popisuje, co jeden veřejný TLS nebo SSH server nabídl klientovi skeneru při navázání spojení. Popis platí pro okamžik skenu. Řadí se k bezpečnostnímu opatření „kryptografické algoritmy“.

Export ve formátu PDF nebo JSON lze stáhnout jen u skenu spuštěného s účtem. Anonymní sken se neukládá a export k němu není.

Organizace může export přiložit k evidenci aktiva, k hodnocení rizik nebo k plánu přechodu na post-kvantovou kryptografii.

Export neříká, že organizace plní zákon o kybernetické bezpečnosti, směrnici NIS2 ani jiný předpis. Neříká, že host je bezpečný. Neříká, že použité algoritmy odpovídají doporučení NÚKIB.

Slovní označení skóre, například „Skóre 80 a více“ nebo „Jen klasická dohoda klíče“, popisuje jen kategorii nabídnuté dohody klíče. Není to hodnocení bezpečnosti hosta ani organizace.

The wording of a score, for example “Score 80 or above” or “Classical key exchange only”, describes only the category of the offered key exchange. It is not an assessment of the security of the host or the organisation.

2. Na které předpisy se popis váže

Směrnice NIS2. Směrnice Evropského parlamentu a Rady (EU) 2022/2555, čl. 21 odst. 2 písm. h). Opatření k řízení kybernetických bezpečnostních rizik zahrnují alespoň „politiky a postupy týkající se používání kryptografie a případně šifrování“.

Zákon č. 264/2025 Sb., o kybernetické bezpečnosti. Účinný od 1. listopadu 2025.

– § 12: poskytovatel regulované služby vymezí rozsah řízení kybernetické bezpečnosti (zákon ho nazývá „stanovený rozsah“). Patří do něj aktiva související s poskytováním regulované služby.

– § 13 odst. 2: v rámci stanoveného rozsahu zavádí a provádí bezpečnostní opatření podle § 14 v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.

– § 13 odst. 3: obsah opatření a způsob jejich zavádění a provádění stanoví Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vyhláškou.

– § 14 odst. 1 písm. b) bod 9: technické opatření „kryptografické algoritmy“ pro poskytovatele v režimu vyšších povinností.

– § 14 odst. 2 písm. m): opatření „kryptografické algoritmy“ pro poskytovatele v režimu nižších povinností.

Vyhlášky NÚKIB. Obě jsou účinné od 1. listopadu 2025.

– Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, § 25. Povinná osoba používá pouze aktuálně odolné kryptografické algoritmy a zohledňuje doporučení a metodiky NÚKIB. U kryptografických klíčů a certifikátů používá pouze aktuálně odolné klíče a certifikáty.

– Vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, § 13. Povinná osoba používá aktuálně odolné kryptografické algoritmy a zohledňuje doporučení a metodiky NÚKIB.

Doporučení NÚKIB. „Minimální požadavky na kryptografické algoritmy“, verze 4.0, platná ke dni 5. 2. 2025. K

němu příloha „Kvantová hrozba a kvantově odolná kryptografie“, verze 2.0. Dokument stále odkazuje na dřívější vyhlášku č. 82/2018 Sb.

Služby podle § 18 zákona. Jde o systém překladu doménových jmen (DNS), služby vytvářející důvěru, správu a provoz registru domény nejvyšší úrovně, cloud computing, datové centrum, síť pro doručování obsahu (CDN), on-line tržiště, internetový vyhledávač, platformu sociální sítě, řízenou službu a řízenou bezpečnostní službu. U těchto služeb se opatření, včetně kryptografických algoritmů, zavádějí v míře a způsobem podle prováděcího předpisu Evropské komise. § 13 odst. 2 se na ně nepoužije. Tím předpisem je prováděcí nařízení Komise (EU) 2024/2690. Kryptografii upravuje bod 9 jeho přílohy. Poskytovatel v režimu vyšších povinností se řídí ustanoveními pro základní subjekty, poskytovatel v režimu nižších povinností ustanoveními pro důležité subjekty (§ 18 odst. 4).

Výstup se týká jen opatření „kryptografické algoritmy“ a jen jednoho veřejného rozhraní. Ostatní opatření podle § 14 sken neobsahuje. Jde například o řízení rizik, řízení dodavatelů, řízení kontinuity činností, řízení přístupu nebo detekci kybernetických bezpečnostních událostí. Nepokrývá ani jiné povinnosti, například hlášení kybernetických bezpečnostních incidentů podle § 15 a § 16.

3. Co se v exportu dokládá

Údaj v exportu — Co k povinnosti dokládá

Host, port, protokol (TLS nebo SSH) a čas skenu; IP adresa cíle, pokud ji skener vrátil — Které rozhraní a v jakém okamžiku bylo měřeno. Časy v PDF jsou uvedeny v pásmu Europe/Prague a jsou tak označeny.

Nabídnutá dohoda klíče, její třída a skóre — Jestli server klientovi skeneru nabídl hybridní dohodu klíče (například X25519MLKEM768), samostatnou post-kvantovou dohodu, jen klasickou dohodu, nebo mechanismus se známou slabinou. Skóre hodnotí jen dohodu klíče. Je to vlastní metodika pqc-ruqa, ne hodnocení NÚKIB. PDF dlouhé seznamy algoritmů zkracuje, úplná naměřená data obsahuje export JSON.

Podpis certifikátu: neměřeno — Sken podpis listového certifikátu zatím neměří. Údaj je v exportu uveden, aby chybějící měření nebylo zaměněno za kladný výsledek.

Vymezení skóre — Odstavec o tom, co skóre hodnotí a co ne.

Chyba spojení, pokud nastala — Že se skener k cíli nepřipojil a výsledek proto nic nevypovídá o nabízené kryptografii.

Prohlášení před skenem — Že osoba, která sken spustila, před spuštěním potvrdila prohlášení o zákonném použití a neinvazivní povaze testu. Export uvádí čas potvrzení, účet a verzi znění prohlášení. U starších skenů export uvede dřívější znění „Mám oprávnění testovat tento server“, nebo že potvrzení nebylo zaznamenáno.

Označení tohoto dokumentu — Slug nis2-mapping, verze dokumentu a hash jeho textu. Podle toho lze zjistit, ke kterému znění mapování se export vztahuje. Hash se týká textu tohoto dokumentu, ne naměřených údajů. Neslouží k ověření, že se výsledek skenu nezměnil.

Současné znění prohlášení před skenem: „Prohlašuji, že tento technický test spouštím v souladu s právem a že výsledky nezneužiji. Rozumím, že jde o neinvazivní kontrolu veřejně nabízené TLS/SSH konfigurace (klientské spojení, bez přihlášení a bez pokusů o průnik).“

Prohlášení je jednostranné potvrzení osoby, která sken spustila. To platí i pro dřívější znění. pqc-ruqa pravdivost prohlášení neověřuje. Prohlášení nedokládá, že tato osoba je provozovatelem hosta ani že od něj má souhlas.

4. Jak export použít v dokumentaci

Organizace sama určí, jestli host patří do stanoveného rozsahu podle § 12 a v jakém režimu povinností je. Když host do rozsahu patří, může export použít jako záznam o stavu kryptografie tohoto aktiva ke dni skenu. Například:

– u aktiva uvést datum skenu, host, port, třídu dohody klíče a skóre,

– výsledek samostatně porovnat s doporučením NÚKIB. Verze 4.0 schvaluje hybridní kombinaci ML-KEM-768

nebo ML-KEM-1024 se schváleným klasickým algoritmem. Samostatný ML-KEM schvaluje jen ve variantě ML-KEM-1024. Skóre pqc-ruqa tento rozdíl nezohledňuje. Vysoké skóre proto samo neznamená, že algoritmus je na seznamu NÚKIB,

– při klasické dohodě klíče zapsat riziko, že provoz lze dnes zachytit a později dešifrovat (harvest now, decrypt later), a plán přechodu. Příloha NÚKIB odhaduje pro ochranu informací kritické úrovně důvěrnosti dokončení přechodu ke kvantově odolnému ustanovení klíčů do konce roku 2030. Je to odhad v doporučení, ne lhůta ze zákona,

– podpis a platnost certifikátu posoudit samostatně, protože je export nedokládá,

– u služeb podle § 18 porovnat výsledek s bodem 9 přílohy prováděcího nařízení (EU) 2024/2690 (politika a postupy pro kryptografii, schválené protokoly a algoritmy, správa klíčů, pravidelný přezkum),

– export si uložit ve vlastní evidenci. Každý sken zakládá nový záznam. Uživatel ale může své záznamy v pqc-ruqa smazat. Po zrušení účtu se záznamy mažou podle zásad ochrany osobních údajů. pqc-ruqa proto neslouží jako archiv evidence,

– při dalším skenu porovnat uložené exporty a ponechat oba.

Za zařazení aktiva, výběr opatření a plnění povinností odpovídá poskytovatel regulované služby.

5. Co výstup neprokazuje

– Soulad organizace se zákonem č. 264/2025 Sb., s vyhláškami NÚKIB ani se směrnicí (EU) 2022/2555.

– Že organizace postupuje podle doporučení NÚKIB nebo podle prováděcího nařízení (EU) 2024/2690.

– Že jsou zavedena ostatní bezpečnostní opatření podle § 14.

– Že osoba, která sken spustila, měla od provozovatele hosta souhlas, ani kdo tato osoba je.

– Že se naměřené údaje v exportu od skenu nezměnily. Export zatím nenese otisk výsledku skenu.

– Verzi skeneru ani verzi metodiky skóre, se kterou sken proběhl.

– Podpis listového certifikátu, řetěz certifikátů, důvěryhodnost certifikační autority ani platnost certifikátu.

– Co server nabídne jinému klientovi, z jiné sítě nebo v jiném čase.

– Stav vnitřní sítě, jiných portů, jiných hostů nebo konfigurace po době skenu.

– Validaci kryptografického modulu podle FIPS ani jinou certifikaci produktu.

– Že je algoritmus vhodný pro danou regulovanou službu. To plyne ze stanoveného rozsahu, z hodnocení rizik, z vyhlášky NÚKIB nebo z prováděcího nařízení Komise, ne ze skóre.

6. Výklad jazykového modelu

Export přihlášeného skenu může obsahovat český výklad. Sestavil ho jazykový model z naměřených údajů. Před vložením do exportu ho nikdo nekontroluje.

Výklad může obsahovat chyby, i v odkazech na předpisy. Není právní ani odborný posudek. Nemění naměřené údaje ani tento dokument. Když si výklad a naměřené údaje odporují, platí naměřené údaje.

V PDF je výklad v samostatné sekci s upozorněním, že ho sestavil jazykový model. Export JSON ho označuje příznakem ai_generated. Naměřené algoritmy a skóre pocházejí ze skeneru.

7. Platnost odkazů

Předpisy a doporučení NÚKIB se mohou změnit. Odkazy v tomto dokumentu odpovídají stavu uvedenému v záhlaví. Organizace si před použitím exportu ověří aktuální znění.