RSA 2048, SHA1 a další kryptografické algoritmy letos dosloužíí. Jste připraveni?

portal.neweb.govcert.cz/informacni-servis/aktuality/rsa-2048-a-dalsi-kryptograficke-algoritmy-letos-doslouzi-jste-pripraveni

TLP:GREEN Autor: Národní úřad pro kybernetickou a informační bezpečnost, 13. 02. 2023

Kryptografické algoritmy jsou důležité pro zajištění důvěrnosti a integrity přenášených a ukládaných dat. NÚKIB proto udržuje dokument MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY, který specifikuje, které prostředky považuje za odolné a doporučuje je používat v regulovaných systémech dle zákona o kybernetické bezpečnosti. Poslední verze 2.0, vydaná dne 8. 6. 2022, rozděluje tyto prostředky na dvě kategorie: schválené a dosluhující.

A právě prostředky z kategorie dosluhující NÚKIB doporučuje přestat využít do konce roku 2023. Mezi nejpoužívanější algoritmy z této kategorie patří:

- Symetrický algoritmus 3DES
- Mód pro ochranu integrity HMAC-SHA1
- Asymetrické algoritmy pro technologii digitálního podpisu DSA 2048 bitů, RSA-PSS 2048 bitů a EC-DSA s využitím délky klíčů 224 bitů
- Asymetrické algoritmy pro procesy dohod nad klíči a šifrování klíčů RSA 2048 bitů a DH 2048 bitů
- Hašovací funkce s délkou výstupu 224 bitů (SHA-224, SHA-512/224, SHA3-224)

Kompletní seznam prostředků, které douslouží v letošním roce, naleznete v odkazovaném dokumentu.

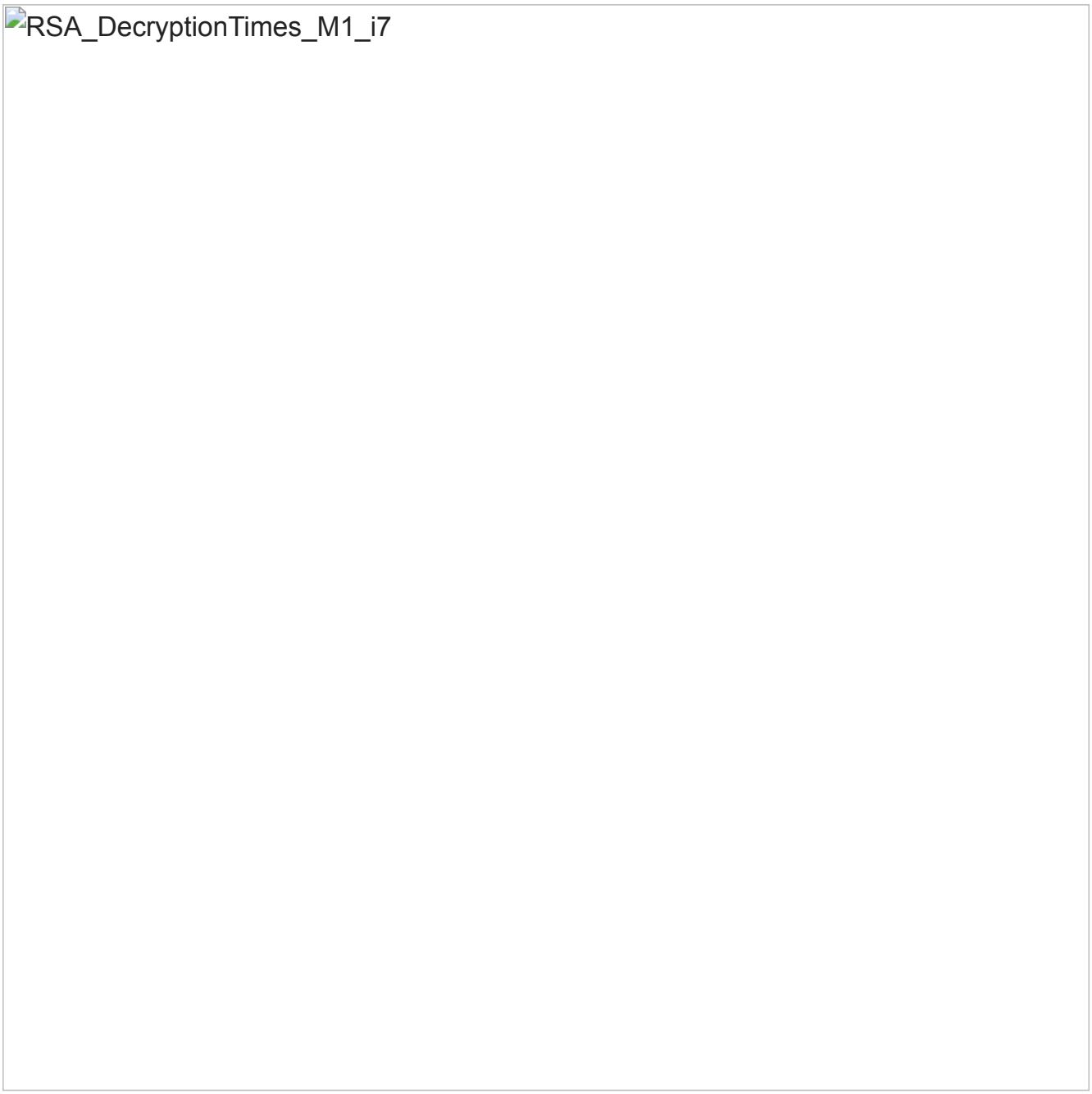
S tímto dokumentem se přímo pracuje ve třech vyhláškách:

- Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti v § 26 Kryptografické prostředky v bodě d) uvádí „Povinná osoba pro ochranu aktiv informačního a komunikačního systému zohledňuje doporučení v oblasti kryptografických prostředků vydaná Úřadem, zveřejněná na jeho internetových stránkách.”
- Ochranné opatření k zabezpečení e-mailové komunikace ze dne 11. 10. 2021 v bodech 1.2.4, 1.8, 2.1 a 3.2 vyžaduje využití pouze odolných kryptografických prostředků dle doporučení NÚKIB.
- Vyhláška č. 316/2021 Sb. o některých požadavcích pro zápis do katalogu cloud computingu v bodě 7.3 vyžaduje, aby: „Poskytovatel umožňuje ochranu zákaznického obsahu šifrováním při přenosu a v úložištích ve službě cloud computingu pomocí některého z algoritmů uvedených v doporučení v oblasti kryptografických prostředků vydaného Národním úřadem pro kybernetickou a informační bezpečnost, které je zveřejněno na jeho internetových stránkách.”

Ze skenování zabezpečení aplikací přístupných z Internetu prováděných NÚKIB vyplývá, že organizace v TLS spojeních z dosluhujících algoritmů nejčastěji využívají v certifikátech RSA o velikosti klíče 2048 bitů, DH o velikosti 2048 bitů a menší a symetrický mód pro ochranu integrity HMAC-SHA1. V případě PKI se jedná i o certifikáty v řetězci certifikátu až ke kořenovému certifikátu.

V případě, že vámi používaná certifikační autorita nepodporuje certifikáty o velikosti RSA 3072 bitů nebo vyšší nebo certifikáty založené na eleptických křivkách (EC), doporučujeme vyměnit certifikační autoritu. V případě využití eleptických křivek doporučujeme preferovat delků klíčů 384 bitů.

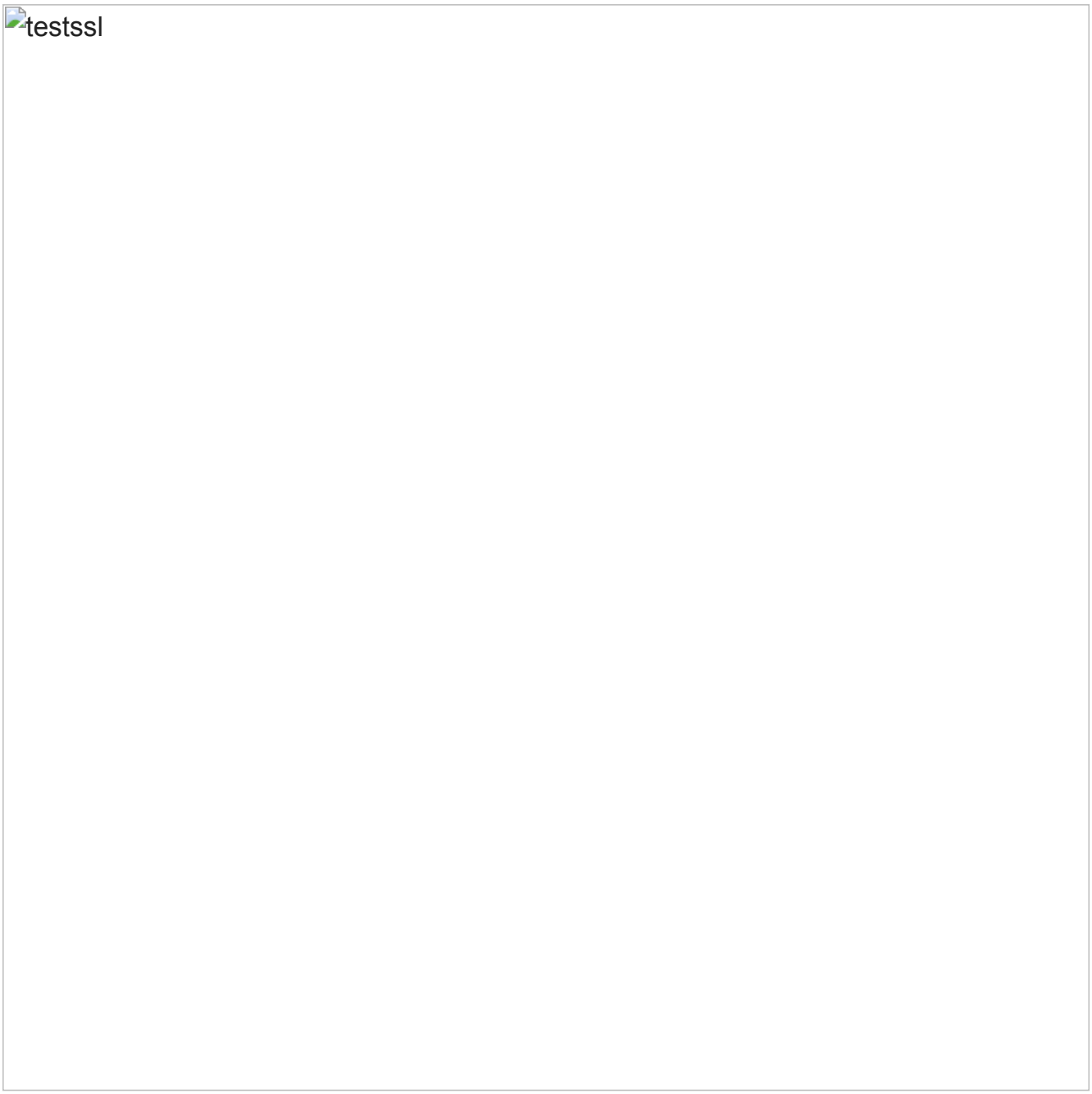
Pokud je to možné, doporučujeme v průběhu tohoto roku se zaměřit na tuto problematiku, upravit Politiku bezpečného používání kryptografické ochrany organizace dle aktuálního doporučení a tam, kde je to možné, provést výměnu kryptografických algoritmů nebo vypnutí dosluhujících algoritmů. Primárně v systémech a použitích, kdy jsou zašifrovaná data předávána pomocí sítě Internet nebo je povaha dat dat taková, že jejich zneužití by bylo problematické i po několika letech. Zároveň doporučujeme změny před nasazením do ostrého provozu předem otestovat, tak aby nebyla narušena dostupnost služeb - některé starší operační systémy či aplikace nemusí moderní kryptografické prostředky podporovat či může být výrazně snížen výkon při využití delších RSA klíčů či prostředku, který není podporován v hardwaru použitého zařízení.



Ukázka vlivu velikosti RSA klíče na výpočetní náročnost (zdroj)

- Pro ověření nabízených algoritmů ze strany serveru při navazování TLS komunikace je možné využít např. nástroje SSL Labs pro webové služby přístupné z Internetu, případně nástroj testssl.sh pro otestování e-mailových serverů nebo serverů nepřístupných z Internetu.
- Pro ověření kryptografických algoritmů v rámci SSH spojení je možné využít nmap: `nmap -p22 --script ssh2-enum-algos target`

Ukázka z výstupu nástroje testssl.sh



Ukázka výstupu nástroje testssl.sh při testování nevhodně nakonfigurovaného e-mailové serveru. Červeně jsou označeny kryptografické algoritmy, které nejsou schválené už od roku 2018. RC4, SEED, IDEA nebo DH o velikosti 1024 bitů nebyly schváleny ani v původní vyhlášce o kybernetické bezpečnosti z roku 2015. Oranžově jsou označeny ty prostředky, které jsou schválené pouze do konce roku 2023.

Obsah

2