EVROPSKÁ
KOMISE

V Bruselu dne 29.9.2025
C(2025) 6484 final

ANNEX

PŘÍLOHA

PROVÁDĚCÍHO NAŘÍZENÍ KOMISE .../...,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o spojení data a času s příslušnými daty a stanovení přesnosti zdrojů času pro poskytování kvalifikovaných elektronických časových razítek

PŘÍLOHA

Seznam referenčních norem a specifikací pro kvalifikované služby časových razítek

Normy ETSI EN 319 421 V1.3.1[1] (dále jen „ETSI EN 319 421“) a ETSI EN 319 422 V1.1.1[2] (dále jen „ETSI EN 319 422“) se použijí s těmito úpravami:

1. Pro normu ETSI EN 319 421

   1) 2.1 Normativní odkazy:

      – [3] ISO/IEC 15408:2022 (části 1 až 5) „Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Kritéria hodnocení bezpečnosti IT“.

      – [4] ETSI EN 319 401 V3.1.1 (2024-06) „Elektronické podpisy a infrastruktury (ESI); Obecné politické požadavky na poskytovatele služeb vytvářejících důvěru“.

      – [5] ETSI EN 319 422 V1.1.1 (2016-03) „Elektronické podpisy a infrastruktury (ESI); Protokol časového razítka a profily tokenu časového razítka“.

      – [6] neplatné.

      – [9] Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování: „Dohodnuté kryptografické mechanismy“ zveřejněné Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA)[3].

      – [10] Prováděcí nařízení Komise (EU) 2024/482[4] ze dne 31. ledna 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC).

      – [11] Prováděcí nařízení Komise (EU) 2024/3144[5] ze dne 18. prosince 2024, kterým se mění prováděcí nařízení (EU) 2024/482, pokud jde o použitelné mezinárodní normy, a kterým se uvedené prováděcí nařízení opravuje.

   2) 3.1 Podmínky

      – doba platnosti certifikátů: časový interval od „notBefore“ do „notAfter“ včetně, během kterého certifikační orgán zaručuje, že bude uchovávat informace o statusu certifikátu.

   3) 3.3 Zkratky

---

1 EN 319 421 – Elektronické podpisy a infrastruktury (ESI) – Politické a bezpečnostní požadavky na poskytovatele služeb vytvářejících důvěru vydávajících časová razítka, V1.3.1.

2 EN 319 422 – Elektronické podpisy a infrastruktury (ESI) – Protokol pro vyznačení času a profily tokenu časového razítka, V1.1.1 (2016-03).https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf

3 https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

4 Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.

5 Úř. věst. L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

– EUCC Evropský systém certifikace kybernetické bezpečnosti založený na společných kritériích.

4) 6.2 Prohlášení o postupech služeb vytvářejících důvěru

– OVR-6.2-03 Autorita vydávající časová razítka (TSA) zahrne prohlášení o dostupnosti své služby časových razítek do svého prohlášení o zpřístupnění informací TSA.

5) 7.3 Bezpečnostní opatření týkající se personálu

– OVR-7.3-02 Pracovníci autority vydávající časová razítka (TSA) na důvěryhodných pozicích a v příslušných případech jeho subdodavatelé na důvěryhodných pozicích musí být schopni splnit požadavek na „odborné znalosti, zkušenosti a kvalifikaci“ prostřednictvím formální odborné přípravy a pověření nebo skutečných zkušeností nebo kombinace obojího.

– OVR-7.3-03 Soulad s OVR-7.3-02 musí zahrnovat pravidelné aktuální informace (alespoň každých dvanáct měsíců) o nových hrozbách a stávajících bezpečnostních postupech.

6) 7.6.2 Generování klíče jednotky pro časová razítka (TSU)

– TIS-7.6.2-03 Generování klíče (klíčů) TSU se provádí v rámci bezpečného kryptografického prostředku, který je důvěryhodným systémem certifikovaným v souladu s/se:

a) společnými kritérii pro hodnocení bezpečnosti informačních technologií stanovenými v normě ISO/IEC 15408 [3] nebo ve společných kritériích pro hodnocení bezpečnosti informačních technologií, verzi CC:2022, části 1 až 5, zveřejněných účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT a certifikovaných na úrovni EAL 4 nebo vyšší, nebo

b) systémem EUCC [10][11] a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [7] úrovně 3.

Tato certifikace musí odpovídat bezpečnostnímu cíli nebo profilu ochrany nebo dokumentaci návrhu modulu a jeho bezpečnosti, která splňuje požadavky tohoto dokumentu na základě analýzy rizik a s přihlédnutím k fyzickým a jiným netechnickým bezpečnostním opatřením.

Pokud je bezpečný kryptografický prostředek certifikován podle EUCC [10][11], musí být tento prostředek nakonfigurován a používán v souladu s touto certifikací.

– TIS-7.6.2-04 neplatné.

– POZNÁMKA 3 neplatné.

– TIS-7.6.2-05A Algoritmus generování klíče TSU, výsledná délka podpisového klíče a podpisový algoritmus používané pro podepisování časových razítek a pro podepisování certifikátů veřejného klíče TSU musí být v souladu s dohodnutými kryptografickými mechanismy

přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti [9] a zveřejněnými agenturou ENISA.

– POZNÁMKA 4 neplatné.

– TIS-7.6.2-06 A Podpisový klíč TSU lze exportovat a importovat do jiného bezpečného kryptografického prostředku pouze tehdy, pokud je tento export a import prováděn bezpečně a v souladu s certifikací tohoto prostředku.

7) 7.6.3 Ochrana soukromého klíče TSU

– TIS-7.6.3-02 Soukromý podpisový klíč TSU musí být uchováván a používán v rámci bezpečného kryptografického prostředku, který je důvěryhodným systémem certifikovaným v souladu se:

a) společnými kritérii pro hodnocení bezpečnosti informačních technologií stanovenými v normě ISO/IEC 15408 [3] nebo ve společných kritériích pro hodnocení bezpečnosti informačních technologií, verzi CC:2002, části 1 až 5, zveřejněných účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT a certifikovaných na úrovni EAL 4 nebo vyšší, nebo

b) evropským systémem certifikace kybernetické bezpečnosti založeným na společných kritériích (EUCC) [10][11] a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [7] úrovně 3.

Tato certifikace musí odpovídat bezpečnostnímu cíli nebo profilu ochrany nebo dokumentaci návrhu modulu a jeho bezpečnosti, která splňuje požadavky tohoto dokumentu na základě analýzy rizik a s přihlédnutím k fyzickým a jiným netechnickým bezpečnostním opatřením.

Pokud je bezpečný kryptografický prostředek certifikován podle EUCC [10][11], musí být tento prostředek nakonfigurován a používán v souladu s touto certifikací.

– TIS-7.6.3-03 neplatné.

– POZNÁMKA 2 neplatné.

8) 7.6.7 Konec životního cyklu klíče TSU

– TIS-7.6.7-03A Datum vypršení platnosti soukromých klíčů TSU musí být v souladu s dohodnutými kryptografickými mechanismy [9].

– POZNÁMKA 1 neplatné.

9) 7.10 Bezpečnost sítí

– OVR-7.10-05 Skenování zranitelnosti požadované v rámci požadavku REQ-7.8-13 normy ETSI EN 319 401 [1] se provádí nejméně jednou za čtvrtletí.

– OVR-7.10-06 Penetrační test požadovaný v rámci požadavku REQ-7.8-17X normy ETSI EN 319 401 [1] se provádí nejméně jednou ročně.

– OVR-7.10-07 Firewally musí být nakonfigurovány tak, aby zabránily veškerým protokolům a přístupům, které nejsou nezbytné pro provoz TSA.

10) 7.14 Ukončení činnosti autority vydávající časová razítka (TSA) a plány ukončení činnosti autority vydávající časová razítka (TSA)

– OVR-7.14-01A Plán ukončení činnosti poskytovatele služeb vytvářejících důvěru musí splňovat požadavky stanovené v prováděcích aktech přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014 [i.4].

2. Pro normu ETSI EN 319 422

1) 2.1 Normativní odkazy

– [5] neplatné.

– [6] neplatné.

– [8] Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování: „Dohodnuté kryptografické mechanismy“.

– [9] RFC 9110 Sémantika protokolu HTTP.

2) 4.1.3 Hašovací algoritmy, které mají být použity

– Použije se toto ustanovení:

Hašovací algoritmy používané k hašování informací, které mají být opatřeny časovým razítkem, očekávaná doba trvání časového razítka a zvolených hašovacích funkcí v závislosti na čase musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

– POZNÁMKA neplatné.

3) 4.2.3 Podporované algoritmy

– Použije se toto ustanovení:

Podporované algoritmy podpisu pomocí tokenu časového razítka musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

– POZNÁMKA neplatné.

4) 4.2.4 Podporované délky klíčů

– Použije se toto ustanovení:

Délky klíčů algoritmu podpisu pro zvolený algoritmus podpisu musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA.

– POZNÁMKA neplatné.

5) 5.1.3 Podporované algoritmy

– Použije se toto ustanovení:

Hašovací algoritmy pro data časových razítek, které mají být podporovány, očekávaná doba trvání časového razítka a zvolené hašovací funkce v závislosti na čase musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

– POZNÁMKA neplatné.

6) 5.2.3 Algoritmy, které mají být použity

– Použije se toto ustanovení:

Hašovací algoritmy používané k hašování informací, které mají být opatřeny časovým razítkem, a algoritmy podpisu pomocí tokenu časového razítka musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

– POZNÁMKA neplatné.

7) 6.3 Požadavky na délky klíčů

– Použije se toto ustanovení:

Délka klíče pro zvolený algoritmus podpisu certifikátu TSU musí být v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

– POZNÁMKA neplatné.

8) 6.5 Požadavky na algoritmus

– Použije se toto ustanovení:

Veřejný klíč TSU a podpis certifikátu TSU používají algoritmy, které jsou v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

– POZNÁMKA neplatné.

9) 7 Profily podporovaných přenosových protokolů

– Klient s časovými razítky a server s časovými razítky musí podporovat protokol časových razítek prostřednictvím protokolu HTTPS [9], jak je vymezen v bodě 3.4 dokumentu IETF RFC 3161 [1].

10) 8 Identifikátory objektů kryptografických algoritmů

– Použije se toto ustanovení:

Veřejný klíč TSU a podpis certifikátu TSU používají algoritmy ve shodě s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [8].

11) 9.1 Prohlášení o souladu s předpisy

– Pokud je token časového razítka prohlášen autoritou vydávající časová razítka (TSA) jako kvalifikované elektronické časové razítko podle

nařízení (EU) č. 910/2014 [i.2], musí v poli pro rozšíření tokenu časového razítka obsahovat jednu instanci rozšíření qcStatements se syntaxí specifikovanou v dokumentu IETF RFC 3739 [i.3], bodě 3.2.6.

– Rozšíření qcStatements musí obsahovat jednu instanci příkazu „esi4-qtstStatement-1“, jak je definováno v příloze B.

– Rozšíření qcStatements nesmí být označeno jako kritické.