EVROPSKÁ
KOMISE

V Bruselu dne 29.9.2025
C(2025) 6490 final

ANNEXES 1 to 2

PŘÍLOHY

PROVÁDĚCÍHO NAŘÍZENÍ KOMISE .../...,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) č. 910/2014, pokud jde o referenční normy pro postupy odesílání a přijímání dat v rámci kvalifikovaných služeb elektronického doporučeného doručování a pokud jde o interoperabilitu těchto služeb

PŘÍLOHA I

Seznam referenčních norem a specifikací uvedených v článku 1

Norma ETSI EN 319 521 V1.1.1 (2019-02) (dále jen „ETSI EN 319 521“) se použije s těmito úpravami:

1. Pro normu ETSI EN 319 521

   1) 2.1 Normativní odkazy:

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

      – [2] ETSI EN 319 411-1 V1.5.1 (2025-04) „Elektronické podpisy a infrastruktury (ESI); Politické a bezpečnostní požadavky na poskytovatele služeb vytvářejících důvěru vydávající certifikáty; Část 1: Obecné požadavky“.

      – [3] ETSI EN 319 522-1 V1.2.1 (2024-01) „Elektronické podpisy a infrastruktury (ESI); Služby elektronického doporučeného doručování; Část 1: Rámec a architektura“.

      – [4] ETSI EN 319 522-2 V1.2.1 (2024-01) „Elektronické podpisy a infrastruktury (ESI); Služby elektronického doporučeného doručování; Část 2: Sémantický obsah“.

      – [5] Evropská skupina pro certifikaci kybernetické bezpečnosti, podskupina pro šifrování: „Dohodnuté kryptografické mechanismy“ zveřejněné Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA)[1].

      – [6] ISO/IEC 15408-1:2022 – Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Kritéria hodnocení bezpečnosti IT.

      – [7] Prováděcí nařízení Komise (EU) 2024/482 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)[2].

      – [8] Prováděcí nařízení Komise (EU) 2024/3144 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.

      – [9] FIPS PUB 140-3 (2019) „Bezpečnostní požadavky na kryptografické moduly“.

   2) 3.1 Podmínky

      – zaručená elektronická pečeť: podle definice v nařízení (EU) 910/2014 [i.1].

[1] https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.

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

– zaručený elektronický podpis: podle definice v nařízení (EU) 910/2014 [i.1].

– kvalifikovaná elektronická pečeť: podle definice v nařízení (EU) 910/2014 [i.1].

– kvalifikovaný elektronický podpis: podle definice v nařízení (EU) 910/2014 [i.1].

– bezpečný kryptografický prostředek: prostředek, který uchovává soukromý klíč uživatele, chrání tento klíč před neoprávněným přístupem a provádí podepisování nebo dešifrovací funkce jménem uživatele.

3) 5.1.1 Společná ustanovení

– REQ-ERDS-5.1.1-01 Služba elektronického doporučeného doručování musí zajistit, aby byla při zpracování uživatelského obsahu službou elektronického doporučeného doručování odpovídajícím způsobem zaručena jeho dostupnost, celistvost a důvěrnost, a to výběrem vhodných technik šifrování celistvosti a důvěrnosti, které jsou v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [5].

4) 5.2.1.1 Obecně

– REQ-QERDS-5.2.1.1-01 Poskytovatel kvalifikované služby elektronického doporučeného doručování ověří s velmi vysokou mírou spolehlivosti totožnost příjemce buď přímo, nebo prostřednictvím třetí strany, a to s použitím jednoho z následujících prostředků nebo jejich kombinace podle potřeby:

  a) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby pomocí vhodných důkazů a postupů v souladu s vnitrostátním právem;

  b) na dálku, s použitím prostředku pro elektronickou identifikaci, který splňuje požadavky stanovené v článku 8 nařízení (EU) č. 910/2014 [i.1], pokud jde o úroveň záruky „vysoká“, nebo prostřednictvím evropské peněženky digitální identity;

  c) pomocí certifikátu kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečetě;

  d) použitím jiných metod identifikace, které zajišťují, že fyzickou osobu nebo oprávněného zástupce právnické osoby lze identifikovat s velmi vysokou mírou spolehlivosti. Ujištění, že tato identifikace je provedena s velmi vysokou mírou spolehlivosti, musí být potvrzeno subjektem posuzování shody.

– REQ-QERDS-5.2.1.1-01A Poskytovatel kvalifikované služby elektronického doporučeného doručování ověří totožnost odesílatele vhodnými prostředky, a to buď přímo, nebo prostřednictvím třetí strany, na základě jedné z následujících metod nebo jejich kombinace:

  a) na základě fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby pomocí vhodných důkazů a postupů v souladu s vnitrostátním právem;

b) na dálku, prostřednictvím evropské peněženky digitální identity nebo oznámeného prostředku pro elektronickou identifikaci, který splňuje požadavky stanovené v článku 8 nařízení (EU) č. 910/2014 [i.1], pokud jde o úroveň záruky „značná“, za předpokladu, že byl vydán na základě předchozí fyzické přítomnosti fyzické osoby nebo oprávněného zástupce právnické osoby;

c) prostřednictvím certifikátu zaručeného elektronického podpisu nebo zaručené elektronické pečetě, pokud byl certifikát vydán fyzické osobě nebo oprávněnému zástupci právnické osoby podle normalizované certifikační politiky (NCP), jak je vymezena v normě ETSI EN 319 411-1 [2]; nebo

d) použitím jiných metod identifikace, které zajišťují, že fyzickou osobu nebo oprávněného zástupce právnické osoby lze identifikovat s velmi vysokou mírou spolehlivosti. Ujištění, že tato identifikace je provedena s vysokou mírou spolehlivosti, musí být potvrzeno subjektem posuzování shody.

– POZNÁMKA Třetí stranou ověřující totožnost odesílatele a příjemce může být jiný poskytovatel kvalifikované služby elektronického doporučeného doručování, pokud jsou odesílatel a příjemce přihlášeni k různým poskytovatelům kvalifikované služby elektronického doporučeného doručování.

5) 5.2.1.2 Identifikace příjemce a předávání uživatelského obsahu

– REQ-QERDS-5.2.1.2-03 Pokud je identifikace příjemce založena na interním procesu kvalifikované služby elektronického doporučeného doručování, musí poskytovatel kvalifikované služby elektronického doporučeného doručování provádět celý proces v zabezpečeném a kontrolovaném prostředí.

6) 5.2.2 Ustanovení pro ověřování kvalifikované služby elektronického doporučeného doručování EU

– REQ-QERDS-5.2.2-03 [PODMÍNĚNÉ] Pokud poskytovatel kvalifikované služby elektronického doporučeného doručování váže prostředky ověření na totožnost odesílatele ověřenou podle bodu 5.2.1, jde o jeden z následujících prostředků:

a) mechanismy dvoufaktorového ověřování;

b) evropská peněženka digitální identity nebo oznámený prostředek pro elektronickou identifikaci, který splňuje požadavky stanovené v článku 8 nařízení (EU) č. 910/2014 [i.1], pokud jde o úroveň záruky „vysoká“ nebo „značná“;

c) vzájemné ověřování totožnosti prostřednictvím protokolu zabezpečení transportní vrstvy (Transport Layer Security – TLS), které zahrnuje certifikát vydaný odesílateli v rámci normalizované certifikační politiky (NCP), jak je vymezeno v normě ETSI EN 319 411-1 [2];

d) digitální podpis podporovaný certifikátem vydaným podle normalizované certifikační politiky (NCP), jak je vymezeno v normě ETSI EN 319 411-1 [2];

e) jiné prostředky, které zajišťují ověření totožnosti identifikovaného odesílatele. Shodu vazby potvrdí subjekt posuzování shody. Příklad: Může to zahrnovat použití jednoho z prostředků uvedených v písmenech a), b) a d) k registraci klientského certifikátu protokolu TLS pro automatizované odesílání prostřednictvím vzájemného TLS nebo k registraci certifikátu digitální pečetě používaného k zapečetění tvrzení pro ověření se službou elektronického doporučeného doručování. Lze použít i jiné mechanismy, při nichž identifikovaní odesílatelé využívají pověřených služeb třetích stran.

– REQ-QERDS-5.2.2-03A [PODMÍNĚNÉ] Pokud poskytovatel kvalifikované služby elektronického doporučeného doručování váže prostředky ověřování na totožnost příjemce ověřenou podle bodu 5.2.1, jde o jeden z následujících prostředků, pokud tento prostředek nebo jakákoli jejich kombinace zajišťují velmi vysokou úroveň spolehlivosti, pokud jde o totožnost ověřovaného příjemce:

a) mechanismusvícefaktorového ověřování;

b) evropská peněženka digitální identity nebo oznámený prostředek pro elektronickou identifikaci, který splňuje požadavky stanovené v článku 8 nařízení (EU) č. 910/2014 [i.1], pokud jde o úroveň záruky „vysoká“ nebo „značná“;

c) certifikát kvalifikovaného elektronického podpisu nebo kvalifikované elektronické pečetě;

d) jiné prostředky, které zajišťují ověření totožnosti identifikovaného příjemce. Shodu vazby potvrdí subjekt posuzování shody. Příklad: Může to zahrnovat použití jednoho z prostředků uvedených v písmenech a), až c) k registraci klientského certifikátu protokolu zabezpečení transportní vrstvy (Transport Layer Security – TLS) pro automatizované odesílání prostřednictvím vzájemného TLS nebo k registraci certifikátu digitální pečetě používaného k zapečetění tvrzení pro ověření se službou elektronického doporučeného doručování. Lze použít i jiné mechanismy, při nichž identifikovaní odesílatelé využívají pověřených služeb třetích stran.

– REQ-QERDS-5.2.2-04 [PODMÍNĚNÉ] Pokud se odesílatel připojuje ke kvalifikované službě elektronického doporučeného doručování zabezpečeným spojením, které vyžaduje vzájemné ověření mezi strojem odesílatele a serverem kvalifikované služby elektronického doporučeného doručování na základě certifikátů vydaných podle normalizované certifikační politiky (NCP), jak je vymezeno v normě ETSI EN 319 411-1 [2], pak po navázání tohoto zabezpečeného spojení mohou být pro druhou fázi ověření odesílatele použity mechanismy jednofaktorového ověření, pokud zavedené organizační postupy a bezpečnostní opatření zajišťují důvěru v ověření odesílatele.

7) 5.4.1 Společná ustanovení

– REQ-ERDS-5.4.1-06 Služba elektronického doporučeného doručování generuje a zpřístupňuje oprávněným zainteresovaným stranám důkazy služby elektronického doporučeného doručování o událostech

elektronického doporučeného doručování, jak je vymezeno v bodě 6 normy ETSI EN 319 522-1 [3].

– REQ-ERDS-5.4.1-07 Poskytovatel služby elektronického doporučeného doručování archivuje důkazy a/nebo přehledy důkazů pro každý vydaný důkaz.

– REQ-ERDS-5.4.1-08 Důkazy služby elektronického doporučeného doručování vygenerované službou elektronického doporučeného doručování jsou v souladu se sémantikou důkazů vymezenou v bodě 8 normy ETSI EN 319 522-2 [4].

8) 7.2.1 Společná ustanovení

– REQ-ERDS-7.2.1-02 Pracovníci poskytovatele služby elektronického doporučeného doručování 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.

– REQ-ERDS-7.2.1-03 Shoda s požadavkem REQ-ERDS-7.2.1-02 musí zahrnovat pravidelné aktuální informace (alespoň každých dvanáct měsíců) o nových hrozbách a stávajících bezpečnostních postupech.

9) 7.3.2 Nakládání s médii

– REQ-ERDS-7.3.1-02 Uplatňují se všechny požadavky stanovené v normě ETSI EN 319 401 [1], bodě 7.3.3.

10) 7.5 Kontroly šifrování

– REQ-ERDS-7.5-01A Služba elektronického doporučeného doručování musí zvolit a používat vhodné techniky šifrování v souladu s dohodnutými kryptografickými mechanismy přijatými Evropskou skupinou pro certifikaci kybernetické bezpečnosti a zveřejněnými agenturou ENISA [5].

– REQ-ERDSP-7.5-03 Soukromý podpisový klíč služby elektronického doporučeného doručování 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 [6] 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) [7][8] a certifikovaným na úrovni EAL 4 nebo vyšší, nebo

c) do 31. 12. 2030 s normou FIPS PUB 140-3 [9] 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 [7][8], musí být tento prostředek nakonfigurován a používán v souladu s touto certifikací.

11) 7.8 Bezpečnost sítí

- REQ-ERDSP-7.8-04 Poskytovatel služby elektronického doporučeného doručování musí používat nejmodernější protokoly a algoritmy pro šifrování na úrovni transportní vrstvy v souladu s dohodnutými kryptografickými mechanismy, které přijala Evropská skupina pro certifikaci kybernetické bezpečnosti a zveřejnila agentura ENISA [5].
- REQ-ERDSP-7.8-06 Skenování zranitelnosti požadované v rámci požadavku REQ-7.8-13 normy ETSI EN 319 401 [1] se provádí nejméně jednou za čtvrtletí.
- REQ-ERDSP-7.8-07 Penetrační test požadovaný v rámci požadavku REQ-7.8-17X normy ETSI EN 319 401 [1] se provádí nejméně jednou ročně.
- REQ-ERDSP-7.8-08 Firewally musí být nakonfigurovány tak, aby zabránily veškerým protokolům a přístupům, které nejsou nezbytné pro provoz poskytovatele služeb vytvářejících důvěru.

12) 7.12 Plán ukončení činnosti poskytovatele služeb elektronického doporučeného doručování a plán ukončení služeb elektronického doporučeného doručování

- REQ-ERDS-7.12-03 Plán ukončení činnosti poskytovatele služeb elektronického doporučeného doručování musí splňovat požadavky stanovené v prováděcích aktech přijatých podle čl. 24 odst. 5 nařízení (EU) č. 910/2014 [i.1].

13) 7.14 Dodavatelský řetězec

- REQ-ERDS-7.14-01 Uplatňují se požadavky stanovené v normě ETSI EN 319 401 [1], bodě 7.14.

PŘÍLOHA II

Seznam referenčních norem a specifikací uvedených v článku 2

Použijí se normy ETSI EN 319 522-1 V1.2.1 (2024-01) (dále jen „ETSI EN 319 522-1“), ETSI EN 319 522-2 V1.2.1 (2024-01) (dále jen „ETSI EN 319 522-2“), ETSI EN 319 522-3 V1.2.1 (2024-01) (dále jen „ETSI EN 319 522-3“), ETSI EN 319 522-4-1 V1.2.1 (2019-01) (dále jen „ETSI EN 319 522-4-1“), ETSI EN 319 522-4-2 V1.1.1 (2018-09) (dále jen „ETSI EN 319 522-4-2“) a ETSI EN 319 522-4-3 V1.1.1 (2018-09) (dále jen „ETSI EN 319 522-4-3“).