2024/2683

15.10.2024

ROZHODNUTÍ EVROPSKÉ CENTRÁLNÍ BANKY (EU) 2024/2683

ze dne 8. října 2024,

kterým se mění rozhodnutí ECB/2013/1, kterým se stanoví rámec infrastruktury veřejných klíčů Evropského systému centrálních bank (ECB/2024/26)

RADA GUVERNÉRŮ EVROPSKÉ CENTRÁLNÍ BANKY,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 127 a čl. 132 odst. 1 této smlouvy,

s ohledem na statut Evropského systému centrálních bank a Evropské centrální banky, a zejména na článek 12.1 ve spojení s články 3.1 a 12.3 a článkem 34 tohoto statutu,

vzhledem k těmto důvodům:

(1) Rozhodnutím Evropské centrální banky ECB/2013/1 [1] byl zaveden rámec pro infrastrukturu veřejných klíčů Eurosystému (dále jen „infrastruktura veřejných klíčů ESCB“) s cílem regulovat vydávání a správu elektronických certifikátů, které jsou nezbytné pro přístup k elektronickým aplikacím, systémům, platformám a službám ESCB a Eurosystému se středním nebo vyšším než středním stupněm kritičnosti a pro jejich používání.

(2) Technologie používaná infrastrukturou veřejných klíčů ESCB dosáhla konce své životnosti a byla nahrazena. Je proto nezbytné zavést novou online certifikační autoritu infrastruktury veřejných klíčů ESCB (dále jen „online certifikační autorita infrastruktury veřejných klíčů ESCB V1.2“), která by měla rovněž zohlednit skutečnost, že tříletá platnost certifikátů vydaných pro uživatele z ESCB a mimo ESCB a pro technické komponenty certifikační autority infrastruktury veřejných klíčů ESCB nemůže skončit později než uplynutím platnosti certifikátu samotné on-line certifikační autority infrastruktury veřejných klíčů ESCB. Platnost certifikátu stávající online certifikační autority infrastruktury veřejných klíčů ESCB skončí dne 22. července 2026 a poté bude on-line certifikační autorita infrastruktury veřejných klíčů ESCB V1.2 jedinou online certifikační autoritou infrastruktury veřejných klíčů ESCB, a to až do skončení platnosti jejího certifikátu.

(3) Rozhodnutí ECB/2013/1 je proto třeba odpovídajícím způsobem změnit,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Změna

Příloha rozhodnutí ECB/2013/1 se nahrazuje přílohou tohoto rozhodnutí.

Článek 2

Vstup v platnost

Toto rozhodnutí vstupuje v platnost pátým dnem po zveřejnění v *Úředním věstníku Evropské unie*.

Ve Frankfurtu nad Mohanem dne 8. října 2024.

Prezidentka ECB
Christine LAGARDE

---

[1] Rozhodnutí Evropské centrální banky ECB/2013/1 ze dne 11. ledna 2013, kterým se stanoví rámec infrastruktury veřejných klíčů Evropského systému centrálních bank (Úř. věst. L 74, 16.3.2013, s. 30).

PŘÍLOHA

„PŘÍLOHA

Informace o certifikační autoritě infrastruktury veřejných klíčů ESCB včetně její totožnosti a technických komponent

Certifikační autorita infrastruktury veřejných klíčů ESCB je ve svém certifikátu určena jako vydavatel a její soukromý klíč se používá k podpisu certifikátů. Certifikační autorita infrastruktury veřejných klíčů ESCB odpovídá za:

i) vydávání certifikátů soukromých a veřejných klíčů,

ii) vydávání seznamů odvolaných certifikátů,

iii) vytváření párů klíčů spojených s určitými certifikáty, např. těmi, u nichž je nutná obnova klíče,

iv) zajištění celkové odpovědnosti za infrastrukturu veřejných klíčů ESCB a zajištění splnění všech nezbytných požadavků na provoz této infrastruktury.

Certifikační autorita infrastruktury veřejných klíčů ESCB zahrnuje všechny fyzické osoby, politiky, postupy a počítačové systémy, jimž bylo svěřeno, aby vydávaly elektronické certifikáty a aby je přidělovaly držitelům certifikátů.

Certifikační autorita infrastruktury veřejných klíčů ESCB zahrnuje tři technické komponenty:

1. **Kořenová certifikační autorita infrastruktury veřejných klíčů ESCB**: Tato certifikační autorita první úrovně vydává certifikáty jen pro sebe a jí podřízené certifikační autority. Je v provozu, jen když plní své úzce vymezené povinnosti. Její nejvýznamnější údaje jsou:

Distinguished name (Jednoznačné jméno)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (Sériové číslo)	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8
Distinguished name of issuer (Jednoznačné jméno vydavatele)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (Doba platnosti)	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
Message digest (Otisk zprávy) (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message digest (Otisk zprávy) (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Cryptographic algorithms (Kryptografické algoritmy)	SHA-256/RSA 4096

2. **Online certifikační autorita infrastruktury veřejných klíčů ESCB**: Tato certifikační autorita druhé úrovně je podřízena kořenové certifikační autoritě infrastruktury veřejných klíčů ESCB. Odpovídá za vydávání certifikátů infrastruktury veřejných klíčů ESCB uživatelům. Její platnost skončí dne 22. července 2026. Její nejvýznamnější údaje jsou:

Distinguished name (Jednoznačné jméno)	CN = ESCB-PKI ONLINE CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (Sériové číslo)	660C 9B12 9A0 A 6C21 5509 38DD 54A0 ED2D
Distinguished name of issuer (Jednoznačné jméno vydavatele)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (Doba platnosti)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (Otisk zprávy) (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message digest (Otisk zprávy) (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Cryptographic algorithms (Kryptografické algoritmy)	SHA-256/RSA 4096

3. **Online certifikační autorita infrastruktury veřejných klíčů ESCB V1.2**: Tato certifikační autorita druhé úrovně je podřízena kořenové certifikační autoritě infrastruktury veřejných klíčů ESCB. Odpovídá za vydávání certifikátů infrastruktury veřejných klíčů ESCB uživatelům. Po 22. červenci 2026 je jedinou online certifikační autoritou infrastruktury veřejných klíčů ESCB, a to až do skončení své platnosti. Její nejvýznamnější údaje jsou:

Distinguished name (Jednoznačné jméno)	CN = ESCB-PKI ONLINE CA V1.2, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (Sériové číslo)	1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653
Distinguished name of issuer (Jednoznačné jméno vydavatele)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (Doba platnosti)	From 08-06-2023 17:07:00 to 08-06-2038 17:07:00
Message digest (Otisk zprávy) (SHA-1)	DC92 042E 6316 CB60 F8F6 109B 8C43 F3C6 AF2F B2F3
Message digest (Otisk zprávy) (SHA-256)	96B7 8E9C F914 ED4D 072D 93C8 C531 DEEF D102 7571 7218 A202 0924 3216 99D8 1C48
Cryptographic algorithms (Kryptografické algoritmy)	SHA-256/RSA 4096“