ROZHODNUTÍ

ROZHODNUTÍ EVROPSKÉ CENTRÁLNÍ BANKY (EU) 2016/187

ze dne 11. prosince 2015,

kterým se mění rozhodnutí ECB/2013/1, kterým se stanoví rámec infrastruktury veřejných klíčů Evropského systému centrálních bank (ECB/2015/46)

RADA GUVERNÉRŮ EVROPSKÉ CENTRÁLNÍ BANKY,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 127 této smlouvy,

s ohledem na statut Evropského systému centrálních bank a Evropské centrální banky, a zejména na článek 12.1 ve spojení s článkem 3.1, článkem 5, článkem 12.3, články 16 až 24 a článkem 34 tohoto statutu,

vzhledem k těmto důvodům:

(1) Nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ([1]) byla s účinkem ode dne 1. července 2016 zrušena směrnice Evropského parlamentu a Rady 1999/93/ES ([2]). Je proto vhodné, aby se v rozhodnutí ECB/2013/1 ([3]) odkazovalo na nařízení (EU) č. 910/2014.

(2) Je třeba aktualizovat informace o certifikační autoritě infrastruktury veřejných klíčů ESCB včetně její totožnosti a technických komponent, uvedené v příloze rozhodnutí ECB/2013/1.

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

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Změny

Rozhodnutí ECB/2013/1 se mění takto:

1) V článku 1 se bod 10 nahrazuje tímto:

„10. ‚certifikační autoritou infrastruktury veřejných klíčů ESCB' subjekt, který je pro uživatele důvěryhodný a který vydává, spravuje, odvolává a obnovuje certifikáty infrastruktury veřejných klíčů ESCB v souladu s rámcem ESCB/SSM pro akceptaci certifikátů;".

2) V článku 4 se odstavec 4 nahrazuje tímto:

„4. Certifikační praxe v rámci infrastruktury veřejných klíčů ESCB je soubor pravidel, jež upravují životní cyklus elektronických certifikátů od počáteční žádosti po skončení platnosti či odvolání, jakož i vztahy mezi žadatelem o certifikát nebo držitelem certifikátu, certifikační autoritou infrastruktury veřejných klíčů ESCB a spoléhajícími se stranami. Vztahuje se na certifikáty, které spadají do oblasti působnosti směrnice 1999/93/ES a nařízení Evropského

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, s. 73).

([2]) Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy (Úř. věst. L 13, 19.1.2000, s. 12).

([3]) 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).

parlamentu a Rady (EU) č. 910/2014 (*), i na certifikáty, které do oblasti působnosti těchto předpisů nespadají. Rovněž vymezuje úlohu a odpovědnost všech stran a zavádí postupy pro vydávání a správu certifikátů. Tvoří přílohu dohody mezi druhou a třetí úrovní řízení.

(*) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, s. 73).“

3) V článku 10 se úvodní část odstavce 1 včetně písmene a) nahrazují tímto:

„1. Ledaže centrální banky Eurosystému prokážou, že nejednaly z nedbalosti, odpovídají v souladu se svými funkcemi a odpovědností v rámci infrastruktury veřejných klíčů ESCB za škodu způsobenou uživateli, který se důvodně spoléhá na kvalifikovaný certifikát ve smyslu směrnice 1999/93/ES a nařízení (EU) č. 910/2014, pokud jde o:

a) přesnost veškerých informací obsažených v kvalifikovaném certifikátu ke dni jeho vydání a o otázku, zda certifikát obsahuje veškeré údaje stanovené pro kvalifikovaný certifikát ve smyslu směrnice 1999/93/ES a nařízení (EU) č. 910/2014;“.

4) Příloha se nahrazuje přílohou tohoto rozhodnutí.

Článek 2

Vstup v platnost

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

Ve Frankfurtu nad Mohanem dne 11. prosince 2015.

Prezident ECB

Mario DRAGHI

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 dvě technické komponenty:

— **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:

a) certifikát SHA-1 ([1]):

Distinguished name (Jednoznačné jméno)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Sériové číslo)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
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 11:58:26 to 21-06-2041 11:58:26
Message digest (Otisk zprávy) (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Message digest (Otisk zprávy) (SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Cryptographic algorithms (Kryptografické algoritmy)	SHA-1/RSA 4096

b) certifikát SHA-256:

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

([1]) Tento certifikát bude používán jen v systémech, které nepodporují vyšší algoritmy.

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

— **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 nejvýznamnější údaje jsou:

a) certifikát SHA-1 ([1]):

Distinguished name (Jednoznačné jméno)	CN=ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Sériové číslo)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
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)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Message digest (Otisk zprávy) (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Cryptographic algorithms (Kryptografické algoritmy)	SHA-1/RSA 4096

b) certifikát SHA-256:

Distinguished name (Jednoznačné jméno)	CN=ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Sériové číslo)	660C 9B12 9A0A 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“

([1]) Tento certifikát bude používán jen v systémech, které nepodporují vyšší algoritmy.