ROZHODNUTIA

ROZHODNUTIE EURÓPSKEJ CENTRÁLNEJ BANKY (EÚ) 2016/187

z 11. decembra 2015,

ktorým sa mení rozhodnutie ECB/2013/1, ktorým sa ustanovuje rámec pre infraštruktúru verejných kľúčov Európskeho systému centrálnych bánk (ECB/2015/46)

RADA GUVERNÉROV EURÓPSKEJ CENTRÁLNEJ BANKY,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 127,

so zreteľom na Štatút Európskeho systému centrálnych bánk a Európskej centrálnej banky, a najmä na jeho článok 12.1 v spojení s článkom 3.1, článkom 5, článkom 12.3 a článkami 16 až 24 a článkom 34,

keďže:

(1) Nariadením Európskeho parlamentu a Rady (EÚ) č. 910/2014 ([1]) bola zrušená smernica Európskeho parlamentu a Rady 1999/93/ES ([2]) s účinnosťou od 1. júla 2016. Preto je vhodné, aby sa v rozhodnutí ECB/2013/1 ([3]) odkazovalo na nariadenie (EÚ) č. 910/2014.

(2) Je potrebné aktualizovať informácie týkajúce sa certifikačnej autority ESCB-PKI vrátane jej identifikačných údajov a technických komponentov, ako sú uvedené v prílohe k rozhodnutiu ECB/2013/1.

(3) Rozhodnutie ECB/2013/1 by sa preto malo zodpovedajúcim spôsobom zmeniť,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Zmeny

Rozhodnutie ECB/2013/1 sa mení takto:

1. V článku 1 sa bod 10 nahrádza takto:

„10. ‚certifikačnou autoritou ESCB-PKI' sa rozumie subjekt, ktorý má dôveru používateľov a vydáva, spravuje, zrušuje a obnovuje certifikáty ESCB-PKI v súlade s rámcom ESCB/JMD pre uznávanie certifikátov;".

2. V článku 4 sa odsek 4 nahrádza takto:

„4. Dokument o certifikačnej praxi ESCB-PKI je súborom pravidiel upravujúcich životný cyklus elektronických certifikátov od podania žiadosti až do ukončenia platnosti certifikátu alebo jeho zrušenia vrátane vzťahov medzi žiadateľom o vydanie certifikátu alebo držiteľom, certifikačnou autoritou ESCB-PKI a osobami spoliehajúcimi sa na certifikát. Tento dokument zahŕňa certifikáty, ktoré sú predmetom úpravy smernice 1999/93/ES a nariadenia

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73).

([2]) Smernica Európskeho parlamentu a Rady 1999/93/ES z 13. decembra 1999 o rámci Spoločenstva pre elektronické podpisy (Ú. v. ES L 13, 19.1.2000, s. 12).

([3]) Rozhodnutie Európskej centrálnej banky ECB/2013/1 z 11. januára 2013, ktorým sa ustanovuje rámec pre infraštruktúru verejných kľúčov Európskeho systému centrálnych bánk (Ú. v. EÚ L 74, 16.3.2013, s. 30).

Európskeho parlamentu a Rady (EÚ) č. 910/2014 (*), ako aj certifikáty, ktoré nepatria do rozsahu ich pôsobnosti. Upravuje tiež úlohy a povinnosti všetkých strán a ustanovuje postupy týkajúce sa vydávania a správy certifikátov. Tvorí prílohu k dohode medzi úrovňou 2 a úrovňou 3 riadenia.

(*) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73).“

3. V článku 10 sa v odseku 1 úvodná časť a písm. a) nahrádzajú takto:

„1. Pokiaľ nepreukážu, že nekonali nedbalo, sú centrálne banky Eurosystému v súlade s ich úlohami a povinnosťami v rámci ESCB-PKI zodpovedné za akúkoľvek škodu spôsobenú používateľovi, ktorý sa odôvodnene spolieha na kvalifikovaný certifikát vymedzený v zmysle smernice 1999/93/ES a nariadenia (EÚ) č. 910/2014, a to pokiaľ ide o:

a) presnosť všetkých informácií uvedených v kvalifikovanom certifikáte v čase vydania a skutočnosť, že certifikát obsahuje všetky náležitosti, ktoré sú pre kvalifikovaný certifikát predpísané v zmysle smernice 1999/93/ES a nariadenia (EÚ) č. 910/2014;“.

4. Príloha sa nahrádza prílohou k tomuto rozhodnutiu.

Článok 2

Nadobudnutie účinnosti

Toto rozhodnutie nadobúda účinnosť tretím dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Vo Frankfurte nad Mohanom 11. decembra 2015

Prezident ECB

Mario DRAGHI

PRÍLOHA

„PRÍLOHA

Informácie týkajúce sa certifikačnej autority ESCB-PKI vrátane jej identifikačných údajov a technických komponentov

Certifikačná autorita ESCB-PKI je identifikovaná vo svojom certifikáte ako vydavateľ a jej súkromný kľúč sa používa na podpisovanie certifikátov. Certifikačná autorita ESCB-PKI má na starosti:

i) vydávanie certifikátov so súkromným kľúčom a verejným kľúčom;

ii) vydávanie zoznamu zrušených certifikátov;

iii) vytváranie kľúčových párov spojených so špecifickými certifikátmi, napr. tými, ktoré si vyžadujú obnovu kľúča;

iv) celkovú zodpovednosť za ESCB-PKI a zodpovednosť za to, že všetky požiadavky potrebné na jej prevádzku sú splnené.

Certifikačnú autoritu ESCB-PKI tvoria všetci jednotlivci, pravidlá, postupy a počítačové systémy podieľajúce sa na vydávaní elektronických certifikátov a priraďovaní týchto certifikátov ich držiteľom.

Certifikačná autorita ESCB-PKI zahŕňa dva technické komponenty:

— **Koreňová certifikačná autorita ESCB-PKI**: Táto certifikačná autorita na prvej úrovni vydáva certifikáty len sebe a svojim podriadeným certifikačným autoritám. Funguje len vtedy, keď vykonáva svoje úzko vymedzené úlohy. Jej najvýznamnejšie údaje sú:

a) certifikát SHA-1 ([1]):

Distinguished name (Rozoznateľný názov)	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 (Rozoznateľný názov vydavateľa)	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 (SHA-1) [Odtlačok údajov (SHA-1)]	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Message digest (SHA-256) [Odtlačok údajov (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 (Rozoznateľný názov)	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 sa bude používať iba v systémoch, ktoré nepodporujú vyššie algoritmy.

Distinguished name of issuer (Rozoznateľný názov vydavateľa)	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 (SHA-1) [Odtlačok údajov (SHA-1)]	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message digest (SHA-256) [Odtlačok údajov (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 certifikačná autorita ESCB-PKI**: Táto certifikačná autorita na druhej úrovni je podriadená koreňovej certifikačnej autorite ESCB-PKI. Je zodpovedná za vydávanie certifikátov ESCB-PKI používateľom. Jej najvýznamnejšie údaje sú:

a) certifikát SHA-1 ([1]):

Distinguished name (Rozoznateľný názov)	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 (Rozoznateľný názov vydavateľa)	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 (SHA-1) [Odtlačok údajov (SHA-1)]	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Message digest (SHA-256) [Odtlačok údajov (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 (Rozoznateľný názov)	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 (Rozoznateľný názov vydavateľa)	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 (SHA-1) [Odtlačok údajov (SHA-1)]	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message digest (SHA-256) [Odtlačok údajov (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 sa bude používať iba v systémoch, ktoré nepodporujú vyššie algoritmy.