

DEĊIŻJONIJIET

DEĊIŻJONI (UE) 2016/187 TAL-BANK ĊENTRALI EWROPEW

tal-11 ta' Diċembru 2015

li temenda d-Deċiżjoni BĊE/2013/1 li tistabilixxi l-qafas għall-infrastruttura taċ-ċavetta pubblika għas-Sistema Ewropea ta' Banek Ċentrali (BĊE/2015/46)

IL-KUNSILL GOVERNATTIV TAL-BANK ĊENTRALI EWROPEW,

Wara li kkunsidra t-Trattat dwar il-Funzjonament tal-Unjoni Ewropea, u b'mod partikolari l-Artikolu 127 tiegħu,

Wara li kkunsidra l-iStatut tas-Sistema Ewropea tal-Banek Ċentrali u tal-Bank Ċentrali Ewropew, u b'mod partikolari l-Artikolu 12.1 flimkien mal-Artikolu 3.1, l-Artikolu 5, l-Artikolu 12.3 u l-Artikoli 16 sa 24 u 34 tiegħu,

Billi:

- (1) Ir-Regolament (UE) Nru 910/2014 tal-Parlament Ewropew u tal-Kunsill ⁽¹⁾ hassar id-Direttiva 1999/93/KE tal-Parlament Ewropew u tal-Kunsill ⁽²⁾ b'effett mill-1 ta' Lulju 2016. Għalhekk, huwa xieraq li ssir referenza għar-Regolament (UE) Nru 910/2014 fid-Deċiżjoni BĊE/2013/1 ⁽³⁾.
- (2) L-informazzjoni dwar l-awtorità għaċ-ċertifikazzjoni tas-SEBĊ-PKI, inklużi l-identità u l-komponenti tekniċi tagħha, kif stipulat fl-Anness għad-Deċiżjoni BĊE/2013/1, għandha tiġi aġġornata.
- (3) Għalhekk, id-Deċiżjoni BĊE/2013/1 għandha tiġi emendata kif meħtieġ,

ADOTTA DIN ID-DEĊIŻJONI:

Artikolu 1

Emendi

Id-Deċiżjoni BĊE/2013/1 hija emendata kif ġej:

1. Fl-Artikolu 1, il-punt 10 huwa mibdul b'dan li ġej:

"10. 'L-awtorità ta' ċertifikazzjoni SEBĊ-PKI' tfisser l-entità, fdata mill-utenti, biex tohrog, tiġġestixxi, tirrevoka u gġedded ċertifikati SEBĊ-PKI skont il-qafas ta' aċċettazzjoni taċ-ċertifikat SEBĊ/MSU;"

2. fl-Artikolu 4, il-paragrafu 4 huwa ssostitwit b'dan li ġej:

"4. L-istqarrija tal-prattika ta' ċertifikazzjoni tas-SEBĊ-PKI hija gabra ta' regoli li jirregolaw iċ-ċiklu tal-hajja taċ-ċertifikati elettronici, mit-talba inizjali sat-tmiem jew ir-revoka tal-abbonament, kif ukoll ir-relazzjonijiet bejn l-applikant taċ-ċertifikat jew l-abbonat, l-awtorità għaċ-ċertifikazzjoni tas-SEBĊ-PKI u l-partijiet dipendenti. Din tkopri ċertifikati li jaqgħu taħt il-kamp ta' applikazzjoni tad-Direttiva 1999/93/KE u r-Regolament (UE) Nru 910/2014

⁽¹⁾ Regolament (UE) Nru 910/2014 tal-Parlament Ewropew u tal-Kunsill tat-23 ta' Lulju 2014 dwar l-identifikazzjoni elettronika u s-servizzi fiduċjarji għal transazzjonijiet elettronici fis-suq intern u li thassar id-Direttiva 1999/93/KE (ĠU L 257, 28.8.2014, p. 73).

⁽²⁾ Direttiva 1999/93/KE tal-Parlament Ewropew u tal-Kunsill tat-13 ta' Diċembru 1999 dwar kwadru tal-Komunità għall-firem elettronici (ĠU L 13, 19.1.2000, p. 12).

⁽³⁾ Deċiżjoni BĊE/2013/1 tal-Bank Ċentrali Ewropew tal-11 ta' Jannar 2013 li tistabilixxi l-qafas għall-infrastruttura taċ-ċavetta pubblika għas-Sistema Ewropea ta' Banek Ċentrali (ĠU L 74, 16.3.2013, p. 30).

tal-Parlament Ewropew u tal-Kunsill (*) u ċertifikati li jaqgħu barra l-kamp ta' applikazzjoni tagħhom. Tistabbilixxi wkoll l-irwoli u r-responsabbiltajiet tal-partijiet kollha u tistabbilixxi l-proċeduri dwar il-hruġ u l-ġestjoni ta' ċertifikati. Hija annessa mal-Ftehim tal-Livell 2 — Livell 3.

(*) Regolament (UE) Nru 910/2014 tal-Parlament Ewropew u tal-Kunsill tat-23 ta' Lulju 2014 dwar l-identifikazzjoni elettronika u s-servizzi fiduċjarji għal transazzjonijiet elettronici fis-suq intern u li jhassar id-Diretiva 1999/93/KE (ĠU L 257, 28.8.2014, p. 73).";

3. fl-Artikolu 10, id-dikjarazzjoni introduttorja u l-punt (a) tal-paragrafu 1 huma ssostitwiti b'dan li ġej:

"1. Hlief jekk igibu prova li ma aġixxewx b'negligenza, il-banek ċentrali tal-Eurosistema għandhom ikunu responsabbli skont il-funzjonijiet u r-responsabbiltajiet tagħhom fis-SEBC-PKI għal kwalunkwe hsara kkawżata lil utent li jiddependi b'mod raġonevoli fuq ċertifikat ikkwalifikat, kif iddefinit fid-Direttiva 1999/93/KE u r-Regolament (UE) Nru 910/2014, fir-rigward ta':

(a) il-precizjoni taż-żmien tal-hruġ tal-informazzjoni kollha li tinsab f'ċertifikat ikkwalifikat, u l-kwistjoni jekk iċ-ċertifikat jinkludix id-dettalji kollha preskritti għal ċertifikat ikkwalifikat kif iddefinit fid-Direttiva 1999/93/KE u r-Regolament (UE) Nru 910/2014;"

4. l-Anness huwa ssostitwit bl-Anness għal din id-Deciżjoni;

Artikolu 2

Dhul fis-sehh

Dan ir-Regolament għandu jidhol fis-sehh fit-tielet jum wara l-pubblikazzjoni tiegħu f'Il-Ġurnal Uffiċjali tal-Unjoni Ewropea.

Magħmul fi Frankfurt am Main, 11 ta' Diċembru 2015.

Il-President tal-BĊE
Mario DRAGHI

ANNEX

"ANNEX

Informazzjoni dwar l-awtorità għaċ-ċertifikazzjoni tas-SEBC-PKI, inkluża l-identità tagħha, u l-komponenti tekniċi tagħha

L-awtorità għaċ-ċertifikazzjoni tas-SEBC-PKI hija identifikata fiċ-ċertifikat tagħha bhala l-emittent u ċ-ċavetta privata tagħha tintuża biex tiffirma ċ-ċertifikati. L-awtorità għaċ-ċertifikazzjoni tas-SEBC-PKI hija inkarigata mill-:

- (i) hruġ ta' ċertifikati ta' ċwieviet privati u pubbliċi;
- (ii) hruġ ta' listi ta' revoka;
- (iii) l-iġġenerar ta' pari ta' ċwieviet assoċjati ma' ċertifikati speċifiċi, eż. dawk li jehtieġu l-irkupru ta' ċavetta;
- (iv) iż-żamma tar-responsabbiltà generali għas-SEBC-PKI u l-iżgurar li r-rekwiziti kollha mehtieġa għat-thaddim tagħha jkunu sodisfatti.

L-awtorità għaċ-ċertifikazzjoni tas-SEBC-PKI tinkludi kull individwu, politika, proċedura u sistema tal-kompjuter fdati bil-hruġ ta' ċertifikati elettronici u tassenjahom lill-abbonati taċ-ċertifikat.

L-awtorità għaċ-ċertifikazzjoni tas-SEBC-PKI tinkludi żewġ komponenti tekniċi:

— **L-awtorità gherq għaċ-ċertifikazzjoni tas-SEBC-PKI:** Din l-awtorità ta' ċertifikazzjoni, fl-ewwel livell, tohroġ biss ċertifikati għaliha nfisha u l-awtoritajiet ta' ċertifikazzjoni subordinati tagħha. Din tkun operattiva biss meta twettaq ir-responsabbiltajiet tagħha stess iddefiniti b'mod ristrett. Id-dejta l-aktar sinifikanti tagħha huma:

a) ċertifikat SHA-1 ⁽¹⁾:

Isem distint	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Numru Serjali:	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Isem distint tal-emittent	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Perijodu ta' validità	Minn 21-06-2011 11:58:26 sa 21-06-2041 11:58:26
Sommarju tal-messaġġ (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Sommarju tal-messaġġ (SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Algoritmi kriptografiċi	SHA-1/RSA 4096

b) Ċertifikat SHA-256:

Isem distint	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Numru Serjali:	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8

⁽¹⁾ Dan iċ-ċertifikat għandu jintuża biss f'sistemi li ma jappoġġawx algoritmi oġhla.

Isem distint tal-emittent	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Perijodu ta' validità	Minn 21-06-2011 12:35:34 sa 21-06-2041 12:35:34
Sommarju tal-messaġġ (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Sommarju tal-messaġġ (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Algoritmi kriptografiċi	SHA-256/RSA 4096

- **L-awtorità għaċ-ċertifikazzjoni tas-SEBĊ-PKI li tinsab online:** Din l-awtorità ta' ċertifikazzjoni, fit-tieni livell, hija subordinata għall-awtorità tal-Gherq għaċ-ċertifikazzjoni tas-SEBĊ-PKI. Hija responsabbli għall-hruġ ta' ċertifikati SEBĊ-PKI għall-utenti. Id-dejta l-aktar sinifikanti tagħha huma:

a) ċertifikat SHA-1 ⁽¹⁾:

Isem distint	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Numru Serjali:	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Isem distint tal-emittent	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Perijodu ta' validità	Minn 22-07-2011 12:46:35 sa 22-07-2026 12:46:35
Sommarju tal-messaġġ (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Sommarju tal-messaġġ (SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Algoritmi kriptografiċi	SHA-1/RSA 4096

b) Ċertifikat SHA-256:

Isem distint	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Numru Serjali:	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Isem distint tal-emittent	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Perijodu ta' validità	Minn 22-07-2011 12:46:35 sa 22-07-2026 12:46:35
Sommarju tal-messaġġ (SHA-1)	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Sommarju tal-messaġġ (SHA-256)	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Algoritmi kriptografiċi	SHA-256/RSA 4096"

⁽¹⁾ Dan iċ-ċertifikat għandu jintuża biss f'sistemi li ma jappoġġawx algoritmi oghla.