PÄÄTÖKSET

EUROOPAN KESKUSPANKIN PÄÄTÖS (EU) 2016/187,

annettu 11 päivänä joulukuuta 2015,

Euroopan keskuspankkijärjestelmässä käytettävää julkisen avaimen infrastruktuuria koskevien periaatteiden vahvistamisesta annetun päätöksen EKP/2013/1 muuttamisesta (EKP/2015/46)

EUROOPAN KESKUSPANKIN NEUVOSTO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 127 artiklan,

ottaa huomioon Euroopan keskuspankkijärjestelmän ja Euroopan keskuspankin perussäännön ja erityisesti sen 12.1 artiklan, tarkasteltuna yhdessä sen 3.1, 5, 12.3, 16, 24 ja 34 artiklan kanssa,

sekä katsoo seuraavaa:

(1) Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY ([1]) on kumottu Euroopan parlamentin ja neuvoston asetuksella (EU) N:o 910/2014 ([2]) 1 päivästä heinäkuuta 2016 alkavin vaikutuksin. Näin ollen päätöksessä EKP/2013/1 ([3]) on asianmukaista viitata asetukseen (EU) N:o 910/2014.

(2) EKPJ-PKI:n varmentajaa koskevat tiedot, mukaan lukien tunnistaminen ja sen tekniset komponentit, sellaisina kuin ne on esitetty päätöksen EKP/2013/1 liitteessä, on tarpeen päivittää.

(3) Tästä syystä päätös EKP/2013/1 olisi muutettava vastaavasti,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Muutokset

Muutetaan päätös EKP/2013/1 seuraavasti:

1) Korvataan 1 artiklan 10 kohta seuraavasti:

”10. ’EKPJ-PKI:n varmentajalla’ luotettua tahoa, joka luo, hallinnoi, sulkee ja uusii EKPJ-PKI:n varmenteita EKPJ:n/YVM:n varmenteiden hyväksymisperiaatteiden mukaisesti;”.

2) Korvataan 4 artiklan 4 kohta seuraavasti:

”4. EKPJ-PKI:n varmentamisen menettelytapakuvaus on sääntökokonaisuus, joka kattaa sähköisten varmenteiden koko elinkaaren ensimmäisestä hakemuksesta käytön päättymiseen tai peruuttamiseen sekä varmenteen hakijan tai haltijan, EKPJ-PKI:n varmentajan ja varmenteeseen luottavan osapuolen väliset suhteet. Se kattaa direktiivin

([1]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY muuttamisesta (EUVL L 257, 28.8.2014, s. 73).

([2]) Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY, annettu 13 päivänä joulukuuta 1999, sähköisiä allekirjoituksia koskevista yhteisön puitteista (EYVL L 13, 19.1.2000, s. 12).

([3]) Euroopan keskuspankin päätös EKP/2013/1, annettu 11 päivänä tammikuuta 2013, Euroopan keskuspankkijärjestelmässä käytettävää julkisen avaimen infrastruktuuria koskevien periaatteiden vahvistamisesta (EUVL L 74, 16.3.2013, s. 30).

1999/93/EY ja Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 (*) soveltamisalaan kuuluvat varmenteet sekä niiden soveltamisalan ulkopuolelle jäävät varmenteet. Siinä määritellään myös kaikkien osapuolten roolit ja velvollisuudet sekä perustetaan varmenteiden luomista ja hallinnointia koskevat menettelytavat. Se on tasojen 2 ja 3 välisen sopimuksen liitteenä.

(*) Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (EUVL L 257, 28.8.2014, s. 73).".

3) Korvataan 10 artiklan 1 kohdan johtolause ja a alakohta seuraavasti:

"1. Elleivät eurojärjestelmän keskuspankit osoita, että ne eivät ole toimineet tuottamuksellisesti, ne vastaavat EKPJ-PKI:hin liittyvien tehtäviensä ja vastuualueidensa mukaisesti kaikesta vahingosta, jota aiheutuu käyttäjälle, joka on perustellusti luottanut hyväksyttyyn varmenteeseen, sellaisena kuin se on määritelty direktiivissä 1999/93/EY ja asetuksessa (EU) N:o 910/2014, siltä osin kuin kyseessä on

a) hyväksyttyyn varmenteeseen sisältyvien tietojen oikeellisuus varmenteen luomishetkenä ja se, sisältääkö varmenne kaikki hyväksyttyyn varmenteeseen, sellaisina kuin ne on määritelty direktiivissä 1999/93/EY ja asetuksessa (EU) N:o 910/2014, osalta säädetyt yksityiskohtaiset tiedot,".

4) Liite korvataan tämän päätöksen liitteellä.

2 artikla

Voimaantulo

Tämä päätös tulee voimaan kolmantena päivänä sen jälkeen, kun se on julkaistu Euroopan unionin virallisessa lehdessä.

Tehty Frankfurt am Mainissa 11 päivänä joulukuuta 2015.

EKP:n puheenjohtaja

Mario DRAGHI

LIITE

"LIITE

EKPJ-PKI:n varmentajaa koskevat tiedot, mukaan lukien tunnistaminen ja sen tekniset komponentit

EKPJ-PKI:n varmentaja nimetään varmenteessa varmenteen luojaksi, ja sen yksityistä avainta käytetään varmenteiden allekirjoittamiseen. EKPJ-PKI:n varmentaja vastaa

i) yksityisen ja julkisen avaimen varmenteiden luomisesta,

ii) varmenteiden sulkulistojen julkaisemisesta,

iii) erityisiin varmenteisiin liittyvien avainparien luomisesta, esim. kun kyse on avaimen palauttamista edellyttävistä varmenteista, ja

iv) kokonaisvastuun kantamisesta EKPJ-PKI:n ylläpitämisessä sekä sen varmistamisesta, että kaikki EKPJ-PKI:n operoinnin edellyttämät vaatimukset täytetään.

EKPJ-PKI:n varmentaja ottaa mukaan kaikki luonnolliset henkilöt, menettelytavat, menetelmät ja tietokonejärjestelmät, joiden tehtäviin kuuluu digitaalisten varmenteiden luominen ja niiden luovuttaminen varmenteen haltijoille.

EKPJ-PKI:n varmentaja koostuu kahdesta teknisestä komponentista:

— **EKPJ-PKI:n juurivarmentaja**: Tämä varmentaja luo varmennushierarkian ylimmällä tasolla varmenteita vain itselleen ja alaisuudessaan oleville varmentajille. Se on toiminnassa vain toimiessaan omalla suppeasti määritellyllä vastuualueellaan. Tärkeimmät sitä koskevat tiedot ovat seuraavat:

a) SHA-1 -varmenne ([1]):

Distinguished name (DN-nimi)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Sarjanumero)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Distinguished name of issuer (Yksilöivä nimi)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Voimassaoloaika)	From 21-06-2011 11:58:26 to 21-06-2041 11:58:26
Message digest (SHA-1) (Tiivistealgoritmi (SHA-1))	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Message Digest (SHA-256) (Tiivistealgoritmi (SHA-256))	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Cryptographic algorithms (Salausta käyttävät algoritmit)	SHA-1/RSA 4096

b) SHA-256 -varmenne:

Distinguished name (DN-nimi)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Sarjanumero)	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8

([1]) Tätä varmennetta käytetään vain järjestelmissä, jotka eivät tue korkeampia algoritmejä.

Distinguished name of issuer (Yksilöivä nimi)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Voimassaoloaika)	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
Message digest (SHA-1) (Tiivistealgoritmi (SHA-1))	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message Digest (SHA-256) (Tiivistealgoritmi (SHA-256))	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Cryptographic algorithms (Salausta käyttävät algoritmit)	SHA-256/RSA 4096

— **EKPJ-PKI:n online-varmentaja**: Tämä varmentaja toimii varmennushierarkian toiseksi ylimmällä tasolla EKPJ-PKI:n juurivarmentajan alaisuudessa. Se vastaa EKPJ-PKI:n varmenteiden luomisesta käyttäjille. Tärkeimmät sitä koskevat tiedot ovat seuraavat:

a) SHA-1 -varmenne ([1]):

Distinguished name (DN-nimi)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Sarjanumero)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished name of Issuer (Yksilöivä nimi)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Voimassaoloaika)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (SHA-1) (Tiivistealgoritmi (SHA-1))	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Message Digest (SHA-256) (Tiivistealgoritmi (SHA-256))	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Cryptographic algorithms (salausta käyttävät algoritmit)	SHA-1/RSA 4096

b) SHA-256 -varmenne:

Distinguished name (DN-nimi)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Sarjanumero)	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
Distinguished name of Issuer (Yksilöivä nimi)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Voimassaoloaika)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (SHA-1) (Tiivistealgoritmi (SHA-1))	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
Message Digest (SHA-256) (Tiivistealgoritmi (SHA-256))	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
Cryptographic algorithms (Salausta käyttävät algoritmit)	SHA-256/RSA 4096”

([1]) Tätä varmennetta käytetään vain järjestelmissä, jotka eivät tue korkeampia algoritmejä.