Euroopan unionin
virallinen lehti

FI
L-sarja

2024/2683

15.10.2024

EUROOPAN KESKUSPANKIN PÄÄTÖS (EU) 2024/2683,

annettu 8 päivänä lokakuuta 2024,

Euroopan keskuspankkijärjestelmässä käytettävää julkisen avaimen infrastruktuuria koskevien periaatteiden vahvistamisesta annetun päätöksen EKP/2013/1 muuttamisesta *(EKP/2024/26)*

EUROOPAN KESKUSPANKIN NEUVOSTO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 127 artiklan ja 132 artiklan 1 kohdan,

ottaa huomioon Euroopan keskuspankkijärjestelmän ja Euroopan keskuspankin perussäännön ja erityisesti sen 12.1 artiklan, luettuna yhdessä sen 3.1, 12.3 ja 34 artiklan kanssa,

sekä katsoo seuraavaa:

(1) Euroopan keskuspankin päätöksellä EKP/2013/1 ([1]) vahvistettiin eurojärjestelmässä käytettävän julkisen avaimen infrastruktuurin (jäljempänä 'EKPJ-PKI') periaatteet, joiden tarkoituksena on säännellä sellaisten digitaalisten varmenteiden liikkeeseenlaskua ja hallinnointia, joita tarvitaan sellaisiin EKPJ:n ja eurojärjestelmän sähköisiin sovelluksiin, järjestelmiin, alustoihin ja palveluihin pääsyä varten, joiden kriittisyys on keskitasoa tai korkeampi, ja niiden käyttöä varten.

(2) EKPJ-PKI:n käyttämä teknologia on elinkaarensa päässä, ja se on korvattu. Sen vuoksi on tarpeen ottaa käyttöön uusi EKPJ-PKI:n online-varmentaja (jäljempänä 'EKPJ-PKI:n online-varmentaja V1.2'), jonka tulisi myös ottaa huomioon se, että EKPJ:n käyttäjille ja EKPJ:n ulkopuolisille käyttäjille annettujen varmenteiden kolmen vuoden pituinen voimassaolo sekä EKPJ-PKI:n online-varmentajaan liittyvien teknisten komponenttien käytettävyys eivät voi päättyä myöhemmin kuin EKPJ-PKI:n online-varmentajan itsensä varmenne. EKPJ-PKI:n online-varmentajan nykyisen varmenteen voimassaolo päättyy 22 päivänä heinäkuuta 2026, minkä jälkeen EKPJ-PKI:n online-varmentaja V1.2 olisi ainoa EKPJ-PKI:n online-varmentaja, kunnes sen varmenteen voimassaolo päättyy.

(3) Näin ollen päätös EKP/2013/1 olisi muutettava vastaavasti,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Muutos

Korvataan suuntaviivojen EKP/2013/1 liite tämän päätöksen liitteellä.

2 artikla

Voimaantulo

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

Tehty Frankfurt am Mainissa 8 päivänä lokakuuta 2024.

EKP:n puheenjohtaja
Christine LAGARDE

([1]) 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).

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 kolmesta teknisestä komponentista:

1. **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:

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
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

2. **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. Sen voimassaolo päättyy 22 päivänä heinäkuuta 2026. Tärkeimmät sitä koskevat tiedot ovat seuraavat:

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

3. **EKPJ-PKI:n online-varmentaja V1.2**: Tämä varmentaja toimii varmennushierarkian toiseksi ylimmällä tasolla EKPJ-PKI:n juurivarmentajan alaisuudessa. Se vastaa EKPJ-PKI:n varmenteiden luomisesta käyttäjille. Se on heinäkuun 22 päivän 2026 jälkeen ainoa EKPJ-PKI:n online-varmentaja voimassaolonsa päättymiseen asti. Tärkeimmät sitä koskevat tiedot ovat seuraavat:

Distinguished name (DN-nimi)	CN = ESCB-PKI ONLINE CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (Sarjanumero)	1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653
Distinguished name of Issuer (Yksilöivä nimi)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (Voimassaoloaika)	From 08-06-2023 17:07:00 to 08-06-2038 17:07:00
Message digest (SHA-1) (Tiivistealgoritmi (SHA-1))	DC92 042E 6316 CB60 F8F6 109B 8C43 F3C6 AF2F B2F3
Message Digest (SHA-256) (Tiivistealgoritmi (SHA-256))	96B7 8E9C F914 ED4D 072D 93C8 C531 DEEF D102 7571 7218 A202 0924 3216 99D8 1C48
Cryptographic algorithms (Salausta käyttävät algoritmit)	SHA-256/RSA 4096”