

PÄÄTÖKSET

EUROOPAN KESKUSPANKIN PÄÄTÖS,

annettu 11 päivänä tammikuuta 2013,

Euroopan keskuspankkijärjestelmässä käytettävää julkisen avaimen infrastruktuuria koskevien periaatteiden vahvistamisesta

(EKP/2013/1)

(2013/132/EU)

EUROOPAN KESKUSPANKIN NEUVOSTO, joka

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

ottaa huomioon Euroopan keskuspankkijärjestelmän ja Euroopan keskuspankin perussäännön (jäljempänä 'EKP:n perussääntö') ja erityisesti sen 12.1 artiklan yhdessä 3.1, 5, 12.3 ja 16–24 artiklan kanssa,

sekä katsoo seuraavaa:

- (1) EKP:n perussäännön 12.1 artiklan mukaan EKP:n neuvosto antaa suuntaviivat ja tekee tarvittavat päätökset varmistaakseen Euroopan keskuspankkijärjestelmälle (EKPJ) ja eurojärjestelmälle perussopimuksen ja EKPJ:n perussäännön nojalla annettujen tehtävien suorittamisen. Tähän kuuluu toimivalta päättää kyseisten tehtävien suorittamisen kannalta tarpeellisen avustavan toiminnan järjestämisestä, kuten EKPJ:n ja eurojärjestelmän sovelluksissa, järjestelmissä, alustoissa ja palveluissa tallennettujen ja käsiteltyjen tietojen turvaamiseksi annettavien digitaalisten varmenteiden luomisesta ja hallinnoinnista, sekä näihin liittyvän tiedonkulun järjestämiseksi.
- (2) EKPJ:n perussäännön 12.3 artiklan mukaan EKP:n neuvostolla on lisäksi toimivalta määrittää Euroopan keskuspankin (EKP) ja sen päätöksentekuelinten sisäinen organisaatio. Näin ollen EKP:n neuvostolla on toimivalta päättää siitä, että EKP käyttää eurojärjestelmän oman julkisen avaimen infrastruktuurin luomia digitaalisia varmenteita.
- (3) EKPJ:n ja eurojärjestelmän jatkuvasti kehittyvien ja lisääntyvien sovellusten, järjestelmien, alustojen ja palvelujen käyttäjämäärä on kasvussa. EKP:n neuvosto katsoo, että on tarpeen ottaa käyttöön kehittyneempiä tietoturvapalveluja, kuten vahva todentaminen, sähköinen allekirjoitus ja salaaminen, digitaalisia varmenteita käyttäen.
- (4) Vain muutamilla EKPJ:n keskuspankeista on oma julkisen avaimen infrastruktuuri, ja harvoilla kolmansina osapuolina olevilla käyttäjillä, jotka toimivat yhteistyössä EKPJ:n keskuspankkien kanssa, on helppo pääsy EKPJ:n varmenteiden hyväksymisperiaatteidensa (ESCB certificate acceptance framework) mukaan hyväksymään varmentajaan.
- (5) Eurojärjestelmä tarvitsee oman julkisen avaimen infrastruktuurin, joka voi luoda kaiken tyyppisiä digitaalisia varmenteita, kuten henkilökohtaisia ja teknisiä varmenteita, EKPJ:lle ja EKPJ:n ulkopuolisille käyttäjille, ja joka on tarpeeksi joustava mukautuakseen EKPJ:n ja eurojärjestelmän sovellusten, järjestelmien, alustojen ja palvelujen kehitykseen. Tämän julkisen avaimen infrastruktuurin (jäljempänä 'EKPJ-PKI' tai 'ESCB-PKI') olisi täydennettävä muita sellaisten varmentajien tarjoamia palveluja, jotka EKPJ on hyväksynyt EKPJ:n varmenteiden hyväksymisperiaatteiden mukaan tai TARGET2:ta ja TARGET2-Securities-ohjelmaa varten.
- (6) EKP:n neuvosto päätti 29 päivänä syyskuuta 2010 käynnistää EKPJ-PKI:tä koskevan hankkeen, jolla luodaan ja pannaan täytäntöön EKPJ-PKI, sekä osoittaa sille resurssit, jotka ovat tarpeen hankkeen loppuun saattamiseksi. Se päätti, että Banco de España kehittää, isännöi ja operoi EKPJ-PKI:tä.
- (7) EKPJ-PKI tukee välillisesti EKPJ:n ja eurojärjestelmän tehtävien suorittamista. Sitä hallinnoidaan kolmella tasolla: EKP:n neuvosto ja johtokunta muodostavat tason 1, eurojärjestelmän keskuspankit tason 2 ja julkisen avaimen tarjoava keskuspankki tason 3.
- (8) Tasolla 1 EKP:n neuvosto on vastuussa EKPJ-PKI:n kehittämiseen ja operointiin tarvittavien toimintojen ja tuotteiden ohjaamisesta, hallinnosta ja kontrolloimisesta. Se on myös vastuussa EKPJ-PKI:tä koskevasta päätöksenteosta ja päättää niiden tehtävien kohdentamisesta, joita ei erityisesti ole osoitettu tasoille 2 ja 3.
- (9) Eurojärjestelmän keskuspankit ovat vastuussa tason 2 tehtävien suorittamisesta EKP:n neuvoston määrittelemiä yleisten periaatteiden mukaisesti. Niillä on toimivalta sen osalta, miten EKPJ-PKI pannaan teknisesti täytäntöön.

- (10) EKPJ:n tietotekniikkakomitea ohjaa EKPJ-PKI:n kehittämistä. Se johtaa, arvioi ja kontrolloi sekä hyväksyy hankkeen tuotteet hyväksymiskriteerien mukaisesti EKPJ:n varmenteen hyväksymisperiaatteiden sekä EKP:n neuvoston hyväksymän laajuuden ja aikataulun perusteella.
- (11) Tasolla 3 Banco de España on nimitetty EKPJ-PKI:n tarjoavaksi keskuspankiksi, joka suorittaa EKP:n neuvoston määrittelemissä yleisissä periaatteissa sille osoitetut tehtävät. EKPJ-PKI:n tarjoava keskuspankki on ottanut käyttöönsä teknisen infrastruktuurin sekä turvalliset laitteet ja palvelut, joita tarvitaan julkisen avaimen luomiseksi ja käyttämiseksi seuraavien säädösten mukaan: a) sähköisiä allekirjoituksia koskevista yhteisön puitteista 13 päivänä joulukuuta 1999 annetun Euroopan parlamentin ja neuvoston direktiivin 1999/93/EY⁽¹⁾ täytäntöönpaneva kansallinen lainsäädäntö, soveltuvin osin; b) yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY⁽²⁾ täytäntöönpaneva kansallinen lainsäädäntö, soveltuvin osin; c) yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18 päivänä joulukuuta 2000 annettu Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001⁽³⁾.
- (12) Digitaaliset varmenteet ovat olennaisen tärkeitä käytettävissä sovelluksia sekä todentamismekanismina sähköisten allekirjoitusten täytäntöönpanemiseksi että julkiseen avaimen pohjautuvassa salauksessa. Tästä syystä EKPJ-PKI:ssä otetaan huomioon jo olemassa olevat EKPJ:n ja eurojärjestelmän sovellukset, järjestelmät, alustat ja palvelut sekä tämänhetkiset EKPJ:n hankkeet, millä varmistetaan siitä, että näiden kaikkien tarpeet otetaan huomioon.
- (13) Euroalueen ulkopuoliset kansalliset keskuspankit voivat päättää käyttää EKPJ-PKI:n luomia varmenteita ja tarjoamia palveluita,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Määritelmät

Tässä päätöksessä tarkoitetaan:

- 'varmenteella' tai 'digitaalisella varmenteella' varmentajan luomaa sähköistä tiedostoa, joka kytkee julkisen avaimen tiettyyn varmenteen haltijaan ja jota käytetään kaikkiin tai johonkin seuraavista: a) vahvistamaan julkisen avaimen kuuluminen tietylle varmenteen haltijalle; b) todentamaan varmenteen haltija; c) tarkastamaan varmenteen haltijan allekirjoitus; d) salaamaan varmenteen haltijalle osoitettu sanoma; e) vahvistamaan varmenteen haltijan käyttöoikeus EKPJ:n ja eurojärjestelmän sovelluksiin, järjestelmiin, alus-

toihin ja palveluihin. Kaikki tässä päätöksessä olevat viittaukset varmenteeseen tai digitaaliseen varmenteeseen viittavat myös tietovälineisiin, joissa varmennetta tai digitaalista varmennetta säilytetään;

- 'EKPJ:n ja eurojärjestelmän sovelluksilla, järjestelmillä, alustoilla ja palveluilla' niitä sovelluksia, järjestelmiä, laitealustoja ja IT-palveluita, joita EKPJ ja/tai eurojärjestelmä käyttävät suorittaessaan niille perussopimuksen ja EKPJ:n perussäännön nojalla annettuja tehtäviä;
- 'julkisen avaimen infrastruktuurilla' sitä yksilöiden, menettelytapojen, menetelmien ja tietokonejärjestelmien muodostamaa kokonaisuutta, joka on tarpeen todentamista, salaamista, eheyttä ja kiistattomuutta koskevien palveluiden tarjoamiseksi käyttämällä julkiseen ja yksityiseen avaimen perustuvaa salausta sekä digitaalisia varmenteita;
- 'käyttäjällä' varmenteen haltijaa tai varmenteeseen luottavaa osapuolta taikka molempia;
- 'todentamisella' varmenteen hakijan tai varmenteen haltijan henkilöllisyyden vahvistamisessa käytettävää menettelyä;
- 'EKPJ:n keskuspankilla' eurojärjestelmän keskuspankkia tai euroalueen ulkopuolista kansallista keskuspankkia;
- 'eurojärjestelmän keskuspankilla' sellaisen jäsenvaltion kansallista keskuspankkia, jonka rahayksikkö on euro, EKPJ-PKI:n tarjoava keskuspankki mukaan lukien, tai EKP:tä;
- 'EKPJ-PKI:n tarjoavalla keskuspankilla' EKP:n neuvoston nimitettävää kansallista keskuspankkia, joka huolehtii EKPJ-PKI:n kehittämisestä ja EKPJ-PKI:n palveluiden tarjoamisesta eurojärjestelmän keskuspankkien puolesta ja hyväksi;
- 'euroalueen ulkopuolisella kansallisella keskuspankilla' sellaisen jäsenvaltion kansallista keskuspankkia, jonka rahayksikkö ei ole euro;
- 'EKPJ-PKI:n varmentajalla' luotettua tahoa, joka luo, hallinnoi, sulkee ja uusii varmenteita EKPJ:n keskuspankkien tai eurojärjestelmän keskuspankkien puolesta EKPJ:n varmenteen hyväksymisperiaatteiden mukaisesti;
- 'EKPJ-PKI:n vahvistajalla' luotettua tahoa, joka tarjoaa tietoa EKPJ-PKI:n varmentajan luomien varmenteiden oikeellisuudesta;
- 'varmenteen haltijalla' luonnollista henkilöä, jota varmenne edustaa ja jolle on annettu digitaalinen varmenne, tai teknisen komponentin hallinnoijaa, joka on hyväksynyt EKPJ-PKI:n varmentajan tekniselle komponentille luoman digitaalisen varmenteen, taikka molempia;
- 'EKPJ:n varmenteen hyväksymisperiaateilla' (ESCB certificate acceptance framework) EKPJ:n tietotekniikkakomitean laatimia kriteerejä, joilla tunnustetaan sellaiset sekä EKPJ:n

⁽¹⁾ EYVL L 13, 19.1.2000, s. 12.

⁽²⁾ EYVL L 281, 23.11.1995, s. 31.

⁽³⁾ EYVL L 8, 12.1.2001, s. 1.

sisäiset että ulkopuoliset varmentajat, joihin EKPJ:n ja eurojärjestelmän sovellukset, järjestelmät, alustat ja palvelut voivat luottaa;

14. 'rekisteröijällä' luotettua tahoja, joka vahvistaa varmenteen hakijan henkilöllisyyden ennen kuin EKPJ-PKI:n varmentaja luovuttaa varmenteen;
15. 'varmenteeseen luottavalla osapuolella' varmenteen hyväksyvää ja siihen luottavaa muuta luonnollista henkilöä tai yhteisöä kuin varmenteen haltijaa;
16. 'sisäisen tarkastuksen periaatteilla' EKP:n verkkosivuilla⁽¹⁾ julkaistuja EKP:n neuvoston 7 päivänä lokakuuta 1998 antamia EKPJ:n sisäisen tarkastuksen periaatteita;
17. 'varmenteen hakijalla' luonnollista henkilöä, joka hakee varmennetta tai teknistä komponenttia itselleen;
18. 'teknisellä komponentilla' ohjelmistoja tai laitteita, jotka voidaan yksilöidä käyttämällä digitaalisia varmenteita.

2 artikla

Soveltamisala

1. Tällä päätöksellä luodaan EKPJ-PKI:tä koskevat periaatteet. EKPJ-PKI on eurojärjestelmän omistama julkisen avaimen infrastruktuuri, jonka EKPJ-PKI:n tarjoava keskuspankki, joka luo, hallinnoi, sulkee ja uusii varmenteet EKPJ:n varmenteen hyväksymisperiaatteiden mukaisesti, on kehittänyt eurojärjestelmän keskuspankkien puolesta ja hyväksi.
2. Koska EKPJ-PKI:n palvelut saattavat vaikuttaa varmenteeseen luottaviin osapuoliin, säädetään tällä päätöksellä myös ehtoista, joiden täyttyessä tällaiset osapuolet voivat luottaa EKPJ-PKI:n varmenteisiin.

3 artikla

EKPJ-PKI:n soveltamisala ja tavoitteet

1. EKPJ:n ja eurojärjestelmän sovelluksia, järjestelmiä, alustoja ja palveluita, joiden kriittisyys on keskitasoa tai korkeampi, voidaan käyttää ja niihin voidaan päästä vain, jos käyttäjä on todennettu sellaisen varmentajan luomalla ja hallinnoimalla varmenteella, jonka EKPJ on hyväksynyt EKPJ:n varmenteen hyväksymisperiaatteiden mukaisesti, mukaan lukien EKPJ-PKI:n varmentaja, tai jonka EKPJ on hyväksynyt TARGET2:ta ja TARGET2-Securities-ohjelmaa varten.
2. EKPJ-PKI:n varmentaja luo digitaaliset varmenteet ja tarjoaa muut digitaalisen varmenteen palvelut EKPJ:n keskuspankkien tai niiden kanssa työskentelevien kolmansien osapuolien varmenteen haltijoille, jotta näillä on turvattu pääsy ja käyttöoikeus EKPJ:n ja eurojärjestelmän sovelluksiin, järjestelmiin, alustoihin ja palveluihin.

3. EKPJ-PKI tarjoaa seuraavia varmennepalveluita:

- a) varmenteen luominen ja luovuttaminen, uusiminen ja sulkeminen sekä varmenteen voimassaolon vahvistaminen eri varmennetyyppien osalta;
- b) varmenteiden luominen todentamiseen, sähköiseen allekirjoittamiseen ja salaamiseen EKPJ:n käyttäjille ja EKPJ:n ulkopuolisille käyttäjille sekä teknisten varmenteiden luominen;
- c) yksityisen avaimen palauttaminen; tämä mahdollistaa julkiseen avaimen perustuvan salatun tiedon palauttamisen varmenteen katoamistapauksissa;
- d) tarvittaessa salaamisvälineiden hallinnointi ja toimittaminen varmenteen haltijoille;
- e) tietojen antaminen EKPJ-PKI:n varmenteen hallinnointimenettelyä koskevista säännöistä sekä sellaisen teknisen tuen antaminen EKPJ:n projektipäälliköille, jolla autetaan heitä integroimaan EKPJ-PKI:n varmenteet sovelluksiinsa.

Tulevaisuudessa voidaan lisätä muita palveluita EKPJ:n ja eurojärjestelmän sovellusten, järjestelmien, alustojen ja palveluiden tarpeiden mukaan.

4 artikla

EKPJ-PKI:n periaatteet

1. EKPJ-PKI:n tarjoavan keskuspankin ja muiden eurojärjestelmän keskuspankkien EKPJ-PKI:n täytäntöönpanoon, toimintaan ja käyttöön liittyvät velvollisuudet ja toiminnot määritellään tasojen 2 ja 3 välisessä sopimuksessa ja ne tarkennetaan EKPJ-PKI:n varmennuspolitiikassa ja EKPJ-PKI:n varmentamisen menettelytapakuvauksessa, jollei tästä päätöksestä muuta johdu.
2. Tasojen 2 ja 3 väliseen sopimukseen kuuluu palvelutasosopimus ja se sisältää EKPJ-PKI:n tarjoavan keskuspankin ja eurojärjestelmän keskuspankkien välisen sopimuksen niiden velvollisuuksista ja toiminnoista. Tasojen 2 ja 3 välinen sopimus toimitetaan hyväksyttäväksi EKP:n neuvostolle, jonka jälkeen EKPJ-PKI:n tarjoava keskuspankki ja eurojärjestelmän keskuspankit allekirjoittavat sen.
3. Palvelutasosopimuksessa määritellään toisaalta niiden EKPJ-PKI:hin liittyvien palvelujen taso, jotka EKPJ-PKI:n tarjoava keskuspankki tarjoaa eurojärjestelmälle, ja toisaalta niiden EKPJ-PKI:hin liittyvien palvelujen taso, jotka eurojärjestelmä tarjoaa euroalueen ulkopuolisille kansallisille keskuspankeille ja kolmansille osapuolille.
4. EKPJ-PKI:n varmentamisen menettelytapakuvaus on sääntökokonaisuus, joka kattaa sähköisten allekirjoitusten koko elinkaaren ensimmäisestä hakemuksesta käytön päättymiseen tai peruuttamiseen sekä varmenteen hakijan tai haltijan, EKPJ-PKI:n varmentajan ja varmenteeseen luottavan osapuolen väliset suhteet. Sitä sovelletaan direktiivin 1999/93/EY soveltamisalaan kuuluviin sähköisiin allekirjoituksiin ja direktiivin soveltamisalan ulkopuolisiin sähköisiin allekirjoituksiin. 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.

⁽¹⁾ www.ecb.europa.eu

5. EKPJ-PKI:n varmennuspolitiikka on sääntökokonaisuus, joka soveltuu jokaiseen annettuun varmennetyypin. Kukin sääntökokonaisuus koskee EKPJ-PKI:n varmentamisen menettelytapakuvausten täytäntöönpanoyksityiskohtia kunkin annettavan varmennetyypin osalta. EKPJ-PKI:n varmennuspolitiikka on tasojen 2 ja 3 välisen sopimuksen liitteenä.

6. EKPJ-PKI:n varmennuspolitiikka ja EKPJ-PKI:n varmentamisen menettelytapakuvaus julkaistaan EKPJ-PKI:n verkkosivulla⁽¹⁾.

7. EKPJ-PKI:n varmentajaa, sen tunniste mukaan luettuna, ja sen teknisiä komponentteja koskevat tiedot esitetään tämän päätöksen liitteessä.

5 artikla

EKPJ-PKI:n tarjoavan keskuspankin toimivalta ja tehtävät

1. EKPJ-PKI:n tarjoava keskuspankki vastaa EKPJ-PKI:n ope-roinnista ja ylläpidosta eurojärjestelmän keskuspankkien hyväk-si, mukaan lukien sen isännöinti, operointi ja hallinnointi, joita suoritetaan tasojen 2 ja 3 välisen sopimuksen mukaisesti. EKPJ-PKI:n tarjoava keskuspankki toimittaa erityisesti varmenteita ja suorittaa EKPJ-PKI:n liittyviä palveluja liiketoiminnan vaatimusten ja teknisten eritelmien mukaisesti, kuten EKPJ:n varmenteen hyväksymisperiaatteiden ja tasojen 2 ja 3 välisessä sopimuksessa vahvistettujen vaatimusten ja eritelmien mukaisesti.

2. EKPJ-PKI:n tarjoava keskuspankki perustaa organisaation, jota tarvitaan varmenteiden luomista, jakelua ja hallinnointia varten, ja varmistaa, että tätä infrastruktuuria pidetään yllä. Tätä tarkoitusta varten EKPJ-PKI:n tarjoava keskuspankki voi tietotekniikkakomiteaa kuultuaan hyväksyä sisäistä organisaatio-taan ja hallintoaan koskevia sääntöjä.

3. EKPJ-PKI:n tarjoava keskuspankki toimii EKPJ-PKI:n varmentajana ja EKPJ-PKI:n vahvistajana.

4. Tasojen 2 ja 3 välisessä sopimuksessa vahvistetaan EKPJ-PKI:n tarjoavaan keskuspankkiin sovellettavat vastuuperusteet.

6 artikla

Eurojärjestelmän keskuspankkien toimivalta ja tehtävät

1. Kukin eurojärjestelmän keskuspankki on vastuussa omien varmenteen haltijoidensa tunnistamisesta. Se perustaa tätä tehtävää hoitamaan rekisterinpitäjän, jolla on toimivalta rekisteröidä kolmansina osapuolina olevat käyttäjät.

2. Kukin eurojärjestelmän keskuspankki toimii varmenteesen luottavana osapuolena niiden salausta ja sähköistä allekirjoitusta koskevien varmenteiden osalta, joita EKPJ-PKI luo eurojärjestelmän muille keskuspankeille tai kolmansissa osapuolissa oleville varmenteen haltijoille.

3. Kukin EKPJ-PKI:n palveluja käyttävä eurojärjestelmän keskuspankki toimii rekisteröijänä varmenteen hakijoihin nähden ja varmistaa, että varmenteen hakijat hyväksyvät käyttöehdot ja soveltavat niitä; käyttöehdot on vahvistettu EKPJ-PKI:n varmentajan palveluja koskevassa hakulomakkeessa.

7 artikla

Eurojärjestelmän keskuspankkien, kolmansien osapuolten ja varmenteen haltijoiden väliset suhteet

Kukin eurojärjestelmän keskuspankki huolehtii järjestelyistä, jotka koskevat kolmansien osapuolten turvattua pääsyä EKPJ:n ja eurojärjestelmän sovelluksiin, järjestelmiin, alustoihin ja palveluihin ja niiden suojattua käyttöä EKPJ-PKI:n varmenteiden käytön avulla. Nämä järjestelyt koskevat yksinomaan asianomaisen eurojärjestelmän keskuspankin ja EKPJ-PKI:n varmenteita käyttävien kolmansien osapuolten välistä suhdetta. Kaikkien kolmansien osapuolten on noudatettava EKPJ-PKI:n varmennuspolitiikkaa, EKPJ-PKI:n varmentamisen menettelytapakuvausta ja käyttöehtoja, jotka vahvistetaan EKPJ-PKI:n varmentajan palveluja koskevassa hakulomakkeessa.

8 artikla

Suhteet varmenteeseen luottaviin osapuoliin

Tämän päätöksen nojalla annettua digitaalista varmennetta voi käyttää sillä edellytyksellä, että varmenteeseen luottava osapuoli

- vahvistaa varmenteen voimassaolon, sekä sen, ettei varmenteen käyttöä ole keskeytetty tai ettei varmennetta ole suljettu käyttämällä voimassa olevia sulkutietoja;
- noudattaa kaikkia varmenteessa yksilöityjä käyttörajoituksia; ja
- hyväksyy EKPJ-PKI:n varmentamisen menettelytapakuvausten ja sovellettavat EKPJ-PKI:n varmennuspolitiikat.

9 artikla

Oikeudet EKPJ-PKI:hin

1. EKPJ-PKI on kokonaan eurojärjestelmän keskuspankkien omistuksessa.

2. Tämän vuoksi EKPJ-PKI:n tarjoavan keskuspankin on annettava eurojärjestelmän keskuspankeille, siinä määrin kuin se on sovellettavan lainsäädännön mukaan mahdollista, kaikki lisenssit, jotka koskevat immateriaalioikeuksia, joita tarvitaan, jotta eurojärjestelmän keskuspankit kykenevät käyttämään EKPJ-PKI:tä ja sen komponentteja ja kaikkia EKPJ-PKI:n palveluja, ja tarjottava myös EKPJ-PKI:n palveluja kolmansille osapuolille EKPJ-PKI:n varmentamisen menettelytapakuvausten ja EKPJ-PKI:n varmennuspolitiikan mukaisesti. EKPJ-PKI:n tarjoava keskuspankki ottaa kantaakseen vastuun eurojärjestelmän keskuspankeille osoitetuista kolmansien osapuolten korvausvaateista, jotka liittyvät tällaisten immateriaalioikeuksien loukkaamiseen.

3. Eurojärjestelmän keskuspankkien oikeudet EKPJ-PKI:hin määritellään yksityiskohtaisemmin tasojen 2 ja 3 välillä tasojen 2 ja 3 välisessä sopimuksessa.

10 artikla

Eurojärjestelmän keskuspankkien vastuu käyttäjiä kohtaan

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

⁽¹⁾ <http://pki.escb.eu>

hyväksytyyn varmenteeseen, sellaisena kuin se on määritelty direktiivissä 1999/93/EY, siltä osin kuin kyseessä on

- a) hyväksytyyn varmenteeseen sisältyvien tietojen oikeellisuus varmenteen luomishetkenä ja se, sisältääkö varmenne kaikki hyväksytyyn varmenteeseen, sellaisena kuin se on määritelty direktiivissä 1999/93/EY, osalta säädetyt yksityiskohtaiset tiedot;
- b) sen varmistaminen, että hyväksytyyn varmenteen luomishetkellä siinä yksilöidyllä varmenteen haltijalla oli allekirjoituksen luomiseen käytettävät tiedot, jotka vastasivat annettuja tai varmenteessa yksilöityjä allekirjoituksen vahvistamiseen käytettäviä tietoja;
- c) sen varmistaminen, että allekirjoituksen luova laite ja allekirjoituksen vahvistava laite täydentävät toisiaan, jos EKPJ-PKI luo molemmat välineet; tai
- d) mikä tahansa hyväksytyyn varmenteeseen sulkemiseen liittyvä virhe.

2. Eurojärjestelmän keskuspankit eivät anna sitoumuksia eivätkä takuita eivätkä hyväksy vahingonkorvausvastuuta käyttäjiin nähden, ellei siitä nimenomaisesti säädetä tässä päätöksessä ja EKPJ-PKI:n varmennuspolitiikassa.

11 artikla

Euroalueen ulkopuolisten kansallisten keskuspankkien osallistuminen EKPJ-PKI:hin

1. Euroalueen ulkopuolinen kansallinen keskuspankki voi toimia rekisteröijänä sisäisiin käyttäjiinsä nähden samoin kuin kolmansina osapuolina oleviin käyttäjiin nähden, ja se voi perustaa rekisterinpitäjän suorittamaan tämän toimen.

2. Euroalueen ulkopuolinen kansallinen keskuspankki voi EKP:n neuvoston suostumuksella myös päättää käyttää EKPJ-PKI:n palveluja samoin edellytyksin kuin eurojärjestelmän keskuspankit. Tätä tarkoitusta varten euroalueen ulkopuolisen kansallisen keskuspankin on toimitettava EKP:n neuvostolle ilmoitus, jossa se vahvistaa noudattavansa tässä päätöksessä ja tasojen 2 ja 3 välisessä sopimuksessa määrättyjä velvoitteita. Euroalueen ulkopuolisesta kansallisesta keskuspankista ei tule EKPJ-PKI:n yhteisomistajaa, eikä se ole velvollinen suorittamaan maksuja EKPJ-PKI:n rahoituskehityksen mukaisesti.

12 artikla

Tietosuojaja

Eurojärjestelmän keskuspankit noudattavat sovellettavaa tietosuojalainsäädäntöä käsitellessään henkilötietoja EKPJ-PKI:hin liittyviä tehtäviä hoitaessaan.

13 artikla

Tarkastukset

EKPJ-PKI:n tarkastukset suoritetaan sisäisen tarkastuksen periaatteissa vahvistettujen periaatteiden ja järjestelyjen mukaisesti. Ne eivät vaikuta eurojärjestelmän keskuspankkeihin sovellettaviin tai niiden hyväksymiin sisäisiin tarkastuksiin ja sisäisen tarkastuksen periaatteisiin.

14 artikla

Rahoitusjärjestelyt

Eurojärjestelmän keskuspankit vastaavat EKPJ-PKI:n kehittämistä ja toimintakuluista siten kuin EKPJ-PKI:n rahoituskehityksessä tarkemmin määritetään.

15 artikla

EKP:n johtokunnan asema

1. Euroopan keskuspankin työjärjestyksen hyväksymisestä 19 päivänä helmikuuta 2004 tehdyn päätöksen EKP/2004/2⁽¹⁾ 17.3 artiklan mukaisesti EKP:n neuvosto siirtää EKP:n johtokunnalle toimivaltansa toteuttaa kaikki ne toimenpiteet tämän päätöksen täytäntöön panemiseksi, jotka ovat tarpeen EKPJ-PKI:n tehokkuuden ja turvallisuuden kannalta, ja hyväksyä muutoksia, jotka liittyvät EKPJ-PKI:n ja EKPJ-PKI:n palvelujen teknisiin seikkoihin, joista määrätään tasojen 2 ja 3 välisen sopimuksen liitteissä, otettuaan tietotekniikkakomitean ja tarvittaessa eurojärjestelmän tietotekniikan ohjauskomitean näkemykset huomioon.

2. EKP:n johtokunta ilmoittaa EKP:n neuvostolle viipymättä kaikista toimenpiteistä, joita se toteuttaa 1 kohdan nojalla, ja noudattaa kaikkia EKP:n neuvoston tältä osin tekemiä päätöksiä.

Tehty Frankfurt am Mainissa 11 päivänä tammikuuta 2013.

EKP:n puheenjohtaja

Mario DRAGHI

⁽¹⁾ EUVL L 80, 18.3.2004, s. 33.

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) avainparien luomisesta liittyen erityisiin varmenteisiin, esim. varmenteisiin, jotka edellyttävät avaimen toivuttamista; ja
- iv) kokonaisvastuun kantamisesta EKPJ-PKI:n ylläpitämisen osalta sekä varmistaa, että kaikki EKPJ-PKI:n operoinnin edellyttämät vaatimukset täytetään.

EKPJ-PKI:n varmentaja kattaa 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:

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) (Tiivistä algoritmi (SHA-1))	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192

- **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:

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 21-06-2011 11:58:26 to 21-06-2041 11:58:26
Message digest (SHA-1) (Tiivistä algoritmi (SHA-1))	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08