

DECIZII

DECIZIA BĂNCII CENTRALE EUROPENE

din 11 ianuarie 2013

de stabilire a cadrului pentru o infrastructură cu cheie publică pentru Sistemul European al Băncilor Centrale

(BCE/2013/1)

(2013/132/UE)

CONSILIUL GUVERNATORILOR BĂNCII CENTRALE EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 127,

având în vedere Statutul Sistemului European al Băncilor Centrale și al Băncii Centrale Europene (denumit în continuare „Statutul SEBC”), în special articolul 12.1, coroborat cu articolul 3.1, articolul 5, articolul 12.3 și articolele 16-24,

întrucât:

(1) În conformitate cu articolul 12.1 din Statutul SEBC, Consiliul guvernatorilor adoptă orientările și ia deciziile necesare pentru a asigura îndeplinirea misiunilor încredințate Sistemului European al Băncilor Centrale (SEBC) și Eurosistemului în temeiul Tratatului și al Statutului SEBC. Aceasta include competența de a decide asupra organizării activităților auxiliare care sunt necesare pentru îndeplinirea acestor sarcini, precum emiterea și gestionarea certificatelor electronice pentru securizarea informațiilor stocate și prelucrate în aplicațiile, sistemele, platformele și serviciile electronice utilizate în SEBC și Eurosistem, precum și pentru transmiterea de date către și de la acestea.

(2) În conformitate cu articolul 12.3 din Statutul SEBC, Consiliul guvernatorilor are, de asemenea, competența de a stabili organizarea internă a Băncii Centrale Europene (BCE) și a organelor de decizie ale acesteia. În consecință, Consiliul guvernatorilor are competența de a decide că BCE va utiliza certificatele electronice emise de infrastructura cu cheie publică proprie Eurosistemului.

(3) Numărul utilizatorilor care accesează din ce în ce mai multe aplicații, sisteme, platforme și servicii electronice utilizate în SEBC și Eurosistem, aflate în constantă evoluție, este în creștere. Consiliul guvernatorilor a identificat nevoia de servicii avansate de securitate a informațiilor, precum autentificarea bine protejată a utilizatorilor, semnăturile electronice și criptarea, prin utilizarea certificatelor electronice.

(4) Puține bănci centrale din SEBC au propria lor infrastructură cu cheie publică și mulți utilizatori ai unor terți care lucrează împreună cu băncile centrale din SEBC nu au acces facil la o autoritate de certificare acceptată de SEBC în conformitate cu cadrul său de acceptare a certificatelor.

(5) Este necesar ca Eurosistemul să-și creeze propria infrastructură cu cheie publică, care să poată emite toate tipurile de certificate electronice, precum certificate personale și tehnice pentru utilizatori din cadrul sau din afara SEBC, și care să fie suficient de flexibilă pentru a se adapta la evoluțiile aplicațiilor, sistemelor, platformelor și serviciilor electronice utilizate în SEBC și Eurosistem. Această infrastructură cu cheie publică (denumită în continuare „ESBC-PKI”) ar trebui să completeze serviciile furnizate de alte autorități de certificare acceptate de către SEBC în conformitate cu cadrul SEBC de acceptare a certificatelor sau de autoritățile de certificare acceptate de SEBC pentru TARGET2 și TARGET2-Securities pentru aceste două aplicații.

(6) La 29 septembrie 2010, Consiliul guvernatorilor a hotărât să lanseze proiectul ESCB-PKI pentru proiectarea și punerea în aplicare a ESCB-PKI și să ofere resursele necesare până la finalizarea sa. S-a decis ca ESCB-PKI să fie dezvoltată, găzduită și operată de către Banco de España.

(7) ESCB-PKI sprijină indirect îndeplinirea misiunilor SEBC și ale Eurosistemului. Aceasta se bazează pe trei niveluri de guvernare: Nivelul 1 constă din Consiliul guvernatorilor și Comitetul executiv, Nivelul 2 din băncile centrale din Eurosistem, iar Nivelul 3 din banca centrală furnizoare.

(8) La Nivelul 1, Consiliul guvernatorilor este responsabil cu conducerea, administrarea și controlul activităților și produselor necesare pentru dezvoltarea și operarea ESCB-PKI. De asemenea, acesta este responsabil cu procesul decizional în ceea ce privește ESCB-PKI și hotărăște cu privire la distribuirea atribuțiilor nerepartizate în mod expres Nivelurilor 2 și 3.

(9) Băncile centrale din Eurosistem sunt responsabile cu atribuțiile alocate Nivelului 2, în limitele cadrului general definit de Consiliul guvernatorilor. Acestea au competențe cu privire la mijloacele tehnice de punere în aplicare a ESCB-PKI.

- (10) Comitetul pentru tehnologia informației (ITC) al SEBC (ESCB *Information Technology Committee*) are un rol de coordonare în dezvoltarea ESCB-PKI. Acesta ghidează, evaluează, controlează și aprobă produsele proiectului în raport cu criteriile de acceptare, în conformitate cu cadrul SEBC de acceptare a certificatelor, domeniul de aplicare și calendarul aprobate de Consiliul guvernatorilor.
- (11) La Nivelul 3, Banco de España a fost desemnată drept banca centrală furnizoare pentru a îndeplini sarcinile alocate acesteia în cadrul general definit de Consiliul guvernatorilor. Banca centrală furnizoare a implementat infrastructura tehnică și dispozitivele și serviciile securizate necesare pentru crearea și utilizarea unei infrastructuri cu cheie publică, în conformitate cu: (a) legislația națională de transpunere a Directivei 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice ⁽¹⁾, astfel cum este aplicabilă acesteia; (b) legislația națională pentru transpunerea Directivei 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date ⁽²⁾, astfel cum este aplicabilă acesteia; și (c) Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date ⁽³⁾.
- (12) Întrucât certificatele electronice sunt elemente esențiale utilizate în aplicațiile electronice, atât ca mecanism de autentificare pentru implementarea semnăturilor electronice, cât și pentru criptarea cu cheie publică, ESCB-PKI va ține cont de aplicațiile, sistemele, platformele și serviciile electronice existente utilizate în SEBC și Eurosystem, precum și de proiectele actuale ale SEBC, pentru a asigura acoperirea nevoilor acestora.
- (13) Băncile centrale naționale (BCN) din afara zonei euro pot decide să utilizeze certificatele și serviciile furnizate de ESCB-PKI,
- cațiile, sistemele, platformele și serviciile electronice utilizate în SEBC și Eurosystem. Orice trimitere din prezenta decizie la un certificat sau un certificat electronic include o trimitere la dispozitivele de stocare a datelor pe care este păstrat certificatul sau certificatul electronic;
2. „aplicațiile, sistemele, platformele și serviciile electronice utilizate în SEBC și Eurosystem” (*ESCB and Eurosystem electronic applications, systems, platforms and services*) înseamnă aplicațiile, sistemele, platformele și serviciile electronice care sunt utilizate în SEBC și/sau Eurosystem pentru îndeplinirea misiunilor încredințate acestora în temeiul Tratatului și al Statutului SEBC;
3. „infrastructura cu cheie publică” (*public key infrastructure*) înseamnă setul de persoane, politici, proceduri și sisteme computerizate necesare pentru a asigura serviciile de autentificare a utilizatorilor, de criptare, integritate și nerespingere prin intermediul criptării cu cheie publică și privată și al certificatelor electronice;
4. „utilizator” (*user*) înseamnă un deținător de certificat sau un beneficiar, sau ambele;
5. „autentificarea utilizatorilor” (*authentication*) înseamnă procesul de verificare a identității unui solicitant de certificat sau a unui deținător de certificat;
6. „bancă centrală din SEBC” (*ESCB central bank*) înseamnă fie o bancă centrală din Eurosystem, fie o BCN din afara zonei euro;
7. „bancă centrală din Eurosystem” (*Eurosystem central bank*) înseamnă fie o BCN a unui stat membru a cărui monedă este euro, inclusiv banca centrală furnizoare, fie BCE;
8. „bancă centrală furnizoare” (*providing central bank*) înseamnă BCN desemnată de Consiliul guvernatorilor să dezvolte ESCB-PKI și să ofere servicii de ESCB-PKI în numele și beneficiul băncilor centrale din Eurosystem;
9. „BCN din afara zonei euro” (*non-euro area NCB*) înseamnă o BCN a unui stat membru a cărui monedă nu este euro;
10. „autoritatea de certificare pentru ESCB-PKI” (*ESCB-PKI certification authority*) înseamnă entitatea, recunoscută de utilizatori, care emite, administrează, revocă și reînnoiește certificatele în numele băncilor centrale din SEBC sau al băncilor centrale din Eurosystem în conformitate cu cadrul SEBC de acceptare a certificatelor;
11. „autoritatea de validare pentru ESCB-PKI” (*ESCB-PKI validation authority*) înseamnă entitatea, recunoscută de utilizatori, care furnizează informații cu privire la validitatea certificatelor emise de autoritatea de certificare pentru ESCB-PKI;
12. „deținătorul de certificat” (*certificate subscriber*) înseamnă fie o persoană care este subiectul unui certificat electronic și căreia i-a fost emis un certificat electronic, fie un administrator al unei componente tehnice care a acceptat un certificat electronic emis de autoritatea de certificare pentru ESCB-PKI pentru o componentă tehnică, sau ambele;
13. „cadrul SEBC de acceptare a certificatelor” (*ESCB certificate acceptance framework*) înseamnă criteriile stabilite de ITC al SEBC pentru a identifica autoritățile de certificare, atât

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Definiții

În sensul prezentei decizii:

1. „certificat” sau „certificat electronic” (*certificate* sau *electronic certificate*) înseamnă un fișier în format electronic, emis de o autoritate de certificare, care leagă o cheie publică de identitatea unui deținător de certificat și care este folosit pentru toate sau pentru unele dintre următoarele scopuri: (a) pentru a verifica dacă o cheie publică aparține unui deținător de certificat; (b) pentru a autentifica un deținător de certificat; (c) pentru a verifica semnătura unui deținător de certificat; (d) pentru a cripta un mesaj adresat unui deținător de certificat; (e) pentru a verifica drepturile de acces ale unui deținător de certificat la apli-

⁽¹⁾ JO L 13, 19.1.2000, p. 12.

⁽²⁾ JO L 281, 23.11.1995, p. 31.

⁽³⁾ JO L 8, 12.1.2001, p. 1.

- interne cât și externe SEBC, care pot fi recunoscute în ceea ce privește aplicațiile, sistemele, platformele și serviciile electronice utilizate în SEBC și Eurosistem;
14. „autoritatea de înregistrare” (*registration authority*) înseamnă entitatea, recunoscută de utilizatori, care verifică identitatea unui solicitant de certificat înainte ca autoritatea de certificare pentru ESCB-PKI să emită un certificat;
15. „beneficiar” (*relying party*) înseamnă persoana sau entitatea, alta decât deținătorul de certificat, care acceptă și utilizează un certificat;
16. „politica de audit” (*audit policy*) înseamnă politica de audit din SEBC definită de Consiliul guvernatorilor la 7 octombrie 1998, astfel cum este publicată pe website-ul BCE ⁽¹⁾;
17. „solicitantul de certificat” (*certificate applicant*) înseamnă persoana care solicită emiterea unui certificat pentru sine sau pentru o componentă tehnică;
18. „componentă tehnică” (*technical component*) înseamnă orice echipament software sau hardware care poate fi identificat prin utilizarea certificatelor electronice.

Articolul 2

Domeniul de aplicare

- (1) Prezentă decizie stabilește cadrul pentru ESCB-PKI. ESCB-PKI este infrastructura cu cheie publică proprie Eurosistemului dezvoltată de banca centrală furnizoare în numele și beneficiul băncilor centrale din Eurosistem, care emite, administrează, revocă și reînnoiește certificatele în conformitate cu cadrul SEBC de acceptare a certificatelor.
- (2) Întrucât serviciile de ESCB-PKI pot afecta beneficiarii, prezentă decizie stabilește și condițiile în care aceste părți pot utiliza certificatele ESCB-PKI.

Articolul 3

Sfera de aplicare și obiectivele ESCB-PKI

- (1) Aplicațiile, sistemele, platformele și serviciile electronice utilizate în SEBC și Eurosistem care au caracter critic mediu sau peste mediu sunt accesate și utilizate doar dacă un utilizator a fost autentificat prin intermediul unui certificat electronic emis și administrat de o autoritate de certificare acceptată de SEBC în conformitate cu cadrul SEBC de acceptare a certificatelor, inclusiv de autoritatea de certificare pentru ESCB-PKI, sau de autoritățile de certificare acceptate de SEBC pentru TARGET2 și TARGET2 Securities pentru aceste două aplicații.
- (2) Autoritatea de certificare pentru ESCB-PKI emite certificate electronice și furnizează alte servicii de certificare electronică pentru deținătorii de certificate ai băncilor centrale din SEBC și ai terților care lucrează cu acestea pentru a le permite accesul la și utilizarea în mod securizat a aplicațiilor, sistemelor, platformelor și serviciilor electronice utilizate în SEBC și Eurosistem.

- (3) ESCB-PKI furnizează următoarele servicii de certificare:
- (a) emiterea, reînnoirea și revocarea certificatelor și confirmarea validității certificatelor în ceea ce privește diferitele tipuri de certificate;
- (b) emiterea de certificate pentru autentificarea utilizatorilor, semnătura electronică și criptarea în ceea ce privește utilizatorii din SEBC și din afara SEBC, precum și de certificate tehnice;
- (c) recuperarea cheii private pentru a asigura recuperarea informațiilor criptate pe bază de cheie publică în caz de pierdere a certificatului;
- (d) livrarea și administrarea token-urilor criptografice pentru deținătorii de certificate atunci când este necesar;
- (e) furnizarea de informații cu privire la procedurile ESCB-PKI de administrare a certificatelor și de suport tehnic pentru administratorii de proiect din SEBC pentru a îi ajuta să integreze certificatele ESCB-PKI în aplicațiile lor.

Alte servicii pot fi adăugate în viitor dacă aplicațiile, sistemele, platformele și serviciile electronice utilizate în SEBC și Eurosistem o vor impune.

Articolul 4

Cadrul ESCB-PKI

- (1) Sub rezerva dispozițiilor prezentei decizii, responsabilitățile și funcțiile băncii centrale furnizoare și ale altor bănci centrale din Eurosistem în ceea ce privește implementarea, operarea și utilizarea ESCB-PKI sunt stabilite printr-un acord între Nivelul 2-Nivelul 3 și detaliate în politicile ESCB-PKI privind certificatele și declarația de practică privind certificarea în ESCB-PKI.
- (2) Acordul dintre Nivelul 2-Nivelul 3, care include acordul privind nivelul de servicii, cuprinde acordul negociat între banca centrală furnizoare și băncile centrale din Eurosistem cu privire la responsabilitățile și funcțiile băncii centrale furnizoare și ale băncilor centrale din Eurosistem. Acesta va fi depus pentru aprobare Consiliului guvernatorilor și apoi semnat de banca centrală furnizoare și băncile centrale din Eurosistem.
- (3) Acordul privind nivelul de servicii este atât un acord care stabilește nivelul serviciilor care urmează a fi furnizate Eurosistemului de banca centrală furnizoare, cât și un acord care stabilește nivelul serviciilor care urmează a fi furnizate de Eurosistem pentru BCN din afara zonei euro și terților în legătură cu ESCB-PKI.
- (4) Declarația de practică privind certificarea în ESCB-PKI reprezintă un set de reguli care guvernează ciclul de viață al certificatelor electronice, de la solicitarea inițială la încetarea sau revocarea dreptului de utilizare, și relația dintre solicitantul de certificat sau deținătorul de certificat, autoritatea de certificare pentru ESCB-PKI și beneficiari. Aceasta acoperă atât certificatele electronice care intră în sfera de aplicare a Directivei 1999/93/CE, cât și certificatele electronice care nu intră în sfera de aplicare a acestei directive. Totodată, aceasta stabilește rolurile și responsabilitățile tuturor părților și stabilește procedurile pentru emiterea și administrarea certificatelor. Este anexată la acordul dintre Nivelul 2-Nivelul 3.

⁽¹⁾ www.ecb.europa.eu

(5) O politică ESCB-PKI privind certificatele reprezintă un set de reguli aplicabil fiecărui tip de certificate emis. Fiecare set stabilește detaliile pentru implementare referitoare la declarația de practică privind certificarea în ESCB-PKI pentru fiecare tip de certificat emis. Politicile ESCB-PKI privind certificatele sunt anexate la acordul dintre Nivelul 2-Nivelul 3.

(6) Politicile ESCB-PKI privind certificatele și declarația de practică privind certificarea în ESCB-PKI sunt publicate pe website-ul ESCB-PKI ⁽¹⁾.

(7) Informațiile privind autoritatea de certificare pentru ESCB-PKI, inclusiv identitatea acesteia, și componentele tehnice ale acesteia sunt incluse în anexa la prezenta decizie.

Articolul 5

Responsabilitățile și rolurile băncii centrale furnizoare

(1) Banca centrală furnizoare este responsabilă cu operarea și mentenanța ESCB-PKI în beneficiul băncilor centrale din Eurosystem, inclusiv găzduirea, operarea și administrarea acesteia în conformitate cu acordul dintre Nivelul 2-Nivelul 3. În special, aceasta furnizează certificate și servicii ESCB-PKI în conformitate cu cerințele operaționale și specificațiile tehnice, precum cadrul SEBC de acceptare a certificatelor și cerințele și specificațiile prevăzute în acordul dintre Nivelul 2-Nivelul 3.

(2) Banca centrală furnizoare face disponibilă infrastructura organizațională necesară pentru crearea, emiterea și administrarea certificatelor și asigură mentenanța infrastructurii respective. În acest scop, cu consultarea ITC, banca centrală furnizoare poate adopta reguli privind organizarea și administrarea sa internă.

(3) Banca centrală furnizoare acționează drept autoritatea de certificare pentru ESCB-PKI și autoritatea de validare pentru ESCB-PKI.

(4) Acordul dintre Nivelul 2-Nivelul 3 stabilește regimul de răspundere aplicabil băncii centrale furnizoare.

Articolul 6

Responsabilitățile și rolurile băncilor centrale din Eurosystem

(1) Fiecare bancă centrală din Eurosystem este responsabilă cu identificarea deținătorilor săi de certificate. Aceasta creează postul de responsabil cu înregistrarea care să îndeplinească această atribuție și care să aibă autoritatea de a înregistra utilizatori ai terților.

(2) Fiecare bancă centrală din Eurosystem acționează drept beneficiar în legătură cu certificatele pentru criptare și semnătură electronică emise de ESCB-PKI pentru alți deținători de certificate ai băncilor centrale din Eurosystem sau ai utilizatorilor unor terți.

(3) Fiecare bancă centrală din Eurosystem care folosește serviciile ESCB-PKI acționează drept autoritate de înregistrare pentru solicitanții săi de certificate și se asigură că solicitanții săi de certificate acceptă și aplică pentru serviciile sale termenii și condițiile pentru utilizatori prevăzute în modelul de cerere al autorității de certificare pentru ESCB-PKI.

Articolul 7

Relația dintre băncile centrale din Eurosystem, terți și deținătorii de certificate

Fiecare bancă centrală din Eurosystem creează mecanisme pentru accesul și utilizarea în mod securizat de către terți a aplicațiilor, sistemelor, platformelor și serviciilor electronice utilizate în SEBC și Eurosystem prin intermediul utilizării certificatelor ESCB-PKI. Aceste mecanisme guvernează exclusiv relația dintre banca centrală din Eurosystem relevantă și terții care utilizează certificatele ESCB-PKI. Toți terții respectă politicile ESCB-PKI privind certificatele, declarația de practică privind certificarea în ESCB-PKI și termenii și condițiile pentru utilizatori prevăzute în modelul de cerere al autorității de certificare pentru ESCB-PKI pentru serviciile acesteia.

Articolul 8

Relațiile cu beneficiarii

Un certificat electronic emis în temeiul prezentei decizii poate fi utilizat dacă un beneficiar:

- verifică validitatea, suspendarea sau revocarea certificatului prin utilizarea informațiilor curente actualizate referitoare la revocare;
- are în vedere orice limitări aplicabile prevăzute în certificat; și
- acceptă declarația de practică privind certificarea în ESCB-PKI și politicile ESCB-PKI privind certificatele aplicabile.

Articolul 9

Drepturile asupra ESCB-PKI

(1) ESCB-PKI este deținută în totalitate de băncile centrale din Eurosystem.

(2) Având în vedere acest fapt, banca centrală furnizoare acordă băncilor centrale din Eurosystem, în măsura posibilă în temeiul legislației aplicabile, toate licențele privind drepturile de proprietate intelectuală necesare pentru a permite băncilor centrale din Eurosystem să utilizeze ESCB-PKI și componentele acesteia, precum și întreaga gamă de servicii ESCB-PKI, și furnizează servicii ESCB-PKI terților în temeiul declarației de practică privind certificarea în ESCB-PKI și al politicilor ESCB-PKI privind certificatele. Banca centrală furnizoare despăgubește băncile centrale din Eurosystem pentru orice acțiuni privind încălcarea acestor drepturi de proprietate intelectuală introduse de terți.

(3) Detaliile privind drepturile băncilor centrale din Eurosystem asupra ESCB-PKI sunt stabilite între Nivelul 2 și Nivelul 3 prin acordul dintre Nivelul 2-Nivelul 3.

Articolul 10

Răspunderea băncilor centrale din Eurosystem față de utilizatori

(1) Dacă nu dovedesc că nu au acționat cu neglijență, băncile centrale din Eurosystem răspund conform funcțiilor și responsabilităților ce le revin în ESCB-PKI pentru orice daună provocată

⁽¹⁾ <http://pki.escb.eu>

unui utilizator care se bazează în mod rezonabil pe un certificat calificat, astfel cum este definit în Directiva 1999/93/CE, în ceea ce privește:

- (a) acuratețea la momentul emiterii a tuturor informațiilor cuprinse într-un certificat calificat și includerea în acel certificat a tuturor detaliilor prevăzute pentru un certificat calificat, astfel cum este definit în Directiva 1999/93/CE;
- (b) orice asigurare că la momentul emiterii unui certificat calificat, deținătorul certificatului identificat în acel certificat a deținut datele de creare a semnăturii corespunzătoare datelor de verificare a semnăturii prevăzute sau identificate în certificat;
- (c) orice asigurare că dispozitivul de creare a semnăturii și dispozitivul de verificare a semnăturii funcționează împreună în mod complementar, în cazurile în care ESCB-PKI le generează pe amândouă;
- (d) orice eroare în înregistrarea revocării unui certificat calificat.

(2) Băncile centrale din Eurosistem nu își asumă niciun angajament, nu oferă nicio garanție și nu acceptă nicio răspundere față de utilizatori înafara celor prevăzute expres în prezenta decizie și în declarația de practică privind certificarea în ESCB-PKI.

Articolul 11

Participarea BCN din afara zonei euro la ESCB-PKI

(1) O BCN din afara zonei euro poate acționa drept autoritate de înregistrare pentru utilizatorii săi interni precum și pentru utilizatori ai terților și poate crea postul de responsabil cu înregistrarea care să îndeplinească această atribuție.

(2) Cu condiția aprobării de către Consiliul guvernatorilor, o BCN din afara zonei euro poate decide să folosească serviciile ESCB-PKI în condițiile aplicabile băncilor centrale din Eurosistem. În acest scop, o BCN din afara zonei euro transmite Consiliului guvernatorilor o declarație prin care confirmă că va îndeplini obligațiile prevăzute în prezenta decizie și în acordul dintre Nivelul 2-Nivelul 3. O BCN din afara zonei nu devine co-proprietar al ESCB-PKI și nu este obligată să contribuie la pachetul financiar ESCB-PKI.

Articolul 12

Protecția datelor

Băncile centrale din Eurosistem respectă legislația privind protecția datelor aplicabilă procesării de către acestea a datelor personale în cadrul îndeplinirii funcțiilor lor legate de ESCB-PKI.

Articolul 13

Audit

Auditul ESCB-PKI este efectuat conform principiilor și mecanismelor prevăzute în politica de audit. Acestea nu aduc atingere normelor interne de control și de audit care se aplică sau sunt adoptate de băncile centrale din Eurosistem.

Articolul 14

Dispoziții financiare

Băncile centrale din Eurosistem suportă costurile dezvoltării și operării ESCB-PKI astfel cum este detaliat în pachetul financiar ESCB-PKI.

Articolul 15

Rolul Comitetului executiv

(1) Conform articolului 17.3 din Decizia BCE/2004/2 din 19 februarie 2004 de adoptare a Regulamentului de procedură al Băncii Centrale Europene⁽¹⁾, Consiliul guvernatorilor delegă Comitetului executiv competențele sale normative în scopul adoptării oricăror măsuri de punere în aplicare a prezentei decizii și necesare pentru eficiența și securitatea ESCB-PKI și al adoptării modificărilor referitoare la aspectele tehnice ale ESCB-PKI și ale serviciilor ESCB-PKI prevăzute în anexele la acordul dintre Nivelul 2-Nivelul 3 după luarea în considerare a avizelor ITC și, după caz, ale Comitetului director în domeniul IT al Eurosistemului (*Eurosystem IT Steering Committee*).

(2) Comitetul executiv notifică fără întârzieri nejustificate Consiliului guvernatorilor orice măsură adoptată în conformitate cu alineatul (1) și respectă orice decizie a Consiliului guvernatorilor cu privire la această chestiune.

Adoptată la Frankfurt pe Main, 11 ianuarie 2013.

Președintele BCE

Mario DRAGHI

⁽¹⁾ JO L 80, 18.3.2004, p. 33.

ANEXĂ

Informații privind autoritatea de certificare pentru ESCB-PKI, inclusiv identitatea acesteia, și componentele tehnice ale acesteia

Autoritatea de certificare pentru ESCB-PKI este identificată în certificatul acesteia drept emitent, iar cheia privată a acesteia este utilizată pentru a semna certificatele. Autoritatea de certificare pentru ESCB-PKI este responsabilă cu:

- (i) emiterea certificatelor cu cheie privată și publică;
- (ii) emiterea listelor privind revocările;
- (iii) generarea perechilor de chei asociate unor certificate specifice, de exemplu celor care presupun recuperarea cheii;
- (iv) asumarea răspunderii generale pentru ESCB-PKI și asigurarea îndeplinirii tuturor cerințelor pentru operarea acesteia.

Autoritatea de certificare pentru ESCB-PKI include toate persoanele, politicile, procedurile și sistemele computerizate cărora le sunt încredințate emiterea de certificate electronice și atribuirea acestora către deținătorii de certificate.

Autoritatea de certificare pentru ESCB-PKI include două componente tehnice:

- **Autoritatea de certificare root pentru ESCB-PKI** (*Root ESCB-PKI certification authority*): Această autoritate, la primul nivel, emite certificate doar pentru sine și autoritățile de certificare care îi sunt subordonate. Aceasta operează doar când îndeplinește una dintre responsabilitățile sale strict definite. Principalele date ale acesteia sunt:

Distinguished name (Denumire specifică) CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU

Serial number (Număr de serie) 596F AC4C 218C 21BC 4E00 6B42 A164 46DD

Distinguished name of issuer (Denumirea specifică a emitentului) CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU

Validity period (Perioada de validitate) From 21-06-2011 11:58:26 to 21-06-2041 11:58:26

Message digest (Prelucrare mesaj) (SHA-1) CEF6 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192

- **Autoritatea de certificare online pentru ESCB-PKI** (*Online ESCB-PKI certification authority*): Această autoritate, la nivel secund, este subordonată Autorității de certificare root pentru ESCB-PKI. Este responsabilă cu emiterea certificatelor ESCB-PKI pentru utilizatori. Principalele date ale acesteia sunt:

Distinguished name (Denumire specifică) CN=ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU

Serial number (Număr de serie) 2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C

Distinguished name of issuer (Denumirea specifică a emitentului) CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU

Validity period (Perioada de validitate) From 22-07-2011 12:46:35 to 22-07-2026 12:46:35

Message digest (Prelucrare mesaj) (SHA-1) D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
