

BESLUT

EUROPEISKA CENTRALBANKENS BESLUT

av den 11 januari 2013

om ett ramverk för en infrastruktur för kryptering med öppen nyckel (PKI) för Europeiska centralbankssystemet

(ECB/2013/1)

(2013/132/EU)

ECB-RÅDET HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktions-sätt, särskilt artikel 127,

med beaktande av stadgan för Europeiska centralbankssystemet och Europeiska centralbanken (nedan kallad *ECBS-stadgan*), särskilt artikel 12.1 jämförd med artiklarna 3.1, 5, 12.3 och 16–24, och

av följande skäl:

- (1) Enligt artikel 12.1 i ECBS-stadgan ska ECB-rådet anta de riktlinjer och fatta de beslut som behövs för att säkerställa att de uppgifter utförs som har anförtratts Europeiska centralbankssystemet (ECBS) och Eurosystemet enligt fördraget och ECBS-stadgan. Detta omfattar befogenheten att besluta om stödaktiviteter som är nödvändiga för att utföra sådana uppgifter, t.ex. att ge ut och hantera elektroniska certifikat för att skydda sådan information som lagras och behandlas i ECBS och Eurosystemets elektroniska applikationer, system, plattformar och tjänster, samt för att skydda datakommunikationen till och från dessa.
- (2) I enlighet med artikel 12.3 i ECBS-stadgan fastställer ECB-rådet även den interna organisationen för Europeiska centralbanken (ECB) och dess beslutande organ. ECB-rådet är alltså behörigt att fatta beslut om att ECB ska använda elektroniska certifikat som ges ut av Eurosystemets egna infrastruktur för kryptering med öppen nyckel (PKI).
- (3) Antalet användare som utnyttjar ett ständigt växande antal elektroniska applikationer, system, plattformar och tjänster inom ECBS och Eurosystemet ökar. ECB-rådet anser att man måste skapa ett avancerat skydd för informationstjänster, t.ex. stark autentisering, elektroniska signaturer och kryptering, med hjälp av elektroniska certifikat.
- (4) Få centralbanker inom ECBS har egen infrastruktur för kryptering med öppen nyckel (PKI) och många användare från tredje parter som samarbetar med centralbanker inom ECBS kan inte på något enkelt sätt få tillgång till en certifikatutfärdare som godkänns av ECBS i enlighet med dess ramverk för godkännande av certifikat.
- (5) Det finns ett behov för Eurosystemet att skapa en egen infrastruktur för kryptering med öppen nyckel (PKI) som kan utfärda alla typer av elektroniska certifikat som personliga och tekniska certifikat för användare inom och utanför ECBS, och som är så flexibel att den kan anpassas till utvecklingen av de elektroniska applikationer, system, plattformar och tjänster som ECBS och Eurosystemet bedriver. Denna infrastruktur för kryptering med öppen nyckel (PKI) (nedan kallad *ECBS-PKI*) bör komplettera de tjänster som andra certifikatutfärdare tillhandahåller och som godkänns av ECBS i enlighet med dess ramverk för godkännande av certifikat eller genom certifikatutfärdare som godkänns av ECBS för Target2 och Target2 Securities för dessa två applikationer.
- (6) Den 29 september 2010 beslutade ECB-rådet att lansera ECBS-PKI-projektet för att bygga upp och implementera ECBS-PKI samt tillhandahålla de resurser som behövs fram till dess att projektet fullbordats. ECB-rådet beslutade att ECBS-PKI ska utvecklas och drivas av Banco de España som även ska vara värd för ECBS-PKI.
- (7) ECBS-PKI hjälper ECBS och Eurosystemet att utföra sina uppgifter. Systemet är baserat på tre ledningsnivåer: nivå 1 består av ECB-rådet och direktionen, nivå 2 av Eurosystemets centralbanker och nivå 3 av den utförande centralbanken.
- (8) På nivå 1 ansvarar ECB-rådet för ledningen, förvaltningen och kontrollen av de åtgärder och resultat som behövs för att utveckla och driva ECBS-PKI. Den ska även svara för slutliga beslut som rör ECBS-PKI samt besluta om fördelningen av arbetsuppgifter som inte specifikt hänförs till nivåerna 2 och 3.
- (9) Eurosystemets centralbanker ansvarar för de arbetsuppgifter som ska utföras på nivå 2, inom den allmänna ram som fastställts av ECB-rådet. De är behöriga att fatta beslut om tekniska åtgärder för att genomföra ECBS-PKI.

- (10) ECBS IT-kommitté (ITC) styr utvecklingen av ECBS-PKI. Den styr, bedömer, kontrollerar och godkänner projektets olika komponenter mot de uppställda målen i enlighet med ECBS ramverk för godkännande av certifikat samt omfattningen och tidsplanen som godkänts av ECB-rådet.
- (11) På nivå 3 har Banco de España utnämnts till den utförande centralbanken som utför uppgifterna enligt det ramverk som ECB-rådet uppställt. Den utförande centralbanken har skapat den tekniska infrastrukturen samt säkra hårdvaror och tjänster som krävs för att skapa och använda infrastrukturen för kryptering med öppen nyckel (PKI) i enlighet med a) den nationella lagstiftningen som införlivar Europaparlamentets och rådets direktiv 1999/93/EG av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer ⁽¹⁾, i tillämpliga delar, och b) den nationella lagstiftningen som införlivar Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ⁽²⁾, i tillämpliga delar, samt c) Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter ⁽³⁾.
- (12) Eftersom elektroniska certifikat är viktiga komponenter som används för elektroniska applikationer både som autentiseringsmekanism för att implementera elektroniska signaturer och för kryptering baserad på öppna nycklar, kommer ECBS-PKI att ta hänsyn till de elektroniska applikationer, system, plattformar och tjänster som ECBS och Eurosystemet redan bedriver eller planerar för att säkerställa att alla behov kan tillgodoses.
- (13) Nationella centralbanker utanför euroområdet kan välja att använda de certifikat och tjänster som ECBS-PKI tillhandahåller.
- certifikat eller elektroniskt certifikat inkluderar en hänvisning till det datamedium på vilket ett certifikat eller elektroniskt certifikat lagras.
2. *elektroniska applikationer, system, plattformar och tjänster som ECBS och Eurosystemet bedriver*: de elektroniska applikationer, system, plattformar och tjänster som ECBS och/eller Eurosystemet använder när de utför sådana uppgifter som åligger dem enligt fördraget och ECBS-stadgan.
 3. *infrastruktur för kryptering med öppen nyckel (PKI)*: den uppsättning individer, regler, förfaranden och datorsystem som är nödvändiga för autentisering, kryptering, integritet och oavvislighet med hjälp av kryptering via öppna och privata nycklar samt elektroniska certifikat.
 4. *användare*: en certifikatanvändare eller en accepterande part, eller båda.
 5. *autentisering*: en process där man verifierar identiteten på den som ansöker om ett certifikat eller en certifikatanvändare.
 6. *centralbank i ECBS*: antingen en av Eurosystemets centralbanker eller en nationell centralbank utanför euroområdet.
 7. *centralbank i Eurosystemet*: antingen en nationell centralbank i en medlemsstat som har euron som valuta, inklusive den utförande centralbanken, eller ECB.
 8. *utförande centralbank*: den nationella centralbank som ECB-rådet har utsett att utveckla ECBS-PKI och tillhandahålla ECBS-PKI-tjänster åt centralbankerna i Eurosystemet.
 9. *nationell centralbank utanför euroområdet*: en nationell centralbank i en medlemsstat som inte har euron som valuta.
 10. *ECBS-PKI-certifikatutfärdare*: den betrodda enhet som utfärdar, hanterar, återkallar och förnyar certifikat för centralbanker i ECBS eller Eurosystemet i enlighet med ECBS ramverk för godkännande av certifikat.
 11. *ECBS-PKI-valideringsinstans*: den betrodda enhet som tillhandahåller information om huruvida certifikat som utfärdats av ECBS-PKI-certifikatutfärdaren är giltiga.
 12. *certifikatanvändare*: antingen en fysisk person som fått ett elektroniskt certifikat utfärdat till sig, eller en person ansvarig för en teknisk komponent som accepterat ett elektroniskt certifikat utfärdat av ECBS-PKI-certifikatutfärdaren för en teknisk komponent, eller båda.
 13. *ECBS ramverk för godkännande av certifikat*: de kriterier som ESCB-ITC uppställt för att identifiera de certifikatutfärdare, både inom och utanför ECBS, som är pålitliga avseende

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Definitioner

I detta beslut gäller följande definitioner:

1. *certifikat eller elektroniskt certifikat*: en elektronisk fil från en certifikatutfärdare som kopplar en öppen nyckel till en certifikatanvändares identitet och används för en eller flera av följande: a) verifiera att den öppna nyckeln tillhör en certifikatanvändare, b) autentisera en certifikatanvändare, c) kontrollera en certifikatanvändares signatur, d) kryptera ett meddelande till en certifikatanvändare, e) verifiera en certifikatanvändares rätt att använda de elektroniska applikationer, system, plattformar och tjänster som ECBS och Eurosystemet bedriver. Varje hänvisning i detta beslut till ett

⁽¹⁾ EGT L 13, 19.1.2000, s. 12.

⁽²⁾ EGT L 281, 23.11.1995, s. 31.

⁽³⁾ EGT L 8, 12.1.2001, s. 1.

elektroniska applikationer, system, plattformar och tjänster som ECBS och Eurosystemet bedriver.

14. *registreringsinstans*: den betrodda enhet som verifierar identiteten på den som ansöker om ett certifikat innan ECBS-PKI-certifikatutfärdaren utfärdar ett certifikat.
15. *accepterande part*: en annan fysisk person eller enhet än en certifikatanvändare som godtar och litar på ett certifikat.
16. *granskningspolicy*: den granskningspolicy för ECBS som fastställts av ECB-rådet den 7 oktober 1998 och som publicerats på ECB:s webbplats⁽¹⁾.
17. *den som ansöker om ett certifikat*: en fysisk person som ansöker om ett certifikat för sig själv eller för en teknisk komponent.
18. *teknisk komponent*: varje programvara eller hårdvara som kan identifieras med hjälp av elektroniska certifikat.

Artikel 2

Tillämpningsområde

1. Genom detta beslut inrättas ramverket för ECBS-PKI. ECBS-PKI är Eurosystemets egna infrastruktur för kryptering med öppen nyckel (PKI) som den utförande centralbanken tagit fram åt Eurosystemets centralbanker, och som utfärdar, hanterar, återkallar och förnyar certifikat i enlighet med ECBS ramverk för godkännande av certifikat.
2. Eftersom ECBS-PKI-tjänster kan påverka accepterande parter, innehåller detta beslut även de förutsättningar under vilka sådana parter kan lita på ECBS-PKI-certifikat.

Artikel 3

Tillämpningsområde och mål för ECBS-PKI

1. Tillträde till, och användning av, elektroniska applikationer, system, plattformar och tjänster som ECBS och Eurosystemet bedriver och som är av medelhög eller högre betydelse får endast ske om användaren har autentiserats genom ett elektroniskt certifikat som utfärdats och hanteras av en certifikatutfärdare som godkänts av ECBS i enlighet med ECBS ramverk för godkännande av certifikat, inklusive av ECBS-PKI-certifikatutfärdaren, eller av certifikatutfärdare som godkänns av ECBS för Target2 och Target2 Securities för dessa två applikationer.
2. ECBS-PKI-certifikatutfärdaren ska utfärda elektroniska certifikat och tillhandahålla andra elektroniska certifikattjänster till certifikatanvändare inom centralbankerna i ECBS och tredje parter som samarbetar med dem för att möjliggöra säker åtkomst och användning av de elektroniska applikationer, system, plattformar och tjänster som ECBS och Eurosystemet bedriver.

3. ECBS-PKI ska tillhandahålla följande certifikattjänster:

- a) utfärda, förnya och återkalla certifikat samt bekräfta ett certifikats giltighet avseende olika typer av certifikat.
- b) utfärda certifikat för autentisering, elektroniska signaturer och kryptering för användare inom och utanför ECBS, samt tekniska certifikat.
- c) återskapa privata nycklar för att säkerställa att krypterad information baserad på publika nycklar kan återställas om ett certifikat förloras.
- d) vid behov leverera och hantera krypteringsverktyg till certifikatanvändare.
- e) tillhandahålla information om hur ECBS-PKI-certifikat hanteras, samt teknisk support för ECBS projektledare så att dessa kan integrera ECBS-PKI-certifikat i sina applikationer.

Andra tjänster kan tillkomma i framtiden om detta krävs för de elektroniska applikationer, system, plattformar och tjänster som ECBS och Eurosystemet bedriver.

Artikel 4

Ramverket för ECBS-PKI

1. Enligt detta beslut ska ansvaret och funktionerna för den utförande centralbanken och centralbankerna i Eurosystemet avseende implementering, drift och användning av ECBS-PKI fastställas i nivå 2/nivå 3-avtal och ytterligare specificeras i ECBS-PKI:s certifikatpolicy samt i ECBS-PKI:s riktlinjer för certifiering.
2. Nivå 2/nivå 3-avtalet, som inkluderar avtalet om servicenivå, beskriver vad som avtalats mellan den utförande centralbanken och centralbankerna i Eurosystemet avseende ansvars- och funktionsfördelningen mellan den utförande centralbanken och centralbankerna i Eurosystemet. Avtalet ska överlämnas till ECB-rådet för godkännande och sedan undertecknas av den utförande centralbanken och centralbankerna i Eurosystemet.
3. Avtalet om servicenivå är samtidigt ett avtal som anger vilken servicenivå som den utförande centralbanken ska tillhandahålla centralbankerna i Eurosystemet och ett avtal som anger vilken servicenivå som Eurosystemet ska tillhandahålla de nationella centralbankerna utanför euroområdet och tredje parter ifråga om ECBS-PKI.
4. ECBS-PKI-riktlinjer för certifiering innehåller regler för ett elektroniskt certifikats livscykel, från första begäran om utfärdande till dess att användningen upphör eller certifikatet återkallas, samt även regler som beskriver förhållandet mellan den som ansöker om ett certifikat eller certifikatanvändare, ECBS-PKI-certifikatutfärdaren samt accepterande parter. Riktlinjerna omfattar både sådana elektroniska certifikat som omfattas av direktiv 1999/93/EG och sådana som inte gör det. De beskriver alla parter roller och ansvar samt reglerar hur certifikat ska utfärdas och hanteras. Riktlinjerna finns som bilaga till nivå 2/nivå 3-avtalet.

⁽¹⁾ www.ecb.europa.eu

5. En ECBS-PKI-certifikatpolicy är en uppsättning regler som är tillämpliga på varje typ av utfärdat certifikat. Varje uppsättning innehåller genomförandedetaljer avseende ECBS-PKI:s riktlinjer för certifiering för varje typ av utfärdat certifikat. ECBS-PKI:s certifikatpolicyer finns som bilaga till nivå 2/nivå 3-avtalet.

6. ECBS-PKI:s certifikatpolicyer och ECBS-PKI:s riktlinjer för certifiering ska publiceras på ECBS-PKI:s webbplats⁽¹⁾.

7. Information om ECBS-PKI-certifikatutfärdaren, inklusive dess identitet och dess tekniska komponenter, framgår av bilagan till detta beslut.

Artikel 5

Den utförande centralbankens roll och ansvar

1. Den utförande centralbanken ansvarar för driften och underhållet av ECBS-PKI för Eurosystemets centralbanker, inklusive värdtjänster, drift och underhåll som utförs enligt nivå 2/nivå 3-avtalet.

2. Den ska särskilt leverera certifikat och ECBS-PKI-tjänster i enlighet med behoven och de tekniska specifikationerna, som ECBS ramverk för godkännande av certifikat och de krav och specifikationer som framgår av nivå 2/nivå 3-avtalet.

3. Den utförande centralbanken ska bygga upp den nödvändiga organisatoriska infrastrukturen för att certifikat ska kunna skapas, utfärdas och hanteras samt säkerställa att denna infrastruktur underhålls. För detta ändamål kan den utförande centralbanken, i samråd med ITC, anta regler om sin interna organisation och förvaltning.

4. Den utförande centralbanken ska vara ECBS-PKI-certifikatutfärdare och ECBS-PKI-valideringsinstans. Ansvarsfrågor som rör den utförande centralbanken ska regleras i nivå 2/nivå 3-avtalet.

Artikel 6

Roll och ansvar för centralbankerna i Eurosystemet

1. Varje centralbank i Eurosystemet ansvarar för att dess certifikatanvändare identifieras. Den ska utse en registreringsansvarig som avgör vem som är behörig att registrera tredje parter som användare.

2. Varje centralbank i Eurosystemet ska uppträda som accepterande part avseende certifikat för kryptering och elektroniska signaturer som utfärdats av ECBS-PKI för andra centralbanker i Eurosystemet eller certifikatanvändare från tredje part.

3. Varje centralbank i Eurosystemet som använder ECBS-PKI-tjänster ska vara registreringsinstans för sina personer som ansöker om ett certifikat och säkerställa att de som ansöker om ett certifikat godkänner och tillämpar de användarvillkor som framgår av ECBS-PKI-certifikatutfärdarens ansökningsblankett för dess tjänster.

Artikel 7

Förhållandet mellan centralbankerna i Eurosystemet, tredje parter och certifikatanvändare

Varje centralbank i Eurosystemet ska vidta åtgärder så att tredje parter via en säker tillgång, med hjälp av ECBS-PKI-certifikat, kan använda elektroniska applikationer, system, plattformar och tjänster som ECBS och Eurosystemet bedriver. Dessa arrangemang ska uteslutande styra förhållandet mellan de berörda centralbankerna i Eurosystemet och tredje parter som använder ECBS-PKI-certifikat. Alla tredje parter ska följa ECBS-PKI:s certifikatpolicyer, ECBS-PKI-riktlinjerna för certifiering samt de användarvillkor som framgår av ECBS-PKI-certifikatutfärdarens ansökningsblankett för dess tjänster.

Artikel 8

Förhållandet till accepterande parter

Ett elektroniskt certifikat som utfärdas enligt detta beslut får accepteras om den accepterande parten

- a) med hjälp av aktuell information om certifikatets status verifierar huruvida certifikatet är giltigt, tillfälligt upphävt eller har återkallats,
- b) beaktar alla användarbegränsningar som framgår av certifikatet, och
- c) godtar ECBS-PKI-riktlinjerna för certifiering och tillämpliga ECBS-PKI-certifikatpolicyer.

Artikel 9

Rättigheter avseende ECBS-PKI

1. ECBS-PKI ägs till 100 procent av centralbankerna i Eurosystemet.

2. Mot bakgrund av detta ska den utförande centralbanken bevilja centralbankerna i Eurosystemet, i den utsträckning som gällande lagstiftning tillåter, alla licenser avseende de immateriella rättigheter som centralbankerna i Eurosystemet behöver för att kunna använda ECBS-PKI och dess komponenter och alla ECBS-PKI-tjänster samt även tillhandahålla ECBS-PKI-tjänster till tredje parter i enlighet med ECBS-PKI-riktlinjerna för certifiering och ECBS-PKI-certifikatpolicyer. Den utförande centralbanken ska ersätta centralbankerna i Eurosystemet för tredje parts eventuella intrångsanspråk som rör sådana immateriella rättigheter.

3. Närmare detaljer om vilka rättigheter centralbankerna i Eurosystemet har till ECBS-PKI ska avtalas mellan nivå 2 och nivå 3 i nivå 2/nivå 3-avtalet.

Artikel 10

Det ansvar som centralbankerna i Eurosystemet har gentemot användare

1. Centralbankerna i Eurosystemet måste visa att de inte har varit vårdslösa, i annat fall ansvarar de, i enlighet med sitt ansvar och sina funktioner inom ECBS-PKI för all skada som

⁽¹⁾ <http://pki.escb.eu>

åsamkas en användare som har rimlig anledning att förlita sig på ett kvalificerat certifikat, enligt definitionen i direktiv 1999/93/EG, för

- a) att all information i det kvalificerade certifikatet är korrekt vid tidpunkten för utfärdandet och att certifikatet innehåller alla de uppgifter som föreskrivs för ett kvalificerat certifikat enligt definitionen i direktiv 1999/93/EG,
- b) att det säkerställs att den användare som anges i det kvalificerade certifikatet vid tidpunkten för utfärdandet av certifikatet var i besittning av de uppgifter för skapande av signaturer som motsvarar de uppgifter för signaturverifiering som anges i certifikatet,
- c) att det säkerställs att uppgifterna för skapande av signaturer och uppgifterna för signaturverifiering kan användas som komplement till varandra, om ECBS-PKI framställer båda dessa,
- d) varje underlåtenhet att registrera återkallandet av ett kvalificerat certifikat.

2. Centralbankerna i Eurosystemet åtar sig inga förpliktelser, ger inga garantier och accepterar inget ansvar gentemot användare om dessa inte uttryckligen nämns i detta beslut och i ECBS-PKI:s riktlinjer för certifiering.

Artikel 11

Hur nationella centralbanker utanför euroområdet kan delta i ECBS-PKI

1. En nationell centralbank utanför euroområdet får agera som registreringsinstans för sina interna användare samt även för användare som är tredje part, och får utse en registreringsansvarig för denna funktion.

2. En nationell centralbank utanför euroområdet får också besluta att använda ECBS-PKI-tjänster under samma förutsättningar som gäller för centralbankerna i Eurosystemet, förutsatt att ECB-rådet godkänner detta. För detta ändamål ska den nationella centralbanken utanför euroområdet skriftligen försäkra för ECB-rådet att den åtar sig alla skyldigheter som framgår av detta beslut och nivå 2/nivå 3-avtalet. En nationell centralbank utanför euroområdet ska inte bli delägare i ECBS-PKI och har ingen skyldighet att bidra till finansieringen av ECBS-PKI.

Artikel 12

Skydd av personuppgifter

Centralbankerna i Eurosystemet ska uppfylla all gällande lagstiftning om skydd för personuppgifter när de behandlar personuppgifter inom ramen för ECBS-PKI.

Artikel 13

Revision

Revision av ECBS-PKI ska utföras i enlighet med de principer och arrangemang som framgår av revisionsriktlinjerna. De gäller utan att det påverkar tillämpningen av interna kontroll- och revisionsregler som gäller för, eller antas av, centralbankerna i Eurosystemet.

Artikel 14

Ekonomiska arrangemang

Centralbankerna i Eurosystemet ska bära kostnaderna för utveckling och drift av ECBS-PKI, såsom framgår av finansieringsplanen för ECBS-PKI.

Artikel 15

Direktionens roll

1. I enlighet med artikel 17.3 i ECB/2004/2 av den 19 februari 2004 om antagande av arbetsordningen för Europeiska centralbanken ⁽¹⁾, kan ECB-rådet delegera sin normgivningsrätt till direktionen för att vidta de genomförandeåtgärder av detta beslut som krävs för att ECBS-PKI ska fungera effektivt och säkert, samt rätten att anta ändringar av de tekniska aspekter av ECBS-PKI och ECBS-PKI-tjänster enligt bilagorna till nivå 2/nivå 3-avtalet, med beaktande av ITC:s synpunkter och, i förekommande fall, synpunkter från Eurosystemets styrkommitté för IT-frågor.

2. Direktionen ska utan opåkallat dröjsmål meddela ECB-rådet om eventuella åtgärder som vidtas enligt punkt 1 och följa alla beslut som ECB-rådet fattar i frågan.

Utfärdat i Frankfurt am Main den 11 januari 2013.

Mario DRAGHI
ECB:s ordförande

⁽¹⁾ EUT L 80, 18.3.2004, s. 33.

BILAGA

Information om ECBS-PKI-certifikatutfärdaren, inklusive dess identitet och dess tekniska komponenter

ECBS-PKI-certifikatutfärdaren identifieras i sitt certifikat som utgivare och dennes privata nyckel används för att signera certifikat. ECBS-PKI-certifikatutfärdaren ska

- i) utfärda certifikat för öppna och privata nycklar,
- ii) publicera förteckningar över återkallade certifikat,
- iii) generera nyckelpar som är associerade med specifika certifikat, t.ex. sådana som kräver att nycklar återskapas,
- iv) ha det övergripande ansvaret för ECBS-PKI och säkerställa att alla kraven för att driva det uppfylls.

ECBS-PKI-certifikatutfärdaren inkluderar alla individer, regler, förfaranden och datorsystem som är betrodda att utfärda elektroniska certifikat och registrera dem på certifikatanvändarna.

ECBS-PKI-certifikatutfärdaren inkluderar två tekniska komponenter:

- **ECBS-PKI-certifikatutfärdaren på rotnivå:** Denna certifikatutfärdare, på den första nivån, utfärdar endast certifikat för sig själv och sina underordnade certifikatutfärdare. Den är endast verksam när den utför sina egna mycket begränsade uppgifter. Dess viktigaste kännetecken är:

Systemets unika namn	CN=ECBS-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
ID-nummer	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Utfärdarens unika namn	CN=ECBS-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Giltighetsperiod	Från 2011-06-21, kl. 11:58:26 till 2041-06-21, kl. 11:58:26
Kontrollsumma (SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192

- **Online ECBS-PKI-certifikatutfärdaren:** Denna certifikatutfärdare, på den andra nivån, är underordnad ECBS-PKI-certifikatutfärdaren på rotnivå. Den ansvarar för utfärdandet av ECBS-PKI-certifikat till användarna. Dess viktigaste kännetecken är:

Systemets unika namn	CN=ECBS-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
ID-nummer	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Utfärdarens unika namn	CN=ECBS-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Giltighetsperiod	Från 2011-07-22, kl. 12:46:35 till 2026-07-22, kl. 12:46:35
Kontrollsumma (SHA-1)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08