Europeiska unionens officiella tidning

SV
L-serien

2024/2683

15.10.2024

EUROPEISKA CENTRALBANKENS BESLUT (EU) 2024/2683

av den 8 oktober 2024

om ändring av beslut ECB/2013/1 om ett ramverk för en infrastruktur för kryptering med öppen nyckel (PKI) för Europeiska centralbankssystemet *(ECB/2024/26)*

ECB-RÅDET HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 127 och 132.1,

med beaktande av stadgan för Europeiska centralbankssystemet och Europeiska centralbanken, särskilt artikel 12.1 jämförd med artiklarna 3.1, 12.3 och 34, och

av följande skäl:

(1) Genom Europeiska centralbankens beslut ECB/2013/1 ([1]) inrättades ramverket för Eurosystemets infrastruktur för kryptering med öppen nyckel (nedan kallat *ECBS-PKI*) för att reglera utfärdande och hantering av elektroniska certifikat som krävs för åtkomst till och användning av ECBS och Eurosystemets elektroniska applikationer, system, plattformar och tjänster av medelhög eller högre betydelse.

(2) Den teknik som används av ECBS-PKI har nått slutet av sin livscykel och har ersatts. Det är därför nödvändigt att införa en ny onlinebaserad ECBS-PKI-certifikatutfärdare (nedan kallad *onlinebaserad ECBS-PKI-certifikatutfärdare V1.2*), som även skulle beakta att den treåriga giltigheten för de certifikat som har utfärdats för användare och tekniska komponenter i och utanför ECBS genom en onlinebaserad ECBS-PKI-utfärdare inte kan upphöra senare än den onlinebaserade ECBS-PKI-certifikatutfärdarens eget certifikat. Certifikatet för den befintliga onlinebaserade ECBS-PKI-certifikatutfärdaren upphör den 22 juli 2026, och därefter skulle den onlinebaserade ECBS-PKI-certifikatutfärdaren V1.2 vara den enda onlinebaserade ECBS-PKI-certifikatutfärdaren fram tills att dess certifikat upphör.

(3) Beslut ECB/2013/1 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Ändring

Bilagan till beslut ECB/2013/1 ska ersättas med bilagan till det här beslutet.

Artikel 2

Ikraftträdande

Detta beslut träder i kraft den femte dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Frankfurt am Main den 8 oktober 2024.

Christine LAGARDE
ECB:s ordförande

([1]) Europeiska centralbankens beslut ECB/2013/1 av den 11 januari 2013 om ett ramverk för en infrastruktur för kryptering med öppen nyckel (PKI) för Europeiska centralbankssystemet (EUT L 74, 16.3.2013, s. 30).

BILAGA

”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 tre tekniska komponenter:

1. **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:

Distinguished name (systemets unika namn)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (ID-nummer)	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8
Distinguished name of issuer (utfärdarens unika namn)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (giltighetsperiod)	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
Message digest (SHA-1)	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
Message digest (SHA-256)	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
Cryptographic algorithms (krypteringsalgoritmer)	SHA-256/RSA 4096

2. **Den onlinebaserade 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. Den kommer att upphöra den 22 juli 2026. Dess viktigaste kännetecken är:

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

3. **Den onlinebaserade ECBS-PKI-certifikatutfärdaren V1.2**: Denna certifikatutfärdare, på den andra nivån, är underordnad ECBS-PKI-certifikatutfärdaren på rotnivå. Den ansvarar för utfärdandet av ECBS-PKI-certifikat till användarna. Efter den 22 juli 2026 kommer detta att vara den enda onlinebaserade ECBS-PKI-certifikatutfärdaren, fram till dess att den löper ut. Dess viktigaste kännetecken är:

Distinguished name (systemets unika namn)	CN = ESCB-PKI ONLINE CA V1.2, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Serial number (ID-nummer)	1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653
Distinguished name of issuer (utfärdarens unika namn)	CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU
Validity period (giltighetsperiod)	From 08-06-2023 17:07:00 to 08-06-2038 17:07:00
Message digest (SHA-1)	DC92 042E 6316 CB60 F8F6 109B 8C43 F3C6 AF2F B2F3
Message digest (SHA-256)	96B7 8E9C F914 ED4D 072D 93C8 C531 DEEF D102 7571 7218 A202 0924 3216 99D8 1C48
Cryptographic algorithms (krypteringsalgoritmer)	SHA-256/RSA 4096”