2024/2683

15.10.2024

# DEN EUROPÆISKE CENTRALBANKS AFGØRELSE (EU) 2024/2683

## af 8. oktober 2024

## om ændring af afgørelse ECB/2013/1 om fastlæggelse af rammerne for en public key-infrastruktur for Det Europæiske System af Centralbanker (*ECB/2024/26*)

STYRELSESRÅDET FOR DEN EUROPÆISKE CENTRALBANK HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 127 og artikel 132, stk. 1,

under henvisning til statutten for Det Europæiske System af Centralbanker og Den Europæiske Centralbank, særlig artikel 12.1 sammenholdt med artikel 3.1 og 12.3, samt artikel 34, og

ud fra følgende betragtninger:

(1) Den Europæiske Centralbanks afgørelse ECB/2013/1 ([1]) fastsatte rammerne for Eurosystemets public key-infrastruktur (herefter »ESCB-PKI«) til regulering af udstedelse og forvaltning af elektroniske certifikater, der er nødvendige for at få adgang til og anvende ESCB's og Eurosystemets elektroniske applikationer, systemer, platforme og tjenester af middel eller over middel kritikalitet.

(2) Den teknologi, der anvendes af ESCB-PKI, er udtjent og er blevet erstattet. Det er derfor nødvendigt at indføre en ny online ESCB-PKI-certificeringsmyndighed (herefter »online ESCB-PKI-certificeringsmyndighed V1.2«), som også bør tage hensyn til, at den tre-årige gyldighed af certifikater udstedt for brugere i og udenfor ESCB og de tekniske komponenter under en online ESCB-PKI certificeringsmyndighed ikke kan udløbe senere end udløbsdatoen for den pågældende online ESCB-PKI certificeringsmyndighed selv. Den online ESCB-PKI-certificeringsmyndigheds certifikat udløber den 22. juli 2026, og derefter er ESCB-PKI-certificeringsmyndigheden V1.2 den eneste online ESCB-PKI-certificeringsmyndighed, indtil dens certifikat udløber.

(3) Afgørelse ECB/2013/1 bør derfor ændres i overensstemmelse hermed —

VEDTAGET DENNE AFGØRELSE:

*Artikel 1*

**Ændring**

Bilaget til afgørelse ECB/2013/1 erstattes af bilaget til denne afgørelse.

*Artikel 2*

**Ikrafttrædelse**

Denne afgørelse træder i kraft på femtedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Frankfurt am Main, den 8. oktober 2024.

Christine LAGARDE
*Formand for ECB*

([1]) Den Europæiske Centralbanks afgørelse ECB/2013/1 af 11. januar 2013 om fastlæggelse af rammerne for en public key-infrastruktur for Det Europæiske System af Centralbanker (EUT L 74 af 16.3.2013, s. 30).

*BILAG*

*»BILAG*

**Oplysninger om ESCB-PKI certificeringsmyndigheden, herunder dens identitet og tekniske komponenter**

ESCB-PKI certificeringsmyndigheden identificeres i dets certifikat som udsteder, og dets private nøgle anvendes til at signere certifikater. ESCB-PKI certificeringsmyndigheden er ansvarlig for:

i) udstedelsen af private og offentlige nøglecertifikater

ii) udstedelsen af tilbagekaldelseslister

iii) genereringen af nøglepar knyttet til specifikke certifikater, f.eks. certifikater, der kræver nøglegenskabelse

iv) det overordnede ansvar for ESCB-PKI og sikring af, at alle krav, der er nødvendige for driften, er opfyldt.

ESCB-PKI certificeringsmyndigheden omfatter alle individer, politikker, procedurer og computersystemer, der har til opgave at udstede elektroniske certifikater og at tildele disse til certifikatindehaverne.

ESCB-PKI certificeringsmyndigheden har tre tekniske komponenter:

1. **ESCB-PKI rodcertificeringsmyndigheden**: Denne certificeringsmyndighed på første niveau udsteder kun certifikater til sig selv og til dets underordnede certificeringsmyndigheder. Den er kun i drift, når den udfører sine egne snævert definerede opgaver. Følgende data udgør dens væsentligste data:

| | |
|---|---|
| **Distinguished name (kendenavn)** | CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU |
| **Serial number (serienummer)** | 4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8 |
| **Distinguished name of issuer (udsteders kendenavn)** | CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU |
| **Validity period (gyldighedsperiode)** | Fra 21-06-2011 12:35:34 til 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 |
| **Kryptografiske algoritmer** | SHA-256/RSA 4096 |

2. **ESCB-PKI onlinecertificeringsmyndigheden**: Denne certificeringsmyndighed på andet niveau er underordnet ESCB-PKI rodcertificeringsmyndigheden. Den har ansvaret for udstedelsen af ESCB-PKI certifikater til brugerne. Den udløber den 22. juli 2026. Følgende data udgør dens væsentligste data:

| | |
|---|---|
| **Distinguished name (kendenavn)** | CN = ESCB-PKI ONLINE CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU |
| **Serial number (serienummer)** | 660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D |
| **Distinguished name of issuer (udsteders kendenavn)** | CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU |
| **Validity period (gyldighedsperiode)** | Fra 22-07-2011 12:46:35 til 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 |
| **Kryptografiske algoritmer** | SHA-256/RSA 4096 |

3. **ESCB-PKI onlinecertificeringsmyndigheden V1.2**: Denne certificeringsmyndighed på andet niveau er underordnet ESCB-PKI rodcertificeringsmyndigheden. Den har ansvaret for udstedelsen af ESCB-PKI certifikater til brugerne. Efter den 22. juli 2026 er den den eneste online ESCB-PKI-certificeringsmyndighed, indtil den udløber. Følgende data udgør dens væsentligste data:

| | |
|---|---|
| **Distinguished name (kendenavn)** | CN = ESCB-PKI ONLINE CA V1.2, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU |
| **Serial number (serienummer)** | 1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653 |
| **Distinguished name of issuer (udsteders kendenavn)** | CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU |
| **Validity period (gyldighedsperiode)** | Fra 08-06-2023 17:07:00 til 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 |
| **Kryptografiske algoritmer** | SHA-256/RSA 4096« |