2024/2683

15.10.2024

SKLEP EVROPSKE CENTRALNE BANKE (EU) 2024/2683

z dne 8. oktobra 2024

o spremembi Sklepa ECB/2013/1 o določitvi okvira za infrastrukturo javnih ključev za Evropski sistem centralnih bank *(ECB/2024/26)*

Svet Evropske centralne banke je –

ob upoštevanju Pogodbe o delovanju Evropske unije ter zlasti člena 127 in člena 132(1) Pogodbe,

ob upoštevanju Statuta Evropskega sistema centralnih bank in Evropske centralne banke ter zlasti člena 12.1 v povezavi s členoma 3.1 in 12.3 in členom 34 Statuta,

ob upoštevanju naslednjega:

(1) Sklep Evropske centralne banke ECB/2013/1 je ([1]) vzpostavil okvir za infrastrukturo javnih ključev Eurosistema (v nadaljnjem besedilu: ESCB-PKI), s katerim se ureja izdajanje in upravljanje elektronskih potrdil, ki so potrebna za dostop do elektronskih aplikacij, sistemov, platform in storitev ESCB in Eurosistema, ki so srednje ali bolj kritični, ter njihovo uporabo.

(2) Tehnologija, ki jo uporablja ESCB-PKI, je prišla do konca življenjske dobe in je bila nadomeščena. Zato je treba uvesti novega overitelja spletnih potrdil ESCB-PKI (v nadaljnjem besedilu: overitelj spletnih potrdil ESCB-PKI V1.2), pri katerem je treba upoštevati tudi to, da triletna veljavnost potrdil, izdanih v okviru overitelja spletnih potrdil ESCB-PKI za uporabnike v ESCB in zunaj ESCB ter tehnične komponente, ne more poteči pozneje, kot poteče veljavnost potrdila tega overitelja spletnih potrdil ESCB-PKI samega. Veljavnost potrdila sedanjega overitelja spletnih potrdil ESCB-PKI poteče 22. julija 2026 in od takrat bo overitelj spletnih potrdil ESCB-PKI V1.2 edini overitelj spletnih potrdil ESCB-PKI, dokler ne poteče veljavnost njegovega potrdila.

(3) Zato je treba Sklep ECB/2013/1 ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Sprememba

Priloga k Sklepu ECB/2013/1 se nadomesti s Prilogo k temu sklepu.

Člen 2

Začetek veljavnosti

Ta sklep začne veljati peti dan po objavi v *Uradnem listu Evropske unije*.

V Frankfurtu na Majni, 8. oktobra 2024

Predsednica ECB
Christine LAGARDE

([1]) Sklep Evropske centralne banke ECB/2013/1 z dne 11. januarja 2013 o določitvi okvira za infrastrukturo javnih ključev za Evropski sistem centralnih bank (UL L 74, 16.3.2013, str. 30).

PRILOGA

„PRILOGA

Informacije o overitelju ESCB-PKI, vključno z njegovo identiteto, in njegovih tehničnih komponentah

Overitelj ESCB-PKI je v svojem potrdilu naveden kot izdajatelj in njegov zasebni ključ se uporablja za podpisovanje potrdil. Overitelj ESCB-PKI je pristojen za:

(i) izdajo potrdil za zasebne in javne ključe;

(ii) izdajo seznamov preklicanih potrdil;

(iii) tvorjenje parov ključev, ki so povezani z določenimi potrdili, npr. tistimi, ki zahtevajo povrnitev ključa;

(iv) ohranjanje splošne odgovornosti za infrastrukturo ESCB-PKI in zagotavljanje, da so izpolnjene vse zahteve za njeno upravljanje.

Overitelj ESCB-PKI vključuje vse posameznike, politike, postopke in računalniške sisteme, ki so namenjeni za izdajo elektronskih potrdil in njihovo dodeljevanje imetnikom potrdil.

Overitelj ESCB-PKI vključuje tri tehnične komponente:

1. **overitelj korenskih potrdil ESCB-PKI**: ta overitelj na prvi ravni izdaja potrdila samo zase in sebi podrejene overitelje. Deluje samo takrat, ko izvaja svoje ozko določene odgovornosti. Njegovi ključni podatki so:

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

2. **overitelj spletnih potrdil ESCB-PKI**: ta overitelj je na drugi ravni podrejen overitelju korenskih potrdil ESCB-PKI. Odgovoren je za izdajo potrdil ESCB-PKI za uporabnike. Njegova veljavnost poteče 22. julija 2026. Njegovi ključni podatki so:

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

3. **overitelj spletnih potrdil ESCB-PKI V1.2**: ta overitelj je na drugi ravni podrejen overitelju korenskih potrdil ESCB-PKI. Odgovoren je za izdajo potrdil ESCB-PKI za uporabnike. Po 22. juliju 2026 je edini overitelj spletnih potrdil ESCB-PKI, dokler ne poteče njegova veljavnost. Njegovi ključni podatki so:

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