2024/2683

15.10.2024 г.

# РЕШЕНИЕ (ЕС) 2024/2683 НА ЕВРОПЕЙСКАТА ЦЕНТРАЛНА БАНКА

**от 8 октомври 2024 година**

**за изменение на Решение ЕЦБ/2013/1 за определяне на рамката за инфраструктура на публичен ключ за Европейската система на централните банки *(ЕЦБ/2024/26)***

УПРАВИТЕЛНИЯТ СЪВЕТ НА ЕВРОПЕЙСКАТА ЦЕНТРАЛНА БАНКА,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 127 и член 132, параграф 1 от него,

като взе предвид Устава на Европейската система на централните банки и на Европейската централна банка, и по-специално член 12.1 във връзка с членове 3.1 и 12.3, както и член 34 от него,

като има предвид, че:

(1) С Решение ЕЦБ/2013/1 на Европейската централна банка ([1]) беше приета рамката за инфраструктурата на публичен ключ на Евросистемата (наричана по-долу „ЕСЦБ-ИПК“) с цел регулиране на издаването и управлението на електронни сертификати, които са необходими за достъп и използване на електронни приложения, системи, платформи и услуги на Европеската система на централните банки (ЕСЦБ) и Евросистемата със средна или над средната критичност.

(2) Технологията, използвана от ЕСЦБ-ИПК, достигна края на жизнения си цикъл и беше заменена. Поради това е необходимо да се въведе нов онлайн удостоверяващ орган на ЕСЦБ-ИПК (наричан по-долу „онлайн удостоверяващ орган на ЕСЦБ-ИПК V1.2“), което също така следва да отчита, че тригодишната валидност на сертификатите, издадени на потребители от и извън ЕСЦБ и технически компоненти на онлайн удостоверяващ орган на ЕСЦБ-ИПК, не може да изтече по-късно от изтичането на срока на сертификата на самия онлайн удостоверяващ орган на ЕСЦБ-ИПК. Срокът на сертификата на съществуващия онлайн удостоверяващ орган на ЕСЦБ-ИПК изтича на 22 юли 2026 г., след което онлайн удостоверяващият орган на ЕСЦБ-ИПК V1.2 ще бъде единственият онлайн удостоверяващ орган на ЕСЦБ-ИПК до изтичането на срока на неговия сертификат.

(3) Поради това Решение ЕЦБ/2013/1 следва да бъде съответно изменено,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

*Член 1*

**Изменение**

Приложението към Решение ЕЦБ/2013/1 се заменя с приложението към настоящото решение.

*Член 2*

**Влизане в сила**

Настоящото решение влиза в сила на петия ден след публикуването му в *Официален вестник на Европейския съюз*.

Съставено във Франкфурт на Майн на 8 октомври 2024 година.

*Председател на ЕЦБ*
Christine LAGARDE

([1]) Решение ЕЦБ/2013/1 на Европейската централна банка от 11 януари 2013 г. за определяне на рамката за инфраструктура на публичен ключ за Европейската система на централните банки (ОВ L 74, 16.3.2013 г., стр. 30).

*ПРИЛОЖЕНИЕ*

*„ПРИЛОЖЕНИЕ*

**Информация относно удостоверяващия орган на ЕСЦБ-ИПК, включително относно неговата идентичност и техническите му компоненти**

Удостоверяващият орган на ЕСЦБ-ИПК е идентифициран в неговото удостоверение като издателя и неговият частен ключ се използва за подписването на удостоверения. Удостоверяващият орган на ЕСЦБ-ИПК отговаря за:

i) издаването на удостоверения за частни и публични ключове;

ii) издаването на списъци за отмяна;

iii) генерирането на двойки ключове, свързани със специални удостоверения, например тези, за които се изисква възстановяване на ключ;

iv) носенето на цялостна отговорност за ЕСЦБ-ИПК и осигуряването, че всички необходими за оперирането ѝ изисквания са изпълнени.

Удостоверяващият орган на ЕСЦБ-ИПК включва всички лица, политики, процедури и компютърни системи, на които е възложено издаването и предоставянето на електронни удостоверения на абонати на удостоверения.

Удостоверяващият орган на ЕСЦБ-ИПК включва три технически компонента:

1. **Рутиращият удостоверяващ орган на ЕСЦБ-ИПК**: този удостоверяващ орган, на първо ниво, издава удостоверения само за себе си и за подчинените му удостоверяващи органи. Той функционира само когато изпълнява собствените си тясно определени отговорности. Неговите най-важни данни са:

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

2. **Онлайн удостоверяващият орган на ЕСЦБ-ИПК**: този удостоверяващ орган, на второ ниво, е подчинен на рутиращия удостоверяващ орган на ЕСЦБ-ИПК. Той отговаря за издаване на удостоверения на ЕСЦБ-ИПК за потребители. Срокът му изтича на 22 юли 2026 г. Неговите най-важни данни са:

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

3. **Онлайн удостоверяващият орган на ЕСЦБ-ИПК V1.2:** този удостоверяващ орган, на второ ниво, е подчинен на рутиращия удостоверяващ орган на ЕСЦБ-ИПК. Той отговаря за издаването на удостоверения на ЕСЦБ-ИПК за потребители. След 22 юли 2026 г. той е единственият онлайн удостоверяващ орган на ЕСЦБ-ИПК до изтичането на срока му. Неговите най-важни данни са:

| | |
|---|---|
| **Distinguished name (Отличително име)** | CN = ESCB-PKI ONLINE CA V1.2, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU |
| **Serial number (Сериен номер)** | 1121 4958 04E1 E706 695D D1D1 2997 FAEF 6653 |
| **Distinguished name of issuer (Отличително име на издателя)** | CN = ESCB-PKI ROOT CA, O = EUROPEAN SYSTEM OF CENTRAL BANKS, C = EU |
| **Validity period (Период на валидност)** | From 08-06-2023 17:07:00 to 08-06-2038 17:07:00 |
| **Message digest (SHA-1) (Резюме на съобщението, SHA-1)** | DC92 042E 6316 CB60 F8F6 109B 8C43 F3C6 AF2F B2F3 |
| **Message digest (SHA-256) (Резюме на съобщението, SHA-256)** | 96B7 8E9C F914 ED4D 072C8 C531 DEEF D102 7571 7218 A202 0924 3216 99D8 1C48 |
| **Cryptographic algorithms (Криптографски алгоритми)** | SHA-256/RSA 4096“ |