РЕШЕНИЯ

РЕШЕНИЕ (ЕС) 2016/187 НА ЕВРОПЕЙСКАТА ЦЕНТРАЛНА БАНКА

от 11 декември 2015 година

за изменение на Решение ЕЦБ/2013/1 за определяне на рамката за инфраструктура на публичен ключ за Европейската система на централните банки (ЕЦБ/2015/46)

УПРАВИТЕЛНИЯТ СЪВЕТ НА ЕВРОПЕЙСКАТА ЦЕНТРАЛНА БАНКА,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 127 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 член 3.1, член 5, член 12.3, както и членове 16—24 и член 34 от него,

като има предвид, че:

(1) Считано от 1 юли 2016 г., с Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета ([1]) се отменя Директива 1999/93/ЕО на Европейския парламент и на Съвета ([2]). Следователно е правилно Решение ЕЦБ/2013/1 ([3]) да препраща към Регламент (ЕС) № 910/2014.

(2) Необходимо е да бъде актуализирана информацията, изложена в приложението към Решение ЕЦБ/2013/1, относно удостоверяващия орган на ЕСЦБ-ИПК, включително относно неговата идентичност и техническите му компоненти.

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

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Изменения

Решение ЕЦБ/2013/1 се изменя, както следва:

1. В член 1 точка 10 се заменя със следното:

„10. „удостоверяващ орган на ЕСЦБ-ИПК“ (*ESCB-PKI certification authority*) е лицето, на което потребителите се доверяват да издава, управлява, отменя и подновява удостоверения за ЕСЦБ-ИПК в съответствие с рамката на ЕСЦБ/ЕНМ за признаване на удостоверения;“.

2. В член 4 параграф 4 се заменя със следното:

„4. Правилата относно практиките за удостоверяване на ЕСЦБ-ИПК са набор от правила, регулиращи жизнения цикъл на електронните удостоверения — от първоначалното искане до края или отмяната на абонамента, както и отношенията между лицето, подало заявление за удостоверение, или абоната на удостоверение, удостоверяващия орган на ЕСЦБ-ИПК и доверяващите се страни. Те обхващат удостоверения, попадащи в приложното поле на Директива

([1]) Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 73).

([2]) Директива 1999/93/ЕО на Европейския парламент и на Съвета от 13 декември 1999 г. относно правната рамка на Общността за електронните подписи (ОВ L 13, 19.1.2000 г., стр. 12).

([3]) 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).

1999/93/ЕО и Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета (*), и удостоверения, непопадащи в приложното им поле. С тях също така се определят ролите и отговорностите на всички страни и се установяват процедурите относно издаването и управлението на удостоверения. Те са приложени към споразумението между ниво 2 и ниво 3.

(*) Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 73).“

3. В член 10, параграф 1 въвеждащата разпоредба и буква а) се заменят със следното:

„1. Освен ако докажат, че те не са действали небрежно, централните банки от Евросистемата носят отговорност в съответствие с техните функции и отговорности в ЕСЦБ-ИПК за вреди, причинени на потребител, който основателно разчита на квалифицирано удостоверение, както е определено в Директива 1999/93/ЕО и Регламент (ЕС) № 910/2014:

а) по отношение на точността на цялата информация, съдържаща се в дадено квалифицирано удостоверение, към момента на издаването му и по отношение на въпроса дали удостоверението съдържа всички елементи, предвидени за квалифицирано удостоверение, както е определено в Директива 1999/93/ЕО и Регламент (ЕС) № 910/2014;“.

4. Приложението се заменя с приложението към настоящото решение.

Член 2

Влизане в сила

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

Съставено във Франкфурт на Майн на 11 декември 2015 година.

Председател на ЕЦБ
Mario DRAGHI

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 два технически компонента:

— **Рутиращ 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:

а) удостоверение SHA-1 ([1]):

Distinguished name (Отличително име)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Сериен номер)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
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 11:58:26 to 21-06-2041 11:58:26
Message digest (SHA-1) (Резюме на съобщението, SHA-1)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
Message digest (SHA-256) (Резюме на съобщението, SHA-256)	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
Cryptographic algorithms (Криптографски алгоритми)	SHA-1/RSA 4096

б) удостоверение SHA-256:

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

([1]) Това удостоверение ще бъде използвано само в системи, които не поддържат по-високи алгоритми.

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

— **Онлайн удостоверяващ 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. Неговите най-важни данни са:

а) удостоверение SHA-1 ([1]):

Distinguished name (Отличително име)	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Сериен номер)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
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)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
Message digest (SHA-256) (Резюме на съобщението, SHA-256)	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
Cryptographic algorithms (Криптографски алгоритми)	SHA-1/RSA 4096

б) удостоверение SHA-256:

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“

([1]) Това удостоверение ще бъде използвано само в системи, които не поддържат по-високи алгоритми.