

# HATÁROZATOK

## AZ EURÓPAI KÖZPONTI BANK (EU) 2016/187 HATÁROZATA

(2015. december 11.)

### a Központi Bankok Európai Rendszere nyilvános kulcsú infrastruktúrája keretrendszerének meghatározásáról szóló EKB/2013/1 határozat módosításáról (EKB/2015/46)

AZ EURÓPAI KÖZPONTI BANK KORMÁNYZÓTANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 127. cikkére,

tekintettel a Központi Bankok Európai Rendszere és az Európai Központi Bank Alapokmányára és különösen annak 3.1., 5. és 12.3. cikkével összefüggésben értelmezett 12.1. cikkére, valamint 16–24. és 34. cikkére,

mivel:

- (1) A 910/2014/EU európai parlamenti és tanácsi rendelet <sup>(1)</sup> 2016. július 1-jei hatállyal hatályon kívül helyezte az 1999/93/EK európai parlamenti és tanácsi irányelvet <sup>(2)</sup>. Ezért az EKB/2013/1 határozatban <sup>(3)</sup> helyénvaló a 910/2014/EU rendeletre hivatkozni.
- (2) Aktualizálni kell a KBER-PKI hitelesítés-szolgáltatóra vonatkozó, az EKB/2013/1 határozat mellékletében meghatározott információkat, beleértve annak személyazonosságát és technikai összetevőit.
- (3) Az EKB/2013/1 határozatot erre tekintettel megfelelően módosítani szükséges,

ELFOGADTA EZT A HATÁROZATOT:

#### 1. cikk

#### Módosítások

Az EKB/2013/1 határozat a következőképpen módosul:

1. Az 1. cikk 10. pontja helyébe a következő szöveg lép:

„10. »KBER-PKI hitelesítés-szolgáltató«: az a jogalany, amelyet a felhasználók a KBER/SSM tanúsítványelfogadási keretrendszerrel összhangban megbíztak a KBER-PKI tanúsítványok kibocsátásával, kezelésével, visszavonásával és megújításával;”.

2. A 4. cikk (4) bekezdésének helyébe a következő szöveg lép:

„(4) A KBER-PKI tanúsítványalkalmazási nyilatkozata egy olyan szabályzat, amely az elektronikus tanúsítványok életciklusát a kezdeti kérelemtől az előfizetés lejártáig illetve annak visszavonásáig, valamint a tanúsítvány-igénylő vagy előfizető, a KBER-PKI hitelesítés-szolgáltató és az érintett felek közti jogviszonyokat szabályozza. Kiterjed az

<sup>(1)</sup> Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 73. o.).

<sup>(2)</sup> Az Európai Parlament és a Tanács 1999/93/EK irányelve (1999. december 13.) az elektronikus aláírásra vonatkozó közösségi keretfeltételekről (HL L 13., 2000.1.19., 12. o.).

<sup>(3)</sup> Az Európai Központi Bank EKB/2013/1 határozata (2013. január 11.) a Központi Bankok Európai Rendszere nyilvános kulcsú infrastruktúrája keretrendszerének meghatározásáról (HL L 74., 2013.3.16., 30. o.).

1999/93/EK irányelv és a 910/2014/EU európai parlamenti és tanácsi rendelet (\*) hatálya alá tartozó, illetve az azok hatályán kívül eső tanúsítványokra is. Meghatározza továbbá a felek feladataira és felelősségeire vonatkozó szabályokat, valamint a tanúsítványok kibocsátására és kezelésére vonatkozó szabályokat. A nyilatkozat a 2. és 3. szintű megállapodás mellékletét képezi.

(\*) Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 73. o.)”

3. A 10. cikk (1) bekezdésének bevezető fordulata és a) pontja helyébe a következő szöveg lép:

„(1) Azt az esetet kivéve, ha bizonyítják, hogy nem terheli őket gondatlanság, az eurorendszer-beli központi bankok a KBER-PKI-n belüli feladataikkal és felelősségeikre tekintettel felelősek minden olyan felhasználónak okozott kárért, amely ésszerűen hagyatkozik valamely jóváhagyott tanúsítványra az 1999/93/EK irányelvben és a 910/2014/EU rendeletben meghatározottak szerint, az alábbiak tekintetében:

a) a minősített tanúsítvány kibocsátásának időpontjában az abban foglalt valamennyi adat helytállóságáért, valamint azért, hogy a tanúsítvány tartalmazza-e az 1999/93/EK irányelvben és a 910/2014/EU rendeletben a minősített tanúsítvánnyal kapcsolatban előírt adatokat;”

4. A melléklet helyébe ezen határozat melléklete lép.

## 2. cikk

### Hatálybalépés

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő harmadik napon lép hatályba.

Kelt Frankfurt am Mainban, 2015. december 11-én.

az EKB elnöke

Mario DRAGHI

## MELLÉKLET

„MELLÉKLET

**A KBER-PKI hitelesítés-szolgáltatóval kapcsolatos információk, beleértve annak személyazonosságát és technikai összetevőit**

A KBER-PKI hitelesítés-szolgáltatót a tanúsítványában kibocsátóként azonosították, és annak magánkulcsát tanúsítványok aláírásához használják. A KBER-PKI hitelesítés-szolgáltató az alábbiakért felelős:

- i. a magánkulcsok és a nyilvános kulcsok tanúsítványainak kibocsátása;
- ii. a visszavonási listák közzététele;
- iii. az egyes tanúsítványokhoz kapcsolódó kulcspárok létrehozatala, például azokhoz, amelyekhez kulcshelyreállítás szükséges;
- iv. a KBER-PKI-ért való átfogó felelősség viselése, valamint annak biztosítása, hogy az annak működtetéséhez szükséges valamennyi követelmény teljesüljön.

A KBER-PKI hitelesítés-szolgáltató magában foglalja mindazon személyeket, politikákat, eljárásokat és számítástechnikai rendszereket, amelyek az elektronikus tanúsítványok kibocsátását, valamint azoknak a tanúsítvány-előfizetőkhez történő rendelkezését végzik.

A KBER-PKI hitelesítés-szolgáltató az alábbi két technikai összetevőből áll:

— **A KBER-PKI gyökérhitelesítés-szolgáltató:** Ez a hitelesítés-szolgáltató az első szinten kizárólag saját maga, valamint az alárendelt hitelesítés-szolgáltatói számára bocsát ki tanúsítványokat. Csak abban az esetben működik, ha a saját, szűkkörűen meghatározott feladatait látja el. A legfontosabb adatai az alábbiak:

a) SHA-1 tanúsítvány<sup>(1)</sup>:

<b>Distinguished name (Megkülönböztető név)</b>	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
<b>Serial number (Sorozatszám)</b>	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
<b>Distinguished name of issuer (A kibocsátó megkülönböztető neve)</b>	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
<b>Validity period (Érvényességi időszak)</b>	From 21-06-2011 11:58:26 to 21-06-2041 11:58:26
<b>Message digest (Az üzenet kivonata) (SHA-1)</b>	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192
<b>Message Digest (Az üzenet kivonata) (SHA-256)</b>	C919 CF49 C024 7E50 2E0C C3C9 81E0 FB88 A013 AA2B 15C9 5142 F491 BDE7 E403 E3FB
<b>Cryptographic algorithms (Kriptográfiai algoritmusok)</b>	SHA-1/RSA 4096

b) SHA-256 tanúsítvány:

<b>Distinguished name (Megkülönböztető név)</b>	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
<b>Serial number (Sorozatszám)</b>	4431 9C5F 91E8 162F 4E00 73F6 6AB8 71D8

<sup>(1)</sup> Ez a tanúsítványt csak olyan rendszerekben fogják használni, amelyek nem támogatnak magasabb algoritmusokat.

<b>Distinguished name of issuer (A kibocsátó megkülönböztető neve)</b>	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
<b>Validity period (Érvényességi időszak)</b>	From 21-06-2011 12:35:34 to 21-06-2041 12:35:34
<b>Message Digest (Az üzenet kivonata) (SHA-1)</b>	3663 2FBA FB19 BDBC A202 3994 1926 ED48 4D72 DD4B
<b>Message Digest (Az üzenet kivonata) (SHA-256)</b>	7963 2A97 1D12 A889 9724 BB35 C37B 51D2 3E21 4DF9 20C3 2450 093E 0EA7 49FB AAEB
<b>Cryptographic algorithms (Kriptográfiai algoritmusok)</b>	SHA-256/RSA 4096

- **A KBER-PKI onlinehitelesítés-szolgáltató:** Ez a hitelesítés-szolgáltató a második szinten a KBER-PKI gyökérhitelesítés-szolgáltató alá van rendelve. A KBER-PKI tanúsítványok felhasználók részére történő kibocsátásáért felelős. A legfontosabb adatai az alábbiak:

- a) SHA-1 tanúsítvány<sup>(1)</sup>:

<b>Distinguished name (Megkülönböztető név)</b>	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
<b>Serial number (Sorozatszám)</b>	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
<b>Distinguished name of issuer (A kibocsátó megkülönböztető neve)</b>	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
<b>Validity period (Érvényességi időszak)</b>	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
<b>Message digest (Az üzenet kivonata) (SHA-1)</b>	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08
<b>Message Digest (Az üzenet kivonata) (SHA-256)</b>	4B18 7644 BF79 4F83 D000 999D 7927 433F 75F3 CFB1 643A 6D0F 8A25 9435 BE86 1B7A
<b>Cryptographic algorithms (Kriptográfiai algoritmusok)</b>	SHA-1/RSA 4096

- b) SHA-256 tanúsítvány:

<b>Distinguished name (Megkülönböztető név)</b>	CN= ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
<b>Serial number (Sorozatszám)</b>	660C 9B12 9A0A 6C21 5509 38DD 54A0 ED2D
<b>Distinguished name of issuer (A kibocsátó megkülönböztető neve)</b>	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
<b>Validity period (Érvényességi időszak)</b>	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
<b>Message digest (SHA-1) (Az üzenet kivonata (SHA-1))</b>	E976 D216 4A5F 62DA C058 6BE0 EC10 EF24 36B8 12AC
<b>Message Digest (SHA-256) (Az üzenet kivonata (SHA-256))</b>	1335 26DC 99E9 CC36 62F8 F5FA 2006 3005 BA90 E663 2BF3 4F18 A84B A39B 5FAA 5700
<b>Cryptographic algorithms (Kriptográfiai algoritmusok)</b>	SHA-256/RSA 4096"

<sup>(1)</sup> Ez a tanúsítványt csak olyan rendszerekben fogják használni, amelyek nem támogatnak magasabb algoritmusokat.