A BIZOTTSÁG (EU) 2016/650 VÉGREHAJTÁSI HATÁROZATA

(2016. április 25.)

a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendeletre [1] és különösen annak 30. cikke (3) bekezdésére és 39. cikkének (2) bekezdésére,

mivel:

(1) A 910/2014/EU rendelet II. melléklete meghatározza a minősített elektronikus aláírást és a minősített elektronikus bélyegzőt létrehozó eszközökre vonatkozó követelményeket.

(2) A szóban forgó termékek előállításához és forgalomba hozatalához szükséges műszaki előírásoknak a technológia mindenkori helyzetének figyelembevételével történő kidolgozásával a szabványosítás területén illetékes szervezetek foglalkoznak.

(3) Az ISO/IEC (Nemzetközi Szabványügyi Szervezet/Nemzetközi Elektrotechnikai Bizottság) megállapítja az informatikai biztonság általános fogalmait és elveit, valamint meghatározza az informatikai eszközök biztonsági jellemzőire vonatkozó értékelés alapjául szolgáló általános értékelési modellt.

(4) Az Európai Szabványügyi Bizottság (CEN) a Bizottság által adott, M/460 sz. szabványosítási megbízás alapján szabványokat dolgozott ki olyan, minősített elektronikus aláírást és bélyegzőt létrehozó eszközökre vonatkozóan, amelyek esetében az elektronikus aláírás, illetve elektronikus bélyegző létrehozásához használt adatokat teljes egészében – de nem feltétlenül kizárólagosan – a felhasználó által kezelt környezetben tárolják. E szabványok alkalmasnak tekinthetők annak értékeléséhez, hogy az ilyen eszközök megfelelnek-e a 910/2014/EU rendelet II. mellékletében megállapított vonatkozó követelményeknek.

(5) A 910/2014/EU rendelet II. melléklete megállapítja, hogy az elektronikus aláírás létrehozásához használt adatokat az aláíró nevében csak minősített bizalmi szolgáltató kezelheti. A biztonsági követelmények és azok vonatkozó tanúsítási előírásai eltérőek abban az esetben, ha az aláíró a terméket fizikailag birtokolja, és amennyiben egy minősített bizalmi szolgáltató folytat az aláíró nevében tevékenységet. Annak érdekében, hogy az előírások mindkét helyzetet lefedjék, valamint hogy idővel lehetővé váljon a speciális igényeket kielégítő termékek és értékelési szabványok kifejlesztése, e határozat mellékletében fel kell sorolni a mindkét helyzetre érvényes szabványokat.

(6) Mire e bizottsági határozat elfogadásra kerül, több minősített bizalmi szolgáltató is kínál majd olyan megoldásokat, amelyek lehetővé teszik, hogy a szolgáltatók elektronikus aláírás létrehozásához használt adatokat kezeljenek ügyfeleik nevében. A terméktanúsítások jelenleg a különféle szabványok szerint tanúsított biztonsági hardvermodulokra korlátozódnak; e termékek tanúsítása azonban még nem a minősített aláírást és bélyegzőt létrehozó eszközökre vonatkozó követelmények szerint történik. Mindazonáltal a közzétett szabványok, mint például az EN 419 211 (amely a teljes egészében – de nem feltétlenül kizárólagosan – a felhasználó által kezelt környezetben létrehozott elektronikus aláírásra alkalmazandó) egyelőre nem érintik a távaláírást létrehozó termékek ugyanilyen fontos piacát. Mivel az ilyen célra vélhetően megfelelő szabványok jelenleg kidolgozás alatt állnak, a Bizottság ki fogja egészíti ezt a határozatot, amikor ilyen szabványok már rendelkezésre állnak és az értékelések alapján megfelelnek a 910/2014/EU rendelet II. mellékletben meghatározott követelményeknek. Az ilyen szabványok jegyzékének létrejöttéig a szóban forgó termékek megfelelésértékelésére a 910/2014/EU rendelet 30. cikk (3) bekezdésének b) pontjában előírt feltételekkel alkalmazható egy alternatív folyamat.

(7) A mellékletben szerepel az EN 419 211 szabvány, amely különböző helyzeteket lefedő különféle részekből (1–6.) áll. Az EN 419 211 szabvány 5. része és a 419 211 szabvány 6. része a minősített aláírást létrehozó eszköz

[1] HL L 257., 2014.8.28., 73. o.

környezetével kapcsolatos tartozékokat határoz meg például a megbízható aláírást létrehozó alkalmazásokkal való kommunikáció tekintetében. A gyártók szabadon alkalmazhatnak ilyen tartozékokat. A 910/2014/EU rendelet 56 preambulumbekezdése értelmében a tanúsítás 30. és 39. cikk szerinti hatálya az aláírás létrehozásához használt adatok védelmére korlátozódik, tehát a tanúsítás nem terjed ki az aláírást létrehozó alkalmazásokra.

(8) Annak érdekében, hogy a minősített aláírást vagy bélyegzőt létrehozó eszközzel létrehozott elektronikus aláírások vagy bélyegzők a 910/2014/EU rendelet II. mellékletének követelményei szerint megbízhatóan védve legyenek hamisítás ellen, a megfelelő kriptográfiai algoritmusok, kulcshosszok és hasítófüggvények elengedhetetlenek a tanúsított termék biztonságához. Mivel ezt a kérdést nem harmonizálták uniós szinten, a tagállamoknak együtt kell működniük, hogy megállapodjanak az elektronikus aláírások és bélyegzők céljára használandó kriptográfiai algoritmusokról, kulcshosszokról és hasítófüggvényekről.

(9) E határozat elfogadása nyomán a 2003/511/EK bizottsági határozat [1] elavulttá válik. Ezért az említett határozatot hatályon kívül kell helyezni.

(10) Az ebben a határozatban előírt intézkedések összhangban vannak a 910/2014/EU rendelet 48. cikkében említett bizottság véleményével,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

(1) Azokat az információtechnológiai termékek biztonsági értékelésére vonatkozó szabványokat, amelyek a 910/2014/EU rendelet 30. cikke (3) bekezdésének a) pontja vagy 39. cikkének (2) bekezdése szerint olyan minősített elektronikus aláírást létrehozó eszközök vagy olyan minősített elektronikus bélyegzőt létrehozó eszközök tanúsítására alkalmazandók, amelyek esetében az elektronikus aláírás, illetve elektronikus bélyegző létrehozásához használt adatokat teljes egészében – de nem feltétlenül kizárólagosan – a felhasználó által kezelt környezetben tárolják, e határozat melléklete sorolja fel.

(2) Amíg a Bizottság össze nem állít egy jegyzéket az információtechnológiai termékek biztonsági értékelésére vonatkozó azon szabványokról, amelyek a minősített elektronikus aláírást létrehozó eszközök vagy a minősített elektronikus bélyegzőt létrehozó eszközök olyan esetben történő tanúsítására alkalmazandók, ha az elektronikus aláírás, illetve elektronikus bélyegző létrehozásához használt adatokat az aláíró vagy a bélyegző létrehozója nevében egy minősített bizalmi szolgáltató kezeli, az ilyen termékek tanúsítását egy olyan folyamatra kell alapozni, amely a 910/2014/EU rendelet 30. cikke (3) bekezdésének b) pontja értelmében a 30. cikk (3) bekezdésének a) pontjában előírt biztonsági szintekhez hasonló szinteket alkalmaz, és amelyet a 30. cikk (1) bekezdése szerinti állami vagy magánszervek bejelentenek a Bizottságnak.

2. cikk

A 2003/511/EK határozat hatályát veszti.

3. cikk

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

Kelt Brüsszelben, 2016. április 25-én.

a Bizottság részéről

az elnök

Jean-Claude JUNCKER

[1] HL L 175., 2003.7.15., 45. o.

MELLÉKLET

AZ 1. CIKK (1) BEKEZDÉSÉBEN EMLÍTETT SZABVÁNYOK JEGYZÉKE

— ISO/IEC 15408 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 1–3. rész az alábbiak szerint:

  — ISO/IEC 15408-1:2009 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 1. rész. ISO, 2009

  — ISO/IEC 15408-2:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 2. rész. ISO, 2008

  — ISO/IEC 15408-3:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés szempontjai, 3. rész. ISO, 2008

  és

— ISO/IEC 18045:2008 – Informatika – Biztonságtechnika – Az informatikai biztonságértékelés módszertana,

  és

— EN 419 211 – Biztonságos aláírás-létrehozó eszköz védelmi profiljai, 1–6. rész – adott esetben – az alábbi felsorolás szerint:

  — EN 419211-1:2014 – Biztonságos aláírás-létrehozó eszköz védelmi profilja – 1. rész: Áttekintés

  — EN 419211-2:2013 – Biztonságos aláírás-létrehozó eszköz védelmi profilja – 2. rész: Kulcsgenerálós eszközök

  — EN 419211-3:2013 – Biztonságos aláírás-létrehozó eszköz védelmi profilja – 3. rész: Kulcsimportáló eszközök

  — EN 419211-4:2013 – Biztonságos aláírás-létrehozó eszköz védelmi profilja – 4. rész: Tartozék kulcsgeneráló eszközökhöz és megbízható csatorna tanúsítványgeneráló alkalmazáshoz

  — EN 419211-5:2013 – Biztonságos aláírás-létrehozó eszköz védelmi profilja – 5. rész: Tartozék kulcsgeneráló eszközökhöz és megbízható csatorna aláírás-létrehozó alkalmazáshoz

  — EN 419211-6:2014 – Biztonságos aláírás-létrehozó eszköz védelmi profilja – 6. rész: Tartozék kulcsimportáló eszközökhöz és megbízható csatorna aláírás-létrehozó alkalmazáshoz