Másodfokú döntés-előkészítő osztály

Iktatószám: MD/26838-17/2011.
Ügyintéző: Pappné dr. Mineva Júlia
Tárgy: NetLock Informatikai és Hálózatbiztonsági Kft. fellebbezése

Határozat

A Nemzeti Média- és Hírközlési Hatóság Elnökhelyettese (a továbbiakban: **másodfokú hatóság**) a NetLock Informatikai és Hálózatbiztonsági Kft. (1023 Budapest, Zsigmond tér 10., cg: 01-09-563961; a továbbiakban: **Szolgáltató** vagy **Fellebbező**) által a Nemzeti Média- és Hírközlési Hatóság Hivatala (a továbbiakban: **elsőfokú hatóság**) 2011. szeptember 27-én kelt EF/26838-8/2011. számú határozata (a továbbiakban: **elsőfokú határozat**) ellen benyújtott fellebbezését

elutasítja,

és az elsőfokú határozatot

helybenhagyja.

A másodfokú határozat a közléssel jogerőssé válik.

A másodfokú határozat ellen a közlés napjától számított 30 napon belül jogszabálysértésre hivatkozással, az illeték előzetes lerovása nélkül, a Fővárosi Bíróságnak címzett, de az elsőfokú határozatot hozó hatóságnál előterjesztett keresettel lehet élni. A közigazgatási határozat felülvizsgálata iránti perben az ügyfél és a kifejezetten rá vonatkozó rendelkezés tekintetében az eljárás egyéb résztvevője tárgyalás tartását kérheti a bíróságtól.

A keresetlevél benyújtásának a határozat végrehajtására nincs halasztó hatálya, a bírósági felülvizsgálat kezdeményezésére jogosult azonban a keresettel támadott hatósági határozat végrehajtásának felfüggesztését kérheti.

Indokolás

Az elsőfokú hatóság az elektronikus aláírásról szóló 2001. évi XXXV. törvény (a továbbiakban: **Eat.**) 18. §-ában foglalt hatáskörében, az Eat 17. § (2) bekezdése alapján a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (a továbbiakban: **Ket.**) rendelkezéseinek megfelelően, hivatalból eljárást indított a Szolgáltatóval szemben az Eat. 6. § (1) bekezdése szerinti elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható biztonságos kriptográfiai algoritmusok, illetve az ezekhez tartozó paraméterek megállapítása tárgyában. Az elsőfokú hatóság az elsőfokú határozatában kötelezte a Szolgáltatót, hogy az elsőfokú határozat jogerőre emelkedésétől számított 30 napon belül az elektronikus aláírással kapcsolatos szolgáltatásainak nyújtása során használt algoritmusokat és paramétereket az elsőfokú határozat 1. számú mellékletének megfelelően állítsa be. Az elsőfokú hatóság felhívta a Szolgáltató figyelmét, hogy az elsőfokú határozatában foglaltak végrehajtását ellenőrizni fogja és a döntés nem, vagy nem megfelelő teljesítése esetén az Eat. 21-23. §-ai szerinti jogkövetkezményeket alkalmazhatja.

A Szolgáltató az elsőfokú határozat ellen – a törvényes határidőn belül – fellebbezést nyújtott be, amelyben az elsőfokú határozat megváltoztatását, illetve hatályon kívül helyezését, továbbá az elsőfokú hatóság új eljárásra való kötelezését kérte.

Elöljáróban a Fellebbező előadta, hogy álláspontja szerint az elsőfokú határozat végrehajtása súlyosabb következményekkel járna, mint a végrehajtás elmaradása, továbbá fogyasztói bizalomvesztést eredményezne valamennyi szolgáltatóra nézve, egyébiránt pedig a döntés több szempontból végrehajthatatlan és nincs összhangban az European Telecommunications Standards Institute (ETSI) ETSI TS 102 176-1 V2.1.1 (2011-07) számon kiadott dokumentumban (a továbbiakban: **ETSI dokumentum** vagy **ALGO paper**) foglaltakkal.

Fellebbezésében kifogásolta, hogy az elsőfokú határozat nem tartalmaz rendelkezéseket a határozat jogerőre emelkedését megelőzően kiadott tanúsítványokkal kapcsolatos szolgáltatói kötelezettségek vonatkozásában, valamint, hogy az elsőfokú hatóság informális e-mail üzenetben, az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 3/2005. (III. 18.) IHM rendeletre (a továbbiakban: **R.**) való utalással értesítette a Szolgáltatót a korábban kiadott, minősített tanúsítványok visszavonásával kapcsolatos kötelezettségéről.

A Fellebbező azt is sérelmezte, hogy az elsőfokú hatóság által 2005-ben és 2008-ban hozott algoritmus határozatokkal ellentétben a jelen fellebbezés tárgyát képező elsőfokú határozat konkrét, „kötelező" időpontot jelöl meg a kriptográfiai algoritmusok felhasználhatósági idejét illetően. Álláspontja szerint a tárgyi határozat nem biztosít az egyes hitelesítés-szolgáltatóknak és felhasználóiknak kellő felkészülési időt arra, hogy „a korábbi tanúsítványok akár azonnali visszavonására felkészüljenek addig, ameddig műszakilag valóban nem indokolt a már korábban kibocsátott tanúsítványok cseréje".

A Fellebbező szerint az, hogy az elsőfokú határozat értelmében a korábban kiadott minősített tanúsítványokat a Szolgáltató csak 2011. december 31-ig használhatja, több aspektusból – technikai, műszaki, adminisztratív okokból, valamint az ágazat megítélése szempontjából – sincs összhangban a már hivatkozott ETSI dokumentum tartalmával, amely szempontokat a másodfokú hatóság lentebb részletesen kifejt.

Mindezek alapján a Fellebbező kérte az elsőfokú határozat oly módon történő módosítását, hogy

- a meglévő tanúsítványok „még normál élettartalmuknál fogva lejárhassanak" és ne legyen szükség a tanúsítványok azonnali cseréjére,
- az elsőfokú határozatban foglalt időpont a nemzetközi ajánlásokban és iparági szabványokban foglaltakkal összhangban kerüljön módosításra,
- a hitelesítés-szolgáltatók az érintett kriptográfiai algoritmust 2011. december 31-ig kibocsátott tanúsítványokban használhassák és az csak 2013. december 31. után ne legyen alkalmazható.

A fentiek hiányában a Fellebbező az elsőfokú határozat hatályon kívül helyezését és az elsőfokú hatóság új eljárásra való kötelezését kérte.

A másodfokú hatóság a Ket. 104. § (3) bekezdésének megfelelően az eljárás során az elsőfokú határozatot és az azt megelőző eljárást, valamint a fellebbezésben foglaltakat megvizsgálva az alábbiakat állapította meg:

Az elsőfokú hatóság eleget tett a Ket. 2. § (3) bekezdésében, a 3. § (2) bekezdés *b)* pontjában, valamint az 50. § (1) bekezdésében foglalt tényállás tisztázási, illetve a Ket. 72. § (1) bekezdés *e)* pontja szerinti indokolási kötelezettségének, az elsőfokú hatóság határozatában tett megállapításai helytállóak, a döntése jogszerű.

A másodfokú hatóság rámutat, hogy a fellebbezéssel megtámadott elsőfokú határozat az Eat.-nak a technológiakövetést előíró 18. §-a alapján került kiadásra, miszerint „[a] Hatóság figyelemmel kíséri az elektronikus aláírással kapcsolatos technológia és kriptográfiai algoritmusok fejlődését és határozatba foglalja a szolgáltatók által szolgáltatásaik nyújtása során használható biztonságos kriptográfiai algoritmusokat és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket".

A Eat. hivatkozott előírása értelmében a Nemzeti Média- és Hírközlési Hatóság (a továbbiakban: **Hatóság**) a törvény erejénél fogva köteles nyomon követni az elektronikus aláírással kapcsolatos szolgáltatást nyújtók körében alkalmazott kriptográfiai algoritmusok biztonságos voltát és ezek figyelemmel kísérése folyamán határozatával döntést hozni arról, hogy a szolgáltatók mely kriptográfiai algoritmusokat és a hozzájuk tartozó paramétereket használhatják szolgáltatásaik nyújtása során. A Hatóság ezen döntését az elektronikus aláírással kapcsolatos szolgáltatások megbízhatóságának fenntartása, a mindenkori, naprakész biztonsági követelményeknek való megfelelés érdekében hozza.

A másodfokú hatóság a Fellebbező indokait nem találta alaposnak az alábbiak miatt:

Nem megalapozott a Fellebbező azon kifogása, hogy **az elsőfokú határozat nem tartalmaz rendelkezéseket a már kiadott tanúsítványokkal kapcsolatos kötelezettségek vonatkozásában**, valamint, hogy a Szolgáltató **informális e-mail üzenetben kapott tájékoztatást az érintett tanúsítványok visszavonására vonatkozó kötelezettségekről**.

Az elsőfokú határozat – az elsőfokú hatóság korábbi gyakorlatával megegyezően – valóban nem tartalmaz rendelkezéseket, előírásokat a tárgyi határozat jogerőre emelkedését megelőzően kiadott tanúsítványokkal kapcsolatos szolgáltatói kötelezettségek tekintetében. Megjegyzi a másodfokú hatóság ugyanakkor, hogy a szolgáltatóknak a mindennapi tevékenységük gyakorlása során tisztában kell lenniük a rájuk vonatkozó hatályos jogi szabályozással. A már fentebb említett, a fellebbezésben is hivatkozott R. 36. § (1) bekezdése egyértelmű szabályozást tartalmaz a minősített tanúsítvány érvényességi idejét illetően. E rendelkezés szerint a minősített tanúsítvány érvényességi ideje nem haladhatja meg azt az időt, amely időpontig a felhasznált kriptográfiai algoritmusok a Hatóság Eat. 18. § szerint kibocsátott határozata értelmében biztonságosan felhasználhatók, de legfeljebb a kibocsátástól számított 2 évet. Az Eat. 18. §-a csak a biztonságos kriptográfiai algoritmusok, illetve az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelmények meghatározására ad felhatalmazást a Hatóságnak. Az elsőfokú hatóságnak nem feladata, hogy megismételje határozatában a jogszabályon alapuló, jelen esetben az R.-ből közvetlenül eredő, az algoritmus határozat kiadásával közvetetten összefüggő egyéb szolgáltatói kötelezettségeket. Amennyiben a Szolgáltató a határozatban foglalt kötelezettségeinek eleget tesz, és a megfelelő biztonságos algoritmusokat alkalmazza, ezzel kapcsolatosan további ellenőrzési kötelezettsége is keletkezik a már kiadott tanúsítványainak felülvizsgálatával kapcsolatosan, hogy azok megfelelnek-e a 2005 óta változatlanul fennálló jogszabályi rendelkezésnek.

Az pedig, hogy az elsőfokú hatóság – az önkéntes jogkövetést előmozdító, figyelemfelhívó céllal – e-mailben tájékoztatta a szolgáltatókat az R. 36. § (1) bekezdésében foglaltakról és az érintett tanúsítványok visszavonására vonatkozó kötelezettségükről csupán azt bizonyítja, hogy az elsőfokú hatóság maximálisan ügyfélbarát módon járt el a szolgáltatókkal szemben.

A Fellebbező azon kifogásaival kapcsolatban, hogy **az elsőfokú határozat a korábban kiadott algoritmus határozatokkal ellentétben konkrét, „kötelező" időpontot jelöl meg a kriptográfiai algoritmusok felhasználhatósági idejét illetően**, a másodfokú hatóság az alábbiakra mutat rá.

Az Eat. 18. §-a alapján a Hatóságnak korlátlan jogköre van a biztonságos kriptográfiai algoritmusok meghatározására, valamint azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelmények előírására, így a megfelelő jogtechnikai megoldás kiválasztására és esetlegesen a felhasználhatósági időpont meghatározására is.

Az elsőfokú hatóság azért jelölt meg konkrét időpontot az algoritmusok felhasználhatósági idejét illetően, mert amennyiben a korábbi, időpont megjelölése nélküli jogtechnikai megoldást alkalmazza, akkor az algoritmus határozata nem tartalmazta volna a nem biztonságosnak tekintett algoritmusokat, így az sh1-with-rsa algoritmust sem és ezt már a határozat jogerőre emelkedését követően nem lehetett volna alkalmazni. Az elsőfokú hatóság által választott, a korábbitól valóban eltérő jogtechnikai megoldás alapján a vonatkozó algoritmus nem a határozat jogerőre emelkedésig, hanem 2011. december 31-éig használható, vagyis ezzel lehetővé vált az algoritmusok további, közel három hónapos felhasználása, ami sokkal kedvezőbb megoldás a szolgáltatók számára.

Ez a megoldás tehát – a Fellebbező által előadottakkal szemben – éppen a megfelelő átállás és intézkedési kötelezettségek végrehajtása érdekében, vagyis a **megfelelő felkészülési idő** biztosítása céljából került kiválasztásra. A kellő felkészülési idő biztosításával kapcsolatban megjegyzendő továbbá, hogy már a 2008-ban kiadott, HL-21917-14/2008. számú algoritmus határozat (melynek címzettje a Fellebbező volt) kifejezetten figyelmeztetett az adott sha1-with-rsa algoritmus vonatkozásában annak kockázataira, így az algoritmus közeljövőben történő kiváltásával kapcsolatos intézkedési szükségletekre is. A hivatkozott algoritmus határozat 2. számú mellékletében található, a kriptográfiai algoritmuskészletek ajánlott felhasználási idejére vonatkozó megjegyzés szerint: „[a] szolgáltató dönthet úgy, hogy az olyan algoritmuskészleteket, amelyek ajánlott felhasználási ideje 2008. év végéig tart, a szolgáltatás nyújtása során 2009. év végéig használja fel, azonban ebben az esetben megfelelően fel kell készülnie arra, hogy az algoritmuskészlet meggyengülése esetén a szükséges intézkedéseket haladéktalanul meg tudja tenni és ennek érdekében az előfizetőkkel is ennek megfelelően kell megállapodnia”.

Ezt követően az elsőfokú hatóság a 2009-ben, 2010-ben és 2011-ben történt éves, helyszíni ellenőrzéseken folyamatos tájékoztatást kért a szolgáltatók algoritmusváltásra történő felkészüléséről. A 2011.06.01-én tartott hatósági helyszíni ellenőrzéskor az elsőfokú hatóság külön felhívta a Fellebbező figyelmét arra, hogy az év folyamán, de legkésőbb év végéig új algoritmus határozat kiadását tervezi, és az sha1-with-rsa algoritmusok felhasználhatósága 2012-ben már nem lesz megengedett. Ezt tanúsítja a helyszíni szemléről felvett jegyzőkönyv (iktatószám: EF/7367-5/2011.) 5. számú melléklet 3. pontja is, amely a következő megállapítást tartalmazza: „A Szolgáltató az algoritmusváltásra felkészült. A Hatóság jelezte, hogy az alkalmazható algoritmusokra vonatkozó követelményekben az év folyamán változás várható.”

Mindezekből kifolyólag megállapítható, hogy a Fellebbező nemcsak, hogy 2008 óta tisztában volt az adott algoritmusváltás szükségességével, de a 2011. évi hatósági ellenőrzés alkalmával maga nyilatkozott arról, hogy felkészült az algoritmusváltásra.

A Fellebbező okfejtése szerint az, hogy **az elsőfokú határozat** 2011. december 31-ét követő időponttal „megtiltja” a korábban kiadott minősített tanúsítványok használatát, több okból **nincs összhangban az ETSI dokumentum tartalmával**.

A Fellebbező **technikai – szabályozási kérdések** címén az alábbi érveket hozta fel:

Hivatkozott egyrészt **az ALGO paper 5.2.1 pont NOTE 2.** megjegyzésre, amely az SHA-1 algoritmust „jelentős mértékben ellenállónak, azaz biztonságosnak tekinti abban az esetben, ha a tanúsítvány megfelelő mennyiségű véletlen adatot tartalmaz”. A Fellebbező előadta, hogy 2010. október 29. után kiadott minden tanúsítványa megfelel az ETSI dokumentumnak, az SHA-1 algoritmus biztonságos alkalmazásával kapcsolatos követelményeinek.
Tekintettel arra, hogy az ALGO paper 5.2.1 pont NOTE 2. megjegyzése egyértelműen és kiemelten kimondja, hogy az SHA-1 algoritmust nem lehet alkalmazni dokumentumok aláírására („SHA-1 SHOULD NOT be used for document signatures”), a másodfokú hatóság nem tudta elfogadni az ezzel kapcsolatos fellebbezői érvelést.

A Fellebbező másrészt felhozta **az ALGO paper 9.2 pontjában foglaltakat**, amely pont az érintett algoritmusok javasolt alkalmazhatósági időtartamáról rendelkezik. Ehhez kapcsolódóan a Fellebbező előadta, hogy az e pontban szereplő táblázat feletti magyarázatból ("3 years" in table 7 means "until the end of 2014" and so on) visszaszámolva az érintett SHA-1 algoritmus 1 éven belüli „unusable" státusza 2012. december 31-et jelent, nem pedig 2011. december 31-et, vagyis az elsőfokú határozat az ajánláshoz képest szükségtelenül szűkre szabja az alkalmazhatósági határidőt.

Az ALGO paper 9.2 pontjában 6. számon szereplő táblázat az alábbiakat tartalmazza:

Table 6: recommended hash functions for a resistance during X years

entry name of the hash function	1 year	3 years	6 years	10 years (speculative)
sha1	unusable	unusable	unusable	unusable
ripemd160	unusable	unusable	unusable	unusable
sha224	usable	usable	usable	unknown
sha256	usable	usable	usable	unknown
sha384	usable	usable	usable	usable
sha512	usable	usable	usable	usable
Whirlpool	usable	usable	usable	usable
NOTE: The listed hash functions are expected to be 2nd pre-image resistant and pre-image resistant for a longer period of time.				

A fenti táblázatból megállapítható, hogy az SHA-1 algoritmus egyértelműen „unusable" minősítést kapott az egy éven belüli alkalmazhatóság tekintetében is, ahol az „unusable" azt jelenti, hogy „az algoritmus nem tekinthető biztonságosnak semmilyen elektronikus aláírással kapcsolatos kontextusban". Ezen túlmenően kiemelendő az is, hogy a Fellebbező által hivatkozott „3 év", azaz a „2014 év végéig" történő felhasználhatóságot jelentő megjegyzés a 7. számú, nem pedig a 6. számú táblázatra vonatkozik.
Mindezekre tekintettel a Fellebbező ezen indokai sem helytállóak, ugyanis az ETSI dokumentum az SHA-1 alkalmazhatatlanságát már 2011. júliusában kimondta, és ez a tény a Fellebbező számára is ismert volt.

A Fellebbező harmadrészt az ETSI dokumentumban is említett, **NIST SP 800-131A ajánlásra** hivatkozott, mely 2013 végéig megengedi az SHA-1 algoritmus alkalmazását.
Ezzel kapcsolatban a másodfokú hatóság leszögezi, hogy a NIST dokumentum – melyet az Amerikai Szabványügyi Testület adott ki – az amerikai felhasználási területen tekinthető irányadónak, míg az Európai Unióban az ALGO paper számít mértékadó dokumentumnak. Az elsőfokú hatóság – a korábbi határozatainak és az uniós gyakorlatnak megfelelően – az ALGO papert tartotta megfelelő követelményrendszernek az algoritmusok biztonságosságára vonatkozóan, különös figyelemmel arra, hogy az SHA-1 vonatkozásában már 2005 óta ismertek támadások. Ebből kifolyólag az elsőfokú hatóság az SHA-1 algoritmus 2013 végéig történő alkalmazhatóságát nem tartotta indokoltnak, mely szakmai álláspontját a másodfokú hatóság teljességgel osztja.

A másodfokú hatóság nem tudta elfogadni a Fellebbezőnek **az elsőfokú határozat által megszabott időponttal és a másodfokú eljárási határidővel** kapcsolatos azon kifogásait sem, miszerint a fellebbezés elutasítása esetén a hitelesítés-szolgáltatók és felhasználóik részére irreálisan rövid és teljesíthetetlen idő áll az elsőfokú határozat előírásainak teljesítésére. Az elsőfokú és másodfokú ügyintézési határidők a Fellebbező által ismert tények. A Fellebbező nyilvánvalóan az összes körülmény és kockázat mérlegelésével nyújtotta be a fellebbezést. A fellebbezői érvek ellen szól továbbá az a körülmény is, hogy az elsőfokú hatóság az elsőfokú határozatot, annak kiadását megelőzően, egyeztetés céljából megküldte minden érintett szolgáltatónak (így a Fellebbezőnek is), de arra észrevétel vagy kifogás nem érkezett.

A Fellebbező **műszaki okokból** is sérelmezte az elsőfokú hatóságnak a korábbi minősített tanúsítványok érvényességi idejével és visszavonásával kapcsolatos megállapításait. Kifejtette, hogy esetében közel 3000 tanúsítvány adata fog felkerülni a visszavonási listára és a visszavonások elvégzése a lista jelentős méretnövekedését fogja eredményezni, mely jelentős műszaki gondokat okozhat a Szolgáltatónak.
A másodfokú hatóság hangsúlyozza, hogy egy hitelesítés-szolgáltatónak kezelnie kell tudnia az algoritmusváltást. Megjegyzi továbbá, hogy a visszavonási listával kapcsolatos teendők más szolgáltatóknak nem okoztak problémát, így a fellebbezésben hivatkozott „más szolgáltatók", akik a Fellebbezőnél több tanúsítvány vonatkozásában kötelezettek az intézkedések végrehajtására, a CRL lista hosszúságával kapcsolatos semmilyen aggályt nem jeleztek, azt végrehajthatónak tartják.

A Fellebbező az **ágazat megítélése szempontjából** aggályosnak tartotta, hogy az általa korábban forgalmazott Micardo, valamint a többi szolgáltató által használt Giesecke kártyák (BALE eszközök) tanúsításának 2011. szeptemberében történt lejárta miatt már sor került egy jelentősebb mértékű tanúsítvány visszavonására, így ugyanezen tanúsítványok ismételt visszavonása – véleménye szerint – jelentősen rombolhatja a hitelesítés szolgáltatók megítélését.
A másodfokú hatóság kiemeli, hogy sem az algoritmus határozat meghozatala, sem a biztonságos algoritmusokkal kapcsolatos kötelezettségek teljesítése nem függhet más okokból eredő tanúsítvány-visszavonási intézkedésektől.
A biztonságos algoritmus alkalmazásával kapcsolatos intézkedések a technológiakövetés szükségszerű velejárói. Teoretikusan bármikor, azonnali és rendkívüli intézkedéseket igényel, ha egy-egy algoritmus biztonsága az arra vonatkozó támadások következtében megrendül. Ezeknek az intézkedéseknek a megtételére tehát a Szolgáltatónak elvileg azonnal készen kell állnia, még akkor is, ha pár hónap eltéréssel már ugyanazon tanúsítványok vonatkozásában – a termék tanúsításának lejárta miatt – egyéb intézkedésekre kényszerült.
A BALE eszközök tanúsításának lejárata már a tanúsítvány kiadásának időpontjában ismert volt a Fellebbező számára. A hivatkozott eszközök 2009-ben történt felülvizsgálata során a tanúsító szervezet a 2009. szeptember 18-án és 2009. szeptember 30-án kelt felülvizsgálati jegyzőkönyveiben külön feltüntette, hogy az adott tanúsítványok érvényességét az RSA 1024-es, valamint az SHA-1 algoritmusok használhatóságának időpontjáig, de legfeljebb további 2 évre hosszabbítja meg azzal, hogy amennyiben a Hatóság megtiltja a BALE által használt RSA 1024 illetve SHA1 algoritmusok használatát, vagy a szakirodalomban megjelennek ezek gyengeségére vonatkozó konkrét adatok, akkor a tanúsítványok érvényességét a tanúsító szervezet visszavonja.
Mivel a Fellebbező mindezekről tudomással bírt, így sem a BALE eszközök tanúsítottságának megszűnése, sem a későbbiekben bekövetkező algoritmusváltás nem tekinthető olyan rendkívüli eseménynek, melyet ne lehetett volna előre látni és felkészülni rá.
A másodfokú hatóság álláspontja szerint az ágazat megítélésének javítását éppen a technológiakövetésből eredő szolgáltatói kötelezettségek teljesítése és a már nem biztonságosnak tekintett algoritmusok „kivezetése" szolgálja.

Végül a Fellebbező **adminisztratív okokból** sérelmezte az elsőfokú hatóság döntését. Kifejtette, hogy a biztonságos aláírás-létrehozó eszközön történő tanúsítvány-kibocsátás és az eszközre töltés adminisztratív időigénye jelentősen megnehezíti az ilyen rövid idő alatt történő mennyiségi tanúsítványcserét, különösen a normál menetben történő egyéb tanúsítványkiadás mellett.
Ezzel kapcsolatosan a másodfokú hatóság kiemeli, hogy az algoritmusok biztonságával kapcsolatos döntések szükségszerűen rendkívüli intézkedéseket igényelnek, de a szolgáltatóknak képesnek kell lenniük ezeket végrehajtani.

Tekintettel arra, hogy a másodfokú hatóság az elsőfokú határozatot jogszerűnek és szakmailag megalapozottnak tartotta, a fellebbezést elutasította.

A Nemzeti Média- és Hírközlési Hatóság Elnöke a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény (a továbbiakban: **Mttv.**) 111. § (2) bekezdés *n)* pontja szerinti másodfokú hatósági döntési hatáskörét – az Mttv. 112. § (2) bekezdése alapján – az elnökhelyettesre delegálta.

A másodfokú hatóság a kifejtettek, illetve a Nemzeti Média- és Hírközlési Hatóság Szervezeti és Működési Szabályzat II. fejezetének 5.3. b) pontja és IV. fejezetének 16.1. *g)* pontja alapján delegált hatáskörében, valamint Ket. 105. § (1) bekezdésében meghatározott hatósági jogkörében eljárva, a már hivatkozott jogszabályi rendelkezések alapján a rendelkező részben foglaltak szerint határozott.

A határozat meghozatalánál a bírósági felülvizsgálat lehetőségéről szóló tájékoztatás az Eht. 44. § (3)-(5) bekezdésein alapul. A közigazgatatási határozat bírósági felülvizsgálatának illetéke tekintetében az illetékekről szóló 1990. évi XCIII. törvény 62. § (1) bekezdés *h)* pontja az irányadó.

Budapest, 2011. november 16.

Mátrai Gábor
hírközlési elnökhelyettes

A határozatot kapják:

1. Nemzeti Média- és Hírközlési Hatóság Hivatala E-szolgáltatás felügyeleti Osztály
   (1088 Budapest, Reviczky utca 5.)
2. NetLock Informatikai és Hálózatbiztonsági Kft.
   (1023 Budapest, Zsigmond tér 10.)
3. Irattár