NETLOCK
Az Első Hitelesítés-szolgáltató
cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

**SAJTÓKÖZLEMÉNY**
**AZONNALI KÖZLÉSRE**
**2009. június 02.**

# Ismét a NetLock az első hitelesítés-szolgáltató

- *A NetLock Kft. új hitelesítési algoritmussal működő tanúsítványai már az egész világon elérhetőek a Microsoft Windows operációs rendszerrel rendelkező számítógépeken*
- *A NetLock Kft. új hitelesítési algoritmussal működő tanúsítványai megfelelnek a hitelesítés-szolgáltatókat felügyelő szervek határozatának*
- *Az új SHA-256 típusú kriptográfiai lenyomatképző algoritmusok a jelenleginél is erősebb hitelesítést tesznek lehetővé, hiszen az általuk képzett lenyomatokat csak $1{,}16 \times 10^{77}$-en számú próbálkozással lehet visszafejteni*

**Budapest, 2009. június 02**. – A NetLock Kft., a magyarországi hiteles elektronikus ügyintézés vezető vállalata a hazai piacon ismét elsőként jelent meg a Microsoft Internet Explorerben a legfrissebb kriptográfiai ajánlásoknak, szabványoknak megfelelő, újonnan bevezetett SHA-256 típusú kriptográfiai lenyomatképző algoritmust használó tanúsítványkiadóival, amelyek a jelenleg használt SHA-1 technológiával működő kiadók mellett működnek majd. Annak ellenére, hogy az SHA-1 algoritmus „feltörése" még rendkívül távol van, az Európai Unió irányadó szervei a technológiai fejlődésre felkészülve 2009 végétől a még nagyobb szintű biztonságot nyújtó új titkosítási algoritmus használatát javasolja a fokozatos átmenet biztosítása érdekében. Az SHA-256 algoritmust alkalmazó tanúsítványok visszafejthetősége gyakorlatilag nulla, hiszen azokat csak 115 quattuorvigintillion számú próbálkozással lehet visszafejteni, amely közelíti a látható világegyetem atomjainak számát.

Az elektronikus aláírás létrehozására és ellenőrzésére szolgáló tanúsítványok a hiteles elektronikus kommunikáció legfontosabb eszközei. Napjainkban számos területen jelen vannak, megtalálhatók többek között az elektronikus számlázásnál, bizonylatmegőrzésnél, archiválásnál, az elektronikus cégeljárásban és az egészségügyben. Emellett alkalmazzák őket az elektronikus ügyintézést lehetővé tevő önkormányzatok, a vizsgaszervezők, a közzétételre kötelezettek, a digitális tachográf rendszer, de ebbe a körbe sorolhatók a minden komoly weboldal védelmét ellátó, ún. SSL tanúsítványokat használó vállalatok és intézmények is.

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

Az Európai Unió kriptográfia szabványosítása kapcsán irányadó testülete, az European Telecommunications Standards Institute (ETSI) legfrissebb vonatkozó ajánlásának (ETSI TS 102 176-1 v2.0.0) hatására a hazai hitelesítés-szolgáltatókat felügyelő szerv, a Nemzeti Hírközlési Hatóság (NHH) 2008. július 9-én közzétette az elektronikus aláírással kapcsolatos szolgáltatások nyújtása során alkalmazható megbízható kriptográfiai algoritmusokról és paraméterekről szóló határozatát. A határozat (HL-21917-14/2008) kifejti, hogy a kriptográfia fejlődésének és a számítási erőforrások gyors növekedésének következtében a jelenleg széles körben használt SHA-1 algoritmussal működő tanúsítványok fokozatos felváltása érdekében a hitelesítés-szolgáltatók készüljenek fel a magasabb szintű titkosítási algoritmusokat használó tanúsítványok kibocsátására.

A NetLock Kft. 1999-ben, a hazai piacon elsőként jelent meg a Microsoft termékekben mint megbízható legfelső szintű hitelesítés-szolgáltató és az elmúlt évtizedben mindig arra törekedett, hogy élen járjon a legbiztonságosabb technológiák bevezetésében. Az NHH határozatának megfelelve kialakította új típusú tanúsítványkiadóit, amelyeket a piacvezető Internet Explorerben már 2009. február 26-tól megtalálhatunk, de hamarosan szinte minden böngészőben jelen lesznek a megbízható hitelesítés-szolgáltatók tanúsítványkiadói között. A felhasználók az első SHA-256 algoritmust alkalmazó tanúsítványokkal a NetLock Kft. – Magyarországon szintén egyedülálló – hamarosan induló online SSL tanúsítvány kibocsátó szolgáltatása keretében találkozhatnak.

„Az Nemzeti Hírközlési Hatóság határozata elsősorban az aláíró tanúsítványokra van hatással, illetve az ilyen típusú tanúsítvánnyal rendelkezők közül is elsősorban azokat érinti, akik 2009 végéig érvényes tanúsítvánnyal rendelkeznek” – fogalmazott Rózsahegyi Zsolt, a NetLock Kft. ügyvezető igazgatója. „A NetLock aláíró tanúsítvánnyal rendelkező felhasználók számára vállalatunk szakemberi ingyenes konzultációs lehetőséget biztosítanak az egyszerű és gördülékeny átálláshoz” – tette hozzá Rózsahegyi Zsolt.

**A legnépszerűbb algoritmusok visszafejthetősége**

- MD5 kriptográfiai algoritmus

  Az MD5 esetén a képzett lenyomat hossza 128 bit (39 karakter), amelyet $3.4 \times 10^{38}$ – on próbálkozással lehet visszafejteni, ami pontosan 340 undecillion lehetőség.

cím: 1023 Budapest, Zsigmond tér 10.
telefon: (06 1) 345 2255
telefax: (06 1) 345 2250
www.netlock.hu

- SHA-1 kriptográfiai algoritmus

  Az SHA-1 esetén a képzett lenyomat hossza 160 bit (49 karakter), amelyet $1.46 \times 10^{48}$ – on próbálkozással lehet visszafejteni, ami pontosan 1 quindecillion lehetőség.

- SHA-256 kriptográfiai algoritmus

  Az SHA-256 esetén a képzett lenyomat hossza 256 bit (79 karakter), amelyet $1.16 \times 10^{77}$ – en próbálkozással lehet visszafejteni, ami pontosan 115 quattuorvigintillion lehetőség, ami közelíti a látható világegyetem atomjainak számát.

**A NetLock Kft.-ről**

A NetLock Kft. Magyarország vezető hitelesítés-szolgáltató, PKI tanácsadó és PKI rendszerintegrátor vállalataként a hazai elektronikus ügyintézés és ügyvitel meghatározó szereplője. Több mint tízéves tevékenysége során megszerezte a hitelesítés-szolgáltatásban Magyarországon elérhető legmagasabb szintű minősítéseket, a felhalmozott szakmai tudásnak köszönhetően pedig a PKI technológia egyik vezető szakértő vállalatává vált. A NetLock Kft. munkatársai a legszigorúbb követelményeknek is megfelelő szolgáltatói hátteret üzemeltetnek, és bevezették az ISO 9001:2002 minőségbiztosítási, majd az ISO 27001:2006 (korábban: a BS7799) információ-biztonsági irányítási rendszert. Mindezek mellett a NetLock Kft. az első, a közigazgatásban is elfogadott hitelesítés-szolgáltató Magyarországon.

Szakértő tanácsadóként segítséget nyújt a vállalatok hosszú távú versenyképességéhez, illetve hatékonyságuk növeléséhez nélkülözhetetlen ügyviteli folyamatok elektronizálásában, valamint rendelkezik nagyvállalati, intézményi hitelesítési infrastruktúrák kialakításához szükséges speciális jogi és informatikai know-how-val.
A NetLock Kft. 1999 óta világszerte valamennyi Microsoft termékben (Internet Explorer, Outlook, Outlook Express), valamint 2005 óta a Mozilla Suite, Firefox, Safari, Thunderbird böngészőkben és levelező szoftverekben, a PGP alkalmazáscsomagban mint megbízható legfelső szintű hitelesítés-szolgáltató szerepel. Nevéhez fűződik az első minősített aláírás létrehozására alkalmas eszköz regisztrációja, az első elektronikus számla kibocsátása, a MELASZ-Ready aláírási szabvány kidolgozása és első alkalmazásai. NetLock tanúsítványokat alkalmaznak a cégbírák, a vizsgaszervezők, ügyvédek, és számos közigazgatási intézmény dolgozói, továbbá a vállalat hozzájárult az első hiteles elektronikus ügyintézést lehetővé tevő önkormányzati rendszer, továbbá a digitális tachográf elindításához is.

**Sajtókapcsolat:**

Jekler Rudolf
ügyvezető igazgató
**Morpho Communications**
tel.: 488 0255
mobil: 20 9675 565
jekler.rudolf@morpho.hu
www.morpho.hu