NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1149 Budapest, Róna utca 52-80.

Fontos teendők kriptográfiai kulcsok gyengülésével kapcsolatban

A Kormányzati Hitelesítésszolgáltató (GovCA) szakmai tájékoztatása

2026. április 17.

A technológiai fejlődés és a kriptográfiai algoritmusok elavulása miatt a korábban általánosan biztonságosnak tekintett és dominánsan alkalmazott 2048 bites RSA (RSA 2K) kulcsok a közeljövőben elveszítik megbízhatóságukat.

Az elektronikus iratok hosszú távú érvényességének és joghatásának (pl. a polgári perrendtartás szerinti teljes bizonyító erejének) megőrzése érdekében a közigazgatási és piaci szereplőknek haladéktalanul meg kell kezdeniük az átállást az elliptikus görbén alapuló (ECC) kriptográfiára.

Ugyanilyen fontos a már meglévő, archív állományok időben történő felülidőbélyegzése is.

Az alábbiakban összefoglaljuk a legfontosabb jogi és szabványügyi fejleményeket, a technikai teendőket, valamint a Kormányzati Hitelesítésszolgáltató (GovCA) által e célra biztosított megoldásokat.

RSA 2K kulcsok gyengülése

Mint ismeretes, **a 2048 bites RSA kriptográfiai** (a továbbiakban: RSA 2K) kulcsok **megbízhatóságuk végéhez közelítenek**, így az **elmúlt évek globális trendje** lett az erősebb algoritmusokra, általában az **ECC kulcsokra való átállás**. Jelenleg a végső kivezetés dátuma bizonytalan, de kétségtelenül egyre közelít. Egyes ajánlások (pl. az uniós ENISA ACM vagy a német BSI TR-02102-1) már jelenleg is megkérdőjelezik az RSA 2K megbízhatóságát, míg mások (ld. ETSI TS 119 312) 2028-ra datálják a kötelező kivezetést, megint mások (pl. az amerikai NIST SP 800-131A Rev. 3) pedig 2030-ra.

Leszűkítve a kört az Európai Unióra, az látszik, hogy **az európai szakmai irányvonal az RSA 2K mielőbbi teljeskörű kivezetését tűzte ki célul**. Ezt jól mutatja, hogy az Európai Bizottság, az eIDAS2.0 végrehajtási rendeleteiben, már az e tekintetben szigorúbb ENISA ACM-et hivatkozza. A bizalmi szolgáltatók ugyan továbbra is alkalmazhatják az e tekintetben engedékenyebb ETSI TS 119 312-t, ugyanakkor ennek 2026 májusára tervezett újabb verziója várhatóan alkalmazkodni fog a Bizottság szigorítási szándékához.

Az Európai Unióban ugyanis – elsősorban az eIDAS2.0 és az Európai Kiberbiztonsági Rendelet révén – **egységesítési törekvések figyelhetők meg a kiberbiztonsági tanúsítási rendszerek terén.** Ennek köszönhetően a SOG-IS-től az ENISA-hoz került az elfogadott kriptográfiai mechanizmusokat tartalmazó dokumentum (Agreed Cryptographic Mechanisms – ACM) kiadása. Ennek pedig várható következménye, hogy **az ETSI szabványok és specifikációk** – melyek eddig szinte kizárólag a SOG-IS ACM-et hivatkozták – a következő verzióikban ezen hivatkozásokat **ENISA ACM hivatkozásokra fogják módosítani**. Tekintettel pedig arra, hogy az ENISA ACM a szigorúbb, kvázi

„azonnali" kivezetést preferálja, így **várhatóan az ETSI TS 119 312 következő, 2026 májusára tervezett újabb verziója is már 2028-nál korábbi dátumot fog tartalmazni** az RSA 2K kivezetésére. Mivel a kivezetések dátuma ebben a specifikációban általában az adott év utolsó napjára esik, így a **legkorábbi várható dátum** az új verzióban **2026. december 31.** lehet.

Mi következik ebből?

Amikor egy adott **algoritmus** – jelen esetben az RSA 2K – **általánosan megbízhatatlanná válik**, az ilyen algoritmussal korábban hitelesített (aláírt vagy bélyegzett, időbélyegzett) **dokumentumok sértetlensége és hitelessége veszélybe kerül**, így bizonyító erejük megdönthetővé válik, végső soron pedig **elveszíthetik a joghatásukat**.

Hogyan előzhetjük ezt meg?

A dokumentumok hitelessége úgy őrizhető meg, hogy a hitelesítésükhöz használt **algoritmus** – jelen esetben az RSA 2K – **gyengülése** (általános megbízhatatlanná válása) **előtt** a dokumentum aláírása **archív formátumra kerül kiterjesztésre (LTA)**, mely esetben az időbélyeg már egy **erősebb, hosszabb távon megbízhatónak tekintett algoritmussal** – jelen esetben ECC-vel – készül.

Amennyiben a dokumentum aláírása LTA szintű, azaz már tartalmaz archív időbélyeget, de az RSA 2K kulcsokkal készült, az **időbélyegzés megismétlése szükséges ECC időbélyeggel**.

Az új időbélyeg hozzáadása a teljes korábbi PDF tartalmat (beleértve az eredeti aláírást és a régi RSA 2K időbélyeget is) „lefedi", ezzel pedig **megőrizi a dokumentum hitelességét**.

Mit javaslunk?

Átállás ECC időbélyegre

Javasoljuk, hogy **haladéktalanul kezdjék meg az ECC alapú időbélyeg-szolgáltatásunk** általános és kizárólagos **alkalmazását**!

A szolgáltatás elérésével, paramétereivel és a technikai beállításokkal kapcsolatban **az** ECC alapú időbélyegző szolgáltatás elindításáról **c. cikkünkből tájékozódhat**.

Kriptográfiai leltár készítése

A puszta technológiaváltás, tehát **az átállás** ECC alapú időbélyeg-szolgáltatásra előremutató, de **nem elegendő**. Azokat a korábban hitelesített **dokumentumokat, amelyek** joghatását és érvényességét hosszú távon fenn kell tartani, de **az aláírásuk még nem archív szintű (LTA) és/vagy nem tartalmaznak ECC időbélyeget**, még az RSA 2K algoritmusok és kulcsok elavulása előtt **felül kell időbélyegezni az új, biztonságos ECC időbélyegzővel**.

Ennek érdekében úgynevezett ***kriptográfiai leltár*** **készítését**, azaz leegyszerűsítve a következőket **javasoljuk**:

1. Azon **dokumentumok vagy dokumentumtípusok meghatározása, melyek hitelességét és érvényességét hosszú távon fenn kell tartani**, mert megőrzési kötelezettség áll fenn velük kapcsolatban. Jelen esetben – a fentiekre való tekintettel – javasoljuk, hogy **amely dokumentum hiteles megőrzése 2026. után jár le, azt tekintsék ebbe a körbe tartozónak**.
2. A fenti körbe eső **dokumentumok kriptográfiai vizsgálata**, vagyis legalább a következők meghatározása:
   - aláírásformátum,
   - aláírási szint,
   - alkalmazott algoritmusok.

Aláíráskiterjesztés ECC alapú időbélyegzéssel

A fentiek szerint elkészített kriptográfiai leltár alapján **javasoljuk megtervezni és 2026 végéig végrehajtani az aláíráskiterjesztéseket** az alábbiak szerint:

- LTA szintű aláírások ECC alapú időbélyeggel: nincs teendő;
- LTA szintű aláírások RSA alapú időbélyeggel: időbélyegzés megismétlése ECC alapú időbélyeggel;
- LT vagy alacsonyabb szintű aláírások: kiterjesztés LTA szintre ECC alapú időbélyeggel.

Amennyiben a fentiekben javasolt kriptográfiai leltár olyan aláírást, bélyegzőt vagy időbélyegzőt is tartalmaz, mely esetében az aláíráskiterjesztés technológiailag nem lehetséges (pl. nem megfelelő aláírásformátum vagy a visszavonási információk már nem állnak rendelkezésre), szakmai egyeztetés céljából, kérjük, forduljanak a GovCA-hoz a konzultacio@hiteles.gov.hu e-mail címen.

LTA szintű aláírásformátumok alkalmazása az új dokumentumok hitelesítéséhez

Javasoljuk a szervezeteknek, hogy a dokumentumkezelési folyamataikban **tegyék kötelezővé az LTA szintű aláírásformátumok alkalmazását**, azaz minden dokumentum létrehozásakor, iktatásakor vagy archiválásakor, vagyis a végleges eltárolásuk előtt, **helyezzenek el egy, az elérhető legerősebb algoritmussal készülő archív időbélyeget is a dokumentumon**.

Hogyan segíthet ebben a GovCA?

ECC alapú időbélyeg-szolgáltatás

A NISZ Zrt. a Kormányzati hitelesítésszolgáltatása keretében az elmúlt években folyamatosan vezette be az ECC alapú szolgáltatásait. 2025 decemberétől megnyílt a lehetőség az ECC alapú időbélyeg-szolgáltatás tesztelésére, **2026 februárjától** pedig elérhető az ECC alapú időbélyeg-szolgáltatás is, így Ügyfeleinknél az ECC alapú időbélyegzéssel történő archiválás megvalósíthatóvá vált.

KEAASZ vastagkliens

A KEAASZ kliensalkalmazás legújabb (v2.0.36.3) verziója már képes az ECC időbélyeg-szolgáltatás használatára, így – amennyiben az alkalmazás beállításaiban az időbélyegprofilhoz az ECC alapú időbélyeg-szolgáltatás URL-je, vagy a „GovCA autentikációs tanúsítvánnyal" opció kerül beállításra – ezen szoftver alkalmas az ECC alapú archív időbélyegzés elvégzésére vagy az ECC alapú archív időbélyeggel történő aláíráskiterjesztésre.

Ahhoz, hogy a KEAASZ vastagkliensben **megfelelő aláírásformátum és -szint** készüljön, az alkalmazás beállításaiban az **Időbélyeges aláírásprofilnál a *Hosszútávú archív aláírás*** konténerrel (XAdES-LTA, PAdES-LTA vagy ASiC-LTA) szükséges a profilt vagy profilokat elmenteni és az aláíráskészítésnél e profilokat alkalmazni.

Amennyiben egy dokumentum aláírásformátuma megfelelő, de a szintje nem LTA, vagy az LTA szintű aláírás RSA 2K archív időbélyeget tartalmaz, a szoftver **Érvényességi idő kiterjesztése funkciójával végezhető el a hosszútávú érvényesíthetőséghez szükséges művelet**. Ebben az esetben is ügyelni kell rá, hogy ECC alapú időbélyeg-szolgáltatás legyen beállítva az aláíráskiterjesztés konténertípusa pedig Hosszútávú aláírás (LTA) legyen.

Adobe Acrobat Reader

Az **Adobe Acrobat Reader népszerű megoldás** a PDF dokumentumok olvasására, aláírására és aláírásának ellenőrzésére, ugyanakkor a szoftver **telepítéskori alapbeállításaival nem az európai jogszabályoknak és szabványoknak megfelelően** végzi a hitelesítési műveleteket.

Ahhoz, hogy Acrobat Readerben megfelelő aláírásformátum és -szint készüljön, megfelelő algoritmust használó időbélyeggel, **a** PDF dokumentum aláírása és időbélyegzése: Adobe Reader XI és Adobe Acrobat Reader DC **útmutató beállításait szükséges követni, az időbélyegző kiszolgálónál pedig** a GovCA ECC alapú időbélyeg-szolgáltatását **szükséges beállítani**.

A **dokumentum hitelessége megőrizhető, ha a beállított alkalmazással új időbélyeget kérünk rá**. Ez akkor szükséges, ha a PDF aláírása még nem LTA szintű, vagy az LTA aláírásban elavuló RSA 2K időbélyeg szerepel.

Megőrzési kötelezettség

Fontos kiemelni, hogy **az elektronikus iratok hitelességének fenntartását a jogalkotó** – összhangban a vonatkozó jogszabályokban foglaltakkal, különösképpen a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény vonatkozó normáival (pl. 4. §) – **a közigazgatási intézményekre, intézetekre és szervekre bízza**.

Jelenleg a hazai decentralizált archiválási modellben **nincs olyan automatikus, központi megoldás, amely ezt a feladatot átvenné, tehát a közigazgatás szereplőinek maguknak kell gondoskodniuk adatvagyonuk védelméről!** (A NISZ Zrt. nem nyújt megőrzési vagy archiválási szolgáltatást!)

Amennyiben a fentiekben további szakmai konzultációra van szüksége, javasoljuk, hogy minél hamarabb vegye fel velünk a kapcsolatot a konzultacio@hiteles.gov.hu e-mail címen!

A fentieket a NISZ Zrt. tájékoztatásul közli, nem minősül hivatalos jogi szakvéleménynek és jogi kötőerővel nem bír!