Az elektronikus ügyintézés alapjai a Nemzeti Hírközlési Hatóságnál

NYULI ATTILA

Nemzeti Hírközlési Hatóság
nyuli.attila@nhh.hu

Kulcsszavak: digitális aláírás, hitelesítés, XAdES, frekvenciagazdálkodás, NHH

A cikk az elektronikus ügyintézés bevezetésével foglalkozik a Nemzeti Hírközlési Hatóság frekvenciagazdálkodási eljárásában. Ismerteti a digitális aláírás alkalmazásával kapcsolatos kérdéseket, a megvalósított rendszer működésének folyamatát és a működtetésével kapcsolatos tapasztalatokat.

1. Bevezetés

A Nemzeti Hírközlési Hatóság (NHH) hatáskörébe tartozó frekvenciagazdálkodás, azon belül a rádiófrekvenciák ügyfelek számára történő kijelölése illetve használatuk engedélyezése során számos technikai adatra van szükség, melyek nagy része az ügyfeleknél keletkezik. A manuális adatrögzítés kiváltása érdekében már a kilencvenes évek elején is elektronikus adatcsere folyt a nagyobb ügyfelek és az NHH jogelődje között. Az adatok először floppy lemezeken cseréltek gazdát, majd a hírközlési hálózatok növekedtével nagyobb kapacitású adathordozók váltak szükségessé.

A bevezetett megoldás ugyan elkerülhetővé tette a manuális adatrögzítést, azonban a hivatali ügyintézés (jog)alapját továbbra is a papíralapon benyújtott kérelmek képviselték, mivel az adathordozón található információk hitelessége nem volt biztosított. A probléma természetesen a hatósági munka más területein is érzékelhető volt, így az informatikai rendszerek fejlesztésével foglalkozó munkatársak fokozott érdeklődéssel várták az elektronikus aláírással foglalkozó törvény megjelenését.

2. Az első nekifutás: XMLDSIG szabvány [1] szerinti elektronikus aláírás

A *2001. évi XXXV. törvény* megjelenése az elektronikus aláírásról jelentősen inspirálta adathitelesítéssel kapcsolatos informatikai fejlesztési szándékainkat, azonban a hitelesítésszolgáltatók magyarországi megjelenéséig még évekre volt szükség.

2003. elején úgy tűnt, hogy elindulhat a régóta várt fejlesztés. A törvényi szabályozás alapjai megvannak, és az NHH nyilvántartásai szerint Magyarországon két hitelesítésszolgáltató is tud minősített elektronikus aláíró tanúsítványokat kibocsátani a nyilvántartásban szintén feltüntetett biztonságos aláírást létrehozó eszközökre (BALE). Így az ábrándozás korszakát lezárva az új technológia beépíthető a megújítás előtt álló ügyiratkezelő rendszerbe, mely ezáltal többek között képessé válik elektronikus aláírással történő kiadmányozásra, illetve a hitelesített dokumentumok iktatására is.

A közbeszerzési eljáráson keresztül kiválasztott szállító 2004. februárjában nagy meglepetést okozott: jelezte, hogy a rendszerfejlesztés határidejét jelentős mértékben veszélyezteti, hogy nem lehetséges minősített elektronikus aláíró tanúsítványokra szert tenni. Némi hitetlenkedés után az NHH egy találkozót szervezett a fejlesztő, a hitelesítésszolgáltatók és az intelligens kártya szállítóinak bevonásával.

Kiderült, hogy a hír bármennyire meghökkentő, de igaz. Magyarországon két kártya kapta meg a BALE minősítést, azonban a minősítéskor előírt feltételeket a kártyák 2004 februárjában még nem teljesítették. A hitelesítésszolgáltatók ezt követően nagy erőkkel dolgoztak a szükséges fejlesztéseken annak érdekében, hogy a fejlesztett aláíró alkalmazás számára szükséges interfészek létrejöjjenek, illetve a kártyákon futó mikrokódok a minősített működés szerinti paraméterezésűek legyenek.

Az e-aláírással hitelesített dokumentumok hatósági ügyintézés során történő kezelésére 2003-ban illetve 2004 elején még nem volt egységes szabályozás, az egyes folyamatlépésekhez tartozó intézkedések kidolgozása (például hogyan működjön egy elektronikus tértivevény) az ügyiratkezelő rendszer fejlesztésének keretein túlmutató erőfeszítéseket igényelt. Ennek volt köszönhető, hogy 2004 nyarára az elektronikus aláírási képesség megszerzésével kapcsolatos elvárások szerényebbé váltak, az ügykezelési folyamatba épülés helyett egy NHH-n belül használható elektronikus aláírást létrehozó program, illetve egy, az ügyfelek számára korlátozásmentesen átadható aláírásellenőrző alkalmazás kifejlesztése lett a cél.

Az egyszerű felhasználói felülettel rendelkező, Microsoft Windows platformon futtatható alkalmazások 2005-ben elkészültek *(1. ábra)*, miközben az NHH kiadmányozó munkakörben dolgozó munkatársai minősített elektronikus aláíró tanúsítványokat kaptak.

Éppen az alkalmazás használatára vonatkozó oktatást szerveztük, mikor számunkra teljesen váratlanul számos új jogszabály jelent meg, új alapokra helyezve az

elektronikus ügyintézést, és jó időre ellehetetlenítve az elektronikus aláírás közigazgatásbeli használatát. Az elkészült rendszert nem lehetett használatba venni.

3. Az új szabályozási környezet

A 2005 végén megjelent jogszabályok új, nagyon részletesen definiált alapokra helyezték az elektronikus ügyintézést. A legfontosabbak:

- *193/2005. (IX. 22.) Korm. rendelet* az elektronikus ügyintézés részletes szabályairól;
- *194/2005. (IX. 22.) Korm. rendelet* a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről;
- *195/2005. (IX. 22.) Korm. rendelet* az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról;
- IHM ajánlások a közigazgatásban alkalmazható
  - tanúsítványokról,
  - időbélyegzésről,
  - aláírási szabályzatokról,
  - elektronikus aláírási formátumokról,
  - viszontazonosításról.

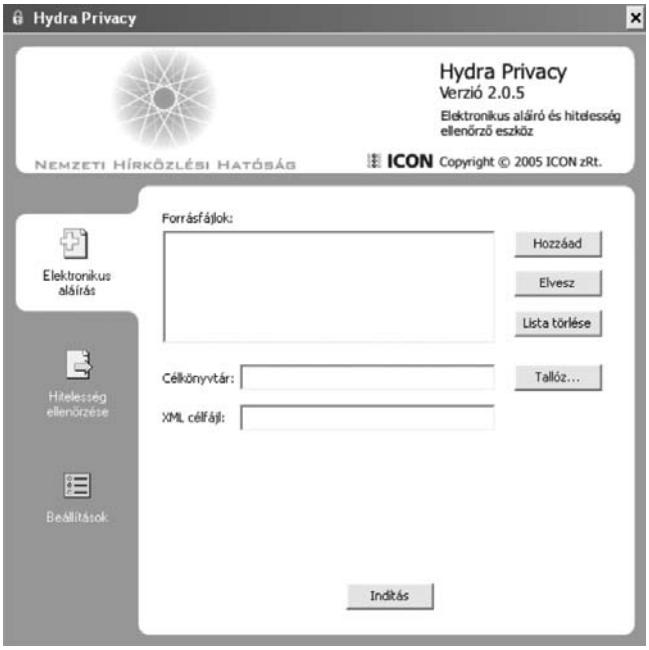
A jogszabályok által indukált főbb változások:

1. Az előírt aláírási formátum az XML Advanced Signature (XAdES) szabvány [2] módosított változata lett.
2. Ékezetes nevek is használhatóak a tanúsítványokban.
3. Csak a Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ) által felülhitelesített tanúsítvány kiadók tanúsítványai alkalmazhatóak közigazgatási eljárásokban.
4. A KGYHSZ felülhitelesítéshez a hitelesítés szolgáltatóknak viszontazonosítási szolgáltatást kell nyújtaniuk a közigazgatás intézményei felé.

4. (Újra)tervezési szempontok

2006. első félévét a vonatkozó jogszabályok tanulmányozásával, értelmezésével, illetve az új informatikai rendszer tervezésével töltöttük. Megfogalmaztuk a célrendszer legfontosabb tulajdonságait:

1. Tegye lehetővé az elektronikus ügyintézést.
2. Teljeskörű megfelelés a jogszabályi elvárásoknak.
3. Infrastruktúraszerűen működjön, az NHH hatósági szakrendszereit lehető legkisebb mértékben kelljen módosítani az elektronikus ügyintézés bevezethetőségéhez.
4. Moduláris felépítésű rendszer legyen.
5. Nyílt interfészeken keresztül nyújtsa szolgáltatásait a többi (más szállító által fejlesztett) informatikai rendszer számára.



1. ábra
Aláírást létrehozó és hitelességet ellenőrző alkalmazás

6. Tanúsított elektronikus aláírást létrehozó motort használjon, miáltal szükségtelenné válik a rendszer tanúsíttatása.

7. Terjedjen ki az Ügyfélkapun keresztüli felhasználóazonosításra is.

8. A megvalósított rendszer tegye lehetővé a teljes elektronikus ügymenetet amennyiben a kapcsolódó rendszerek erre alkalmassá váltak, azonban addig is rendelkezzen olyan (átmenetileg használt) interfészekkel, melyeken keresztül humán beavatkozással a folyamat felépíthető. Ezen interfészek használhatóak a rendszer átvételi teszteléséhez is.

9. Legyen egy hordozható számítógépeken is alkalmazható (tehát az NHH informatikai hálózatától függetlenül is működőképes) elektronikus aláírást létrehozó illetve hitelesítést ellenőrző komponense is. Ez a modul rendelkezzen függvény- és adatkapcsolati interfésszel annak érdekében, hogy más alkalmazások (tipikusan az ügyiratkezelő rendszer) a modul által nyújtott hitelesítési funkciókat igénybe tudják venni.

5. Aláírásformátumok

Mielőtt az elkészült rendszer működési koncepcióját ismertetnénk, célszerű kitérni a közigazgatásban használható elektronikus aláírásformátumok ismertetésére. Az IHM *elektronikus aláírás formátumok műszaki specifikációja* címet viselő ajánlása négy közigazgatási formátumot különböztet meg:

- A **„pillanatnyi”** közigazgatási formátum egy olyan pillanatnyi aláírás, mely sem visszavonási információkat, sem időbélyegzést nem tartalmaz. Olyan esetekben alkalmazható, amikor az aláírt dokumentum sértetlenségének ellenőrizhetősége önmagában is elegendő. Ez a formátum a szabványos XAdES-EPES formátumnak

felel meg. Élettartama rövidebb az aláírást követő első visszavonási állapot információ kiadásánál.

• A **„rövid távú”** közigazgatási formátum egy olyan rövid távú aláírás, melyhez időbélyeg kapcsolódik, de nem tartalmaz visszavonási információkat. Olyan esetekben alkalmazható, amikor az aláírt dokumentum sértetlenségének ellenőrizhetőségén túl szükség van a dokumentum adott időpont előtti létezésének az igazolására is (de alkalmazható pillanatnyi aláírásként is). Ez a formátum megfeleltethető a szabványos XAdES-T formátumnak. Az aláírás ellenőrzése nem szükséges az aláíró tanúsítványának lejárta után.

• A **„hosszú távú”** közigazgatási formátum egy speciális hosszú távú aláírás (mely értelemszerűen alkalmazható pillanatnyi és rövid távú aláírásként is). Ez a formátum megfeleltethető a szabványos XAdES-C formátumnak. Jellemzője, hogy az elektronikus aláírás ellenőrizhetősége szükséges a tanúsítványlánc bármely elemének a lejárta után is.

• Az **„archív”** közigazgatási formátum egy speciális archív aláírás, egyúttal megfelel a szabványos XAdES-A formátumnak. Jellemzője, hogy ellenőrzése szükséges az aláírás során használt algoritmusok kriptográfiai elavulása után is.

A „hosszú távú” és „archív” közigazgatási formátum visszavonási információkat és időbélyeget egyaránt tartalmaz, így olyan esetekben is alkalmazható, amikor az első két aláírási formátummal ellentétben az aláírások utólagos letagadhatatlanságára (az aláíró kilétének harmadik fél előtti bizonyíthatóságára) is szükség van.

Az NHH elektronikus ügykezelést lehetővé tévő rendszerének működése során rövid távú és archív elektronikus aláírások keletkeznek.

6. Működési logika

A rendszer elektronikus aláírásra vonatkozó működési folyamatait a *2. ábra* szemlélteti.

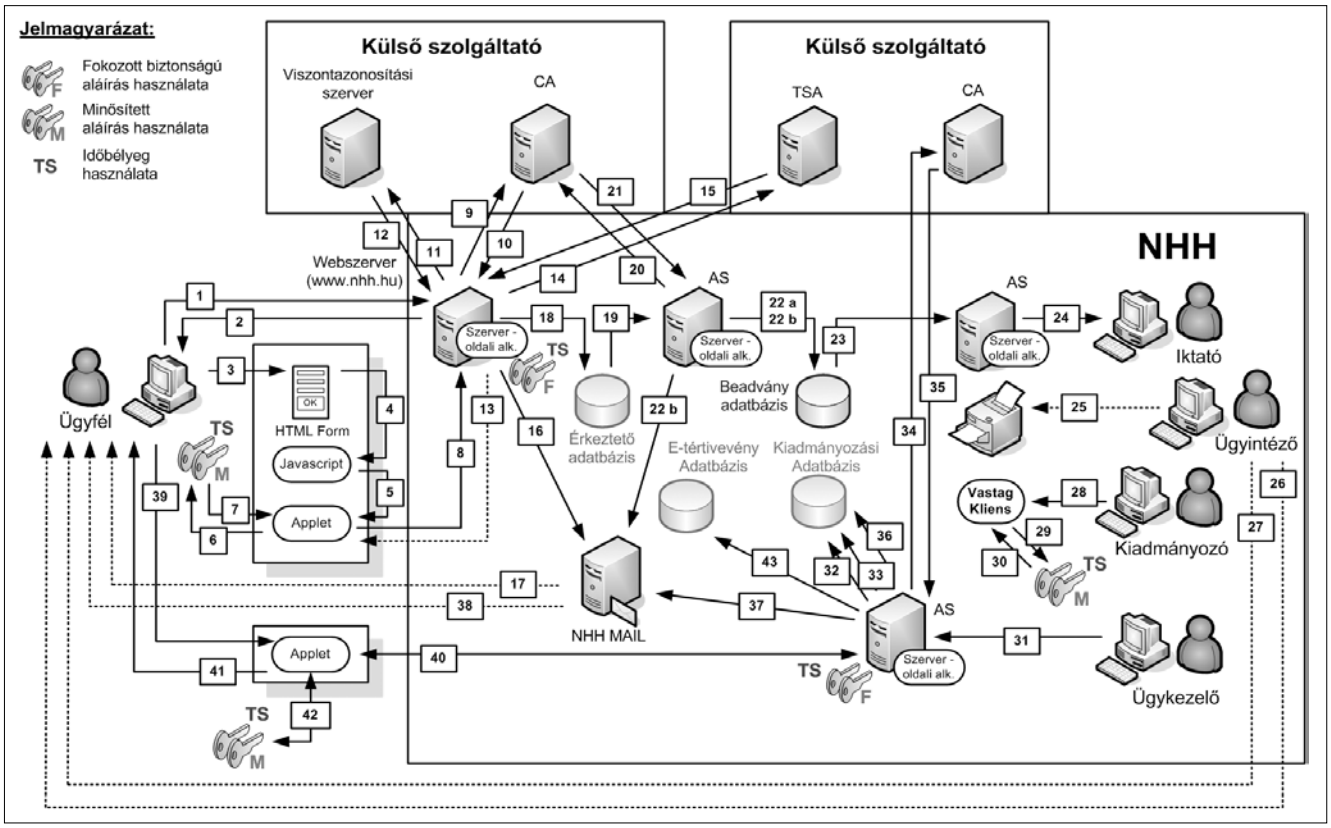
A működési folyamat a következő lépésekből épül fel:

1. Az elektronikus hatósági ügyintézést kezdeményező ügyfél az elérni kívánt szolgáltatást biztosító weblaphoz kapcsolódik. A személyes adatok és a bizalmasság megőrzése érdekében az NHH és az ügyfél közötti kapcsolat SSL protokoll felhasználásával titkosított.

2. A weblap tartalma – amely bármilyen tetszőleges kialakítású (UTF-8 kódolású) űrlap lehet –, letöltődik az ügyfél böngészőjébe. Az űrlapok a benyújtandó tényleges adatokon kívül tartalmazzák a viszontazonosításhoz és a rendeletekben megfogalmazott nyilatkozási lehetőségekhez szükséges mezőket is.

3. Az ügyfél az űrlap kitöltését és az űrlapon jelzett, elektronikus formában rendelkezésre álló és mellékelendő fájlok becsatolását követően, az űrlap tartalmának jóváhagyásaként, a weblapon található *Továbbítás elektronikus aláírással* gomb vagy a *Továbbítás ügyfélkapu azonosítóval* gomb segítségével kezdeményezi az űrlap és a kapcsolódó adatok feldolgozását. A becsatolásra kerülő fájlok tartalmát a feldolgozó alkalmazás nem vizsgálja/értelmezi (ezek akár aláírt XML állományok is lehetnek). A rendszer számára az első aláírást a bead-

2. ábra A rendszer elektronikus aláírásra vonatkozó működési folyamatai



ványt benyújtó ügyfél aláírása jelenti. Az ilymódon keletkezett állományt fogja a fogadó rendszer hitelesíteni. Amennyiben egy ügyfél egy másik személy által aláírt XML állományt kíván hiteles módon becsatolni, úgy azt kötelezően XAdES-A formátumban kell megtennie. A csatolható fájlok méretét a hosszú feldolgozási idők elkerülése érdekében a rendszer korlátozza. Az egy-egy űrlapra becsatolt állományok összmérete nem haladhatja meg a 100 MB-ot. A csatolt fájlok típusára, formátumára nincs külön megkötés, azonban a rendszer paraméterezésén keresztül űrlaponként szabályozhatóak az elfogadott MIME típusok.

4. A feldolgozás első lépéseként egy kliens-oldali Javascript program kigyűjti az űrlapot alkotó weblapból az egyes adatbeviteli mezőket és azok tartalmát. A Javascript program lehetőséget biztosít az űrlap adatbeviteli mezőinek tartalmi validálására is (tartományba esés, dátum, IP cím, e-mail cím stb.) Amennyiben vannak csatolmányok, azok alapján egy csatolmánylista készül, majd az adatokból egy XML alapú adattömböt képez.

5. A Javascript letölt egy elektronikus aláírással hitelesített Applet-et, amelynek átadja az űrlap adataiból képzett XML adattömböt.

6. Az alkalmazás az XML adatstruktúrát ismételten olvashatóvá alakítja és a csatolt fájlok listájával együtt (amennyiben ilyenek léteznek) megjeleníti az ügyfél számára az aláírás előtt. A letöltésre került Applet létrehozza a közigazgatásban elvárt XAdES alapú XML aláírási formátumot és kezdeményezi a bevitelre került adatok és a csatolt állományok ügyfél általi aláírását.

7. Az ügyfél az aláíró eszközének és az aláírásra használt kulcspárjának (tanúsítványának) kiválasztását követően fokozott biztonságú, vagy minősített elektronikus aláírással látja el a bevitelre került adatokat. (Mind a viszontazonosításra használt, mind az ügyintézési tevékenységhez szükséges adatmezők és csatolt állományok aláírásra kerülnek.)

8. Az Applet az ügyfél elektronikus aláírásával ellátott, XAdES-EPES formátumú adatokat továbbítja az NHH Webszervere felé.

9. Az NHH Webszerverén futó szerver oldali komponens az Applet által beküldött XAdES állomány részeként csatolt ügyfél tanúsítványt megvizsgálja. Amennyiben a tanúsítvány már/még érvényes, úgy a tanúsítványt kibocsátó szolgáltató (CA) rendszeréből megpróbálja letölteni a vonatkozó tanúsítvány visszavonási listát (CRL), illetve adott esetben megpróbálja lekérdezni a tanúsítvány érvényességét a szolgáltató által biztosított OCSP szolgáltatás igénybevételével.

10. A vonatkozó tanúsítvány visszavonási lista (CRL) sikeres letöltését, illetve az OCSP válasz visszaérkezését követően a szerver oldali komponens megvizsgálja, hogy az ügyfél tanúsítvány szerepel-e a CRL listán (visszavonásra került-e).

11. Amennyiben a csatolt tanúsítvány érvényes és nem került visszavonásra, úgy az ügyfél által kitöltött adatok alapján a rendszer megkísérli az ügyfél viszontazonosítását a tanúsítványt kibocsátó szolgáltató viszontazonosítási szolgáltatásának igénybevételével.

12. A viszontazonosítási válasz visszaérkezését követően a rendszer értékeli az ügyfél személyazonossága és a tanúsítvány megfelelőségét.

13. Amennyiben az ügyfél tanúsítványa még/már nem érvényes, visszavonásra került, vagy a viszontazonosítási kérelemre érkezett válasz nemleges, úgy a rendszer visszajelez az ügyfélnek, hogy ügyintézési kérelme nem került elfogadásra és mellékeli a visszautasítás okának leírását.

14. Amennyiben az ügyfél tanúsítványa érvényes, és a viszontazonosítás eredménye pozitív, valamint az ügyfél által beküldött, aláírt adatállomány hitelessége megfelelő, úgy a rendszer generál egy 26 számjegyű érkeztető számot az 193/2005. (IX. 22.) Korm. rendelet mellékletében leírtaknak megfelelően. A beküldésre került adatok érkeztetési idejének rögzítésére a rendszer időbélyeget kér az NHH-val szerződött külső szolgáltatótól (TSA).

15. Az időbélyeg sikeres fogadását követően a rendszer a fogadó szerver kulcsával aláírja a beérkezett, érkeztető számmal és időbélyeggel ellátott adatokat.

16. Az ügyfél ügyintézési kérelemének sikeres fogadásáról e-mailben kap visszajelzést a beadvány űrlapján megadott kapcsolattartási e-mail címre. A visszajelzés az ügyfél által benyújtott kérelmet, valamint a beadvány benyújtásakor csatolt dokumentumok listáját, a fogadó rendszer által generált érkeztető számot és a fogadás időpontját rögzítő időbélyeget tartalmazza a feldolgozó szerver által aláírt XML formátumban (csatolmányként) és olvasható formában a levél törzseként. Így az e-mail külön alkalmazás nélkül is olvasható.

17. Az előkészített e-mailt az NHH levelező szervere továbbítja az ügyfélnek.

18. A beérkezett, érkeztető számmal és időbélyeggel ellátott adatok az érkeztető adatbázisban kerülnek tárolásra, a későbbi feldolgozásra várva. (Az archív aláírási formátum előállításához szükséges a kivárási idő biztosítása.)

19. Az alkalmazásszerveren futó szerver oldali komponens adott időközönként megvizsgálja az érkeztető adatbázisban lévő beadványokat, hogy a beadványokon szereplő időbélyegen található időponttól számított kivárási idő eltelt-e már.

20. Amennyiben az adott beadványra vonatkozó kivárási idő már eltelt, úgy a rendszer a tanúsítványt kibocsátó szolgáltató rendszeréből megpróbálja letölteni a vonatkozó tanúsítvány-visszavonási listát (CRL), illetve adott esetben megpróbálja lekérdezni a tanúsítvány érvényességét a szolgáltató által biztosított OCSP szolgáltatás igénybevételével.

21. A vonatkozó tanúsítvány-visszavonási lista (CRL) sikeres letöltését, illetve az OCSP válasz visszaérkezését követően a szerver oldali komponens megvizsgálja, hogy az ügyfél tanúsítványa szerepel-e a CRL listán (visszavonásra került-e).

22. a) Amennyiben a kivárási idő letelt és a beadványt aláíró ügyfél tanúsítványa továbbra is érvényes, úgy a rendszer összeállítja a beadvány archiválásához szükséges információkat és létrehoz egy XAdES-A for-

mátumú állományt, amely a beadvány adatbázisba kerül eltárolásra és az érkeztető adatbázisból törlésre kerül. Az NHH egy központi e-mail címére elküldésre kerül egy e-mail, amely az iktatók felé jelzi az elkészült beadvány rendelkezésre állását és tartalmazza a beadvány letöltési link-jét. (Ez utóbbi lépés csak a teszteléshez illetve az ügyiratkezelő rendszerhez történő integrációig volt használatban).

b.) Amennyiben a kivárási idő letelt és a kérelmet aláíró ügyfél tanúsítványa nem érvényes, úgy a rendszer az ügyfél által benyújtott és aláírt XAdES formátumú beadványt érvénytelen jelöléssel látja el és automatikusan értesítő e-mailt küld az ügyfélnek (az e-mail a beadvány űrlapján megadott kapcsolattartási e-mail címre és az NHH egy központi e-mail címére is elküldésre kerül), melyben tájékoztatja, hogy beadványa nem került feldolgozásra. Az értesítő levél olvasható formában a levél törzseként a beadvány érkeztető számát és a beadvány érvénytelen aláírás miatti elutasításának tényét tartalmazza. Az érvénytelen jelöléssel ellátott beadvány is a beadvány adatbázisban kerül eltárolásra és az érkeztető adatbázisból törlésre kerül.

23. Az (ügyiratkezelő rendszerrel megvalósított integrációig) az iktatók az alkalmazásszerveren futó webes felület és egy szerver oldali komponens segítségével kaphattak lehetőséget a beérkezett beadványok megtekintésére, illetve azoknak az NHH jelenlegi elektronikus ügyviteli rendszerébe áthelyezésére. Ezen a felületen az iktatók/ügyintézők azon beadványokat is látják külön jelöléssel ellátva, amelyek aláírása a kivárási időt követően érvénytelennek bizonyult (a tárolás és megjelenítés célja, hogy esetleges reklamációk esetén előkereshető és ellenőrizhető legyen a beadvány állapota).

24. Az ügyiratkezelő rendszerrel megvalósított integrációig az iktatók egy adott kérvénnyel kapcsolatos ügyintézési tevékenységük megkezdésekor a beadványhoz egy új iktatási számot rendeltek, és az XAdES-A formátumú aláírt beadványt munkaállomásukra letöltve csatolták az NHH elektronikus ügyiratkezelő rendszerébe.

25. Az ügyintéző az ügyiratkezelő rendszerből az XAdES formátumú aláírt beadványt a munkaállomására telepített vastag kliens alkalmazás segítségével meg tudja nyitni. Így a beérkezett és feldolgozásra került kérelmet illetve a hozzá csatolt dokumentumokat bármikor meg tudja tekinteni. (Erre a lépésre csak a szakrendszerrel és a SZÜR integrációjáig van szükség).

26. Az ügyfél az ügyintézési folyamat megkezdéséről, vagyis az ügyével kapcsolatos ügyiratszámról és az ügyét kezelő ügyintézőről, e-mailben tájékoztatást kap az ügyirattal kapcsolatos dokumentumokba való betekinthetőség biztosítása érdekében. A tájékoztató e-mailben az ügyiratszám és az ügyét kezelő ügyintéző neve csatolmányként, a kiadmányozó által aláírt XAdES formátumban és az e-mail törzseként, szöveges formában kerül elküldésre.

27. Amennyiben az ügyfél által benyújtott beadvány (akár elektronikus módon, akár papíron lett indítva) nem tartalmaz minden, az ügyintézéshez feltétlenül szükséges információt, úgy a kiadmányozó egy hiánypótlási eljárást kezdeményez az ügyfél felé. A hiánypótlási eljáráson belül az ügyfél e-mailben tájékoztatást kap a hiánypótlásra vonatkozóan, és kap egy speciálisan kialakított URL-t (a link a hiánypótlási eljáráshoz kapcsolódó ügy iktatási számát/azonosítóját tartalmazza hivatkozási információként), amelyre kattintva egy webes űrlaphoz kapcsolódik. Itt a szükséges információk/adatok/dokumentumok megadhatóak, illetve pótolhatóak. A linkben megadott hivatkozási adatok az űrlapon automatikusan kitöltésre kerülnek, ezáltal elkerülve az azonosítók téves megadásából származó problémákat. A kiadmányozó a tájékoztató szöveget és a linket az e-mail törzseként, szöveges formában, illetve a vastag kliens alkalmazás segítségével elektronikusan aláírva (minősített aláírással), az e-mailhez csatolva is elküldi. A hiánypótlásra való felszólítás átvételének igazolása az ügyfél felelőssége. A hiánypótlási űrlap kezelése és feldolgozása a 2.1. ponttól leírtak szerint történik.

28. Amennyiben a beérkezett kérvénnyel kapcsolatosan dokumentum keletkezik, úgy annak hitelesítését a kiadmányozó a vastag kliens alkalmazás segítségével teheti meg.

29. Az elektronikus aláírás létrehozásához a kiadmányozónak ki kell jelölnie az aláíráshoz használt eszközt, illetve az aláírásra használt eszközön található, aláírásra használt kulcspárt (tanúsítványt).

30. A kiadmányozó a kiválasztott tanúsítvánnyal a vastagkliens-alkalmazás segítségével aláírja, és egyúttal időbélyeggel is ellátja a kiadásra kerülő dokumentumot.

31. Az aláírt dokumentum (a SZÜR integrációig) egy webes felületen keresztül feltöltésre kerül az alkalmazásszerverre az ügykezelő által.

32. A dokumentum feltöltésre került a Kiadmányozási adatbázisba.

33. Az alkalmazásszerveren futó szerver oldali komponens adott időközönként megvizsgálja a Kiadmányozási adatbázisban lévő állományokat, hogy a dokumentumon szereplő időbélyegen található időponttól számított kivárási idő eltelt-e már.

34. Amennyiben az adott dokumentumra vonatkozóan a kivárási idő eltelt, úgy a rendszer a tanúsítványt kibocsátó szolgáltató rendszeréből megpróbálja letölteni a vonatkozó tanúsítvány visszavonási listát (CRL).

35. A vonatkozó tanúsítvány visszavonási lista (CRL) sikeres letöltését követően a szerver oldali komponens megvizsgálja, hogy a tanúsítvány szerepel-e a CRL listán (visszavonásra került-e).

36. Amennyiben a kivárási idő letelt és a dokumentumot aláíró kiadmányozói tanúsítvány továbbra is érvényes, úgy a rendszer létrehoz egy XAdES-A formátumú állományt, amelyet a Kiadmányozási adatbázis másik táblájában tárol el. Amennyiben a kivárási idő letelt és a dokumentumot aláíró kiadmányozói tanúsítvány nem érvényes, úgy erről a rendszer e-mailben tájékoztatja a kiadmányozót. Ezek az érvénytelen aláírással rendelkező dokumentumok is eltárolásra kerülnek a Kiadmányozási adatbázisban. A rendszer egyúttal visszaküldi a dokumentumot a kiadmányozó vezetőnek, meg-

jelölve, hogy lejárt tanúsítvány miatt ismételt – most már az új és érvényes tanúsítvánnyal történő – kiadmányozás, aláírás szükséges. Az eljárás ebben az esetben a 28. ponttól ismétlődik.

37. A rendszer automatikusan megvizsgálja a dokumentumhoz (az NHH meglévő ügyintéző rendszere által) csatolásra kerülő címzettek listáját és mindegyik címzett számára automatikusan generál egy egyedi azonosítót (az azonosító a dokumentumhoz kapcsolódó azonosítószámból és a dokumentum sha-256 lenyomatából tevődik össze) linkként kialakítva, amelyen keresztül az adott ügyfél a számára kiadott dokumentumot átveheti.

38. A létrehozott egyedi linkek e-mail formájában kiküldésre kerülnek az ügyfelek számára. Az e-mailben a link csatolmányként, a szerver által aláírt XAdES formátumban és az e-mail törzseként, szöveges formában kerül elküldésre.

39. Az ügyféloldalon a link-re kattintva egy Applet-et töltődik le, amely felkéri az ügyfelet, hogy egy 'dokumentum letöltési kérés' aláírásával azonosítsa magát és kezdeményezze a számára kiadott dokumentum letöltését.

40. Az Applet a link-ben megadott paraméterek és az aláírt 'dokumentum letöltési kérés' alapján az alkalmazásszerveren található szerver oldali komponens segítségével megállapítja, hogy a letöltést kérelmező ügyfél a dokumentum letöltésére jogosult-e. Amennyiben a kérelmező jogosult a dokumentum letöltésére, úgy a szerver oldali komponens a Kiadmányozási adatbázis megfelelő táblájából kiolvassa az ügyfél számára kiadott dokumentumot és átadja a kapcsolódó Applet-nek. Amennyiben a kérelmező nem jogosult a dokumentum letöltésére, úgy letöltési kérését a rendszer elutasítja, amely visszajelzésre kerül a kérelmező felé az Applet segítségével.

41. Amennyiben a kérelmező jogosult a dokumentum letöltésére, úgy a dokumentum letöltése az ügyfél munkaállomásán futó Applet segítségével történik, mely integritás ellenőrzést is végez a letöltés sikerességének ellenőrzésére.

42. A dokumentum letöltésének utolsó lépéseként a letöltött állomány sikeres ellenőrzését követően, az ügyfélnek egy időbélyeggel és elektronikus aláírásával ellen kell jegyeznie a dokumentum 'kézhezvételét' (az időbélyeg kérés és az aláírás az Applet és a szerver oldali komponens segítségével történik).

Amennyiben az állomány letöltése, illetve ellenőrzése során valamilyen probléma merül fel, úgy a letöltött állomány a helyi fájlrendszerből törlésre kerül és a rendszer tájékoztatja a felhasználót a hiba okáról.

43. A kézhezvételt igazoló *„e-tértivevényt"* a rendszer e-mailben továbbítja az előre meghatározott, NHH-n belüli e-mail címekre, illetve egy adatbázisban (e-tértivevény adatbázis) helyezi el.

Amennyiben az ügyfél a kormányzati ügyfélkapus azonosításon keresztül használja a rendszert, úgy az ügyfél oldali aláírási funkciókat az ügyfélkapus felhasználó azonosítás helyettesíti, miközben a szerver oldali aláírási/időbélyegzési funkciók változatlanul működnek.

7. Hitelesítéskezelő alkalmazás

A kialakított rendszer kicsi, de fontos eleme a folyamat diagramon vastag kliensnek nevezett hitelesítéskezelő alkalmazás. A program az NHH hálózatától függetlenül is működőképes, használatához csupán internetkapcsolatra van szükség.

Az egyszerű felhasználói felületen keresztül három fő funkció indítható *(3. ábra)*.

3. ábra
A hitelesítéskezelő alkalmazás felhasználói felülete (1)

– Az *Elektronikus aláírás* menüpont segítségével pillanatnyi, illetve az időbélyeg-kérést is bekapcsolva rövidtávú elektronikus aláírás hozható létre.
– A *Kiegészítés* menüpont szolgál a rövidtávú aláírással ellátott tartalmak archív közigazgatási formátumra történő kiegészítésére.

4. ábra
A hitelesítéskezelő alkalmazás felhasználói felülete (2)

– A *Hitelesség ellenőrzése* menüpontot kiválasztva lehetséges az aláírt tartalmak ellenőrzése, illetve az eredeti tartalom visszaállítása. A felhasználói felület gondos tervezéssel úgy lett kialakítva, hogy a lehető legegyértelműbb módon mutassa az aláírás érvényességét vagy érvénytelenségét *(4. ábra)*. Érvénytelen aláírás jelzésére a ✖, hiányos (nem kiegészített) aláírás jelzésére a ! ikonok szolgálnak. Természetesen ennél részletesebb információk is megjeleníthetőek az eredményre kattintva *(5. ábra)*.

5. ábra
A hitelesítéskezelő alkalmazás felhasználói felülete (3)

Az intuitív felhasználói felületen kívül egy XML paraméter fájlon keresztül is vezérelhető az alkalmazás. Ez a tulajdonsága teszi lehetővé, hogy más – elektronikus aláíró illetve ellenőrző képességgel nem rendelkező – alkalmazások is kezdeményezzenek hitelesítéskezelést.

8. Integrációs pontok

A hitelesítési infrastruktúra közvetlenül négy rendszerrel áll kapcsolatban:

• A rendszer működéséhez szükséges az *Ügyfélkapu-kapcsolat*.

• Az NHH felé adatszolgáltatási kötelezettséggel rendelkező hírközlési szolgáltatók előzetes regisztráció után, az *Adatkapu-rendszeren* keresztül teljesíthetik adatbeadásaikat. Az adatok beadása struktúrált formában, űrlapok kitöltésén keresztül történik, a hitelesítési infrastruktúra szolgáltatásainak igénybevételével.

• A Nemzeti Hírközlési Hatóság ügyfelei számára az *e-nhh* nevű alkalmazás webes űrlapjai teremtik meg az elektronikus ügyintézés alapjait. E rendszer a cikk írásakor még átvételi tesztelés alatt áll.

• A negyedik kapcsolódó rendszer az NHH *ügyiratkezelő rendszere*. Mivel minden egyes webes űrlap egy adott szervezeti egység tevékenységéhez köthető, az ügyiratkezelő rendszer a űrlapazonosító alapján gondoskodik az információ szervezeti egységre szignálásáról. A hiteles űrlaptartalmak feldolgozását a szervezeti egység informatikai szakrendszere végezheti.

9. Működtetési tapasztalatok

A rendszer látszólagos bonyolultsága mellett is jól üzemeltethető. Ez egyrészt moduláris felépítésének, másrészt a robusztus futtató környezetnek (UNIX) köszönhető.

A rendszer gyors működéséhez elengedhetetlen, hogy az aláíró tanúsítványok érvényessége online tanúsítvány állapot szolgáltatás (OCSP) segítségével lekérdezhető legyen. Az aláíró tanúsítvány érvényességének tanúsítvány visszavonási lista (CRL) alapján megvalósított ellenőrzése esetén egy kérelem beadása és annak ügyiratkezelő rendszerbe történő megérkezése között akár 24 óra is eltelhet!

Az NHH hitelesítési infrastruktúrájával kapcsolatba kerülő felhasználók döntő többsége jelenleg még nem rendelkezik elektronikus aláíró tanúsítvánnyal, az adatbeadás többnyire az Ügyfélkapun keresztüli felhasználóazonosítás nyomán történik. Reményeink szerint a vállalati körökben biztató ütemben terjedő elektronikus aláírási technológia (2007-ben a hazai hitelesítés szolgáltatók által kibocsátott minősített tanúsítványok száma megnégyszereződött, a fokozott biztonságú tanúsítványok száma 24%-os növekedést mutatott [3]) néhány éven belül meg fogja találni az állampolgárokhoz vezető utat is, megteremtve a biztonságos és kényelmes otthoni ügyintézés lehetőségét.

A szerzőről

NYULI ATTILA 1965-ben született Székesfehérváron. A Budapesti Műszaki Egyetem Villamosmérnöki Karának Híradástechnika Szakán kitüntetéssel diplomázott 1990-ben. 1992-ben kitüntetéses szakmérnöki diplomát, 1993-ban pedig informatikai egyetemi doktori címet szerzett a BME-n. 1992-ben a Frekvenciagazdálkodási Intézetben kezdett dolgozni, ahol fő érdeklődési körét az elektromágneses hullámterjedés számítási modellek pontosságának vizsgálata és a földrajzi információs rendszerek alkalmazásának kérdései jelentették. Érdeklődési és feladatköre később az informatikai biztonságtechnikai területtel is kibővült. Jelenleg a Nemzeti Hírközlési Hatóság alkalmazásfejlesztési tevékenységeit irányítja.

Irodalom

[1] RFC 3275 XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core/
[2] XML Advanced Electronic Signatures (XAdES) http://www.w3.org/TR/XAdES/
[3] Az elektronikus aláíráshoz és alkalmazásaihoz kapcsolódó monitoring felmérések, http://www.nhh.hu/dokumentum.php?cid=16013