Nemzeti Média- és Hírközlési Hatóság

KRA Elektronikus aláírási szabályzat

7.01 VÁLTOZAT

2022. május 31.

TARTALOMJEGYZÉK

1 BEVEZETÉS

Ez a dokumentum a számhordozási Központi Referencia Adatbázisban használt elektronikus hitelesítésekkel kapcsolatos gyakorlati tudnivalókat tartalmazza, amely kiegészíti a KRA felhasználói kézikönyvben és a KRA SOAP interfész specifikációban ismertetett funkciókat és eljárásokat.

Az ebben a dokumentumban leírtakat a KRA minden felhasználójának be kell tartania, mert ezek nélkül a KRA elérése, az üzenetek felhasználói elektronikus aláírása, vagy a KRA által aláírt állományok aláírásának ellenőrzése nem lehetséges.

A számhordozási Központi Referencia Adatbázis (KRA) a számhordozhatóság nemzeti szintű hálózati megvalósításának eleme. Alapfeladata a hordozott számokkal kapcsolatos irányítási információk összegyűjtése a szolgáltatóktól, és a hordozott számokra irányuló hívások megfelelő irányításához szükséges adatokhoz való hozzáférés biztosítása a szolgáltatók számára.

A számhordozással és a KRA-val kapcsolatos részletes szabályokat jogszabályok tartalmazzák. Emellett a hatóság kidolgozza, a szolgáltatókkal egyezteti és a honlapján közzéteszi a KRA működésére vonatkozó műszaki leírásokat, melyek az NMHH honlap Számhordozás (KRA) oldaláról letölthetők.

A **KRA Elektronikus aláírási szabályzat** a műszaki leírás része, a KRA rendszer használatához a rendszer védelme és az adatbázis hitelességének megőrzése érdekében alkalmazott elektronikus hitelesítéseket tárgyalja.

A 2. fejezet az általános rendelkezéseket tartalmazza a szabályzat céljáról, hatályáról, szereplőiről, valamint felsorolja a kapcsolódó alapvető normatívákat.

A 3. fejezet az elektronikus aláírásra vonatkozó szabályozást, valamint a KRA-ban alkalmazott tanúsítvány típusokat ismerteti.

A 4. fejezet az aláíró tanúsítványok KRA-ban való használatának további feltételeit ismerteti. Összefoglalja, hogy miként történik a KRA-ban a felhasználóktól beérkező üzenetek elektronikus aláírásának ellenőrzése, és miként készíti el a KRA a kiküldendő üzenetek aláírását és hogyan ellenőrizhető az aláírás hitelessége.

Az M1 melléklet a KRA által támogatott biztonságos aláírás létrehozó eszközök (BALE) felsorolása.

2 ÁLTALÁNOS RENDELKEZÉSEK

2.1 A szabályozás célja

Az elektronikus aláírási szabályzat célja olyan értelmezési, kezelési és jogi ismereteket nyújtani az elektronikus aláíráshoz kötött számhordozási eljárásokban, amely biztosítja az együttműködés helyességét az aláíró és az aláírás-ellenőrző felek között, beleértve a harmadik felekkel (3rd party szolgáltatókkal) kapcsolatos szabályokat is.

2.2 A szabályozás hatálya

Jelen dokumentum a Nemzeti Média- és Hírközlési Hatóság (továbbiakban: NMHH) által üzemeltetett számhordozási Központi Referencia Adatbázis rendszer elektronikus aláírásainak használatát szabályozza.

2.2.1 Személyi hatálya

A szabályzat hatálya kiterjed minden *szolgáltatói, operátori* és jogszabály alapján *jogosult* KRA felhasználóra, továbbiakban felhasználóra.

2.2.2 Tárgyi hatálya

A szabályzat tárgyi hatálya kiterjed:

- elektronikus aláírással ellátott minden hordozás tranzakciók bejelentésére, fogadására és feldolgozására;
- minden elektronikus aláírással ellátott válasz, vagy nyugta elkészítésére, küldésére és feldolgozására;
- KRA által előállított elektronikus aláírással ellátott irányítási listákat tartalmazó állományokra.

2.2.3 Időbeli hatálya

A szabályozás 2022. április 1-jén lép hatályba és a visszavonásig érvényes.

2.3 Kötelező felülvizsgálat időpontja

A szabályzatban leírt követelmények alapját a hatályos jogszabályi környezet és a KRA rendszer szolgáltatói egyeztetések nyomán kialakult műszaki specifikációja képezi.

A jogszabályi környezet, az alkalmazható technológia fejlődése illetve a KRA műszaki specifikáció elektronikus aláírással kapcsolatos változása ezen dokumentum értelemszerű változtatását vonja maga után. A dokumentum felülvizsgálatát évente el kell végezni. Újabb változat kiadásakor a régi automatikusan érvényét veszti. Újabb változat érvénybe lépése esetén az új változatot elektronikus formában NMHH a szolgáltatók kapcsolattartóinak az érvénybe lépés időpontja előtt 30 nappal eljuttatja.

2.4 Szerepkörök

Az elektronikus aláírás használatához az alábbi szerepköröket kell megkülönböztetni:

- az aláírás létrehozója,
- az aláírás elfogadója,
- hitelesítés szolgáltató,
- kriptográfiai eszközkibocsátók,
- elektronikus aláírás termékek szállítói,
- KRA kapcsolattartó,
- KRA felhasználó,
- szakértői támogatás.

2.4.1 Az aláírás létrehozója (aláíró)

Az aláíró az a természetes személy, aki az aláírás-létrehozó adatot és az aláírás-létrehozó eszközt birtokolja, valamint a saját vagy más személy (természetes, illetve jogi személy vagy jogi személyiség nélküli szervezet) nevében, vagy egy felügyelt automatizmusra (aláíró szerverre) vonatkozó szabályozás alapján aláírásra jogosult.

A KRA az egyes szolgáltatásainak igénybe vétele céljából regisztrálja és nyilvántartásba veszi a jogosult aláírókat. A regisztráció során a KRA kapcsolattartó megadja az aláíró KRA rendszer használatához szükséges azonosító adatait.

2.4.2 Az aláírás elfogadója (aláírást ellenőrző)

Az aláírást ellenőrző fél az a személy, vagy felügyelt aláíró automatizmus, aki/amely az elektronikusan aláírt elektronikus üzenetek aláíráskori, illetve ellenőrzéskori tartalmát összeveti, továbbá az aláíró személyét azonosítja az üzenet, illetve a hitelesítés-szolgáltató által közzétett aláírás-ellenőrző adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával.

2.4.3 Hitelesítés szolgáltató

A hitelesítés szolgáltató az elektronikus aláírással kapcsolatos szolgáltatást nyújtó természetes személy, jogi személy vagy jogi személyiség nélküli szervezet.

Az NMHH az egyes szolgáltatásainak igénybe vétele céljából nyilvántartásba veszi az általa elfogadható hitelesítés szolgáltatókat. A NMHH fenntartja magának a jogot, hogy megvizsgálja az egyes szolgáltatók által követett, az adott aláíró tanúsítványban megadott hitelesítési rendet, esetenként a hitelesítés szolgáltatási szabályzatot is.

Az elfogadott hitelesítési rendek az NMHH által nyilvántartásba vett és hatályos, a közigazgatásban alkalmazható tanúsítvány hitelesítési rendek.

2.4.4 Kriptográfiai eszközkibocsátók

Az aláírónak, vagy a felügyelt automatizmusnak, megfelelő gondosságot kell tanúsítania annak érdekében, hogy megelőzze aláírás-létrehozó adatának (kriptográfiai magánkulcsának) illetéktelen felhasználását.

A NMHH a KRA-val kapcsolatban használt kriptográfiai eszközök használatára egyéb kikötést nem tesz. Jelen dokumentum M1. mellékletében felsorolásra kerülnek a KRA-val kompatibilis kliens oldali kriptográfiai eszközök.

2.4.5 Elektronikus aláírás termékek szállítói

Jelen szabályzat útmutatóul szolgál az elektronikus aláírás termékek fejlesztőinek, illetve az ilyen termékek szállítóinak és rendszerintegrátorainak is.

2.4.6 KRA kapcsolattartó

Szolgáltató által kijelölt természetes személy, aki eljárhat a szolgáltató részéről a KRA szolgáltatásokkal kapcsolatos ügyintézés és képviselet során.

2.4.7 KRA felhasználó

A KRA rendszerhez való hozzáférésre feljogosított személy vagy felügyelt automatizmus, aki/amely az általa képviselt szolgáltató vagy szervezet nevében a KRA rendszerben hordozási műveleteket végezhet vagy adatokat kérdezhet le.

NMHH ügyfélszolgálatát ellátó KRA operátorok emellett jogosultak a szolgáltatói és felhasználói adatok adminisztrációjára és a rendszer paraméterek módosítására.

2.4.8 Szakértői támogatás

A NMHH az elektronikus aláírás során felmerülő vitás technikai megoldások kezelésére szakértőn keresztül támogatást nyújt. Ezen szakértőket a KRA ügyfélszolgálatán keresztül lehet elérni.

2.5 Kapcsolódó szabályozások

A szabályozás az alábbi mértékadó normatívákon és dokumentumokon alapul:

- 2015. évi CCXXII. törvény
  Törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól[1],
- 24/2016. (VI. 30.) BM rendelet
  Rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről[2],
- 910/2014/EU európai parlamenti és a tanácsi rendelet (eIDAS rendelet)[3],
- ITU-T X.509
  Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks[4],

[1] https://njt.hu/jogszabaly/2015-222-00-00
[2] https://njt.hu/jogszabaly/2016-24-20-0A
[3] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32014R0910&from=EN
[4] https://www.itu.int/rec/T-REC-X.509

- ETSI TS 102 176
  Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures[5];
- ETSI TS 119 312
  Electronic Signatures and Infrastructures (ESI); Cryptographic Suites[6],
- ETSI TS 102 918 Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (ASiC)[7]
- W3C TR XML Signature Syntax and Processing[8]
- W3C TR Canonical XML[9]
- PKCS #11 Cryptographic Token Interface Standard[10]
- 23/2020. (XII.21.) NMHH rendelet
  Rendelet a szolgáltatóváltás és számhordozás részletes szabályairól[11].

[5] https://www.etsi.org/standards-search#page=1&search=ETSI%20TS%20102%20176&title=0&etsiNumber=1&content=0&version=0&onApproval=1&published=0&historical=1&startDate=1988-01-15&endDate=2019-09-01&harmonized=0&keyword=&TB=&stdType=TS&frequency=&mandate=&collection=&sort=1

[6] https://www.etsi.org/standards-search#page=1&search=TS%20119%20312&title=1&etsiNumber=1&content=0&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2017-02-14&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1

[7] https://www.etsi.org/standards-search#page=1&search=TS%20102%20918&title=1&etsiNumber=1&content=0&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2017-02-14&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1

[8] https://www.w3.org/TR/xmldsig-core1/

[9] https://www.w3.org/TR/xml-c14n11/

[10] https://www.cryptsoft.com/pkcs11doc/

[11] https://njt.hu/jogszabaly/2020-23-20-3H

3 ELEKTRONIKUS ALÁÍRÁSHOZ KAPCSOLÓDÓ KÖVETELMÉNYEK

Az elektronikus aláírás az adatok hitelesítésére szolgál.

Egyrészt a szolgáltató felhasználója az általa a rendszer felé küldendő adatokat elektronikus aláírásával látja el, ezzel igazolva, hogy az adatokat ő maga küldte. Az aláíró mechanizmus működéséből következik az is, hogy ha az adatcsomag az átvitel során sérülne, illetve megváltozna, az azonnal kiderülne, és a sérült adatok nem kerülnének be az adatbázisba, így a beérkező adatok szempontjából az adatbázis hiteles marad.

Másrészt a KRA, az általa küldött válaszüzeneteket, nyugtákat és listákat elektronikus aláírással látja el, azok hitelességének igazolására és ellenőrizhetőségére.

3.1 Alkalmazható algoritmusok

A KRA-ban kizárólag az ETSI TS 102 176 szerinti RSA-SHA256 aláíró algoritmus alkalmazható.

3.2 A KRA-ban kezelt aláírási formátum

Az elektronikus aláírás a KRA-ban egyrészt az XML üzenetek aláírását jelenti a felhasználó és a KRA által készített üzenetek esetében egyaránt.

Az XML üzenetek aláírása csak a World Wide Web Consortium (W3C) által specifikált szintaktika és feldolgozás szerint lehetséges. A W3C szerinti „enveloping signature” egy XML elektronikus aláírás elembe ágyazott XML elem, amely az aláírt adatokat XML-ként tartalmazza.
A pontos részletek a következő helyeken találhatók meg:

- W3C TR XML Signature Syntax and Processing[12]
- W3C TR Canonical XML[13].

Másrészt a KRA az irányítási listákat CSV formátumban állítja elő, melyeket úgynevezett ASiCe konténerbe csomagol. Ennek részletei a következő specifikációban találhatók:

- ETSI TS 102 918 Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (AsiC)[14].

A KRA-ban nem lehet használni többek között:

- Aláírt XML-be ágyazott elektronikus aláírás elemet,
- XML tartalomtól elválasztott XML elektronikus aláírást,
- Többszörös aláírással küldött üzenetet.

[12] https://www.w3.org/TR/xmldsig-core1/
[13] https://www.w3.org/TR/xml-c14n11/
[14] https://www.etsi.org/standards-search#page=1&search=TS%20102%20918&title=1&etsiNumber=1&content=0&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2017-02-14&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1

3.3 Elektronikus aláíró tanúsítványok

Aláírásra csak olyan tanúsítvány használható, melyben a Kulcshasználat beállítás a „Letagadhatatlanság (c0)” kijelölését mutatja (NR-bit: true).

A tanúsítvány lehet személyes vagy szervezeti aszerint, hogy milyen információkat tartalmaz a tanúsítvány birtokosával kapcsolatban. A szervezetek részére kibocsátott tanúsítvány elnevezése **bélyegző**. Jelen dokumentumban az elektronikus aláíró tanúsítványba mind a személyes aláírói, mind a bélyegző tanúsítványt beleértjük.

A KRA az alábbi tanúsítvány-típusokat fogadja el:

- fokozott biztonságú (nem minősített) hitelesítés szolgáltatótól származó tanúsítvány
    - közigazgatásban nem alkalmazható tanúsítványok
    - közigazgatásban alkalmazható tanúsítványok
- minősített hitelesítés szolgáltatótól származó tanúsítvány
    - közigazgatásban nem alkalmazható tanúsítványok
    - közigazgatásban alkalmazható tanúsítványok

Az aláíró tanúsítványt a szolgáltatónak egy magyarországi tanúsítványt kibocsátó hitelesítés-szolgáltatótól kell beszereznie. A magyarországi hitelesítés szolgáltatók listája az NMHH honlapján: NMHH a szakmáért > Bizalmi aláírással kapcsolatos nyilvántartások[15].

KRA-ban használható elektronikus aláíró és elektronikus bélyegző tanúsítványokat jelen dokumentum érvényessége alatt a MICROSEC zrt.[16], a Netlock Kft.[17] és a NISZ Zrt.[18] hitelesítés szolgáltatóktól lehet beszerezni.

3.3.1 A tanúsítványok érvényessége

A KRA csak akkor tekint egy tanúsítványt érvényesnek, ha az alábbi körülmények egyike sem áll fenn:

- a tanúsítvány lejárt („notAfter” szerinti érvényességi idő elmúlt) vagy ha a tanúsítvány még nem érvényes („notBefore” szerinti érvényességi idő meg nem kezdődött el),
- a tanúsítvány a hitelesítés szolgáltató visszavonási listáján szerepel,
- a tanúsítványban feltüntetett adatok nem a valóságnak megfelelően szerepelnek,
- kompromittált, amikor a tanúsítványhoz kapcsolódó érvényességi lánc bármely eleméhez tartozó adat bizalmassága sérült, vagy a tanúsítvány illetéktelen kézbe került,
- az alkalmazott aláírási algoritmusok nem megfelelőek, vagy nem biztonságosak (az aláírás-ellenőrző adatból származtatható az aláírás-létrehozó adat, vagy egy előre meghatározott lenyomathoz utólag elkészíthető egy e-üzenet).

[15] http://webpub-ext.nmhh.hu/esign2016/setLanguageAction.do?lang=hu
[16] https://e-szigno.hu/
[17] https://netlock.hu/
[18] https://hiteles.gov.hu/

A NMHH fenntartja magának a jogot, hogy törölje és ezzel az adatkezelésből kizárja azokat a tanúsítványokat, amelyekhez az informatikai rendszerének védelme érdekében jogos érdeke fűződik.

3.3.2 Aláíró tanúsítványok azonosítása

A számhordozásban résztvevő szolgáltatók és megbízottjaik aláírási jogosultságát az KRA a tanúsítványaik azonosítóinak felhasználásával tartja nyilván, és ennek alapján kezeli. A felhasznált azonosítók a következők: a szolgáltató azonosítói és az aláíró tanúsítványok Base64 kódolású X.509 formátumú állományai.

3.4 Aláírás-létrehozó termékek és alkalmazás szolgáltatók igénybe vétele

Az aláírók az aláírás-létrehozó termékek (aláírás termékek) és az alkalmazás szolgáltatók vonatkozásában az elektronikus aláírás törvény alapján viselnek felelősséget.

A KRA rendszereiben az aláíró automatizmusoknál, valamint a védett kommunikációs csatornák esetében a kriptográfiai kulcsok védelme megoldott, az alkalmazott eszközök és eljárások nem publikusak.

3.5 Aláírás-ellenőrző termékek

Az aláírást ellenőrző felek (érintettek) az aláírás-ellenőrző termékek (aláírás termékek) és az alkalmazás szolgáltatók vonatkozásában az elektronikus aláírás törvény alapján viselnek felelősséget.

4 AZ ALÁÍRÓ TANÚSÍTVÁNYOK HASZNÁLATÁNAK TOVÁBBI FELTÉTELEI ÉS SZABÁLYAI A KRA-BAN

4.1 Aláíró tanúsítvány regisztrálása a KRA-ban

A KRA rendszerben az aláíró tanúsítvány használatának feltétele a regisztráció, amely az aláíró tanúsítvány hozzárendelését tartalmazza egy adott KRA felhasználói hozzáféréshez.

Egy aláíró tanúsítvány csak egy hozzáféréshez, azaz felhasználónévhez regisztrálható, azonban egy felhasználónévhez két aláíró tanúsítvány regisztrálására is lehetőség van.

Az aláíró tanúsítvány regisztrációját a szolgáltató által megbízott KRA kapcsolattartó kérheti. A regisztráció során az aláíró tanúsítványban szereplő adatok és magának a tanúsítványnak a Base64 kódolású ITU-T X.509 formátumú állománya kerül rögzítésre a KRA-ban.

4.2 Aláíró tanúsítvány cseréje

Az aláíró tanúsítvány megújítása vagy új tanúsítvány készíttetés esetén az új tanúsítvány és a lejáró tanúsítvány egyidejűleg regisztrálható a KRA felhasználónévhez.

A KRA a felhasználónévhez regisztrált bármelyik érvényes aláíró tanúsítvány használatát elfogadja.

4.3 A felhasználói aláírás létrehozása

A SOAP interfészen keresztül kommunikáló szolgáltatónak úgy kell elkészítenie alkalmazását, amely megfelel a KRA SOAP interfész specifikációban leírt előírásoknak.

A KRA alkalmazás használata esetén maga az alkalmazás alakítja át az egyes tranzakcióknál bevitt adatokat a SOAP interfész specifikáció előírásainak megfelelő XML formátumú üzenetté, amelyet a bejelentkezés során kiválasztott aláíró tanúsítvánnyal aláír.

4.4 A felhasználói aláírás ellenőrzése

A felhasználók által beküldött XML formátumú üzenet aláírásának KRA oldali ellenőrzési folyamata a következő:

- Az üzenet struktúrájának az ellenőrzése;
- XML tartalom megfelelősségének ellenőrzése a SOAP interfész specifikációban leírtak szerint;
- Integritás ellenőrzése az XML aláírás előírásai szerint;
- Aláíró tanúsítvány ellenőrzése
    - tanúsítási lánc felépítése;
    - aláíró tanúsítvány érvényességének ellenőrzése;
    - visszavonási listák (CRL) ellenőrzése.

4.5 A KRA aláírás létrehozása

A KRA által küldött XML formátumú üzenet aláírásának folyamata a következő:

- Válasz üzenet (üzenet, nyugta, hibaüzenet, lista) tartalmi összeállítása az XML tartalom specifikáció szerint;
- Aláíró tanúsítvány ellenőrzése;
- XMLDsig[19] szerinti aláírás elkészítése.

A KRA által készített irányítási listák aláírási folyamata a következő:

- Az irányítási lista állományok összeállítása a specifikáció szerint
- Aláíró tanúsítvány ellenőrzése
- ETSI TS 102 918 [20] AsiCe szabvány szerinti aláírás elkészítése

4.6 A KRA aláírás ellenőrzése

A KRA által előállíttott XML formátumú üzenet aláírásának ellenőrzési folyamata a felhasználó oldalon a következő lépéseket kell tartalmazza:

- Az üzenet struktúrájának az ellenőrzése;
- XML tartalom megfelelősségének ellenőrzése a SOAP interfész specifikációban leírtak szerint;
- Integritás ellenőrzése az XML aláírás előírásai szerint;
- XML aláírás ellenőrzése;
- Aláíró tanúsítvány ellenőrzése
    - tanúsítási lánc felépítése;
    - aláíró tanúsítvány érvényességének ellenőrzése;
    - visszavonási listák (CRL) ellenőrzése.

A KRA által elkészített és ASICe aláírással elllátott állományok esetén az ASICe konténer szabványos aláírás ellenőrzése a következő lépéseket tartalmazza:

- A konténer integritásának és struktúrájának az ellenőrzése
    - A konténer tartalmazza az ASICe leíróban (manifest.xml) szereplő állományokat
- ASICe aláírás ellenőrzése
- Aláíró tanúsítvány ellenőrzése

[19] https://www.w3.org/TR/xmldsig-core1/

[20] https://www.etsi.org/standards-search#page=1&search=TS%20102%20918&title=1&etsiNumber=1&content=0&version=1&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2017-02-14&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1

- tanúsítási lánc felépítése;
- aláíró tanúsítvány érvényességének ellenőrzése;
- visszavonási listák (CRL) ellenőrzése.

5 MELLÉKLETEK

5.1 Támogatott Biztonságos Aláírás Létrehozó Eszközök (BALE)

Szolgáltatói felhasználó, azaz az aláíró által használt BALE-kel kapcsolatban a cél, hogy az elfogadott hitelesítés szolgáltatók által kínált BALE-k legbővebb halmaza támogatott legyen. Jelen dokumentum érvényessége alatt támogatott eszközök:

Eszköz	Eszköz operációs rendszer	Eszköz chip	Támogatott hoszt operációs rendszer
Aladdin e-Token PRO	CardOS/M4.01	SLE66CX320P	Microsoft Windows, Linux, Macintosh
Oberthur CosmopolIC intelligens kártya	nyílt Java platform 2.1 V4 verzió	P8WE5033V0G	Microsoft Windows
ORGA intelligens kártya	MICARDO v2.1	SLE66CX320P	Microsoft Windows
Giesecke & Devrient token	STARCOS SPK 2.3 v7.0	P8WE5032v0G	Microsoft Windows
SUN Crypto Accelerator	Solaris 10 SPARC		Microsoft Windows
Axalto Cyberflex Access 64K v2a	Global Platform – Open Platform v2.0.1	SLE66CX640P	Microsoft Windows
nChiper NetHSM 2000			Microsoft Windows, Linux
eToken PRO Java Card 72K	OS755, eToken Java Applet 1.0.37	AT90SC25672RCT-USB	Microsoft Windows

KRA rendszer képes a fent felsoroltakon kívül minden BALE-vel együttműködni, amely képes megvalósítani a szabványos PKCS11 kommunikációt.

5.2 Kártyaolvasóval és kártyával kapcsolatos beállítások

Az aláíró tanúsítvány kártyán vagy más biztonsági eszközön (pl. USB Token) történő tárolása esetén az ezek működéséhez szükséges fájlokat is telepíteni kell.

Ellenőrzendő, hogy a Windows operációs rendszer telepítés során a C:\WINDOWS\system32 mappájában a kártya típusától függően az alábbi listában szereplő, a kártyának megfelelő dll kiterjesztésű fájl megtalálható-e!

Megjelenített név	dll
ORGA Micardo	MicardoPKCS11.dll
ActivCard Gold	acpkcs.dll
Oberthur	OCSCryptolib_P11.dll
Oberthur AuthentIC	OCSCryptoki.dll
Oberthur ID One	AuCryptoki2-0.dll
Schlumberger Cyberflex	slbck.dll
Rainbow iKey 3000	aetpkss1.dll
Giesecke	htaetfix.dll
Giesecke SmartSign	hthlkfix.dll
Giesecke SmartSign (ht)	htsspk11.dll
Rainbow iKey 2000	dkck201.dll
Rainbow CryptoSwift HSM	iveacryptoki.dll
Aladdin e-Token	eTpkcs11.dll
OpenSmartCard	opensc-pkcs11.dll
Axalto	xltCk.dll
Gemalto Cryptoflex .NET	gtop11dotnet.dll
Gemalto Classic V3 GemP15-1	gclib.dll
Touch&Sign2048	bit4ipki.dll
Gemalto IDPrime	IDPrimePKCS11.dll

Ha a kártyaolvasó működik, de a kívánt dll nem található, akkor a dll helye megadható a KRA kliens alkalmazás részére. Ehhez az alkalmazásban *tanúsítványtár beállítások* gombra kattintva, a megjelenő ablakon a *kártyaolvasó illesztőprogram hozzáadása* lehetőséget választva meg kell adni a dll helyét, mely általában a C:\Program files könyvtárban keresendő, illetve a kártyát és a kártyaolvasót rendelkezésre bocsátótól tudható meg. A dll-t és egy tetszőleges elnevezést csak egyszer kell megadni, az alkalmazás megjegyzi.

Linux operációs rendszer esetén az alábbi táblázat mutatja az alapértelmezetten támogatott kártyák listáját:

Megjelenített név	so
Aladdin e-Token	libeTPkcs11.so

MacOS esetén a támogatott kártyák:

Megjelenített név	**dylib**
Aladdin e-Token	libeTPkcs11.dylib
GemP15-1	libgclib.dylib
GemP15_El-Capitan	libgclib.dylib

KRA rendszer a fent felsoroltakon kívül képes minden BALE-vel együttműködni, amely meg tudja valósítani a szabványos PKCS11 kommunikációt.

6 VÁLTOZTATÁSOK ÖSSZEFOGLALÁSA

Változat száma:	Kiadás időpontja:	Változtató:	Változtatás:
1.0	2009. november 12.	NHH, IQSYS	KRA továbbfejlesztés 5. fázis – alapdokumentum kiadása
1.01	2010. július 12.	NHH, IQSYS	A dokumentum véglegesítése
1.02	2012. szeptember 24.	NMHH, IQSYS	Jogszabályváltozás miatti pontosítás Bizalmi lista bevezetése
1.1	2016. június 10.	T-Systems	SHA1 kivezetése
5.00	2017. február 16.	NMHH, T-Systems	Kiegészítés a 2016 évi fejlesztésekkel A műszaki leírások szerkezetének átrendezése
5.01	2018. február 9.	NMHH	NMHH honlap változások, jogszabályváltozások
6.00	2019. október 1.	NMHH	Pontosítások
6.01	2020. június 24.	NMHH	Jogszabályok frissítése KRA aláíró tanúsítvány csere miatti módosítás
6.02	2021. január 11.	NMHH	KRA weboldalak ssl tanúsítványai és a Java applet kódaláíró tanúsítvány csere miatti módosítás
7.00	2022.március 1.	NMHH, T-Systems	A KRA webes hozzáférés megszűnése és a KRA alkalmazás bevezetése miatti változások
7.01	2022. május 31.	NMHH	A dokumentum akadálymentesítése

A specifikáció készítői mindent megtesznek annak érdekében, hogy a dokumentumban található adatok a lehető legpontosabbak legyenek, de az esetleg mégis előforduló hibákból eredő következményekért felelősséget nem vállalnak.

Kérjük, hogy a dokumentummal kapcsolatos észrevételeit küldje el a NMHH KRA ügyfélszolgálata részére, a kra-uszi@nmhh.hu email címre! Ezzel kapcsolatos fáradozásait előre is köszönjük.