Nemzeti Média- és Hírközlési Hatóság

KRA Elektronikus aláírási kézikönyv

6.02 VÁLTOZAT

2021. január 11.

Készítette:

Nemzeti Média- és Hírközlési Hatóság

Azonosítógazdálkodási Osztály

TARTALOMJEGYZÉK

BEVEZETÉS

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

Az ebben a kézikönyvben 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.

Az 1. fejezet megismerteti a KRA szerepét a számhordozásban, továbbá ismerteti a KRA műszaki leírás dokumentumok tartalmi elemeit.

A 2. fejezet felsorolja az elektronikus hitelesítésekre vonatkozó alapvető normatívákat, valamint ismerteti a KRA-ban alkalmazott tanúsítvány típusokat.

A 3. fejezet a KRA hozzáférési tanúsítványok és az aláíró tanúsítványok beszerzéséhez tartalmaz útmutatást.

A 4. fejezet a tanúsítványok érvényességének feltételeit ismerteti.

Az 5. fejezet a tanúsítványok különböző eszközökön való tárolásához kapcsolódó tudnivalókat tartalmazza.

A 6. fejezet bemutatja a KRA használatához szükséges tanúsítványokat és támogatást nyújt a tanúsítványok telepítéséhez.

A 7. fejezet az aláíró tanúsítványok KRA-ban való használatának további fontos feltételeit ismerteti. Részletes útmutatót tartalmaz a web felület használatánál szükséges Java futtatókörnyezet telepítéséhez és beállításához, valamint ismerteti a SOAP interfészen alkalmazható elektronikus aláírás algoritmusokat és formátumokat.

A 8. fejezet összefoglalja, hogy miként történik a KRA-ban a felhasználóktól beérkező üzenetek elktronikus aláírásának ellenőrzése, és miként készíti el a KRA a kiküldendő üzenetek aláírását.

Az M1 melléklet a KRA-val kapcsolatos internetes hivatkozások gyűjteménye.

1 SZÁMHORDOZÁSI KÖZPONTI REFERENCIA ADATBÁZIS

1.1 A KRA feladata

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 számra irányuló hívások megfelelő irányításához szükséges adatokhoz való hozzáférés biztosítása a szolgáltatók számára.

A KRA nem tartalmaz előfizetői adatokat, ezért nem feladata a számhordozási eljárásban a hordozást igénylő előfizetők azonosításának és az adatok egyeztetésének támogatása, ez a számhordozásban érintett átadó és átvevő szolgáltató kétoldalú ügyfélszolgálati eljárásának a feladata. A számhordozási eljárás így két részre osztható, a hordozási igények és előfizetői adatok szolgáltatók közötti egyeztetésére és az egyeztetés alatt álló hordozások irányítási adatainak KRA-ba való bevitelére.

1.2 KRA műszaki leírás

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.

A KRA műszaki leírását a szolgáltatók részére a számhordozást és a KRA-t bemutató ismertető és a felhasználói kézikönyvek együtt alkotják. A dokumentumok az NMHH honlap Számhordozás (KRA) oldaláról, valamint a KRA rendszer és a teszt rendszer Súgó oldaláról letölthetők.

A KRA műszaki leírás dokumentumok a következők.

KRA Általános ismertető

A dokumentum a számhordozási és a KRA ismereteket különböző szempontok szerint tagolva tartalmazza.

KRA WEB felhasználói kézikönyv

A kézikönyv a webes felületet használó személyek részére ismerteti a KRA-hoz való hozzáférés módját, a KRA-val való kommunikáció szabályait és a web felület használatát.

KRA SOAP felhasználói kézikönyv

A kézikönyv a szolgáltatói automata rendszerek kommunikációjának, a gép-gép kapcsolatnak a szabályait, eljárásait tartalmazza. A dokumentumban elsősorban azok az XML-kommunikációs konvenciók, formátumok kerülnek kifejtésre, melyek a KRA-rendszer *Integrált szolgáltatásain* keresztül történő kapcsolatkialakításhoz, a szolgáltatói oldali fejlesztéséhez szükségesek.

KRA Elektronikus aláírási kézikönyv

Ez a dokumentum a KRA rendszer használatához a rendszer védelme és az adatbázis hitelességének megőrzése érdekében alkalmazott elektronikus hitelesítéseket tárgyalja. A kézikönyv a szolgáltatói számhordozási ügyintézők számára összefoglalja a KRA-ban használt tanúsítvány fajtákat, valamint a tanúsítványok beszerzésének és tárolásának egyes kérdéseit, majd a fejlesztők számára is részletekbe menően tárgyalja a tanúsítványok használatának szabályozását a számhordozási rendszerben.

2 ELEKTRONIKUS HITELESÍTÉSEK A KRA-BAN

A KRA rendszer használatához a rendszer védelme és az adatbázis hitelességének megőrzése érdekében elektronikus hitelesítéseket használunk.

Általánosságban, az alkalmazott elektronikus hitelesítéseknek meg kell felelniük az alábbi alapvető normatíváknak:

- 2015. évi CCXXII. törvény
  Törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól,
- 24/2016. (VI. 30.) BM rendelet
  Rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről,
- 910/2014/EU európai parlamenti és a tanácsi rendelet (eIDAS rendelet),
- ITU-T X.509
  Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,
- ETSI TS 102 176
  Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures;
- ETSI TS 119 312
  Electronic Signatures and Infrastructures (ESI); Cryptographic Suites,
- ETSI TS 102 918 Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (ASiC)
- W3C TR XML Signature Syntax and Processing
- W3C TR Canonical XML
- PKCS #11 Cryptographic Token Interface Standard
- 2/2012. (I.24.) NMHH rendelet
  Rendelet a számhordozás részletes szabályairól,

A KRA-ban használt elektronikus hitelesítésekkel kapcsolatos gyakorlati tudnivalókat a KRA WEB felhasználói kézikönyvben és a KRA SOAP felhasználói kézikönyvben ismertetetteken túl ebben a leírásban tesszük közzé.

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

Feltételezzük, hogy a KRA felhasználója alapismeretekkel rendelkezik a PKI (Public Key Infrastructure) rendszerű elektronikus hitelesítések terén, így csak annyit említünk meg, hogy a KRA-ban használt az elektronikus hitelesítések *készítéséhez* egy kulcs-párra (magán kulcsra és nyilvános kulcsra) és a kulcs-párhoz tartozó, megbízható hitelesítés szolgáltató által kiállított tanúsítványra van szükség. A hitelesség *ellenőrzéséhez* egy megfelelő tanúsítványra van szükség (mely tartalmazza a nyilvános kulcsot). A

továbbiakban előfordulhat, hogy az egyszerűség kedvéért, ha ez nem okozhat félreértést, *tanúsítványnak* nevezzük a kulcs-pár és a tanúsítvány együttesét is.

A számhordozási rendszerben különböző célokra használunk tanúsítványokat:

- weboldalak azonosítására,
- a KRA weboldalak eléréséhez (hozzáférési vagy autentikációs tanúsítványok)
- az üzenetek és irányítási listák elektronikus aláírására (aláíró tanúsítványok),
- az elektronikus aláírás készítését segítő kisalkalmazás (más néven segédprogram vagy applet) megbízhatóságának igazolására (kódaláíró tanúsítvány).

A KRA és a teszt rendszerben kevés kivételtől eltekintve rendszerenként különböző tanúsítványokat használunk.

2.1 A számhordozási rendszer weboldalainak azonosítására szolgáló tanúsítványok

A számhordozási rendszer weboldalaihoz (https://kra.nmhh.hu és https://kra-test.nmhh.hu) tanúsítványok tartoznak, azokkal a biztonságos kapcsolat a https protokoll szerint történik, így a kommunikáció titkosított csatornán folyik.

2.2 Felhasználói hozzáférési tanúsítványok

A számhordozási rendszer https protokoll szerinti elérése egyúttal lehetővé teszi azoknak a felhasználóknak az azonosítását, idegen szóval autentikációját, akik engedélyt kaptak ezeknek a weboldalaknak az eléréséhez, azaz a számhordozási rendszer használatához. Ezt az engedélyt, azaz a KRA rendszer, mint informatikai rendszer használatára szóló engedélyt tanúsítvány formájában kapja meg a felhasználó. Ezt a tanúsítványt hozzáférési, más néven autentikációs tanúsítványnak nevezzük.

2.3 Aláíró tanúsítványok

Az aláíró tanúsítvány 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.

2.4 Kódaláíró tanúsítvány

Ha a felhasználó WEB interfészen keresztül használja a KRA-t, akkor a felhasználói elektronikus aláírás készítésének bonyolult folyamatát a háttérben egy Java programozási nyelven készült kisalkalmazás segíti. A kisalkalmazás kódsorainak eredetiségét egy kódaláíró tanúsítvány által készített aláírás igazolja.

3 A TANÚSÍTVÁNYOK BESZERZÉSE

A nemzetközi szabványoknak megfelelő, így széles körben használható tanúsítványokat a szigorú és rendszeres ellenőrzés mellett működő úgynevezett hitelesítés szolgáltatók állítják ki. A hitelesítés szolgáltatókon kívül más szervezetek is bocsáthatnak ki tanúsítványokat. Ilyen az NMHH is, mely saját maga állítja ki azokat a tanúsítványokat, melyek a számhordozási rendszer hozzáférési engedélyeként szolgálnak.

Egy tanúsítvány egy meghatározott érvényességi ideig használható, melyet követően újat kell kiváltani. A lejárat előtt egy tanúsítvány általában egyszer megújítható. A megújítás során a kulcspár nem változik, csak a kulcspárhoz tartozó tanúsítvány kerül újbóli kiadásra a már frissített adatokkal. Ha már nem újítható meg a tanúsítvány, akkor az új tanúsítvány kiállítása mellett új kulcspár generálására is sor kerül. A magyarországi hitelesítés szolgáltatók aláíró tanúsítványokat általában egy-két évig, míg az NMHH a hozzáférési tanúsítványokat három évig érvényesen adja ki. A megújítás egyszerűbb eljárás, mint az új tanúsítvány igénylés.

Egy tanúsítványban számos adat szerepel a kiadójáról, a tulajdonosáról és a felhasználhatóságáról. Egy tanúsítvány csak arra a célra használható, melyre kiállításra került. Például egy hozzáférésre kiadott tanúsítvány csak autentikációra használható, aláírásra nem.

A számhordozási rendszerben korlátozva van a tanúsítvány használat, olyan értelemben, hogy csak arra van lehetőség, hogy egy adott tevékenységhez kizárólag a rendszerben is regisztrált tanúsítványt lehessen használni. Ez a gyakorlatban azt jelenti, hogy ha egy hitelesítés szolgáltató kiállított egy aláíró tanúsítványt, az csak akkor használható a KRA-ban is aláírásra, ha a KRA-ban is regisztrálásra került és akkor is csak az a felhasználó használhatja, akihez az a tanúsítvány hozzárendelésre került!

3.1 A hozzáférési tanúsítványok beszerzése

A hozzáférési tanúsítványt az NMHH állítja ki a szolgáltató igényére, a felhasználója részére a *Felhasználó regisztráció* adatlapon közölt adatok alapján, azt követően, hogy a szolgáltató kapcsolattartója eljuttatta azt a KRA ügyfélszolgálatához. Minden felhasználó saját tanúsítványt kap külön a KRA rendszerhez és a teszt rendszerhez egyet-egyet, ha igényli. Ennek a fajta tanúsítványnak a kiállításáért **az NMHH díjat nem számít fel**. (Ha egy szolgáltató több szolgáltató kóddal (SK) rendelkezik vagy egy felhasználót több szolgáltató is megbíz nevében KRA műveletek végzésére, akkor nem kell szolgáltató kódonként hozzáférési tanúsítvány(oka)t igényelnie, hanem egy meglévő hozzáférési tanúsítvánnyal a felhasználó több SK-hoz is regisztrálható, és az NMHH nem állít ki új tanúsítványt SK-nként.)

Az NMHH a hozzáférési tanúsítványokat legtöbbször **CD-n adja ki**, de igény esetén egyeztetést követően, bizonyos **intelligens kártyákon is elő tudja állítani**. Ilyen igény esetén a felhasználónak, vagy megbízottjának a kártyát az NMHH KRA ügyfélszolgálatának rendelkezésére kell bocsátania a hozzáférési tanúsítványok generálása céljára. Időegyeztetéstől függően a tanúsítványokat az NMHH a kért időpontban, vagy néhány nap alatt elkészíti. Ebben az esetben – ahogyan azt már említettük – ha a kártyát a tulajdonosa kiadja a kezéből, akkor ezt a kiállító hitelesítés szolgáltatónál jeleznie kell. A jelzést követően a hitelesítés szolgáltató a tanúsítványt haladéktalanul felfüggeszti, majd a tulajdonos kérésére később aktiválja. Figyelemmel kell lenni arra, hogy a felfüggesztésre kért idő nem lehet több tipikusan egy hétnél, ezt túllépve a tanúsítványt újra ki kell váltani, mely költséggel jár!

Általában egy felhasználó egyszerre igényel hozzáférési tanúsítványt a KRA-hoz és a teszt rendszerhez is (így érdemes, mert a rendszer megismerése, az egyes műveletek kipróbálása, gyakorlása következmények nélkül végezhető a teszt rendszeren), és rendelkezik egy aláíró tanúsítvánnyal is, azaz összességében tipikusan három olyan tanúsítványa van, melyhez magán kulcs is tartozik.

A hozzáférési tanúsítvány megújítását a KRA kapcsolattartó igényelheti. Ezt ajánlott annak érvényességi határideje előtt 2-4 héttel megtenni, amennyiben továbbra is szükség lenne rá. A hozzáférési tanúsítvány közeledő lejáratáról a számhordozási rendszer e-mail értesítést küld először egy hónappal, majd héttel a lejárat előtt, végül a lejárat napján.

A megújításkor ugyanúgy kell eljárni, mintha az első tanúsítvány igénylése történne, azaz egy új felhasználói regisztrációs lapon kell a felhasználó részére az új tanúsítványt kérni. Ez a tanúsítvány ugyanolyan eljárással vehető át, mint a felhasználó legelső tanúsítványa, vagyis CD-n vagy kártyán, amit postázva vagy személyesen ad át az NMHH. A tanúsítvány telepítéséhez szükséges jelszót sms-ben küldjük el a regisztrációnál kötelezően megadandó mobil telefonszámra. Ameddig a korábban kibocsátott tanúsítvány érvényes (nem járt le vagy nincs visszavonva) és már az új tanúsítvány is a felhasználó rendelkezésére áll, akkor mindkét tanúsítvánnyal lehetséges a KRA elérése.

3.2 A felhasználói aláíró tanúsítványok beszerzése

Az aláíró tanúsítványt a szolgáltatónak kell beszereznie egy magyarországi tanúsítványt kibocsátó hitelesítés-szolgáltatótól. A hitelesítés szolgáltatók listája az NMHH honlapján is megtekinthető (NMHH a szakmáért > E-szolgáltatások > Bizalmi szolgáltatások > Nyilvántartások > Elektronikus aláírással kapcsolatos nyilvántartások > Nem-minősített szolgáltatások vagy Minősített szolgáltatások) helyen.

Jelenleg a Microsec e-Szignó és a Netlock hitelesítés szolgáltatóktól lehet beszerezni KRA-ban használható aláíró tanúsítványokat (ld. *M1 Melléklet*). Pontos részleteket az egyes hitelesítés-szolgáltatóktól lehet megtudni.

ALÁÍRÓ TANÚSÍTVÁNY ÉS BÉLYEGZŐ

Az aláíró tanúsítvánnyal kapcsolatos feltétel, hogy az **legalább fokozott biztonságú** legyen (a minősített tanúsítvány a fokozottnál magasabb szintű, ezért megfelelő, vagy a közigazgatásban alkalmazható tanúsítvány szintén megfelelő, de kizárólag a KRA használatához gazdaságtalan).

A tanúsítványok aszerint is csoportosíthatók, hogy milyen információkat tartalmaznak a tanúsítvány birtokosával kapcsolatban. Ebből a szempontból egy tanúsítvány lehet **személyes vagy szervezeti** tanúsítvány, de kibocsátható **automaták** (tipikusan számítógépek vagy szerverek) részére is.

A szervezetek részére kibocsátott tanúsítvány elnevezése **bélyegző**. Bélyegző tanúsítvány kiváltása illetve használata gazdaságos, mert azt a szolgáltató minden alkalmazottja használhatja, akit felhatalmaznak rá, azaz nem kell minden személy részére külön-külön tanúsítványt vásárolni. A továbbiakban az aláíró tanúsítvány kifejezésbe beleértjük a szervezetek bélyegző tanúsítványát is.

Megemlítendő, hogy a különböző hitelesítés-szolgáltatók egymáshoz képest esetenként különböző néven nevezik az azonos célú tanúsítványokat, a hitelesítés-szolgáltatók ismertetői és ügyfélszolgálati tájékoztatói segítségével könnyű ezek között eligazodni.

Összességében a célnak, a kínálatnak és a felhasználónak legmegfelelőbb aláíró tanúsítványt érdemes és kell beszerezni. Nem rendeltetésszerű használatnak jogi következményei lehetnek.

KIADÓI TANÚSÍTVÁNY

A tanúsítványokat kibocsátó szervezetek a kiállított tanúsítványok hitelességét azok elektronikus aláírásával biztosítják. Ezeket a kibocsátó aláíró tanúsítványokat kiadói tanúsítványoknak nevezik. A KRA-ban aláírásra azok az aláíró tanúsítványok használhatók, melyek kiadói szerepelnek a KRA > Súgó > Rendszer információ > Digitális aláíráshoz regisztrált kiadói tanúsítványok > Közbenső szintű hitelesítésszolgáltatók tanúsítványai listában! Amennyiben igény merül fel más európai megbízható hitelesítésszolgáltató aláíró tanúsítványának használatára, úgy arra az NMHH KRA ügyfélszolgálatával történt egyeztetést követően nyílik lehetőség.
(*Megjegyzés*: Kizárólag az NMHH megbízásából történő KRA fejlesztésre néhány teszt kiadó is engedélyezésre került. Teszt aláíró tanúsítvány szolgáltatói használatát nem engedélyezzük.)

ALÁÍRÓ TANÚSÍTVÁNY CSERÉJE

A fentiekből következik, hogy fontos, ha a felhasználó aláíró tanúsítványa megújítás vagy új tanúsítvány készíttetés miatt megváltozik, akkor azt a KRA ügyfélszolgálatánál a szolgáltató kapcsolattartójának legalább e-mailben jeleznie kell, a *Felhasználói adatok módosítása* adatlapon található adattartalommal.

A közölt adatok alapján a KRA ügyfélszolgálata az elektronikus aláírást kibocsátó hitelesítés szolgáltató tanúsítványtárából letölti a felhasználó által használni kívánt tanúsítványt, és a KRA felhasználóhoz rendeli.

A hozzárendelés során az aláíró tanúsítványban szereplő adatok és magának a tanúsítványnak a Base64 kódolású ITU-T X.509 formátumú állománya kerül rögzítésre a KRA-ban.

3.3 A rendszer oldali tanúsítványok beszerzése

A webhelyek (KRA oldalak) azonosítására szolgáló tanúsítványokat, a KRA által küldött válaszüzenetek, nyugták és listák aláírásához szükséges tanúsítványokat és a kódaláíró tanúsítványt az **NMHH szerzi be**, így az NMHH gondoskodik megújításukról és cseréjükről is. Cseréjük előtt, a csere pontos időpontjáról és szolgáltatókat érintő minden olyan adatról, mely a folyamatos KRA használathoz szükséges **a szolgáltatókat körlevélben értesíti**.

4 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).

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.

5 A TANÚSÍTVÁNYOK TÁROLÁSA

A szolgáltató tulajdonába kerülő hozzáférési és aláíró tanúsítványok és a hozzájuk tartozó jelszavak biztonságos tárolásáról a szolgáltatónak – a saját biztonságpolitikai megfontolásai és a különböző tanúsítványkiadók által felkínált lehetőségek alapján – döntést kell hoznia, annak érdekében, hogy azok illetéktelen kézbe ne kerülhessenek, illetve ha megsérülnek vagy megsemmisülnek, esetleges reprodukciójuk lehetséges legyen.

Általánosságban igaz, hogy jogszerűen csak az használhat egy tanúsítványt a magánkulcsával együtt, akinek a nevére kiállításra került. Ez lehet egy szervezet is, ekkor a szervezet illetékese dönti el, mely alkalmazottjai számára tesz hozzáférhetővé egy tanúsítványt és az opcionálisan hozzá tartozó jelszót.

Ha egy tanúsítvány és a magánkulcs illetéktelen kézbe kerül, vagy helyrehozhatatlanul megsérül, akkor azt a kiadójánál jelezni kell, aki ennek hatására visszavonási listára helyezi azt. A KRA a magyarországi kiadók visszavonási listáit figyeli, így az azokon megjelenő tanúsítványokkal végzett műveleteket nem tekinti hitelesnek, a műveletet végző felhasználót üzenetben értesíti erről a tanúsítványhasználati hibáról.

Tanúsítvány és kulcspár – legyen az bármilyen hordozón – biztonságos kezelésével kapcsolatos tudnivalókról a hitelesítés szolgáltatók tájékoztatóiban további fontos ismeretekhez lehet jutni.

A különböző tárolási lehetőségek eltérő biztonságú megoldásokat jelentenek.

5.1 Tanúsítványok intelligens kártyán

Az egyik legbiztonságosabb módszer, ha a felhasználó kulcs-párja (kulcs-párjai) intelligens kártyán (idegen szóval SmartCard vagy chipkártya) kerül generálásra, mert ekkor a magánkulcsból csak egy létezik és az kizárólag a kártyát birtoklónál van, a magánkulcsot az eszközből kimásolni semmilyen módon sem lehet. Ebben az esetben a kártya használatához **kártyaolvasóra is szükség van**. A kártyán lévő tanúsítványok használatához jelszavas védelem is tartozik. A kártyaolvasó és a kártyán lévő tanúsítvány használatához szükséges telepítő szoftverekről és használati útmutatókról a kibocsátó ad részletes felvilágosítást.

Ha a szolgáltató döntése az, hogy egy felhasználójának minden tanúsítványát kártyán kívánja tárolni, akkor **először az aláíró tanúsítványt kell beszereznie**, mert ekkor tudja ugyanerre a kártyára az NMHH is a hozzáférési tanúsítványokat kiállítani. A **kártyát a hitelesítés szolgáltató adja**, kártyaolvasó is beszerezhető náluk. Az NMHH jogállásából következik, hogy nem folytathat kereskedelmi tevékenységet, így nem tud a felhasználó részére kártyát biztosítani.

Fontos tisztázni, hogy a kiválasztott hitelesítés szolgáltató által kibocsátandó kártyára lehet-e az NMHH-nak további kulcspárokat és tanúsítványokat generálnia, van-e rajta elegendő hely legalább 2db 2048 bit hosszúságú kulcs-pár és tanúsítvány (a KRA és a teszt rendszer hozzáférési tanúsítványai) számára. Kártya választása esetén, a kártyára történő újabb kulcspár létrehozása előtt át kell adni a kártyát védő jelszót („PIN” kódot) is! Ekkor a szolgáltató köteles gondoskodni a kártyán már meglévő bizalmas adatok megfelelő kezeléséről, azaz kártyán lévő tanúsítvány érvényességének felfüggesztéséről az azt kibocsátó hitelesítés szolgáltatónál.

Ha az az igény, hogy a tanúsítványok több intelligens kártyán legyenek, előzőleg mindenképp fel kell mérni az ebből fakadó előnyöket és kényelmetlenséget, valamint azt, hogy a használni kívánt operációs rendszer képes-e szükség esetén egyszerre több kártyaolvasót is kezelni!

5.2 Tanúsítványok CD-n

Lehetőség van a kulcs-pár és tanúsítvány kiadására valamilyen egyéb hordozón is, pl. CD-n. Ekkor a kiadott tanúsítványt általában – a hozzáférési tanúsítványokat mindenképp – a használt **operációs rendszer tanúsítványtárába vagy a KRA használatára alkalmas böngészőbe kell vagy célszerű telepíteni**. A CD-n lévő tanúsítványok telepítéséhez **jelszó szükséges**. A böngészőbe telepített tanúsítvány használatához egyéb eszközre nincs szükség. A böngészőkbe általában úgy is telepíthető egy tanúsítvány, hogy teljes körű használata mellett onnan a magán kulcs másolhatósága tiltva legyen.

Egyes esetekben a CD-n kiadott kulcspár és tanúsítvány intelligens kártyára is másolható, de ez nem ad akkora biztonságot, mintha a kulcspár magán az intelligens kártyán került volna generálásra!

5.3 Tanúsítványok a MS Windows operációs rendszer vagy egy böngésző tanúsítványtárában

A hitelesítésszolgáltatók leggyakrabban használt eljárása szerint a kulcs-pár és **a tanúsítvány a felhasználó számítógépének memóriájában keletkezik** egy tanúsítvány tárból elérhető helyen. Ebben az esetben megfontolandó, hogy a felhasználó a tanúsítványról és a kulcs-párról együtt (!) egy biztonsági másolatot készítsen (exportálás a tanúsítványtárból pfx vagy p12 kiterjesztésű fájlba). Az exportálás során a tanúsítványhoz és a hozzá tartozó magánkulcsot is tartalmazó fájlhoz jelszó is rendelhető.

Egyes esetekben a számítógép memóriájából a tanúsítványok intelligens kártyára is másolhatók, de ez nem ad akkora biztonságot, mintha a kulcspár az intelligens kártyán került volna generálásra!

5.4 Tanúsítványok egyéb eszközökön

Léteznek további kulcstároló eszközök is, például úgynevezett tokenek vagy más speciális biztonsági berendezések, melyeket összefoglaló néven Biztonságos Elektronikus Aláírás Létrehozó Eszközöknek (BALE) nevezik. A KRA-val kapcsolatban a webes felhasználói oldalon ritkábban fordulnak elő az intelligens kártyán és a tokeneken kívül más BALE-k, használatukról és alkalmazhatóságukról a hitelesítés szolgáltatóknál, illetve a KRA ügyfélszolgálatánál lehet tájékozódni. SOAP interfészt használó szolgáltatók által használt BALE-val kapcsolatban nincs megkötés, azon kívül, hogy pontosan a KRA Műszaki leírásaiban specifikált aláírás létrehozására alkalmas legyen és az elvárt védelmet biztosítsa a tulajdonos kriptográfiai magánkulcsának.

5.5 Tanúsítványok többféle eszközön

Annak sincs akadálya, hogy a felhasználó egyes tanúsítványait kártyán, másokat a számítógépe valamelyik tanúsítvány tárában tárolja. Ebben az esetben az előzőekben leírtakat kombináltan kell alkalmazni.

6 TANÚSÍTVÁNYOK TELEPÍTÉSE

A tanúsítványok telepítésére egyrészt azért van szükség, mert előfordulhat, hogy a hitelesítés szolgáltató által kibocsátott tanúsítvány nem olyan formátumban kerül tulajdonosa birtokába, ahogyan az közvetlenül használható lehet, vagy használni célszerű.

Másrészt a különböző célú hitelesítések akkor lesznek biztonságosak és zökkenőmentesek, ha az ezekhez használni kívánt összes tanúsítvány és kiadói tanúsítványaik is telepítésre kerülnek.

A SOAP kommunikációt használó szolgáltatók egyedi fejlesztései egyedi telepítési lépéseket igényelhetnek, így az alábbiaknak elsősorban a webes felhasználók vehetik hasznát.

A tanúsítványok kezelése során a használt számítógépes rendszer biztonsági elemeihez kell hozzáférni, így előfordulhat, hogy rendszergazdai jogosultsággal kell rendelkezni a műveletek végrehajtásához.

6.1 Saját tanúsítványok telepítése

A KRA teljes körű használatához a felhasználónak rendelkezésére kell, hogy álljanak saját tanúsítványai, az autentikációs és aláíró tanúsítványai, azaz a tanúsítványok és a kulcspárok egyaránt. Korábban már említettük, ha ezek a kulcspárok a kártyán kerültek generálásra, akkor ezek a tanúsítványok, mint személyes tanúsítványok nem telepíthetők, de nincs is rá szükség, mert ezek közvetlenül használhatók a KRA-ban. Ebben az esetben nem a tanúsítványok telepítésére van vagy lehet szükség, hanem a kártyahasználatot lehetővé tevő kártyaolvasó és a konkrét kártyát felismerő segédprogram (általában dll kiterjesztésű állomány) futtatására, melyre még kitérünk.

Azt is említettük már, hogy, ha a tanúsítványokat a tulajdonos internet böngészője által elérhető tanúsítvány tárán keresztül kapta meg, akkor sincs feltétlenül szükség további telepítésre. Ebben az esetben azonban nagyon ajánlott ezekről a tanúsítványokról egy biztonsági másolatot készíteni, és a másolatokat olyan külső helyen tárolni, mely a felhasználó számítógépének bármilyen meghibásodása esetén is hozzáférhető marad. Mindig ügyelni kell azonban arra, hogy a kulcspár és a tanúsítvány a hozzá tartozó jelszóval együtt ne kerülhessen illetéktelen kezekbe!

Megjegyzés:

> Ha pl. a MS Internet Explorer tanúsítvány exportáló varázslójának a Személyes kulcs exportálása oldalán nem lehet kiválasztani az „Igen, a személyes kulcs exportálását választom” lehetőséget, az azt jelentheti, hogy nem közvetlenül az exportálást végző számítógépére került letöltésre a hitelesítés szolgáltatótól a tanúsítvány, vagy arra úgy került telepítésre a tanúsítvány, hogy nem engedélyezték a személyes kulcs exportálását. Ebben az esetben forduljunk segítségért ahhoz a személyhez, aki az aláíró tanúsítványt a számítógépre telepítette.

Előre bocsátjuk, hogy az elektronikus aláírás KRA weboldalakon keresztüli teljes körű használata csak akkor lehetséges, ha a használt internet böngésző program képes Java kisalkalmazások futtatására. Jelenleg csak kettő ilyen széles körben használt böngésző ismeretes (Microsoft – Internet Explorer, Mozilla – Firefox), így példáinkban csak e két böngészőt említjük.

6.1.1 Saját tanúsítvány fájlok telepítése az MS Windows tanúsítványtárába

Feltételezzük, hogy a telepítendő fájl (pfx vagy p12 típusok) és a hozzá tartozó jelszó rendelkezésre áll. Jellemzően ez az eset, amikor az NMHH által CD-n kiadott hozzáférési tanúsítványt szeretnénk használatba venni.

A telepítés lépései:

> Tanúsítványfájl kiválasztása > PFX telepítése … majd kövessük a Tanúsítvány Importáló Varázsló utasításait, a lépések során válasszuk „A tanúsítvány típusának megfelelő tanúsítványtároló automatikus választása” lehetőséget. A telepítés közben felkínált egyéb lehetőségek kiválasztása előtt ajánlott tájékozódni legalább a Varázsló által felkínált „További tudnivalók a titkos kulcsok védelméről” helyen.

6.1.2 Saját tanúsítvány fájlok telepítése a Mozilla Firefox tanúsítványtárába

A telepítés lépései:

> Mozilla Firefox > Eszközök > Beállítások > Speciális > Tanúsítványok > Tanúsítványkezelő > Saját tanúsítványok lap > Importálás. Ezt követően válasszuk ki az importálandó fájlt, adjuk meg a jelszavát.

6.2 Nem saját tanúsítvány fájlok telepítése

Említettük már, hogy a tanúsítványhasználat akkor lesz biztonságos és zökkenőmentes, ha a használni kívánt tanúsítványok és kiadói tanúsítványaik is telepítésre kerülnek. Ez egyaránt vonatkozik a saját tanúsítványok kiadóira és a számhordozási rendszer által használt tanúsítványok kiadóira egyaránt.

A hitelesítés-szolgáltatóktól vásárolt saját tanúsítványok kiadói tanúsítványai a hitelesítés szolgáltatók szolgáltatói tanúsítványtáraiban megtalálhatók. Az NMHH számhordozási rendszerében a rendszer oldal által használt aktuális tanúsítványokat és kiadóikat az NMHH közzéteszi az nmhh.hu > NMHH a szakmáért > Azonosítógazdálkodás > Számhordozás (KRA) > KRA tájékoztató anyagok > Központi Referencia Adatbázis (KRA) – Tanúsítványtár helyen és a KRA > Súgó > Tanúsítványtár > KRA tanúsítványok és kiadóik helyen, vagy közvetlenül letölthetők a

> https://kra.nmhh.hu/lists/archivum/kiadoi_tanusitvanytar

oldalról. A KRA-ban használt tanúsítványok hierarchikus rendjét a következő ábra mutatja.

A fenti helyeken található kiadói tanúsítványok (cer vagy crt típusok) az adott weboldal kialakításától és böngészőtől függően közvetlenül telepíthetők, vagy mentést követően a következő lépésekkel telepíthetők importálással, ha ez korábban még nem történt meg más okból:

MS Internet Explorer böngésző használata esetén:

> Eszközök > Internetbeállítások > Tartalom > Tanúsítványok > Importálás… majd kövessük a Tanúsítványmportáló varázsló utasításait, a lépések során válasszuk a „A tanúsítvány típusának megfelelő tanúsítványtároló automatikus választása” lehetőséget..

Előfordulhat, hogy egy legfelső szintű tanúsítvány a fenti módszerrel nem telepíthető, ekkor használjuk az MS Windows Microsoft Management Console (MMC) alkalmazását. A telepítési lépések a Windows súgójában megtalálhatók.

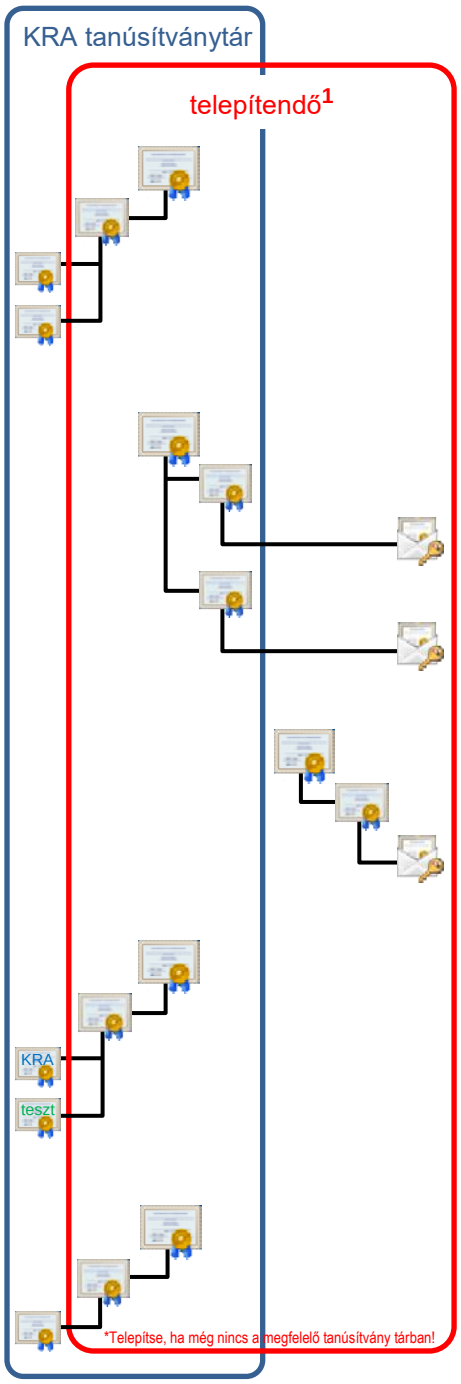
Mozilla – Firefox böngésző használata esetén:

> Mozilla Firefox > Eszközök > Beállítások > Speciális > Tanúsítványok > Tanúsítványkezelő > Hitelesítésszolgáltatók lap > Importálás… > A „Válassza ki a fájlt, melyben az importálandó CA-tanúsítvány van” lapon tallózzuk a tanúsítványt > A „Tanúsítvány letöltése” lapon jelöljük be az összes jelölő négyzetet > OK

Ha ezeket a telepítéseket kihagyjuk, könnyen megeshet, hogy a tanúsítvány kezelőnk bizonyos tanúsítványokat megbízhatatlannak fog tekinteni és esetleg nem engedélyezi majd az ehhez kapcsolódó elemek használatát!

KRA-ban használt tanúsítványok és kiadóik

tanúsítvány láncok, nevek, sorozatszámok és érvényességi idők.



Tulajdonos neve	sorozatszám	érvényesség
KRA WEBOLDALAK SSL TANÚSÍTVÁNYAI		
NetLock Arany (Class Gold) Főtanúsítvány	49412ce40010	2028-12-06
NetLock Üzleti (Class B) Tanúsítványkiadó	49412ce40014	2024-06-24
kra.nmhh.hu	5ae1f18f05ac7248ef913d55159f	2021-10-09
kra.nmhh-test.hu	5ae1f18f05ab6829d3fdfa7ed8bb	2021-10-09
FELHASZNÁLÓI HOZZÁFÉRÉSI TANÚSÍTVÁNYOK		
NMHH Legfelső Hitelesítés-szolgáltató IIe	7a5b5f6ad70a0425	2036-02-21
NMHH KRA CA IIe	5346e29f8a7555e9	2031-06-13
Felhasználó neve a KRA rendszerben		***Kiállítástól 3 év***
NMHH KRA Test CA	0a4f402bdd93b193	2031-06-13
Felhasználó neve a teszt rendszerben		***Kiállítástól 3 év***
FELHASZNÁLÓI ALÁÍRÓ TANÚSÍTVÁNYOK		
Hitelesítésszolgáltató főtanúsítványa [2]		
Hitelesítésszolgáltató kiadói tanúsítványa [2]		
Szolgáltató vagy természetes személy [3]		***Kiállítástól 1-2 év***
KRA OLDALI ALÁÍRÓ TANÚSÍTVÁNYOK		
KGYHSZ (Public Administration Root CA - Hungary)	437c92a4	2029-12-10
Minősített Közigazgatási Tanúsítványkiadó - GOV CA	437c9841	2024-03-20
Nemzeti Média- és Hírközlési Hatóság	74aaa1309ddf2ceb	2022-06-08
Nemzeti Média- és Hírközlési Hatóság	7a18fc459d981db	2022-06-08
JAVA APPLET KÓDALÁÍRÓ TANÚSÍTVÁNY, KRA ÉS TESZT		
USERTrust RSA Certification Authority	01fd6d30fca3ca51a81bbc640e35032d	2038-01-19
Sectigo RSA Code Signing CA	1da248306f9b2618d082e0967d33d36a	2031-01-01
Nemzeti Média- és Hírközlési Hatóság	00d761abfa822106df4eb796decb6bc41f	2023-11-18

[1] Felhasználó által telepítendő, ha még nincs a megfelelő tanúsítvány tárban!

[2] Annak a hitelesítésszolgáltatónak a tanúsítványai ahonnan az aláíró tanúsítványok beszerzésre kerültek. Általában eSzignó vagy Netlock vagy más európai hitelesítésszolgáltatóé, amelyik szerepel az EU megbízható hitelesítés szolgáltatók listájában.

[3] A szolgáltatói felhasználók kivétel nélkül ugyan azt az aláíró tanúsítványt használják a KRA-ban és a teszt rendszerben.

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

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

A tanúsítványokban szereplő nevekre (CN=) nincs megkötés, azon kívül, hogy ez nem hiányozhat, továbbá a nevekben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve, az UTF-8 kódolásban kell kezelni.

7.1 Az aláíró tanúsítványok használatának további feltételei a web felületi környezetben

A web felületet használó felhasználónak a KRA-val történő munkavégzés során a tanúsítványok használata igen egyszerű, mindössze ki kell választania az adott munkafázisban a megfelelő tanúsítványt és ha kell, megadnia a tanúsítványhoz tartozó jelszót (ld. KRA WEB felhasználói kézikönyv).

A felhasználó jogosultságának ellenőrzését majd a weboldalon megadott adatokból készült xml üzenet létrehozását és az elektronikus aláírásának bonyolult folyamatát a KRA végzi egy kisalkalmazás (KRAXmlSigner) segítségével. Azonban ahhoz, hogy ez a kisalkalmazás működni tudjon – a programsorai futni tudjanak – be kell állítani az úgynevezett futtató környezetét.

7.1.1 Java futtatókörnyezet telepítése és beállítása

A KRA futtatható MS Internet Explorer 11+ vagy Mozilla Firefox 45…52 böngésző alatt illetve minden olyan böngésző segítségével, mely támogatja Java programozási nyelven készült kisalkalmazások (Java applet) futtatását. (A Mozilla Firefox 52-nél újabb változatok már nem kezelik a Java kisalkalmazásokat, így nem használhatók.)

A kisalkalmazás futtatásának lehetőségét egy Java futtatókörnyezet (Java Runtime Environment – JRE) teremti meg, **így 32 bites változatának telepítése szükséges a web böngészőt futtató számítógépre, még akkor is, ha az operációs rendszer 64 bites**, amennyiben az még nem történt meg más okból.

Ellenőrzés Windows operációs rendszer esetén:

> Start > Vezérlőpult > Java > Java Control Panel > General lap > About…: Itt megtekinthető a telepített változat sorozat és frissítés száma. A javasolt érték legalább: Version 7 Update 51.

Amennyiben nem található a felhasználó számítógépén ez a program, akkor ezt az alábbi helyről letölthető megfelelő változatú program futtatásával lehet telepíteni:

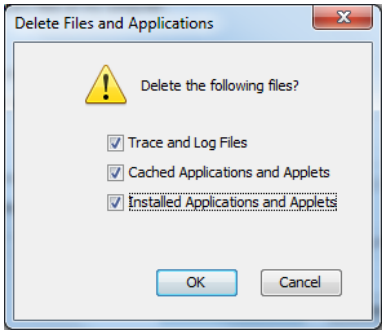
https://java.com/en/download/

A fenti oldalon válasszuk a „Java Download” lehetőséget, majd az „Agree and Start Free Download” opciót!

Ha egyéb függőség miatt a legújabb változat nem telepíthető, akkor kövesse az ORACLE corporation következő oldalán található utasításokat:
https://www.java.com/en/download/help/windows_manual_download.xml#download.
(Tapasztalataink szerint két különböző JRE-t is lehet telepíteni egy számítógépre, de előfordulhat, hogy mégis a frissebb változat alatt fog futni a Java kisalkalmazásunk, még akkor is, ha a Java Control Panel > Java lap > View > Java Runtime Enviroment Settings oldalán a régebbi változatot jelöljük csak be.)

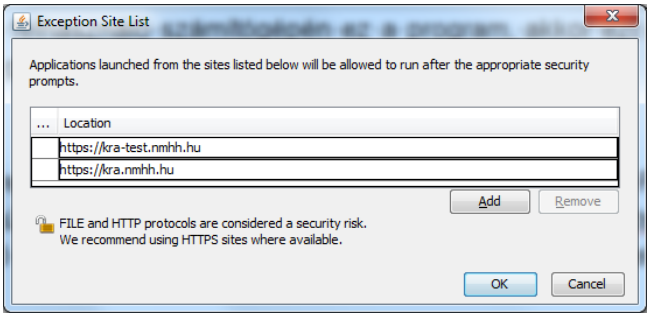
További beállítások:

- Ha a felhasználó számítógépén korábban már futott JRE, akkor első lépésként javasoljuk a Java átmeneti tároló (cache) ürítését:
  Java Control Panel > General lap > Settings > Delete Files > Delete Files and Applications ablakon jelöljünk be minden lehetőséget > OK > OK:

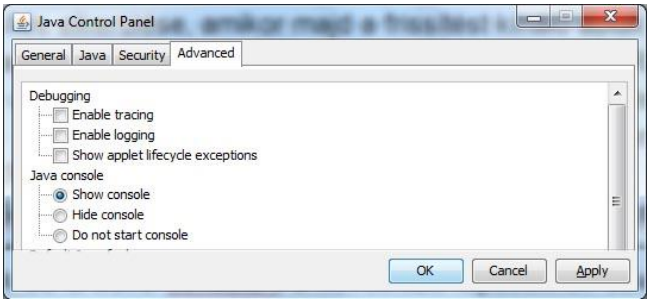


- A Java Control Panel > Security lapján a High lehetőséget kell kiválasztani vagy más változat esetén a biztonsági csúszkát alsó állásba kell helyezni (Medium). Ezen beállítás mellett lehetséges a JRE frissítés elkerülése, amikor majd a frissítést kínáló ablak megjelenésekor a „Later” lehetőséget választjuk. (Ha a Java futtatókörnyezet fejlesztője, az ORACLE Corporation új változatot bocsát ki a JRE-ből, akkor az NMHH megvizsgálja annak és a KRAXmlSigner kisalkalmazásnak az együttműködését. Hibás együttműködés esetén a tennivalókról körlevélben értesíti a KRA felhasználókat.)

- Java Control Panel > Security lap > Edit Site List gombra kattintás > Exeption Site List lapon: Add > Kattintás az üres mezőre és a következő url bemásolása: https://kra.nmhh.hu Enter > Add > https://kra-test.nmhh.hu Enter > OK



- Kapcsoljuk be a Java console-t a következő lépésekkel:
  Java Control Panel > Advanced lap > Java console részében a „Show console" lehetőséget választjuk.

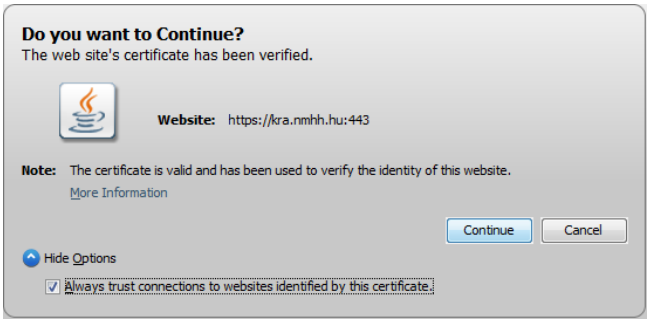


Nyissuk meg a KRA vagy a teszt rendszer oldalát!
(A böngésző címsorába írjuk be a https://kra.nmhh.hu vagy a https://kra-test.nmhh.hu címet és a felugró ablakban válasszuk ki a megnyitandó oldalhoz tartozó autentikációs tanúsítványt.
JRE változattól függően, vagy ha a felhasználó proxy szerveren keresztül kapcsolódik a számhordozási rendszerhez, akkor beállítástól függően előfordulhat, hogy többször is ki kell választani a belépés során a rendszerhez történő hozzáférést lehetővé tevő tanúsítványt! (Tehát nem a vásárolt aláíró tanúsítványt, hanem azt, amelyet az NMHH bocsátott a felhasználó részére.))

Nemsokára felugrik a Java console ablaka, melynek első soraiban olvasható az aktuálisan futó JRE változat, majd ha minden rendben történik, akkor ezt követően sokféle üzenet jelenik meg a Java console-on melyekkel nem kell foglalkozni, végül a következő sorok:

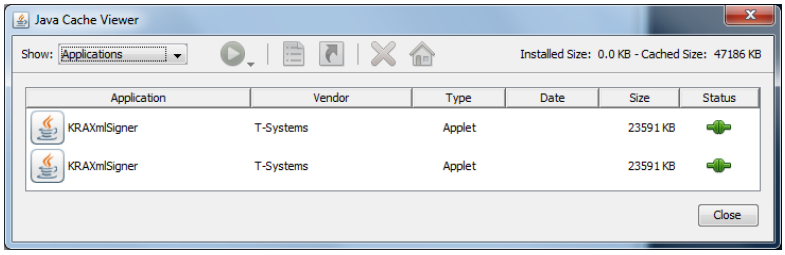
INFO – Applet initizalized.
DEBUG – start ….

Ameddig a fenti Java consol üzenetekre várunk az esetlegesen megjelenő ablakban engedélyezzük a folytatást a Continue gombra kattintva:



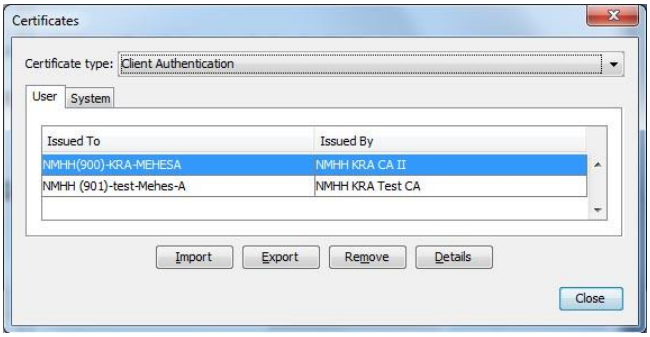
Az első sikeres belépés során a felhasználó gépére egyszer le kell, hogy töltődjenek a KRA-hoz és a teszt rendszerhez tartozó KRAXmlSigner fájlok, melyek végleges változatai azonosak (Vendor: T-Systems, vagy NMHH, a Size (méret) eltérhet az alábbi ábrán láthatótól. A teszt rendszerhez tartozó fájl csak akkor töltődik le, ha a felhasználó belép a teszt rendszerbe is.)
KRAXmlSigner fájlok sikeres letöltését a Java Control Panel megfelelő oldalán lehet ellenőrizni:

Java Control Panel > General lap > View… > Java Cashe Viewer, Show: Applications



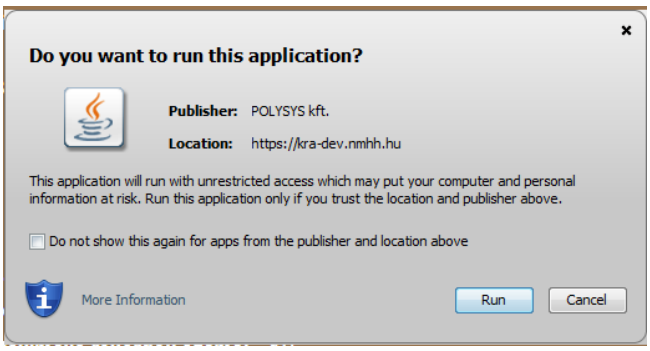
Amennyiben a KRAXmlSigner nem töltődne le, vagy nem futna, akkor a fenti beállításokon túl a következőket kell tenni:

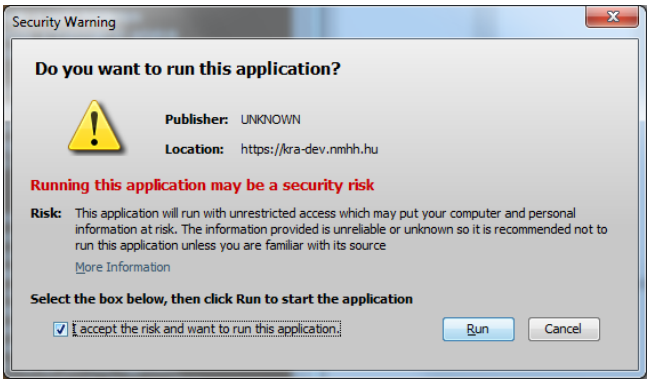
Java Control Panel > Security lap > Manage Certificates… > Certificate type: Client Authentication > User lap > Import (az NMHH által kiadott felhasználói tanúsítvány a CD-ről, vagy onnan, ahová biztonsági másolat készült róla, vagy onnan ahova a Windows tanúsítványtárából került korábban exportálva, pfx vagy p12 fájlba a személyes kulccsal együtt):



Ha a KRA weboldalának megjelenés után felugrik egy java ablak: Authetication Required, itt a fenti importálásnál megadott jelszót várja a Java.

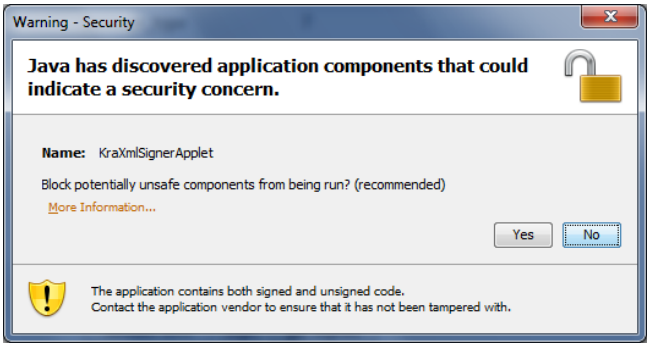
Ha nem sikerült minden tanúsítványt telepíteni, vagy a böngészőnek különleges biztonsági beállításai vannak, akkor Windows operációs rendszerben egy figyelmeztető ablak jelenhet meg:





Fogadjuk el a figyelmeztetést: „I accept..” kezdetű sorban, majd a helyes válasz ebben az esetben: „Run”

A böngésző, illetve a telepített Java futtatókörnyezet változatától függően esetleg előfordulhat, hogy a KRAXmlSigner kisalkalmazás egyik összetevője biztonsági figyelmeztetéseket generál:



A helyes válasz ebben az esetben: „No”!

Ha azt szeretnénk, hogy ez utóbbi figyelmeztetés többet ne jelenjen meg, akkor tegyük a következőt:

> Java Control Panel > Advanced lap> Mixed code (sandboxed vs. trusted) security verification:
> Itt válasszuk az: „Enable – hide warning and run with protections” lehetőséget!

Figyelem! Ez a beállítás minden más Java kisalkalmazás futására is vonatkozik. A beállítással kapcsolatban további tudnivalók találhatóak a http://download.oracle.com/javase/6/docs/technotes/guides/jweb/mixed_code.html *oldalon.*

Egy tranzakció aláírása előtt) mindenképp meg kell várni a „DEBUG – start ….” **sor megjelenését a Java console ablakában, illetve azt, hogy a „BETÖLTÉS…” gomb felirata „Aláír és elküld” –re váltson!**

Ha az említett sorok néhány perc várakozást követően sem jelennek meg, akkor egy hibaüzenet jelenik meg a tennivalókkal. Ha a Java console ablakában üzenet jelent meg, kérjük, hogy másolják le és e-mail-ben küldjék el a kra-hiba@nmhh.hu címre.

Hibátlan működés esetén nincs szükség a Java console további megjelenítésére, mivel a működésre nincs hatással, csak ellenőrzési célra van, így akár ki is kapcsolható. (Java Control Panel > Advanced lap > Java console részében a „Hide console” választása.)

Megjegyzés Linux operációs rendszert használók részére:

Egyes Linux disztribúciók (pl. Ubuntu) alapértelmezetten nem az Oracle Java verzióját használják, mely a kisalkalmazás hibás vagy működésképtelenségét okozhatja. Ubuntu esetén 10.04 változatnál újabbak esetén a következő lépések segítségével lehet telepíteni az Oracle Java futtató környezetet: https://help.ubuntu.com/community/Java#Oracle_Java_7

7.1.2 Kártyaolvasóval és kártyával kapcsolatos futtatókörnyezet ellenőrzése és beállítása

Amennyiben a felhasználó az aláíró tanúsítványát kártyán vagy más biztonsági eszközön (pl. USB Token) tárolja, akkor az ezek működéséhez szükséges fájlokat is telepítenie kellett. 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**
ActivCard Gold	acpkcs.dll
Aladdin e-Token	eTpkcs11.dll
Aladdin e-Token PRO	
Axalto	xltCk.dll
Axalto Cyberflex Access 64K v2a	
eToken PRO Java Card 72K	
Gemalto Classic V3 GemP15-1	gclib.dll
Gemalto Cryptoflex .NET	gtop11dotnet.dll
Gemalto IDClassic 340	
Giesecke	htaetfix.dll
Giesecke & Devrient token	
Giesecke SmartSign	hthlkfix.dll
Giesecke SmartSign (ht)	htsspk11.dll
nChiper NetHSM 2000	
Oberthur	OCSCryptolib_P11.dll
Oberthur AuthentIC	OCSCryptoki.dll
Oberthur CosmopolIC intelligens kártya	
Oberthur ID One	AuCryptoki2-0.dll
OpenSmartCard	opensc-pkcs11.dll
ORGA intelligens kártya	
ORGA Micardo	MicardoPKCS11.dll
Rainbow CryptoSwift HSM	iveacryptoki.dll
Rainbow iKey 2000	dkck201.dll
Rainbow iKey 3000	aetpkss1.dll
Schlumberger Cyberflex	slbck.dll
SUN Crypto Accelerator	

Ha a kártyaolvasó működik, de a kívánt dll nem található, akkor a dll helye megadható a Java kisalkalmazás részére.

Ehhez egy hordozási tranzakció végzése során, az *Aláír és elküld* gombra kattintva, a megjelenő KRA Digitális Aláírás ablakon válasszuk a Beállítások > Kártyaolvasó telepítése lehetőséget, majd adjuk meg a dll helyét, mely általában a C:\Program files könyvtárban keresendő, illetve a kártyát és a kártyaolvasót

rendelkezésre bocsátótól tudható meg. A dll-t csak egyszer kell megadni, a kisalkalmazás megjegyzi azt, amennyiben a sütik engedélyezve vannak.

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

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

7.2 Az aláíró tanúsítványok használatának további feltételei a SOAP kommunikációs környezetben

A SOAP interfészen keresztül kommunikáló szolgáltatónak úgy kell elkészítenie alkalmazását, mely a következőkben leírásra kerülő előírásoknak is megfelel. A számhordozási rendszer által készített aláírások is megfelelnek ezeknek az előírásoknak. Ez biztosítja az elektronikus aláíráshoz kötött számhordozási eljárásokban az együttműködés helyességét az aláíró és az aláírás-ellenőrző felek között, beleértve a harmadik felekkel (hitelesítés szolgáltatókkal) kapcsolatos szabályokat is.

7.3 Alkalmazható algoritmusok

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

7.4 A KRA-ban kezelt aláírási formátum

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

Az XML üzenetek aláírása a World Wide Web Consortium (W3C) által specifikált szintaktika és feldolgozás szerint lehetséges csak. 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
- W3C TR Canonical XML

A KRA az XML formátum mellett előállítja az irányítási listákat – a delta listát kivéve – CSV formátumban is, melyeket úgynevezett ASiCe konténerbe csomagol. Ennek részletei a következő

specifikációban találhatók:

- ETSI TS 102 918 Electronic Signatures and Infrastructures (ESI) - Associated Signature Containers (ASiC)

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.

8 KRA ALÁÍRÁS ELLENŐRZÉSI ÉS LÉTREHOZÁSI ELJÁRÁSOK

A szolgáltatói felhasználók által készített aláírások ellenőrzéséhez KRA nyilvántartja a felhasználói aláíró tanúsítványokat, és az azokhoz tartozó kiadói láncok tanúsítványait.

Az aláírás létrehozása a KRA WEB felhasználói kézikönyvben vagy a KRA SOAP felhasználói kézikönyvben leírt eljárással kell, hogy történjék. WEB felület használata esetén maga az oldal „mögötti" kódsorok alakítják át az egyes tranzakcióknál bevitt adatokat aláírt XML üzenetté, pontosan olyanná, mint amilyent a SOAP felhasználóknak kell készíteniük. Végeredményben a szolgáltatók tranzakciói a KRA rendszerbe egységes XML formátumban, a korábban meghatározott XML aláírással érkeznek.

8.1 A KRA aláírás ellenőrzési folyamata

- Az üzenet struktúrájának az ellenőrzése,
- Aláíró tanúsítvány kiadójának ellenőrzése az érvényességi lánc felépítésével,
- Aláíró tanúsítvány érvényességének ellenőrzése,
- XML tartalom megfelelősségének ellenőrzése a SOAP felhasználói kézikönyvben leírtak szerint,
- Az aláíró jogosultságának ellenőrzése a KRA-ban kezelt jogosultsági adatok, és az aláíró-tanúsítvány felhasználásával,
- Integritás ellenőrzése az XML aláírás előírásai szerint,
    - A megfelelő integritású üzenetek archiválása.

8.2 A KRA aláírás létrehozási folyamata

- Válasz üzenet (üzenet, nyugta, hibaüzenet, lista) tartalmi összeállítása
    - XML tartalom specifikáció szerinti összeállítása
- Aláíró tanúsítvány ellenőrzése
- XMLDsig (http://www.w3.org/TR/xmldsig-core/) szerinti aláírás elkészítése

MELLÉKLET

M1 Internet hivatkozások gyűjteménye

Számhordozási rendszerek

KRA rendszer: https://kra.nmhh.hu/

KRA listakönyvtár: https://kra.nmhh.hu/lists/

teszt rendszer: https://kra-test.nmhh.hu/

teszt rendszer listakönyvtár: https://kra-test.nmhh.hu/lists/

NMHH weboldalai http://nmhh.hu

Azonosítógazdálkodás

Azonosítógazdálkodási nyilvántartás

Számhordozás

KRA műszaki leírások

KRA Általános ismertető

KRA WEB felhasználói kézikönyv

KRA SOAP felhasználói kézikönyv

KRA Elektronikus aláírási kézikönyv

KRA ügyfélszolgálati eljárások

Szolgáltató kódok listája (XLSX) (CSV)

Időablakok

Számmezőátadás lista

KRA továbbfejlesztés

Számhordozottság tudakozó

Tájékoztató a számmezőátadás műszaki megvalósításáról

KRA-ban használható aláírás kibocsátó szolgáltatók

Microsec e-Szignó

Netlock

Más Európai Uniós tagállam hitelesítés szolgáltatója által kibocsátott tanúsítvány használatának igénye esetén keresse a KRA ügyfélszolgálatot.

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

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.