Gazdasági Fejlesztési Minisztérium
Kommunikációs és Információ Technológiai Intézet

Informatikai Biztonsági Tanúsítási Szervezet

Országos rendszer az ICT rendszerek és termékek biztonságának értékelésére és tanúsítására
(2003. október 30-i Minisztertanács Elnöki Rendelet –
2004. április 27-i 93. sz. Jogi Közlöny)
Az Európai Parlament és a Tanács elektronikus aláírásról szóló 1999/93/EK Irányelvének 3. szakasz 4. bekezdése értelmében felhatalmazott szervezet, amely ugyanezen Irányelv 11. szakasz 1. bekezdés b) pontja értelmében kijelölésre került Olaszországban, mint elektronikus aláírásokat létrehozó eszköznek a hivatkozott irányelv III. Mellékletében foglalt biztonsági követelményeknek való megfelelőségének értékeléséért felelős hatóság.

Eljárás az Elektronikus Aláírásokat Létrehozó Eszköz az Európai Parlament és a Tanács 1999/93/EK Irányelvének III. Melléklete által meghatározott Biztonsági Követelményeknek való Megfelelőség Értékelésére

2/14. sz. Megfelelőségi Tanúsítvány

Berendezés: **CoSign v7.1**

Fejlesztő: **ARX**

A jelen tanúsítványban megjelölt elektronikus aláírásokat létrehozó eszköz megfelel az Európai Parlament és a Tanács1999/93/EK Irányelvének III. Melléklete által meghatározott Biztonsági Követelményeknek.

Igazgató
(dr. Rita FORSI)
[olvashatatlan aláírás]

Első kiadás: 2014. szeptember 30.
Módosítás: 2015. július 23.
A jelen Megfelelőségi Tanúsítványt az Informatikai Biztonsági Tanúsítási Szervezet (OCSI) bocsátotta ki a 2005. március 7-i 82. sz., „Digitális adminisztrációs kódról” szóló Törvényerejű Rendelet 35. szakasz 5. bekezdése értelmében, amelyet kiegészítettek és módosítottak a 2010. december 30-i 235. sz. Törvényerejű Rendelettel.
A jelen Megfelelőségi Tanúsítvány érvényessége a Tanúsítványhoz mellékelt Értékelési Jelentésben (OCSI/ACC/SFNT/01/2010/RA) foglalt feltételektől és követelményektől függ, amely a tanúsítvány szerves és lényeges részét képezi.

NYILATKOZAT
A KFI Fordítóiroda ezúton igazolja, hogy Goják Éva szakfordító (L-285/2007) által végzett magyar nyelvű fordítás tartalmában és formájában megegyezik az olasz nyelvű eredetivel.
Budapest, 2015.09.02.

A jelen oldal szándékosan maradt üres.

NYILATKOZAT

A KFI Fordítóiroda ezúton igazolja, hogy Goják Éva szakfordító (L-285/2007) által végzett magyar nyelvű fordítás tartalmában és formájában megegyezik az olasz nyelvű eredetivel.
Budapest, 2015.09.02.

Gazdasági fejlesztési Minisztérium
Kommunikációs és Információ Technológiai Intézet

Informatikai Biztonsági Tanúsítási Szervezet

Eljárás az Elektronikus Aláírásokat létrehozó eszköz az Európai Parlament és a Tanács 1999/93/EK Irányelvének III. Melléklete által meghatározott Biztonsági Követelményeknek való Megfelelőség Értékelésére

Értékelési Jelentés

ARX CoSign v7.1

OCSI/ACC/ARX/01/2010/RA

1.1 verzió

2015. július 23.

NYILATKOZAT
A KFI Fordítóiroda ezúton igazolja, hogy Goják Éva szakfordító (L-285/2007) által végzett magyar nyelvű fordítás tartalmában és formájában megegyezik az olasz nyelvű eredetivel.
Budapest, 2015.09.02.

A jelen oldal szándékosan maradt üres.

NYILATKOZAT

A KFI Fordítóiroda ezúton igazolja, hogy Goják Éva szakfordító (L-285/2007) által végzett magyar nyelvű fordítás tartalmában és formájában megegyezik az olasz nyelvű eredetivel.
Budapest, 2015.09.02.

1 Dokumentum felülvizsgálatai

Verzió	Szerző	Módosítás	Dátum
1.0	OCSI (Informatikai Biztonsági Tanúsítási Szervezet)	Első kiadás	2014/09/30
1.1	OCSI	Módosítás	2015/07/23

NYILATKOZAT

A KFI Fordítóiroda ezúton igazolja, hogy Goják Éva szakfordító (L-285/2007) által végzett magyar nyelvű fordítás tartalmában és formájában megegyezik az olasz nyelvű eredetivel.
Budapest, 2015.09.02.

2 Tartalomjegyzék

1 Dokumentum felülvizsgálatai 5

2 Tartalomjegyzék 6

3 Mozaikszavak listája 7

4 Hivatkozások 8

5 Megfelelőség Értékelésének hatóköre 9

6 Értékelés összegzése 10

6.1 Bevezetés 10

6.2 Értékelés összefoglaló leírása 11

6.3 Értékelt eszköz leírása 11

7 Megfelelőségi Tanúsítvány érvényességének feltételei 14

8 Értékelt eszköz használati feltételei 15

3 Mozaikszavak listája

CC	Common Criteria
DL	Törvényerejű Rendelet
DPCM	Minisztertanács Elnöki Rendelet
EAL	Biztonsági Szint Értékelés (Evaluation Assurance Level)
OCSI	Informatikai Biztonsági Tanúsítási Szervezet
ODV	Értékelés Tárgya
PP	Védelmi Profil (Protection Profile)
SSCD	Biztonságos Aláírás Létrehozó Eszköz (Secure Signature Creation Device)
TDS	Biztonsági Követelmény (Security Target)
TLS	Transport Layer Security titkosítási protokoll

NYILATKOZAT

A KFI Fordítóiroda ezúton igazolja, hogy Goják Éva szakfordító (L-285/2007) által végzett magyar nyelvű fordítás tartalmában és formájában megegyezik az olasz nyelvű eredetivel.
Budapest, 2015.09.02.

4 Hivatkozások

[CAD] 2005. március 7-i 82. sz. Törvényerejű Rendelet, 2005. május 16-i 112. sz. Jogi Közlöny, 93. sz. Általános Kiegészítés: „Digitális adminisztrációs kód”, amelyet a 2010. december 30-i 235. sz. Törvényerejű Rendelettel, és a 2010. január 10-i 6. sz. Jogi Közlöny 8. sz. Általános kiegészítésével módosítottak és egészítettek ki.

[CD] A Bizottság 2003. július 14-i 2003/511/EK Határozata az Európai Parlament és a Tanács 1999/93/EK Irányelvének megfelelő elektronikus aláírásra vonatkozó általános szabályozások hivatkozási számaira vonatkozóan, 2003. július 15-i 175. sz. Jogi Közlöny

[DEL] „CNIPA (Közigazgatási Informatikai Rendszerek Országos Központja) 2009. május 21-i 45. sz. Határozata, amelyet a DigitPA 2010. július 28-i 69. sz. Határozatával módosítottak”, 2010. augusztus 17-i 191. sz. Jogi Közlöny.

[DIR] „Európai Parlament és a Tanács 1999. december 13-i, elektronikus aláírásról szóló 1999/93/EK Irányelve”, 2000. január 19-i 13. sz. Jogi Közlöny.

[DPCM] 2010. február 10-i Minisztertanács Elnöki Rendelet, 2010. április 28-i 98. sz. Jogi Közlöny: „Azon eljárás meghatározása, amely felhatalmazást ad a saját részről kiadott igazolásra az elektronikus aláírást automatikusan létrehozó eszközök biztonsági követelményeknek való megfelelőségére vonatkozóan”.

[DS] „Információs Dokumentum az Elektronikus Aláírás Létrehozó Eszköz azon Biztonsági Követelményeknek való Értékelési Eljárásához, amelyeket az 1999/93/EK Irányelv III. Melléklete tartalmaz: OCSI/ACC/02/201/DDS, 1.0 verzió, 2010. november 2.

[PR] „Eljárás az Elektronikus Aláírás Létrehozó Eszköz Európai Parlament és a Tanács 1999/93/EK Irányelvének III. Melléklete által meghatározott Biztonsági Követelményeknek való Megfelelőség Értékelésére”, OCSI/ACC/01/2010/PROC, 1.0 verzió, 2010. november 2.

[RC] Tanúsítási Jelentés, „ARX CoSign v.7.1”, OCSI/CERT/IMQ/01/2011/RC, 1.1 verzió, 2015. július 23.

[RT] „Fokozott biztonságú, minősített és digitális elektronikus aláírások létrehozására, elhelyezésére és ellenőrzésére vonatkozó műszaki szabályok”, 2013. február 22-i Minisztertanács Elnöki Rendelet, 2013. május 21-i 117. sz. Jogi Közlöny.

[TDS] ARX CoSign Security Target (Biztonsági Követelmény), 1.19. verzió, 2015. június 15.

5 Megfelelőség Értékelésének hatóköre

Az OCSI (Informatikai Biztonsági Tanúsítási Szervezet) az Európai Parlament és a Tanács elektronikus aláírásról szóló 1999/93/EK Irányelvének 3. szakasz 4. bekezdése értelmében (továbbiakban: Irányelv) [DIR] felhatalmazott szervezet, és ugyanezen Irányelv 11. szakasz 1. bekezdés b) pontja értelmében kijelölésre került Olaszországban, mint egy aláírást létrehozó eszköznek a hivatkozott irányelv III. Mellékletében foglalt biztonsági követelményeknek való megfelelőségének értékeléséért felelős hatóság.

Az OCSI (Informatikai Biztonsági Tanúsítási Szervezet) értékelési feladatáról a 2005. március 7-i 82. sz., „Digitális adminisztrációs kódról" szóló Törvényerejű Rendelet 35. szakasz 5. bekezdése rendelkezik, amelyet kiegészítettek és módosítottak a 2010. december 30-i 235. sz. Törvényerejű Rendelettel [CAD].

A Megfelelőségi Értékelés tárgya a „CoSign v7.1" elnevezésű eszköz, amit az ARX gyárt (továbbiakban: CoSign vagy „értékelés tárgyát képező eszköz" vagy egyszerűen „eszköz").

Az eszközre vonatkozóan az Értékelési Eljárás kezdeti időpontjában alkalmazásra került (lásd 6.2 pont) a 2010. február 10-i Minisztertanács Elnöki Rendelet: „Azon eljárás meghatározása, amely felhatalmazást ad a saját részről kiadott igazolásra az elektronikus aláírást automatikusan létrehozó eszközök biztonsági követelményeknek való megfelelőségére vonatkozóan" [DPCM].

Ezen túlmenően az Eszköz Megfelelőségének Értékelésénél nem alkalmazható a 2003/511/EK Európai Határozat [CD], amely az Európai Parlament és a Tanács 1999/83/EK Irányelv III. Mellékletében [DIR] foglalt biztonsági követelmények kielégítésére vonatkozik.

6 Értékelés összegzése

6.1 Bevezetés

A jelen Értékelési Jelentés az ARX által gyártott „CoSign v7.1” elnevezésű eszköznél alkalmazott Megfelelőségi Értékelési folyamat eredményeit tartalmazza, és az a célja, hogy információkkal szolgáljon a nevezett eszköz potenciális vevői és használói részére, illetve hogy igazolja, hogy az eszköz megfelel a minősített elektronikus aláírások (automatikus és távolról történő) létrehozására alkalmas biztonságos eszközökre vonatkozó, érvényben levő jogszabályok által előírt követelményeknek.

Az Értékelést az OCSI (Informatikai Biztonsági Tanúsítási Szervezet) végezte az „Eljárás az Elektronikus Aláírás Létrehozó Eszköz Európai Parlament és a Tanács 1999/93/EK Irányelvének III. Melléklete által meghatározott Biztonsági Követelményeknek való Megfelelőség Értékelésére”, OCSI/ACC/01/2010/PROC, 1.0 verzió, 2010. november 2. [PR] (továbbiakban: Eljárás), illetve az „Információs Dokumentum az Elektronikus Aláírás Létrehozó Eszköz azon Biztonsági Követelményeknek való Értékelési Eljárásához, amelyeket az 1999/93/EK Irányelv III. Melléklete tartalmaz, OCSI/ACC/02/201/DDS, 1.0 verzió, 2010. november 2. [DS] (továbbiakban: Információs Dokumentum) szerint.

Különösképpen, miután az Értékelési Eljárás elindításakor még nem állt rendelkezésre a Common Criteria Tanúsítvány, és nem is indították el a vonatkozó Tanúsítási Eljárást, a 2. sz. Módszer szerinti eljárás került alkalmazásra. Emiatt az első szakaszban az OCSI (Informatikai Biztonsági Tanúsítási Szervezet) megvizsgálta az eszköz Biztonsági Követelményét, és kiadta a Megfelelőségét Elfogadó Nyilatkozatot 2010. szeptember 13. napján.

2011. október 31. napján elindították, szintén az OCSI-nál (Informatikai Biztonsági Tanúsítási Szervezet) a CC értékelési és tanúsítási eljárást: az LVS által végzett értékelési tevékenységek pozitív eredménnyel zárultak 2014. június 25. napján, ugyanakkor a Tanúsítási Jelentést és a vonatkozó CC Tanúsítványt az OCSI (Informatikai Biztonsági Tanúsítási Szervezet) 2014. szeptember 10. napján adta ki.

Miután az ARX Fejlesztő cég kicserélte a véletlenszám generáló hardver chipjét, szükségessé vált az ODV újraértékelése az LVS részéről, mely cég a korábbi értékelés eredményeit is megerősítette.

Ezért az OCSI ((Informatikai Biztonsági Tanúsítási Szervezet) intézkedett a Tanúsítási Jelentés felülvizsgálatáról és ezt követően 2015. július 23-ai dátummal kibocsájtotta jelen Megfelelőségi Tanúsítvány módosított változatát.

Kérjük figyelembe venni, hogy a végrehajtott módosítás maga után vonta a (Biztonsági Követelmény) TDS felülvizsgálatát. Az ODV korábbi verziójának használóit kérjük az új (Biztonsági Követelmény) TDS áttanulmányozására.

Az értékelés tárgyát képező eszköz, mint ahogy az leírásra kerül a vonatkozó Biztonsági Követelményben [TDS], megfelel a hivatkozott Irányelv III. Mellékletében foglalt biztonsági követelményeknek, illetve más megfelelőségi követelményeknek az Eljárásban kifejezett Értékelés szerint, illetve a minősített elektronikus aláírások (automatikus és távolról történő) elhelyezésére vonatkozó biztonságos eszközökről szóló, hatályban levő jogszabályok által előírt követelményeknek.

A jelen Értékelési Jelentést a Biztonsági Követelménnyel [TDS] együtt kell tanulmányozni, amely utóbbi meghatározza a funkcionális és garanciális követelményeket, illetve a használati környezetet, illetve figyelembe kell venni a Tanúsítási Jelentést [RC].

Az Értékelés tárgyát képező eszközre kiadott Megfelelőségi Tanúsítvány érvényessége a jelen Értékelési Jelentésben foglalt feltételek és elvek (lásd 7. fejezet) betartásához kötött, amely ezáltal a Tanúsítvány szerves és lényeges részét képezi.

A Megfelelőségi tanúsítvány OCSI (Informatikai Biztonsági Tanúsítási Szervezet) részéről történő kiadása nem jelent semmiféle támogatást vagy promóciót a Szervezet részéről az értékelt eszköz használatára vonatkozóan.

6.2 Értékelés összefoglaló leírása

Értékelést kérő vállalat	ARX
Eszköz neve	CoSign
Eszköz verzió	7.1
Biztonsági Követelmény	ARX CoSign Security Target, 1.19 verzió, 2015. június 15.
Garancia szint	EAL4 kiegészítve AVA_VAN.5-tel
CC (Common Criteria) verzió	3.1, 2. Felülvizsgálat
PP-megfelelőség (Protection Profile)	Nincs semmi bejelentett megfelelőség
Eljárás kezdetének időpontja	2010. február 26.
Értékelés kezdetének időpontja	2011. október 31.
Értékelés befejezésének időpontja	2014. június 25.
Újraértékelés kezdetének időpontja	2015. június 15.
Újraértékelés befejezésének időpontja	2015. július 15.
CC Tanúsítvány kiadásának időpontja	2014. szeptember 10.
Eljárás befejezésének időpontja	2014. szeptember 30.
CC tanúsítvány módosításának időpontja	2015. július 23.
Értékelés módosításának időpontja	2015. július 23.

6.3 Értékelt eszköz leírása

A „CoSign v7.1” eszközt (továbbiakban egyszerűen CoSign) arra tervezték, hogy „Biztonságos Aláírás Létrehozó Eszközként (Secure Signature Creating Device, SSCD)” kerüljön felhasználásra egy szervezetnél, fizikailag telepítésre kerüljön egy biztonságos környezetbe a szervezet adatközpontjába, és csatlakozzon ugyanazon szervezet informatikai hálózatára.

A tanúsított eszköz (ODV) egy fizikai berendezésből és különböző szoftver modulokból áll, amelyek biztosítják a felhasználó számára, hogy távolról csatlakozzon az eszközre és aláírási műveleteket hajtson végre. A CoSign eszközhöz való hozzáférés a CoSign ügyfél (kliens) alkalmazáson keresztül lehetséges, amelyet a végfelhasználó munkaállomásán telepítenek, és amely lehetővé teszi egy TLS session létrehozását az ügyfél és a berendezés között. A CoSign eszközhöz egy REST interfésszel (Representational State Transfer) is lehet csatlakozni egy REST alapú kliens alkalmazás révén, amely lehetővé teszi az Aláíró felhasználó részére, hogy ugyanazokat a műveleteket végezze el mint a CoSign kliens alkalmazáson keresztül, továbbra is egy TLS kapcsolat felhasználásával. A továbbiakban minden CoSign kliensre történő hivatkozást REST alapú kliensre történő hivatkozásként is értelmezni kell.

Egyetlen eszköz biztonságosan tud kezelni több felhasználót és minden felhasználói fiókhoz létre lehet hozni különböző aláírási kulcsokat és hozzátartozó tanúsítványokat.

Három különböző típusú felhasználó számára engedélyezett az ODV-n való eljárás: egyszerű felhasználói (Aláíró), illetve két különböző adminisztrációs felhasználói profil:

- Appliance Administrator: telepíti az eszközt és irányítja a működését;
- Users Administrator: kezeli a felhasználók fiókjait.

Minden egyes Aláíró felhasználó rendelkezésére bocsátanak egy OTP (One Time Password) eszközt, amelyet egyértelműen azonosítottak és egyértelműen egy használóhoz rendeltek. Az aláíró hitelesítése egy statikus jelszó és egy – az OTP eszköz kijelzőjén megjelenő – dinamikus jelszó megadása alapján történik. Amikor a felhasználó szándékában áll elektronikusan aláírni egy okiratot, a CoSign kliens létrehoz egy védett felhasználó session-t, felhasználva az erre a célra létrehozott biztonságos kommunikációs csatornát a TLS 1.0 protokollon keresztül. Ez a biztonságos csatorna kerül felhasználásra minden, a CoSign kliens és a CoSign eszköz közötti kommunikáció során.

A CoSign egy ciklikus audit log-ban rögzíti az összes adminisztrációs tevékenységet és a felhasználó bármely aláírási kulcsának minden egyes használatát. Az audit log nem törölhető és csak az erre felhatalmazással rendelkező adminisztrátor olvashatja el.

Az ODV által nyújtott biztonsági funkciók a következők:

- Hozzáférés ellenőrzése
- Azonosítás és hitelesítés
- Kriptográfiai műveletek
- Biztonsági audit
- Biztonságos kommunikáció és session kezelés
- Támadási kísérletek észlelése
- Ön-teszt

Az ODV tulajdonságaira és a biztonságpolitikára vonatkozó részletesebb információkért olvassa el a Biztonsági Követelmény [TDS] és a Tanúsítási Jelentés [RC] dokumentumokat.

NYILATKOZAT

A KFI Fordítóiroda ezúton igazolja, hogy Goják Éva szakfordító (L-285/2007) által végzett magyar nyelvű fordítás tartalmában és formájában megegyezik az olasz nyelvű eredetivel.
Budapest, 2015.09.02.

6.3.1 ODV értékelt konfigurációi

A CoSign eszköz Biztonsági Követelmény c. dokumentum két különböző, lehetséges konfigurációt mutat be:

1) PRIMARY-HIGH AVAILABILITY WITH KEY REPLICATION (HA-PRI-REPL-INC-SIGKEY)

2) ALTERNATE-HIGH AVAILABILITY WITH KEY REPLICATION (HA-ALT-REPL-INC-SIGKEY)

A két konfiguráció lehetővé teszi, hogy az ODV-t **Magas fokú rendelkezésre állásban, az aláíró magánkulcsainak replikációjával** használják: az operatív környezetben csak egy PRIMARY eszköz kerül telepítésre HA-PRI-REPL-INC-SIGKEY konfigurációban, és egy vagy több ALTERNATE eszköz (HA-ALT-REPL-INC-SIGKEY) konfigurációban.

További információkért olvassa el a [TDS] 1.3.2. pontját.

7 Megfelelőségi Tanúsítvány érvényességének feltételei

Az Értékelés tárgyát képező eszközre kiadott Megfelelőségi Tanúsítvány kizárólag az alábbi feltételek teljesülése esetén érvényes és hatályos:

i. a kiadott Biztonsági Tanúsítvány (lásd [RC]) érvényes, azaz a Tanúsítványt nem vonták vissza;

ii. a felhasznált eszköz megfelel a TDS-ben tanúsított és leírt eszköznek;

iii. az eszköz üzemeltetési környezete megfelel a TDS-ben leírt környezetnek;

iv. a jelen értékelési Jelentés 8. pontjában felsorolt - az eszköz használatára vonatkozó - valamennyi kiegészítő feltételt betartják.

Az (i) feltétel megsértése a Megfelelőségi Tanúsítvány érvényességének elvesztését vonja maga után.

A (ii), (iii) és (iv) feltételek bármelyikének nem teljesülése a Megfelelőségi Tanúsítvány hatályának elvesztését vonja maga után, ugyanakkor a Tanúsítvány érvényessége megmarad.

A jelen Megfelelőségi tanúsítvány érvényességének elvesztését eredményező bármilyen körülmény – akár közvetlenül a kibocsátó Tanúsító Szervezet (OCSI) által kerül megállapításra, akár egyéb felek hozzák ezt a szervezet tudomására – a Tanúsító Szervezet hivatalos kommunikációs csatornáján keresztül kerül kihirdetésre az érintett felek részére.

Amennyiben a jelen tanúsítvány hatályának elvesztését eredményező körülmény merül fel, a minősített elektronikus aláírást szolgáltatók felügyeletét ellátó hatóság köteles meghozni a szükséges korrigáló intézkedéseket.

8 Értékelt eszköz használati feltételei

A CoSign eszközt a Biztonsági Követelmények [TDS] és a Tanúsítási Jelentés [TR] c. dokumentumokban foglalt összes előírást betartva kell használni.

Különösképpen az ODV átadását, biztonságos telepítését és az operatív környezet biztonságos előkészítését kell elvégezni a [TDS]-ben foglalt biztonsági céloknak megfelelően, betartva az [RC] A. Melléklet 8. fejezetben foglalt utasításokat is.

Ezen túlmenően, ami az eszköz használatát illeti, az elektronikus aláírásról szóló, hatályos olasz rendelkezéseknek megfelelően felhívjuk a figyelmet arra, hogy különösképpen az alábbi aspektusokat kell figyelembe venni:

- **Kriptográfiai algoritmusok:** a lenyomatképző (hash) függvényekkel, a kriptográfiai kulcspárok létrehozásával és az aláírási módszerekkel kapcsolatban olvassa el a CNIPA (Közigazgatási Informatikai Rendszerek Országos Központja) 45/2009. sz. Határozatában foglaltakat, amelyet a 69/2010 sz. DigitPA Határozattal módosítottak [DEL].

- **Backup és aláíró kulcs visszaállítása:** miután lehetőség van arra, hogy az aláírást létrehozó eszközön kívülre exportálják a magánkulcsokat kizárólagosan helyreállítási célokkal a használt eszköz meghibásodása vagy frissítése miatt, illetve az exportált kulcsok megőrzésére vonatkozóan, győződjön meg arról, hogy betartják-e a „Fokozott biztonságú, minősített és digitális elektronikus aláírások létrehozására, kibocsátására és ellenőrzésére vonatkozó műszaki szabályok” által előírtakat ([RT] 8. szakasz. 3. bekezdés).

- **Magas fokú megbízhatósággal rendelkező konfiguráció:** azzal kapcsolatban, hogy az aláírást létrehozó eszköz magas megbízhatósággal rendelkező konfigurálására van lehetőség, amelyet a tanúsított konfiguráció ír le (lásd 6.3.1 pont), ellenőrizze, hogy betartották-e a fent hivatkozott műszaki szabályozások által előírtakat ([RT] 8. szakasz. 4. bekezdés).

Végül, figyelembe véve, hogy az elektronikus aláírásra vonatkozó, hivatkozott jogszabályok frissítésre és módosításra kerülnek az idő folyamán, azt tanácsoljuk, hogy kísérje figyelemmel ezeket, és mindig a fent hivatkozott dokumentumok és azok esetleges kiegészítéseinek legutolsó rendelkezésre álló verzióját vegyék figyelembe.