TANÚSÍTVÁNY

(I-NL20T1_TAN-SW) MELLÉKLETE

Dokumentumazonosító	**TAN-SW.ME-01**	
Projektazonosító	**I-NL20T1**	**Netlock Kft. által fejlesztett NCA TWS V2.11 Elektronikus aláírási rendszer tanúsítás 2020**
MATRIX tanúsítási igazgató	**Molnár Ádám**	
Kelt	**Budaörs, 2020. április 21.**	
 ……. MATRIX tanúsítási igazgató		

1. A TANÚSÍTÁS KÖRÜLMÉNYEI

A MATRIX Kft. a NAH-6-0054/2019/K számon a Nemzeti Akkreditáló Hatóság által akkreditált terméktanúsító szervezet.

A Netlock Kft. informatikai termékek fejlesztésével és forgalmazásával foglalkozó vállalkozás.

A Netlock Kft. az NCA TWS V2.11 Tanúsítvány kiadó, OCSP szolgáltató, kulcs helyreállító és időbélyegző rendszer dokumentációját a MATRIX Kft.-nek átadta.

A MATRIX Kft. az SW értékelése során a kötelező érvényű és az önként vállalt normatívák pontról pontra történő vizsgálatát végezte el.

2. AZ ÉRTÉKELÉS TÁRGYA

Megnevezés: Netlock CA Trustworthy System V2.11 Tanúsítvány kiadó, OCSP szolgáltató, kulcs helyreállító és időbélyegző rendszer.

2.1. ÉT azonosítása

Jellemző	Érték
ÉT megnevezése	NCA TWS
ÉT verzió	2.11.
Dátum	2020.04.11
Fejlesztő	Netlock Kft.
Termék típus	Tanúsítvány kiadó, OCSP szolgáltató, kulcs helyreállító és időbélyegző rendszer
Platform	Windows, Linux
CC verzió	Common Criteria version 3.1R3

PP megfelelés	EN 419261:2015 Security requirements for trustworthy systems managing certificates and time-stamps A PP csomag megfelelése: EAL4 augmented with assurance component ALC_FLR.3
ST megfelelés	Netlock CA Trustworthy System V2.11 biztonsági előirányzat

2.2. Az értékelés tárgyát képző dokumentációk

Típus	Tárgy	Verzió	Megjelenés
Szoftver	NCA TWS	2.11	Elektronikus
Dokumentum	Security Target NCA 2.11 EN419261 v2.2.pdfx	2.2	Elektronikus
Dokumentum	NCA_TDS-HLD_v2_1.pdf	2.1	Elektronikus
Dokumentum	NCA_TAT_v2_1_.pdf	2.1	Elektronikus
Dokumentum	NCA_IMP (TDS-ARC) v_2_.pdf	2.0	Elektronikus
Dokumentum	NCA_FSP_v2_2.pdf	2.2	Elektronikus
Dokumentum	NCA_ARC-LLD_v2_1.pdf	2.1	Elektronikus
Dokumentum	NCA TWS Telepítesi es adminisztracios utmutato_V3.2.pdf	3.2	Elektronikus
Dokumentum	NCA_TAT_v2_1.pdf	2.1	Elektronikus
Dokumentum	NCA_LCD_v2_0.pdf	2.0	Elektronikus
Dokumentum	NCA_FLR_v2_0.pdf	2.0	Elektronikus
Dokumentum	NCA_DVS_v2_0.pdf	2.0	Elektronikus
Dokumentum	NCA_CMS_V2_2.pdf	2.2	Elektronikus
Dokumentum	NCA_TAT_v2_1.pdf	2.1	Elektronikus
Dokumentum	NCA_LCD_v2_0	2.0	Elektronikus
Dokumentum	NCA_FLR_v2_0.pdf	2.0	Elektronikus
Dokumentum	NCA_DPT_v2_0.pdf	2.0	Elektronikus
Dokumentum	NCA_COV_v2_0.pdf	2.0	Elektronikus

2.3. A tanúsítás megrendelője

NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság

Székhely: 1101 Budapest, Expo tér 5-7.

Cégjegyzékszám: 01-09-563961

Adószám: 12201521-2-42

3. FUNKCIONÁLIS LEÍRÁS

Az TOE szoftver NCA olyan speciális elektronikus aláírási termék, amely különböző hitelesítés-szolgáltatást biztosító funkciókkal rendelkezik.

Az TOE a meghívó alkalmazásoktól szolgáltatási üzeneteket, parancsokat fogad, azokat (amennyiben erre szükség van) jogosultságellenőrzés alá veti, majd végrehajtja. Az alábbi hitelesítés-szolgáltatásokat támogatja:

Alap szolgáltatások (minden üzemmód része):

- regisztráció szolgáltatás,
- tanúsítvány előállítás szolgáltatás,
- tanúsítvány szétosztás szolgáltatás,
- visszavonás kezelés szolgáltatás (CRL, OCSP),
- visszavonás állapot szolgáltatás.

Kiegészítő szolgáltatások (egyes üzemmódok része):

- időbélyegzés szolgáltatás,
- titkosító magánkulcs letétbe helyezése szolgáltatás,
- titkosító magánkulcs helyreállítása szolgáltatás.

Az TOE a tanúsítvány kibocsátásra vonatkozó kérelmeket képes a konfigurációjában meghatározott ellenőrzések és folyamatvezérlési utasítások alapján emberi beavatkozás segítségével vagy anélkül végrehajtani. Képes kezelni a kérelmek, majd később tanúsítványok teljes életciklusát, a kérelem bejelentésétől (előkérelem), a kulcsgeneráláson, az ellenőrzött tanúsítványban szereplő adatok összeállításán (előtanúsítvány) keresztül, a tanúsítvány kiadásáig, valamint a tanúsítvány felfüggesztéséig, visszavonásáig.

Az életciklus különböző szakaszaiban a kezelőknek, vizsgálóknak, valamint a külvilágnak pontos információkat képes adni (pl. statisztikák, egyedi státuszok és információk) ember által (HTML lapok, elektronikus levelek), valamint gépek által értelmezhető formákban (pl. CRL, OCSP vagy akár egyedi protokollok).

4. MEGFELELŐSÉG

4.1. Megfelelőség a normatív dokumentumoknak

Az ÉT megfelel az alábbi követelményeknek:

4.1.1. Kötelezően betartandó normatívák

- - EN 419 261:2015 Security Requirements for trustworthy systems managing certificates and time-stamps
- - ISO/IEC 15408-1:2009 Informatika Biztonságtechnika Az informatikai biztonság értékelés szempontjai, 1. rész. ISO, 2009
- - ISO/IEC 15408-2:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés szempontjai, 2. rész. ISO, 2008
- - ISO/IEC 15408-3:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés szempontjai, 3. rész. ISO, 2008

4.1.1.1. A vizsgálat módszertana a következő normatíváknak megfelelő

- - ISO/IEC 18045:2008 Informatika Biztonságtechnika Az informatikai biztonság értékelés módszertana

4.1.2. Önként vállalt normatívák

- ETSI TS 119 101 V1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI) Policy and security requirements for applications for signature creation and signature validation

- Netlock CA Trustworthy System V2.11 biztonsági előirányzat

Az aláírási termék megfelel a fenti követelményeknek a 4.2 és a 4.3 pontban leírt biztonságos felhasználási és működési környezetben az alábbi feltételek teljesülése mellett:

A tanúsítás kizárólag a vizsgált rendszer aktuális verziójára vonatkozik, bárminemű változás esetén a módosított verzióra jelen tanúsítvány érvénytelen.

Nem képezi a tanúsítás tárgyát a program működési környezete így az:

- Operációs rendszer,

- a felhasznált külső szoftver modulok, illetve programok,

- a működéshez használt hardver elemek,

- standard PC szerver,

- HSM kártya, netHSM

- a biztonságos működéshez olyan HSM szükséges, amely rendelkezik a tanúsítvány kiadáshoz szükséges tanúsításokkal

- időbélyegzés szolgáltatáshoz megfelelő megbízható időforrás.

4.2. A biztonságos felhasználás feltételei

A tanúsítvány érvényessége a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesítésén múlik.

Az alábbi (biztonsági előirányzatban is szereplő) feltételezések az informatikai környezetre vonatkoznak:

Biztonsági célok a környezetre vonatkozóan

A csak a TOE környezetére vonatkozó biztonsági célok két csoportra oszthatók: informatikai és nem informatikai biztonsági célok.

A környezetre vonatkozó nem informatikai biztonsági célok

OE.Administrators, Operators, Officers and Auditors guidance documentation

Meg kell gátolni a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók hibáit azáltal, hogy megfelelő dokumentációt kell számukra biztosítani a TOE biztonságos konfigurálásához és üzemeltetéséhez.

OE.Auditors Review Audit Logs

A biztonság-kritikus eseményeket azonosítani és felügyelni kell, megkövetelve a rendszervizsgálóktól a naplóbejegyzések kellő (kockázatokkal arányban álló) gyakoriságú átvizsgálását.

OE.Authentication Data Management

A hitelesítési adat kezelésre vonatkozó szabályzat érvényre juttatásával biztosítani kell, hogy a felhasználók hitelesítési adataikat (jelszavaikat, aktivizáló kódjaikat) megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtassák.

OE.Communication Protection

A rendszert megfelelő fizikai biztonság biztosításával védeni kell a kommunikációs képességekre irányuló fizikai támadásokkal szemben.

OE.Competent Administrators, Operators, Officers and Auditors

Biztosítani kell a TOE megfelelő kezelését, hozzáértő és feljogosított rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók kijelölésével a TOE és az általa tartalmazott információk biztonságának kezelésére.

OE.Cooperative Users

Biztosítani kell, hogy a felhasználók együttműködőek legyenek néhány olyan feladat vagy feladatcsoport végrehajtásában, amelyek biztonságos IT környezetet, s a TOE által kezelt információkat igényelnek.

OE.CPS

Minden rendszeradminisztrátornak, rendszerüzemeltetőnek, tisztviselőnek és rendszervizsgálónak jól kell ismernie azt a hitelesítési rendet (CP) és szolgáltatási szabályzatot (CPS), mely alatt a TOE-t működtetik.

O(E).Cryptographic functions

Jóváhagyott kriptográfiai algoritmusokat kell megvalósítani a titkosításra/dekódolásra, hitelesítésre és aláírás létrehozására/ellenőrzésére, jóváhagyott kulcsgenerálási technikákat kell alkalmazni, valamint tanúsított kriptográfiai modulokat kell használni.

OE.Disposal of Authentication Data

Biztosítani kell a hitelesítési adatok és az ezekhez tartozó jogosultságok megfelelő eltávolítását, miután a hozzáférési jogosultság megszűnt (pl. munkahelyváltozás, vagy munkaköri felelősség megváltozása következtében).

OE.Installation

A TOE-ért felelős személyeknek biztosítaniuk kell, hogy a TOE olyan módon legyen szállítva, telepítve, kezelve és üzemeltetve, amely megőrzi az informatikai biztonságot.

OE.Lifecycle security

A fejlesztési fázisban olyan eszközöket és technikákat kell biztosítani, hogy használatukkal biztosítva legyen a biztonság TOE-ba tervezése. A működtetés során észlelni és javítani kell a hibákat.

OE.Malicious Code Not Signed

A TOE-t védeni kell a rosszindulatú kódokkal szemben, úgy, hogy a rendszerbe letöltött minden kódot aláír egy megbízható entitás.

OE.Notify Authorities of Security Issues

Értesíteni kell a megfelelő vezetőket a rendszert érintő bármely biztonsági eseményről, az adatvesztés vagy kompromittálódás lehetőségének minimalizálása érdekében.

OE.Physical Protection

A TOE-ért felelős személyeknek biztosítaniuk kell, hogy a TOE biztonságkritikus elemei védve legyenek az informatikai biztonságot veszélyeztető fizikai támadásokkal szemben.

OE.Repair identified security flaws

A gyártónak javítani kell a felhasználók által azonosított biztonsági hibákat.

O(E).Security roles

Biztonsági szerepköröket kell fenntartani, és kezelni kell a felhasználóknak ezen szerepkörökkel való társítását.

OE.Social Engineering Training

Az általános felhasználók, a rendszeradminisztrátorok, a rendszerüzemeltetők, a tisztviselők és a rendszervizsgálók számára képzést kell biztosítani a "social engineering" típusú támadások megakadályozási technikáira.

O.Sufficient backup storage and effective restoration

Elegendő mentés tárolást és hatékony visszaállítást kell biztosítani a rendszer újra felépíthetősége érdekében.

A környezetre vonatkozó informatikai biztonsági célok

OE.Operating System

A TOE IT környezete csak olyan operációs rendszert használhat, mely garantálja a TOE számára a tartomány szétválasztást és a biztonsági funkciók megkerülhetetlenségét.

OE.Periodically check integrity

Időszakosan ellenőrizni kell mind a rendszer, mind a szoftver sértetlenségét.

OE.Trusted Path

Megbízható útvonalat kell biztosítani a felhasználó és a rendszer között. Megbízható útvonalat kell biztosítani a biztonság-kritikus (TSF) adatok számára, aminek mindkét végpontja megbízhatóan azonosított.

OE.Validation of security function

Funkciók és eljárások alkalmazásával biztosítani kell, hogy a biztonság-kritikus szoftver, hardver és förmver elemek helyesen működnek.

Időbélyegzésre vonatkozó környezeti

OE.TSS

Az időbélyegző rendszer megfelel az ETSI EN 319 421 feltételeinek.

Továbbá a TOE biztonságosan védett behatolás ellen és cber támadások ellen.

A működési környezet biztonságos kommunikációs csatornát biztosít, mint pl. HTTPS és hasonlók és védi az információcserét a TOE és a külső entitások ellen.

OE.KEY_PAIR_GENERATION

Public Key/Private Key Pair Generation

A TSU kulcspárait (R.KEY_PAIR_PUB/R.KEY_PAIR_PRIV) jogszabály vagy hatósági ajánlás által jóváhagyott kriptográfiai algoritmusokat használva kell létrehozni.

OE.PRIVATE_KEY_MANAGEMENT

Secure Management of Private Key

A TOE környezete felel a konfidentalitásáért és integriátásért azR.KEY_PAIR_PRIV-nek.

Ebbe beleértett az R.KEY_PAIR_PRIV részben vagy egyészben közzé téve egy lokai interfészen keresztül. Konfidentalitási és integritási célokból a TOE környezet továbbá olyan biztonságos algoritmusokat kell használjon, amit jogszabály vagy hatósági ajánlás által jóváhagyott kriptográfiai algoritmusokat használva kell létrehozni

OE.PROTECT_ACCESS

Prevention of Unauthorised Physical Access

A TOE védett fizikai és szervezeti kontrollokal, amit a TOE környezet valósít meg. Ez továbbá védve az assetek közzétételétől is,

Ezek a kontrollok korlátozzák a fizikai hozzáférést (adminisztrációs célokra) és kettős kontrollt igényének.

A TOE-nak meg kell felelnie az ETSI EN 319 421 követelményeinek.

OE.PERSONNEL

Liability and Training

A személyzetnek, akinek hozzáférése van a TOE-hez jogi felelőssége van, és kötelezettségekkel rendelkezik szerepköréből adódóan.

A személyzetnek képzettnek kell lennie a TOE használatához.

OE.SECURE_INIT

Secure Initialisation Procedures

Eljárások és kotnrollok a TOE környezetben definiáltak és implementáltak, hogy biztosítsák a biztonságos beállítását és inicalizálását a TOE-nak a CSP rendszerén belül, megfelelve az uniós előírásoknak, amit a minősített bizalmi szolgáltatóknak kell követniük.

Ez tartalmazz a z kezdeti R.TSF_DATA konfigurációt, TSU konfigurációt és a TSU indítását bizalmi tisztviselő által.

A TSU inicailizálása során a bizalmi tisztviselőnek ellenőrizne kell, hogy au R.DATE_AND_TIME szinkronizál egy külső megbízható UTC időforráshoz.

OE.SECURE_OPER

Secure Operating Procedures

Eljárások és kotnrollok a TOE környezetben definiáltak és implementáltak, hogy biztosítsák a biztonságos működését a TOE-nak a CSP rendszerén belül, megfelelve az uniós előírásoknak amit a minősített bizalmi szolgáltatóknak kell követniük.

OE.TIMESTAMP_VERIFICATION

Time-stamp verification

A kérő ellenőrzi a megfelelősségét a válaszul kapott időbélyegnek, és biztosítja megőrzését, ha szükséges:

A kérő:

ellenőrzi az időbélyeg aláírását

ellenőrzi, hogy a hash amit kapott az időbélyegben egyezik azzal mait küldött a kérsében

OE.AUDIT_REVIEW

Audit review

A TOE auditorok ellenőrzik az audit nyomokat rendszeresen, és jelentik a incidenseket a megfelelő szervnek.

OE.CA

A tanúsítványkiadó, aki kiadja a tanúsítvány a TOE számára olyan szabályokat használ, ami megfelel a szolgáltatás CP/CPS-ének.

OE.CERTIFIED_CM

A TOE által használt kriptográfiai modul megfelel az ETSI EN 319 421 követelményeinek amik a következők

FIPS 140-2 level 3

EN 419221-5

fentiekkel ekvivalens jogszabály által engedélyezett (eIDAS Article 30.)

OE.SECURE_BACKUP Secure backup of private keys

3 The following documents may also be used:

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1,

Revision 4. CCMB-2012-09-002, September 2012.

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1,

Revision 4. CCMB-2012-09-003, September 2012.

Amennyiben a használt kriptográfiai modul lehetővé teszi a TSU privát kulcs exportálását, azt csak megfelelő bizalmi szerepkörrel (OE.PERSONNEL) lehet, kettős kontrollal, fizikailag biztonságos környezetben (lásd A.ACCESS_PROTECTED).

A végrehajtásra jogosult személyzet csak az lehet, aki erre kötelezett.

Minden a TSU-n kívül tárolt privát kulcs esetében a kriptográfiai modulnak biztosítania kell az integritást és a konfidentalitást az eszközön kívül.

Lejárat után a tanúsítványhoz kapcsolódó privát kulcsot, és minden mentését vagy elegendő mentés ahhoz, hogy ne lehessen használatba venni meg kell semmisíteni.

A TOE-ra és környezetére egyaránt vonatkozó biztonsági célok

O(E).Configuration Management

Konfiguráció kezelési tervet kell megvalósítani. A konfiguráció kezelést abból a célból kell alkalmazni, hogy biztosítva legyen a rendszer csatlakoztatások (szoftver, hardver és förmver) és komponensek (szoftver, hardver és förmver) beazonosítása, a konfigurációs adatok naplózása, valamint a konfiguráció tételekben történő változások ellenőrzése.

O(E).Data import/export

Az adatok formájában megjelenő értékeket védeni kell a TOE felé vagy a TOE-tól történő átvitel közben, ahol az átvitel akár egy közbeiktatott nem megbízható komponensen keresztül, akár közvetlenül az emberi felhasználókhoz/tól történik.

O(E).Detect modifications of firmware, software, and backup data

Sértetlenség védelmet kell biztosítani a förmverek, a szoftverek, valamint a mentett adatok megváltozásának észlelése érdekében.

O(E).Individual accountability and audit records

Egyéni felelősségrevonhatóságot kell biztosítani a naplózott események vonatkozásában. A naplóeseményeknek tartalmazniuk kell az alábbiakat: az esemény dátuma és időpontja, az eseményért felelős entitás.

O(E).Integrity protection of user data and software

Megfelelő sértetlenség védelmet kell biztosítani a felhasználói adatokra és a szoftverre.

O(E).Limitation of administrative access

Az adminisztratív funkciókat úgy kell megtervezni, hogy a rendszeradminisztrátorok, rendszerüzemeltetők, tisztviselők és rendszervizsgálók automatikusan ne rendelkezzenek hozzáféréssel a felhasználói objektumokhoz, a szükséges kivételeken kívül. Ellenőrizni kell a rendszeradminisztrátorok és rendszerüzemeltetők rendszerhez való hozzáférését, akik a rendszer hibák elhárítását, illetve új verziók telepítését végzik.

O(E).Maintain user attributes

Az egyéni felhasználókkal kapcsolatosan kezelni kell egy biztonsági tulajdonság együttest (amely tartalmazhat szerepkörhöz tartozást, hozzáférési privilégiumokat stb.). Ez kiegészíti a felhasználói azonosítót.

O(E).Manage behavior of security functions

Menedzsment funkciókat kell biztosítani a biztonsági mechanizmusok konfigurálására, működtetésére és kezelésére.

O(E).Object and data recovery free from malicious code

Egy rosszindulatú kód bejutása és károkozása után egy működőképes állapotba kell tudni visszaállni. Ennek az állapotnak mentesnek kell lennie az eredeti rosszindulatú programkódtól.

O(E).Procedures for preventing malicious code

A rosszindulatú programkódokat meggátoló beépített eljárásoknak és mechanizmusoknak kell létezniük.

O(E).Protect stored audit records

A naplórekordokat védeni kell a jogosulatlan hozzáféréssel, módosítással vagy törléssel szemben abból a célból, hogy biztosítva legyen a felelősségre vonhatóság a felhasználói tevékenységekért.

O(E).Protect user and TSF data during internal transfer

Biztosítani kell a rendszeren belül átvitt felhasználói és TSF adatok sértetlenségét.

O(E).React to detected attacks

Automatizált értesítést (vagy más reagálásokat) kell megvalósítani a TSF által felfedett támadások esetében a támadások azonosítása és elrettentése érdekében.

O(E).Require inspection for downloads

Meg kell követelni a letöltések/átvitelek felügyeletét.

O(E).Respond to possible loss of stored audit records

Amennyiben a napló eseménysor tároló területe megtelt vagy majdnem megtelt, a naplózható események korlátozásával meg kell akadályozni a naplórekordok lehetséges elvesztését.

O(E).Restrict actions before authentication

Korlátozni kell azokat a tevékenységeket, amelyeket egy felhasználó végrehajthat, mielőtt a TOE hitelesíti felhasználói azonosítóját.

O(E).Security-relevant configuration management

Kezelni és frissíteni kell a rendszer biztonsági szabályzatok adatait és érvényre juttató funkcióit, valamint a biztonság-kritikus konfigurációs adatokat annak biztosítása érdekében, hogy ezek konzisztensek legyenek a szervezeti biztonsági szabályzatokkal.

O(E).Time stamps

Pontos időpontot kell biztosítani az időfüggő hitelesítés-szolgáltatásokhoz, valamint a napló események sorrendjének ellenőrizhetőségéhez.

O(E).User authorization management

Kezelni és frissíteni kell a felhasználói jogosultság és privilégium adatokat annak biztosítása érdekében, hogy ezek konzisztensek legyenek a szervezeti biztonsági és személyzeti szabályzatokkal.

4.3. Működési környezet

A fenti megfelelőség feltétele az alábbi működési környezetre vonatkozó követelményrendszer teljesülése, amelynek betartása a felhasználó felelőssége.

4.3.1. Hardver és szoftver környezet

Az értékelt aláírási termék csak olyan működési környezetben használható hitelesítési szolgáltató, amelynek minden eleme kielégíti az általánosan elvárható biztonsági követelményeket, és együttesen egy megfelelően biztonságos informatikai rendszert hoznak létre. Az értékelésnek nem tárgya a környezet elemeinek vizsgálata, az itt megfogalmazott követelmények iránymutató jellegűek az alkalmazás megfelelő használatához.

4.3.2. A fizikai védelem

Az üzemeltetés során a fizikai védelem tekintetében az alábbi intézkedések betartásáról kell gondoskodni:

- Az aláírási termék használatát biztosító rendszer által tartalmazott hardver, szoftver és firmware elemeket megfelelően kell védeni az illetéktelen fizikai módosítások ellen.
- Az aláírási termék által használt kommunikációs csatornákat megfelelően védeni kell az illetéktelen fizikai módosítások ellen.
- Az aláírási termék által használt kommunikációs csatornákat megfelelő módon védeni kell az illetéktelen lehallgatás ellen. Lehallgatás alatt logika (pl.: kémprogramok) és fizikai (EMC) módszerekkel végzett adatgyűjtés értendő.

4.3.3. Szállítás és telepítés

A rendszer telepítésével kapcsolatos biztonsági előírások:

- A program telepítőkészletét nem módosítható biztonságos adathordozón kell a felhasználónak átadni. Az átadás-átvételt hitelt érdemlő módon igazolni kell az átadás pontos időpontjának rögzítésével. A felhasználók az internetről is letölthetik a terméket, ebben az esetben biztosítani kell számukra az ellenőrzési lehetőséget, hogy a program megbízható forrásból származik.
- A telepítést csak megfelelően előkészített, biztonságos környezetben szabad megkezdeni, a telepítési útmutatóban rögzített pontos lépések betartásával.
- A terméket ajánlott rendszeresen frissíteni az új verziókra.

4.3.4. Algoritmusok és kapcsolódó paraméterek

A rendszer csak a mindenkor érvényes szabályzásnak megfelelő algoritmusokkal és paraméterekkel használható. Az elektronikus aláíráshoz használható kriptográfiai algoritmusokat egységesen szabályozzák az Európai Unióban, aktuális információ az alábbi normatívákból nyerhető:

- Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms. ETSI TS102 176-1 V2.1.1 2011-07.

- ETSI, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices (ETSI TS102 176-2) V1.2.1. 2005-07.

- (ESI); Cryptographic Suites

A specifikációk rendszeresen megújításra kerülnek, ezért a felhasználónak folyamatosan figyelemmel kell kísérnie az elektronikus aláírás létrehozatalához használható kriptográfiai algoritmusokra vonatkozó normatívák változását, s az annak megfelelő algoritmusokat és paramétereket kell használnia.

4.4. Értékelési módszertan

Az értékelés nyelvezete az ISO/IEC 15408-ban meghatározott, az értékelés módszertanának alapját az ISO/IEC 15408 használt módszertani ajánlás képezi.

A tanúsítási eljárás során elvégzett, fejlesztőktől független értékelés az ISO/IEC 15408 szerinti EAL4 szint volt. Az EAL4 jelentős garancianövekedést jelent az EAL3-hoz képest azzal, hogy a biztonsági funkciók és mechanizmusok és/vagy eljárások vizsgálatának sokkal teljesebb lefedettségét követeli, ami bizonyos mértékű bizalmat teremt abban, hogy a fejlesztés során a TOE-t nem hamisítják meg.

4.5. Biztonsági garancia szint

A MATRIX Vizsgáló, Ellenőrző és Tanúsító Kft. igazolja, hogy az Netlock Kft. által kifejlesztett „NCA TWS V2.11 Tanúsítvány kiadó, OCSP szolgáltató, kulcs helyreállító és időbélyegző rendszer" megfelel a normatív dokumentumokban foglalt követelményeknek.

A megfelelés biztonsági garancia szintje az ISO/IEC 15408 értékelési rendszere szerinti EAL 4 + ALC_FLR.3 szint.

A megfelelőségre vonatkozó megállapítást a témakör biztonságát érintő jelentős tudományos felfedezés, illetve új verzió kiadása esetén felül kell vizsgálni.

4.6. Rövidítések

Rövidítés	Tartalom
BE	Biztonsági Előirányzat
CC	Common Criteria for Information Technology Security Evaluation- Az informatikai biztonság értékelésének közös szempontrendszere
ÉT	ÉT Értékelés Tárgya - az a termék, amelynek leírását és rendszertervét a BE (ST) tartalmazza
PP	Protection Profile – Védelmi profil
ST	Security target – Biztonsági Előirányzat
TOE	Target of Evaluation – az értékelés tárgya
VP	Védelmi profil – Protection Profile
OCSP	Online Certificate Status Protocol

Dokumentum vége