Tanúsítási Jelentés

CECE Software System v1.1.0

mint informatikai biztonsági funkciókat megvalósító szoftver termék

HUNG-TJ-15408-001-2022

Verzió:	1.0
Fájl:	HUNG-TJ-15408-001-2022_v10.pdf
Minősítés:	Nyilvános
Oldalak:	17

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2021.12.17.	A szerkezet felállítása
v0.8	2022.01.12.	Belső egyeztetésre kiadott verzió
v0.9	2022.01.13.	Külső egyeztetésre kiadott verzió
v1.0	2022.01.13.	Végleges verzió

A Tanúsítási Jelentést készítette:

Digitálisan aláírta:
Endrődi Zsolt Attila

dr. Szabó István
HUNGUARD Kft.
Tanúsítási divízió

Tartalom

I. Összefoglaló

I.1. A tanúsítás (és az értékelés, melyen a tanúsítás alapul) jellemzői

TOE név:	**CECE Software System v1.1.0**
TOE rövid neve:	CECE Software System v1.1.0
TOE verzió:	CECE Software System v1.1.0: CECE Drive Eraser v1.8.0-rc5 (computer application) CECE Android Eraser v1.5.0-rc3 (mobile application) CECE iOS Eraser v1.1.0-rc5 (computer application)
Fejlesztő:	Certus Software Zrt. (székhely: 1037 Budapest, Csillaghegyi út 13.)
Értékelő:	HUNGUARD Kft. Értékelési Divízió 1123 Budapest, Kékgolyó u. 6.
Értékelés befejezése:	2022. január 13.
Az értékelés módszere:	MSZ EN ISO/IEC 18045:2020
Az értékelés garanciaszintje:	EAL3

I.2. A tanúsítás tárgya

A tanúsítás tárgya a CECE Software System v1.1.0, amely az alábbi három komponensből áll:

- CECE Drive Eraser v1.8.0-rc5 (computer application)
- CECE Android Eraser v1.5.0-rc3 (mobile application)
- CECE iOS Eraser v1.1.0-rc5 (computer application)

I.2.1. A TOE szolgáltatásainak összefoglalása

A CECE Drive Eraser egy olyan szoftver, amely a számítógéphez csatlakoztatott tárolómeghajtókon tárolt adatok végleges törlésére szolgál. A terméket ISO-képfájlként szállítják, amelyet egy USB flash meghajtóra kell írni, azzal a céllal, hogy egy „bootolható” adathordozót hozzon létre, mely által egy saját, aktív operációs rendszerként fut, a célszámítógép RAM-jában.

A törlési eljárás megfelel az amerikai DoD 5220.22-M adattörlési szabványnak a HDD-meghajtók és USB flash meghajtók esetében, azaz minden szektort háromszor ír felül, elsőnek 0x00, majd 0xFF és végül véletlen értékkel. A törlés eredménye ellenőrzésre kerül a törölt terület egy százalékában. Az SDD flash meghajtók esetében a firmware-alapú törlési módszerek halmazát (rangsorolt listáját) használja, amelyek automatikusan kiválasztásra kerülnek az SSD firmware képességei alapján. A törlési módszer automatikusan a következő sorrendben kerül kiválasztásra, az SSD flash-meghajtó által támogatott firmware-funkciók függvényében:

1. ATA Sanitize Crypto Scramble (Firmware alapó törlés)
2. ATA Sanitize Block Erase (Firmware alapó törlés)
3. ATA Secure Erase (Firmware alapó törlés)

4. US DoD 5220.22-M (minden szektort háromszor ír felül, elsőnek 0x00, majd 0xFF és végül véletlen értékkel)

A CECE Android Eraser egy olyan szoftver, amely az Android mobileszközökön tárolt felhasználói adatok végleges törlésére szolgál, Android OS 7-es vagy annál frissebb operációs rendszerrel rendelkező eszköz esetében. A szoftver a CECE Web Managerről letölthető alkalmazásként kerül kiszállításra, és közvetlenül a törlendő célkészülékre telepíthető. A kriptográfiai törlés megfelel a DoD szabványt megújító NIST SP 800-88 Rev1 Guidelines for Media Sanitization, 2014 2.6. fejezetében szereplő Cryptografic Erase eljárásnak, azaz a kriptográfiai kulcsok törlésével teszi elérhetetlenné a tárolt, titkosított adatot. Az alkalmazás három fő lépést hajt végre:

- Első lépés - Az alkalmazás felszabadítja a tárhelyet.

- Második lépés - Felülírja az eszközön rendelkezésre álló összes helyet.

- Harmadik lépés - A kriptográfiai törlés végrehajtása (CECE Az Android Eraser az Android API segítségével hívja meg a Device Policy Manager metódust, amely végrehajtja a kriptográfiai törlést.) A Device Policy Manager az Android operációs rendszer azon interfésze, mellyel eszköz adminisztrátor („device administrator”) szintű feladatokat lehet végrehajtani.

A folyamat befejezése után gyári visszaállítás történik.

A CECE iOS Eraser egy olyan szoftver, amely az iOS 10.3-as vagy annál frissebb operációs rendszerrel rendelkező mobileszközökön tárolt felhasználói adatok végleges törlésére szolgál. Alkalmazásként szállítják, amely letölthető a CECE Web Managerről, majd átvihető egy USB flash meghajtóra, és végül elindítható egy számítógépen. A bootolás után a célzott iOS-eszközt USB-kábelen keresztül kell csatlakoztatni a számítógéphez. A kriptográfiai törlés megfelel a DoD szabványt megújító NIST SP 800-88 Rev1 Guidelines for Media Sanitization, 2014 2.6. fejezetében szereplő Cryptografic Erase eljárásnak, azaz a kriptográfiai kulcsok törlésével teszi elérhetetlenné a tárolt, titkosított adatot.

Az alkalmazás három fő lépést hajt végre:

- Első lépés - Felülírja az online elérhető legfrissebb firmware-verzióval.

- Második lépés - kriptográfiai adattörlés végrehajtása, melynek során a törölhető tárhelyet („Effaceable Storage”) formázza, és a fájlrendszer titkosítási kulcsait megsemmisíti. Megjegyzendő, hogy az iOS felépítése miatt a tárhely bizonyos részeit csak és kizárólag a gyártó (Apple) éri el, azt nyilvánosan elérhető, logikai megoldással nem lehet törölni.

- Harmadik lépés - érvényesítés (a törlési folyamat sikerét az iOS-eszköz naplóiban az Effaceable Storage törlési bizonyítékok ellenőrzése igazolja).

Mindhárom esetben a céltároló vagy meghajtó feldolgozása (törlése) után törlési jelentés készül, amelyet digitális aláírásra elküld a szerverre. Az adott törlési folyamatnak megfelelő elektronikus aláírás igazolja a dokumentum sértetlenségét és az aláíró személyazonosságát. Ez a jelentés internetes kapcsolaton keresztül feltöltésre kerül a CECE Web Manager portálra.

I.2.2. A TOE biztonsági céljai

A biztonsági előirányzat az alábbiak szerin azonosítja a TOE által megvalósított biztonsági célokat:

O.PROPER_ERASE: A TOE-nak képesnek kell lennie a kiválasztott tárolómeghajtón vagy mobilon tárolt összes címezhető adat törlésére (Android és iOS) úgy, hogy az adatok ne legyenek helyreállíthatók.

O.AUTHENTICATED_USERS: A TOE csak akkor engedheti meg a felhasználóknak a használatát, ha a licenckód érvényes kombinációját adják meg. és az e-mail címet.

O.PROPER_AUDIT: A TOE-nak eszközöket kell biztosítania a biztonság szempontjából releváns események rögzítésére és a felhasználó (személy használó) számára a törlési szabványról, a folyamatban lévő törlési folyamat állapotáról, a különleges területek kezeléséről és a nem törölhető területekről.

O.PROPER_REPORTS: A TOE-nak a törlési folyamatra vonatkozó információkat tartalmazó jelentéseket kell exportálnia, és a következőket kell biztosítania az exportált adatok integritásának jövőbeli ellenőrzéséhez.

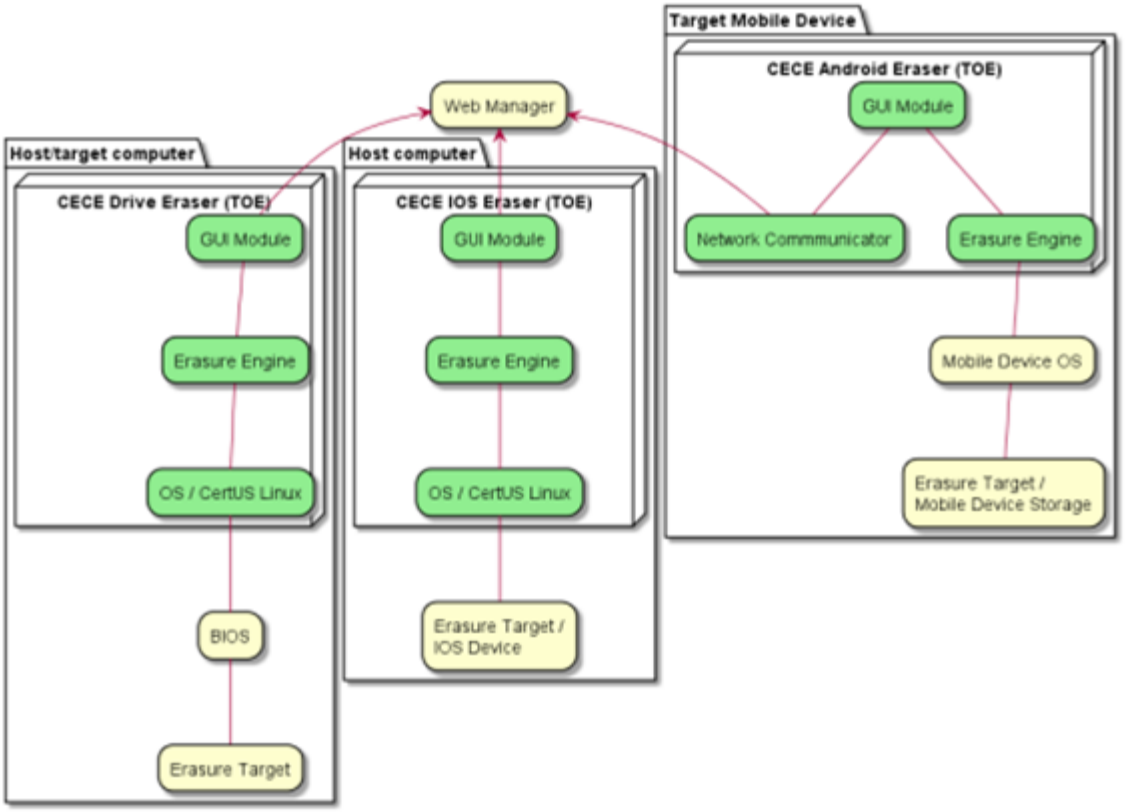
O.PROPER_INTEGRITY_TRACEBILITY: A TOE-nak olyan eszközöket kell biztosítania, amelyek feltárják a törlési jelentésen végrehajtott tartalmi változásokat a létrehozás után (digitális aláírás).

I.3. A TOE biztonsági környezete és határai

A TOE fizikai határain belüli komponensek:

- A CECE Drive Eraser (“CECE Drive Eraser (TOE)”-ként jelölve az 1. ábrán) egy iso fájl, ami egy bootolható lemezképet tartalmaz, és készen áll egy bootolható USB flash meghajtó létrehozására.
- CECE Android Eraser (“CECE Android Eraser (TOE)”- ként jelölve az 1. ábrán) egy apk file, ami az Android alkalmazást tartalmazza.
- CECE iOS Eraser (“CECE iOS Eraser (TOE)”- ként jelölve az 1. ábrán) egy iso fájl, ami egy bootolható lemezképet tartalmaz, és készen áll egy bootolható USB flash meghajtó létrehozására.
- CECE Software System - Kezelési Útmutató[1] file amely magyar nyelven tartalmazza a CECE szoftverrendszer használatának teljes útmutatóját.

[1] https://veglegestorles.hu/download/products/cece/manuals/CECE_Felhasznaloi_Kezikonyv.pdf



1. számú ábra: A CECE Software System magas szintű architektúra diagramja

TOE-n kívüli szoftver elemek:

Az alábbiak azok a szoftverkomponenseket, amelyek nem részei az összeállított TOE-nek.

A CECE Drive Eraser komponenshez kapcsolódók:

- CECE USB Tool a CECE Drive Eraser bootolható USB flash meghajtó létrehozásához.
- A CECE Drive Eraser rendszerindításához használt USB flash meghajtó firmware-je.
- Annak a számítógépnek a firmware-je (BIOS), amelyen a CECE Drive Eraser elindul.
- A használt Linux segédprogramok
- A célmeghajtók firmware-je
- A CECE Web Manager komponens

A CECE Android Eraser komponenshez kapcsolódók:

- Annak az Android-eszköznek a firmware-je, amelyen a CECE Android Eraser elindul.
- Az Android operációs rendszer, amelyen a TOE fut.
- A CECE Web Manager komponens

A CECE iOS Eraserhez komponenshez kapcsolódók:

- CECE USB Tool a CECE iOS Eraser bootolható USB flash meghajtó létrehozásához
- A CECE iOS Eraser indításához használt USB flash meghajtó firmware-je
- Annak a számítógépnek a firmware-je (BIOS), amelyen a CECE iOS Eraser elindul.
- A használt Linux segédprogramok

- Az iOS-eszköz operációs rendszere
- A CECE Web Manager komponens

TOE-n kívüli hardver komponensek:

CECE Drive Eraser esetén:

- A számítógép-rendszer architektúrája, amelyen a CECE Drive Eraser elindul.
- A CECE Drive Eraser indításához használt USB flash meghajtó
- A céltároló meghajtó

CECE Android Eraser esetén:

- A cél Android eszköz
- Az SD-kártya (opcionális)

CECE iOS Eraser esetén:

- A számítógép rendszerarchitektúrája, amelyen a CECE iOS Eraser elindul
- A CECE iOS Eraser indításához használt USB flash meghajtó
- A cél iOS-eszköz

I.4. A rendszer komponenseinek azonosítása

Értékelt TOE verzió:

Fájlnév	Verzió
cecede-1.8.0-rc5-x64-uefi.iso	1.8.0-rc5
SHA256: 15A7E4E31973E80A98CA5C0C86BD7763BC124844D941F1285DDFFC19F6D94D2C	

Fájlnév	Verzió
ceceie-1.1.0-rc5-x64-uefi.iso	1.1.0-rc5
SHA256: 2C2EB27262945AD31FE327ACFCE815E6449F3B27559AC3C13CA09DBED4B77D6C	

Fájlnév	Verzió
ceceae-1.5.0-rc3.apk	1.5.0-rc3
SHA256: 8BC77291646331BF36D763EB8150A0B9C9667F88E336FB8F33C19DC357A96752	

II. A tanúsítás jellemzése

Jelen tanúsítás a termék biztonsági előirányzatában lefektetetett követelmények teljesülését vizsgálja.

II.1. Az alkalmazott értékelési módszer

A CECE Software System v1.1.0 modul termék értékelésére az MSZ EN ISO/IEC 18045:2020 /Informatika. Biztonságtechnika. Az informatikai biztonságértékelés módszertana/ értékelési módszertant alkalmazták.

Az értékelés garanciaszintje MSZ EN ISO/IEC 15408-3:2020 szerinti EAL3-as.

II.2. A tanúsításhoz felhasznált értékelési jelentések azonosítása

Értékelési Jelentés:

- ÉRTÉKELÉSI JELENTÉS CECE Software System v1.1.0 v1.0, száma: CA081-01/P/E/ETR

II.3. Biztonsági előirányzat

Az értékelés az alábbi biztonsági előirányzat 2. fejezetében kinyilvánított megfelelőségi állításokra vonatkozott:

- Security Target for CECE Software System v0.9 /2021. december 16./

II.4. Az értékeléshez felhasznált fejlesztői bizonyítékok

Az értékelés, a fejlesztőkkel történt folyamatos konzultáció mellett, az alábbi fejlesztői bizonyítékok végleges verzióit használta fel:

Cím	Verzió	Dátum
Security Target for CECE Software System	0.9	2021.12.16.
CECE Software System Documentation for Common Criteria Evaluation ADV_ARC Development Security Architecture Description	0.7	2021.11.25.
CECE Software System Documentation for Common Criteria Evaluation ADV_TDS Development Architectural Design	0.6	2021.11.25.
CECE Software System Documentation for Common Criteria Evaluation ADV_FSP Development Functional Specification with complete summary	0.7	2021.12.18.
Adattörlő alkalmazás Felhasználói kézikönyv veglegestorles.hu	5.4	2021.12.06.
CECE Software System Documentation for Common Criteria Evaluation ALC_CMC.3 Life-cycle Support Authorization Controls	1.2	2021.12.17.
CECE Software System Documentation for Common Criteria Evaluation ALC_LCD.1 Life-cycle Support Developer defined life-cycle model	1.1	2021.12.17.
CECE Software System Documentation for Common Criteria Evaluation ALC_DVS.1 Life-cycle Support Identification of security measures	1.1	2021.12.17.
CECE Software System Documentation for Common Criteria Evaluation ALC_DEL Life-cycle Support Delivery procedures	1.5	2021.12.15.

CECE Software System Documentation for Common Criteria Evaluation ALC_CMS.3 Life-cycle Support Implementation representation CM coverage	1.5	2021.12.17.
CECE Software System Documentation for Common Criteria Evaluation ATE_FUN, ATE_COV, ATE_DPT Test documentation (Functional testing, Analysis of coverage, Testing: basic design)	0.7	2021.12.17.

II.5. Az értékelési folyamat tanúsítási szempontú ellenőrzése

A Tanúsítási Jelentés készítői a teljes értékelési folyamatot figyelemmel kísérték, ellenőrizték:

- az értékelési folyamatok módszertani szempontú ellenőrzésével;
- különböző szakértői megbeszéléseken való részvétellel.

III. Az értékelés eredményei

III.1. A garanciális biztonsági követelményeknek való megfelelés

Az értékelés módszertana a MSZ EN ISO/IEC 18045:2020 szabványt követte, az eredmények leírása is az ott meghatározott jelöléseket alkalmazza.

III.1.1. A biztonsági előirányzat értékelése

Értékelői feladatelem	határozat
ASE_INT.1: Biztonsági előirányzat, Bevezetés	megfelelt
ASE_CCL.1: Biztonsági előirányzat, Megfelelőségi nyilatkozatok	megfelelt
ASE_SPD.1: Biztonsági előirányzat, Biztonsági probléma meghatározás	megfelelt
ASE_OBJ.2: Biztonsági előirányzat, Biztonsági célok	megfelelt
ASE_ECD.1: Biztonsági előirányzat, Kiterjesztett biztonsági követelmények	megfelelt
ASE_REQ.2: Biztonsági előirányzat, Biztonsági követelmények	megfelelt
ASE_TSS.1: Biztonsági előirányzat, Az értékelés tárgya összefoglaló előírása	megfelelt

III.1.2. A fejlesztés értékelése

Értékelői feladatelem	határozat
ADV_ARC.1: Biztonsági szerkezet leírás	megfelelt
ADV_FSP.3: Funkcionális specifikáció teljes összegzéssel	megfelelt
ADV_TDS.2: Szerkezeti terv	megfelelt

III.1.3. Az útmutatók értékelése

Értékelői feladatelem	határozat
AGD_OPE.1: Üzemeltetési felhasználói útmutató	megfelelt
AGD_PRE.1: Előkészítő eljárások	megfelelt

III.1.4. Az életciklus támogatás értékelése

Értékelői feladatelem	határozat
ALC_CMC.3: Engedélyezéssel kapcsolatos intézkedések	megfelelt
ALC_CMS.3: A megvalósítási reprezentáció CM lefedettsége	megfelelt
ALC_DEL.1: Szállítási eljárások	megfelelt
ALC_DVS.1: A biztonsági intézkedések azonosítása	megfelelt
ALC_LCD.1: A fejlesztő által meghatározott életciklus modell	megfelelt

III.1.5. A tesztelés értékelése

Értékelői feladatelem	határozat
ATE_FUN.1: Funkcionális tesztelés	megfelelt
ATE_COV.2: A lefedettség vizsgálata	megfelelt
ATE_DPT.1: Az alap terv tesztelése	megfelelt
ATE_IND.2: Független tesztelés - minta	megfelelt

A TOE három fő elemének (Drive Eraser, Android Eraser, iOS Eraser) a fejlesztő külön tesztelési dokumentációt készített. Mindhárom esetben készül egy teszteset leírás, melynek végrehajtásáról külön dokumentum készült. A tesztek jelentős része automatizáltan is végrehajtásra került, melynek eredményeit a bemutatott dokumentációk tartalmazták. A tesztesetek kellő mélységben kerültek leírásra és végrehajtásra.

A TOE értékelői tesztelése a veglegtorles.hu oldalon közétett, letöltött szoftver használatával történt. A TOE vonatkozásában mindhárom komponens (Drive Eraser, Android Eraser, iOS Eraser) tesztelésre került, az értékelő által készített teszterv alapján, saját tesztkörnyezetünkben. A tesztelés eredménye külön jegyzőkönyvben került rögzítésre.

A „bootolható” USB elkészítés tesztelése az alábbi operációs rendszereken történt:

- Windows 10 version 21H2
- Ubuntu 20.04
- MacOS 11.4

A törlés tesztelése az alábbi eszközökön történt:

- iOS 12.5.5 – Iphone 6 (MG4F2) – 64 GB tárhellyel
- iOS 15.1 – Apple iPad 9, 64 GB tárhellyel
- Android 9 – Samsung Galaxy J3 PRO, 16 GB tárhellyel
- SSD meghajtó – Samsung MZ7LN256HCHP-0000, 256 GB tárhellyel (laptop: Fujitsu Lifebook E746 – DSES012640)
- Verbatim SmartDisk 320 GB – külső winchester
- USB Pendrive, NTFS formázás, 16 GB, Kingston

III.1.6. A sebezhetőség értékelése

Az értékelő tanulmányozta a nyilvános adatbázisokat, információ forrásokat a TOE lehetséges sebezhetőségeinek meghatározása céljából. A szervezet saját maga is azonosította azon harmadik féltől származó komponenseket, melyek sérülékenységeket tartalmazhatnak. Vizsgálatunk során megállapítottuk, hogy a feltárt sérülékenységek a TOE esetében nem jelentenek kockázatok, mert egyik sérülékenység sem kihasználható a vizsgált TOE-ban.

Az értékelő megtervezte az áthatolás teszteket. A tesztek elvégzéséhez az értékelő saját sérülékenységvizsgálati környezetét és eszköztárát használta. Az áthatolás tesztelés célja az volt, hogy a kiszolgálói infrastruktúra (a szoftver elérhetőségét biztosító weboldal) kívülről támadható-e, illetve maga a szoftver tartalmaz-e olyan sérülékenységeket, mellyel a rendeltetés szerű használat megkerülhető. Ennek elvégzésére azért volt szükség, mert a biztonságos szállítás biztosítását ez a weboldal teszi lehető (kizárólag ezen keresztül érhető el a felhasználónak a TOE)

Az áthatolás tesztelések eredményei alapján az értékelő megállapította, hogy a TOE az üzemeltetési környezetében ellenáll egy alap támadó képességgel rendelkező támadónak.

Értékelői feladatelem	határozat
AVA_VAN.2: Sebezhetőség vizsgálat	megfelelt

IV. Következtetés

A rendszer értékelés fő következtetése az alábbi:

A CECE Software System v1.1.0 megfelel biztonsági előirányzatának, kielégíti az abban megfogalmazott funkcionális és garanciális biztonsági követelményeket.

Az értékelés eredménye alapján a Tanúsító megállapítja, hogy a CECE Software System v1.1.0, mint informatikai biztonsági funkciókat megvalósító szoftver termék megfelel a II.3 fejezetben meghatározott Biztonsági Előirányzatnak az MSZ EN ISO/IEC 15408-3:2020 szabvány EAL 3-as garancia szinten.

IV.1. Feltételek

Az értékelés következtetései a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlnak.

Ezek a feltételek (melyeket az CECE Software System v1.1.0 nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezet teljesítse) az alábbiak:

OE.COMPETENT_USERS: A felhasználóknak (a TOE-t használó személyeknek) jó szándékúaknak kell lenniük, és követniük kell a rendelkezésre álló útmutató online dokumentumot (CECE Web Manager).

OE.FIRMWARE_NOT_PREVENTING: A célszámítógép firmware (BIOS) beállításainak, amelyek zavarhatják a törlési folyamatot, megfelelően konfigurálva kell lennie, hogy ne akadályozza a CECE Drive Eraser által végzett törlési folyamatot. Az Android OS vagy iOS beállításainak, amelyek zavarhatják a törlési folyamatot, megfelelően konfigurálva kell lennie, hogy ne akadályozza a CECE Android Eraser vagy a CECE iOS által végzett törlési folyamatot.

OE.FUNCTIONAL_STORAGE: A CECE Drive Eraser által törlendő céltároló meghajtóknak az elvárásoknak megfelelően kell viselkedniük és a teljes tárolókapacitást az operációs rendszer számára hozzáférhetővé kell tenniük. Ezen túlmenően a célmeghajtó eszközök vezérlőjének megfelelően kell továbbítania a törléssel és a törlési ellenőrzés adatok visszakeresésével kapcsolatos parancsokat. Az Android és iOS céleszközöknek elérhetővé kell tenniük a teljes tárolási területet, ahol a felhasználói adatokat tárolják a CECE Android törlőprogram, illetve a CECE iOS törlőprogram számára.

OE.ACCURATE_SYSTEM_TIME: Az üzemeltetési környezetnek pontos rendszeridőt kell biztosítania.

OE.TRUSTED_NETWORK: Az üzemeltetési környezetnek biztosítania kell a TOE számára egy olyan megbízható hálózatot, ahol a TOE komponensei ellen nem érkeznek rosszindulatú támadások a csatlakoztatott interfészekről.

OE.PROPER_INTEGRITY_TRACEBILITY: A CECE Web Managernek az egyes eszközökre alkalmazott adattörlési folyamat bizonyítása érdekében a törlési jelentéseket dekódolnia, aláírnia és időbélyegzővel kell ellátnia.

V. Hivatkozások, rövidítések

V.1. A követelményeket tartalmazó dokumentum

MSZ EN ISO/IEC 15408-1:2020 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 1. rész: Bevezetés és általános modell

MSZ EN ISO/IEC 15408-2:2020 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 2. rész: A biztonság funkcionális követelményei

MSZ EN ISO/IEC 15408-3:2020 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 3. rész: A biztonság garanciális követelményei

V.2. Figyelembe módszertani dokumentumok

MSZ EN ISO/IEC 18045:2020 Informatika. Biztonságtechnika. Az informatikai biztonságértékelés módszertana

V.3. Rövidítések

ADV (Assurance: Development)	Fejlesztés értékelése
AGD (Assurance: Guidance documents)	Útmutató dokumentumok értékelése
ALC (Assurance: Life cycle support)	Életciklus támogatás értékelése
ASE (Assurance: Security Target)	Biztonsági előirányzat értékelése
ATE (Assurance: Tests)	Tesztelés értékelése
AVA (Assurance: Vulnerability assessment)	Sebezhetőségi elemzés értékelése
CC (Common Criteria)	Közös szempontok
CM (Configuration management)	Konfiguráció kezelés
EAL (Evaluation Assurance Level)	Értékelési garanciaszint
ETR (Evaluation Technical Report)	Értékelési jelentés
ST (Security Target)	Biztonsági előirányzat
TOE (Target of Evaluation)	TOE, Értékelés tárgya
API (Application Interface)	Applikációs interfész

Felelőségi nyilatkozat[2]

A tanúsítási folyamat és a tanúsítvány teljes mértékben a termék kiberbiztonsági tanúsítási követelményeihez kötődik a tanúsítvány kiállításának időpontjában, nem magához a termékhez, sem annak egyéb funkcióihoz, garanciális elvárásaihoz.

A tanúsítvány nem jelenti sem a termék, sem az átadásának, csomagolásának vagy a termékkel összefüggő egyéb tényezőknek a megfelelőségét. Kizárólag arra vonatkozik, hogy a termék kapcsán bemutatott dokumentumok és információk, melyek valódiságáért, helyességéért a termék tulajdonosa vagy üzemeltetője felelős megfelelnek a tanúsítással kapcsolatos információk kiberbiztonsági követelményeinek. Nem ad garanciát a kereskedelmi forgalomban való alkalmazhatóságra, a hiányosságoktól hibáktól való mentességére, a szellemi tulajdonjogok, a fogyasztói jogok és bármely más kapcsolódó jog megsértésének tilalmára. A tanúsítás kiállítója vagy a kiberbiztonsági tanúsítási rendszer tulajdonosa semmilyen körülmények között nem vállal felelősséget a termék használatának elmulasztásából vagy használatából eredő bármilyen közvetlen, közvetett, anyagi, technikai és informatikai funkcionalitással kapcsolatos vagy erkölcsi kárért.

A tanúsítvány kibocsátója vagy a tanúsítási rendszer kidolgozója, illetve bármely más, a tanúsítványt elismerő vagy érvényre juttató szervezet számára nem keletkezik felelősség a jó hírnév elvesztéséért, a munka leállásáért, az informatikai eszköz, alkalmazás vagy rendszer meghibásodásáért vagy hibás működéséért, a veszteségért vagy kárért, a módosításokért, a nem megfelelő használatért, a visszaélésért, a megváltoztatásért, a megsemmisítésért, a lopásért, a zsarolásért vagy az adatokhoz való jogosulatlan hozzáférés bármely más formájáért, illetve bármilyen kereskedelmi kárért.

[2] Jelen Nyilatkozat az ENISA (European Union Agency for Cybersecurity) EUCC (Common Criteria based European candidate cybersecurity certification scheme) sémadokumentum elvárásai alapján készült (https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1)