TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft, mint tanúsító szervezet

tanúsítja,

hogy a

NETI Informatikai Tanácsadó Kft.
által kifejlesztetett

OneWayer 1.0 hálózatbiztonsági eszköz

Szoftver verzió: 1.0.34

az 1. számú mellékletben áttekintett funkcionalitással, valamint

a 2. számú melléklet biztonságos felhasználásra vonatkozó feltételek figyelembe vételével

a KIB 28-as Ajánlásában szereplő
MIBÉTS módszertan alapján értékelve, tanúsítva
kiemelt biztonsági szinten (mely megfelel a CC EAL 4-es szintjének)
alkalmas

kizárólag egyirányú kommunikáción keresztüli fájl továbbítás funkció megvalósítására
egy alacsonyabb biztonsági besorolású környezetből („Low Security Side” hálózat)
egy magasabb biztonsági besorolású környezet („High Security Side” hálózat) felé.

Jelen tanúsítvány a **HUNG-TJ-MIBÉTS-01-2011** számú tanúsítási jelentés alapján került kiadásra.
Készült a Neti Informatikai Tanácsadó Kft. megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-MIBÉTS-01-2011.**
A tanúsítás kelte: 2011. augusztus 03.
A tanúsítvány érvényességi ideje: 2014. augusztus 03.
Melléklet: tulajdonságok, feltételek, követelmények, egyéb jellemzők összesen 8 oldalon.

PH.

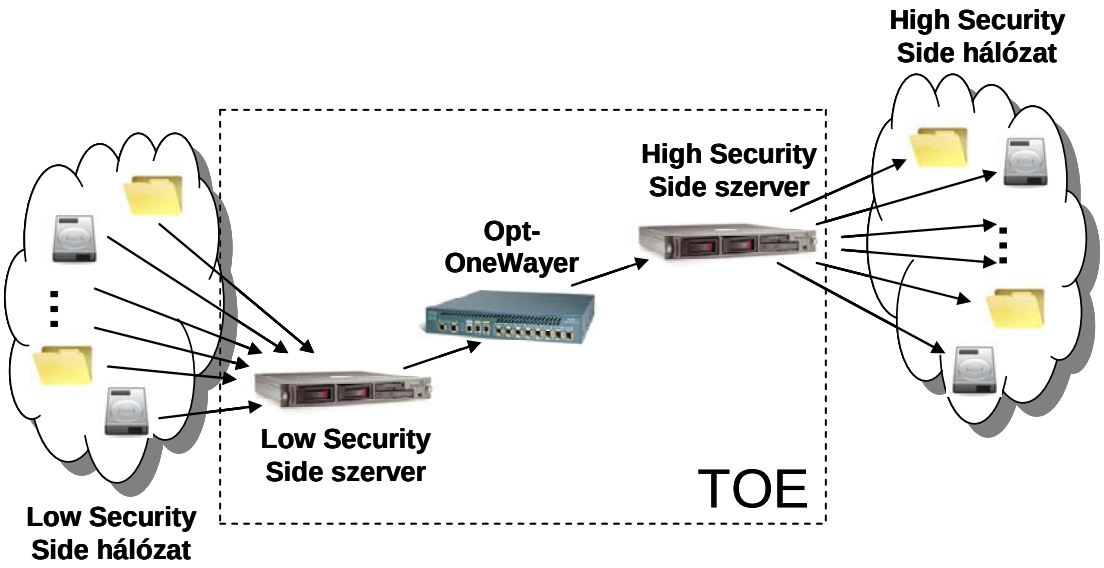
dr. Szabó István
Ügyvezető igazgató

1. számú melléklet

A OneWayer 1.0 eszköz legfontosabb tulajdonságainak összefoglalása

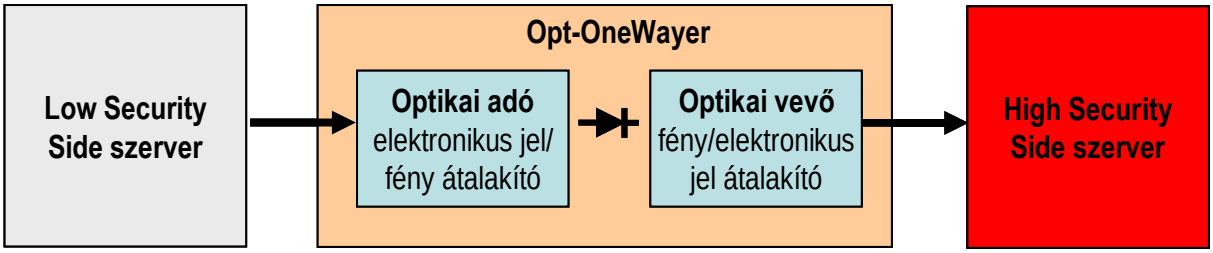
A OneWayer egy olyan informatikai hálózati eszköz, amely kizárólag egyirányú kommunikáción keresztül fájltovábbítás funkciót valósít meg egy alacsonyabb biztonsági besorolású környezetből (Low Security Side /LSS/ hálózat, pl. tipikusan internet) egy magasabb biztonsági besorolású környezet (High Security Side /HSS/ hálózat, tipikusan a belső, védett hálózat) felé.

Az LSS hálózat felhasználói információt küldhetnek a HSS hálózat felhasználóinak (fordítva viszont nem). Az LSS hálózaton kijelölhető több (legfeljebb 10) átviteli kezdőpont (megosztott hálózati erőforrás), melybe az LSS hálózatról információ helyezhető el. Ezt az információt a megfelelően konfigurált OneWayer automatikusan továbbítja a HSS hálózat egy-egy (szintén legfeljebb 10) átviteli célpontjába.



A OneWayer három rendszer összetevőből áll: Low Security Side szerver, Opt-OneWayer és High Security Side szerver.

Az Opt-OneWayer egy opto-elektronikai eszköz, mely az LSS és HSS szerverek között helyezkedik el. Az Opt-OneWayer berendezésen belül egy optikai adó-vevő pár továbbítja a jeleket. A megoldásból adódóan semmilyen galvanikus kapcsolat sincs a két csatlakoztatott hálózat között. Az optikai adó-vevő pár kizárólag az egyik irányba működik, így megvalósítva a garantáltan egyirányú kommunikációt:



A OneWayer hálózatbiztonsági eszköz legfontosabb biztonsági tulajdonságai az alábbiak:

Egyirányú adattovábbítás
- ellenőrzött információáramlás LSS hálózatból HSS hálózatba;
- HSS-ből semmilyen információ nem juthat ki visszafelé.

Integritás védelem
- a továbbított adatok sértetlenségét biztosító hibajavítás alkalmazása;
- az átvitt adatok sértetlenségének figyelése, az integritás hibák észlelése;
- átviteli hiba esetén az ismételt adattovábbítás lehetőségének támogatása.

Rendelkezésre állás
- kétszintű „Watchdog” funkció;
- „heartbeat” figyelés;
- riasztás működési hiba esetén.

Biztonsági menedzsment támogatása
- az eszköz felhasználóinak (adminisztrátor, operátor, auditor) egyedi azonosítása és hitelesítése;
- szerepkör alapú jogosultság kezelés;
- naplózás és utólagos felelősségre vonhatóság biztosítása.

Önvédelem
- fizikai behatolást észlelő és erre reagáló bontásvédelem;
- önteszt a hibátlan működés ellenőrzésére;
- működési hiba és behatolás észlelése esetén biztonságos állapotba állás.

2. számú melléklet

A biztonságos felhasználás feltételei

Az alábbiakban összefoglaljuk azokat a kötelezően betartandó, a jelen tanúsítvány érvényességére kiható feltételeket, melyek hozzájárulnak a OneWayer v1.0 hálózatbiztonsági eszköz biztonságához.

Az értékelés – a Biztonsági előirányzatban meghatározott – az üzemeltetési környezetre vonatkozó biztonsági feltételrendszer teljesülése esetén ad garanciákat az eszköz (TOE) biztonsági tulajdonságainak érvényesülésére.

A feltétel leírása mellett megadjuk a feltétel környezeti célokkal CC terminológiában megfogalmazott leírását is /OE: Operational Environment/ valamint a kiegészítő feltételezéseket /A: Assumptions/ is.

Ezek a feltételek (melyeket tehát a OneWayer maga nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezete teljesítse) az alábbiak.

1. számú feltétel:.

OE.DELIVERY *Az eszköz /TOE/ szállítása biztonságos, így megakadályozza a TOE szállítás közben történő módosítását.*

Megjegyzés: a OneWayer hardver szállítás közben is védi a biztonsági funkciókat magas színvonalú bontásvédelemmel. Ennek ellenére fizikai és szervezési intézkedésekkel az illetéktelen manipulálás elleni védelem erősítendő.
A gyártóval történt egyeztetés szerint a gyártó őrizet mellett maga szállítja ki a megrendelőhöz a készüléket (nem harmadik fél bevonásával történő szállítás révén, ún. „dobozos" termékként).

2. számú feltétel:.

OE.CONNECTION *A TOE az egyetlen eszköz, mely összeköti az LSS és HSS hálózatokat.*

Megjegyzés: más összeköttetési eszközök létezése mellett, melyek összekötik az alacsonyabb biztonsági besorolású környezetet a magasabb biztonsági besorolású környezettel, a jelen Tanúsítványban megfogalmazott garancia nem vonatkozhat a tiltott információáramlás kizárására.

3. számú feltétel:

OE. PHYSICAL_PROT A *hálózatbiztonsági eszközt /TOE-t/ fizikailag biztonságos környezetben tárolják és működtetik, mely környezetre teljesülnek legalább a HSS hálózat szervereire vonatkozó követelmények.*

4. számú feltétel:

OE.INSTALL *A hálózatbiztonsági eszközt az előírásoknak megfelelően úgy telepítik és konfigurálják, hogy az csak az LSS hálózatból a HSS hálózatba való információáramlást tegye lehetővé.*

Megjegyzés: a tervezettel ellentétesen információáramlást a HSS és LSS szervereken futó eltérő alkalmazások is kivédik, de a fizikai védelmi szint hibás telepítés esetén kiesne.

További biztonsági feltétel:

A.TRAINING Az installálásban közreműködőket kiképezték a TOE helyes használatára.

5. számú feltétel:

OE.OPERATE *A TOE-t az „üzemeltetési felhasználói útmutató" című dokumentumban foglaltaknak megfelelően úgy üzemeltetik, hogy az folyamatosan az LSS-ből a HSS felé irányuljon.*

Megjegyzés: a fenti feltétel szerint üzemeltetés közben nem rontják le a telepítéskor beállított konfigurációt /pl. áthelyezéskor, vagy más, újabb installálást, konfigurálást igénylő esetekben/

További biztonsági feltétel:

A.TRAINING Valamennyi felhasználót (operátort, rendszergazdát) kiképezték a TOE helyes használatára.

6. számú feltétel:

OE.SOURCE_CONTROL *Az LSS és a HSS hálózatokon összehangolt szervezeti és technológiai intézkedések biztosítják, hogy az LSS hálózatról átemelésre kerülő fájlok nem tesznek kárt a HSS hálózatban /az eszközön keresztül vírus és rosszindulatú kód nem juthat át, a rendszert használó alkalmazottak az LSS hálózatról adatdömpinggel nem árasztják el a HSS hálózatot/.*

Megjegyzés: a hálózatbiztonsági eszköz nem végez tartalomelemzést, a vírusvédelem, annak frissítése a TOE-n kívüli feladat, legjobb, ha mind az LSS, mind a HSS oldal ellenőriz. Fontos, hogy az IT rendszert használó alkalmazottak ne jelöljenek ki átemelésre indokolatlan mennyiségű adatot.

További biztonsági feltétel:

A.TRAINING Valamennyi felhasználót (IT rendszert használót, TOE operátort, TOE rendszergazdát) kiképezték a TOE helyes használatára**.**

A.SOURCE Az LSS hálózaton szervezeti és technológiai intézkedések biztosítják, hogy csak valóban a HSS hálózatra szánt fájlok kerülnek be az átviteli kezdőpontokba, köztük nincs vírus és rosszindulatú kód.

A.DESTINATION A HSS hálózaton szervezeti és technológiai intézkedések biztosítják, hogy a TOE-n keresztül vírus és rosszindulatú kód nem jut át.

7. számú feltétel:

OE.NOEVIL *Az adminisztrátorok és operátorok szándékosan nem hajtanak végre jogosulatlan tevékenységeket*

Megjegyzés: A fenti felhasználók véletlenül hibázhatnak, erre vannak védelmi mechanizmusok, de szándékosan nem rontják le a biztonsági funkciókat.

További elvárás, hogy a biztonság-kritikus eseményekről készült bejegyzéseket az auditor rendszeresen ellenőrizze, esemény esetén az okokat kivizsgálja.

3. számú melléklet

A tanúsítással és értékeléssel kapcsolatos módszertani hivatkozások

[1]: A MIBÉTS értékelési módszertana (mely a Közigazgatási Informatikai Bizottság 28. számú ajánlásának /Az E-közigazgatási Keretrendszer követelménytár, 2009/ részét képezi az alábbi címen: Termékekre vonatkozó értékelési módszertan)

[2]: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model - CCMB-2009-07-001 - Version 3.1, Revision 3, Final, July 2009.

[3]: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components - CCMB-2009-07-002 - Version 3.1, Revision 3 Final, July 2009.

[4]: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components - CCMB-2009-07-003 - Version 3.1, Revision 3 Final, July 2009.

[5]: Common Methodology for Information Technology Security Evaluation, Evaluation methodology - CCMB-2009-07-004 - Version 3.1, Revision 3 Final, July 2009.

[6]: ISO/IEC 15408-1: 2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

[7]: ISO/IEC 15408-2: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[8]: ISO/IEC 15408-3: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

[9]: ISO/IEC 18045: 2008 Information technology — Security techniques — Evaluation criteria for IT security — Methodology for IT Security Evaluation

4. számú melléklet

A tanúsítási eljárás egyéb jellemzői

A tanúsításhoz figyelembe vett, fejlesztői dokumentumok

- OneWayer Biztonsági előirányzat v1.0
- OneWayer v1.00 Biztonsági szerkezetleírás
- OneWayer v1.00 Funkcionális specifikáció
- OneWayer v1.00 TOE terv

A tanúsításhoz figyelembe vett, fejlesztőktől független dokumentumok

- OneWayer Software v1.0 ÉRTÉKELÉSI JELENTÉS

A követelményeknek való megfelelést ellenőrző vizsgálat garancia szintje

A jelen tanúsítási jelentéshez figyelembe vett, a fejlesztőktől független ellenőrző vizsgálat garancia szintje MIBÉTS kiemelt, mely megfelel az ISO 15408 /Common Criteria/ **EAL 4**-es garanciaszint követelményeinek.

Rövidítések és meghatározások

CC	Common Criteria	közös szempontok
CEM	Common Evaluation Methodology	közös értékelési módszertan
EAL	Evaluation Assurance Level	értékelési garanciaszint
HSS	High Security Side	magas biztonság szintű oldal
KIB		Közigazgatási Informatika Bizottság Ajánlása
LSS	Low Security Side	alacsony biztonság szintű oldal
MIBÉTS	-	Magyar Informatika Biztonsági Értékelési és Tanúsítási Séma
SAR	Security Assurance Requirement	garanciális biztonsági követelmény
SF	Security Function	biztonsági funkció
SFR	Security Functional Requirement	funkcionális biztonsági követelmény
ST	Security Target	biztonsági előirányzat
TOE	Target of Evaluation	az értékelés tárgya
TSF	TOE Security Functionality	az értékelés tárgya biztonsági funkcionalitása