

Megvalósítási dokumentum

Jelen dokumentum célja annak ismertetése, hogy a vizsgált IoT-eszköz (a továbbiakban: VE) megvalósítása során alkalmazott, a VE értékelése szempontjából lényeges, részletes információkat tartalmazza.

A dokumentum a megfelelőségértékelés/ megfelelőségi önértékelés során a vizsgálatok alapjául szolgál, és közvetlen bemenetet biztosít az értékelést megalapozó dokumentum elkészítéséhez.

1.1. MD 1-UserInfo: Felhasználói információk

A módosítási mechanizmusok dokumentálása	
Az érzékelők dokumentációja	
A biztonságos beállítás dokumentációja	
A beállítási ellenőrzés dokumentációja	
A személyes adatok dokumentálása	
A telemetriai adatok dokumentálása	
A törlés dokumentálása	
Modell megnevezése	
Támogatási időszak	
A támogatási időszak közzététele	
A sebezhetőség közzététele	
A nem frissíthető komponensek közzététele	

1.2. MD 2-SecDev: Biztonságos fejlesztési folyamatok

ID	SecDev-1
Leírás	

Az összes olyan folyamat felsorolása szükséges, amelyet a gyártó a VE-re vonatkozóan végrehajtott vagy végrehajtatott. (SecDev-2, SecDev-3, stb.)

1.3. MD 3-VulnTypes: Releváns sebezhetőségek

ID	VulnTypes-1
Leírás	
Intézkedés	
Időkeret	

Az összes típusú sebezhetőség felsorolása szükséges, amely a VE szempontjából lényeges. (VulnTypes-2, VulnTypes-3, stb.)

1.4. MD 4-Conf: Nyilatkozatok

A sebezhetőségi intézkedések megerősítése	
A sebezhetőségi felügyelet megerősítése	
A frissítési eljárások megerősítése	
A biztonságos irányítás megerősítése	
A biztonságos fejlesztés megerősítése	

1.5. MD 5-VulnMon: Sebezhetőség monitorozás

ID	VulnMon-1
Leírás	

Az összes olyan eljárás felsorolása szükséges, amely a sebezhetőségek ellenőrzésére, azonosítására és kijavítására szolgál. (VulnMon-2, VulnMon-3, stb.)

1.6. MD 6-UpdProc: Frissítési eljárások

ID	UpdProc-1
Leírás	
Időkeret	

A gyártó összes olyan eljárásának felsorolása szükséges, amely a biztonsági frissítések kiadására vonatkozik. (UpdProc-2, UpdProc-3, stb.)

1.7. MD 7-Intf: Interfészek

ID	Intf-1
Leírás	
Típus	
Állapot	
Állapotváltozás	
Kapcsolat felépítés	
Közzétett információk	
Hibakeresési interfész	

Védelem	
----------------	--

A VE összes hálózati, fizikai és logikai interfészének felsorolása szükséges. (Intf-2, Intf-3, stb.)

1.8. MD 8-DevID: Eszközazonosítók

ID	DevID-1
Azonosító típusa	
Azonosító hozzáférhetősége	
Azonosító forrása	
Azonosítógeneráló mechanizmus	
Műveletvégzés	
Biztonsági célok	
Brute Force védelem	
Timing attack elleni védelem	

A VE összes, az eszköz azonosítására szolgáló azonosítóját. (DevID-2, DevID-3, stb.)

1.9. MD 9-Role: Szerepkörök

ID	Role-1
Leírás	

Cél	
Műveletek	

Az összes, VE által gyári állapotban kezelt szerepköröket szükséges szerepeltetni, ideértve a nem azonosításkötelezett szereplőket és gép-gép közötti kapcsolatokat is. (Role-2, Role-3, stb.)

1.10. MD 10-AuthMech: Hitelesítési mechanizmusok

ID	AuthMech-1
Leírás	
Authentikációs faktor	
Jelszógeneráló mechanizmus	
Biztonsági garanciák	
Kriptográfiai részletek	
Brute Force védelem	
Timing attack elleni védelem	
Testreszabás	
Alkalmazás	
Kezelés	

A VE összes hitelesítési mechanizmusát szükséges feltüntetni. (AuthMech-2, AuthMech-3, stb.)

1.11. MD 11-Account: Fiókkezelés

ID	Account-1
Művelet	
Leírás	
Konfiguráció	

Az összes felhasználói fiókok kezeléséhez kapcsolódó megoldást szükséges szerepeltetni. (Account-2, Account-3, stb.)

1.12. MD 12-SoftComp: Szoftverkomponensek

ID	SoftComp-1
Leírás	
Frissítési mechanizmus	
Kriptográfiai felhasználás	

A VE összes szoftverkomponensét szükséges felsorolni. (SoftComp-2, SoftComp-3, stb.)

1.13. MD 13-UpdMech: Frissítési mechanizmusok

ID	UpdMech-1
Leírás	
Biztonsági garanciák	
Kriptográfiai részletek	
Kezdeményezés és interakció	
Konfiguráció	

Frissítés ellenőrzése	
Felhasználói értesítés	
Verziókezelés	

A VE összes frissítési mechanizmusát szükséges felsorolni. (UpdMech-2, UpdMech-3, stb.)

1.14. MD 14-SecParam: Biztonsági paraméterek

ID	SecParam-1
Leírás	
Tárolás helye	
Típus	
Biztonsági garanciák	
Védelmi rendszer	
Elosztási mechanizmus	
Kommunikációs mechanizmusok	
Létrehozási mechanizmus	

Az összes olyan érzékeny (nyilvános és kritikus) biztonsági paramétert szükséges felsorolni, amelyet a rendeltetésszerű használat során tartósan tárolnak a VE-n. (SecParam-2, SecParam-3, stb.)

1.15. MD 15-SecMgmt: Biztonságos irányítási folyamatok

ID	SecMgmt-1
-----------	------------------

Leírás	
---------------	--

A kritikus biztonsági paraméterekre vonatkozó összes biztonságos kezelési folyamatot szükséges felsorolni, amelyet a gyártó megvalósított a VE életciklusa során. (SecMgmt-2, SecMgmt-3, stb.)

1.16. MD 16-ComMech: Kommunikációs mechanizmusok

ID	ComMech-1
Leírás	
Biztonsági garanciák	
Kriptográfiai részletek	
Kezdeményezés és interakció	

A VE összes kommunikációs mechanizmusát szükséges felsorolni. (ComMech-2, ComMech-3, stb.)

1.17. MD 17-NetSecImpl: Hálózati és biztonsági megvalósítások

ID	NetSecImpl-1
Leírás	
Felülvizsgálati/értékelési módszer	
Jelentés	

A VE hálózati és biztonsági funkcióinak összes megvalósítását szükséges felsorolni. (NetSecImpl-2, NetSecImpl-3, stb.)

1.18. MD 18-SoftServ: Szoftverszolgáltatások

ID	SoftServ-1
Leírás	
Állapot	
Indokolás	
Konfiguráció	
Hitelesítési mechanizmus	
Harmadik feles SW	

A VE összes szoftverszolgáltatását szükséges felsorolni. (SoftServ-2, SoftServ-3, stb.)

1.19. MD 19-CodeMin: Kódminimalizálás

ID	CodeMin-1
Leírás	

Az összes, a kódok minimalizálására alkalmazott módszer felsorolása szükséges. (CodeMin-2, CodeMin-3, stb.)

1.20. MD 20-PrivCtrl: Jogosultságszabályozás

ID	PrivCtrl-1
Leírás	
Mátrix	
Hitelesítés	

Az összes jogosultságszabályozási mechanizmust szükséges felsorolni. (PrivCtrl-2, PrivCtrl-3, stb.)

1.21. MD 21-AccCtrl: Hozzáférés-védelem

ID	AccCtrl-1
Leírás	

Az összes memóriához való hozzáférés-védelmi mechanizmust szükséges felsorolni. (AccCtrl-2, AccCtrl-3, stb.)

1.22. MD 22-SecBoot: Biztonságos rendszerindítási mechanizmusok

ID	SecBoot-1
Leírás	
Biztonsági garanciák	
Érzékelési mechanizmusok	
Felhasználói értesítés	
Értesítési funkciók	

A VE összes biztonságos indítási mechanizmusát szükséges felsorolni. (SecBoot-2, SecBoot-3, stb.)

1.23. MD 23-Store: Tárolás és visszaállítás

ID	Store-1
Tároló	
Redundancia	

Az adatok visszaállításának módja	
Titkosítás	

A VE által kezelt adatok összes tárolási módját, illetve az adatok visszaállíthatóságának módját szükséges felsorolni. (Store-2, Store-3, stb.)

1.24. MD 24-DataSec: Adatvédelem

ID	DataSec-1
Leírás	
Feldolgozási tevékenységek	
Kommunikációs mechanizmusok	
Érzékenység	
Hozzájárulás megszerzése	
A hozzájárulás visszavonása	
Kriptográfiai védelem	
Tároló	

A VE által feldolgozott összes adatot szükséges felsorolni. (DataSec-2, DataSec-3, stb.)

1.25. MD 25-ExtSens: Külső érzékelők

ID	ExtSens-1
Leírás	

A VE összes külső érzékelési képességét szükséges felsorolni. (ExtSens-2, ExtSens-3, stb.)

1.26. MD 26-ResMech: Ellenálló képességi mechanizmusok

ID	ResMech-1
Leírás	
Típus	
Biztonsági garanciák	

Az összes olyan ellenálló képességi mechanizmust szükséges felsorolni, amely a VE hálózati kapcsolatának megszakadására vagy áramkimaradás esetére irányul. (ResMech-2, ResMech-3, stb.)

1.27. MD 27-TelData: Telemetriai adatok

ID	TelData-1
Leírás	
Cél	
Biztonsági vizsgálat	
Adatkapcsolatok	

A VE által gyűjtött összes telemetriai adatot szükséges felsorolni. (TelData-2, Teldata-3, stb.)

1.28. MD 28-DelFunc: Törlési funkciók

ID	DelFunc-1
Leírás	
Céltípus	

Kezdeményezés és interakció	
Megerősítés	

A felhasználó adatainak összes törlési funkcióját szükséges felsorolni. (DelFunc-2, DelFunc-3, stb.)

1.29. MD 29-UserDec: Felhasználói döntések

ID	UserDec-1
Leírás	
Lehetőségek	
Döntés	

A telepítés és karbantartás során meghozandó összes döntést szükséges felsorolni. (UserDec-2, UserDec-3, stb.)

1.30. MD 30-UserIntf: Felhasználói interfészek

ID	UserDec-1
Leírás	
Konfigurációs interfész	
Kommunikációs mechanizmus	

1.31. MD 31-ExtAPI: Külső API-k

ID	ExtAPI-1
Leírás	

A VE összes API-ját szükséges felsorolni, amely lehetővé teszi a külső forrásokból történő adatbevitelt. (ExtAPI-2, ExtAPI-3, stb.)

1.32. MD 32-InpVal: Adatbeviteli érvényesítés

ID	InpVal-1
Leírás	

A VE összes adatbeviteli érvényesítési módszerét szükséges felsorolni. (InpVal-2, InpVal-3, stb.)

1.33. MD 33-Notif: Értesítések

ID	Notif-1
Értesítés módja	
Értesítés kezelése	
Tartalom	

A felhasználói értesítések összes módját szerepeltetni szükséges. (Notif-2, Notif-3, stb.)

1.34. MD 34-AuditLog: Naplóadatok

ID	AuditLog-1
Leírás	
Biztonsági garanciák	
Védelmi rendszer	

A VE összes naplózási módszerét szükséges felsorolni. (AuditLog-2, AuditLog-3, stb.)