A Szabályozott Tevékenységek Felügyeleti Hatósága elnökének 10/2024. (VIII. 8.) SZTFH rendelete az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről

A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény 28. § (3) bekezdés c) pontjában kapott felhatalmazás alapján, a Szabályozott Tevékenységek Felügyeleti Hatóságáról szóló 2021. évi XXXII. törvény 13. § n) és q) pontjában meghatározott feladatkörömben eljárva a következőket rendelem el:

1. § (1) E rendelet alkalmazásában IoT-eszköz az olyan, a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (a továbbiakban: Kibertan.tv.) szerinti IKT-termék, amely jelátalakítás révén a környezettel kölcsönhatásba lép. A kölcsönhatás formája lehet

a) érzékelés, amelynek során az IoT-eszköz a környezetről adatot gyűjt, illetve

b) beavatkozás, amely által a környezetben változás következik be.

(2) Az (1) bekezdés szerinti környezettel való kölcsönhatás megvalósulhat

a) alkalmazásprogramozási felület (a továbbiakban: API) által, amely biztosítja, hogy más számítástechnikai eszközök kommunikáljanak egy IoT-eszközzel az IoT-eszköz által biztosított alkalmazáson keresztül,

b) felhasználói felület által, amely biztosítja az IoT-eszköz és a felhasználó közötti közvetlen kommunikáció lehetőségét, vagy

c) hálózati kapcsolat által, amely biztosítja az IoT-eszköz elektronikus hírközlő hálózattal való kommunikációját adatok IoT-eszközre vagy IoT-eszközről történő közlése céljából vagy a hálózati felhasználói felület elérését.

(3) A (2) bekezdés c) pontja alkalmazása szempontjából a hálózati kapcsolatot lehetővé tévő interfészképesség magában foglalja mind a hardvert, mind az azt működtető és kiszolgáló szoftverkörnyezetet.

2. § (1) E rendeletet – a (2) és (3) bekezdésben foglalt kivétellel – az IoT-eszközök megfelelőségi önértékelésére és megfelelőségértékelésére (a továbbiakban együtt: értékelés) kell alkalmazni.

(2) Nem terjed ki e rendelet hatálya azoknak az IoT-eszközöknek az értékelésére, amelyekre vonatkozóan a Szabályozott Tevékenységek Felügyeleti Hatóságának elnöke külön rendeletben nemzeti kiberbiztonsági tanúsítási rendszert határozott meg.

(3) Az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszerének (a továbbiakban: tanúsítási rendszer) célja, hogy biztosítsa az állampolgárok, a gazdálkodó szervezetek és az állami szervek IoT-eszköz beszerzése során hozott döntéseinek támogatását és az eszközök összehasonlíthatóságát a tanúsítási rendszerben meghatározott megbízhatósági szintek alapján.

3. § (1) A tanúsítási rendszer a Kibertan.tv. 8. § (1) bekezdése szerinti „alap", „jelentős" és „magas" megbízhatósági szintre vonatkozóan tartalmaz követelményeket.

(2) Ha európai uniós vagy magyar jogszabály eltérően nem rendelkezik, az IoT-eszköz forgalmazásának vagy használatának nem feltétele az, hogy az IoT-eszköz rendelkezzen jelen tanúsítási rendszer alapján kiadott nemzeti megfelelőségi nyilatkozattal vagy nemzeti kiberbiztonsági tanúsítvánnyal (a továbbiakban együtt: nemzeti tanúsítvány).

(3) A tanúsítási rendszer alapján „alap" megbízhatósági szinten megfelelőségi önértékelés végezhető.

(4) A megfelelőségértékelő szervezet megfelelőségértékelést legfeljebb a Szabályozott Tevékenységek Felügyeleti Hatósága mint a Kibertan.tv. 4. § (1) bekezdés a) pontjában kijelölt nemzeti kiberbiztonsági tanúsító hatóság (a továbbiakban: tanúsító hatóság) által nyilvántartásba vett megbízhatósági szinten végezhet, a Kibertan.tv. szerinti gyártó (a továbbiakban: gyártó) megbízására.

4. § (1) A gyártó a nemzeti megfelelőségi önértékelési eljárást vagy a megfelelőségértékelő szervezet a megfelelőségértékelési tevékenységet akkor kezdheti meg, ha a gyártó által előállított, 1. melléklet szerinti dokumentumok rendelkezésre állnak. Az 1. melléklet szerinti dokumentumok mintáját a tanúsító hatóság honlapján közzéteszi.

(2) A nemzeti tanúsítvány akkor állítható ki egy adott megbízhatósági szintre, ha az értékelés tárgyát képző IoT-eszköz megfelel a 2. mellékletben az adott megbízhatósági szintre vonatkozóan meghatározott követelményeknek.

(3) A (2) bekezdés szerinti megfelelés – a 3. mellékletben meghatározott követelmények esetében sérülékenységvizsgálat elvégzésével – a 4. melléklet szerinti értékelési módszertan alapján lefolytatott vizsgálat alapján kiállított értékelési jelentés (a továbbiakban: értékelési jelentés) alapján igazolható.

(4) A (2) bekezdés szerinti megfelelés igazolására – a (3) bekezdés szerinti igazolási mód helyett – nemzetközi, európai vagy nemzeti szabvány alapján kiállított tanúsítvány nem fogadható el.

(5) A gyártó az 5. melléklet szerinti megfelelőségi nyilatkozatot, a megfelelőségértékelő szervezet a 6. melléklet szerinti nemzeti kiberbiztonsági tanúsítványt akkor állíthatja ki, ha az értékelési jelentés összesítetten megfelelt minősítésű.

(6) A gyártó a nemzeti megfelelőségi nyilatkozatot, valamint az 1. melléklet szerinti dokumentumokat és az értékelési jelentést a tanúsító hatóság által e célra rendszeresített elektronikus űrlapon nyújtja be a tanúsító hatósághoz nyilvántartásba vételre.

(7) A megfelelőségértékelő szervezet a nemzeti kiberbiztonsági tanúsítványt, valamint az 1. melléklet szerinti dokumentumokat és az értékelési jelentést a tanúsító hatóság által e célra rendszeresített elektronikus űrlapon nyújtja be a tanúsító hatósághoz nyilvántartásba vételre.

(8) A (6) és (7) bekezdés szerint nyilvántartásba vétel ügyintézési határideje 45 nap.

5. § (1) A nemzeti tanúsítvány érvényességi ideje (a továbbiakban: érvényességi idő) a kiállítás dátumától számított legfeljebb 365 nap.

(2) A gyártó a tanúsító hatóság határozatában megjelölt tartalommal köteles a Szabályozott Tevékenységek Felügyeleti Hatósága elnökének az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendelete szerinti címke mint megfelelőségi jelölés elhelyezésére az érvényességi idő végéig gyártott nemzeti tanúsítvánnyal rendelkező IoT-eszközön.

(3) A gyártó az érvényességi idő alatt folyamatosan és folytatólagosan minden IoT-eszközt érintő változás vonatkozásában biztonsági hatáselemzést végez, amelyben rögzíti

a) a változás dátumát,

b) a változást kiváltó okot,

c) azt, hogy a változás érinti-e a változást megelőzően gyártott IoT-eszközöket,

d) a változás elemeinek részletes leírását,

e) azt, hogy a változás mely kockázatokra van kihatással, és

f) azt, hogy a változás sérülékenységet kezel-e, vagy új biztonsági kontrollt vezet-e be.

(4) A (3) bekezdés alkalmazásában változásnak minősül minden olyan változás, amely befolyásolja az IoT-eszköz biztonsági állapotát, ideértve az új fenyegetések és sebezhetőségek megjelenését is.

(5) A gyártó az 1. melléklet szerinti megvalósítási dokumentumot az érvényességi idő alatt folyamatosan és folytatólagosan frissíti.

6. § (1) A gyártó – az (5) bekezdésben foglalt kivétellel – a tanúsító hatóság nyilvántartásában szereplő nemzeti megfelelőségi nyilatkozat érvényességének fenntartására irányuló kérelmet (a továbbiakban: fenntartási kérelem) nyújthat be a tanúsító hatóság felé – a tanúsító hatóság által e célra rendszeresített elektronikus űrlapon – az érvényességi idő lejártát megelőző legkorábban 60 napon, de legkésőbb 30 napon belül.

(2) A fenntartási kérelemhez csatolni kell az 5. § (3) bekezdése szerinti biztonsági hatáselemzést, az 1. melléklet szerinti megvalósítási dokumentum 5. § (5) bekezdésének megfelelően frissített verzióját, és a kérelemben meg kell jelölni a kérelmezett új érvényességi időt, amely legfeljebb 365 nap.

(3) A fenntartási eljárás során a tanúsító hatóság ügyintézési határideje 30 nap.

(4) A tanúsító hatóság a fenntartási kérelemben feltüntetett érvényességi időtől eltérő, de legalább az eredeti érvényességi idő végétől számított 120 napos érvényességi időt állapíthat meg, ha nem állapítható meg az, hogy – a vizsgált IoT-eszközben bekövetkezett változások mellett – a vizsgált IoT-eszköz a nemzeti megfelelőségi nyilatkozat kiállításától kezdődően folytatólagosan teljesíti a tanúsítási rendszerben foglalt követelményeket, és biztosítja a biztonsági célok megvalósulását. Ha a fenntartási kérelemben megjelölt új érvényességi idő kevesebb, mint 120 nap, a tanúsító hatóság az új érvényességi időt a kérelemnek megfelelően állapítja meg.

(5) A (4) bekezdés szerinti esetben a gyártó az érintett IoT-eszköz vonatkozásában kiállított megfelelőségi nyilatkozatra újabb fenntartási kérelmet nem nyújthat be.

(6) A (4) bekezdés szerinti esetben, vagy ha az IoT-eszköz vonatkozásában kiállított megfelelőségi nyilatkozat érvényességi ideje lejárt, a gyártó az IoT-eszköz vonatkozásában a nemzeti megfelelőségi nyilatkozat megújítására irányuló kérelmet nyújthat be a tanúsító hatósághoz a tanúsító hatóság által e célra rendszeresített elektronikus űrlapon.

(7) A (6) bekezdés szerinti kérelemhez csatolni kell a 4. § (1)–(4) bekezdése szerinti vizsgálat alapján, a 4. § (5) bekezdése szerint kiállított új megfelelőségi nyilatkozatot, az 1. melléklet szerinti dokumentumokat és az értékelési jelentést.

(8) A (6) bekezdés szerinti megújítási eljárás ügyintézési határideje 45 nap.

(9) A (6) bekezdés szerinti kérelem alapján a tanúsító hatóság által nyilvántartásba vett új megfelelőségi nyilatkozat érvényességének fenntartására az (1)–(4) bekezdés alkalmazandó.

7. § (1) A megfelelőségértékelő szervezet által kiállított nemzeti kiberbiztonsági tanúsítvány alapján nyilvántartásba vett IoT-eszköz tanúsítványa érvényességi idejének meghosszabbítása érdekében a gyártó a megfelelőségértékelő szervezet rendelkezésére bocsátja az érvényességi idő lejártát megelőző 60 napon belül az 5. § (3) bekezdése szerinti biztonsági hatáselemzést és az 1. melléklet szerinti megvalósítási dokumentum 5. § (5) bekezdésének megfelelően frissített változatát.

(2) A megfelelőségértékelő szervezet az (1) bekezdés szerinti dokumentumok vizsgálata alapján – ha a vizsgált IoT-eszközben bekövetkezett változások mellett az IoT-eszköz a nemzeti kiberbiztonsági tanúsítvány kiállításától kezdődően folytatólagosan teljesíti a tanúsítási rendszerben foglalt követelményeket, és biztosítja a biztonsági célok megvalósulását – az érvényességi idő lejártát megelőző legkésőbb 8 napon belül a lejáró tanúsítványt meghosszabbítja, azzal, hogy az új érvényességi idő nem haladhatja meg az eredeti érvényességi idő végétől számított 365 napot.

(3) Ha az (1) bekezdés szerinti dokumentumok alapján nem állapítható meg az, hogy a vizsgált IoT-eszköz a nemzeti kiberbiztonsági tanúsítvány kiállításától kezdődően folytatólagosan teljesíti a tanúsítási rendszerben foglalt követelményeket, és biztosítja a biztonsági célok megvalósulását, a megfelelőségértékelő szervezet a lejáró tanúsítványt azzal a feltétellel hosszabbíthatja meg, hogy az új érvényességi idő nem haladhatja meg az eredeti érvényességi idő végétől számított 90 naptári napot.

(4) A (3) bekezdés szerinti esetben az érintett IoT-eszköz vonatkozásában kiállított nemzeti kiberbiztonsági tanúsítvány érvényességi ideje a (3) bekezdés szerinti új érvényességi idő lejártát követően nem hosszabbítható meg, hanem annak megújítása kezdeményezhető.

(5) A gyártó az IoT-eszköz nemzeti kiberbiztonsági tanúsítványának megújítását a megfelelőségértékelő szervezetnél a (3) bekezdés szerinti esetben vagy akkor kezdeményezheti, ha a nemzeti kiberbiztonsági tanúsítvány érvényességi ideje lejárt.

(6) A megfelelőségértékelő szervezet a megújítás keretében az IoT-eszközre vonatkozóan – a 4. § (1)–(4) bekezdése szerinti vizsgálat alapján, a 4. § (5) bekezdése szerint – kiállított új nemzeti kiberbiztonsági tanúsítványt, továbbá az 1. melléklet szerinti dokumentumokat és az értékelési jelentést a tanúsító hatóság által e célra rendszeresített elektronikus űrlapon nyilvántartásba vételre benyújtja.

8. § A nemzeti tanúsítvány érvényességi idejét nem érinti, ha az érvényességi idő alatt az IoT-eszköz tekintetében a 2. § (2) bekezdése szerint új nemzeti kiberbiztonsági tanúsítási rendszer kerül meghatározásra, de ezt követően az IoT-eszköz nemzeti tanúsítványának érvényességi ideje nem hosszabbítható meg, arra fenntartási kérelem nem nyújtható be, és a nemzeti tanúsítvány nem újítható meg.

9. § Ez a rendelet a kihirdetését követő 3. napon lép hatályba.

10. § E rendelet tervezetének a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról szóló, 2015. szeptember 9-i (EU) 2015/1535 európai parlamenti és tanácsi irányelv 5–7. cikke szerinti előzetes bejelentése megtörtént.

Dr. Nagy László s. k.,
elnök

1. melléklet a 10/2024. (VIII. 8.) SZTFH rendelethez

Dokumentációs követelmények

1. IoT-eszköz azonosító dokumentum

1.1. A megfelelőségi önértékelés vagy megfelelőségértékelési vizsgálat alá vont IoT-eszköz (a továbbiakban: VE) azonosítására szolgáló információkat tartalmazó dokumentum, amely a lehető legrészletesebb információkat tartalmazza a vizsgálat tárgyáról, kiemelten a verziószámok és a konfigurációs lehetőségek tekintetében.

1.2. Az azonosító dokumentum minimális tartalmi elemei:

a) Vizsgált termék megnevezése
b) Márka megjelölése
c) Kereskedelmi forgalomban használt név
d) Modellazonosító
e) Hardverkonfiguráció (beleértve a kiadási számot és a sorozatszámot)
f) Futtatókörnyezet vagy operációs rendszer
g) Firmware verzió gyári állapotban
h) Gyártó adatai:
   ha) megnevezése
   hb) rövid neve
   hc) székhelye
   hd) telefonszáma
   he) e-mail-címe
   hf) kapcsolattartó személy adatai: neve, állampolgársága, telefonszáma, e-mail-címe
i) A VE tervezett éves gyártási darabszáma
j) Annak megjelölése, hogy a vizsgált eszköz mely kereskedelmi piacokon kerül értékesítésre várhatóan a következő 1 évben:
   ja) csak Magyarország
   jb) EU-tagállamok (ha nem a teljes EU területén, akkor a tagállamok felsorolása) vagy
   jc) egyéb
k) Annak megjelölése, hogy a vizsgálat milyen megbízhatósági szintnek megfelelően történik: alap/jelentős/magas

2. Megvalósítási dokumentum

2.1. A megvalósítási dokumentum (a továbbiakban: MD) az 1. pont szerint azonosított IoT-eszköz megvalósítása során alkalmazott, a 2. melléklet szerinti követelmények értékelése szempontjából lényeges, részletes információkat tartalmazza.

2.2. Az MD minimális tartalmi elemei

2.2.1. MD 1-UserInfo: Felhasználói információk

Az MD felsorolja a dokumentációkat, kiadványokat és a felhasználóknak nyújtott információkat. Ide sorolandó mind a gyártó weboldala és a megfelelő URL, a felhasználói kézikönyv vagy a beépített súgó. A lista a következő egymástól független funkciók, mechanizmusok működése kapcsán elérhető információkat tartalmazza:

	A	B
1.	A módosítási mechanizmusok dokumentálása	A hitelesítési értékek módosítási mechanizmusainak dokumentálása a felhasználó számára, beleértve a dokumentációhoz való hozzáféréshez szükséges összes információt.
2.	Az érzékelők dokumentációja	A külső érzékelési képességekkel kapcsolatos információknak a felhasználó számára való dokumentálása, beleértve a dokumentációhoz való hozzáféréshez szükséges összes információt.
3.	A biztonságos beállítás dokumentációja	A VE biztonságos beállítása felhasználói dokumentációjának módszere, beleértve dokumentációhoz való hozzáféréshez szükséges összes információt.
4.	A beállítási ellenőrzés dokumentációja	Annak leírása, hogy a felhasználó számára hogyan dokumentálják a VE biztonságos beállításának ellenőrzésére szolgáló módszert, beleértve a dokumentációhoz való hozzáféréshez szükséges összes információt.
5.	A személyes adatok dokumentálása	A személyes adatok feldolgozására vonatkozó információknak a felhasználó számára történő dokumentálási módja, beleértve a dokumentációhoz való hozzáféréshez szükséges összes információt.
6.	A telemetriai adatok dokumentálása	A telemetriai adatok gyűjtésével kapcsolatos információknak a felhasználó számára történő dokumentálási módja, beleértve a dokumentációhoz való hozzáféréshez szükséges összes információt.
7.	A törlés dokumentálása	A személyes adatok törlési módjának a felhasználó számára történő leírása, beleértve a dokumentációhoz való hozzáféréshez szükséges összes információt.
8.	Modell megnevezése	A VE modell megjelölése és annak rövid leírása, hogy a VE modellmegjelölését a felhasználó hogyan ismerheti fel. Itt kell megadni, ha hálózati lekérdezéssel is lekérdezhető a VE és szoftverkomponensei verziószáma, illetve, hogy az milyen módon történik. Itt kell jelölni nyílt forráskódú szoftverek használata esetén a nyílt forráskódú operációs rendszerek rendszermagjainak és alkalmazásainak verzióit, illetve azt, hogy az rendelkezik hosszú távú támogatási (LTS) idővel.
9.	Támogatási időszak	Az az időtartam, amely alatt a terméket vagy szolgáltatást a gyártó karbantartja, pl. frissítések formájában, ideértve a nyílt forráskódú operációs rendszerek rendszermagjainak és alkalmazásainak verzióit.
10.	A támogatási időszak közzététele	A támogatási időszak közzétételének és dokumentálásának módja a felhasználó számára, beleértve a közzétételhez való hozzáférés összes információját.

11.	A sebezhetőség közzététele	A sebezhetőségek közzétételének módja, beleértve a közzétételhez való hozzáférés összes információját.
12.	A nem frissíthető komponensek közzététele	A szoftverfrissítések hiánya indokolásának leírása, beleértve a közzétételhez való hozzáféréshez szükséges összes információt.

2.2.2. MD 2-SecDev: Biztonságos fejlesztési folyamatok

Az MD felsorolja az összes biztonságos fejlesztési folyamatot, amelyet a gyártó a VE-re vonatkozóan végrehajtott vagy végrehajtatott. Az MD a következő bejegyzéseket tartalmazza:

	A	B
1.	ID	Folyamatonként egyedi azonosító SecDev-1-gyel kezdődően.
2.	Leírás	A biztonságos fejlesztési folyamat rövid leírása. Ha egy meglévő szabványt használnak, akkor a megfelelő szabványra való hivatkozást kell megadni. Ki kell térni az alkalmazott programozási technikák ismertetésére annak igazolására, hogy az alkalmas a manipulációs, hibát, illetve információszivárgást előidéző (tampering, fault and leakage) támadások mérséklésére.

2.2.3. MD 3-VulnTypes: Releváns sebezhetőségek

Az MD felsorolja az összes olyan típusú sebezhetőséget, amely a VE szempontjából lényeges. Az MD a következő bejegyzéseket tartalmazza:

	A	B
1.	ID	Sebezhetőségenként egyedi azonosító VulnTypes-1-gyel kezdődően.
2.	Leírás	A VE szempontjából releváns sebezhetőség rövid leírása.
3.	Intézkedés	A sebezhetőség feltárása esetén az ilyen típusú sebezhetőséggel kapcsolatos intézkedés módjának leírása, beleértve az intézkedésben részt vevő összes szervezetet és felelősségüket.
4.	Időkeret	Célzott időkeret, amelyben a sebezhetőség esetén a cselekvés adott lépéseit ütemezik. Példa: 5 nap az első válaszadásra és 90 nap a javítás közzétételéig.

2.2.4. MD 4-Conf: Nyilatkozatok

Az MD felsorolja a folyamatok létrehozására vonatkozó nyilatkozatokat. Az MD a következő, egymástól független bejegyzéseket tartalmazza, amelyek kapcsán egyértelmű IGEN vagy NEM válaszokat kell jelölni.

	A	B
1.	A sebezhetőségi intézkedések megerősítése	Annak megerősítése, hogy az MD 3-VulnTypes-ban leírt minden egyes „Intézkedés" esetében a szükséges infrastruktúra rendelkezésre áll, és az üzemeltetők tájékoztatást kaptak a megcélzott „Időkeret" elérése érdekében.
2.	A sebezhetőségi felügyelet megerősítése	Annak megerősítése, hogy az MD 5-VulnMonban leírt minden egyes sebezhetőség figyelemmel kíséréséhez, azonosításához és kijavításához a szükséges infrastruktúra rendelkezésre áll, és az üzemeltetők tájékoztatást kaptak.
3.	A frissítési eljárások megerősítése	Annak megerősítése, hogy az MD 6-UpdProc-ban leírt minden egyes frissítési eljáráshoz a szükséges infrastruktúra rendelkezésre áll, és az üzemeltetők tájékoztatást kaptak a célzott „Időkeret" elérése érdekében.

4.	A biztonságos irányítás megerősítése	Annak megerősítése, hogy az MD 15-SecMgmt dokumentumban leírt biztonságos irányítási folyamatokat létrehozták.
5.	A biztonságos fejlesztés megerősítése	Annak megerősítése, hogy az MD 2-SecDevben leírt biztonságos fejlesztési folyamatokat létrehozták.

2.2.5. MD 5-VulnMon: Sebezhetőség monitorozás

Az MD felsorolja a sebezhetőségek ellenőrzésére, azonosítására és kijavítására szolgáló összes eljárást, a következő bejegyzéseket tartalmazza.

	A	B
1.	ID	Eljárásonként egyedi azonosító VulnMon-1-gyel kezdődően.
2.	Leírás	A termékek és szolgáltatások biztonsági rései nyomon követésének, azonosításának és kijavításának leírása.

2.2.6. MD 6-UpdProc: Frissítési eljárások

Az MD felsorolja a gyártó eljárásait a biztonsági frissítések kiadására vonatkozóan a következő adatokkal:

	A	B
1.	ID	Eljárásonként egyedi azonosító UpdProc-1-gyel kezdődően.
2.	Leírás	A biztonsági frissítések kiadására vonatkozó eljárás rövid leírása, beleértve az összes szervezetet és felelősséget.
3.	Időkeret	Az eljárás befejezésének tervezett időkerete.

2.2.7. MD 7-Intf: Interfészek

Az MD a VE összes hálózati, fizikai és logikai interfészét felsorolja a következő paraméterekkel:

	A	B
1.	ID	Interfészenként egyedi azonosító Intf-1-gyel kezdődően.
2.	Leírás	Az interfész leírása, beleértve annak célját is. Fizikai interfészek esetében azt is le kell írni, hogy az interfészre mindig szükség van-e, vagy csak bizonyos, a leírásban kifejtett esetekben (pl. időszakos használat), illetve azt is, ha arra soha nincs szükség.
3.	Típus	Annak jelzése, hogy az interfész hálózati, fizikai (beleértve a vezeték nélküli interfészeket is), logikai vagy többféle típusú.
4.	Állapot	Annak jelzése, hogy az interfész engedélyezve vagy letiltva van az inicializált állapotban. Engedélyezett interfészek esetén indokolás szükséges.
5.	Állapotváltozás	Az interfész állapotainak listája, azzal, hogy az állapotváltozásokat milyen módon és milyen szerepkörű felhasználó – hivatkozva az MD 9-Role szerinti szerepkörre – idézheti elő.
6.	Kapcsolat felépítése	Annak a leírása, hogy az interfész a kapcsolatot milyen módon építi fel, milyen validálási és hitelesítési mechanizmusokat használ, utóbbi esetén hivatkozva az MD-10-Auth szerinti hitelesítési mechanizmusra.
7.	Közzétett információk	Ha az interfész hálózati interfész: az inicializált állapotban hitelesítés nélkül nyilvánosságra hozott információk leírása és a nyilvánosságra hozatal oka, továbbá annak feltüntetése, hogy a nyilvánosságra hozatal információbiztonsági szempontból releváns-e.
8.	Hibakeresési interfész	Ha az interfész fizikai interfész: az interfész használható-e hibakeresési interfészként.

9.	Védelem	Ha az interfész fizikai interfész: az interfész kitettségének korlátozásához szükséges védelmi módszerek leírása. A hibakeresési interfészek esetében elvárás az interfész letiltására használt szoftvermechanizmus leírása.

2.2.8. MD 8-DevID: Eszközazonosítók

Az MD-ben szerepeltetni kell a VE összes, az eszköz azonosítására szolgáló azonosítóját.

	A	B
1.	ID	Eszközazonosítónként egyedi azonosító DevID-1-gyel kezdődően.
2.	Azonosító típusa	Az azonosító formájára (címke, fizikai vagy logikai azonosító) és annak egyediségére vonatkozó információk.
3.	Azonosító hozzáférhetősége	Az azonosító az eszköz egyes állapotaiban (gyári csomagolt, gyári alapértelmezett és beüzemelt) milyen úton, milyen szerepkörrel rendelkező felhasználó által és milyen módon ismerhető meg. Ha az azonosító interfészen keresztül elérhető, hivatkozni szükséges az MD 7-Intf szerinti interfészre.
4.	Azonosító forrása	„Előre telepített" vagy „Felhasználó által hozzáadható".
5.	Azonosítógeneráló mechanizmus	Az azonosító generálására használt algoritmus rövid leírása, ismertetve azokat az intézkedéseket, amelyek kockázatarányosan biztosítják, hogy az azonosítók csökkentik a nyilvánvaló szabályszerűségeken, közös karakterláncokon, nyilvánosan elérhető információkon vagy nem megfelelő összetettségen alapuló automatikus támadások kockázatát.
6.	Műveletvégzés	Az azonosító ismeretében végrehajtható műveletek leírása és azok végrehajtásának módja, hivatkozással a műveletvégzésben érintett, az MD 7-Intf szerinti interfészekre.
7.	Biztonsági célok	A megvalósított biztonsági célok és a mechanizmus által elhárítandó fenyegetések leírása.
8.	Brute Force védelem	Ha az azonosító közvetlenül egy hálózati interfészről elérhető, az annak megakadályozására kialakított módszer leírása, hogy a támadó a hálózati interfészeken keresztül brute force támadással megszerezze az azonosító adatokat.
9.	Timing attack elleni védelem	Ha az azonosító közvetlenül egy hálózati interfészről elérhető, az annak megakadályozására kialakított módszer leírása, hogy a támadó időzítések kihasználásával szerezzen jogosulatlan felhatalmazást.

2.2.9. MD 9-Role: Szerepkörök

Az MD-ben szerepeltetni kell a VE által gyári állapotban kezelt szerepköröket, ideértve a nem azonosításkötelezett szereplőket és gép-gép közötti kapcsolatokat is.

	A	B
1.	ID	Szerepkörönként egyedi azonosító Role-1-gyel kezdődően.
2.	Leírás	A szerepkör rövid leírása.
3.	Cél	A szerepkörbe tartozó felhasználók általános célja.
4.	Műveletek	A szerepkörbe tartozó felhasználók által elvégezhető műveletek listája.

2.2.10. MD 10-AuthMech: Hitelesítési mechanizmusok

Az MD-ben szerepeltetni kell a VE összes hitelesítési mechanizmusát. Az MD a következő bejegyzéseket tartalmazza:

	A	B
1.	ID	Hitelesítési mechanizmusonként egyedi azonosító AuthMech-1-gyel kezdődően.
2.	Leírás	A hitelesítési mechanizmus és a hozzá tartozó engedélyezési folyamat rövid leírása. Meg kell adni, hogy a mechanizmust a felhasználó vagy a gép-gép közötti hitelesítésre használják-e, és hogy az közvetlenül egy hálózati interfészről érhető-e el. Harmadik feles megvalósítás esetén ismertetni kell, hogy az ellátási lánc tervezése miképpen akadályozza meg a VE-specifikus hitelesítő adatok kiszivárgását.
3.	Authentikációs faktor	A hitelesítéshez használt attribútum típusa. Jelszavak esetében azt is jelezni kell, hogy a jelszót a felhasználó állítja-e be, és használja-e az inicializált állapotban.
4.	Jelszógeneráló mechanizmus	Ha a hitelesítési tényező egy jelszó, amelyet nem a felhasználó állít be, a jelszó generálására szolgáló mechanizmus leírása, azzal, hogy részletes leírás nem szükséges. A leírásban meg kell adni, hogy a jelszó eszközönként egyedi-e, és hogy előre telepített-e, ismertetni kell azokat az intézkedéseket, amelyek biztosítják, hogy a jelszavak a gyári alapértelmezettől eltérő bármely állapotban eszközönként egyediek legyenek, és csökkentik a nyilvánvaló szabályszerűségeken, közös karakterláncokon, nyilvánosan elérhető információkon vagy nem megfelelő összetettségen alapuló automatikus támadások kockázatát, ha előre telepített és eszközönként egyedi jelszóként használják.
5.	Biztonsági garanciák	A megvalósított biztonsági célok és a mechanizmus által elhárítandó fenyegetések leírása.
6.	Kriptográfiai részletek	A kulcskezelés figyelembevételével a hitelesítési mechanizmus biztosítására és a leírt „biztonsági garanciák” megkönnyítésére használt kriptográfiai módszerek (protokollok, műveletek, primitívek, módok és kulcsméretek) leírása.
7.	Brute Force védelem	Ha a hitelesítési mechanizmus közvetlenül egy hálózati interfészről elérhető, annak megakadályozására kialakított módszer leírása, hogy a támadó a hálózati interfészeken keresztül brute force támadással megszerezze a hitelesítő adatokat.
8.	Timing attack elleni védelem	Ha a hitelesítési mechanizmus közvetlenül egy hálózati interfészről elérhető, az annak megakadályozására kialakított módszer leírása, hogy a támadó időzítések kihasználásával szerezzen jogosulatlan felhatalmazást.
9.	Testreszabás	A hitelesítési mechanizmushoz kapcsolódó beállítási lehetőségek.
10.	Alkalmazás	A hitelesítési mechanizmust használó interfészek és felhasználók szerepköre, hivatkozással az MD 7-Intf szerinti interfészekre és MD 9-Role szerepkörökre.
11.	Kezelés	A hitelesítő azonosító megváltoztatása folyamatának leírása.

2.2.11. MD 11-Account: Fiókkezelés

Az MD-ben szerepeltetni kell a felhasználói fiókok kezeléséhez kapcsolódó megoldásokat.

	A	B
1.	ID	Műveletenként és megoldásonként egyedi azonosító Account-1-gyel kezdődően.
2.	Művelet	Művelet megnevezése.
3.	Leírás	A megvalósított művelet mechanizmusának részletes leírása.
4.	Konfiguráció	Annak leírása, hogy a fiókkezelési műveletben milyen adatok konfigurálhatóak és milyen MD 9-Role szerinti szerepkörrel rendelkező felhasználók számára.

2.2.12. MD 12-SoftComp: Szoftverkomponensek

Az MD a VE összes szoftverkomponensét felsorolja. Az alkalmazott részletezettségi szint a vizsgált szoftver szoftverkomponensekre való felosztására vonatkozóan azt a célt szolgálja, hogy esetleges sérülékenységvizsgálat esetén azonosítani lehessen, hogy mely komponensek frissíthetőek, és melyek nem. Az MD a következő bejegyzéseket tartalmazza:

	A	B
1.	ID	Szoftverkomponensenként egyedi azonosító SoftComp-1-gyel kezdődően.
2.	Leírás	A szoftverkomponens rövid leírása. Külön jelezni kell, ha a szoftverkomponens frissítése érzékeny adatot tartalmaz.
3.	Frissítési mechanizmus	Hivatkozás az MD 13-UpdMech frissítési mechanizmusaira, amelyeket a szoftverkomponens frissítésére használnak. A frissítési mechanizmusok üres listája a szoftverkomponens frissítésének hiányát jelzi, amelynek elmaradását indokolni szükséges.
4.	Kriptográfiai felhasználás	Jelzi, hogy a szoftverkomponens használ-e kriptográfiai algoritmusokat vagy primitíveket (igen/nem), és ha igen, akkor azt is tartalmazza, hogy a gyártó figyelembe vette-e ezen algoritmusok és a primitívek frissítésének mellékhatásait (igen/nem).

2.2.13. MD 13-UpdMech: Frissítési mechanizmusok

Az MD felsorolja a VE összes frissítési mechanizmusát, amelyek kapcsán a következő bejegyzéseket tartalmazza:

	A	B
1.	ID	Frissítési mechanizmusonként egyedi azonosító UpdMech-1-gyel kezdődően.
2.	Leírás	A frissítési mechanizmus rövid leírása, beleértve annak főbb jellemzőit. Ezenkívül meg kell adni, hogy a frissítés kézbesítése hálózati alapú-e.
3.	Biztonsági garanciák	A megvalósított biztonsági célkitűzések és a mechanizmus által elhárítandó fenyegetések leírása. A hitelesség és az integritás érdekében ezenfelül azt is fel kell tüntetni, hogy a biztonsági garanciát maga a VE adja-e.
4.	Kriptográfiai részletek	A kulcskezelést figyelembe vevő frissítési mechanizmus biztonságának biztosítására és a leírt „Biztonsági garanciák” megkönnyítésére használt kriptográfiai módszerek (protokollok, műveletek, primitívek, módok és kulcsméretek) leírása. Az ellenőrzésre használt nyilvános kulcsok telepítésének módja.

5.	Kezdeményezés és interakció	A frissítéskezdeményezés módjának, valamint a frissítés kezdeményezéséhez és alkalmazásához szükséges felhasználói interakció rövid leírása, jelezve, hogy automatikus frissítési mechanizmusról van-e szó.
6.	Konfiguráció	Rövid leírás arról, hogy a felhasználó hogyan konfigurálhatja a szoftverfrissítések automatizálását és értesítését, és milyen lehetőségek (pl. engedélyezés, letiltás, elhalasztás) közül választhat. Az alapértelmezett konfigurációt is itt kell megadni.
7.	Frissítés ellenőrzése	A biztonsági frissítések elérhetősége lekérdezési mechanizmusának és ütemezésének rövid leírása, továbbá annak rögzítése, hogy a biztonsági frissítés elérhetőségének ellenőrzését maga a VE végzi-e.
8.	Felhasználói értesítés	Rövid leírás arról, hogy a felhasználót hogyan tájékoztatják az elérhető frissítésről és a frissítési mechanizmus által okozott zavarokról, pl. bizonyos funkciók korlátozott elérhetőségéről, megjelölve, hogy az értesítés milyen információkat tartalmaz, és hogy az értesítést maga a VE valósítja-e meg.
9.	Verziókezelés	Rövid leírás arról, hogy a VE miként ellenőrzi és érvényesíti a frissítés verzióját a telepítés előtt.

2.2.14. MD 14-SecParam: Biztonsági paraméterek

Az MD felsorolja az összes olyan érzékeny (nyilvános és kritikus) biztonsági paramétert, amelyet a rendeltetésszerű használat során tartósan tárolnak a VE-n, az alábbi paraméterekkel:

	A	B
1.	ID	Paraméterenként egyedi azonosító SecParam-1-gyel kezdődően.
2.	Leírás	A biztonsági paraméter rövid leírása, beleértve annak célját is, megjelölve, hogy az adott biztonsági paraméter az eszközben biztonsági célokra használt, hard kódolt egyedi eszközönkénti azonosító, illetve az eszköz szoftverének forráskódjában hard kódolt.
3.	Tárolás helye	A biztonsági paraméter tárolásának helye és módja.
4.	Típus	Annak rögzítése, hogy a biztonsági paraméter nyilvános vagy kritikus.
5.	Biztonsági garanciák	A megvalósított alapvető biztonsági célkitűzések és a fenyegetések leírása, amelyekkel szemben a biztonsági paraméter a tartós tárolás során védelmet élvez.
6.	Védelmi rendszer	A biztonsági garanciák elérése érdekében alkalmazott intézkedések leírása, ideértve azokat a felhatalmazásokat és szerepköröket, amelyeken keresztül a paraméterhez való hozzáférés lehetséges, továbbá az egyes szerepkörökhöz kapcsolódó jogosultságokat.
7.	Elosztási mechanizmus	Ha a „Típus" azt jelzi, hogy a paraméter kritikus: annak a mechanizmusnak a leírása, amelyen keresztül a paraméter értéket kap.
8.	Kommunikációs mechanizmusok	Hivatkozás az MD 16-ComMech-ben a paraméterek közlésére használt kommunikációs mechanizmusokra és annak feltüntetése, hogy a kommunikáció távolról elérhető interfészeken keresztül történik-e.

9.	Létrehozási mechanizmus	Ha a „Típus" azt jelzi, hogy a paraméter kritikus, vagy a szoftverfrissítések integritásának és hitelességének ellenőrzésére vagy a kapcsolódó szolgáltatásokkal való kommunikáció védelmére használják: a paraméter értékeinek létrehozására használt mechanizmus leírása és ezenfelül annak feltüntetése, hogy a paramétert a szoftverfrissítések integritásának és hitelességének ellenőrzésére vagy a kapcsolódó szolgáltatásokkal való kommunikáció védelmére használják.

2.2.15. MD 15-SecMgmt: Biztonságos irányítási folyamatok

Az MD felsorolja a kritikus biztonsági paraméterekre vonatkozó összes biztonságos kezelési folyamatot, amelyet a gyártó megvalósított a VE életciklusa során.

	A	B
1.	ID	Folyamatonként egyedi azonosító SecMgmt-1-gyel kezdődően.
2.	Leírás	A biztonságos kezelési folyamat rövid leírása a kritikus biztonsági paraméterek teljes életciklusára vonatkozóan egy meglévő szabvány használata esetén a megfelelő szabványra való hivatkozás megadásával. A kritikus biztonsági paraméterek életciklusa jellemzően a generálást, a rendelkezésre bocsátást, a tárolást, a frissítéseket, a kivonást, az archiválást, a megsemmisítést, a lejáratot kezelő folyamatokat és a paraméter veszélyeztetettségét veszi figyelembe. A generálás során a felhasznált véletlenszámok előállításának, annak entrópiájának mérési módját is ismertetni kell. Ha fájl-integritásellenőrzést alkalmaz az eszköz, annak módját is ismertetni kell.

2.2.16. MD 16-ComMech: Kommunikációs mechanizmusok

Az MD felsorolja a VE összes kommunikációs mechanizmusát a következő részletes információkkal:

	A	B
1.	ID	Mechanizmusonként egyedi azonosító ComMech-1-gyel kezdődően.
2.	Leírás	A kommunikációs mechanizmus rövid leírása, beleértve a célját és a használt protokoll leírását. Szabványosított protokollok esetén elegendő egy hivatkozás verziószámmal. Ezenkívül fel kell tüntetni, hogy a mechanizmus távolról elérhető-e.
3.	Biztonsági garanciák	A megvalósított biztonsági célkitűzések és a mechanizmus által elhárítandó fenyegetések leírása.
4.	Kriptográfiai részletek	A kommunikációs mechanizmus biztosításához használt kriptográfiai módszerek (protokollok, műveletek, primitívek, módok és kulcsméretek) leírása a kulcskezelés figyelembevételével, a leírt „Biztonsági garanciák" céljainak elérése érdekében.
5.	Ellenállási intézkedések	Az intézkedések leírása, amelyek biztosítják, hogy a kapcsolat létrehozása rendezett módon történik, beleértve a stabil kapcsolat elérését eredményező, elvárt, működőképes és stabil állapotot.

2.2.17. MD 17-NetSecImpl: Hálózati és biztonsági megvalósítások

Az MD felsorolja a VE hálózati és biztonsági funkcióinak összes megvalósítását.

	A	B
1.	ID	Elemenként egyedi azonosító NetSecImpl-1-gyel kezdődően.
2.	Leírás	A hálózati vagy biztonsági funkció megvalósításának rövid leírása, beleértve a célját és a hatókörét.
3.	Felülvizsgálati/értékelési módszer	A végrehajtás felülvizsgálatára vagy értékelésére alkalmazott módszer leírása, beleértve az alapelveket is (pl. audit, szakértői értékelés, automatikus kódelemzés), és a módszer által lefedett megvalósítás hatókörének ismertetése.
4.	Jelentés	A felülvizsgálat vagy értékelés eredménye vagy hivatkozás a tanúsítványra vagy az értékelő jelentésre, amely bizonyítja, hogy a végrehajtást sikeresnek értékelték.

2.2.18. MD 18-SoftServ: Szoftverszolgáltatások

Az MD felsorolja a VE összes szoftverszolgáltatását a következők szerint:

	A	B
1.	ID	Szolgáltatásonként egyedi azonosító SoftServ-1-gyel kezdődően.
2.	Leírás	A szolgáltatás rövid leírása, beleértve annak célját, feltüntetve, hogy a szolgáltatás elérhető-e és mely MD 7-Intf szerinti hálózati interfészen keresztül, és azt, hogy ez az inicializált állapotban is így van-e.
3.	Állapot	Annak jelzése, hogy a szolgáltatás engedélyezett vagy letiltott az inicializált állapotban.
4.	Indokolás	Ha a szolgáltatás engedélyezett, annak indokolása, hogy a szolgáltatás miért szükséges a VE rendeltetésszerű használatához vagy működéséhez.
5.	Konfiguráció	Ha a szolgáltatás hálózati interfészen keresztül elérhető: tájékoztatás arról, hogy a szolgáltatás lehetővé teszi-e a konfiguráció biztonsági szempontból fontos módosítását, és ha igen, a lehetséges konfiguráció rövid leírása. Harmadik feles szoftverkomponens esetén nyilatkozat a szolgáltatás alapértelmezés szerinti tiltásáról.
6.	Hitelesítési mechanizmus	Ha a szolgáltatás hálózati interfészen keresztül elérhető: hivatkozás az MD 10-AuthMech-ben a hitelesítési mechanizmusokra, amelyeket a szolgáltatás használata előtti hitelesítésre használnak.
7.	Harmadik feles SW	Annak jelölése, hogy a szoftverkomponens harmadik féltől származik-e. Ha igen, akkor az elkülönítésre vonatkozó eljárás leírása.

2.2.19. MD 19-CodeMin: Kódminimalizálás

Az MD felsorolja a kódok minimalizálására alkalmazott módszereket.

	A	B
1.	ID	Módszerenként egyedi azonosító CodeMin-1-gyel kezdődően.
2.	Leírás	A kódnak a szükséges funkcionalitásra való minimalizálására használt módszer rövid leírása.

2.2.20. MD 20-PrivlCtrl: Jogosultságszabályozás

Az MD felsorolja az összes jogosultságszabályozási mechanizmust a következők szerint:

	A	B
1.	ID	Mechanizmusonként egyedi azonosító PrivlCtrl-1-gyel kezdődően.
2.	Leírás	A VE-n lévő szerepkörök és szoftverek jogosultságainak ellenőrzésére szolgáló mechanizmus rövid leírása.
3.	Mátrix	Az adott jogosultság-ellenőrző mechanizmus által kezelt jogosultsági mátrix.
4.	Hitelesítés	Az adott jogosultság-ellenőrző mechanizmus által elvárt hitelesítési mechanizmusra való hivatkozás.

2.2.21. MD 21-AccCtrl: Hozzáférés-védelem

Az MD felsorolja a memóriához való hozzáférés-védelmi mechanizmusokat hardveres szinten a következők szerint:

	A	B
1.	ID	Mechanizmusonként egyedi azonosító AccCtrl-1-gyel kezdődően.
2.	Leírás	A hardverszintű hozzáférés-szabályozási mechanizmus rövid leírása, amely tartalmazza azt is, hogy a VE operációs rendszere hogyan támogatja azt.

2.2.22. MD 22-SecBoot: Biztonságos rendszerindítási mechanizmusok

Az MD felsorolja a VE összes biztonságos indítási mechanizmusát a következők szerint:

	A	B
1.	ID	Mechanizmusonként egyedi azonosító SecBoot-1-gyel kezdődően.
2.	Leírás	A VE biztonságos indítási folyamatához használt mechanizmus rövid leírása (beleértve a biztonsággal kapcsolatos feltételezéseket) és a szoftver védett részének azonosítása. Külön ki kell térni mindazon vezérlési lehetőségekre, API-hívásokra, amelyek a mechanizmus működését befolyásolják. Ha a VE alkalmaz biztonsági másolatot a védett szoftverről, annak használati módja is a leírás része.
3.	Biztonsági garanciák	A mechanizmus megvalósított biztonsági célkitűzéseinek leírása. A mechanizmusok az operációs rendszerek rendszermagjának hitelességét és integritását valósítják meg.
4.	Érzékelési mechanizmusok	A VE szoftverének jogosulatlan módosítását észlelő mechanizmus leírása.
5.	Felhasználói értesítés	Rövid leírás arról, hogy hogyan értesül a felhasználó a szoftver jogosulatlan módosításáról, kiegészítésként feltüntetve, hogy az értesítés milyen információkat tartalmaz.
6.	Értesítési funkciók	A felhasználó értesítéséhez szükséges hálózati funkciók rövid leírása.

2.2.23. MD 23-Store: Tárolás és visszaállítás

Az MD felsorolja, hogy a VE által kezelt adatok milyen módon kerülnek tárolásra, illetve az adatok visszaállíthatóságának módját a következők szerint:

	A	B
1.	ID	Tárolási módonként egyedi azonosító Store-1-gyel kezdődően.
2.	Tároló	A VE által kezelt adatok tárolásának módja és helye.
3.	Redundancia	A tárolási mechanizmusban bekövetkező hiba esetén annak pótmechanizmusa.
4.	Az adatok visszaállításának módja	Az elsődleges tároló vagy a VE meghibásodása esetén a korábbi adatok visszaállításának módja.
5.	Titkosítás	A tárolón alkalmazott titkosítási algoritmus, feltüntetve, hogy gyári alapértelmezett állapotban a titkosítás engedélyezett-e, továbbá hogy a titkosított tárolás milyen módon és milyen szerepkörrel rendelkező felhasználó által állítható be.

2.2.24. MD 24-DataSec: Adatvédelem

Az MD felsorolja a VE által feldolgozott összes adatot – a telemetriaadatok kivételével – a következők szerint:

	A	B
1.	ID	Adatonként egyedi azonosító DataSec-1-gyel kezdődően.
2.	Leírás	A VE által feldolgozott adatok kategóriájának rövid leírása. Személyes adat bármely azonosított vagy azonosítható, természetes személyre vonatkozó információ.
3.	Feldolgozási tevékenységek	Az adatok feldolgozásának leírása, ismertetve az összes érintett felet, továbbá annak leírása, hogy milyen célból történik az adatfeldolgozás.
4.	Kommunikációs mechanizmusok	Hivatkozás az adatok közlésére használt MD 16-ComMech kommunikációs mechanizmusokra, valamint annak feltüntetése, hogy a kommunikációs partner társított szolgáltatás-e (igen/nem). A kommunikációs mechanizmusok üres listája azt jelzi, hogy az adatokat nem továbbítják.
5.	Érzékenység	Annak jelzése, hogy az adatok érzékeny adatok-e. Érzékeny adat az az adat, amelynek nyilvánosságra hozatala nagy valószínűséggel kárt okozhat az érintettnek. Az, hogy mi minősül érzékeny adatnak, termékenként és felhasználási esetenként eltérő lehet, de példaként említhetőek a fizetési információk, kommunikációs adatok tartalma és az időbélyegzővel ellátott helymeghatározási adatok.
6.	Hozzájárulás megszerzése	Ha a személyes adatok feldolgozása az érintett hozzájárulása alapján történik: annak leírása, hogy a hozzájárulás megszerzése hogyan történik.
7.	A hozzájárulás visszavonása	Ha a személyes adatok feldolgozása az érintett hozzájárulása alapján történik: leírás arról, hogy az érintett hogyan vonhatja vissza a személyes adatok feldolgozásához adott hozzájárulását.
8.	Kriptográfiai védelem	A személyes adatok védelme érdekében alkalmazott kriptográfiai algoritmus MD 12-SoftComp hivatkozással.
9.	Tároló	Az adatokat tároló MD 23-Store szerinti tároló(k).

2.2.25. MD 25-ExtSens: Külső érzékelők

Az MD felsorolja a VE összes külső érzékelési képességét a következők szerint:

	A	B
1.	ID	Érzékelőnként egyedi azonosító ExtSens-1-gyel kezdődően.
2.	Leírás	Az érzékelési képesség rövid leírása.

2.2.26. MD 26-ResMech: Ellenálló képességi mechanizmusok

Az MD felsorolja az összes ellenálló képességi mechanizmust a VE hálózati kapcsolatának megszakadására vagy áramkimaradás esetére a következők szerint:

	A	B
1.	ID	Mechanizmusonként egyedi azonosító ResMech-1-gyel kezdődően.
2.	Leírás	Annak az ellenálló képességi mechanizmusnak a leírása, amely hozzájárul a VE ellenálló képességéhez a hálózati, illetve áramkimaradásokkal szemben.
3.	Típus	Az ellenálló képességi mechanizmus a hálózati kapcsolat megszakadására, az áramkimaradás esetére vagy mindkettő kezelésére szolgál.
4.	Biztonsági garanciák	A megvalósított biztonsági célok és a mechanizmus által elhárítandó fenyegetések leírása.

2.2.27. MD 27-TelData: Telemetriai adatok

Az MD a VE által gyűjtött összes telemetriai adatot felsorolja a következők szerint:

	A	B
1.	ID	Adatonként egyedi azonosító TelData-1-gyel kezdődően.
2.	Leírás	A VE által gyűjtött és a gyártónak szolgáltatott telemetriai adatok rövid leírása.
3.	Cél	Rövid leírás arról, hogy milyen célból gyűjtik az adatokat.
4.	Biztonsági vizsgálat	Ha az adatokat biztonsági vizsgálatra használják, annak leírása, hogy a telemetriai adatokat hogyan és ki (eszköz vagy kapcsolódó szolgáltatás) vizsgálja biztonsági rendellenességek szempontjából.
5.	Adatkapcsolatok	A telemetriai adatokban feldolgozott adatokra való hivatkozás az MD 24-DataSecben.

2.2.28. MD 28-DelFunc: Törlési funkciók

Az MD felsorolja a felhasználó adatainak összes törlési funkcióját a következők szerint:

	A	B
1.	ID	Törlési funkciónként egyedi azonosító DelFunc-1-gyel kezdődően.
2.	Leírás	A felhasználó adatainak törlésére használt funkció rövid leírása. Ha a „Céltípus” azt jelzi, hogy egy kapcsolódó szolgáltatásnak van címezve, a funkció által lefedett kapcsolódó szolgáltatást is fel kell tüntetni.
3.	Céltípus	Annak megjelölése, hogy a funkció az eszközön lévő felhasználói adatokra vagy a kapcsolódó szolgáltatásokban kezelt személyes adatokra vagy mindkettőre vonatkozik.
4.	Kezdeményezés és interakció	A törlési funkció elindításához és alkalmazásához szükséges felhasználói interakció rövid leírása.

5.	Megerősítés	Rövid leírás arról, hogy a felhasználó a törlési funkció alkalmazása után hogyan kap jelzést arról, hogy az érintett adatok törlésre kerültek.

2.2.29. MD 29-UserDec: Felhasználói döntések

Az MD felsorolja a telepítés és karbantartás során meghozandó összes döntést a következők szerint:

	A	B
1.	ID	Döntésenként egyedi azonosító UserDec-1-gyel kezdődően.
2.	Leírás	A felhasználó által a telepítési és karbantartási folyamatokon belül meghozandó döntések leírása, rögzítve a felhasználó telepítési vagy karbantartási folyamaton belüli szerepkörét is.
3.	Lehetőségek	A felhasználó által választható, biztonság szempontjából fontos opciók leírása és az alapértelmezett érték megjelölése.
4.	Döntés	Rövid leírás arról, hogy a döntéshozatal hogyan történik, rögzítve, hogy a döntést a végfelhasználó is megteheti-e.

2.2.30. MD 30-UserIntf: Felhasználói interfészek

Az MD felsorolja a VE összes olyan felhasználói felületét, amely lehetővé teszi a felhasználó általi bevitelt a következők szerint:

	A	B
1.	ID	Felületenként egyedi azonosító UserIntf-1-gyel kezdődően.
2.	Leírás	A felhasználó által történő adatbevitelt lehetővé tevő felhasználói felület céljának, funkciójának, beviteli mezőinek leírása, ismertetve azt is, hogy a felhasználó hogyan férhet hozzá a felülethez.
3.	Konfigurációs interfész	Annak rögzítése, hogy az interfész a VE konfigurációjára használható-e.
4.	Kommunikációs mechanizmus	Ha az interfész a VE konfigurációjára használható, akkor hivatkozás a kommunikációs mechanizmusokra az MD 16-ComMech-ben, amelyet az interfész védelmére használnak.

2.2.31. MD 31-ExtAPI: Külső API-k

Az MD felsorolja a VE összes API-ját, amely lehetővé teszi a külső forrásokból történő adatbevitelt a következők szerint:

	A	B
1.	ID	API-nként egyedi azonosító ExtAPI-1-gyel kezdődően.
2.	Leírás	A VE külső forrásból történő adatbevitelt lehetővé tevő API leírása. A külső API-kat jellemzően a gép-gép közötti kommunikációra használják.

2.2.32. MD 32-InpVal: Adatbeviteli érvényesítés

Az MD felsorolja a VE összes adatbeviteli érvényesítési módszerét a következők szerint:

	A	B
1.	ID	Módszerenként egyedi azonosító InpVal-1-gyel kezdődően.
2.	Leírás	A felhasználói felületeken keresztül bevitt vagy API-kon keresztül, illetve a hálózatok között a szolgáltatásokban és eszközökben továbbított adatok érvényesítésére szolgáló módszer leírása, beleértve a váratlan adatok kezelését. Meg kell adni azt is, hogy a módszer az adatbevitel forrásai közül melyeket célozza meg. Az adatbevitel érvényesítéséhez ellenőrizni lehet, hogy az adat megengedett típusú (formátum és szerkezet), megengedett értékű, megengedett számosságú vagy megengedett sorrendű.

2.2.33. MD 33-Notif: Értesítések

Az MD-ben szerepeltetni kell a felhasználói értesítések összes módját a következők szerint:

	A	B
1.	ID	Értesítési módonként egyedi azonosító Notif-1-gyel kezdődően.
2.	Értesítés módja	Annak leírása, hogy az értesítés mely, az MD 7-Intf szerinti interfészen jelenik meg és mely felhasználók számára.
3.	Értesítés kezelése	A felhasználó által elvégzendő műveletek az értesítés kapcsán.
4.	Tartalom	Az értesítések tartalmi elemei, ha konfigurálhatóak, akkor annak leírása, hogy milyen MD 9-Role szerinti szerepkörrel rendelkező felhasználó és milyen mélységben konfigurálhatja az adattartalmat.

2.2.34. MD 34-AuditLog: Naplóadatok

Az MD felsorolja a VE összes naplózási módszerét a következők szerint:

	A	B
1.	ID	Naplóelemenként egyedi azonosító AuditLog-1-gyel kezdődően.
2.	Leírás	A naplózási tevékenység hatóköre, a naplók tartalma.
3.	Biztonsági garanciák	A megvalósított alapvető biztonsági célkitűzések és a fenyegetések leírása, amelyekkel szemben a naplóadatok a tartós tárolás során védelmet élveznek.
4.	Védelmi rendszer	A biztonsági garanciák elérése érdekében alkalmazott intézkedések leírása, ismertetve azokat a felhatalmazásokat és szerepköröket, amelyeken keresztül a paraméterhez való hozzáférés lehetséges, beleértve az egyes szerepekhez kapcsolódó jogosultságokat.

3. Értékelést megalapozó dokumentum

3.1. A gyártó a tesztelendő VE vizsgált megbízhatósági szintje szempontjából a 2. melléklet szerint meghatározott követelményeknek való megfelelést megalapozó, értékelést megalapozó dokumentumot (a továbbiakban: ÉMD) állít ki.

3.2. A dokumentum tartalmazza a cél megbízhatósági szintre vonatkozó, 2. melléklet szerinti követelmények listáját, továbbá a következő adatokat:

a) gyártói besorolás: a gyártó nyilatkozata az adott követelmény teljesítése vonatkozásában. Értékei lehetnek:

aa) „Nem alkalmazható": akkor jelölhető, ha a VE vonatkozásában a követelmény nem értelmezhető, a VE fizikai kialakítása, tervezett funkciói és felhasználási területe a követelmény teljesítését nem teszi lehetővé.

ab) „Alkalmazható és teljesített": akkor jelölhető, ha a VE vonatkozásában a követelmény értelmezhető, és a VE a követelményt teljesíti;

b) teljesítés módja: „Alkalmazható és teljesített" jelölés esetén annak leírása, hogy a követelmény kapcsán az MD-ben szereplő mely komponensek érintettek, és azok a követelményt egyesével vagy együtt hogyan teljesítik;

c) indokolás: „Nem alkalmazható" jelölés esetén annak indokolása az összes körülményre tekintettel.

2. melléklet a 10/2024. (VIII. 8.) SZTFH rendelethez

Követelményrendszer

1. A biztonsági követelményrendszer tekintetében az 1. melléklet 1. pontja szerinti IoT-eszköz azonosító dokumentumban meghatározott eszköz által – megbízhatósági szintenként – teljesítendő követelményeket a C–E oszlop rögzíti.
2. A követelményrendszer a következő európai, illetve nemzeti szabványokra figyelemmel került kialakításra:
   a) ETSI EN 303 645 V2.1.1,
   b) NIST Special Publication 800-213A és
   c) NIST Special Publication 800-53 Revision 5.
3. Bármely oszlopban
   a) „–"-lel jelölt sorok a kontrollcsaládok elnevezését jelzik;
   b) „X" jelzi, hogy az adott sorban szereplő biztonsági követelmény teljesítése a C–E oszlop szerinti megbízhatósági szinten kötelező;
   c) „0" jelzi, hogy az adott sorban szereplő biztonsági követelmény teljesítése a C–E oszlop szerinti megbízhatósági szinten nem kötelező.

	A	B	C	D	E
1.	Azonosító	Leírás	alap	jelentős	magas
2.		ESZKÖZ AZONOSÍTÁSA	–	–	–
3.		Eszközazonosítás	–	–	–
4.	DEVID-1	Az IoT-eszköz modelljelölése egyértelműen felismerhető, akár az eszközön található címkén, akár egy fizikai interfészen keresztül.	X	X	X
5.	DEVID-2	Az IoT-eszköz egyedi, az eszközön található címkén vagy interfészen keresztül lekérdezhető logikai azonosítóval rendelkezik.	X	X	X
6.	DEVID-3	Távolról vezérelhető IoT-eszköz egyedi azonosítója és modelljelölése megállapítható.	X	X	X
7.	DEVID-4	Az IoT-eszköz lehetőséget biztosít egyedi fizikai azonosító hozzáadására, amelyhez az arra jogosult entitások hozzáférnek.	0	X	X
8.		Műveletvégzés	–	–	–

9.	DEVOP-1	Az IoT-eszköz képes olyan műveletek végrehajtására, amelyek az eszköz azonosítása alapján vagy a felhasználásával előfordulhatnak.	X	X	X
10.	DEVOP-2	Az IoT-eszköz képes különbséget tenni azonosított és nem azonosított felhasználók között.	X	X	X
11.	DEVOP-3	Nem jogosult felhasználó által az egyedi logikai IoT-eszközazonosító nem megismerhető.	0	X	X
12.	DEVOP-4	Az IoT-eszköz azonosító ismeretében az aktuális szoftververzió ellenőrizhető.	0	X	X
13.	DEVOP-5	A hálózati eszközök azonosítása és kezelése céljából az eszközazonosító felhasználható az IoT-eszköz felderítésére.	0	0	X
14.		Eszközazonosítás támogatása	–	–	–
15.	IDSUPP-1	Az IoT-eszköz képes arra, hogy más eszközök számára előzetesen azonosított entitásként hirdesse magát.	0	X	X
16.	IDSUPP-2	Más IoT-eszközök hitelességének ellenőrzése biztosított.	0	X	X
17.	IDSUPP-3	Az IoT-eszköz hálózati és távoli hálózati kapcsolat esetén az azonosított kapcsolat felépítése előtt kriptográfiai alapú, kétirányú azonosítást végez.	0	0	X
18.	IDSUPP-4	Az IoT-eszköz tanúsítványalapú azonosítást és hitelesítést támogat.	0	0	X
19.		ESZKÖZ KONFIGURÁCIÓJA	–	–	–
20.	DEVCONF-1	A logikai hozzáférési jogosultságok beállítására, az IoT-eszköz konfigurációjára – Külső kapcsolatok, interfész-kontroll követelményeknek megfelelően – csak privilegizált felhasználókon keresztül nyílik lehetőség.	X	X	X
21.	DEVCONF-2	Csak arra jogosult felhasználók konfigurálhatják az IoT-eszköz azonosítási házirendjét és a hozzáférési korlátozási listákat a Külső kapcsolatok, interfész-kontroll követelményekkel összhangban.	X	X	X
22.	DEVCONF-3	Csak arra jogosult felhasználók konfigurálhatják az IoT-eszköz logikai és fizikai interfészeit a Külső kapcsolatok, interfész-kontroll követelményekkel összhangban.	X	X	X
23.	DEVCONF-4	Feljogosított felhasználók konfigurálhatják az IoT-eszköz szoftverbeállításait.	X	X	X
24.	DEVCONF-5	Feljogosított felhasználók az IoT-eszközt gyári állapotára visszaállíthatják.	X	X	X
25.	DEVCONF-6	Feljogosított felhasználók az IoT-eszközt valamely korábbi – a gyáritól eltérő – biztonságos állapotára visszaállíthatják.	0	0	X
26.	DEVCONF-7	Az IoT-eszköz szervizelése, javítása alatt vagy után a korábbi konfigurációs állapot biztosított.	0	X	X
27.		ADATVÉDELEM	–	–	–
28.		Kriptográfiai támogatás	–	–	–
29.	CRYPT-1	Az IoT-eszköz megfelelő erősségű és hatékonyságú kriptográfiai algoritmust biztosít az adatok védelme érdekében.	X	X	X

30.	CRYPT-2	Az IoT-eszköz képes egyedi tanúsítványok érvényesítésére.	0	X	X
31.	CRYPT-3	Digitális aláírások ellenőrzése biztosított.	0	X	X
32.	CRYPT-4	Az IoT-eszköz képes Hash algoritmusok futtatására.	X	X	X
33.	CRYPT-5	A kriptográfiai algoritmusoknak és primitíveknek ajánlott verziókra frissíthetőek.	0	X	X
34.	CRYPT-6	Az eszköz forráskódja nem tartalmaz hard-coded kritikus biztonsági paramétereket.	0	X	X
35.	CRYPT-7	A szoftverfrissítések integritásának és hitelességének ellenőrzésére, valamint az eszközszoftverben a kapcsolódó szolgáltatásokkal folytatott kommunikáció védelmére használt kritikus biztonsági paraméterek eszközönként egyediek, és azokat olyan mechanizmussal állítják elő, amely csökkenti az automatizált támadások kockázatát.	X	X	X
36.		Kriptográfiai kulcsok támogatása	–	–	–
37.	CRYKEY-1	Az IoT-eszköz a kriptográfiai kulcsokat biztonságosan kezeli.	X	X	X
38.	CRYKEY-2	Az IoT-eszköz képes kulcspárok generálására.	X	X	X
39.	CRYKEY-3	Az IoT-eszköz a kriptográfiai kulcsokat biztonságosan tárolja.	X	X	X
40.	CRYKEY-4	Az IoT-eszköz a kriptográfiai kulcsok változtatását biztonságosan végzi.	X	X	X
41.	CRYKEY-5	Az IoT-eszköz a külső rendszerek által generált kriptográfiai kulcsokat ellenőrzi.	0	X	X
42.		Biztonságos tárolás	–	–	–
43.	SECSTR-1	Az IoT-eszköz a jelszavakat nem tárolja – ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hash érték tárolást – és nem továbbítja.	X	X	X
44.	SECSTR-2	Biztonságos tárolás engedélyezhető az IoT-eszközön vagy annak interfészén keresztül.	X	X	X
45.	SECSTR-3	Gyári állapotban az adatok biztonságos, titkosított tárolása engedélyezett.	X	X	X
46.	SECSTR-4	A személyes adatok védelme a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelettel (általános adatvédelmi rendelet) összhangban biztosított.	X	X	X
47.	SECSTR-5	Az IoT-eszköz – ideértve az adatok elérését biztosító felhőinfrastruktúrát is – csak az üzemszerű működéséhez szükséges mennyiségű adatot tárolja.	X	X	X
48.	SECSTR-6	Az IoT-eszköz az adatokat képes lokálisan titkosítottan tárolni.	X	X	X
49.	SECSTR-7	Az IoT-eszközhöz kapcsolódó távoli rendszerelemek (pl. felhő) az adatokat titkosítottan tárolják.	0	X	X

50.	SECSTR-8	Érzékeny biztonsági paraméterek perzisztens tárolóban tárolódnak.	0	X	X
51.	SECSTR-9	A rendszer- és felhasználói adatok külön partíciókon helyezkednek el.	0	X	X
52.	SECSTR-10	Az adatok biztonságos mentése biztosított.	0	X	X
53.	SECSTR-11	Az IoT-eszközön lokálisan tárolt felhasználói adatok egyszerűen, visszaállíthatatlanul törölhetőek.	X	X	X
54.	SECSTR-12	Az IoT-eszközhöz kapcsolódó távoli rendszerelemek által tárolt felhasználói adatok egyszerűen törölhetőek.	0	X	X
55.		Biztonságos adatátvitel	–	–	–
56.	SECDT-1	Az IoT-eszköz be- és kimeneti interfészein az adatáramlás biztonságos.	X	X	X
57.	SECDT-2	A biztonságos adatátvitel kriptográfiai algoritmusa konfigurálható.	0	X	X
58.	SECDT-3	Az IoT-eszköz rendelkezik a jogosulatlan hozzáférés és módosítás elleni védelemmel az adatkapcsolati közegben.	X	X	X
59.	SECDT-4	Az IoT-eszköz a továbbított és fogadott adatok integritását kriptográfiai megoldással ellenőrzi.	0	X	X
60.		LOGIKAI HOZZÁFÉRÉS AZ INTERFÉSZEKHEZ	–	–	–
61.		Azonosítás támogatása	–	–	–
62.	AUTH-1	Az IoT-eszköz támogat authentikációs metódusokat.	X	X	X
63.	AUTH-2	Az IoT-eszköz a kapcsolatok felépítéséhez – kiemelten a távoli kapcsolatok esetén – authentikációs metódus megkövetelésére képes.	X	X	X
64.	AUTH-3	Az IoT-eszköz többfaktoros hitelesítési metódust támogat meghatározott felhasználói kör esetén.	0	X	X
65.	AUTH-4	Ha az IoT-eszköz gyári alapértelmezett jelszavakat használ, azok eszközönként egyediek.	0	X	X
66.	AUTH-5	Az IoT-eszköz a gyári alapértelmezett jelszavak generálása során olyan generálási algoritmust alkalmaz, amely csökkenti az automata támadások kockázatát.	0	X	X
67.	AUTH-6	A használatban lévő hitelesítési mechanizmusnak megfelelő hitelesítő azonosító megváltoztatása egyszerűen biztosított a felhasználó számára.	X	X	X
68.	AUTH-7	Az IoT-eszköz a hitelesítési folyamat során az adatokat elrejti.	X	X	X
69.	AUTH-8	Az IoT-eszköz standardizált, egységes authentikációs metódust támogat (pl. SAML, OAuth2).	0	X	X
70.	AUTH-9	Az IoT-eszköz távoli elérés esetén az authentikációs adatokat műveletenként ellenőrzi.	0	0	X
71.	AUTH-10	Az IoT-eszköz a hitelesítési metódus feedbackjében található információk rejtett visszacsatolásával biztosítja, hogy a hitelesítési azonosítók illetéktelenek számára megismerhetővé, újrafelhasználhatóvá váljanak.	X	X	X
72.		Azonosítás konfigurációja	–	–	–
73.	IDENT-1	Az IoT-eszköz életciklusa során az authentikációs metódusok, szabályok és korlátozások beállíthatóak és változtathatóak.	0	X	X

74.	IDENT-2	Az IoT-eszköz a fiókkezelést automatizált módon támogatja.	0	0	X
75.	IDENT-3	A sikertelen azonosítási kísérletek száma konfigurálható, amely után az IoT-eszköz az adott felhasználót tiltja meghatározott, beállítható időtartam erejéig.	0	X	X
76.	IDENT-4	Az IoT-eszköz a sikertelen azonosítási kísérletek miatt tiltott felhasználói fiók visszaállítását alternatív azonosítási metódussal támogatja.	0	0	X
77.	IDENT-5	Az IoT-eszköz visszajelzést ad a legutolsó sikeres authentikáció időpontjáról.	0	X	X
78.	IDENT-6	Az IoT-eszköz az inaktív fiókok kijelentkeztetését támogatja, amelynek időtartama konfigurálható.	X	X	X
79.	IDENT-7	Az IoT-eszköz az ideiglenes felhasználói fiókokat konfigurálható módon, automatikusan tiltja.	0	X	X
80.	IDENT-8	Az IoT-eszköz a sikertelen belépési kísérleteket naplózza, amelyekről riport készíthető.	X	X	X
81.	IDENT-9	Az IoT-eszköz a sikertelen belépési kísérletek számát a következő sikeres bejelentkezés során jelzi a felhasználó számára.	0	X	X
82.	IDENT-10	Az IoT-eszköz a külső felhasználók és rendszerek authentikációját támogatja.	X	X	X
83.	IDENT-11	A felhasználói fiókok, külső felhasználók és rendszerek hozzáférése visszavonható, amely esetében az IoT-eszköz a fennálló kapcsolatot bontja.	0	X	X
84.	IDENT-12	Az IoT-eszköz támogatja fiókok lejárati dátumának beállítását, amely lejárati dátumon túl az érintett fiók tiltásáról gondoskodik.	0	X	X
85.		Felhasználók értesítése	–	–	–
86.	NOTIF-1	Az IoT-eszköz állapota ránézésre megállapítható státuszállapot-jelzők segítségével.	X	X	X
87.	NOTIF-2	Az IoT-eszköz kijelzőjén megjelenő információk konfigurálhatóak.	0	X	X
88.	NOTIF-3	Az IoT-eszköz képes a felhasználók számára (konfigurált módon) értesítéseket küldeni.	X	X	X
89.	NOTIF-4	Személyes adatokat tartalmazó, továbbá biztonsági értesítések teljes tartalma csak azonosítás után megismerhető, érzékeny adatok a figyelmeztető üzenetben nem jelennek meg.	0	X	X
90.	NOTIF-5	Az IoT-eszköz által kijelzett, küldött üzenetek tartalma konfigurálható.	0	X	X
91.	NOTIF-6	Ha a figyelmeztető üzenet az IoT-eszköz kijelzőjén jelenik meg, az IoT-eszköz biztosítja, hogy az üzenet felhasználói interakcióig a kijelzőn maradjon.	0	X	X
92.		Hozzáférés-kezelés támogatása	–	–	–
93.	ACCESS-1	Az IoT-eszköz a jogosulatlan műveleteknek ellenáll.	X	X	X
94.	ACCESS-2	Az IoT-eszköz képes a felhatalmazott felhasználók és folyamatok (pl. csatlakozó rendszerek) azonosítására.	X	X	X
95.	ACCESS-3	Az IoT-eszköz különbséget tesz a feljogosított és nem feljogosított felhasználók között.	X	X	X

96.	ACCESS-4	Bizonyos, az üzemeltető által meghatározható funkciók azonosítás nélkül elérhetőek.	X	X	X
97.		Szerepkörtámogatás és -kezelés	–	–	–
98.	ROLE-1	Az IoT-eszköz több típusú felhasználói fiók kezelésére képes.	X	X	X
99.	ROLE-2	Az IoT-eszköz elkülöníti legalább a következő típusú felhasználói fiókokat: személyhez kötött fiókok (általános és privilegizált), osztott privilegizált fiókok.	0	X	X
100.	ROLE-3	Az IoT-eszköz támogatja a felhasználói fiókok hozzáadását.	0	X	X
101.	ROLE-4	A felhasználói fiókokhoz szerepkörök rendelhetőek.	0	X	X
102.	ROLE-5	A felhasználói fiókok egyedi azonosítóval vannak ellátva.	0	X	X
103.	ROLE-6	Az IoT-eszköz szerepköralapú logikai hozzáférés-vezérlést végez.	0	X	X
104.	ROLE-7	Adminisztrátor felhasználó által a szerepkörökkel elérhető funkciók, folyamatok konfigurálhatóak.	0	X	X
105.	ROLE-8	A szerepkörök standardizált, egységes authorizációs metódusokkal kompatibilisek, a megfeleltetés konfigurálható (pl. LDAPS).	0	X	X
106.	ROLE-9	Adminisztrátor felhasználó által új szerepkör konfigurálható.	0	0	X
107.	ROLE-10	Alapértelmezetten a szerepkörök a legkisebb jogosultság elve mentén kerülnek kialakításra.	X	X	X
108.	ROLE-11	Az audit naplókhoz és biztonsági beállításokhoz való hozzáférés-kezelés konfigurációja támogatott.	0	X	X
109.	ROLE-12	Az IoT-eszköz az egyes felhasználótípusokhoz korlátozó feltételek megadására biztosít lehetőséget (pl. időalapú korlátozás, IP-korlát).	0	0	X
110.	ROLE-13	A szerepkörökhöz rendelt feljogosítók ellenőrzése a privilegizált funkciók és folyamatok elérésére irányuló felhasználói interakció esetén megtörténik.	0	0	X
111.	ROLE-14	Az egyes felhasználói fiókok esetén használt authentikációs metódusok konfigurálhatóak.	0	0	X
112.	ROLE-15	Osztott fiókok esetén konfigurálható fiókonként az egyidejű bejelentkezés engedélyezése (gyári állapotban tiltott).	0	X	X
113.	ROLE-16	Az IoT-eszköz képes előre beállított korlátozások érvényesítésére az eszköz használata során.	0	X	X
114.		Külső kapcsolatok, interfész-kontroll	–	–	–
115.	INTCTRL-1	Az IoT-eszköz külső, 3rd party rendszerekkel való kapcsolatát biztonságos metódussal biztosítja.	X	X	X
116.	INTCTRL-2	Az IoT-eszköz komponenseinek használata korlátozható (portok, funkciók, be- és kimeneti eszközök).	X	X	X
117.	INTCTRL-3	Azok a fizikai vagy logikai interfészek, amelyek nem szükségesek az IoT-eszköz működéséhez, tilthatóak.	X	X	X
118.	INTCTRL-4	Gyári alapértelmezett állapotban csak a telepítéshez, beüzemeléshez minimálisan szükséges logikai és fizikai interfészek engedélyezettek.	X	X	X

119.	INTCTRL-5	Gyári alapértelmezett állapotban az IoT-eszköz védelmet biztosít a biztonsági információk azonosítás nélküli kinyerése ellen.	X	X	X
120.	INTCTRL-6	A fizikai interfészeket a hardver szükségtelen kockázatnak nem teszi ki.	0	X	X
121.	INTCTRL-7	Az IoT-eszköz szolgáltatásainak használata korlátozható.	0	X	X
122.	INTCTRL-8	A menedzsment felület elérésének külső hozzáférése tiltható.	0	X	X
123.	INTCTRL-9	Az IoT-eszköz logikai interfészeinek elérése szabályozható.	X	X	X
124.	INTCTRL-10	Az IoT-eszköz vezeték nélküli kapcsolatot támogat, amelynek biztonságos és engedélyezett authentikációs protokollja konfigurálható.	X	X	X
125.	INTCTRL-11	Ha az IoT-eszköz rendelkezik debug interfésszel, az szoftveresen tiltott.	0	X	X
126.		SZOFTVERFRISSÍTÉS	–	–	–
127.		Frissítési képességek	–	–	–
128.	UPD-1	Az IoT-eszköz szoftvere biztonságosan frissíthető a szoftver által biztosított módon vagy interfészen keresztül.	X	X	X
129.	UPD-2	A szoftverfrissítés azonosított, arra feljogosítással rendelkező felhasználói fiókkal végezhető el, biztonságos és konfigurálható mechanizmussal támogatva.	0	X	X
130.	UPD-3	Az IoT-eszköz szoftverének aktuális verziója lekérdezhető.	X	X	X
131.	UPD-4	Feljogosított fiókok a szoftvert korábbi szoftververzióra visszaállíthatják.	0	X	X
132.	UPD-5	A szoftverfrissítések hiteles forrásból származnak, és ennek a feltételnek a teljesülését az IoT-eszköz ellenőrzi.	X	X	X
133.	UPD-6	A szoftverfrissítések nem okozzák az IoT-eszköz kiberbiztonsági felkészültségének csökkenését, és ennek a követelménynek az ellenőrzésére az IoT-eszköz beépített metódussal rendelkezik.	0	X	X
134.		Frissítések kezelése alkalmazástámogatás által	0	0	0
135.	UPDCTRL-1	Az IoT-eszköz a frissítések hitelességét és integritását ellenőrzi.	X	X	X
136.	UPDCTRL-2	Az IoT-eszköz automatikus frissítése kikapcsolható.	X	X	X
137.	UPDCTRL-3	Manuális és automatikus frissítési metódus támogatott.	X	X	X
138.	UPDCTRL-4	A frissítési metódus megválasztható.	X	X	X
139.	UPDCTRL-5	A szoftver állítható időközönként ellenőrzi új frissítés rendelkezésre állását.	X	X	X
140.	UPDCTRL-6	Újonnan megjelenő szoftververziókról az IoT-eszköz értesítést küld, amely funkció kikapcsolható.	X	X	X
141.	UPDCTRL-7	Újonnan megjelenő szoftververziókról az IoT-eszköz értesítést küld, az értesítendők köre konfigurálható.	0	0	X
142.	UPDCTRL-8	Az IoT-eszköz tájékoztatja a felhasználót arról, ha a frissítés az IoT-eszköz alapvető működésére kockázatot jelent.	0	X	X
143.		ESEMÉNYKEZELÉS TÁMOGATÁSA	–	–	–

144.		Naplózás	–	–	–
145.	LOG-1	Az IoT-eszköz képes események naplózására.	X	X	X
146.	LOG-2	Az IoT-eszköz külső naplózó rendszer kapcsolatot támogat.	0	X	X
147.	LOG-3	A naplóbejegyzések minimális tartalma a következő: az IoT-eszköz egyedi azonosítója, időjelzés, esemény forrása, esemény típusa, esemény besorolása, felhasználóazonosító vagy folyamatazonosító, esemény leírása.	0	X	X
148.	LOG-4	Az IoT-eszköz képes a hálózati kommunikáció naplózására.	0	X	X
149.	LOG-5	Az IoT-eszköz képes az eszközkonfiguráció változásainak naplózására.	0	X	X
150.	LOG-6	Az IoT-eszköz képes a sikeres és sikertelen hozzáférési kísérletek naplózására.	X	X	X
151.	LOG-7	Az IoT-eszköz képes a saját és szenzorai állapotának naplózására.	0	X	X
152.	LOG-8	A naplózható események listája alapján a naplózandó események konfigurálhatóak.	0	0	X
153.	LOG-9	Az IoT-eszköz állapota interfészen lekérdezhető.	0	X	X
154.	LOG-10	Az események maximális megőrzési ideje, a tárolt naplóesemények száma, illetve a naplóállomány maximális mérete beállítható.	0	X	X
155.	LOG-11	Az IoT-eszközön a megőrzési kritériumokon túli naplóállomány maradéktalan törlése biztosított.	0	X	X
156.		Időjelzés kezelése	–	–	–
157.	TIMESTP-1	Az IoT-eszköz által naplózott események időjelzése legalább másodperc pontosságú.	0	X	X
158.	TIMESTP-2	Az IoT-eszköz NTP hálózati protokollt támogat.	0	X	X
159.	TIMESTP-3	Megbízható időforrás konfigurálható.	0	X	X
160.	TIMESTP-4	Az IoT-eszköz szabványos, UTC-re visszavezethető időjelzést használ.	0	X	X
161.		Eseménykezelés támogatása	–	–	–
162.	INC-1	Az IoT-eszköz figyelmeztetést küld a biztonsági eseménynek tekintendő, konfigurált eseményekről.	0	X	X
163.	INC-2	Az IoT-eszköz figyelmeztetést küld a biztonsági eseménynek tekintendő, konfigurált eseményekről a kapcsolódó információs rendszerek felé.	0	0	X
164.	INC-3	A figyelmeztetés módja konfigurálható.	0	0	X
165.	INC-4	Az IoT-eszköz alternatív naplózási megoldást támogat az elsődleges naplózási mechanizmus kiesése esetére.	0	0	X
166.		ESZKÖZBIZTONSÁG	–	–	–
167.		Biztonságos kommunikáció	–	–	–
168.	SECCOM-1	Más eszközökkel való kapcsolat kezdeményezése és lezárása biztonságosan történik.	X	X	X
169.	SECCOM-2	Az IoT-eszköz forgalomirányítási szabályok érvényesítésére képes.	0	X	X
170.	SECCOM-3	Az IoT-eszköz a kommunikáció során standardizált protokollokat használ.	X	X	X
171.	SECCOM-4	Az IoT-eszköz IP-címe beállítható.	X	X	X

172.	SECCOM-5	Az IoT-eszköz interfészeinek portjai konfigurálhatóak.	0	X	X
173.	SECCOM-6	Az IoT-eszköz DNS-támogatással rendelkezik.	X	X	X
174.		Erőforrások biztonságos használata	–	–	–
175.	RESRC-1	Az IoT-eszköz erőforrások megosztott használatára képes.	0	X	X
176.	RESRC-2	Az IoT-eszköz képes memóriaterületeket folyamatokhoz rendelni.	0	X	X
177.	RESRC-3	Az egyes folyamatok más folyamathoz rendelt memóriaterületet nem érnek el.	0	X	X
178.	RESRC-4	A memóriaterület csak kernelen keresztül hozzáférhető.	0	X	X
179.	RESRC-5	A memória hardveralapú hozzáférés-vezérléssel védett.	0	X	X
180.	RESRC-6	A lemezhasználathoz kvóták rendelhetőek.	0	0	X
181.	RESRC-7	Hálózati kapcsolat elvesztése esetén korlátozott működés biztosított.	X	X	X
182.	RESRC-8	Az IoT-eszköz tömörített adattárolást támogat.	0	0	X
183.		Integritásvédelem	–	–	–
184.	INT-1	Az IoT-eszköz egyedi, nem hiteles forrásból származó kód futtatása elleni védelemmel rendelkezik.	0	X	X
185.	INT-2	Az IoT-eszköz rendelkezik a nem kívánt hardver- és szoftvermódosítás észlelési képességgel.	0	X	X
186.	INT-3	Az IoT-eszköz az alapkonfiguráció biztonsági megfelelőségét ellenőrző funkcióval rendelkezik.	0	X	X
187.	INT-4	Az IoT-eszköz integritás-ellenőrző funkcióval rendelkezik.	0	X	X
188.	INT-5	Az IoT-eszköz a szoftverét biztonságos rendszerindítási mechanizmusok segítségével ellenőrzi.	0	X	X
189.	INT-6	Ha az IoT-eszköz a szoftver jogosulatlan módosítását észleli, figyelmezteti a felhasználót, illetve a rendszergazdát a problémára, és nem csatlakozik a riasztási funkció végrehajtásához szükségesnél szélesebb hálózatokhoz.	0	X	X
190.	INT-7	Az IoT-eszköz a rendszer fejlesztési életciklusa során manipuláció észlelésére képes.	0	0	X
191.	INT-8	A futtató környezet read-only adathordozón tárolódik.	0	X	X

3. melléklet a 10/2024. (VIII. 8.) SZTFH rendelethez

Sérülékenységvizsgálattal érintett követelmények

A 2. melléklet szerinti követelmények közül a következő követelmények esetében végzendő sérülékenységvizsgálat az értékelés során:

	A	B
1.	Azonosító	Leírás
2.	DEVID-3	Távolról vezérelhető IoT-eszköz egyedi azonosítója és modelljelölése megállapítható.
3.	DEVID-4	Az IoT-eszköz biztosítson egyedi fizikai azonosító hozzáadására lehetőséget, amelyhez az arra jogosult entitások hozzáférnek.
4.	DEVOP-3	Nem jogosult felhasználó által az egyedi logikai IoT-eszközazonosító nem megismerhető.
5.	IDSUPP-2	Más IoT-eszközök hitelességének ellenőrzése biztosított.
6.	IDSUPP-3	Az IoT-eszköz hálózati és távoli hálózati kapcsolat esetén az azonosított kapcsolat felépítése előtt kriptográfiai alapú, kétirányú azonosítást végez.
7.	IDSUPP-4	Az IoT-eszköz tanúsítványalapú azonosítást és hitelesítést támogat.
8.	DEVCONF-1	A logikai hozzáférési jogosultságok beállítására, az IoT-eszköz konfigurációjára – A logikai hozzáférés az Interfészekhez című részben leírtak szerint – csak privilegizált felhasználókon keresztül nyílik lehetőség.
9.	DEVCONF-2	Csak arra jogosult felhasználók konfigurálhatják az IoT-eszköz azonosítási házirendjét és a hozzáférési korlátozási listákat. A logikai hozzáférés az Interfészekhez című résszel összhangban.
10.	DEVCONF-3	Csak arra jogosult felhasználók konfigurálhatják az IoT-eszköz logikai és fizikai interfészeit A logikai hozzáférés az Interfészekhez című résszel összhangban.
11.	CRYPT-1	Az IoT-eszköz megfelelő erősségű és hatékonyságú kriptográfiai algoritmust biztosít az adatok védelme érdekében.
12.	CRYPT-2	Az IoT-eszköz képes egyedi tanúsítványok érvényesítésére.
13.	CRYPT-3	Digitális aláírások ellenőrzése biztosított.
14.	CRYPT-4	Az IoT-eszköz képes Hash algoritmusok futtatására.
15.	CRYPT-6	Az eszköz forráskódja nem tartalmaz hard-coded kritikus biztonsági paramétereket.
16.	CRYPT-7	A szoftverfrissítések integritásának és hitelességének ellenőrzésére, valamint az eszközszoftverben a kapcsolódó szolgáltatásokkal folytatott kommunikáció védelmére használt kritikus biztonsági paramétereknek eszközönként egyedinek kell lenniük, és azokat olyan mechanizmussal kell előállítani, amely csökkenti az eszközosztályok elleni automatizált támadások kockázatát.
17.	CRYKEY-1	Az IoT-eszköz a kriptográfiai kulcsokat biztonságosan kezeli.
18.	CRYKEY-2	Az IoT-eszköz képes kulcspárok generálására.
19.	CRYKEY-3	Az IoT-eszköz a kriptográfiai kulcsokat biztonságosan tárolja.
20.	CRYKEY-4	Az IoT-eszköz a kriptográfiai kulcsok változtatását biztonságosan végzi.
21.	CRYKEY-5	Az IoT-eszköz a külső rendszerek által generált kriptográfiai kulcsokat ellenőrzi.
22.	SECSTR-1	Az IoT-eszköz a jelszavakat nem tárolja – ide nem értve az irreverzibilis kriptográfiai hasító függvénnyel a jelszóból képzett hash érték tárolást – és nem továbbítja.

23.	SECSTR-4	A személyes adatok védelme a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelettel (általános adatvédelmi rendelet) összhangban biztosított.
24.	SECDT-3	Az IoT-eszköz rendelkezik a jogosulatlan hozzáférés és módosítás elleni védelemmel az adatkapcsolati közegben.
25.	SECDT-4	Az IoT-eszköz a továbbított és fogadott adatok integritását kriptográfiai megoldással ellenőrzi.
26.	AUTH-3	Az IoT-eszköz többfaktoros hitelesítési metódust támogat meghatározott felhasználói kör esetén.
27.	AUTH-5	Az IoT-eszköz a gyári alapértelmezett jelszavak generálása során olyan generálási algoritmust alkalmaz, amely csökkenti az automata támadások kockázatát.
28.	AUTH-7	Az IoT-eszköz a hitelesítési folyamat során az adatokat elrejti.
29.	AUTH-8	Az IoT-eszköz standardizált, egységes authentikációs metódust támogat (pl. SAML, OAuth2).
30.	AUTH-9	Az IoT-eszköz távoli elérés esetén az authentikációs adatokat műveletenként ellenőrzi.
31.	AUTH-10	Az IoT-eszköz a hitelesítési metódus feedbackjében található információk rejtett visszacsatolásával biztosítja, hogy a hitelesítési azonosítók illetéktelenek számára megismerhetővé, újrafelhasználhatóvá váljanak.
32.	IDENT-10	Az IoT-eszköz a külső felhasználók és rendszerek authentikációját támogatja.
33.	NOTIF-4	Személyes adatokat tartalmazó, továbbá biztonsági értesítések teljes tartalma csak azonosítás után megismerhető, érzékeny adatok a figyelmeztető üzenetben nem jelennek meg.
34.	ACCESS-1	Az IoT-eszköz a jogosulatlan műveleteknek ellenáll.
35.	ROLE-12	Az IoT-eszköz az egyes felhasználótípusokhoz korlátozó feltételek megadására biztosít lehetőséget (pl. időalapú korlátozás, IP-korlát).
36.	INTCTRL-2	Az IoT-eszköz komponenseinek használata korlátozható (portok, funkciók, be- és kimeneti eszközök).
37.	INTCTRL-3	Azok a fizikai vagy logikai interfészek, amelyek nem szükségesek az IoT-eszköz működéséhez, tilthatóak.
38.	INTCTRL-4	Gyári alapértelmezett állapotban csak a telepítéshez, beüzemeléshez minimálisan szükséges logikai és fizikai interfészek engedélyezettek.
39.	INTCTRL-5	Gyári alapértelmezett állapotban az IoT-eszköz védelmet biztosít a biztonsági információk azonosítás nélküli kinyerése ellen.
40.	INTCTRL-8	A menedzsment felület elérésének külső hozzáférése tiltható.
41.	INTCTRL-9	Az IoT-eszköz logikai interfészeinek elérése szabályozható.
42.	INTCTRL-10	Az IoT-eszköz vezeték nélküli kapcsolatot támogat, amelynek biztonságos és engedélyezett authentikációs protokollja konfigurálható.
43.	INTCTRL-11	Ha az IoT-eszköz rendelkezik debug interfésszel, az szoftveresen tiltott.
44.	UPD-4	Feljogosított fiókok a szoftvert korábbi szoftververzióra visszaállíthatják (pl. downgrade attack).
45.	UPD-5	A szoftverfrissítések hiteles forrásból származnak, és ennek a feltételnek a teljesülését az IoT-eszköz ellenőrzi.
46.	SECCOM-2	Az IoT-eszköz forgalomirányítási szabályok érvényesítésére képes.
47.	RESRC-3	Az egyes folyamatok más folyamathoz rendelt memóriaterületet nem érnek el.
48.	RESRC-4	A memóriaterület csak kernelen keresztül hozzáférhető.
49.	RESRC-5	A memória hardveralapú hozzáférés-vezérléssel védett.

50.	INT-1	Az IoT-eszköz egyedi, nem hiteles forrásból származó kód futtatása elleni védelemmel rendelkezik.
51.	INT-2	Az IoT-eszköz rendelkezik a nem kívánt hardver- és szoftvermódosítás észlelési képességgel.
52.	INT-4	Az IoT-eszköz integritás-ellenőrző funkcióval rendelkezik.
53.	INT-5	Az IoT-eszköz a szoftverét biztonságos rendszerindítási mechanizmusok segítségével ellenőrzi.
54.	INT-6	Ha az IoT-eszköz a szoftver jogosulatlan módosítását észleli, figyelmezteti a felhasználót, illetve a rendszergazdát a problémára, és nem csatlakozik a riasztási funkció végrehajtásához szükségesnél szélesebb hálózatokhoz.

4. melléklet a 10/2024. (VIII. 8.) SZTFH rendelethez

Értékelési módszertan

1. A tesztelendő IoT-eszköz

1.1. A tesztelendő VE egy konkrét IoT-eszköz, amelyet a jelen tanúsítási rendszer rendelkezései alapján kell értékelni. Az értékelést végző gyártó vagy megfelelőségértékelő szervezet képes a VE-t a rendelkezésre álló interfészeken keresztül vezérelni, és az MD-ben megadott információk alapján részben ismeri annak kialakítását (gray box tesztelés). A VE-nek az értékelés során üzemképes állapotban kell lennie, továbbá a kapcsolódó egyéb szolgáltatásoknak működnie kell akkor is, ha azokat a gyártó vagy a megfelelőségértékelő szervezet nem ellenőrzi.

2. Értékelést megalapozó dokumentum

2.1. Az 1. melléklet szerinti ÉMD-t a jelen tanúsítási rendszer rendelkezései alapján a gyártó készíti el a VE-ben megvalósított és támogatott képességekről. Az ÉMD-ben a gyártónak a vizsgálat tárgyát képező megbízhatósági szinthez tartozó összes, 2. melléklet szerinti követelmény teljesüléséről nyilatkoznia szükséges.

3. Megvalósítási dokumentum

3.1. A gyártó az 1. mellékletben foglaltak szerint MD-t készít, amely az értékelés elvégzéséhez szükséges további, részletesebb információkat tartalmazza. Az MD az értékeléshez használt módszertan alapja, illetve tartalmaz néhány tervezési részletet is a megfelelőségértékelő szervezet számára.

3.2. A gyártó teljes körű, részletes és helyes információkat szolgáltat az MD kitöltése során.

3.3. Az MD kitöltése során a gyártó hivatkozhat meglévő dokumentációra is, ebben az esetben a hivatkozott dokumentációt a megfelelőségértékelő szervezet rendelkezésére bocsátja.

4. A gyártó feladata

4.1. A gyártó mint az értékelést kezdeményező szervezet egy adott VE jelen tanúsítási rendszer alapján történő vizsgálatát kéri. A gyártó a megfelelőségértékelő szervezet egyetlen kapcsolattartó pontja, és feladata, hogy koordináljon a VE ellátási láncában és ökoszisztémájában részt vevő felekkel, így különösen az alkatrészgyártókkal, a szolgáltatókkal és az alkalmazásfejlesztőkkel.

4.2. A meglévő biztonsági tanúsítványok vagy a VE egyes részeinek harmadik fél által végzett értékelései részben felhasználhatóak a megfelelőség bizonyítékaként az értékeléshez szükséges erőforrások, illetve időszükséglet csökkentése érdekében. Ebben az esetben a gyártó az ÉMD-ben jelezi, hogy a megfelelőség már értékelésre került, a megfelelő bizonyítékra való hivatkozással együtt. A gyártónak továbbá a bizonyíték ellenőrzéséhez szükséges összes információt – így különösen a tanúsítás részleteit és a vizsgálati jelentéseket – a megfelelőségértékelő szervezet rendelkezésére kell bocsátania. A megfelelőségértékelő szervezet az értékelés során ellenőrzi, hogy a bizonyíték alkalmas-e az érintett 2. melléklet szerinti követelmény teljesítésének igazolására.

5. A megfelelőségértékelő szervezet feladata

5.1. A megfelelőségértékelő szervezet által vizsgálatba bevont vizsgáló laboratórium végzi el a VE megfelelőségértékelését. Az értékelés során figyelembe kell venni a kapcsolódó szolgáltatásokkal és a VE fejlesztési, kezelési folyamataival való kapcsolatot is. Megfelelőségi önértékelés esetében a 6. pont alkalmazásában megfelelőségértékelő szervezet alatt a gyártó értendő.

6. Az értékelési eljárás

6.1. Az értékelési eljárás fázisai a következők:

6.2. A megfelelőségértékelő szervezet az ÉMD-ben „Alkalmazható és teljesített"-ként megjelölt minden egyes követelmény esetében, a 7. pont szerinti módon rögzíti a teszteseteket, kidolgozza a VE-re vonatkozó tesztelési tervet, és elvégzi a tesztelést.

6.3. Az ÉMD-ben megjelölt minden egyes követelmény esetében több teszteset vizsgálata szükséges a 6.3.1–6.3.5. pont szerint.

6.3.1. Teszteset: <követelményazonosító>-T0 – Alkalmazhatóság

A vizsgálat célja:

Ezen teszteset célja egy adott, 2. melléklet szerinti követelmény alkalmazhatóságának értékelése.

Tesztegységek:

a) A megfelelőségértékelő szervezet ellenőrzi, hogy a gyártó a követelményt „Alkalmazható és teljesített"-ként jelölte-e meg.

b) Ha a követelmény „Alkalmazható és teljesített" besorolást kapott, a megfelelőségértékelő szervezet megvizsgálja, hogy a gyártó a Teljesítés módját feltüntette-e.

c) Ha a követelmény „Nem alkalmazható" besorolást kapott, a megfelelőségértékelő szervezet megvizsgálja annak indokolását, és értékeli azt.

A döntés hozzárendelése:

„Megfelelt" döntést akkor hozható meg, ha

– „Alkalmazható és teljesített" besorolás esetén a Teljesítés módja kitöltésre került,

– „Nem alkalmazható" besorolás esetén az indokolás megalapozott.

Ellenkező esetben a döntés „Nem megfelelt".

6.3.2. Teszteset: <követelményazonosító>-T1 – Dokumentáció

Előfeltétel:

A 2. melléklet szerinti követelmény ÉMD szerint „Alkalmazható és teljesített" és a korábbi teszteset (<követelményazonosító>-T0) értékelése „Megfelelt".

A vizsgálat célja:

Ezen teszteset célja egy adott, 2. melléklet szerinti követelmény dokumentáltságának megállapítása. A teszteset minden megbízhatósági szinten alkalmazandó.

Tesztegységek:

A megfelelőségértékelő szervezet ellenőrzi, hogy a gyártó a követelmény teljesítését megfelelően dokumentálta-e, azonosítja a követelménynek való megfelelés alátámasztására használható, MD szerinti elemeket.

A döntés hozzárendelése:

A „Megfelelt" döntés akkor hozható meg, ha az MD a követelményre vonatkozó összes releváns információt tartalmazza.

Ellenkező esetben a döntés „Nem megfelelt".

6.3.3. Teszteset: <követelményazonosító>-T2 – Koncepcionális vizsgálat

Előfeltétel:

A 2. melléklet szerinti követelmény ÉMD szerint „Alkalmazható és teljesített" és a korábbi teszteset (<követelményazonosító>-T1) értékelése „Megfelelt".

A vizsgálat célja:

Ezen teszteset célja a 2. melléklet szerinti követelmény dokumentáció szerinti teljesítése koncepcionális megfelelőségének megállapítása. A teszteset minden megbízhatósági szinten alkalmazandó.

Tesztegységek:

A megfelelőségértékelő szervezet ellenőrzi, hogy a <követelményazonosító>-T1 tesztesetben azonosított információk alapján a VE megfelel-e koncepcionálisan a 2. melléklet szerinti követelménynek.

A döntés hozzárendelése:

„Megfelelt" döntés akkor hozható meg, ha a <követelményazonosító>-T1 tesztesetben azonosított információk alapján a VE koncepcionálisan megfelel a 2. melléklet szerinti követelménynek, az alkalmazott védelmi kontroll és megvalósítás a megbízhatósági szinten kockázatarányosan megfelelő.

Ellenkező esetben a döntés „Nem megfelelt".

6.3.4. Teszteset: <követelményazonosító>-T3 – Megvalósítási vizsgálat

Előfeltétel:

A 2. melléklet szerinti követelmény ÉMD szerint „Alkalmazható és teljesített" és a korábbi teszteset (<követelményazonosító>-T2) értékelése „Megfelelt".

A vizsgálat célja:

Ezen teszteset célja a 2. melléklet szerinti követelmény dokumentáció szerinti teljesítésének megállapítása. A teszteset minden megbízhatósági szinten alkalmazandó.

Tesztegységek:

A megfelelőségértékelő szervezet ellenőrzi, hogy a <követelményazonosító>-T1 tesztesetben azonosított információk szerint történt-e a megvalósítás.

A döntés hozzárendelése:

„Megfelelt" döntés akkor hozható meg, ha a megvalósítás a <követelményazonosító>-T1 tesztesetben azonosított információk alapján került elvégzésre.

Ellenkező esetben a döntés „Nem megfelelt".

6.3.5. Teszteset: <követelményazonosító>-T4 – Sérülékenységi vizsgálat

Előfeltétel:

A 2. melléklet szerinti követelmény ÉMD szerint „Alkalmazható és teljesített" és a korábbi teszteset (<követelményazonosító>-T2) értékelése „Megfelelt".

A vizsgálat célja:

Ezen teszteset célja a 3. melléklet szerinti követelmény sérülékenységvizsgálati módszerrel történő értékelése. A tesztesetet legalább „jelentős" megbízhatósági szinten kell alkalmazni.

Tesztegységek:

A megfelelőségértékelő szervezet ellenőrzi, hogy az alkalmazott megoldások tekintetében ismert sérülékenység fennáll-e, továbbá manuális sérülékenységvizsgálattal a biztonsági cél teljesülését.

A döntés hozzárendelése:

„Megfelelt" döntés akkor hozható meg, ha nincs feltárt, kihasználható sérülékenység a vizsgálat alapján.

Ellenkező esetben a döntés „Nem megfelelt".

7. Az értékelés eredménye

Az értékelés eredményeként tesztesetenként rögzítésre kerül a teszteset eredménye. A tesztesetek végrehajtásáról a megfelelőségértékelő szervezet Értékelési jelentést készít, amely tartalmazza

– az ÉMD-ben rögzített információkat,
– az egyes követelményekhez tartozó tesztesetek azonosítóit,
– a tesztesetek értékelésének módját,
– a tesztesethez tartozó döntést megalapozó tényeket,
– sérülékenységvizsgálati teszteset esetén a vizsgálati jelentést,
– a tesztesethez tartozó döntést,
– a követelmények összesített értékelését.

A követelmény értékelése:

– „Teljesített" az értékelés, ha a követelményhez tartozó valamennyi teszteset „Megfelelt",
– „Nem teljesített" az értékelés, ha a követelményhez tartozó valamely teszteset „Nem megfelelt".

Megfelelőségi nyilatkozat vagy nemzeti kiberbiztonsági tanúsítvány abban az esetben állítható ki, ha a VE az ÉMD-ben rögzített valamennyi követelmény vonatkozásában „Teljesített" az értékelés.

5. melléklet a 10/2024. (VIII. 8.) SZTFH rendelethez

Megfelelőségi nyilatkozat

NEMZETI KIBERBIZTONSÁGI MEGFELELŐSÉGI NYILATKOZAT

Gyártó neve:	
Gyártó címe:	

IoT-eszköz	
megnevezése:	
verziószáma:	
modellszáma:	
megbízhatósági szint:	Jelöljön ki egy elemet.

Egyéb műszaki előírások, szabványok és eljárások:

Alkalmazási terület és körülmény korlátozás:

Érvényességi idő: **nap**

Kijelentem, hogy a fent részletezett termék megfelel az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről szóló SZTFH rendeletben foglalt követelményeknek. Kijelentem, hogy jelen nyilatkozat kiállítására kizárólag a *[gyártó neve]* jogosult.

Kiállítás dátuma: Dátum megadásához kattintson ide.

---

gyártó cégszerű aláírása

.....

SZTFH tölti ki!

Nyilvántartásba vétel dátuma:	
Nyilvántartási azonosító:	

SZTFH Szabályozott Tevékenységek Felügyeleti Hatósága

6. melléklet a 10/2024. (VIII. 8.) SZTFH rendelethez

Nemzeti kiberbiztonsági tanúsítvány

NEMZETI KIBERBIZTONSÁGI

TANÚSÍTVÁNY

A **<megfelelőségértékelő szervezet neve>** (székhely), mint a Szabályozott Tevékenységek Felügyeleti Hatósága által az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló SZTFH rendelet szerinti <megbízhatósági szint> megbízhatósági szintű kiberbiztonsági tanúsítvány kiállítására vonatkozó feltételeknek megfelelő, <iktatószám> számon nyilvántartásba vett **megfelelőségértékelő szervezet, tanúsítja,** hogy a(z)

<gyártó neve>

által gyártott

<IoT-eszköz megnevezése>

az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről szóló SZTFH rendeletben foglalt

<megbízhatósági szint>

megbízhatósági szinten előírt követelményeknek megfelel.

Jelen tanúsítvány a <szám> számú értékelési jelentés alapján került kiadásra.

Készült a <megbízó neve> (székhely) megbízásából.

Érvényességi idő: **nap**

Kiállítás dátuma: Dátum megadásához kattintson ide.

---

megfelelőségértékelés szakmai igazolója

---

megfelelőségértékelő szervezet cégszerű aláírása

.....

SZTFH tölti ki!

Nyilvántartásba vétel dátuma:	
Nyilvántartási azonosító:	

SZTFH Szabályozott Tevékenységek Felügyeleti Hatósága