TANÚSÍTÁSI JELENTÉS

MobilSign bolti aláíró rendszer

verzió: R1

HUNG-TJ-071-2015

Verzió:	1.0	
Fájl:	Hung-TJ-EAT-071-2015.pdf	
Minősítés:	Nyilvános	
Oldalak:	30	

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2015.07.03	A szerkezet felállítása
v0.2	2015.07.20	Belső egyeztetésre kiadott változat
v0.9	2015.07.23	Külső egyeztetésre kiadott változat
v1.0	**2015.07.24**	**Végleges verzió**

A tanúsítási jelentést készítette:

dr. Szabó István
Hunguard Kft
Tanúsítási divízió

Tartalomjegyzék

1 Összefoglaló

1.1 A tanúsítás jellemzői

STOE név:	MobilSign bolti aláíró rendszer
STOE verzió:	R1
Rövid elnevezés:	MobilSign rendszer
Rendszer integrátor:	ProfiTrade 90 Kft. 1013 Budapest, Pauler utca 6.
Rendszer működtető:	Magyar Telekom Nyrt. 1013 Budapest, Krisztina krt. 55.
Rendszer üzemeltető:	Magyar Telekom Nyrt. 1013 Budapest, Krisztina krt. 55.
Értékelő szervezet:	Hunguard Kft. Értékelési Divízió 1123 Budapest, Kékgolyó u. 6.
Az értékelés módszere:	KIB 28 ajánlás szerinti Rendszerekre vonatkozó értékelési módszertan
Az értékelés garanciaszintje:	MIBÉTS fokozott (SAP-F)

1.2 STOE áttekintés

A rendszer értékelés tárgya a Magyar Telekom által üzemeltetett, kézi aláírás dinamika előállítására képes, azokat PDF dokumentumokkal összekapcsoló, majd az így létrejött dokumentumokra fokozott biztonságú elektronikus aláírásokat létrehozó informatikai rendszer (a továbbiakban MobilSign rendszer).

MobilSign rendszer feladata, hogy a Magyar Telekom üzleteiben a megkötendő szerződéseket az ügyfelek egy tablet-en, elektronikus formában, kézírással alá tudják írni. A szerződések elektronikus aláírással ellátva, PDF formátumban érkeznek a Magyar Telekom eStore rendszeréből. A rendszer a kézírás dinamikájának adatait, kiszámolja és tárolja, azokból képzett bizonyítékrekord lenyomatát beilleszti a PDF fájlba, majd az aláírásra került dokumentum és bizonyítékrekord lenyomatát, és a kézi aláírás képét tartalmazó PDF-et fokozott biztonságú elektronikus aláírással látja el.

A MobilSign-hoz fejlesztett ellenőrző eszköz a kézzel aláírt PDF és a bizonyítékrekord összetartozását meg tudja állapítani, illetve a bizonyítékrekordból képes olyan a védett PC-n megtekinthető formátumot előállítani, amelynek alapján az írásszakértő képes a kézírás megfelelőségét ellenőrizni.

A MobilSign rendszer által megvalósítandó folyamat magában foglalja az alábbiakat:

- az ügyfél által aláírandó szerződések átvétele egy külső rendszerből,
- az ügyfél által aláírandó szerződések megtekintése az ügyfél által,

- az ügyfél kézi aláírásának rögzítése,
- a kézi aláírásból képzett bizonyíték titkosítása,
- a bizonyíték és az aláírandó dokumentum összekapcsolása,
- a dokumentumra fokozott biztonságú elektronikus aláírás létrehozása (a MTrack/NCA és Luna SA7000 HSM-en elérhető magánkulcs aktivizálásával) és időbélyegzése időbélyeg-szolgáltatótól kért időbélyeggel,
- az aláírások kezdeti ellenőrzése,
- a bizonyíték megoldása és prezentálása,
- a bizonyíték és az aláírt dokumentum összetartozásának ellenőrzése.

A MobilSign elektronikus aláírás létrehozását teszi lehetővé az alábbi jellemzőkkel:

- az aláírandó PDF állományok egy külső rendszerben (JAZZ) keletkeznek, és eStore-on keresztül kerülnek átadásra az Aláíró kliens számára;
- mielőtt az Aláíró kliens számára az aláírandó PDF állomány átadásra kerülne, az eStore-ban aláírásra kerül az MTrack/NCA által szervezeti tanúsítvánnyal;
- az ügyintéző saját jelszavával jelentkezik be az Aláíró kliensre, az aláírási folyamat kezdeményezése előtt, egy saját maga által megadott munkamenet PIN kódot is meg kell adnia;
- a végleges aláírandó dokumentum az alkalmazás szerveren áll elő, a kézi aláíráshoz tartozó bizonyíték és a PDF állomány összekapcsolásával,
- az aláírás egy aláíró szerveren (MTrack/NCA) hajtódik végre Luna SA7000 HSM-en elérhető magánkulcs aktivizálásával,
- a tablet és az alkalmazás szerver, az alkalmazásszerver és az aláíró szerver, az aláíró szerver és az MTrack/NCA, valamint az MTrack/NCA és a Luna SA7000 HSM közötti kommunikációt megbízható útvonal védi.

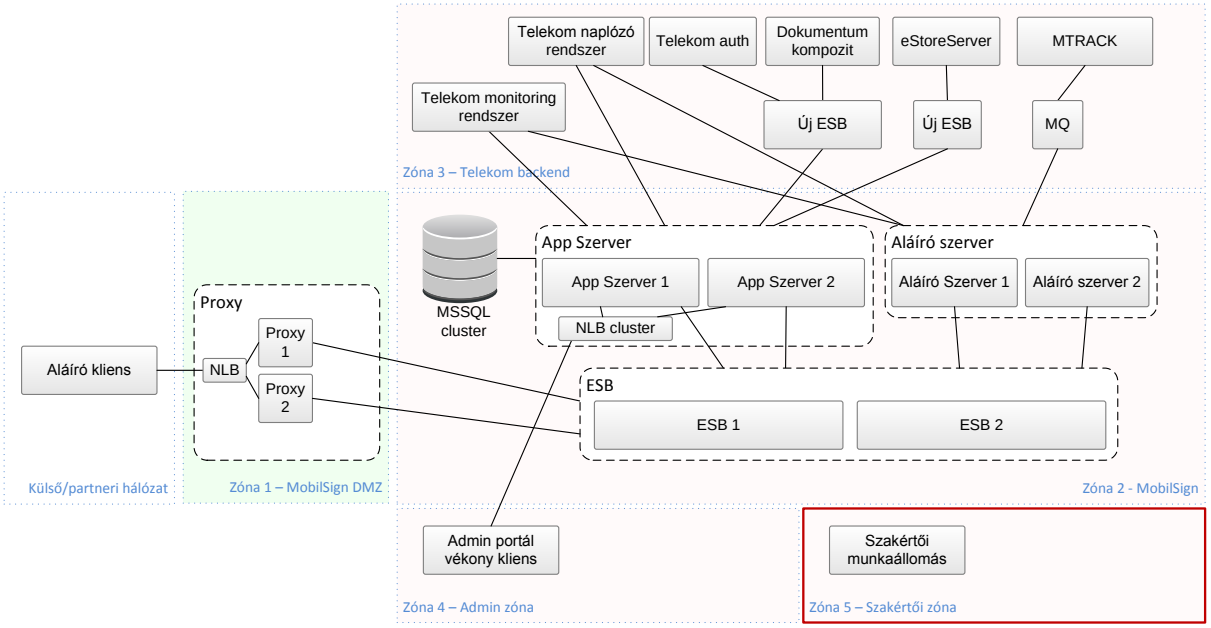
A MobilSign rendszer biztonsági funkciói magában foglalják az alábbiakat:

- a rendszerhez hozzáférő különböző szerepkörű felhasználók (ügyintézők, adminisztrációs portál felhasználói) azonosítása és hitelesítése,
- hozzáférés ellenőrzés (a nyújtott szolgáltatásokat csak az arra jogosultak érik el, a megfelelő azonosítás és hitelesítés után),
- fokozott biztonságú elektronikus aláírás létrehozása és kezdeti ellenőrzése,
- időbélyeg kérés, és a kapott időbélyeg válasz elhelyezése az elektronikus aláíráson,
- naplózás (biztonsági naplóbejegyzések készítése a rendszer működéséről),
- rendszer és információ sértetlenség védelem (benne: rosszindulatú kódok elleni védelem, biztonsági funkcionalitás ellenőrzése, szoftver és információ sértetlenség ellenőrzés, a bemeneti információra vonatkozó korlátozások érvényesítése),
- bizonyíték rekordok bizalmasságának védelme,
- rendszer és kommunikáció védelem (biztonságos csatornák kiépítése),
- önvédelem (a biztonsági funkciók megkerülése vagy lerontása elleni védelem pl codesigning alkalmazása a biztonságkritikus komponenseken).

1.3 A tanúsítás tárgyának biztonsági környezete és határai

A MobilSign aláíró rendszer kliens-szerver architektúrában működik. Az aláíró kliensek a Magyar Telekom boltjaiban lesznek elhelyezve. A tablet-eken Android operációs rendszer fut, menedzselésük központosított rendszeren keresztül történik, amit a Magyar Telekom egy külön szervezeti egysége felügyel. A policy a működéséhez szükséges alkalmazásokon kívül csak a MobilSign klienst engedi futtatni. MobilSign kliens WIFI-n keresztül csatlakozik a Magyar Telekom MobilSign számára fenntartott, zárt hálózatához.

Az adatokat egy köztes réteg fogadja, terheléselosztással 2 proxy (Frontend.Proxy) fogadja a kéréseket, amely ellenőrzések (pl. túl sok próbálkozás egy címről) után továbbítja a kéréseket az alkalmazásszervernek.



1. ábra MobilSign szerkezeti felépítése a funkcionális specifikáció alapján

Az alkalmazásszervereken (ESBEPRD1,2) a következő komponensek találhatóak:

- CoreServices (adatok fogadásáért, bizonyítékok aláírásáért felelős komponens)
- NotificationService (SignalR)
- MobilSign.Web (Adminisztrátori portál webalkalmazás)

Az adatok tárolását cluster-ezett SQL Server végzi.

Az aláírószerverek (ESSGNPRD1,2) komponensei:

- SignServer (Bizonyíték technikai aláírása, Aláírás összeállítása)
- MtrackInterface (Mtrack kommunikáció Message Queue-n keresztül)

MTrack/NCA a Netlock CA szerverére épül.

MobilSign szerverek az Aláíró kliensen keletkezett naplóeseményeket is összegyűjtik.

A rendszer naplóeseményei Syslog segítségével továbbításra kerülnek a Magyar Telekom központi naplógyűjtő rendszere felé, ahol 13 hónapig tárolásra kerülnek.

A MobilSign rendszer az alábbi összetevőkből áll:

- Aláíró kliens (az ügyfél és ügyintéző számára az aláírandó dokumentum és az aláíró tulajdonságok megjelenítése, a kézi aláírás elkészítése stylus segítségével, az

ügyintéző számára az aláírás kezdeményezésének biztosítása, bizonyíték adatok titkosított formában továbbítása az alkalmazásszerver felé)

- MobilSign proxy (Frontend) (HTTPS csatorna terminálása, az alkalmazásszerver tehermentesítése, a bejövő kérések korlátozása túl sok próbálkozás esetén)
- MobilSign alkalmazás szerver (Backend) (kézírás dinamika adatok ellenőrzése, bizonyíték adatok átkódolása – titkosítás a bizonyíték titkosító kulccsal, az aláírás képének és a bizonyíték lenyomatának elhelyezése az aláírandó PDF dokumentumban)
- MobilSign aláírószerver (a bizonyíték technikai digitális aláírásának elkészítése, Mtrack/NCA segítségével a dokumentum aláírása, időbélyegzése, aláírás összeállítása az NCA-tól kapott adatok alapján)
- MobilSign adatbázisszerver
- Adminisztrációs portál (biztonsági paraméterek, bizonyíték titkosító és bizonyíték titkosító kulcsok menedzselése, tablet-ek munkameneteinek a kezelése, titkosított bizonyíték rekordok exportálása)
- LADS (Lightweight Active Directory Service) – LDAP kiszolgáló az adminisztrátori portál felhasználóinak a hitelesítésére
- MTrack/NCA (a dokumentumok szervezet általi fokozott biztonságú elektronikus aláírásához a lenyomat aláírása, az aláíró tanúsítvány érvényességi információk beszerzése és ellenőrzése, az időbélyeg beszerzése a Magyar Telekom időbélyeg szolgáltatásától)
- Luna SA7000 HSM (a dokumentumok szervezet általi fokozott biztonságú elektronikus aláírásához használt privát kulcs tárolása, és a digitális aláírás művelet elvégzése a lenyomaton)
- Szakértői munkaállomás (a bizonyítékadatok és az aláírt dokumentumok összetartozásának ellenőrzése, az írásszakértő számára a kézi aláírás dinamika adatainak prezentálása)
- Kulcsgeneráló munkaállomás (a MobilSign rendszer infrastrukturális kulcsainak védett környezetben történő előállítására)
- MobilSign Admin eszközök (parancssoros eszközök a szakértői vagy kulcsgeneráló munkaállomáson való használatra)
- SignServer Tools (random generátor eToken létrehozása, kliens adatátvitelt titkosító kulcsok készítése, bizonyíték aláíró kulcs létrehozása)
- DocumentStore Security Admin (bizonyíték titkosító kulcs létrehozása, eToken-ekre másolás)
- Evidence Tool (a bizonyítékrekordok megoldása, összetartozás ellenőrzése, elemzésre előkészítés)
- nCipher Edge (bizonyíték titkosító kulcs tárolása)
- eToken (bizonyíték titkosító kulcs tárolása)

A rendszer integrátor által fejlesztett rendszerelemek teljes listája, és a hozzájuk tartozó SHA256 lenyomat a következő:

Név	**SHA256 lenyomat**
Telekom.ClientSecurityAdmin.exe	EE347D7393F40DEE8E1771AA9FC83323881F7CE07486CBF705EA82221B8507DD
Telekom.CommandPromptAdmin.exe	2F365855D97F5757FCF4665EC42BEE93E470171D30C9ADCF573EE096C857C578
Telekom.DocumentStoreSecurityAdmin.exe	0CD000D4BE5FA4BE19EF359F9EF1596B2477E2806F781673207D14840FD198AA
Telekom.RandomGeneratorAdmin.exe	E54A0EE87B19BB5169DF98043DA3FC88F2C1E5A639280521171C499C7D8DE0AD
Common.Collections.dll	5103F7D01C7E23B455715FAC822937DD99B2852AC8C46FD5225BCB40B2A86ED5
Common.ColoredConsole.dll	7D474B8EB7C6067F9F0F6AB5164EDF19ED58AC64328F01920F72BC71A86544DD
Common.Converters.dll	A42BC26949E78C01BB8712F75782EF1A8551DE31C40426F6536B9364AF3A6B7B
Common.Logging.dll	C5267CA6435EB9977CFA8491F438897F71B41F9E16C1DB2F4569666D2017E3D4
Common.Logging.resources.dll	FF1DF67761B4D723088E03F38B0F45DEF75EB43AA077D93B1584F8D83446D4FD
Common.Attributes.dll	DF21A4E159335BCF9DB65C93243E0B4AF66C8064FC3DB0911B1DB38512724859
Common.Enums.dll	01D9F5CA2C0FCD389F9B98417E0508BEEF7E64ED4A2A7C8A7A270393C749D88C
Common.ErrorHandling.dll	FF9122DF04FA432F24F14113DCE1B9A5622A494349C7C7A4192DA3C358B2C213
Common.FileHandling.dll	F8FCC071D0BDA8171FAE96532E846E2825A8EE20660F1E52AC7F6CBAEAC0D990
Common.Formatting.dll	10009264DD677D5C8F6F3D4479880A660B8BF87BC10DB42B99F19A6DAE31D077
Common.Utils.dll	49B7C1E9D76EC0FAF644DBF30625AF9539DF610F3C7A764004A4C17676D93D75
Common.Wcf.SwaMessageEncoder.dll	5327518BB6B1C6FB52FC7E1FBF842BA5832C9A202C9AEBDFBE4AAF764F44E7BC
Common.Web.dll	8EC6FF93E45864ADC273C88AD056A14B86E048226D16190DCA36F1529687A77E
Common.YAXLib.dll	BAE1D1794F25A12DF5F6D0F87106A244A8C4328040726999EE973357ADFCD509
CryptoLib.Cryptoki.Admin.dll	6D75D7A18BD645B2DD2F6308B056109DE31598A7A26024CBDEDAA3EE9C04A410
CryptoLib.Cryptoki.Device.dll	9C7EDF19A4C57FBFD68E1B0BA09750539620CF132B350C8F692E74D5641C4C0B
CryptoLib.dll	18A729DC7D7BA04E94B5267863863245473CCE46548EB063F0D11F539F504174
CryptoLib.eToken.Device.dll	64BAE2452FCBE0B13CD7BD103598F0FD1B797211C37317538998E40A39D09A4F
CryptoLib.eToken.Interface.dll	18BA65E5D1DD2EEB61DABDCCD0CC738ECB8E22B3A29DF173B06FD027E88892A5
CryptoLib.eToken.Proxy.dll	2EF21E66BDB62283D6CBD679C6E541EF0C93D74A70DD157354F1F31E55C732BA
CryptoLib.Evidence.dll	306406E01FF7829704135340E0C216A3FC58982C01D2D89F2763BA3194BD9781
CryptoLib.Evidence.Excel.dll	81B8A7867C22BDC32E2DC112A3EF764159A423E913F94BCF6BF0129D83010E98
CryptoLib.Logging.dll	244825F278850FFC7F383EBF0B1A07123C279E40184526D93F2FF30DF25127AC
CryptoLib.Logging.resources.dll	86E741442C787DB24862242E860B30C5F4B351CCEF8B61BE797F560C3769AFE7
CryptoLib.nShield.Device.dll	4A48921B3CF897F84F6A95E04DCFF06326FF7DCA3473C7EB2C54C15991D3A61F
CryptoLib.nShield.Interface.dll	C137E67C63CD6082FC3619488B977626E95C14F678AAB667B99A325EFDD101B2
CryptoLib.nShield.Proxy.dll	728B3BA01C33B1E22153FDE3F2B3DC4B6ED8E23D08E1FA27FD666E61D58DF6BA
CryptoLib.Pdf.dll	13241F2572DCA41F89C79D51A086A650E04F858C6CBE4F1F71DC1D165FEFB637
CryptoLib.Signature.dll	7A352B3E9E2D9CCA6D3EA65485F19078E4FEF74278E20FF2665F5D484C47C9CD
CryptoLib.SoftHSM.Device.dll	5D9EBDF14253A894F3CF5A2DBD2186A13AAF2ABE1E8D7E37918B2FE0AF51F48B
CryptoLib.SoftHSM.Interface.dll	B6F97E4EFCF640260CA6D9617BD10EE70B3D9244D17D2478CE56096775C4F8B0
CryptoLib.SoftHSM.Proxy.dll	1D5313268C6EA2C23FEFCD08EE1E9C368AB513BE3F66097D222586E8866F055B
CryptoLib.Telekom.Server.AppServer.dll	E46B89F87AD73D8C39ABB1BFCF939F96987D1F0CDB9FB8DE5576211B39CBDD90
CryptoLib.Telekom.Server.Common.dll	65F4CF5F0DF85890119C442188B6F68386B0ABCE9C00B7B3FDD2F7D10AB3C8D2
CryptoLib.Telekom.Server.SignServer.dll	32C48C4BC3BC77060641D3F59D6B2366332AC281044BB896C98CED659F8A0C54
Telekom.CommandPromptAdmin.exe	480D2CF1F8A1AC9C709795B8C5AD8ABE99A78DE45BDCA1090C3ABF868C721237
Telekom.Evidence.dll	2739C9DAD6707135866C8ACDDF1988C86674777E4D3F3F186C613D71155EFEEC

Név	**SHA256 lenyomat**
Telekom.EvidenceTool.exe	01F34C19F974DC87FDE30919EB816FE5D3D21C5D47C84B7073030CC43FCA50E7
Telekom.CommandPromptAdmin.exe	2F365855D97F5757FCF4665EC42BEE93E470171D30C9ADCF573EE096C857C578
Telekom.CommandPromptAdmin.exe.config	C66E1BA36E874342CD570CF5BDD3D8B73864A4C9E9D802398BE7F46FE39A8532
Telekom.RandomGeneratorAdmin.exe	E54A0EE87B19BB5169DF98043DA3FC88F2C1E5A639280521171C499C7D8DE0AD
Telekom.SignServerSecurityAdmin.exe	A3E888EC8B8CD2B39C8A36D85B1ACB4BBDC148338541744F092208CD01FE3CBD
MobilSign.CoreComponents.dll	33B4119E2BBFA631B8DC85F7BC943F26035A09C088A9880BAD6239CB342616FF
MobilSign.Login.Wcf.dll	687A2D8FF44225256004C4C15D718E4368AC37ABF16CF23F9CE000741C057693
MobilSign.Notification.Wcf.dll	BC167D7AD0AEDECE2D4BAF830A997FCE1770EC15EBC3E91D4959C2E9A60FDA0F
MobilSign.ProxyWcfCommon.dll	68A41DE9B5941AB827698F6D5A22F71FE6F08DBBE63DA9A9A969099DF18FF055
MobilSign.TelekomComponents.dll	7E3683EB723381AB65FDFDFF22221B0A710B1281AC2E20F0D54437EECD620109
MobilSign.Proxy.Wcf.dll	7265BFE03EDC0FE63E8DBA3820DD3F2B4237E87F18521ACBBC5FBD4F5235263E
Telekom.MtrackInterface.dll	3DE15C47F904E71F00D822072E6BA2C512FDE5A1266841DCE458C4C57D99FF6E
Telekom.SignServer.dll	8643A8544DB5C171AB32F527EB3944435A70E55AACF1A55BE1E5E76A436B8ED4

2 A tanúsítás jellemzése

2.1 Az alkalmazott tanúsítási és értékelési módszer

Az alábbiakban az értékelés és tanúsítás során alkalmazott értékelési módszereket, technikákat és szabványokat dokumentáljuk.

A tanúsítási eljárás célja annak megállapítása, hogy az EAT-ban [1] meghatározott fokozott biztonságú elektronikus aláírás feltételeinek a MobileSign rendszer megfelel-e. Ennek eldöntésére a tanúsító MIBÉTS rendszerértékelés és kiegészítő értékelés eredményeit vizsgálta meg.

MIBÉTS rendszerértékelési és tanúsítási módszertan

A MobilSign rendszer műszaki szempontú értékelésére az [5]-ben és [6]-ben meghatározott, rendszerekre vonatkozó értékelési módszertant alkalmaztuk, az alábbi pontosításokkal:

- a rendszer értékelés típusa[1]: kezdeti
- a rendszer értékelés garanciaszintje[2]: MIBÉTS fokozott (SAP-F)

A rendszer értékelés keretében elvégzett fő feladat-csoportok az alábbiak voltak:

a) a rendszer biztonsági előirányzat értékelése,
b) a rendszer biztonsági architektúrájának értékelése,
c) a rendszer telepítési és üzemeltetési útmutatóinak a vizsgálata,
d) a rendszer konfiguráció vizsgálata,
e) a rendszer biztonsági tesztelése,
f) a rendszer sebezhetőség vizsgálata.

Kiegészítő értékelések

Az értékelés kiterjedt a [2] CEN/TS 419241:2014, valamint a [3] CWA 14170:2004 dokumentumokban meghatározott funkcionális és biztonsági követelmények teljesülésének ellenőrzésére is. Ez utóbbi vizsgálatok kiegészítő módszere a következő volt:

Minden követelményekre külön-külön határozat születik valamelyik alábbi lehetséges eredménnyel:

- megfelel
- nem felel meg
- nem vonatkozik rá a követelmény.

Az egyes követelményekre meghozott határozatok az alábbiak alapján születhetnek:

- interjú: a fejlesztőkkel folytatott személyes konzultációk alapján,
- dokumentáció: a fejlesztők által készített írásos dokumentációk alapján,
- tapasztalat: a rendszer használata során szerzett az értékelő, mint „felhasználói” tapasztalata alapján,
- teszt: a fejlesztők és az értékelők által végzett tesztelés eredményei alapján,
- forrás kód: a fejlesztők által biztosított forráskód értékelők általi elemzése alapján.

[1] A rendszer értékelés típusai: kezdeti, tervezett felülvizsgálati, rendkívüli felülvizsgálati, megismételt kezdeti.
[2] A rendszer értékelés lehetséges garanciaszintjei: MIBÉTS alap (SAP-A), MIBÉTS fokozott (SAP-F) és MIBÉTS kiemelt (SAP-K) rendszer értékelési garanciacsomag.

Erről a vizsgálatról egy külön megfelelés értékelési jelentés készült és ebben csak „*megfelel*” és „*nem vonatkozik rá a követelmény*” határozat született.

2.2 A tanúsításhoz felhasznált értékelési jelentések azonosítása

Rendszer értékelési jelentés:

> MobilSign - bolti aláíró rendszer R1 verziója RENDSZER ÉRTÉKELÉSI JELENTÉS V1.0

Mértékadó követelményrendszernek való megfelelés elemzés:

> MobilSign informatikai rendszer R1 megfelelése a CEN/TS 419241 által meghatározott követelményeknek MEGFELELÉS ÉRTÉKELÉSI JELENTÉS V1.0
>
> MobilSign informatikai rendszer R1 megfelelése a CWA 14170:2004 és CWA 14171:2004 követelményeinek MEGFELELÉS ÉRTÉKELÉSI JELENTÉS V1.0
>
> MobilSign informatikai rendszer R1 megfelelése a NIST Special Publication 800-53 Revision 4 dokumentumban szereplő a biztonsági előirányzatban meghatározott logikai védelmi intézkedéseknek MEGFELELÉS ÉRTÉKELÉSI JELENTÉS V1.0

2.3 Az értékeléshez felhasznált fejlesztői bizonyítékok

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

cím	fájl	időpont
MobilSign_SST	MobilSign biztonsági előirányzat	2015.07.13
Rendszerterv	TSign_Rendszerterv.docx	2015.03.18
Funkcionális Specifikáció	Funkcionalis_Specifikacio_ MobilSign.docx	2015.03.18
WebPolicy 1.0	MobilSign_WebPolicy.pdf	2015.05.11
AdminTools dokumentáció 1.0	MobilSign_AdminTools.pdf	2015.05.11
Rendszer telepítési útmutató 1.0	MobilSign_Rendszer_Telepitesi_Utmutato.pdf	2015.05.11
NetLock CA server (NCA) üzemeltetési dokumentációja	NCA_uzemeltetesi_doc_v02_1.doc	2015.03.18
M4	"MobilSign_692-M4_ v20_BRU.docx"	2015.07.01
Admin portál felhasználói kézikönyv	Felhasznaloi kezikonyv - Admin portal - v1.0.pdf	2015.07.11
Aláíró kliens felhasználói kézikönyv	Felhasznaloi kezikonyv - Alairo kliens - v1.0.pdf	2015.07.11
Naplózási összefoglaló	TSign_Naplozasi_osszefoglalo.pdf	2015.06.24
Kripto környezet folyamat működtetésének leírása	Mobilsign crypto környezet működtetési folyamatleírása.doc	2015.07.01
Harmadik feles alkalmazások	TSign_Harmadik_feles_alkalmazasok.docx	2015.03.18

MobilSign-hoz átadott telepítőkészletek listája	Telepítőkészletek mappája	2015.06.18
MobilSign rendszer leltár	MobilSignProd_Leltár_HW SW.docx	2015.06.19
Log minta	log_data.zip	2015.03.18
Funkcionális teszt terv	TSign_Funkcionalis_Teszt_ Terv.docx	2015.03.18
Aláíró tanúsítvány 1.	MagyarTelekom_aláíró_1_c er.pem	2015.04.03
Aláíró tanúsítvány 2.	MagyarTelekom_aláíró_2_c er.pem	2015.04.03
Aláírás minta	sinature.pem	2015.04.03
Időbélyeg minta	timestamp.pem	2015.04.03
Értékelői kérdésekre válaszok 2015.04.30.	Hunguard QandA_final.doc	2015.04.30
eToken tanúsítvány kérések	eToken_req.zip	2015.05.16
Fejlesztői válaszok a feltett kérdésekre	Kérdések.docx	2015.07.11

3 Értékelés eredményei

3.1 A rendszer biztonsági előirányzat értékelése

A *rendszer biztonsági előirányzat* felépítése és tartalma megfelel az elvárásoknak:

Az SST egy belső ellentmondásoktól mentes, teljes és egymást erősítő biztonsági követelményrendszert határoz meg, egyúttal magas szinten át is tekinti, hogy a MobilSign rendszer hogyan teljesíti a biztonsági követelményeket.

3.2 Az értékelt rendszer biztonsági architektúrájának értékelése

MobilSign csak egyetlen külső rendszerhez csatlakozik:

1. Netlock hitelesítés-szolgáltatóhoz, ahonnan a funkcionalitásához elengedhetetlenül szükséges visszavonási listákat kér le, szabványos protokollon keresztül.

MobilSign a Magyar Telekom egyéb belső rendszereitől is a funkcionálisan lehetséges módon leválasztásra került, jelenleg csak az alábbi belső kapcsolódásai vannak:

1. JAZZ rendszer értesíti a MobilSign rendszert letölthető dokumentumokról;
2. eStore-on keresztül történik a dokumentum letöltése;
3. az aláírt dokumentumot a rendszer szintén az eStore-ba tölti vissza;
4. az Aláíró kliens a JAZZ rendszerben hitelesíti az ügyintéző felhasználót;
5. az intraneten keresztül éri el a rendszer a Magyar Telekom időbélyeg szolgáltatását, amely az aláíráshoz az időbélyeget szolgáltatja;
6. az aláíráshoz MobilSign az Mtrack/NCA aláíró szervert használja, ami a Magyar Telekom egy már létező szolgáltatása. A kapcsolódás Message Queue-n keresztül történik, megfelelő hitelesítéssel.

Valamennyi fenti kapcsolódás (interfész) jól meghatározott.

A tervezési dokumentációk értékelése alapján megállapítható, hogy MobilSign rendszer egy jól átgondolt, a biztonságot kitüntetett szempontként kezelt fejlesztés, illetve integrálás eredménye.

3.3 A rendszer telepítési, konfigurálási és üzemeltetési útmutatóinak a vizsgálata

A telepítési útmutatók a Frontend, alkalmazásszerver, aláírószerver valamint a szakértői és adminisztrációs munkaállomás telepítését és konfigurálását írják le. Az útmutatóban leírt lépések egy általános Windows Server ismeretekkel rendelkező rendszergazda számára egyértelműen követhetőek.
Üzemeltetési útmutatók közül az M4 tartalmazza a rendszer legfontosabb üzemeltetési paramétereit, mint pl. kulcsok cseréje, mentések kezelése. Az adminisztrációs munkaállomásokon és a szakértői munkaállomáson használt parancssoros programok összes lehetséges funkcióját részletesen ismerteti az AdminTools leírás. WebPolicy konfigurációs paraméterek leírása részletesen ismerteti a Frontend, Alkalmazásszerver és Aláírószerveren használt program policy fájljaiban alkalmazható konfigurációs beállításokat. A Naplózási

összefoglaló a rendszerben előforduló hibaüzenetek és azoknak lehetséges okait sorolja fel. Kripto környezet folyamat működtetésének leírása a kriptográfiai kulcsok generálásának és a bizonyíték rekord megoldásának folyamatát mutatja be. Az NCA üzemeltetési leírás az NCA-val kapcsolatos üzemeltetési feladatokat írja le. Az üzemeltetési útmutatók egymással összhangban vannak, ellentmondásoktól mentesek, általános rendszergazdai ismeretekkel egyértelműen követhetőek.
Az Admin portál Felhasználói kézikönyv megfelelő részletességgel ismerteti az Admin portál funkcióit, megtalálhatóak benne a különböző szerepkörök által elérhető funkciók. Az Aláíró kliens Felhasználói kézikönyv szintén megfelelő részletességgel ismerteti az Aláíró kliens funkcióit.

Az útmutatók értékelésével megállapítható, hogy az MobilSign rendszer biztonságosan lett kialakítva és konfigurálva, valamint biztonságosan üzemeltethető.

3.4 A rendszer konfiguráció vizsgálata

A konfigurációs változások kezelése szabályozott:

- az alkalmazás verziókezelése megoldott,
- az informatikai környezet változásait a szervezet változáskezelési szabályainak megfelelően, megfelelő dokumentáltság mellett (HP SM) végzik,
- az alkalmazás később feltárt hibáinak bejelentésére a ClearQuest hibabejelentő oldalát használják,
- az eToken-ek, nShield ACS, OCS és Security World, valamint a hozzájuk tartozó jelszavak változásának kezelését a „Mobilsign crypto környezet működtetési folyamatleírása.doc”-ban leírt folyamat biztosítja.

A rendszer konfiguráció listája teljes, tartalmazza a rendszer valamennyi hardver és szoftver elemét, köztük a telepített programokat, a telepített szolgáltatásokat, az IIS-en futó webes alkalmazásokat, valamint a harmadik felek által készített szoftver komponensek táblázatát is (ez utóbbit a fejlesztőkkel és a használt verziószámokkal).

3.5 A rendszer biztonsági tesztelése

A rendszer biztonsági tesztelésének értékelése a fejlesztőktől és az üzemeltetőktől kapott *tesztelési dokumentációk* vizsgálatán, valamint az értékelők által elvégzett független tesztelés eredményein alapult.

A biztonsági teszteléssel kapcsolatosan az alábbi állítások összegezhetők:

- Az egyes alkalmazásmodulok fejlesztői alaposan tesztelték moduljaikat.
- MobilSign biztonsági funkcionalitása megfelelő módon tesztelésre került.
- A tesztelés érintette a rendszer külső interfészeinek és biztonsági moduljainak nagy részét.
- Az értékelők független teszteléssel megerősítették a helyes és biztonságos működést.

A rendszer tesztelése megfelelő eredményt mutatott.

3.6 A rendszer sebezhetőség vizsgálata

Mivel a MobilSign rendszer a környezetéhez jól meghatározott interfészeken keresztül kapcsolódik, illetve a belső komponensek is jól meghatározott interfészeken kapcsolódnak egymáshoz, ezeknek az interfészeknek a megvalósítását vizsgáltuk sebezhetőség szempontjából. A rendszer összetett kriptográfiai megoldásokat használ, a rendelkezésre álló dokumentációk alapján ellenőrzésre került, hogy a használt kriptográfiai megoldások megvalósítása megfelelő-e.

A sebezhetőség vizsgálat másik része a konfigurációs lista és ezen belül a harmadik fél által készített alkalmazások listája alapján ellenőrizte a felhasznált biztonsági szempontból kritikus komponenseket, elemezve, hogy a felhasznált verziókhoz tartozik-e a nyilvános sérülékenység adatbázisban ismert sebezhetőség.

A rendszer interfészei mind a belső, mind a külső interfészek esetén megfelelően védettek, a tartományok közötti kommunikációhoz tartozó interfész kriptográfiai eszközökkel is védett.

A rendszerben használt kriptográfiai megoldások szabványos megoldásokat használnak, a leírások alapján megfelelő módon.

Az interfészek és a kriptográfiai funkciók biztonsági tesztelése megfelelő.

A komponenseken végzett nyilvános sérülékenységi adatbázisokon alapuló vizsgálat eredménye szerint a feltárt sérülékenységek között nincsen magas kockázatúnak minősített, a rendszer által használt funkciót érintő hiba.

Az éles rendszer végleges (R1) verziójának elemzése legalább közepes támadói potenciállal kihasználható sebezhetőséget nem tárt fel.

3.7 A biztonsági előirányzatban meghatározott követelményeknek való megfelelés

3.7.1 A CEN/TS 419241 által meghatározott követelményeknek való megfelelés

Követelmény	Teljesülés
SRG_M.1.1	megfelel
SRG_M.1.2	megfelel
SRG_M.1.3	megfelel
SRG_M.1.4	megfelel
SRG_M.1.5	megfelel
SRG_SO.1.1	megfelel
SRG_SO.2.1	megfelel
SRG_IA.1.1	megfelel
SRG_IA.1.2	megfelel
SRG_IA.1.3	megfelel
SRG_IA.1.4	megfelel
SRG_IA.2.1	megfelel
SRG_SA.1.1	megfelel
SRG_SA.1.2	megfelel
SRG_KM.1.1	megfelel
SRG_KM.1.2	megfelel
SRG_KM.1.3	megfelel
SRG_KM.2.1	megfelel
SRG_KM.2.2	megfelel
SRG_KM.2.3	megfelel
SRG_KM.3.1	megfelel
SRG_KM.3.2	megfelel
SRG_KM.3.3	megfelel
SRG_KM.4.1	megfelel
SRG_KM.4.2	megfelel
SRG_KM.6.1	megfelel
SRG_KM.6.2	megfelel
SRG_KM.6.3	megfelel
SRG_KM.7.1	megfelel
SRG_AA.1.1	megfelel
SRG_AA.1.2	megfelel
SRG_AA.2.1	megfelel
SRG_AA.2.2	megfelel
SRG_AA.2.3	megfelel
SRG_AA.3.1	megfelel
SRG_AA.4.1	megfelel
SRG_AA.4.2	megfelel
SRG_AA.5.1	megfelel
SRG_AA.6.1	megfelel
SRG_AA.7.1	megfelel
SRG_AA.7.2	megfelel
SRG_AA.8.1	megfelel
SRG_AR.1.1	megfelel
SRG_AR.1.2	megfelel
SRG_AR.1.3	megfelel
SRG_AR.1.4	megfelel
SRG_AR.3.1	megfelel
SRG_BK.1.1	megfelel
SRG_BK.1.2	megfelel
SRG_BK.2.1	megfelel
SRG_BK.2.2	megfelel
SRC_DS.1.1	megfelel

Követelmény	Teljesülés
SRC_DS.1.2	megfelel
SRC_DS.1.3	megfelel
SRC_SA.1.1	megfelel
SRC_SA.1.2	megfelel
SRC_SA.1.3	megfelel
SRC_SA.2.1	megfelel
SRC_SA.2.2	megfelel
SRC_SC.1.1	megfelel
SRC_SC.1.2	megfelel
SRC_SC.2.1	megfelel
SRA_DA.1.1	nem vonatkozik
SRA_DA.1.2	nem vonatkozik
SRA_DA.1.3	nem vonatkozik
SRA_DA.2.1	nem vonatkozik
SRA_DA.2.2	nem vonatkozik
SRA_DA.2.3	nem vonatkozik
SRA_DA.3.1	nem vonatkozik
SRA_DA.3.2	nem vonatkozik
SRA_DA.3.3	nem vonatkozik
SRA_DA.3.4	nem vonatkozik
SRA_DA.3.5	nem vonatkozik
SRA_DA.3.6	nem vonatkozik
SRA_DA.3.7	nem vonatkozik
SRA_DA.3.8	nem vonatkozik

3.7.2 A CEN munkacsoport megállapodásban a minősített elektronikus aláírásokat létrehozó rendszerektől megkövetelt funkcionális és biztonsági követelményeknek való megfelelés.

Funkcionális követelmény	Teljesülés
F_SCA_1	részlegesen megfelel
F_SDP_1	megfelel
F_SDP_2	megfelel
F_SDP_3	megfelel
F_SDP_4	megfelel
F_SAV_1	megfelel
F_SAV_2	megfelel
F_SAV_3	megfelel
F_SIC_1	megfelel
F_SIC_2	megfelel
F_SIC_3	megfelel
F_DTBSF_1	megfelel
F_DTBSF_2	megfelel
F_DHC_1	megfelel
F_DHC_2	megfelel
F_SSC_1	megfelel
F_SSC_2	megfelel
F_SSC_3	megfelel
F_SSC_4	megfelel
F_SSC_5	megfelel
F_SSC_6	megfelel
F_SSC_7	megfelel
F_SSC_8	megfelel
F_SSA_1	megfelel
F_SDC_1	megfelel
F_SDOC_1	megfelel
F_I/O-1	megfelel

Funkcionális követelmény	Teljesülés
F_I/O-2	megfelel
F_I/O-3	megfelel
F_ISV-1	megfelel
F_ISV-2	megfelel
F_ISV-3	megfelel
F_USV-1	nem vonatkozik rá a követelmény
F_human_1	nem vonatkozik rá a követelmény
F_human_2	nem vonatkozik rá a követelmény
F_human_3	nem vonatkozik rá a követelmény
F_human_4	nem vonatkozik rá a követelmény
F_human_5	nem vonatkozik rá a követelmény
F_human_6	nem vonatkozik rá a követelmény
F_human_7	megfelel
F_machine_1	nem vonatkozik rá a követelmény
F_machine_2	megfelel
F_general_1	megfelel
F_protocol	megfelel
F_format	részlegesen megfelel
F_principles	megfelel

Biztonsági követelmény	Teljesülés
S_SCA_1	megfelel
S_SCA_2	megfelel
S_SCA_3	nem vonatkozik rá a követelmény
S_SCA_4	nem vonatkozik rá a követelmény
S_SCA_5	megfelel
S_SCA_6	megfelel
S_SCA_7	megfelel
S_SCA_8	megfelel
S_SCA_9	megfelel
S_SCA_10	megfelel
S_SCA_11	megfelel
S_SCA_12	megfelel
S_SDP_1	megfelel
S_SDP_2	megfelel
S_SDP_3	megfelel
S_SDP_4	megfelel
S_SDP_5	megfelel
S_SDP_6	megfelel
S_SDP_7	megfelel
S_SDP_8	megfelel
S_SDP_9	megfelel
S_SDP_10	megfelel
S_SDP_11	megfelel
S_SDP_12	megfelel
S_SAV_1	megfelel
S_SAV_2	megfelel
S_SAV_3	megfelel
S_SAV_4	megfelel
S_SAV_5	megfelel
S_SAV_6	megfelel
S_SAV_7	megfelel
S_SAV_8	megfelel
S_SIC_1	megfelel
S_SIC_2	megfelel
S_SIC_3	megfelel
S_SIC_4	megfelel

Biztonsági követelmény	Teljesülés
S_SIC_5	megfelel
S_SAC_1	megfelel
S_SAC_2	megfelel
S_SAC_3	megfelel
S_SAC_4	megfelel
S_SAC_5	nem vonatkozik rá a követelmény
S_SAC_6	megfelel
S_SAC_7	megfelel
S_SAC_8	megfelel
S_SAC_9	nem vonatkozik rá a követelmény
S_SAC_10	nem vonatkozik rá a követelmény
S_SAC_11	nem vonatkozik rá a követelmény
S_SAC_12	nem vonatkozik rá a követelmény
S_DTBSF_1	megfelel
S_DHC_1	megfelel
S_DHC_2	megfelel
S_DHC_3	megfelel
S_SSC_1	megfelel
S_SSC_2	nem vonatkozik rá a követelmény
S_SSC_3	megfelel
S_SSC_4	megfelel
S_SSA_1	megfelel
S_SDC_1	megfelel
S_I/O_1	megfelel
S_I/O_2	megfelel
S_I/O_3	megfelel
S_VER_1	megfelel

3.7.3 A NIST Special Publication 800-53 Revision 4 dokumentumban szereplő logikai védelmi intézkedéseknek való megfelelés

Konfigurációkezelés

Azonosító	Intézkedés, értékelés
CM-1	**3.3.1.1 Konfigurációkezelési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
CM-2	**3.3.1.2 Alapkonfiguráció** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
CM-3	**3.3.1.3 A konfigurációváltozások felügyelete, változáskezelés** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
CM-3 (2)	**3.3.1.3.2 Előzetes tesztelés és megerősítés** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
CM-4	**3.3.1.4 Biztonsági hatásvizsgálat** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
CM-6	**3.3.1.6 Konfigurációs beállítások** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
CM-7	**3.3.1.7 Legszűkebb funkcionalitás** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
CM-8	**3.3.1.8 Elektronikus információs rendszerelem leltár**

	Döntés: megfelelt *Vizsgálati módszerek: Audit*
CM-10	**3.3.1.10 A szoftverhasználat korlátozásai** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
CM-11	**3.3.1.11 A felhasználó által telepített szoftverek** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*

Üzletmenet (ügymenet) folytonosság

Azonosító	Intézkedés, értékelés
CP-1	**3.3.2.1 Üzletmenet folytonosságra vonatkozó eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
CP-2	**3.3.2.2 Üzletmenet folytonossági terv informatikai erőforrás kiesésekre** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Audit*
CP-3	**3.3.2.3 A folyamatos működésre felkészítő képzés** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
CP-9	**3.3.2.8 Az elektronikus információs rendszer mentései** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
CP-10	**3.3.2.9 Az elektronikus információs rendszer helyreállítása és újraindítása** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Interjú, Audit*

Karbantartás

Azonosító	Intézkedés, értékelés
MA-1	**3.3.3.1 Rendszer karbantartási eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
MA-2	**3.3.3.2 Rendszeres karbantartás** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
MA-5	**3.3.3.5 Karbantartók** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*

Adathordozók védelme

Azonosító	Intézkedés, értékelés
MP-1	**3.3.4.1 Adathordozók védelmére vonatkozó eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
MP-2	**3.3.4.2 Hozzáférés az adathordozókhoz** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
MP-6	**3.3.4.6 Adathordozók törlése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
MP-7	**3.3.4.7 Adathordozók használata** *Döntés: kockázat felvállalást igényel* *Vizsgálati módszerek: Interjú, Audit*

Azonosítás és hitelesítés

Azonosító	Intézkedés, értékelés
IA-1	**3.3.5.1 Azonosítási és hitelesítési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú , Audit*
IA-2	**3.3.5.2 Azonosítás és hitelesítés (belső felhasználók)** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
IA-2 (1)	**3.3.5.2.2 Hálózati hozzáférés privilegizált fiókokhoz** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
IA-4	**3.3.5.4 Azonosító kezelés** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
IA-5	**3.3.5.5 A hitelesítésre szolgáló eszközök kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
IA-6	**3.3.5.6 A hitelesítésre szolgáló eszköz visszacsatolása** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
IA-7	**3.3.5.7 Hitelesítés kriptográfiai modul esetén** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IA-8	**3.3.5.8 Azonosítás és hitelesítés (szervezeten kívüli felhasználók)** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IA-H	**3.3.5.8.2 Hitelesítésszolgáltatók tanúsítványának elfogadása** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*

Hozzáférés ellenőrzés

Azonosító	Intézkedés, értékelés
AC-1	**3.3.6.1 Hozzáférés ellenőrzési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AC-2	**3.3.6.2 Felhasználói fiókok kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AC-3	**3.3.6.3 Hozzáférés ellenőrzés érvényesítése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
AC-7	**3.3.6.7 Sikertelen bejelentkezési kísérletek** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
AC-8	**3.3.6.8 A rendszerhasználat jelzése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AC-14	**3.3.6.12 Azonosítás/hitelesítés nélkül engedélyezett tevékenységek** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
AC-17	**3.3.6.13 Távoli hozzáférés** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AC-18	**3.3.6.14 Vezeték nélküli hozzáférés** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AC-19	**3.3.6.15 Mobil eszközök hozzáférés ellenőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AC-20	**3.3.6.16 Külső elektronikus információs rendszerek használata** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú,Audit*
AC-22	**3.3.6.18 Nyilvánosan elérhető tartalom** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú,*

Rendszer- és információsértetlenség

Azonosító	Intézkedés, értékelés
SI-1	**3.3.7.1 Rendszer- és információsértetlenségre vonatkozó eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
SI-2	**3.3.7.3 Hibajavítás** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
SI-3	**3.3.7.4 Kártékony kódok elleni védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
SI-4	**3.3.7.5 Az elektronikus információs rendszer felügyelete** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
SI-5	**3.3.7.6 Biztonsági riasztások és tájékoztatások** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*

Azonosító	Intézkedés, értékelés
SI-12	**3.3.7.12 A kimeneti információ kezelése és megőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*

Naplózás és elszámoltathatóság

Azonosító	Intézkedés, értékelés
AU-1	**3.3.8.1 Naplózási eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AU-2	**3.3.8.2 Naplózható események** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
AU-3	**3.3.8.3 Naplóbejegyzések tartalma** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AU-12	**3.3.8.12 Naplógenerálás** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú, Audit*
AU-4	**3.3.8.4 Napló tárkapacitás** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AU-5	**3.3.8.5 Naplózási hiba kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AU-6	**3.3.8.6 Naplóvizsgálat és jelentéskészítés** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AU-8	**3.3.8.8 Időbélyegek** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
AU-9	**3.3.8.9 A naplóinformációk védelme** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*
AU-11	**3.3.8.11 A naplóbejegyzések megőrzése** *Döntés: megfelelt* *Vizsgálati módszerek: Interjú*

Rendszer- és kommunikációvédelem

Azonosító	Intézkedés, értékelés
SC-1	**3.3.9.1 Rendszer- és kommunikációvédelmi eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-5	**3.3.9.5 Túlterhelés –szolgáltatás megtagadás alapú támadás– elleni védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-7	**3.3.9.6 A határok védelme** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-12	**3.3.9.10 Kriptográfiai kulcs előállítása és kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-13	**3.3.9.11 Kriptográfiai védelem** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-15	**3.3.9.12 Együttműködésen alapuló számítástechnikai eszközök** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-20	**3.3.9.16 Biztonságos név/cím feloldó szolgáltatások (hiteles forrás)** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-21	**3.3.9.17 Biztonságos név/cím feloldó szolgáltatás (gyorsító táras)** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-22	**3.3.9.18 Architektúra és tartalékok név/cím feloldási szolgáltatás esetén** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
SC-39	**3.3.9.22 A folyamatok elkülönítése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*

Reagálás a biztonsági eseményekre

Azonosító	Intézkedés, értékelés
IR-1	**3.3.10.1 Biztonsági eseménykezelési eljárásrend** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IR-2	**3.3.10.2 Képzés a biztonsági események kezelésére** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IR-4	**3.3.10.4 A biztonsági események kezelése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IR-5	**3.3.10.5 A biztonsági események figyelése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IR-6	**3.3.10.6 A biztonsági események jelentése** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*
IR-7	**3.3.10.7 Segítségnyújtás a biztonsági események kezeléséhez** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*

Azonosító	Intézkedés, értékelés
IR-8	**3.3.10.8 Biztonsági eseménykezelési terv** *Döntés: megfelelt* *Vizsgálati módszerek: Audit*

3.8 Következtetések

A rendszer értékelés az alábbi fő következtetésekre jutott:

1. A MobilSign rendszer teljesíti a rendszer biztonsági előirányzatában felvállalt, MIBÉTS fokozott garanciaszinthez (SAP-F) tartozó garanciális elvárásokat.
2. A MobilSign rendszer kielégíti a rendszer biztonsági előirányzatában felvállalt, [2] CEN/TS 419241 által meghatározott követelményeket.
3. A MobilSign rendszer kielégíti a rendszer biztonsági előirányzatában felvállalt, egyúttal a [3] CEN munkacsoport megállapodásban a minősített elektronikus aláírásokat létrehozó rendszerektől megkövetelt funkcionális és biztonsági követelményeket.
4. A MobilSign rendszer kielégíti a rendszer biztonsági előirányzatában felvállalt, [4] NIST Special Publication 800-53 Revision 4 dokumentumban szereplő logikai védelmi intézkedésekhez tartozó követelményeket.

3.9 Feltételek

1. A jelen dokumentumban tanúsított kezdeti rendszerértékelés eredményeinek megerősítése, a tanúsítvány érvényességének megtartása és a maradvány kockázatok csökkentése céljából felülvizsgálati rendszerértékelést kell végrehajtani az alábbi esetekben:
   - a tanúsítvány érvényességi időszakában évente egy alkalommal (tervezett felülvizsgálati rendszerértékelés),
   - a rendszer architektúrájában vagy funkcionalitásában bekövetkezett változtatásokra reagálva (rendkívüli felülvizsgálati rendszerértékelés).

2. A működtetett rendszer architektúrájában vagy funkcionalitásában bekövetkezett jelentős változásokat a Megrendelő köteles a Tanúsítónak a változás érvénybe léptetését követő 30 napon belül bejelenteni, a tanúsítvány kiállítását megelőző vizsgálatoknak megfelelő mélységben a változások leírását tartalmazó dokumentációkat megküldeni.

3. A 2. esetben a tanúsítvány érvényességének fenntartásához a tanúsító értékeli a változásnak a hatásait és dönt a rendkívüli felülvizsgálati rendszerértékelés szükségességéről. A módosított rendszer állapotra – megfelelőség esetén - Tanúsítvány Karbantartási Jegyzőkönyvet állít ki. A tervezett vagy rendkívüli felülvizsgálati rendszerértékelés végrehajtásának feltételeit a Megrendelő köteles biztosítani.

4. A Rendszer Biztonsági Előirányzatban megfogalmazott alábbi környezeti biztonsági célokat, a rendszer üzemeltetőjének folyamatosan teljesíteni kell:

   OE.PM A szervezet teljesíti NIST SP 800-53 R4 következő intézkedéseit: PM-1, PM-2, PM-5, PM-10.

   OE.RA A szervezet teljesíti NIST SP 800-53 R4 következő intézkedéseit: RA-1, RA-2, RA-3.

   OE.PS A szervezet teljesíti NIST SP 800-53 R4 következő intézkedéseit: PS-4, PS-8

   OE.AT A szervezet teljesíti NIST SP 800-53 R4 következő intézkedéseit: AT-1, AT-2

   OE.PE A szervezet teljesíti NIST SP 800-53 R4 következő intézkedéseit: PE-1, PE-2, PE-3

3.10 Elvárások

A tanúsító elfogadja az értékelők által tett javaslatokat a rendszer vizsgálata során feltárt maradványkockázatok csökkentésére. Elvárja a működtetőtől, hogy az értékelők javaslatait, vagy azokkal egyenértékű egyéb intézkedésekkel az értékelési jelentésben szereplő maradványkockázatokat csökkentse. A tervezett felülvizsgálati rendszerértékelés során ezen intézkedések vizsgálata kiemelt szerepet fog kapni.

4 Javaslat a Tanúsítvány szövegezésére

4.1 Javaslat a Tanúsítvány főlapjának szövegezésére

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. a 9/2005. (VII.21.) IHM rendelet alapján, mint a Nemzeti Fejlesztési Minisztérium IKF/19519-2/2012/NFM számú Kijelölési okiratával kijelölt tanúsító szervezet

tanúsítja,

hogy a

Magyar Telekom Nyrt.

által üzemeltetett

MobilSign bolti aláíró rendszer

R1 verziója

az 1.számú mellékletben áttekintett funkcionalitással, valamint
a 2. számú melléklet feltételének figyelembe vételével

megfelel

a 2001. évi XXXV. törvényben szereplő

fokozott biztonságú elektronikus aláírás

létrehozására és kezdeti ellenőrzésére.

Jelen tanúsítvány a HUNG-TJ-071-2015. számú tanúsítási jelentés alapján került kiadásra. Készült a Magyar Telekom Nyrt. (1013 Budapest, Krisztina krt. 55.) megbízásából.

A tanúsítvány regisztrációs száma: **HUNG-T-071-2015.**
A tanúsítás kelte: 2015. július 24.
A tanúsítvány érvényesség vége: 2018. július 24.

4.2 Javaslat a Tanúsítvány mellékleteire

Javasoljuk, hogy a Tanúsítvány mellékleteiben a következők szerepeljenek:

- A MobilSign R1 legfontosabb tulajdonságainak összefoglalása az alábbi fejezetet alapján:

  1.2 a tanúsítás tárgya

- A tanúsítvány érvényességének feltétele az alábbi fejezet alapján

  3.9 Feltételek

- A tanúsítással és értékeléssel kapcsolatos módszertani hivatkozások az alábbi fejezet alapján:

  2.1 az alkalmazott módszertan

- A tanúsítási eljárás egyéb jellemzői
  - A tanúsításhoz figyelembe vett, fejlesztőtől független dokumentumok
  - A követelményeknek való megfelelést ellenőrzés vizsgálat garancia szintje

5 Hivatkozások

[1]: 2001. évi XXXV törvény az elektronikus aláírásról

[2]: Security Requirements for Trustworthy Systems supporting Server Signing; English version CEN/TS 419241:2014

[3]: CWA 14170:2004: Security Requirements for Signature Creation System, May 2004

[4]: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

[5]: MIBÉTS 2009 Rendszerekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása" projekt keretében kidolgozott dokumentum, v4 2008.09.19) (a KIB 28-as számú Ajánlás része)

[6]: MIBÉTS 2009 Útmutató rendszer értékelőknek (az „e-Közigazgatási Keretrendszer Kialakítása" projekt keretében kidolgozott dokumentum, v3 2008.09.19 (a KIB 28-as számú Ajánlás része)