Tanúsítási jelentés

Audi Hungaria Motor Kft. hiteles elektronikus másolatképzésre kialakított informatikai rendszer

HUNG-TJ-PEM-02-2016

Verzió:	1.0
Fájl:	HUNG-TJ-PEM-02-2016_v10.pdf
Minősítés:	Nyilvános
Oldalak:	18

Változáskezelés

Verzió	Dátum	A változás leírása
v0.1	2016.01.15.	A szerkezet felállítása
v0.2	2016.02.03.	Belső egyeztetésre kiadott verzió
v0.9	2016.02.04.	Külső egyeztetésre kiadott verzió
v1.0	**2016.02.05.**	**Végleges verzió**

A tanúsítási jelentést készítette:

dr. Szabó István
Hunguard Kft.
Tanúsítási divízió

Tartalom

I. Összefoglaló 4
I.1. A tanúsítás (és az értékelés, melyen a tanúsítás alapul) jellemzői 4
I.2. A tanúsítás tárgya 4
I.3. A rendszer főbb komponenseinek azonosítása 5
II. A tanúsítás jellemzése 6
II.1. Az alkalmazott értékelési módszer 6
II.2. A MIBÉTS fokozott garanciaszintű értékelés jellegzetességei 6
II.3. A tanúsításhoz felhasznált értékelési jelentések azonosítása 7
II.4. Az értékeléshez felhasznált fejlesztői bizonyítékok 7
II.5. Az értékelési folyamat tanúsítási szempontú ellenőrzése 8
III. Követelmények 9
III.1. Az értékelés eredménye 14
III.2. A biztonságos felhasználás feltételei 14
III.3. Javaslatok 16
IV. Javaslat a Tanúsítvány szövegezésére 17
IV.1. Javaslat a Tanúsítvány főlapjának szövegezésére 17
IV.2. Javaslat a Tanúsítvány mellékleteire 17
V. Hivatkozások 18
V.1. Módszertani hivatkozások 18

I. Összefoglaló

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

STOE név:	**Audi Hungaria Motor Kft. hiteles elektronikus másolatképzésre kialakított informatikai rendszer**
STOE rövid neve:	AHMK
STOE verzió:	2016.02.01-i állapot
Rendszer integrátor:	itelligence Hungary Informatika Kft. (1117 Budapest, Neumann János u. 1. Infopark A épület fsz.)
Rendszer működtető:	Audi Hungaria Motor Kft. (9027 Győr, Kardán utca 1)
Rendszer üzemeltető:	Audi Hungaria Motor Kft., IT Irányítási-/Támogató folyamatok csoport (SUP) (9027 Győr, Kardán utca 1)
Rendszer értékelő:	Hunguard Kft. Értékelési Divízió 1123. Budapest, Kékgolyó u. 6.

I.2. A tanúsítás tárgya

A tanúsítás tárgya az Audi Hungaria Motor Kft. által üzemeltetett hiteles másolatkészítő rendszer, amely a Microsec E-Szignó termékkel létrehozott elektronikus aláírás segítségével hitelesíti a beolvasott dokumentumok másolatát.

Az AHMK rendszer nagyszámú, elektronikus másolat létrehozását teszi lehetővé az alábbi jellemzőkkel:

- Az aláírandó TIFF állományok egy lapolvasó eszközben keletkeznek, papír alapú dokumentumok beolvasásával kerülnek aláírási műveletre átadásra az aláíró komponensnek, majd az ebből a kötegből elválasztott aláírt XML állományokat és az aláírt TIFF fájlokat egy külső rendszer használja fel.
- Az aláíró egy dedikált munkaállomáson áttekintheti, kihagyhatja vagy jóváhagyhatja az aláírandó állományokat, miután behelyezte a titkot tartalmazó operátori kártyáját a munkaállomáson elhelyezett kártyaolvasójába, illetve a munkaállomáson begépelte jelszavát.
- A hozzáférést a kártyaolvasó és a kliens oldali felület között kiépített megbízható útvonal védi.
- Az AHMK rendszer által megvalósítandó folyamat magában foglalja az alábbiakat:
    - az aláírandó dokumentumok beolvasása dedikált hardverről, papír alapú dokumentum konvertálásával,
    - az aláírandó dokumentumok opcionális megtekintése, esetleges kihagyása az aláírandó dokumentumok közül,
    - a kiválasztott dokumentumokra egyenként fokozott elektronikus aláírás létrehozása (az operátori munkaállomásra csatlakoztatott kártyaolvasón keresztül az aláíró operátori kártyáján lévő információkkal elérhető magánkulcs aktivizálásával),
    - a kiválasztott dokumentumokra egyenként fokozott elektronikus aláírás létrehozása a szerveren tárolt magánkulcs automatikus aktivizálásával és időbélyegzése időbélyeg-szolgáltatótól kért időbélyeggel,
    - az aláírások kezdeti ellenőrzése,
    - az aláírás eredményeinek opcionális lekérése.

Az AHMK rendszer biztonsági funkciói magában foglalják az alábbiakat:

- hozzáférés ellenőrzés (a nyújtott szolgáltatásokat csak az arra jogosultak érik el, a megfelelő azonosítás és hitelesítés után);
- a hitelesített dokumentum integritásának és megfelelőségének garantálása;
- a hitelesített dokumentumhoz kapcsolt, aláírt metaadatok integritásának és megfelelőségének garantálása;
- fokozott 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),
- rendszer és kommunikáció védelem,
- önvédelem (a biztonsági funkciók megkerülése vagy lerontása elleni védelem).

I.3. A rendszer főbb komponenseinek azonosítása

A rendszer elemei és az elemek funkciói:

Hiteles másolatképzés folyamatrész	Kapcsolódó rendszerkomponens	Komponens verziószám
Hitelesítendő dokumentumok szkennelése	Enterprise Scan (OpenText Imaging Enterprise Scan)	v 10.2.0.
Digitális másolat aláírása és időbélyegzése	e-Szignó Hitelesítő Szerver és kliens	v 3.2.8.1.
Hitelesített digitális másolat továbbítása a rendszerben	Document Pipeline DocTool-ok: - signdoccli - doctosrvdp - addts - waitgp - signdocsrv	v 1.0.0.
Dokumentumok megjelenítése	TCP kliens- és szerver komponensek - TCP Application Server - TCP Business Object Layer (Context Server) - TCP User Management Server - TCP WebClient - Imaging Viewer - OpenText Archive Server	v 10.2.1.
Tárolt dokumentumok letöltése ('Download Signed Document' TCP funkció)	SignedDocument TCP WebClient Plugin	v 1.0.0.
Dokumentumok hitelességének ellenőrzése ('Validate Document' TCP funkció)	SignedDocument TCP WebClient Plugin	v 1.0.0.
Újrahitelesítés	ReCertify web application	v 1.0.0.

II. A tanúsítás jellemzése

Jelen tanúsítás a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól szóló 13/2005. (X. 27.) IHM rendelet elvárásainak teljesülését vizsgálja, azon belül annak megerősítését, hogy a vizsgált rendszer által a papíralapú dokumentumokról elektronikus úton készített másolatok hitelesnek - joghatás kiváltására alkalmasnak - tekinthetők-e.

II.1. Az alkalmazott értékelési módszer

Az AHMK rendszer értékelésére az V.1 fejezetben meghatározott, rendszerekre vonatkozó értékelési módszertant alkalmazták, az alábbi pontosításokkal:

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

Az alkalmazott értékelési módszertan megkülönbözteti a kezdeti és a felülvizsgálati értékelés típust, s ezekhez eltérő értékelői feladatokat rendel.

II.2. A MIBÉTS fokozott garanciaszintű értékelés jellegzetességei

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

a) a rendszer biztonsági előirányzatának és biztonsági architektúrájának az értékelése,

b) a rendszer telepítési és üzemeltetési útmutatóinak a vizsgálata,

c) a rendszer konfiguráció vizsgálata,

d) a rendszer biztonsági tesztelése,

e) a rendszer sebezhetőség vizsgálata.

A rendszer biztonsági előirányzatának és a biztonsági architektúra értékelése alapvetően arra a kérdéskörre koncentrál, hogy mennyiben tekinthető a rendszer zártnak, vagyis megvédi-e magát a nem-megbízható aktív egyedek hamisításaitól (önvédelem) és a biztonsági funkcionalitást nem lehet-e megkerülni (megkerülhetetlenség). A különböző terv dokumentációk tanulmányozása egyúttal elősegíti az értékelt rendszer jobb megismerését, s ezen keresztül a további vizsgálatok hatékony végrehajtását.

A rendszer telepítési és üzemeltetési útmutatók vizsgálatának célja annak ellenőrzése, hogy a rendszer biztonságában különböző felelősségeket betöltő szereplők rendelkeznek-e a szükséges információkkal.

A rendszer konfiguráció vizsgálatának elsődleges célja annak megerősítése, hogy minden rendszer komponens helyes verziója, beállítása az értékelő rendelkezésére áll.

A rendszer biztonsági tesztelésének célja annak ellenőrzése, hogy a működő informatikai rendszer – miután a rendszer architektúrájának és a rendszer konfigurálási útmutatójának megfelelően telepítették, integrálták és konfigurálták - a biztonsági követelményeknek megfelelően működnek.

[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.

A rendszer sebezhetőség vizsgálat célja annak a megállapítása, hogy vannak-e hibák vagy gyengeségek a rendszerben, ahogyan azt konkrét környezetében megvalósították, konfigurálták, illetve, hogy ezek kihasználhatók-e.

II.3. A tanúsításhoz felhasznált értékelési jelentések azonosítása

Rendszer értékelési jelentés:

- Audi Hungaria Motor Kft. hiteles elektronikus másolatképzésre kialakított informatikai rendszer RENDSZER ÉRTÉKELÉSI JELENTÉS v1.0

Mértékadó követelményrendszernek való megfelelés elemzés:

- Audi Hungaria Motor Kft. hiteles elektronikus másolatképzésre kialakított informatikai rendszer megfelelése a 13/2005. (X. 27.) IHM rendeletben meghatározott követelményeknek MEGFELELÉS ÉRTÉKELÉSI JELENTÉS v 1.0

II.4. Az értékeléshez felhasznált fejlesztői bizonyítékok

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

Tervezési dokumentációk:

- Audi Hungaria Motor Kft. hiteles elektronikus másolatképzésre kialakított informatikai rendszer, Rendszer Biztonsági Előirányzat v1.0
- Itelligence AUDI Hiteles másolatképzés Rendszerterv Hiteles másolatképzés v1.4.docx

Tesztelési dokumentációk:

- AUDI Hiteles másolat teszteset 01-Szkennelés indexelés v1.6
- AUDI Hiteles másolat teszteset 02-Ellenőrzés hibajavítás Pipelineban v1.6
- AUDI Hiteles másolat teszteset 03-Megjelenítés TCP-ben v1.6
- AUDI Hiteles másolat teszteset 04-Validálás letöltés TCP-ben v1.6
- AUDI Hiteles másolat teszteset 05-Újrahitelesítés v1.6
- AUDI Hiteles másolat teszteset 06-Biztonsági funkciók (kliens) v1.7
- AUDI Hiteles másolat teszteset 07-Biztonsági funkciók (szerver) v1.6
- AUDI Hiteles másolat teszteset 08-Csatornák v1.6

Felhasználási dokumentációk:

- itelligence -AUDI_Hiteles_másolatképzés_Telepítés_és_konfigurálás_kézikönyv_v1_3.docx
- itelligence -AUDI_Hiteles_másolatképzés_Üzemeltetői kézikönyv_Admin_v1_3.docx
- Itelligence-AUDI_Hiteles_másolatképzés_Felhasználói_kézikönyv_v1_3.docx
- AUDI DMS Felhasználói kézikönyv v 1 1.pdf
- AUDI DMS Üzemeltetési kézikönyv v1.pdf
- ES 102 User&AdministrationGuide.pdf
- e-Szignó Hitelesítő szerver telepítési útmutató.pdf
- e-Szigno kartya utmutato.pdf
- JRE telep segedlet v1.pdf
- OpenText Archive Server 10.1.1 - Installation on UNIX-Linux English (AR100101-IASUO-EN-8).pdf
- OpenText Document Pipeline 10.1.1 - Installation Guide English (AR100101-IDPDP-EN-2).pdf
- OpenText Imaging Enterprise Scan 10.2.0 - Installation Guide English (CLES100200-IGD-EN-2).pdf
- TCP 102 AdministratorsGuide.pdf
- TCP 102 UserGuide.pdf

II.5. Az értékelési folyamat tanúsítási szempontú ellenőrzése

A tanúsítási jelentés készítői a teljes értékelési folyamatot figyelemmel kísérték, ellenőrizték:

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

III. Követelmények

Az alábbiakban megadjuk a jogszabályban előírt követelményeket, melyek értékelése a III.1. alfejezetben kerül megadásra.

Általános_szabály_1_elv /4. § (1)[3]/

A papíralapú dokumentumról történő elektronikus másolatkészítés során a másolatkészítő biztosítja a papíralapú dokumentum és az elektronikus másolat képi vagy tartalmi megfelelését, és azt, hogy minden – az aláírás elhelyezését követően az elektronikus másolaton tett – módosítás érzékelhető legyen.

Általános_szabály_2_folyamat /4. § (2)/

Papíralapú dokumentumról történő elektronikus másolat készítése során a másolat készítője elkészíti az elektronikus másolatot, megállapítja a papíralapú dokumentum és az elektronikus másolat képi vagy tartalmi megfelelését, majd a (3) bekezdésben meghatározott metaadatok elhelyezését követően az elektronikus másolatot hitelesítési záradékkal („Az eredeti papíralapú dokumentummal egyező") és a (4) bekezdésben meghatározott követelményeknek megfelelő elektronikus aláírással látja el.

Általános_szabály_3_metadatok /4. § (3)/

Az elektronikus másolatot a következő metaadatok elhelyezésével kell létrehozni és azt egyértelműen az eredeti papíralapú dokumentumhoz rendelni:

a) a papíralapú dokumentum megnevezése;

b) a papíralapú dokumentum fizikai méretei;

c) a másolatkészítő szervezet elnevezése és – ha a másolatkészítés nem az automatikus másolatkészítés 4/A. §-ban lévő szabályai szerint történik – a másolat képi vagy tartalmi egyezéséért felelős személy neve;

d) a másolatkészítő rendszer, illetve a másolatkészítési szabályzat pontos megnevezése és verziószáma;

e) a másolatkészítés ideje;

f) az irányadó másolatkészítési rend elérhetősége.

Általános_szabály_4_részleges_másolat /4. § (3a)/

Ha a papír alapú dokumentum tulajdonságai miatt az elektronikus másolat nem tartalmazza a papír alapú dokumentum teljes tartalmát, a (3) bekezdés szerinti metaadatok között azt is fel kell tüntetni, hogy a másolat a készítésének alapjául szolgáló papír alapú dokumentumot mely részében tartalmazza. Az igénylő ilyen rendelkezése esetén a másolatkészítő elektronikus kivonatot is készíthet a papír alapú dokumentumról, a másolaton rögzítve azt, hogy a készített elektronikus kivonat a papír alapú dokumentumot mely részében, a dokumentumba foglalt információtartalmat milyen korlátozásokkal tartalmazza.

[3] 13/2005. (X. 27.) IHM rendelet alapján

Általános_szabály_5_aláírás /4. § (4)/

A másolaton szervezeti aláírást vagy olyan, legalább fokozott biztonságú elektronikus aláírást kell elhelyezni, amelyre vonatkozóan a hitelesítés-szolgáltató kizárja az álnév használatát, és az álnév használatának kizárása céljából biztosítja, hogy a regisztráció alapjául szolgáló személyazonosság igazolására alkalmas hatósági igazolványban foglalt névvel betű szerint azonos a tanúsítványba foglalt név.

Általános_szabály_6_dokumentum-csoportok /4. § (5)/

Több dokumentumon is elhelyezhető egy elektronikus aláírás, illetőleg egy időbélyegző, valamint a (3) bekezdés szerinti metaadatok több dokumentumon együttesen is elhelyezhetőek. Ez esetben a dokumentumok a továbbiakban csak együtt kezelhetők.

Általános_szabály_7_érvényességi_idő /4. § (6)/

Az aláírónak külön jogszabályban meghatározott követelmények szerint gondoskodnia kell az elhelyezett aláírás érvényességének érvényességi időn belüli – ha az érvényességi idő nem meghatározott, úgy korlátlan ideig történő – folyamatos megállapíthatóságáról.

Általános_szabály_8_feljogosítás /4. § (7)/

A másolatkészítéssel megbízott vagy arra feljogosított személy, személyek körét belső szabályzatban kell meghatározni.

Általános_szabály_9_hozzájárulás /4. § (8)/

A másolatkészítőnek rendelkeznie kell a másolatkészítő személy külön jogszabályban meghatározott hozzájárulásával, amelyben a másolatkészítő személy e §-ban meghatározott személyes adatainak a másolatkészítés céljára történő kezelését engedélyezi.

Általános_szabály_10_dokumentáltság /4. § (9)/

A másolatkészítőnek rendelkeznie kell a másolatkészítő rendszer olyan részletességű dokumentációjával, amelyből a rendszerrel szemben e rendeletben megállapított követelmények teljesülése megállapítható, vagy a rendszer gyártója/forgalmazója által kiállított, a megfelelésre vonatkozó igazolással.

Általános_szabály_11_másolatkészítési_rend /4. § (10)/

A másolatkészítőnek rendelkeznie kell a másolatkészítés eljárási és műszaki feltételeit, valamint a kapcsolódó felelősségi kérdéseket tartalmazó másolatkészítési renddel. A másolatkészítő a másolatkészítési rendet nyilvánosan, elektronikus úton közzéteszi.

Általános_szabály_12_dokumentumformátum /4 § (11)/

Az elektronikus másolatot olyan dokumentumformátumban kell létrehozni, ami lehetővé teszi a hiteles elektronikus másolat jogszabályban meghatározott módon történő hosszú távú megőrzését.

Automatikus_másolatkészítés_1_feltételek /4/A § (1)/

A másolat automatikusan is elkészíthető, ha

a) a másolatkészítés zárt rendszerben történik, amelynek külső beavatkozástól mentes, az eredeti és a másolat összerendelését tekintve garantáltan hibamentes működését auditálás igazolja;

b) a másolatkészítő rendszer megfelelő műszaki és szervezési megoldással biztosítja a másolat olvashatóságát és a mintavételezésen alapuló minőségbiztosítást;

c) a záradék tartalmazza az automatikus másolatkészítés tényét.

Automatikus_másolatkészítés_2_mintavételezés /4/A § (2)/

Automatikus másolatkészítés esetén a dokumentumonkénti tartalmi ellenőrzés helyett véletlenszerű mintavételezésen alapuló ellenőrzés is alkalmazható. Ha jogszabály az eredeti dokumentum megsemmisítését lehetővé teszi, az eredeti dokumentum megőrzését abban az esetben is legalább addig biztosítani kell, amíg a másolat olvashatóságát (megnyithatóságát) a másolatkészítő vagy a másolatot felhasználó nem ellenőrizte és vissza nem igazolta.

Automatikus_másolatkészítés_3_hitelesítés /4/A § (3)/

Az automatikusan készített másolatot szervezeti aláírással és időbélyegzővel kell ellátni.

Automatikus_másolatkészítés_4_kivételek /4/A § (4)/

Automatikus másolatkészítésre a 4. § rendelkezései a 4. § (3) bekezdés a) és b) pontja, valamint a 4. § (8) bekezdése kivételével alkalmazandóak.

Közokirat_másolata_1_előírt_formátum /5 § (1)/

A papíralapú közokiratról vagy papíralapú teljes bizonyító erejű magánokiratról és egyéb papíralapú magánokiratról közokirat kiállítására jogosult vagy a jogszabály szerint közokiratról hiteles másolat készítésére jogosult kijelölt szervezet (jelen alcím alkalmazásában a továbbiakban: közokirat kiállítására jogosult) általi hiteles másolatkészítés esetén az elektronikus másolatot a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (a továbbiakban: Ket.) szerinti elektronikus ügyintézési felügyelet által, a papír alapú irat átalakítása hiteles elektronikus irattá szabályozott elektronikus ügyintézési szolgáltatásra vonatkozóan előírt valamely formátumban kell létrehozni.

Közokirat_másolata_2_eltérések /5 § (2)/

Papíralapú közokiratról vagy papíralapú teljes bizonyító erejű magánokiratról és egyéb papíralapú magánokiratról történő elektronikus másolat készítése során a közokirat kiállítására jogosult a 4. § valamint a 4/A. § rendelkezéseit azzal az eltéréssel alkalmazza, hogy az elektronikus másolatot

a) olyan elektronikus aláírással látja el, amely aláírás megfelel az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól szóló kormányrendeletben a hatóság nevében dokumentum hitelesítésére alkalmazható elektronikus aláírással szemben meghatározott követelményeknek, vagy

b) az elektronikus ügyintézés részletes szabályairól szóló kormányrendeletben megadott egyéb módon hitelesíti.

Közokirat_másolata_3_automatikus_másolatkészítés /5 § (3)/

A papíralapú közokiratról vagy papíralapú teljes bizonyító erejű magánokiratról és egyéb papíralapú magánokiratról a közokirat kiállítására jogosult általi másolatkészítés során, a 4/A. § szerinti automatikus másolatkészítési eljárás alkalmazható a szervezethez érkezett papíralapú iratokról az ügyintézés céljára szolgáló másolat készítésére.

Közokirat_másolata_4_egyedi_ellenőrzés /5 § (4)/

Amennyiben a közokirat kiállítására jogosult a 4/A. § szerinti automatikus másolatkészítési eljárást ügyfelek vagy más szervek számára megküldendő iratok esetében alkalmazza, úgy köteles egyedileg ellenőrizni a másolatok egyezőségét.

Közokirat_másolata_5_kiszervezhetőség /5 § (5)/

A közokirat kiállítására jogosult a jelen § szerinti másolatkészítést a Ket. szerinti szabályozott elektronikus ügyintézési szolgáltatóra kiszervezheti.

Okirat_másolata_1_kiállított_okirat_képi_vagy tartalmi_megfelelése /6 § (1)/

Ha a papíralapú teljes bizonyító erejű magánokiratot vagy egyéb magánokiratot a gazdálkodó szervezet állította ki, akkor az erről az okiratról készített elektronikus másolat esetén e gazdálkodó szervezetnek, mint másolatkészítőnek a papíralapú okiratnak való képi vagy tartalmi megfelelést kell biztosítania. A másolatkészítő az elektronikus másolatot a 4. § (4) bekezdésében meghatározott követelményeknek megfelelő elektronikus aláírásával látja el, és arra időbélyegzőt helyeztet el olyan szolgáltatóval, amely ezt a szolgáltatást külön jogszabály szerinti minősített szolgáltatóként nyújtja.

Okirat_másolata_2_őrzött_okirat_képi_megfelelése /6 § (2)/

Ha a papíralapú közokiratot, a más által kiállított papíralapú teljes bizonyító erejű magánokiratot vagy egyéb magánokiratot a gazdálkodó szervezet őrzi, akkor az erről az okiratról készített elektronikus másolat esetén e gazdálkodó szervezetnek, mint másolatkészítőnek a papíralapú okiratnak való képi megfelelést kell biztosítania. A másolatkészítő az elektronikus másolatot a 4. § (4)

bekezdésében meghatározott követelményeknek megfelelő elektronikus aláírásával látja el, és arra időbélyegzőt helyeztet el olyan szolgáltatóval, amely ezt a szolgáltatást külön jogszabály szerinti minősített szolgáltatóként nyújtja.

Számviteli_bizonylat_másolata_1_képi_megfelelés /7 § (1)-(2)/

(1) Papíralapú számviteli bizonylatról történő elektronikus másolatkészítésre abban az esetben is ezt a §-t kell alkalmazni, ha az papíralapú közokiratnak vagy papíralapú teljes bizonyító erejű magánokiratnak minősül.

(2) A papíralapú számviteli bizonylatról az azt kiállító vagy őrző gazdálkodó szervezet által készített elektronikus másolat esetén biztosítani kell a papíralapú dokumentumnak történő képi megfelelést. Másolatkészítő az elektronikus másolatot a 4. § (4) bekezdésében meghatározott követelményeknek megfelelő elektronikus aláírásával látja el, és arra időbélyegzőt helyeztet el olyan szolgáltatóval, amely ezt a szolgáltatást külön jogszabály szerinti minősített szolgáltatóként nyújtja.

III.1. Az értékelés eredménye

Követelmény	Teljesülés
Általános_szabály_1_elv	teljesül
Általános_szabály_2_folyamat	teljesül
Általános_szabály_3_metadatok	teljesül
Általános_szabály_4_részleges_másolat	nem vonatkozik rá a követelmény
Általános_szabály_5_aláírás	teljesül
Általános_szabály_6_dokumentum-csoportok	nem vonatkozik rá a követelmény
Általános_szabály_7_érvényességi_idő	teljesül
Általános_szabály_8_feljogosítás	teljesül
Általános_szabály_9_hozzájárulás	teljesül
Általános_szabály_10_dokumentáltság	teljesül
Általános_szabály_11_másolatkészítési_rend	teljesül
Általános_szabály_12_dokumentumformátum	teljesül
Automatikus_másolatkészítés_1_feltételek	nem vonatkozik rá a követelmény
Automatikus_másolatkészítés_2_mintavételezés	nem vonatkozik rá a követelmény
Automatikus_másolatkészítés_3_hitelesítés	nem vonatkozik rá a követelmény
Automatikus_másolatkészítés_4_kivételek	nem vonatkozik rá a követelmény
Közokirat_másolata_1_előírt_formátum	nem vonatkozik rá a követelmény
Közokirat_másolata_2_eltérések	nem vonatkozik rá a követelmény
Közokirat_másolata_3_automatikus_másolatkészítés	nem vonatkozik rá a követelmény
Közokirat_másolata_4_egyedi_ellenőrzés	nem vonatkozik rá a követelmény
Közokirat_másolata_5_kiszervezhetőség	nem vonatkozik rá a követelmény
Okirat_másolata_1_kiállított:_képi_vagy tartalmi_megfelelés	teljesül
Okirat_másolata_2_őrzött:_képi_megfelelés	teljesül
Számviteli_bizonylat_másolata_1_képi_megfelelés	teljesül

III.2. A biztonságos felhasználás feltételei

Az aláírások érvényességének folyamatos megállapíthatósága az AHMK vizsgált *Másolatkészítés, Előfeldolgozás*, *Felülhitelesítés* alap funkcióin alapul. Annak érdekében, hogy az aláírások érvényesek is maradjanak a rendszerben, más védelmi intézkedésekre is szükség van. Az alábbi (1.-7.) feltételek olyan védelmi intézkedéseket várnak el, melyek együttesen alkalmasak a sértetlen megőrzésre is.

1. Feltétel (hibátlan aláírás)

Az adminisztrátorok a *Másolatkészítés*-kor végrehajtott aláírás ellenőrzés hibájáról kapott jelzés esetén derítsék fel a hiba okát, kezeljék az esetleges hiányosságokat, ellenőrizzék a rendszer integritását, vizsgálják felül a tanúsítványokat és készítsék el újra a másolatot.

2. Feltétel (hibátlan előfeldolgozás)

Az adminisztrátorok az *Előfeldolgozás*-kor végrehajtott ismételt aláírás ellenőrzés hibájáról kapott jelzés esetén derítsék fel a hiba okát, kezeljék az esetleges hiányosságokat, ellenőrizzék a rendszer integritását, vizsgálják felül a tanúsítványokat és kérjék az adott állomány ismételt küldését a másolatkészítőtől.

3. Feltétel (rendszer mentések)

Az üzemeltető:

- meghatározott gyakorisággal végezzen mentést a rendszerben tárolt felhasználószintű információkról (archívumról, adatbázisról);
- meghatározott gyakorisággal mentse el a vizsgált rendszerben tárolt rendszerszintű információkat;
- meghatározott gyakorisággal mentse el a vizsgált rendszer dokumentációját, köztük a biztonságra vonatkozókat is;
- védje meg a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását;
- meghatározott ideig őrizze meg a mentett információkat;
- biztosítsa a környezet fizikai biztonságát.

4. Feltétel (rendszer helyreállítása és újraindítása)

Az üzemeltető gondoskodjon a rendszer utolsó ismert állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

5. Feltétel (felülhitelesítés)

Rendszeresen kísérjék figyelemmel a használt kriptográfiai algoritmusokra vonatkozó biztonsági elvárásokat. Még azelőtt, hogy a TIFF és XML állományokra(ban) számolt hash algoritmus meggyengülne, az erre jogosult adminisztrátor alkalmazza az „újrahitelesítés”-t úgy, hogy a kiválasztott minta a teljes korábbi időszakra vonatkozó hitelesítő időpecsétek összessége legyen, az új (a korábban alkalmazott algoritmusnál erősebb) hash algoritmussal számoltasson hash értékeket és kérjen időpecsétet.

A tárolt adatok felülhitelesítéséről (speciális időszakos ellenőrzéséről) minden esetben jegyzőkönyvet kell felvenni, feltüntetve az ellenőrzés időpontját, végrehajtóját, eredményét, illetve a konfigurált új hash algoritmust. Sikertelen eredmény esetén a jegyzőkönyv a rendszer adatbázisában tárolt aláírt TIFF állományok (és a hozzá tartozó XML fájlok) helyreállítását is dokumentálja.

6. Feltétel (hitelesítés-szolgáltató konfigurálása)

A rendszer legyen úgy előkészítve (konfigurálva), hogy azokban csak az elfogadott hitelesítés-szolgáltatók felsőszintű és köztes tanúsítványai szerepeljenek.

7. Feltétel (a másolatkészítő rendszer felhasználói)

Az aláíró tanúsítványok címtár-felhasználóhoz rendelő konfigurációját maradéktalanul tartsák karban a másolatkészítők körének változása esetén.

III.3. Javaslatok

Az alábbi javaslatok a rendszer jelenlegi vizsgálata szempontjából nem tartoznak az értékelés hatókörébe, de a környezeti biztonságot nagymértékben növelhetik.

1. Javaslat

Fokozottan figyeljenek arra, hogy a másolatkészítő munkaállomásokat ne hagyják felügyelet nélkül, zárolatlanul.

2. Javaslat

Végezzenek a rendszer zártságára vonatkozó rendszeres (belső) vizsgálatokat. A biztonsági vizsgálatok során kimutathatóak az esetleges eltérések, ellentmondások a szabályzatok és megvalósítások között, valamint a logikai kontrollokkal alá nem támasztott adminisztratív intézkedések. Ezek eredményeit felhasználva a szervezet kockázatkezelési eljárásába a vonatkozó kockázatok csökkenthetőek.

3. Javaslat

Terjesszék ki a biztonságosság-tudatossági képzéseket az elektronikus aláírással, annak helytelen kezelésével, az azzal való visszaélések veszélyeivel kapcsolatos képzésekkel.

4. Javaslat

Javasoljuk az algoritmus meggyengülésekhez kapcsolódó tevékenységeket, felelősségeket és határidőket a vonatkozó szabályzatokba, üzemeltetési előírásokba beemelni.

IV. Javaslat a Tanúsítvány szövegezésére

IV.1. Javaslat a Tanúsítvány főlapjának szövegezésére

A HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft., mint a NAT által NAT-6-0048/2015 számon akkreditált terméktanúsító szervezet

tanúsítja,

hogy az

Audi Hungaria Motor Kft.

által üzemeltetett

Audi Hungaria Motor Kft. hiteles elektronikus másolatképzésre kialakított informatikai rendszer

2016.02.01-én vizsgált állapota

mint papíralapú dokumentumokról elektronikus úton történő másolatot készítő rendszer

megfelel

a 13/2005. (X. 27.) IHM rendelet (a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól) követelményeinek biztosítására

papíralapú dokumentumok hiteles elektronikus másolataként digitalizált, TIFF formátumú, hitelesítési záradékkal és metaadatokkal kiegészített, fokozott biztonságú aláírással és időbélyeggel ellátott állományokra vonatkozóan,

a felhasználásra vonatkozó feltételek figyelembe vételével.

Jelen tanúsítvány a HUNG-TJ-PEM-002-2016. számú tanúsítási jelentés alapján került kiadásra.

Készült a USER Rendszerház Kft. (1025 Budapest, Szépvölgyi u. 86/b) megbízásából.

A tanúsítvány regisztrációs száma: HUNG-T-PEM-002-2016

A tanúsítás kelte: 2016. február 05.

A tanúsítvány érvényességi ideje /évenkénti felülvizsgálat mellett/: 2019. február 05.

Mellékletek: feltételrendszer, dokumentumok

IV.2. Javaslat a Tanúsítvány mellékleteire

Javasoljuk, hogy a Tanúsítvány mellékleteiben a következők szerepeljenek:

- A biztonságos felhasználás feltételei lásd az alábbi fejezetet
  III.2 A biztonságos felhasználás feltételei
- A tanúsítással és értékeléssel kapcsolatos módszertani hivatkozások lásd az alábbi fejezetet:
  II.1 az alkalmazott módszertan
- A tanúsítási eljárás egyéb jellemzői
  - A tanúsításhoz figyelembe vett, fejlesztőtől független dokumentumok
  - A követelményeknek való megfelelést ellenőrzés vizsgálat garancia szintje

V. Hivatkozások

V.1. Módszertani hivatkozások

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)

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)

MIBÉTS 2009 IT biztonsági műszaki követelmények a különböző biztonsági szintekre - Követelmény előírás (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum, v1.01, 2008.08.22) (a KIB 28-as számú Ajánlás része)

CWA 14170:2004; Security requirements for signature creation applications

CWA 14171:2004; General guidelines for electronic signature verification