TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft (1123 Budapest, Kékgolyó u. 6.), 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

papíralapú dokumentumok hiteles elektronikus másolataként digitalizált, TIFF formátumú, hitelesítési záradékkal és metaadatokkal kiegészített, fokozott biztonságú aláírással és időbélyeggel ellátott állományokra vonatkozóan, a papíralapú dokumentumokról elektronikus úton történő másolat készítésének szabályairól szóló 13/2005. (X. 27.) IHM rendelet követelményeinek biztosítására, 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 tanúsítvány érvényességének kezdete: *2016. február 05.*
A tanúsítvány érvényességének vége: *2019. február 05*.
Jelen tanúsítvány állításait éves felülvizsgálati eljárásokkal meg kell erősíteni.
A tanúsítvány terjedelme 5 oldal az érvényességi feltételeket és egyéb jellemzőket tartalmazó mellékletekkel együtt.

Kelt: Budapest, 2016. február 05.

PH.

Endrődi Zsolt
Tanúsítási igazgató

Szűcs Ákos Balázs
Ügyvezető igazgató

1. számú melléklet

A tanúsítvány érvényességi 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.

2. számú melléklet

A követelményeket tartalmazó dokumentum

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

3. számú melléklet

A tanúsítási eljárás egyéb jellemzői

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

A követelményeknek való megfelelést ellenőrzés vizsgálat garancia szintje:

> MIBÉTS fokozott (SAP-F)

Figyelembe vett módszertani dokumentum

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)

CWA 14170:2004; Security requirements for signature creation applications

CWA 14171:2004; General guidelines for electronic signature verification