VIZSGÁLATI BIZONYÍTVÁNY

A HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. értékelési divíziója, mint
a NAT által a NAT-1-1578/2008 számon akkreditált vizsgáló laboratórium

igazolja,

hogy

a NOREG Információvédelmi Kft. által fejlesztett

Margaréta Kártya Menedzsment Rendszer v2.0

CAWeb.ear	[SHA256: d7c0100e8fda765affdba85dddf967ac33f15ccdbf31c6702245884d299b7eef]
EEWs.war	[SHA256: d5bde34285a80310321bb9f1ba96a079a18b30b504152173fcddae625c8aae85]
Margareta.ear	[SHA256: 20978434e6915ac15b7ad24e9dd5b090c4de0e5bfdfc8ed9e46e1c70d34a380b]
Margareta-EE.war	[SHA256: 9929e04af49946c555ab76623f2223065765cf468133791252e45a76717d87ee]
TokenWS.war	[SHA256: e5e4959569520f6494e3c2119438cfda245c788224d3c4696504063ed982042f]
Resources_2.0.war	[SHA256: 4236cb00ac46d7e6a6b9b6511eb6b85dd137ad945ef888e7a2b4867c51c1ead6]

az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel

a

„Margaréta Kártya Menedzsment Rendszer v2.0 - Biztonsági előirányzat”
című dokumentumban (verzió: 2.0) megfogalmazott
funkcionális és garanciális biztonsági követelményeknek

Jelen vizsgálati bizonyítvány a „Margaréta Kártya Menedzsment Rendszer v2.0 - Értékelési jelentés” v1.0 dokumentum alapján került kiadásra.
Az értékelés a Közigazgatási Informatikai Bizottság 28. számú Ajánlása (e-Közigazgatási Keretrendszer) termékekre vonatkozó MIBÉTS (Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma) értékelési módszertana alapján készült.
Az értékelésre MIBÉTS kiemelt garanciaszinten került sor.

A vizsgálati bizonyítványt a NOREG Információvédelmi Kft. kérésére állítottuk ki.

A vizsgálati bizonyítvány regisztrációs száma: **HUNG-M-007/2010.**
A vizsgálati bizonyítvány kelte: 2010. szeptember 30.
Melléklet: a vizsgálati bizonyítvány érvényességi feltételei, összesen: + 3 oldal.

Dr. Balázs István

Digitally signed by Dr. Balázs István
DN: CN = Dr. Balázs István, SN = Dr. Balázs, C = HU, L = Budapest, O = HUNGUARD Kft., OU = értékelési divízió, T = értékelési divízió vezető
Reason: I am the author of this document
Date: 2010.09.30 17:16:32 +02'00'

PH.

Dr. Szabó István

Digitally signed by Dr. Szabó István
DN: CN = Dr. Szabó István, C = HU, L = Budapest, O = HUNGUARD KFT.
Reason: I am approving this document
Date: 2010.09.30 17:34:14 +02'00'

Értékelési divízió vezető
dr Balázs István

Ügyvezető igazgató
dr Szabó István

1. számú melléklet
A vizsgálati bizonyítvány érvényességi feltételei

A vizsgálati bizonyítvány érvényessége a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlnak.

Ezek a feltételek (melyeket tehát a Margaréta Kártya Menedzser Rendszer v2.0 nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezete teljesítse) az alábbiak:

OE.Authentication data management
A környezetnek egy hitelesítési adat kezelésre vonatkozó szabályzat érvényre juttatásával biztosítani kell, hogy a felhasználók hitelesítési adataikat (jelszavaikat, magánkulcsukat aktivizáló PIN kódjaikat) megfelelő időközönként, és megfelelő értékekre (azaz megfelelő hosszúsággal, előtörténettel, változatossággal stb. rendelkező értékekre) változtassák.

OE.Backup and recovery
A környezetnek a Margaréta rendszerre biztosítania kell az alábbiakat:
- álljon rendelkezésre egy rendszer mentési funkció,
- a rendszer mentésében tárolt adatok elegendőek legyenek a rendszer állapotának visszaállítására,
- az adatbázis adminisztrátor szükség esetén képes legyen a mentési funkció meghívására,
- a mentést védeni kell a módosítás ellen,
- a kritikus biztonsági paraméterek és más bizalmas információk csak titkosított formában tárolhatók,
- álljon rendelkezésre egy helyreállítási funkció is, amely képes egy mentésből helyreállítani a rendszert,
- az adatbázis adminisztrátor szükség esetén legyen képes a helyreállítási funkció meghívására.

OE.CA
A Margaréta rendszerrel kapcsolatban álló PKI rendszernek (CA) megbízhatónak kell lennie.

OE.Changing compromised infrastructure key
A Margaréta rendszert a különböző felhasználók felé hitelesítő saját infrastrukturális kulcsainak kompromittálódása esetén biztosítani kell az azonnali cserét.
A CA és IDM rendszereket a Margaréta rendszer felé hitelesítő infrastrukturális kulcsok kompromittálódása esetén biztosítani kell a Margaréta rendszerben tárolt, ezekhez tartozó tanúsítványok azonnali cseréjét. Ilyen esetben az új tanúsítvány subject mezője nem lehet azonos a régivel.
A rendszerfelhasználók (A, O, HD) hitelesítő kulcsainak kompromittálódása esetén biztosítani kell az azonnali cserét.

OE.Communication protection
A környezetnek biztosítania kell a Margaréta rendszer és felhasználói közötti külső, illetve a Margaréta rendszer egyes alrendszerei közötti belső kommunikáció védettségét (a hitelesség, bizalmasság és sértetlenség szempontjából egyaránt).

OE.Competent privileged users
Biztosítani kell a Margaréta rendszer megfelelő kezelését megbízható, hozzáértő és feljogosított adminisztrátorok, operátorok és Helpdesk-esek kijelölésével.
A környezetnek biztosítania kell továbbá a Margaréta rendszerhez közvetlenül hozzá nem férő, ugyanakkor az IT környezetben fontos bizalmi munkakört betöltő személyek (operációs rendszer, alkalmazásszerver és adatbázis adminisztrátorok, valamint a rendszervizsgáló) számára az alábbiakat:

- e szerepkörök összerendelése hitelesített felhasználókkal,
- az operációs rendszer és adatbázis adminisztrátor, valamint a rendszervizsgáló szerepköröket betöltő felhasználók kellő biztonságú azonosítása és hitelesítése egyedi hitelesítő adat használatával, kilépés utáni belépésnél újra hitelesítés kikényszerítésével, a hitelesítési kísérletek számának korlátozásával,
- e szerepköröket betöltő felhasználók hozzáféréseinek ellenőrzése és korlátozása szigorú hozzáférés ellenőrzési szabályok érvényre juttatásával,
- e szerepköröket betöltő felhasználók kellőképpen képzettek, megbízhatók, megfelelően ellátják feladataikat.

OE.Configuration management
A környezetben konfiguráció kezelési tervet kell megvalósítani. A konfiguráció kezelés alkalmazásával biztosítani kell a Margaréta rendszer (szoftver, hardver és förmver) összetevőinek azonosítását, valamint a konfiguráció tételekben történő változások ellenőrzését és nyomon követését.

OE.Control keys on hard token
A Margaréta rendszer bizalmi munkakört betöltő rendszerfelhasználóinak (A, O, HD) hitelesítését megalapozó rendszervezérlő magánkulcsait egy hardver kriptográfiai eszközben (pl. Aladdin eToken) kell generálni, tárolni és aktivizálni.

OE.Cryptographic functions
A környezetnek biztosítania kell, hogy jóváhagyott kriptográfiai algoritmusokat alkalmazzanak titkosításra/dekódolásra, hitelesítésre/ellenőrzésre, aláírás létrehozásra /ellenőrzésre, illetve jóváhagyott kulcsgenerálási technikákat használjanak.

OE.Disposal of Authentication Data
A környezetben biztosítani kell a hitelesítési adatok és az ezekhez tartozó jogosultságok megfelelő eltávolítását, miután a hozzáférési jogosultság megszűnt (pl. munkahelyváltozás, vagy munkaköri felelősség megváltozása következtében).

OE.IDM
A Margaréta rendszerrel kapcsolatban álló IDM rendszernek megbízhatónak kell lennie.

OE.Integrity protection of user data and software
A környezetnek megfelelő védelmet kell biztosítania a felhasználói adatok és a szoftver sértetlenségére.

OE.Non repudiation
A környezetnek biztosítania kell a Margaréta rendszerből a PKI rendszerbe küldött üzenetek digitális aláírását. A digitális aláírásnál alkalmazott infrastrukturális magánkulcsra teljesíteni kell az alábbiak elvárásokat is:

- szabályos időközönként, legalább évente cserélni kell,
- kompromittálódás esetén biztosítani kell az azonnali cseréjét,
- a kulcs cserét biztonságosan kell végrehajtani,

Ezáltal biztosítható a személyes felelősségre vonhatóság egy biztonsági szempontból kritikus üzenet elküldéséért, bizonyítékot szolgáltatva arra, hogy ki küldte az üzenetet.

OE.Operating System
A Margaréta rendszer csak olyan operációs rendszert használhat, mely garantálja számára a tartomány szétválasztást és a biztonsági funkciók megkerülhetetlenségét.

OE.Physical protection
A környezetnek biztosítania kell a Margaréta rendszer hardver, szoftver és förmver elemeinek fizikai védelmét a jogosulatlan módosításokkal szemben.

OE.Protect stored audit records
A futtatókörnyezet biztosítsa a Margaréta rendszer naplózási paramétereit is tartalmazó konfigurációs állomány módosításának és a naplózás tárolási hibájának naplózását.
A környezet biztosítsa a Margaréta rendszerben keletkezett naplóadatok védelmét a jogosulatlan hozzáféréssel, módosítással vagy törléssel szemben, s így biztosítva legyen a felelősségre vonhatóság a felhasználói tevékenységekért. Ennek érdekében biztosítandók az alábbiak:

- megbízható továbbítás egy Syslog szerverre,
- a szükséges tároló hely garantálása a Syslog szerveren, a naplóbejegyzések automatikusan felülírásának megakadályozásával,
- a tárolt naplóbejegyzések sértetlenségének biztosítása,
- a tárolt naplóbejegyzések módosításának megakadályozása,
- a naplóesemények közötti keresési lehetőség biztosítása az esemény időpontja, típusa és/vagy a felhasználó személye szerint,
- a naplóbejegyzések megjeleníthetősége ember számára értelmezhető módon,
- a naplóbejegyzésekhez való hozzáférés (beleértve a keresést és megtekintést is) rendszervizsgáló szerepkörre való korlátozása.

OE.Time stamp
A futtatókörnyezet operációs rendszere(i) megbízható (és szinkronizált) időpontot biztosíts(on/anak) a Margaréta rendszer számára, a naplózott események időpontjának pontos jelzésére, valamint a napló események sorrendjének ellenőrizhetőségéhez.