MINŐSÍTÉS

A HUNGUARD Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft.
Értékelési Divíziója,
mint a NEMZETI AKKREDITÁLÓ TESTÜLET által a NAT-1-1578/2008 számon bejegyzett
akkreditált vizsgáló laboratórium

igazolja,

hogy a

Kripto Kft. által kidolgozott NPS (CodeFish) hash függvény az Értékelési jelentés mellékletében szereplő módosításokkal, valamint az ezt a Brainstorming Design Bt. által megvalósított

hash_001_1.00_nkht_akf.jar Jáva program

(MD5: 705E69EAAA9E7C7A9847FE11C1A2B966 SHA1: A6C383A3EDC176A224DDAF4D796CF18424C975C8),
valamint az rgen_001_1.00_nkht_akf.zip
(MD5: E7E6F351B50D4154EABEF3CFF4F25AD6 SHA1: CC709988A3C6C986CB2FC1D66056C5A57577A665)
file-ban megadott, véletlen generálást végző

rgen_001_1.00_nkht_akf.jar Jáva program

az 1. számú mellékletben részletezett feltételrendszer teljesülése esetén

megfelel

"A döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról"
szóló 2007. évi CI. Törvény 2.-4.-5. és 8. § -ban közvetlenül, vagy közvetve
megfogalmazott alábbi, kriptográfiai biztonsággal kapcsolatos elvárásoknak:

- *az adatokat meg kell fosztani személyes adat jellegüktől /2.§ (3) pont/;*
- *az adatátadást anonim kapcsolati kóddal …kell teljesíteni /4.§ (2) pont/;*
- *a kódképzés módszere tartalmazzon egyedi, véletlenszerűen megállapított elemet /5.§ (1) c)/;*
- *anonim kapcsolati kód: az ugyanazon személyre vonatkozó személyazonosító adatokból olyan, véletlenszerű elemet is tartalmazó módszerrel képzett karaktersor, amellyel ugyanazokból az adatokból mindig ugyanaz a karaktersor jön létre, de amely eredményeképpen létrejött karaktersorból a személyazonosító adatok nem állíthatók helyre /8.§/.*

Jelen minősítés a HUNG-ÉJ-002-2008. számú Értékelési jelentés alapján került kiadásra.

A minősítést a Neumann János Digitális Könyvtár és Multimédia Központ Kht. kérésére állítottuk ki.

A Minősítés regiszterszáma: **HUNG-M-002/2008.**

A Minősítés kelte: 2008. december 15.

Mellékletek: feltételrendszer, követelmények, dokumentumok, összesen 4 oldalon.

dr. Balázs István

Digitally signed by dr. Balázs István
DN: CN = dr. Balázs István, C = HU, L = Budapest, O = HUNGUARD Kft., OU = értékelési divízió, T = értékelési divízió vezető
Location: Budapest
Date: 2008.12.15 16:37:34 +01'00'

PH:

Értékelési divízió vezető
dr. Balázs István

Ügyvezető igazgató
dr. Szabó István

1. számú melléklet

A minősítés érvényességi feltételei

Az alábbiakban összefoglaljuk azokat az általános feltételeket, melyek **együttes** betartása feltétele a minősítés érvényességének. A minősítés a kriptográfiai szempontú biztonsági követelmények teljesülését állítja, a megfelelés matematikai, kriptográfiai bizonyításokon alapul, mely bizonyítások akkor érvényesek, ha

- az anonimizálás erősségét meghatározó, a bevizsgált algoritmus, program által használt véletlen elemek – sem az anonimizálási folyamatban résztvevő, sem harmadik felek részére – nem hozzáférhetőek, nem megismerhetőek;
- pontosan a bevizsgált algoritmus, program kerül alkalmazásra.

A fentiek alapján a minősítés érvényességéhez szervezési és szabályozási intézkedésekkel, informatikai rendszerértékeléssel az alábbi feltételek garanciáinak kidolgozása és ellenőrzése szükséges:

1. számú feltétel: Biztosítani kell, hogy mindig a bevizsgált programok kerüljenek futtatásra, azokat illetéktelenek ne tudják módosítani.

2. számú feltétel: A kapcsolati kódok kialakításához az rgen_001_1.00_nkht_akf.jar program által generált, a hash_001_1.00_nkht_akf.jar program által felhasznált véletlen elemeket a kapcsolati kódokhoz hozzáférő, de a személyazonosító adatok megismerésére illetéktelen személyek ne ismerhessék meg.

2. számú melléklet

TERMÉKMEGFELELŐSÉGI KÖVETELMÉNYEK

A követelményeket tartalmazó dokumentumok

- *"A döntéselőkészítéshez szükséges adatok hozzáférhetőségének biztosításáról" szóló 2007. évi CI. Törvény*
- *www.nfu.hu/download/2074/CI_2007_tv.pdf :A 2007. évi CI. Törvény előírásaihoz fűzött Magyarázat,*
- *A hash függvényekkel kapcsolatos nemzetközi követelmények:*
  - FIPS PUB 180-2 (*http://csrc.nist.gov/encryption/tkhash.html*), *Secure Hash Standard*;
  - RFC 3174 (*http://www.ietf.org/rfc/rfc3174.txt*), *US Secure Hash Algorithm 1 (SHA1);*
  - *Az Európai Unió ECRYPT projektjének dokumentumai a hash függvények követelményeiről pl.: http://ehash.iaik.tugraz.at/wiki/The_eHash_Main_Page*
  - Az SHA3 új hash függvény szabványosításának követelményei, ld. Pl.
    - *http://csrc.nist.gov/groups/ST/hash/sha-3/index.html*
    - *http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf /Federal Register Vol.72,No. 212, Nov.2, 2007/*
- *Hash függvények biztonsági vizsgálata:*
  - www.131002.net/data/papers/Aum08.pdf

3. számú melléklet

A minősítéshez figyelembe vett egyéb dokumentumok

- *KRIPTO RESEARCH Kft dokumentumai:*
  - *„Személyes adatokat tartalmazó adatbázisok egyesítése kutatható, anonim adatbázisokká” c. elektronikusan megkapott (71 oldal terjedelmű) dokumentáció.*
  - *Kriptográfiai kutatási és implementációs projekt, Követelmény specifikáció, v1.0, 2005, szeptember (KRIPTO RESEARCH Kft: file név: 15_követelmenyspecifikacio.pdf);*
  - *NPSHASH Egyirányú hash függvény – Adatlap (ld: http://www.kripto.hu/kripto/codefish.html, file-név: Kripto_HASH_DataSheet.pdf).*
  - www.kripto.hu/kripto/attachments/HASH-DataSheet_en.**pdf**
- **hash_001_1.00_nkht_akf.jar** *JAVA program*

(MD5: 705E69EAAA9E7C7A9847FE11C1A2B966 SHA1: A6C383A3EDC176A224DDAF4D796CF18424C975C8)
készítette Brainstorming Design Bt.

- **rgen_001_1.00_nkht_akf.zip file**

(MD5: E7E6F351B50D4154EABEF3CFF4F25AD6 SHA1: CC709988A3C6C986CB2FC1D66056C5A57577A665)

tartalma:

- ***rgen_001_1.00_nkht_akf.jar*** *file;*
- ***lib könyvtár****, melyben megtalálható a*
  - *hash_001_1.00_nkht_akf.jar file és*
  - *a szükséges segédprogramok: AnnonimizalasUtils.jar néven (inputkezelő, kivételkezelő (pl. hibás billentyűzet-leütés kezelő) osztályok, stringkezelő, időmérő, naplófile-osztály, byte-lista osztály, sha1 számoló osztály /a generált véletlen elemek integritásához/, AES számoló osztály /a véletlen elemek összefűzéséhez)*

- *Megbeszélések, levelezések során pontosító dokumentumok:*
  - *a Megbízóval történő előzetes egyeztetések;*
  - *az APEH adatbiztonsággal kapcsolatos elvárásait ismertető, 2008. november 6-i megbeszélésről készült Emlékeztető;*
  - *A Kripto Research Kft pontosító dokumentumai, file nevek:*
    - audit valaszok.pdf
    - audit valaszok2.pdf