TANÚSÍTVÁNY

A **HUNGUARD** Számítástechnikai-, informatikai kutató-fejlesztő és általános szolgáltató Kft. (1123 Budapest, Kékgolyó u. 6.) mint a NAH által NAH-6-0048/2018 számon akkreditált terméktanúsító szervezet a HUNG_TMK-2-termek_20180629 azonosítójú tanúsítási rendszer szerint

tanúsítja, hogy a

polysys ®

által fejlesztett

A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal v2.5.0

verziója

mint elektronikus aláírási termék

megfelel

az ETSI TS 119 101 V1.1.1 (2016-03) mértékadó dokumentumokban szereplő, a fejlesztői könyvtárra vonatkoztatható követelményeknek.

Jelen Tanúsítvány a **HUNG-TJ-ESIGN-001-2018** számú Tanúsítási Jelentés alapján került kiadásra.

Készült a Polysys Kft. (*1162 Budapest, Margitháza u. 1.*) megbízásából.
A Tanúsítvány regisztrációs száma: **HUNG-T-ESIGN-001-2018**
A Tanúsítvány érvényességének kezdete: *2018. december 28.*
A Tanúsítvány érvényességének vége: *2021. december 28*.
A Tanúsítvány terjedelme öt oldal az érvényességi feltételeket és egyéb jellemzőket tartalmazó mellékletekkel együtt.

Kelt: Budapest, 2018. december 28.

PH.

Endrődi Zsolt
Tanúsítási igazgató

Digitálisan aláírta: HUNGUARD

Szűcs Ákos Balázs
Ügyvezető igazgató

1. számú melléklet

A Tanúsítvány érvényességi feltételei

Az üzemeltetési környezetre vonatkozó biztonsági célok:

Az értékelés következtetései a biztonsági előirányzatban megfogalmazott, az üzemeltetési környezetre vonatkozó feltételezések teljesülésén múlnak.

Ezek a feltételek (melyeket az A2-Polysys CryptoSigno Interop JAVA API nem kezel, nem kényszerít ki, hanem elvárja, hogy az informatikai és a nem informatikai környezet teljesítse) az alábbiak:

OE.AUDIT_GENERATION Az IT környezetnek észlelni és naplózni kell a felhasználóra vonatkozó biztonsági eseményeket.

OE.AUDIT_PROTECTION Az IT környezet biztosítsa a napló információk védelmét.

OE.AUDIT_REVIEW Az IT környezet biztosítson szelektív megjelenítést a napló információk tekintetében.

OE.Configuration A TOE megfelelően telepített és a konfigurált legyen a biztonságos állapotban történő elindításhoz.

OE.CORRECT_TSF_OPERATION Az IT környezet biztosítsa a TOE biztonsági funkcióinak tesztelését biztosítva azok ügyféloldali megfelelő működését.

OE.CRYPTOGRAPHY Az IT környezetnek FIPS 140-2 szabványnak megfelelő kriptográfiai szolgáltatásokat kell nyújtania a TOE számára. Minősített elektronikus aláírás vagy elektronikus bélyegző létrehozása esetén a TOE-nak véletlenszám generátort és QSCD által biztosított kriptográfiai szolgáltatást kell használnia.

OE.DISPLAY_BANNER Az IT környezetnek tájékoztató figyelmeztetést kell adnia a TOE használatával kapcsolatban.

OE.Basic A TOE tervezése és megvalósítása alap támadópotenciál elleni védelmet biztosít, ahogy a sérülékenység elemzés megállapította. (Az IT környezetet nem fenyegetheti ennél nagyobb támadópotenciál.)

OE.NO_EVIL A TOE felhasználási helyein az adminisztrátorok nem lehetnek rosszindulatúak, megfelelően képzettek és követik az adminisztrátori útmutató előírásait.

OE.PHYSICAL A TOE fizikai környezete elfogadható szintű biztonságot nyújtson, így a TOE nem manipulálható, illetve nem lehet alanya különböző típusú (pl. áramfelvétel analízis) side-channel támadásnak.

OE.RESIDUAL_INFORMATION Az IT környezet biztosítsa, hogy a tárgykörbe tartozó védett erőforrások által kezelt információk bizalmassága az erőforrások újra alkalmazása esetén sem sérül.

OE.SELF_PROTECTION Az IT környezet olyan működési környeztetett biztosítson, ami védi önmagát és erőforrásait a külső káros megzavarástól, módosítástól vagy jogosulatlan felfedéstől.

OE.TIME_STAMPS Az IT környezet megbízható időszolgáltatást biztosítson, ahol az adminisztrátor képes az alkalmazandó idő beállítására.

OE.TIME_TOE Az IT környezet megbízható idő jelzést biztosítson a TOE számára

OE.TOE_ACCESS Az IT környezet kontroll mechanizmust biztosítson a felhasználók TOE-hez való logikai hozzáférése tekintetében.

OE.TOE_PROTECTION Az IT környezet védje meg a TOE-t és erőforrásait a külső káros megzavarástól, módosítástól vagy jogosulatlan felfedéstől.

2. számú melléklet

A követelményeket tartalmazó dokumentum

ETSI TS 119 101 V1.1.1 (2016-03) Policy and security requirements for applications for signature creation and signature validation

A Tanúsítási Jelentés III.2-es fejezete részletezi, hogy egyes követelmények milyen mértékben vonatkoztathatók a termékre.

3. számú melléklet

A tanúsítási eljárás egyéb jellemzői

Jelen Tanúsítvány az alábbi értékelési dokumentum alapján került kiadásra:

- A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal V2.5.0 ÉRTÉKELÉSI JELENTÉS v1.0, C077-02/P/E
- MEGFELELÉS ÉRTÉKELÉSI JELENTÉS Az A2-Polysys CryptoSigno JAVA API for Qualified Electronic Signature and Seal V2.5.0 megfeleltetése az ETSI TS 119 101 v1.1.1 (2016-03) követelményeinek v1.0, C077-02/P/M

Az értékelés garancia szintje: MIBÉTS Fokozott

Figyelembe vett jogszabályok

Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről

2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól

Figyelembe vett mértékadó dokumentumok

MIBÉTS 2009 Termékekre vonatkozó értékelési módszertan (az „e-Közigazgatási Keretrendszer Kialakítása” projekt keretében kidolgozott dokumentum v4 2008.09.19. a KIB 28-as számú Ajánlás része)

Common Criteria for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4) – Part 1: Introduction and general model

Common Criteria for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4) – Part 2: Security functional components

Common Criteria for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4) – Part 3: Security assurance components

Common Methodology for Information Technology Security Evaluation (September 2012 - version 3.1, revision 4)