Szabadság – Egyenlőség Testvériség

FRANCIA KÖZTÁRSASÁG

MINISZTERELNÖK

Honvédelmi és
nemzetbiztonsági
főtitkárság

Nemzeti Informatikai Rendszer-biztonsági Ügynökség

Párizs, 2019. február 11
szám: 568 / ANSSI/SDE/PSS/BQA

ELEKTRONIKUS ALÁÍRÁS ÉS ELEKTRONIKUS BÉLYEGZŐ LÉTREHOZÓ ESZKÖZ MEGFELELŐSÉGE TANÚSÍTÁSÁRÓL SZÓLÓ HATÁROZTAT

IAS CLASSIC 4.4.2 verziójú kártya MOC 1.1 szerverrel *MULTTAPP* v 4.0.1 platformon

GEMALTO SA

6, rue de la Verrerie
92 197 Meudon
Franciaország

A Nemzeti Informatikai Rendszer-biztonsági Ügynökség főigazgatója

Tekintettel az Európai Parlament és Tanács 2014. július 23-i, a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló 910/2014/EU számú rendeletére, többek között a rendelet 30. cikke első bekezdésére és a 39. cikk 2. bekezdésére;

A Bizottság a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról szóló 2016. április 25-i végrehajtási határozata (értelmében;

Tekintettel a „Nemzeti Informatikai Rendszer-biztonsági Ügynökség” megnevezésű. országos hatáskörű szervezet megalapításáról szóló 2009. július 7-i 2009-834 számú módosított kormányrendeletre, többek között annak 1. cikkére;

Figyelemmel a Nemzeti Informatikai Rendszer-biztonsági Ügynökség főigazgatóját - POUPARD (Guillaume) urat - kinevező 2014. március 27-i kormányrendeletre;

Tekintettel az Európai ügyek Főtitkárságának Franciaország EU nagykövetéhez 2016. április 29-én írott ITEC/2016/0529 hivatkozási számú levelére, amelynek tájékoztatása alapján a 910/2014/EU rendelet 30 és 39 cikkeinek alkalmazásaként tanúsító szervezetként a Nemzeti Informatikai Rendszer-biztonsági Ügynökséget jelölték ki;

Tekintettel az ANSSI "Minősített elektronikus aláírás / bélyegző létrehozó eszközök – az eIDAS szabályzat szerinti megfelelőség tanúsítása" dokumentuma hatályos verziójában megfogalmazott követelményekre;

Figyelemmel a 2018. június 11-i ANSSI-CC-2018/24 számú tanúsítási jelentésre

a következő határozatot hozza

1. cikk

A GEMALTO Rt fejlesztette IAS CLASSIC 4.4.2 verziójú kártya MOC 1.1 szerverrel MULTTAPP v 4.0.1 platformon termék a 910/2014/EU számú rendelet 29. és 30. cikkében a minősített elektronikus aláírás / bélyegző létrehozó eszközökre[1] meghatározott követelményeknek megfelelő minősítésű tanúsítást kap.

2. cikk

A terméket a tanúsítási jelentésben és a következőkben felsorolt használati és korlátozási feltételeknek megfelelően kell használni.

3. cikk

A jelen határozat a Közös szempontrendszer szerinti tanúsítási határozat időpontjától számított tíz évig, azaz 2028. június 11-ig érvényes.

4. cikk

A jelen határozat érvényességének feltétele, hogy a GEMALTO Rt betartja:

- a társaság részéről a termék biztonság nyomon követésére a tanúsítási kérelmében tett kötelezettségvállalásait a "Minősített elektronikus aláírás / bélyegző létrehozó eszközök – az eIDAS szabályzat szerinti megfelelőség tanúsítása dokumentum 2. mellékletének megfelelően;
- továbbá, hogy átadják az ANSSI számára a termék a Közös szempontrendszer szerinti tanúsítási határozat időpontjától számított legkésőbb öt év múltán, azaz legkésőbb 2023. június 11-ig a felügyeleti audit igazolását

.

A Nemzeti Informatikai Rendszer-biztonsági Ügynökség főigazgatója

[1] A BSI-CC- PP-0059-2009-MA-02, BSI-CC-PP-0075-2012-MA-0 1, BSI- CC-PP-0071-2012-MA-01 , BSJ-CC-PP-0072-2012-MA-0I és BSI-CC- PP-0076-2012- MA-0 1 tanúsítás fenntartási jelentéseknek megfelelően a tanúsítási jelentésben hivatkozott védelmi profilok a Bizottság 2016. április 25-i 2016/650/EU végrehajtási határozatában hivatkozottakkal azonosak

.

Feltételek

A megfelelőség tanúsítási határozat a következőkben meghatározott feltételek betartásának kitételével érvényes.

A termék bevezetésekor a rendszer üzemeltetőjének gondoskodnia kell a következőkről:

C1.	Az IAS alkalmazás és a MULTIAPP v 4.01 platform tanúsítási jelentései 2.3 és 3.2 fejezeteiben meghatározott felhasználási korlátozások megfelelő betartása, különös tekintettel a tanúsított termék felhasználójának gondoskodnia kell az IAS alkalmazás és a MULTIAPP v 4.01 platform biztonsági előirányzataiban specifikált működtetési környezet biztonsági céljainak megfelelő betartásáról.
C2.	Az IAS alkalmazás és a MULTIAPP v 4.01 platform telepítési és használati útmutatóit a termék konfigurálása és használata általános bevezetésekor, teljes életciklusa során, valamint a platformon kiegészítő alkalmazások fejlesztésének adott esetében is alkalmazni kell.
C3.	Az útmutatóknak megfelelően a MULTIAPP v 4.01 platformra telepített összes alkalmazás ellenőrzésére a *BYTE CODE VERJFIER* legújabb verzióját kell használni.
C4.	Az SHA-1 kriptográfiai kivágás funkció az aláírási mechanizmushoz nem használható
C5.	Az RSA magánkulcsok és kitevők, valamint a véges test alapú kriptográfia paramétereinek méretének az aláírási mechanizmusoknak megfelelő hosszúságúnak kell lennie (az RSA magánkulcs és kitevő hossza legalább 2048 bit).
C6.	Az RSA magán kitevők hossza nem lehet kisebb az aláírási mechanizmus kulcsainak méreténél.
C7.	Túl rövid nyilvános RSA kitevő nem használható az aláírási mechanizmusokhoz (a nyilvános kitevő mérete kötelezően $2^{16} + 1$, vagy annál nagyobb).
C8.	A termék személyre szabási fázisában a SCP03 protokollt kell használni.
C9.	A TDES rejtjelezéssel megvalósított külső hitelesítés nem használható az aláírási kulcsok védelmére.
C10	A személyre szabás biztosítására az *IAS* alkalmazás zárolt.
C11	Az SCP01 és az SCP02 protokollok nem használandók.