Overeni prevod veran originalu na francuskom jeziku

Sloboda- Jednakost-Bratstvo
Republika Francuska

Predsednik Vlade

Generalni sekretar za odbranu
i nacionalnu bezbednost

Pariz, 11. februar 2019.
No 568 /ANSSI/SDE/PSS/BQA

Nacionalna agencija za bezbednost informacionih sistema

Odluka o sertifikaciji uskladjenosti kvalifikovanog sredstva za kreiranje elektronskog potpisa i elektronskog pečata

Kartica *IAS Classic* u verziji 4.4.2 sa serverom MOC 1.1 na platformi *MULTIAPP* v 4.0.1
GEMALTO SA

6, rue de la Verrerie
92 197 Meudon
Francuska

Generalni direktor Nacionalne agencije za bezbednost informacionih sistema,

Na osnovu Pravilnika (EU) No 910/2014 Evropskog parlamenta i Evropskog saveta od 23. jula 2014. o elektronskoj identifikaciji i uslugama poverljive prirode koje su u vezi sa elektronskim transakcijama u okviru unutrašnjeg tržišta, kojim se ukida direktiva 1999/93/CE, a naročito paragraf 1 njegovog člana 30 i paragraf 2 njegovog člana 39;

Na osnovu odluke Evropske komisije o implementaciji (EU) 2016/650 od 25. aprila 2016. na osnovu koje se kreiraju standardi koji se odnose na procenu bezbednosti kvalifikovanih sredstava za kreiranje elektronskog potpisa i elektronskog pečata, u skladu sa paragrafom 3 člana 30 i paragrafom 2 člana 39, Pravilnika (EU) No 910/2014 Evropskog parlamenta i Evropskog saveta o elektronskoj identifikaciji i uslugama poverljive prirode koje su u vezi sa elektronskim transakcijama u okviru unutrašnjeg tržišta;

Na osnovu izmenjenog dekreta No 2009-834 od 7. jula 2009. koji se odnosi na osnivanje jedne službe koja bi bila u nadležnosti države, koja je nazvana „Nacionalna agencija za bezbednost informacionih sistema“, a posebno njegovog člana broj 1;

Na osnovu dekreta od 27. marta 2014. koji se odnosi na imenovanje Generalnog direktora Nacionalne agencije za bezbednost informacionih sistema- G-dina Guillaume-a POUPARD;

Na osnovu dopisa Generalnog sekretarijata za evropske poslove upućenog Gospodinu Ambasadoru, stalnom predstavniku Francuske u institucijama Evropske Unije, od 29. aprila 2016, upisanog pod oznakom/ref. ITEC/2016/0529, kojim se on informiše, da je na osnovu primene članova 30 i 39 Pravilnika (EU) No 910/2014 od 23. jula 2014, Nacionalna agencija za bezbednost informacionih sistema imenovana za sertifikaciono telo;

Na osnovu zahteva ANSSI koji su formulisani u dokumentu „Sredstva za kreiranje kvalifikovanog elektronskog potpisa i elektronskog pečata – sertifikacija uskladjenosti sa Pravilnikom *EIDAS* „ verzija koja je na snazi;

Na osnovu izveštaja o sertifikaciji ANSSI-CC-2018/24 od 11. juna 2018;

Donosi sledeću odluku:

- **Član 1 – Proizvod *IAS CLASSIC* u verziji 4.4.2 sa serverom MOC 1.1 na platformi *MULTIAPP* v 4.0.1 koji je razvilo društvo *GEMALTO SA*, uskladjen je zahtevima utvrdjenim u članovima 29 i 39 Pravilnika (EU) No 910/2014 koji se odnose na kvalifikovana sredstva za kreiranje elektronskog potpisa i elektronskog pečata.[1]**
- **Član 2 – Proizvod se mora koristiti u skladu sa uslovima i uz poštovanje ograničenja pri upotrebi koji su definisani u izveštaju o sertifikaciji i onima koji će biti navedeni u daljem tekstu.**
- **Član 3- Ova Odluka važi tokom perioda od 10 godina računajući od donošenja odluke o sertifikaciji proizvoda po *Zajedničkim kriterijumima*, dakle do 11. juna 2028. godine.**
- **Član 4- Ova Odluka uslovljena je, od strane društva *GEMALTO SA*:**
  - **poštovanjem angažmana koji se odnose na praćenje bezbednosti proizvoda, a koje je društvo preuzelo na ime svog zahteva o sertifikaciji, u skladu sa aneksom 2 dokumenta „Kvalifikovana sredstva za kreiranje elektronskog potpisa i pečata- sertifikacija uskladjenosti sa pravilnikom *EIDAS*“,**
  - **pribavljanjem u korist ANSSI-ja sertifikata o nadzoru najkasnije pet godina posle donošenja odluke o sertifikaciji proizvoda po *Zajedničkim kriterijumima*, to jest do 11. juna 2023.**

Guillaume POUPARD
Generalni direktor
Nacionalne agencije za bezbednost informacionih sistema
/potpisano/

---

[1] *U skladu sa izveštajima o održavanju BSI-CC-PP-0059-2009-MA-02, BSI-CC-PP-0075-2012-MA-01, BSI-CC-PP-0071-2012-MA-01, BSI-CC-PP-0072-2012-MA-01 i BSI-CC-PP-0076-2012-MA-01, navedeni profili zaštite u izveštaju o sertifikaciji ekvivalentni su sa onima koji su navedeni u Odluci o implementaciji (EU) 2016/650 Evropske Komisije od 25. aprila 2016.*

СУДСКИ ПРЕВОДИЛАЦ ЗА ФРАНЦУСКИ ЈЕЗИК * БЕОГРАД * ВЕСНА МАРИНКОВИЋ

USLOVI

Odluka o sertifikaciji uskladjenosti biće važeća pod uslovom da se poštuju sledeći dole navedeni uslovi.
Prilikom primene proizvoda, nadležni organ koji ga primenjuje mora da proveri i obezbedi sledeće:
Uslov 1: Da se restrikcije, to jest ograničenja pri upotrebi koja su navedena u poglavljima 2.3 i 3.2 izveštaja o sertifikaciji primene *IAS* i platforme *MULTIAPP* v 4.0.1 dobro poštuju, a korisnik sertifikovanog proizvoda mora naročito da se uveri da li se poštuju ciljevi zaštite u radnom okruženju, onako kako je specificirano u ciljevima zaštite koji se odnose na primenu *IAS-a* i platforme *MULTIAPP* v 4.0.1.

Uslov 2: Vodiči ili uputstva za instaliranje, korišćenje i primenu *IAS-a* i platforme *MULTIAPP* v 4.0.1, primenjuju se tokom razvoja, definisanja konfiguracije i korišćenja proizvoda, tokom čitavog trajanja njegovog životnog ciklusa, kao i u slučaju, -kada je to potrebno-, razvoja komplementarnih aplikacija na platformi.

Uslov 3: Poslednja verzija *BYTE CODE VERIFIER* koristi se za proveru svih aplikacija instaliranih na platformi *MULTIAPP* v 4.0.1 , u skladu sa uputstvima.

Uslov 4: Heš (Hash) funkcija SHA-1 ne koristi se za mehanizme potpisa.

Uslov 5: Veličina modula i privatnih eksponenata RSA i parametara kriptografije na bazi Polja (*Corps*) dovoljna je (veličina modula i privatnog eksponenta RSA je najmanje 2048 bits-a) za mehanizme potpisa.

Uslov 6: Veličina privatnih eksponenata RSA nije manja od veličine modula za mehanizme potpisa.

Uslov 7: Javni eksponent RSA koji je previše mali, ne koristi se (javni eksponent mora da bude veličine koja je veća ili jednaka $2^{16}+1$) za mehanizme potpisa.

Uslov 8: Protokol SCP03 koristi se za fazu personalizacije proizvoda.

Uslov 9: Eksterna autentifikacija sa enkripcijom TDES ne koristi se za zaštitu ključeva potpisa.

Uslov 10: Aplikacija *IAS* je zaključana radi personalizacije.

Uslov 11: Protokoli SCP01 i SCP02 ne koriste se.

..... ***KRAJ PREVODA***.....

Tvrdim da je gornji prevod na srpskom jeziku veran originalu na francuskom i overavam svojim potpisom i pečatom.
Br. 154/2019
Beograd, 15/04/2019

Vesna Marinković, sudski prevodilac za francuski jezik, postavljena rešenjem Ministarstva pravde R.S, br. 740-06-786/2000-04 od 06.09.2000.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Paris, le 11 FEV. 2019
N° 568 /ANSSI/SDE/PSS/BQA

DECISION DE CERTIFICATION DE CONFORMITE D'UN DISPOSITIF DE CREATION DE SIGNATURE ELECTRONIQUE ET DE CACHET ELECTRONIQUE QUALIFIE

CARTE *IAS CLASSIC* en version 4.4.2 avec serveur MOC 1.1 sur plateforme *MULTIAPP* v 4.0.1

GEMALTO SA

6, rue de la Verrerie
92 197 Meudon
France

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information,

Vu le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, notamment l'alinéa 1 de son article 30 et l'alinéa 2 de son article 39 ;

Vu la décision d'exécution (UE) 2016/650 de la Commission du 25 avril 2016 établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'alinéa 3 de l'article 30, et à l'alinéa 2 de l'article 39, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », notamment son article 1er ;

Vu le décret du 27 mars 2014 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Vu le courrier du Secrétariat général des affaires européennes à Monsieur l'ambassadeur représentant permanent de la France auprès de l'Union européenne en date du 29 avril 2016, référence ITEC/2016/0529, informant qu'en application des articles 30 et 39 du règlement (UE) n° 910/2014 du 23 juillet 2014, l'Agence nationale de la sécurité des systèmes d'information est désignée comme organisme certificateur ;

51, boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél +33.1.71.75.82.78 - Fax +33.1.71.75.84.90

Vu les exigences de l'ANSSI formulées dans le document « Dispositifs de création de signature / cachet électronique qualifiés – certification de la conformité au règlement *EIDAS* », version en vigueur ;

Vu le rapport de certification ANSSI-CC-2018/24 du 11 juin 2018,

Décide :

Art. 1er – Le produit *IAS CLASSIC* en version 4.4.2 avec serveur MOC 1.1 sur plateforme *MULTIAPP* v 4.0.1 développé par la société *GEMALTO SA* est certifié conforme aux exigences fixées par les articles 29 et 39 du règlement (UE) n° 910/2014 pour les dispositifs de création de signature et de cachet électronique qualifiés[1].

Art. 2 – Le produit doit être utilisé conformément aux conditions et restrictions d'utilisation définies dans le rapport de certification et à celles listées ci-dessous.

Art. 3 – La présente décision est valable dix ans à compter de la décision de certification du produit selon les *Critères Communs*, à savoir jusqu'au 11 juin 2028.

Art. 4 – La présente décision est conditionnée au respect par la société *GEMALTO SA* :

- des engagements relatifs au suivi de sécurité du produit pris par la société au titre de sa demande de certification, conformément à l'annexe 2 du document « Dispositifs de création de signature / cachet électronique qualifiés – certification de la conformité au règlement *EIDAS* » ;
- à la fourniture à l'ANSSI du certificat de surveillance au plus tard cinq ans après la décision de certification du produit selon les *Critères Communs*, à savoir le 11 juin 2023.

Guillaume POUPARD
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

[1] Conformément aux rapports de maintenance BSI-CC-PP-0059-2009-MA-02, BSI-CC-PP-0075-2012-MA-01, BSI-CC-PP-0071-2012-MA-01, BSI-CC-PP-0072-2012-MA-01 et BSI-CC-PP-0076-2012-MA-01, les profils de protection référencés dans le rapport de certification sont équivalents à ceux référencés dans la décision d'exécution (UE) 2016/650 de la Commission du 25 avril 2016.

Conditions

La décision de certification de conformité est valide sous réserve du respect des conditions énoncées ci-après.

Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que :

C1. Les restrictions d'usage figurant aux chapitres 2.3 et 3.2 des rapports de certification de l'application *IAS* et de la plateforme *MULTIAPP* v 4.0.1 sont bien respectées, en particulier l'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans les cibles de sécurité de l'application *IAS* et de la plateforme *MULTIAPP* v 4.0.1.

C2. Les guides d'installation, d'utilisation de l'application *IAS* et de la plateforme *MULTIAPP* v 4.0.1 sont mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout le long de son cycle de vie ainsi que le cas échéant pour le développement d'applications complémentaires sur la plateforme.

C3. La dernière version du *BYTE CODE VERIFIER* est utilisée pour vérifier toutes les applications installées sur la plateforme *MULTIAPP* v 4.0.1 conformément aux guides.

C4. La fonction de hachage SHA-1 n'est pas utilisée pour les mécanismes de signature.

C5. La taille des modules et exposants privés RSA et des paramètres de la cryptographie à base de Corps est suffisante (la taille du module et de l'exposant privé RSA est d'au moins 2048 bits) pour les mécanismes de signature.

C6. La taille des exposants privés RSA n'est pas inférieure à celle des modules pour les mécanismes de signature.

C7. Un exposant public RSA trop petit n'est pas utilisé (l'exposant public doit être de taille supérieure ou égale à $2^{16}+1$) pour les mécanismes de signature.

C8. Le protocole SCP03 est utilisé pour la phase de personnalisation du produit.

C9. L'authentification externe avec un chiffrement TDES n'est pas utilisée pour la protection des clés de signature.

C10. L'application *IAS* est verrouillée en fin de personnalisation.

C11. Les protocoles SCP01 et SCP02 ne sont pas utilisés.


СУДСКИ ПРЕВОДИЛАЦ ЗА ФРАНЦУСКИ ЈЕЗИК
ВЕСНА МАРИНКОВИЋ
БЕОГРАД