REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Svet za upravljanje z infrastrukturo javnih ključev na MO

Vojkova cesta 55, 1000 Ljubljana

T: 01 230 53 14
F: 01 471 29 78
E: glavna.pisarna@mors.si
www.mors.si

Številka: 386-12/2018-16
Datum: 28. 03. 2018

Na podlagi 102. člena Zakona o obrambi (Uradni list RS, št. 103/04 - uradno prečiščeno besedilo in 95/15) in Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES izdajam

PRAVILA O SPREMEMBI IN DOPOLNITVAH

PRAVIL DELOVANJA IZDAJATELJA SIMoD-CA-RESTRICTED, JAVNI DEL

(Javna pravila SIMoD-CA-Restricted)

Verzija 3.0

1. V Pravilih delovanja izdajatelja SIMoD-CA-Restricted, javni del (Javna pravila SIMoD-CA-Restricted) Verzija 3.0 (MO; št. 386-12/2017-41 z dne 03.05.2017) se v poglavju 1.2. Identifikacijske oznake politik delovanja na koncu tabele doda nova vrstica, ki se glasi:

»

Sistemi za podpis programske kode	Digitalno potrdilo za preverjanje digitalnega podpisa programske kode	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.7.6.2	
		SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.7.6.2	
		NIZKA	1.3.6.1.4.1.22295.10.1.2.2.7.6.2	

« .

2. V poglavju 1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO se dodajo nov drugi, tretji in četrti odstavek, ki se glasijo:

   »Svet za upravljanje z infrastrukturo javnih ključev na MO je odgovoren, da izdajatelj SIMoD-CA-Restricted kot ponudnik storitev zaupanja izpolnjuje zahteve [3] Uredbe eIDAS.

   Svet za upravljanje z infrastrukturo javnih ključev na MO ima v zvezi z izvajanjem [3] Uredbe eIDAS naslednje naloge obveščanja:

   - obvesti nadzorni organ, kot ga določa [2] Uredba o izvajanju eIDAS, o vseh dejstvih, okoliščinah in spremembah, vezanih na status izdajatelja SIMoD-CA-Restricted kot ponudnika kvalificiranih storitev zaupanja,
   - brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po ugotovitvi, uradno obvesti nadzorni organ, po potrebi pa tudi druge pristojne organe, kot je pristojni nacionalni organ za varnost informacij ali organ za varstvo podatkov, o kršitvah varnosti ali izgubi celovitosti, ki znatno vpliva na storitev zaupanja ali na osebne podatke, vsebovane v njej.

   Način obveščanja določi nadzorni organ oziroma drugi pristojni organ. Če način obveščanja ni določen, se uporabi najbolj učinkovit način sporočanja, v primeru potrebe po hitrem ukrepanju je to uradni elektronski naslov ali uradna telefonska številka organa.«.

3. V poglavju 1.4.1. Dovoljena uporaba digitalnih potrdil se v prvem odstavku na koncu tabele doda nova vrstica, ki se glasi:

» | za sisteme za podpis programske kode | digitalno podpisovanje programske kode | preverjanje digitalnega podpisa programske kode | « .

4. V poglavju 1.5.1. Organ, ki upravlja s tem dokumentom se doda nov tretji odstavek, ki se glasi:

»Svet za upravljanje z infrastrukturo javnih ključev na MO pregleda ustreznost Pravil delovanja izdajatelja SIMoD-CA-Restricted, javnega in zaupnega dela, ter ostalih dokumentov, povezanih z delovanjem izdajatelja SIMoD-CA-Restricted, vsaj enkrat (1 x) letno. Na osnovi pregleda potrdi ustreznost ali predlaga spremembe oziroma dopolnitve dokumentov.«.

5. V poglavju 6.1.7. Namen uporabe ključev se v drugem odstavku na koncu tabele doda nova vrstica, ki se glasi:

» | sistemi za podpis programske kode | *digitalSignature* | *codeSigning* | « .

6. V poglavju 6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil se v drugem odstavku na koncu tabele doda nova vrstica, ki se glasi:

»	sistemi za podpis programske kode	zasebni	pet (5) let
		javni	pet (5) let « .

7. V poglavju 6.5.1. Specifične varnostne zahteve za računalnike se na koncu sedme alineje črta besedilo » ter«, na koncu osme alineje pa se ».« nadomesti z besedo » in« in se doda nova deveta alineja, ki se glasi:

» • redno izvajanje vdornih testov in testov ranljivosti.«.

8. V poglavju 7.1.2. Razširitvena polja se napovedni stavek prvega odstavka spremeni tako, da se glasi:

»Standardna razširitvena polja po priporočilu [19] RFC 5280 uporabljena v digitalnih potrdilih izdajatelja SIMoD-CA-Restricted, izdajateljev časovnega žiga, sistemov OCSP in sistemov za podpis programske kode so:«.

Za obstoječo tabelo se doda nova tabela, ki se glasi:

»

Ime razširitvenega polja / prevod ali opis		Digitalna potrdila za sisteme za podpis programske kode
Authority Key Identifier / odtis javnega ključa izdajatelja		SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Restricted
Subject Key Identifier / odtis imetnikovega javnega ključa		SHA256 odtis javnega ključa sistema za podpis programske kode
Key Usage / namen uporabe ključa		**Kritično** digitalSignature
Extended Key Usage / razširjen namen uporabe		codeSigning
Private Key Usage Period / veljavnost zasebnega ključa		Ni uporabljeno
Certificate Policies / oznaka politike potrdila		*Certificate Policy*
	Policy Identifier / enolična oznaka politike	Skladno s *1.2. ,OID:* *1.3.6.1.4.1.22295.10.1.1.1.7.6.2* *1.3.6.1.4.1.22295.10.1.1.2.7.6.2* *1.3.6.1.4.1.22295.10.1.2.2.7.6.2*
	Policy Qualifier / podatki o politiki	*Qualifiers OID* *Qualifier: http:/www.simod-pki.mors.si*
CRL Distribution Point / naslovi registra preklicanih potrdil		LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Restricted
subject Alternative Name / alternativno ime imetnika		DNS ime sistema
Basic Constraints / osnovne omejitve		**Kritično** CA =: False
Authority Info Access / dostop do informacij o izdajatelju		URL naslov izdajatelja

« .

9. V poglavju 8.1. Pogostost inšpekcije se dodajo nov drugi, tretji in četrti odstavek, ki se glasijo:

   »Nadzor izdajatelja SIMoD-CA-Restricted kot ponudnika storitev zaupanja je v skladu z oddelkom 2 [3] Uredbe eIDAS.

   Nadzor izdajatelja SIMoD-CA-Restricted kot ponudnika kvalificiranih storitev zaupanja je v skladu z 20. členom [3] Uredbe eIDAS.

   V skladu z prvim odstavkom 20. člena [3] Uredbe eIDAS je pogostost nadzora za ugotavljanje skladnosti ponudnika kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja vsaj vsakih 24 mesecev.«.

   Dosedanji drugi odstavek postane peti odstavek.

10. V poglavju 8.2. Pogoji za inšpektorja se doda nov drugi odstavek, ki se glasi:

    »Skladnost izdajatelja SIMoD-CA-Restricted kot ponudnika kvalificiranih storitev zaupanja z zahtevami [3] Uredbe eIDAS ugotavlja organ za ugotavljanje skladnosti, ki je opredeljen v 3. členu [3] Uredbe eIDAS.«.

    Dosedanji drugi odstavek postane tretji odstavek.

11. V poglavju 8.3. Relacija med inšpektorjem in izdajateljem SIMoD-CA-Restricted se doda nov drugi odstavek, ki se glasi:

    »Organ za ugotavljanje skladnosti ponudnikov kvalificiranih storitev zaupanja z [3] Uredbo eIDAS je neodvisen od infrastrukture javnih ključev na MO.«.

12. V poglavju 8.4. Področja inšpekcije se doda nov drugi odstavek, ki se glasi:

    »Organ za ugotavljanje skladnosti ugotavlja skladnost ponudnika kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja z zahtevami [3] Uredbe eIDAS.«.

    Dosedanji drugi odstavek postane tretji odstavek.

13. V poglavju 8.5. Postopki po opravljeni inšpekciji se doda nov tretji odstavek, ki se glasi:

    »Nadaljnji postopki po opravljenem pregledu skladnosti ponudnika kvalificiranih storitev zaupanja so v skladu z drugim in tretjim odstavkom 20. člena [3] Uredbe eIDAS.«.

14. V poglavju 8.6. Prejemniki ugotovitev o inšpekciji se doda novi tretji odstavek, ki se glasi:

    »V skladu s prvim odstavkom 20. člena [3] Uredbe eIDAS mora ponudnik kvalificiranih storitev zaupanja poročilo o ugotovitvi skladnosti predložiti nadzornemu organu, ki je določen v 3. členu [2] Uredbe o izvajanju eIDAS, v treh (3) dneh po njegovem prejemu.«.

15. V poglavju 9.6.1. Odgovornosti in jamstva izdajatelja SIMoD-CA-Restricted se doda nov drugi odstavek, ki se glasi:

    »Svet za upravljanje z infrastrukturo javnih ključev na MO je odgovoren, da izdajatelj SIMoD-CA-Restricted kot ponudnik storitev zaupanja izpolnjuje zahteve [3] Uredbe eIDAS.«.

16. Ta pravila začnejo veljati naslednji dan po podpisu.

Mag. Viktor Sterle

Vodja Sveta za upravljanje z
infrastrukturo javnih ključev na MO