Na podlagi 102. člena Zakona o obrambi (Uradni list RS, št. 103/04 - uradno prečiščeno besedilo in 96/12 - ZPIZ) v zvezi z 28. in 29. členom Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06) izdajam

PRAVILA O SPREMEMBAH IN DOPOLNITVAH

PRAVIL DELOVANJA OVERITELJA SIMOD-CA-RESTRICTED, JAVNI DEL

(Javna pravila SIMoD-CA-Restricted)

Verzija 2.0

1. V Pravilih delovanja overitelja SIMoD-CA-Restricted, javni del (Javna pravila SIMoD-CA-Restricted) Verzija 2.0 (MO; št. 382-5/2006-121 z dne 23.11.2010 in št. 386-6/2011-336 z dne 21.12.2011) se v poglavju 6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil besedilo:

»

digitalno potrdilo overitelja SIMoD-CA-Restricted	zasebni	tri (3) leta
	javni	šest (6) let

«

nadomesti z besedilom:

»

digitalno potrdilo overitelja SIMoD-CA-Restricted	zasebni	šest (6) let
	javni	šest (6) let

«.

2. V poglavju 7.1.1. Verzija digitalnih potrdil se beseda »*sha1WithRSAEncryption*« nadomesti z besedo »*sha256WithRSAEncryption*«.

3. V poglavju 7.1.2. Razširitvena polja se beseda »SHA-1« nadomesti z besedo »SHA256«

4. V poglavju 7.1.2. Razširitvena polja se v prvem odstavku na koncu tabele doda vrstica:

»

AuthorityInfoAccess / dostop do informacij o overitelju	URL naslov overitelja	URL naslov overitelja

« .

5. V poglavju 7.1.2. Razširitvena polja se v drugem odstavku na koncu tabele doda vrstica:

»

AuthorityInfoAccess / dostop do informacij o overitelju	URL naslov overitelja	URL naslov overitelja	URL naslov overitelja

« .

6. V poglavju 7.1.3. Identifikacijske oznake algoritmov se besedilo:

»

sha1WithRSAEncryption	1.2.840.113549.1.1.5

«

nadomesti z besedilom:

»

sha256WithRSAEncryption	1.2.840.113549.1.1.11

« .

7. V poglavju 7.2.1. Verzija registrov preklicanih potrdil se beseda »*sha1WithRSAEncryption*« nadomesti z besedo »*sha256WithRSAEncryption*«.

8. V poglavju 7.2.2. Razširitvena polja registrov preklicanih potrdil se besedilo »*KeyID* = SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted« nadomesti z besedilom »SHA256 odtis javnega ključa overitelja«.

9. Ta pravila začnejo veljati naslednji dan po podpisu.

Številka: 386-11/2014-23
Datum: 07.02.2014

Mag. Viktor Strele

Vodja Sveta za upravljanje z
infrastrukturo javnih ključev na MO