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 OVEROTELJA SIMOD-CA-ROOT, JAVNI DEL

(Javna pravila SIMoD-CA-Root)

Verzija 2.0

1. V Pravilih delovanja overitelja SIMoD-CA-Root, javni del (Javna pravila SIMoD-CA-Root) Verzija 2.0 (MO; št. 382-5/2006-119 z dne 23.11.2010 in št. 386-6/2011-337 z dne 21.12.2011) se v poglavju 7.1.1. Verzija digitalnih potrdil beseda »*sha1WithRSAEncryption*« nadomesti z besedo »*sha256WithRSAEncryption*«.

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

3. V poglavju 7.1.2. Razširitvena polja se na koncu tabele doda vrstica:

» | *AuthorityInfoAccess* / dostop do informacij o overitelju | ni uporabljeno | URL naslov overitelja | «

4. 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 | « .

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

6. V poglavju 7.2.2. Razširitvena polja registrov preklicanih potrdil se besedilo »*KeyID* = <SHA-1 odtis javnega ključa overitelja>« nadomesti z besedilom »SHA256 odtis javnega ključa overitelja«.

7. Ta pravila začnejo veljati naslednji dan po podpisu.

Številka: 386-11/2014-22
Datum: 07.02.2014

Mag. Viktor Strele

Vodja Sveta za upravljanje z
infrastrukturo javnih ključev na MO