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

PRAVIL DELOVANJA INFRASTRUKTURE JAVNIH KLJUČEV NA MINISTRSTVU ZA OBRAMBO REPUBLIKE SLOVENIJE

(Politika SIMoD-PKI)

Verzija 2.0

1. V Pravilih delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije (Politika SIMoD-PKI) Verzija 2.0 (MO; št. 382-5/2006-109 z dne 24.08.2010, št. 386-6/2011-229 z dne 08.09.2011 in št. 386-6/2011-304 z dne 14.11.2011) se v poglavju 7.1.1. Verzija digitalnih potrdil beseda »*sha1WithRSAEncryption*« nadomesti z besedo »*sha256WithRSAEncryption*«.

2. V poglavju 7.1.2. Razširitvena polja se besedna zveza »*KeyID* = SHA-1« in beseda »SHA-1« nadomestita z besedo »SHA256«.

3. 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 | « .

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

5. V poglavju 7.2.2. Razširitvena polja registrov preklicanih potrdil se besedna zveza »*KeyID* = SHA-1« nadomesti z besedo »SHA256«.

6. Ta pravila začnejo veljati naslednji dan po podpisu.

Številka: 386-11/2014-20
Datum: 07.02.2014

Roman Jakič

Minister