

Na podlagi 102. člena Zakona o obrambi (Uradni list RS, št. 103/04 - uradno prečiščeno besedilo) 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) ter v skladu s 7. odstavkom poglavja 1.1. Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije (Politika SIMoD-PKI), šifra 382-5/2006-11 z dne 17.7.2006 in številka 382-5/2006-42 z dne 27.12.2007 izdajam

SPREMEMBE PRAVIL DELOVANJA OVERITELJA SIMoD-CA-Root, JAVNI DEL

(JAVNA PRAVILA SIMoD-CA-Root)

1. V Pravilih delovanja overitelja SIMoD-CA-Root, javni del (Javna pravila SIMoD-CA-Root), šifra 382-5/2006-12 z dne 17.7.2006, se spremeni peti odstavek poglavja 1.2. Naziv dokumenta in identifikacijska oznaka tako, da se glasi:

»Identifikacijska oznaka Javnih pravil SIMoD-CA-Root se torej določi po pravilu:

1.3.6.1.4.1.22295.10.2.<vrsta dokumenta>.<verzija>

in ima vrednost 1.3.6.1.4.1.22295.10.2.2.1. Identifikacijska oznaka se uporablja za enolično označevanje dokumenta in njegove verzije. Oznaka se ne uporablja za označevanje digitalnih potrdil.«.

2. Tretji odstavek poglavja 1.3.3 Imetniki digitalnih potrdil se spremeni tako, da se glasi:

»SIMoD-CA-Root izdaja poleg digitalnih potrdil za podrejene overitelje in medsebojno priznane overitelje tudi digitalna potrdila operativnemu osebju, izključno za potrebe upravljanja z overiteljevo infrastrukturo. Postopki upravljanja teh digitalnih potrdil so določeni v zaupnem delu pravil delovanja overitelja SIMoD-CA-Root in niso obravnavani v nadaljevanju pričujočega dokumenta.«.

3. Poglavje 3.1.1 Vrste imen se spremeni tako, da se glasi:

»Vsako izdano X.509v3 digitalno potrdilo vsebuje polje *Subject* z edinstvenim razločevalnim imenom - X.501 DN (angl.: Distinguished Name, DN) v skladu z RFC3280. Razločevalno ime je v digitalno potrdilo zapisano v obliki X.501 UTF8String in ni nikdar prazno. Digitalna potrdila, izdana podrejenim overiteljem, imajo lahko tudi alternativno ime overitelja, ki je zapisano v razširitvenem polju *subjectAltName*, v skladu z RFC3280 in RFC4043.«.

4. Poglavje 3.1.4 Pravila za interpretacijo različnih oblik imen se spremeni tako, da se glasi:

»Imena se interpretirajo v skladu z definicijami v poglavju 3.1.1. Vrste imen in 3.1.2. Potreba po smiselnosti imen.«.

5. V poglavju 5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje se črta četrta alineja.

6. Te spremembe Pravil delovanja overitelja SIMoD-CA-Root, javni del začnejo veljati naslednji dan po podpisu.

Številka: 382-5/2006-43

Datum: 27.12.2007

Karl ERJAVEC

MINISTER