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 IN DOPOLNITVE PRAVIL DELOVANJA OVERITELJA SIMoD-CA-Restricted, JAVNI DEL

(*JAVNA PRAVILA SIMoD-CA-Restricted*)

1. V Pravilih delovanja overitelja SIMoD-CA-Restricted, Javni del (Javna pravila SIMoD-CA-Restricted), šifra 382-5/2006-13 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-Restricted se torej določi po pravilu:

1.3.6.1.4.1.22295.10.3.<vrsta dokumenta>.<verzija>

in ima vrednost 1.3.6.1.4.1.22295.10.3.2.1. Identifikacijska oznaka se uporablja za enolično označevanje dokumenta in njegove verzije. Oznaka se ne uporablja za označevanje digitalnih potrdil.«.

2. 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 imetnika - 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. Imetnik ima lahko tudi eno ali več alternativnih imen, ki so zapisana v razširitvenem polju *subjectAltName* digitalnega potrdila, v skladu z RFC3280 in RFC4043.«.

3. 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, 3.1.2. Potreba po smiselnosti imen in 3.1.7. Alternativno ime imetnika.«.

4. Za poglavjem 3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk se doda novo poglavje 3.1.7. Alternativno ime imetnika, ki se glasi:

»3.1.7. Alternativno ime imetnika

Imetnik ima lahko eno ali več alternativnih imen, ki so zapisana v razširitvenem polju *subjectAltName* digitalnega potrdila. Tip alternativnega imena je:

- *rfc822Name*; vrednost alternativnega imena je naslov elektronske pošte in se določi v skladu z RFC3280 ali

- *otherName*; vrednost alternativnega imena je enolična oznaka *Permanent Identifier* in se določi v skladu z RFC4043. Enolično oznako *Permanent Identifier* sestavljata dva dela:
    - vrsta enolične oznake (*assigner*); vsebuje OID številko vrste oznake;
    - vrednost oznake (*identifierValue*); vsebuje enolično številko v okviru dane vrste oznake.

Digitalno potrdilo lahko vsebuje eno ali več alternativnih imen tipa *rfc822Name* in največ eno alternativno ime tipa *Permanent Identifier*.

Digitalna potrdila za zaposlene lahko vsebujejo enega ali več elektronskih naslovov, iz katerih lahko imetnik pošilja pošto ter enolično oznako imetnika *Permanent Identifier*.

Digitalna potrdila za splošne nazive oziroma organizacijske enote MO in institucije lahko vsebujejo pripadajoči elektronski naslov ter enolično oznako *Permanent Identifier*.

Digitalna potrdila za poveljniške dolžnosti v SV lahko vsebujejo pripadajoči elektronski naslov ter enolično oznako *Permanent Identifier*.

Digitalna potrdila za strežnike ter drugo strojno in programsko opremo lahko vsebujejo naslov elektronske pošte pripadajočega skrbnika oziroma poštne skupine. Lahko vsebujejo tudi pripadajočo enolično oznako *Permanent Identifier*, če obstaja.

Digitalna potrdila za izdajatelje časovnih žigov lahko vsebujejo naslov elektronske pošte pripadajočega skrbnika oziroma poštne skupine. Lahko vsebujejo tudi pripadajočo enolično oznako *Permanent Identifier*, če obstaja.«.

5. V poglavju 4.1.2. Postopek obdelave vloge in odgovornosti se doda nov tretji odstavek, ki se glasi:

»Operativno osebje overitelja SIMoD-CA-Restricted preveri pravilnost in veljavnost naslovov elektronske pošte bodočega imetnika. V primeru nepravilnega ali neveljavnega elektronskega naslova, operativno osebje zadrži postopek izdajanja digitalnega potrdila, dokler se problem ne razreši. Če v roku iz poglavja 4.2.3. Čas za obdelavo vloge za izdajo digitalnega potrdila problem ni odpravljen, se izdaja digitalnega potrdila zavrne.«.

Dosedanji tretji, četrti in peti odstavek postanejo četrti, peti in šesti odstavek.

V četrtem odstavku se za kratico »SIMoD-CA-Restricted« doda besedilo »po uspešnem preverjanju veljavnosti naslovov elektronske pošte«.

6. V drugi alinei prvega odstavka poglavja 4.8. Sprememba digitalnega potrdila se zbriše beseda »*subjectAlternativeName*« in za besedo »polju« doda beseda »*subjectAltName*«.

7. V poglavju 5.7.4. Naravne in druge nesreče se črta beseda »notranjih«.

8. Prvi odstavek poglavja 6.1.1. Generiranje para ključev se spremeni tako, da se glasi:

»Ključi SIMoD-CA-Restricted overitelja se generirajo po formalnem, podrobno predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje SIMoD-CA-Restricted overitelja. Poleg operativnega osebja overitelja so prisotne tudi zaupanja

vredne priče, ki nadzorujejo izvajanje postopka. Postopek je podrobno opisan v zaupnem delu pravil delovanja overitelja. Izvedba postopka se podrobno dokumentira v zapisniku, ki ga podpišejo vsi prisotni.«.

9. V četrtem odstavku poglavja 7.1.2. Razširitvena polja se spremeni tabela tako, da se glasi:

»

Polje (Field)	Potrdilo za preverjanje digitalnega podpisa…[24]	Potrdilo za šifriranje…[25]	Potrdilo za preverjanje digitalnega podpisa in šifriranje…[26]
odtis javnega ključa overitelja (authority Key Identifier)	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted s katerim je podpisano potrdilo	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted s katerim je podpisano potrdilo	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted s katerim je podpisano potrdilo
odtis imetnikovega javnega ključa (subject Key Identifier)	SHA-1 odtis imetnikovega javnega ključa	SHA-1 odtis imetnikovega javnega ključa	SHA-1 odtis imetnikovega javnega ključa
namen uporabe ključa (key Usage)	**Kritično** digitalSignature	**Kritično** keyEncipherment	**Kritično** DigitalSignature keyEncipherment
razširjen namen uporabe (extended Key Usage)	Ni uporabljeno	Ni uporabljeno	Ni uporabljeno
obdobje veljavnosti zasebnega ključa (privateKeyUsagePeriod)	V skladu s poglavjem 6.3.2	V skladu s poglavjem 6.3.2	V skladu s poglavjem 6.3.2
OID oznaka tipa potrdila (certificate Policies)	**Kritično** CertPolicyId: v skladu s poglavjem 1.2.> UserNotice: kot določeno v poglavju 7.1.8>	**Kritično** CertPolicyId: v skladu s poglavjem 1.2.> UserNotice: kot določeno v poglavju 7.1.8>	**Kritično** CertPolicyId: v skladu s poglavjem 1.2.> UserNotice: kot določeno v poglavju 7.1.8>
naslovi registera preklicanih potrdil (CRL Distribution Points)	LDAP in http URL naslov SIMoD-CA-Restricted registra preklicanih potrdil	LDAP in http URL naslov SIMoD-CA-Restricted registra preklicanih potrdil	LDAP in http URL naslov SIMoD-CA-Restricted registra preklicanih potrdil
Alternativno ime imetnika (subject Alternative Name)	V skladu s poglavjem 3.1.7	V skladu s poglavjem 3.1.7	V skladu s poglavjem 3.1.7
Osnovne omejitve (basicConstraint)	**Kritično** CA =: False	**Kritično** CA =: False	**Kritično** CA =: False

«.

10. V poglavju 7.1.4 Oblike imen se za besedami »Kot v poglavju 3.1.1. Vrste imen« doda besedilo »in 3.1.7. Alternativno ime imetnika«.

11. Te spremembe in dopolnitve Pravil delovanja overitelja SIMoD-CA-Restricted, javni del začnejo veljati naslednji dan po podpisu.

Številka: 382-5/2006-44
Datum: 27.12.2007

Karl ERJAVEC
MINISTER