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) izdajam

SPREMEMBE IN DOPOLNITVE PRAVIL DELOVANJA INFRASTRUKTURE JAVNIH KLJUČEV NA MINISTRSTVU ZA OBRAMBO REPUBLIKE SLOVENIJE

(*POLITIKA SIMoD-PKI*)

1. V Pravilih delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije (Politika SIMoD-PKI), šifra 382-5/2006-11 z dne 17.7.2006, se spremeni prvi odstavek poglavja 1.2. Naziv dokumenta in identifikacijske oznake tako, da se glasi:

»Pravilo dodeljevanja identifikacijskih oznak (angl. Object Identifiers – OIDs) na MO je "1.3.6.1.4.1.22295.<storitev>.<overitelj>…", v skladu z naslednjo tabelo:

Del identifikacijske oznake	Vrednost	
1.3.6.1.4.1.22295	enolična identifikacijska oznaka MO, registrirana pri www.iana.org (http://www.iana.org/assignments/enterprise-numbers)	
storitev	1..100	Storitve PKI:
	10	storitve SIMoD-PKI
	101..1000	druge storitve v MO
overitelj	1	infrastruktura SIMoD-PKI
	2	SIMoD-CA-Root
	3	SIMoD-CA-Restricted
	4	SIMoD-CA-Secret
	…	rezervirano za overitelje SIMoD-PKI

«.

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. V poglavju 3.1.4. Pravila za interpretacijo različnih oblik imen se besedilo »7.1.4. Oblike imen« nadomesti z besedilom »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 ustreznega overitelja SIMoD-PKI 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-PKI« doda besedilo »po uspešnem preverjanju veljavnosti naslovov elektronske pošte«.

6. V poglavju 7.1.2. Razširitvena polja se spremeni tabela tako, da se glasi:

»

Standardno razširitveno polje - angleški naziv	Standardno razširitveno polje - slovenski opis	Vrednost
authorityKeyIdentifier	odtis javnega ključa overitelja	<SHA-1 odtis javnega ključa overitelja>
subjectKeyIdentifier	odtis imetnikovega javnega ključa	<SHA-1 odtis javnega ključa imetnika>
keyUsage	namen uporabe	Kot določeno v 6.1.7 Namen in uporabe ključev oziroma v pravilih delovanja overitelja
extendedKeyUsage	razširjen namen uporabe	Kot določeno v 6.1.7 Namen in uporabe ključev oziroma v pravilih delovanja overitelja
privateKeyUsagePeriod	veljavnost zasebnega ključa	*Not Before*: <začetek veljavnosti po GMT> *Not After*: <konec veljavnosti po GMT>
certificatePolicies:	oznaka politike potrdila	Določeno v pravilih delovanja overitelja; za imetniška potrdila je *UserNotice* predpisan v 7.1.8 Specifični podatki o politiki
CertPolicyID	enolična oznaka politike	
UserNotice	obvestilo uporabnikom	
CRLDistributionPoints	naslovi, na katerih je objavljen register preklicanih potrdil	Določeno v pravilih delovanja overitelja
subjectAltName	alternativno ime imetnika	Določeno v pravilih delovanja overitelja
issuerAltName	alternativno ime izdajatelja	se ne uporablja
subjectDirectoryAttributes	atributi imenika	se ne uporablja
basicConstraints	osnovne omejitve	Določeno v pravilih delovanja overitelja

«.

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

8. Te spremembe in dopolnitve Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije začnejo veljati naslednji dan po podpisu.

Številka: 382-5/2006-42

Datum: 27.12.2007

Karl ERJAVEC

MINISTER