



Državni center za storitve zaupanja
Izdajatelj kvalificiranih digitalnih potrdil SIGEN-CA



POLITIKA SIGEN-CA

za spletna kvalificirana digitalna potrdila za fizične osebe

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 6. junija 2016
verzija: 6.0

CP_{Name}: SIGEN-CA-2

CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.4



Zgodovina politik

Izdaje politik delovanja SIGEN-CA	
verzija: 6.0, veljavnost: od 6. junija 2016	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP _{OID} : 1.3.6.1.4.1.6105.2.2.3.4 CP _{Name} : SIGEN-CA-2	<i>Spremembe z verzijo 6.0:</i> <ul style="list-style-type: none">• tvorjeno je bilo drugo lastno digitalno potrdilo izdajatelja SIGEN-CA z zasebnim ključem dolžine 3072 bitov, ki se hrani na strojni opremi za varno shranjevanje zasebnih ključev,• v potrdilu izdajatelja SIGEN-CA in vseh potrdilih imetnikov se uporablja zgostitveni algoritem SHA-256,• spremenjeno je razločevalno ime digitalnega potrdila izdajatelja SIGEN-CA,• spremenjena so razločevalna imena potrdil imetnikov, ki lahko vključujejo znake iz kodne tabele UTF-8,• podprto je sprotno preverjanje statusa potrdil po protokolu OCSP,• izdajatelj SIGEN-CA je priznan s strani korenkega izdajatelja SI-TRUST Root,• pri potrdilih imetnikov je v polju uporaba ključa (angl. Key Usage) dodana vrednost ContentCommitment
verzija: 5.0, veljavnost: od 7. novembra 2015	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP _{OID} : 1.3.6.1.4.1.6105.2.2.3.3 CP _{Name} : SIGEN-CA-2	<i>Spremembe z verzijo 5.0:</i> <ul style="list-style-type: none">• uporaba novega naziva za overitelja na Ministrstvu za notranje zadeve, po novem je to »Državni center za storitve zaupanja«,• kvalificirano potrdilo lahko pridobi procesno sposobna oseba, starejša od 15 let,• novi kontaktni podatki izdajatelja SIGEN-CA.
amandma k politiki verzije 4.0, veljavnost: od 21. marca 2014	
Amandma k Politiki SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe št. 2 / 4.0	<i>Sprememba z amandmajem št. 2 / 4.0:</i> <ul style="list-style-type: none">• uporaba novega naziva za overitelja na Ministrstvu za pravosodje in javno upravo, po novem je to »Overitelj na Ministrstvu za notranje zadeve«.
amandma k politiki verzije 4.0, veljavnost: od 23. julija 2012	
Amandma k Politiki SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe št. 1 / 4.0	<i>Sprememba z amandmajem št. 1 / 4.0:</i> <ul style="list-style-type: none">• uporaba novega naziva za overitelja na Ministrstvu za javno upravo, po novem je to »Overitelj na Ministrstvu za pravosodje in javno upravo«.
verzija: 4.0, veljavnost: od 14. septembra 2009	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP _{OID} : 1.3.6.1.4.1.6105.2.2.3.2 CP _{Name} : SIGEN-CA-2	<i>Spremembe z verzijo 4.0:</i> <ul style="list-style-type: none">• izdajatelj digitalnih potrdil SIGEN-CA izdaja kvalificirana digitalna potrdila s ključi minimalne dolžine 2048 bitov;• v kvalificiranih dig. potrdilih za fizične osebe je dodana ustrezna oznaka za kvalificirana potrdila.
verzija: 3.1, veljavnost: od 18. maja 2007	



Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP _{OID} : 1.3.6.1.4.1.6105.2.2.3.1 CP _{Name} : SIGEN-CA-2	<i>Spremembe z verzijo 3.1:</i> <ul style="list-style-type: none">• <i>izdajatelj SIGEN-CA bodočemu imetniku potrdila avtorizacijske kode ne posreduje več po priporočeni pošti temveč z navadno pošto pošiljko;</i>• <i>oddaja zahtevka za pridobitev digitalnega potrdila je omogočena tudi na elektronski način z veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, izdanim s strani izdajatelja SIGEN-CA;</i>• <i>omogočena je predhodna pridobitev novega potrdila pred potekom veljavnosti prejšnjega;</i>• <i>prijavne službe overitelja morajo pri svojem delu upoštevati poslovnike za delo prijavnih služb.</i>
<i>verzija: 3.0, veljavnost: od 28. februarja 2006</i>	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP _{OID} : 1.3.6.1.4.1.6105.2.2.3 CP _{Name} : SIGEN-CA-2	<i>Spremembe z verzijo 3.0:</i> <ul style="list-style-type: none">• <i>uporaba novega naziva za overitelja na Centru Vlade za informatiko, po novem je to »Overitelj na Ministrstvu za javno upravo«;</i>• <i>osebna kvalificirana digitalna potrdila se po novem imenujejo »posebna kvalificirana digitalna potrdila«;</i>• <i>preklic je po novem mogoč samo v času uradnih ur, razen v nujnih primerih;</i>• <i>uporaba novega naziva za imetnike SIGEN-CA, in sicer za imetnike »pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti« uporablja izraz »poslovni subjekt«;</i>• <i>struktura dokumenta je v skladu s priporočili RFC 3647.</i>
<i>verzija: 2, veljavnost: od 15. julija 2002</i>	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP _{OID} : 1.3.6.1.4.1.6105.2.2.2 CP _{Name} : SIGEN-CA-2	/
<i>verzija: 1, veljavnost: od 9. julija 2001</i>	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP _{OID} : 1.3.6.1.4.1.6105.2.2.1 CP _{Name} : SIGEN-CA-2	/



VSEBINA

1.	UVOD	12
1.1.	Pregled.....	12
1.2.	Identifikacijski podatki politike delovanja	13
1.3.	Udeleženci infrastrukture javnih ključev	13
1.3.1	Overitelj.....	13
1.3.2	Prijavna služba.....	17
1.3.3	Imetniki potrdil.....	20
1.3.4	Tretje osebe	20
1.3.5	Ostali udeleženci.....	20
1.4.	Namen uporabe potrdil.....	20
1.4.1	Pravilna uporaba potrdil in ključev	20
1.4.2	Nedovoljena uporaba potrdil in ključev	21
1.5.	Upravljanje s politiko	21
1.5.1	Upravljaavec politike	21
1.5.2	Kontaktne osebe	21
1.5.3	Odgovorna oseba glede skladnosti delovanja izdajatelja s politiko	21
1.5.4	Postopek za sprejem nove politike	21
1.6.	Izrazi in okrajšave	21
1.6.1	Izrazi	21
1.6.2	Okrajšave.....	23
2.	OBJAVE IN ODGOVORNOSTI GLEDE REPOZITORIJA	25
2.1.	Repozitoriji.....	25
2.2.	Objava informacij o potrdilih	25
2.3.	Pogostnost javne objave.....	26
2.4.	Dostop do repozitorijev	26
3.	ISTOVETNOST IN VERODOSTOJNOST	26
3.1.	Določanje imen.....	26
3.1.1	Oblika imen	26
3.1.2	Zahteva po smiselnosti imen	27
3.1.3	Uporaba anonimnih imen ali psevdonimov	27
3.1.4	Pravila za interpretacijo imen.....	27
3.1.5	Enoličnost imen.....	27
3.1.6	Priznavanje, verodostojnost in vloga blagovnih znamk	28
3.2.	Začetno preverjanje istovetnosti	28
3.2.1	Metoda za dokazovanje lastništva zasebnega ključa	28
3.2.2	Preverjanje istovetnosti organizacij.....	28
3.2.3	Preverjanje istovetnosti fizičnih oseb	28
3.2.4	Nepreverjeni podatki pri začetnem preverjanju.....	28
3.2.5	Preverjanje pooblastil.....	28
3.2.6	Merila za medsebojno povezovanje.....	28
3.3.	Istovetnost in verodostojnost ob obnovi potrdila.....	29
3.3.1	Istovetnost in verodostojnost ob obnovi.....	29
3.3.2	Istovetnost in verodostojnost ob obnovi po preklicu	29
3.4.	Istovetnost in verodostojnost ob zahtevi za preklic	29



4.	UPRAVLJANJE S POTRDILI.....	29
4.1.	Zahtevek za pridobitev potrdila	29
4.1.1	Kdo lahko predloži zahtevek za pridobitev potrdila.....	29
4.1.2	Postopek za pridobitev potrdila in odgovornosti	30
4.2.	Postopek ob sprejemu zahtevka za pridobitev potrdila	30
4.2.1	Preverjanje istovetnosti in verodostojnosti bodočega imetnika.....	30
4.2.2	Odobritev/zavrnitev zahtevka.....	30
4.2.3	Čas za izdajo potrdila.....	30
4.3.	Izdaja potrdila.....	31
4.3.1	Postopek izdajatelja ob izdaji potrdila.....	31
4.3.2	Obvestilo imetniku o izdaji potrdila.....	31
4.4.	Prevzem potrdila	31
4.4.1	Postopek prevzema potrdila	31
4.4.2	Objava potrdila.....	31
4.4.3	Obvestilo o izdaji tretjim osebam	32
4.5.	Uporaba potrdil in ključev	32
4.5.1	Uporaba potrdila in zasebnega ključa imetnika	32
4.5.2	Uporaba potrdila in javnega ključa za tretje osebe	32
4.6.	Ponovna izdaja potrdila brez spremembe javnega ključa.....	32
4.6.1	Razlogi za ponovno izdajo potrdila	33
4.6.2	Kdo lahko zahteva ponovno izdajo	33
4.6.3	Postopek ob ponovni izdaji potrdila	33
4.6.4	Obvestilo imetniku o izdaji novega potrdila.....	33
4.6.5	Prevzem ponovno izdanega potrdila.....	33
4.6.6	Objava ponovno izdanega potrdila	33
4.6.7	Obvestilo o izdaji drugim subjektom	33
4.7.	Obnova potrdila.....	33
4.7.1	Razlogi za obnovo potrdila.....	33
4.7.2	Kdo lahko zahteva obnovo potrdila	33
4.7.3	Postopek pri obnovi potrdila.....	33
4.7.4	Obvestilo imetniku o obnovi potrdila	34
4.7.5	Prevzem obnovljenega potrdila.....	34
4.7.6	Objava obnovljenega potrdila	34
4.7.7	Obvestilo o izdaji drugim subjektom	34
4.8.	Sprememba potrdila	34
4.8.1	Razlogi za spremembo potrdila	34
4.8.2	Kdo lahko zahteva spremembo	34
4.8.3	Postopek ob spremembi potrdila	34
4.8.4	Obvestilo imetniku o izdaji novega potrdila	34
4.8.5	Prevzem spremenjenega potrdila	34
4.8.6	Objava spremenjenega potrdila	35
4.8.7	Obvestilo o izdaji drugim subjektom	35
4.9.	Preklic in začasna razveljavitev potrdila.....	35
4.9.1	Razlogi za preklic.....	35
4.9.2	Kdo lahko zahteva preklic.....	35
4.9.3	Postopek za preklic.....	35
4.9.4	Čas za izdajo zahtevka za preklic.....	36
4.9.5	Čas od prejetega zahtevka za preklic do izvedbe preklica	36
4.9.6	Zahteve po preverjanju registra preklicanih potrdil za tretje osebe.....	36
4.9.7	Pogostnost objave registra preklicanih potrdil	37



4.9.8	Čas do objave registra preklicanih potrdil	37
4.9.9	Sprotno preverjanje statusa potrdil	37
4.9.10	Zahteve za sprotno preverjanje statusa potrdil	37
4.9.11	Drugi načini za dostop do statusa potrdil	37
4.9.12	Druge zahteve pri zlorabi zasebnega ključa	37
4.9.13	Razlogi za začasno razveljavitev	37
4.9.14	Kdo lahko zahteva začasno razveljavitev	37
4.9.15	Postopek za začasno razveljavitev	38
4.9.16	Čas začasne razveljavitve.....	38
4.10.	Preverjanje statusa potrdil	38
4.10.1	Dostop za preverjanje	38
4.10.2	Razpoložljivost	38
4.10.3	Druge možnosti	38
4.11.	Prekinitev razmerja med imetnikom in izdajateljem	38
4.12.	Odkrivanje kopije ključev za dešifriranje.....	38
4.12.1	Postopek za odkrivanje ključev za dešifriranje.....	38
4.12.2	Postopek za odkrivanje ključa seje	38
5.	UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE.....	39
5.1.	Fizično varovanje	39
5.1.1	Lokacija in zgradba overitelja.....	39
5.1.2	Fizični dostop do infrastrukture overitelja.....	39
5.1.3	Napajanje in prezračevanje	39
5.1.4	Zaščita pred poplavo.....	39
5.1.5	Zaščita pred požari	39
5.1.6	Hramba nosilcev podatkov.....	40
5.1.7	Odstranjevanje odpadkov	40
5.1.8	Hramba na oddaljeni lokaciji.....	40
5.2.	Organizacijska struktura izdajatelja oz. overitelja	40
5.2.1	Organizacija overitelja in zaupanja vredne vloge.....	40
5.2.2	Število oseb za posamezne vloge	41
5.2.3	Izkazovanje istovetnosti za opravljanje posameznih vlog.....	41
5.2.4	Nezdružljivost vlog	42
5.3.	Nadzor nad osebjem	42
5.3.1	Potrebne kvalifikacije in izkušnje osebja ter njegova primernost	42
5.3.2	Preverjanje primernosti osebja	42
5.3.3	Izobraževanje osebja	42
5.3.4	Zahteve za redna usposabljanja	43
5.3.5	Menjava nalog.....	43
5.3.6	Sankcije	43
5.3.7	Zahteve za zunanje izvajalce.....	43
5.3.8	Dostop osebja do dokumentacije.....	43
5.4.	Varnostni pregledi sistema	43
5.4.1	Vrste dnevnikov	43
5.4.2	Pogostost pregledov dnevnikov beleženih dogodkov	44
5.4.3	Čas hrambe dnevnikov beleženih dogodkov	44
5.4.4	Zaščita dnevnikov beleženih dogodkov	44
5.4.5	Varnostne kopije dnevnikov beleženih dogodkov	44
5.4.6	Zbiranje podatkov za dnevnike beleženih dogodkov	44
5.4.7	Obveščanje povzročitelja dogodka	45
5.4.8	Ocena ranljivosti sistema	45



5.5.	Arhiviranje podatkov	45
5.5.1	Vrste arhiviranih podatkov	45
5.5.2	Čas hrambe.....	45
5.5.3	Zaščita arhiviranih podatkov	45
5.5.4	Varnostno kopiranje arhiviranih podatkov	46
5.5.5	Zahteva po časovnem žigosanju	46
5.5.6	Način zbiranja arhiviranih podatkov	46
5.5.7	Postopek za dostop do arhiviranih podatkov in njihova verifikacija	46
5.6.	Obnova izdajateljevega potrdila	46
5.7.	Okrevalni načrt	46
5.7.1	Postopek v primeru vdorov in zlorabe.....	46
5.7.2	Postopek v primeru okvare strojne in programske opreme ali podatkov	47
5.7.3	Postopek v primeru ogroženega zasebnega ključa izdajatelja	47
5.7.4	Okrevalni načrt.....	47
5.8.	Prenehanje delovanja izdajatelja	47
6.	TEHNIČNE VARNOSTNE ZAHTEVE.....	47
6.1.	Generiranje in namestitvev ključev	47
6.1.1	Generiranje ključev	47
6.1.2	Dostava zasebnega ključa imetnikom.....	47
6.1.3	Dostava javnega ključa izdajatelju potrdil	48
6.1.4	Dostava izdajateljevega javnega ključa tretjim osebam.....	48
6.1.5	Dolžina ključev	48
6.1.6	Generiranje in kakovost parametrov javnih ključev.....	48
6.1.7	Namen ključev in potrdil.....	48
6.2.	Zaščita zasebnega ključa in varnostni moduli	48
6.2.1	Standardi za kriptografski modul.....	49
6.2.2	Nadzor zasebnega ključa s strani pooblaščenih oseb	49
6.2.3	Odkrivanje kopije zasebnega ključa.....	49
6.2.4	Varnostna kopija zasebnega ključa	49
6.2.5	Arhiviranje zasebnega ključa	49
6.2.6	Prenos zasebnega ključa iz/v kriptografski modul	49
6.2.7	Zapis zasebnega ključa v kriptografskem modulu	49
6.2.8	Postopek za aktiviranje zasebnega ključa	50
6.2.9	Postopek za deaktiviranje zasebnega ključa	50
6.2.10	Postopek za uničenje zasebnega ključa	50
6.2.11	Lastnosti kriptografskega modula	50
6.3.	Ostali vidiki upravljanja ključev	50
6.3.1	Arhiviranje javnega ključa	50
6.3.2	Obdobje veljavnosti potrdila in ključev	50
6.4.	Gesla za dostop do zasebnega ključa.....	51
6.4.1	Generiranje gesel.....	51
6.4.2	Zaščita gesel	51
6.4.3	Drugi vidiki gesel.....	51
6.5.	Varnostne zahteve za računalniško opremo izdajatelja	51
6.5.1	Specifične tehnične varnostne zahteve	51
6.5.2	Nivo varnostne zaščite	52
6.6.	Tehnični nadzor življenjskega cikla izdajatelja	52
6.6.1	Nadzor razvoja sistema	52
6.6.2	Upravljanje varnosti	52
6.6.3	Nadzor življenjskega cikla.....	52



6.7.	Varnostna kontrola računalniške mreže	52
6.8.	Časovno žigosanje.....	52
7.	PROFIL POTRDIL, REGISTRA PREKLICANIH POTRDIL IN SPROTNEGA PREVERJANJA STATUSA POTRDIL.....	52
7.1.	Profil potrdil.....	52
7.1.1	Različica potrdil.....	53
7.1.2	Profil potrdil z razširitvami	53
7.1.3	Identifikacijske oznake algoritmov	55
7.1.4	Oblika imen	55
7.1.5	Omejitve glede imen	55
7.1.6	Oznaka politike potrdila.....	55
7.1.7	Uporaba razširitvenega polja za omejitev uporabe politik.....	55
7.1.8	Oblika in obravnava specifičnih podatkov o politiki.....	55
7.1.9	Obravnava kritičnega razširitvenega polja politike.....	55
7.2.	Profil registra preklicanih potrdil.....	55
7.2.1	Različica.....	56
7.2.2	Vsebina registra in razširitve.....	56
7.3.	Profil sprotnega preverjanja statusa potrdil.....	57
7.3.1	Različica.....	57
7.3.2	Razširitve sprotnega preverjanje statusa.....	57
8.	INŠPEKCIJSKI NADZOR.....	57
8.1.	Pogostnost inšpekcijskega nadzora	57
8.2.	Inšpekcijska služba.....	57
8.3.	Neodvisnost inšpekcijske službe	58
8.4.	Področja inšpekcijskega nadzora	58
8.5.	Ukrepi overitelja	58
8.6.	Objava rezultatov inšpekcijskega nadzora.....	58
9.	OSTALE POSLOVNE IN PRAVNE ZADEVE.....	58
9.1.	Cenik storitev	58
9.1.1	Cena izdaje in obnove potrdil.....	58
9.1.2	Cena dostopa do potrdil.....	58
9.1.3	Cena dostopa do statusa potrdila in registra preklicanih potrdil	58
9.1.4	Cene drugih storitev.....	58
9.1.5	Povrnitev stroškov.....	59
9.2.	Finančna odgovornost	59
9.2.1	Zavarovalniško kritje	59
9.2.2	Drugo kritje.....	59
9.2.3	Zavarovanje imetnikov	59
9.3.	Varovanje poslovnih podatkov	59
9.3.1	Varovani podatki	59
9.3.2	Nevarovani podatki	59
9.3.3	Odgovornost glede varovanja poslovnih podatkov	59
9.4.	Varovanje osebnih podatkov	60
9.4.1	Načrt varovanja osebnih podatkov.....	60
9.4.2	Varovani osebni podatki.....	60
9.4.3	Nevarovani osebni podatki.....	60
9.4.4	Odgovornost glede varovanja osebnih podatkov.....	60



9.4.5	Pooblastilo glede uporabe osebnih podatkov	60
9.4.6	Posredovanje osebnih podatkov na uradno zahtevo	60
9.4.7	Druga določila glede posredovanja osebnih podatkov	60
9.5.	Določbe glede pravic intelektualne lastnine	60
9.6.	Obveznosti in odgovornosti.....	61
9.6.1	Obveznosti in odgovornosti izdajatelja.....	61
9.6.2	Obveznost in odgovornost prijavnne službe	62
9.6.3	Obveznosti in odgovornost imetnika	62
9.6.4	Obveznosti in odgovornost tretjih oseb	63
9.6.5	Obveznosti in odgovornosti drugih subjektov	63
9.7.	Zanikanje odgovornosti.....	63
9.8.	Omejitev odgovornosti	64
9.9.	Poravnava škode.....	64
9.10.	Veljavnost politike.....	64
9.10.1	Čas veljavnosti	64
9.10.2	Konec veljavnosti politike	64
9.10.3	Učinek poteka veljavnosti politike	64
9.11.	Komuniciranje med subjekti	64
9.12.	Spreminjanje dokumenta	65
9.12.1	Postopek uveljavitve sprememb	65
9.12.2	Veljavnost in objava sprememb	65
9.12.3	Sprememba identifikacijske oznake politike.....	65
9.13.	Postopek v primeru sporov.....	65
9.14.	Veljavna zakonodaja	65
9.15.	Skladnost z veljavno zakonodajo.....	66
9.16.	Splošne določbe	66
9.16.1	Celovit dogovor	66
9.16.2	Prenos pravic	66
9.16.3	Neodvisnost določil	66
9.16.4	Terjatve	66
9.16.5	Višja sila	66
9.17.	Ostale določbe	66
9.17.1	Razumevanje določil	67
9.17.2	Nasprotujoča določila	67
9.17.3	Odstopanje od določil.....	67
9.17.4	Navzkrižno overjanje.....	67



POVZETEK

Politike za kvalificirana digitalna potrdila in varne časovne žige predstavljajo celoten javni del notranjih pravil Državnega centra za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo (v nadaljevanju *overitelj na MJU*) in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, dodeljevanje časovnih žigov, odgovornost overitelja na MJU ter zahteve, ki jih morajo izpolnjevati uporabniki in tretje osebe, ki uporabljajo in se zanašajo na kvalificirana digitalna potrdila in na varne časovne žige, in drugi overitelji, ki želijo uporabljati storitve overitelja na MJU.

Overitelj na MJU izdaja kvalificirana digitalna potrdila ter varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06), Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (eIDAS; Uradni list EU, št. L 257/73), evropskimi direktivami in standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

Overitelj na MJU izdaja tudi normalizirana digitalna potrdila ter digitalna potrdila za posebne namene oz. zaprte sisteme. Pravila delovanja izdajateljev takih potrdil se določijo s politiko delovanja takega izdajatelja.

Normalizirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:

- izdajateljem potrdil, izdajateljem časovnih žigov, strežnikom oz. informacijskim sistemom, sistemom OCSP, podpisovanju programske kode in registra preklicanih potrdil ter v ostalih primerih, kjer ni možna uporaba kvalificiranih potrdil,
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

Kvalificirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:

- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil,
- za varno elektronsko komuniciranje med imetniki potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

Varni časovni žigi overitelja na MJU so namenjeni:

- zagotavljanju obstoja dokumenta v določenem časovnem trenutku in sicer tako, da se poveže datum in čas žigosanja z vsebino dokumenta na kriptografsko varen način,
- povsod, kjer je potrebno na varen način dokazati časovne lastnosti transakcij in drugih storitev,
- za druge potrebe, kjer se potrebuje varni časovni žig.

Znotraj overitelja na MJU deluje izdajatelj kvalificiranih digitalnih potrdil SIGEN-CA (angl. *Slovenian General Certification Authority*), <http://www.sigen-ca.si>, ki izdaja potrdila za poslovne subjekte in fizične osebe.

Izdajatelj SIGEN-CA je registriran v skladu z veljavno zakonodajo in priznan s strani korenskega izdajatelja SI-TRUST Root (angl. *Slovenian Trust Service Root Certification Authority*).

Politika delovanja SIGEN-CA za fizične osebe določa notranja pravila delovanja izdajatelja, ki definirajo namen, delovanje in metodologijo upravljanja z digitalnimi potrdili, odgovornosti in zahteve, ki jih morajo izpolnjevati vsi subjekti.

Pričujoči dokument določa politiko izdajatelja SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe. Na podlagi tega dokumenta SIGEN-CA izdaja spletna kvalificirana digitalna potrdila, ki izpolnjujejo najvišje varnostne zahteve, po politiki CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.4.



Pričujoči dokument nadomešča prejšnjo objavljeno politiko SIGEN-CA za fizične osebe. Vsa digitalna potrdila, izdana po datumu veljavnosti nove politike, se obravnavajo po novi politiki, za vsa ostala pa velja, da se obravnavajo po novi politiki glede tistih določil, ki lahko smiselno nadomestijo oz. dopolnijo določila iz politike, po kateri je bilo digitalno potrdilo izdano (na primer postopek za preklic velja po novi politiki).

Spremembe, ki jih prinaša nova politika, so sledeče:

- tvorjeno je bilo drugo lastno digitalno potrdilo izdajatelja SIGEN-CA z zasebnim ključem dolžine 3072 bitov, ki se hrani na strojni opremi za varno shranjevanje zasebnih ključev,
- v potrdilu izdajatelja SIGEN-CA in vseh potrdilih imetnikov se uporablja zgostitveni algoritem SHA-256,
- spremenjeno je razločevalno ime digitalnega potrdila izdajatelja SIGEN-CA,
- spremenjena so razločevalna imena potrdil imetnikov, ki lahko vključujejo znake iz kodne tabele UTF-8,
- podprto je sprotno preverjanje statusa potrdil po protokolu OCSP,
- izdajatelj SIGEN-CA je priznan s strani korenkega izdajatelja SI-TRUST Root,
- pri potrdilih za imetnike je v polju uporaba ključa (angl. *Key Usage*) dodana vrednost ContentCommitment,

Kvalificirana digitalna potrdila se pridobijo na podlagi zahtevka, ki ga mora podpisati bodoči imetnik. Izpolnjen zahtevek se odda osebno na prijavno službo (seznam je objavljen na spletni strani <http://www.sigen-ca.si/prijavne-slu.php>) ali pa se zahtevek digitalno podpiše z veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, ki ga je imetniku izdal izdajatelj SIGEN-CA. Digitalno podpisan zahtevek se po elektronski poti posreduje izdajatelju SIGEN-CA.

SIGEN-CA na podlagi odobrenega zahtevka pripravi referenčno številko in avtorizacijsko kodo, ki sta unikatni za vsakega bodočega imetnika kvalificiranega digitalnega potrdila in ju bodoči imetnik potrebuje za prevzem svojega potrdila, ki ga opravi na svoji delovni postaji v skladu z navodili izdajatelja SIGEN-CA. Bodoči imetnik prejme referenčno številko po elektronski pošti, avtorizacijsko kodo pa s pošto pošiljko na svoj stalni ali drug izbran naslov.

Spletno kvalificirano digitalno potrdilo je povezano z enim parom ključev, ki se tvori z imetnikovo programsko ali strojno opremo. SIGEN-CA nikoli ne hrani in tudi nima dostopa do zasebnega ključa. Javni ključ se pošlje izdajatelju SIGEN-CA, ki izda potrdilo, katerega sestavni del je javni ključ. Spletno potrdilo se shrani pri imetniku, dostopno pa je tudi v javnem imeniku potrdil.

SIGEN-CA poleg podatkov, ki so vključeni v digitalno potrdilo, hrani ostale potrebne podatke o imetniku za namen elektronskega poslovanja v skladu z veljavnimi predpisi.

Imetnik mora skrbno varovati zasebne ključe in svoje kvalificirano digitalno potrdilo ter ravnati v skladu s politiko, obvestili izdajatelja SIGEN-CA in veljavno zakonodajo.

1. UVOD

1.1. Pregled

(1) V okviru Ministrstva za javno upravo (v nadaljevanju *MJU*) deluje Državni center za storitve zaupanja (v nadaljevanju *overitelj na MJU*).

(2) Politike overitelja predstavljajo celoten javni del notranjih pravil overitelja na MJU in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi in normaliziranimi digitalnimi potrdili, dodeljevanje časovnih žigov, odgovornost overitelja na MJU ter zahteve, ki jih morajo izpolnjevati imetniki, uporabniki in tretje osebe, ki se zanašajo na kvalificirana in normalizirana digitalna potrdila ter na varne časovne žige, in drugi overitelji, ki želijo uporabljati storitve overitelja na MJU.

(3) Overitelj na MJU izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06), Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (eIDAS; Uradni list EU, št. L 257/73), evropskimi direktivami in standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

(4) Overitelj na MJU izdaja tudi normalizirana digitalna potrdila ter digitalna potrdila za posebne namene oz. zaprte sisteme. Pravila delovanja izdajateljev takih potrdil se določijo s politiko delovanja takega izdajatelja.

(5) Normalizirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:

- izdajateljem potrdil, izdajateljem časovnih žigov, strežnikom oz. informacijskim sistemom, sistemom OCSP, podpisovanju programske kode in registra preklicanih potrdil ter v ostalih primerih, kjer ni možna uporaba kvalificiranih potrdil,
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

(6) Kvalificirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:

- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil,
- za varno elektronsko komuniciranje med imetniki potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

(7) Varni časovni žigi overitelja na MJU so namenjeni:

- zagotavljanju obstoja dokumenta v določenem časovnem trenutku in sicer tako, da se poveže datum in čas žigosanja z vsebino dokumenta na kriptografsko varen način,
- povsod, kjer je potrebno na varen način dokazati časovne lastnosti transakcij in drugih storitev,
- za druge potrebe, kjer se potrebuje varni časovni žig.

(8) Znotraj overitelja na MJU deluje izdajatelj SIGEN-CA (angl. *Slovenian General Certification Authority*), <http://www.sigen-ca.si>, ki izdaja digitalna potrdila za poslovne subjekte in fizične osebe. Pričujoči dokument določa politike izdajatelja SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe.

(9) Izdajatelj SIGEN-CA je registriran v skladu z veljavno zakonodajo in priznan s strani korenskega izdajatelja SI-TRUST Root (angl. *Slovenian Trust Service Root Certification Authority*).

(10) Po pričujoči politiki SIGEN-CA izdaja spletna kvalificirana digitalna potrdila za fizične osebe po CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.4.



(11) Digitalna potrdila SIGEN-CA se lahko uporabljajo za:

- šifriranje podatkov v elektronski obliki,
- overjanje digitalno podpisanih podatkov v elektronski obliki ter izkazovanje istovetnosti imetnika,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil overitelja na MJU.

(12) Za potrdila, izdana na podlagi te politike, je potrebno upoštevati priporočila izdajatelja SIGEN-CA za zaščito zasebnih ključev oz. uporabo varnih kriptografskih modulov.

(13) Pričujoča politika je pripravljena skladno s priporočilom RFC 3647 »Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework«, določa pa notranja pravila izdajatelja SIGEN-CA, ki definirajo namen, delovanje in metodologijo upravljanja z digitalnimi potrdili, odgovornost overitelja na MJU ter zahteve, ki jih morajo izpolnjevati imetniki digitalnih potrdil izdajatelja SIGEN-CA, tretje osebe, ki se zanašajo na digitalna potrdila, in drugi subjekti, ki skladno s predpisi uporabljajo storitve izdajatelja SIGEN-CA.

(14) Medsebojna razmerja med tretjimi osebami, ki se zanašajo na potrdila izdajatelja SIGEN-CA, in overiteljem na MJU se izvajajo tudi na podlagi morebitnega pisnega dogovora.

(15) Overitelj na MJU se preko korenkega izdajatelja SI-TRUST Root lahko povezuje z drugimi overitelji, kar se ureja z medsebojnim dogovorom oz. pogodbo.

1.2. Identifikacijski podatki politike delovanja

(1) Pričujoči dokument je Politika SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe (v nadaljevanju *politika SIGEN-CA*).

(2) Oznaka pričujoče politike je CPName: SIGEN-CA-2, identifikacijska oznaka politike SIGEN-CA-2 pa CPOID: 1.3.6.1.4.1.6105.2.2.3.4.

(3) V vsakem potrdilu je navedba ustrezne politike v obliki oznake CP_{OID}, glej podpogl. 7.1.2.

1.3. Udeleženci infrastrukture javnih ključev

1.3.1 Overitelj

(1) Državni center za storitve zaupanja izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z veljavnimi predpisi in priporočili.

(2) Kontaktni podatki Državnega centra za storitve zaupanja so:

Naslov:	Republika Slovenija Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
Telefon:	01 4788 330
Spletna stran:	http://www.ca.gov.si
Oznaka:	State-institutions

(3) Naloge upravljanja Državnega centra za storitve zaupanja opravlja upravni odbor overitelja na MJU (glej



podpogl. 5.2.1).

(4) V okviru overitelja na MJU deluje korenski izdajatelj SI-TRUST Root ter drugi izdajatelji potrdil. SI-TRUST Root je ob začetku svojega produkcijskega delovanja tvoril svoje lastno digitalno potrdilo, ki je namenjeno overjanju potrdil, ki jih je SI-TRUST Root izdal podrejenim in povezanim izdajateljem kvalificiranih digitalnih potrdil.

Potrdilo SI-TRUST Root vsebuje naslednje podatke¹:

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. <i>Version</i>	3
Identifikacijska oznaka potrdila, angl. <i>Serial Number</i>	90AE 7776 0000 0000 571D D06F
Algoritem za podpis, angl. <i>Signature algorithm</i>	sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. <i>Issuer</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Imetnik, angl. <i>Subject</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Pričetek veljavnosti, angl. <i>Validity: Not Before</i>	Apr 25 07:38:17 2016 GMT
Konec veljavnosti, angl. <i>Validity: Not After</i>	Dec 25 08:08:17 2037 GMT
Algoritem za javni ključ, angl. <i>Subject Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. <i>RSA Public Key</i>	<i>ključ dolžine 3072 bitov</i>
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	4CA3 C368 5E08 0263
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. <i>Certificate Fingerprint – SHA1</i>	3A49 79B4 0FA8 4148 8200 B582 FBEE B63A AB99 19AE
Odtis potrdila SHA-256, angl. <i>Certificate Fingerprint – SHA256</i>	FAD5 4081 1AFA E0DC 767C DF65 72A0 88FA 3CE8 493D D82B 3B86 9A67 D10A AB4E 8124

(5) V okviru overitelja na MJU deluje izdajatelj kvalificiranih digitalnih potrdil SIGEN-CA.

(6) Kontaktni podatki izdajatelja SIGEN-CA so:

¹ Pomen je podan v podpogl. 3.1 in 7.1.



Naslov:	SIGEN-CA Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
E-pošta:	sigen-ca@gov.si
Telefon:	01 4788 330
Spletna stran:	http://www.sigen-ca.si
Dežurna tel. številka za preklice (24 ur vse dni v letu):	01 4788 777
Enotni kontaktni center:	080 2002, 01 4788 590 ekc@gov.si

(7) Izdajatelj SIGEN-CA opravlja naslednje naloge:

- izdaja kvalificirana in normalizirana digitalna potrdila,
- določa in objavlja svojo politiko delovanja,
- določa obrazce za zahtevke za svoje storitve,
- določa in objavlja navodila in priporočila za varno uporabo svojih storitev,
- skrbi za javni imenik potrdil,
- objavlja register preklicanih potrdil,
- skrbi za nemoteno delovanje svojih storitev v skladu s politiko in ostalimi predpisi,
- obvešča svoje uporabnike,
- skrbi za delovanje svoje prijavnne službe in,
- opravlja vse ostale storitve v skladu s to politiko in ostalimi predpisi.

(8) Izdajatelj SIGEN-CA je ob začetku svojega produkcijskega delovanja generiral svoje lastno digitalno potrdilo, ki je namenjeno overjanju potrdil, ki jih je SIGEN-CA izdal imetnikom.

Potrdilo št. 1 SIGEN-CA vsebuje naslednje podatke²:

Naziv polja	Vrednost potrdila izdajatelja SIGEN-CA
Osnovna polja v potrdilu	
Različica, angl. <i>Version</i>	3
Identifikacijska oznaka, angl. <i>Serial Number</i>	3B3C F9C9
Algoritem podpis, angl. <i>Signature Algorithm</i>	sha1WithRSAEncryption
Izdajatelj, angl. <i>Issuer</i>	c=si, o=state-institutions, ou=sigen-ca
Imetnik, angl. <i>Subject</i>	c=si, o=state-institutions, ou=sigen-ca
Pričetek veljavnosti, angl. <i>Validity: Not Before</i>	Jun 29 21:27:46 2001 GMT
Konec veljavnosti, angl. <i>Validity: Not After</i>	Jun 29 21:57:46 2021 GMT
Algoritem za javni ključ, angl. <i>Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)

² Pomen je podan v podpogl. 3.1 in 7.1.



Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. <i>RSA Public Key</i>	<i>ključ dolžine 2048 bitov</i>
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
Odtis potrdila (ni del potrdila)	
Odtis potrdila MD-5, angl. <i>Certificate Fingerprint – MD5</i>	49EF A6A1 F0DE 8EA7 6AEE 5B7D 1E5F C446
Odtis potrdila SHA-1, angl. <i>Certificate Fingerprint – SHA-1</i>	3E42 A187 06BD 0C9C CF59 4750 D2E4 D6AB 0048 FDC4
Odtis potrdila SHA-256, angl. <i>Certificate Fingerprint – SHA-256</i>	12D4 80C1 A3C6 6478 1B99 D9DF 0E9F AF3F 1CAC EE1B 3C30 C312 3A33 7A4A 454F FED2

(9) Izdajatelj SIGEN-CA je pet (5) let pred potekom veljavnosti prvega lastnega digitalna potrdila tvoril drugo lastno digitalno potrdilo, ki je namenjeno overjanju potrdil, ki jih je SIGEN-CA izdal imetnikom ali izdajateljem varnih časovnih žigov od 6.6.2016 dalje.

Potrdilo št. 2 SIGEN-CA vsebuje naslednje podatke:

Naziv polja	Vrednost potrdila izdajatelja SIGEN-CA
Različica, angl. <i>Version</i>	3
Identifikacijska oznaka, angl. <i>Serial Number</i>	CD81 8601 0000 0000 571E 043E
Algoritem za podpis, angl. <i>Signature Algorithm</i>	sha256WithRSAEncryption
Izdajatelj, angl. <i>Issuer</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Imetnik, angl. <i>Subject</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Pričetek veljavnosti, angl. <i>Validity: Not Before</i>	Apr 25 11:19:25 2016 GMT
Konec veljavnosti, angl. <i>Validity: Not After</i>	Apr 25 11:49:25 2036 GMT
Algoritem za javni ključ, angl. <i>Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. <i>RSA Public Key</i>	<i>ključ dolžine 3072 bitov</i>
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)



Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	4C25 278C A82D 729E
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	4C25 278C A82D 729E
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. <i>Certificate Fingerprint – SHA-1</i>	335F 27AE EE7A EA9B D4E3 FE59 EB65 B4AC 8926 E0E7
Odtis potrdila SHA-256, angl. <i>Certificate Fingerprint – SHA-256</i>	C4B9 BB09 EA4E F4A1 37EC 573A EFC1 23C4 B509 62CF B99A E13A 9331 14DB 4A34 274D

(10) Korenski izdajatelj SI-TRUST Root je izdajatelju SIGEN-CA izdal povezovalni potrdili z naslednjimi podatki:

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. <i>Version</i>	3
Identifikacijska oznaka, angl. <i>Serial Number</i>	A668 BD51 0000 0000 571D D0E8
Algoritem za podpis, angl. <i>Signature Algorithm</i>	sha256WithRSAEncryption
Izdajatelj, angl. <i>Issuer</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Imetnik, angl. <i>Subject</i>	c=si, o=state-institutions, ou=sigen-ca
Pričetek veljavnosti, angl. <i>Validity: Not Before</i>	May 24 11:58:27 2016 GMT
Konec veljavnosti, angl. <i>Validity: Not After</i>	Jun 27 22:00:00 2021 GMT
Algoritem za javni ključ, angl. <i>Subject Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. <i>RSA Public Key</i>	<i>ključ dolžine 2048 bitov</i>
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. <i>CRL Distribution Points</i>	Url: http://www.ca.gov.si/crl/si-trust-root.crl Url: ldap://x500.gov.si/cn=SI-TRUST Root, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root, cn=CRL1



Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. <i>Authority Information Access</i>	Access Method=OCSP http://ocsp.ca.gov.si Access Method=CA Issuers http://www.ca.gov.si/crt/si-trust-root.crt
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. <i>certificatePolicies</i>	Certificate Policy: PolicyIdentifier=2.5.29.32.0 (»anyPolicy«) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. <i>Certificate Fingerprint – SHA-1</i>	EF9B C82D C8B0 F209 4529 447F 3BB6 6AC9 9C25 7C66
Odtis potrdila SHA-256, angl. <i>Certificate Fingerprint – SHA-256</i>	E016 01D8 F0D6 9434 E699 735C 4F34 8FC1 5FB4 8F2C 2B20 03FE E0F5 4A90 E819 48FD

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. <i>Version</i>	3
Identifikacijska oznaka, angl. <i>Serial Number</i>	28C3 981D 0000 0000 571D D0E7
Algoritem za podpis, angl. <i>Signature Algorithm</i>	sha256WithRSAEncryption
Izdajatelj, angl. <i>Issuer</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Imetnik, angl. <i>Subject</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Pričetek veljavnosti, angl. <i>Validity: Not Before</i>	May 24 11:49:41 2016 GMT
Konec veljavnosti, angl. <i>Validity: Not After</i>	Apr 23 22:00:00 2036 GMT
Algoritem za javni ključ, angl. <i>Subject Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. <i>RSA Public Key</i>	<i>ključ dolžine 3072 bitov</i>
Razširitve X.509v3	



Objava registra preklicanih potrdil, OID 2.5.29.31, angl. <i>CRL Distribution Points</i>	Url: http://www.ca.gov.si/crl/si-trust-root.crl Url: ldap://x500.gov.si/cn=SI-TRUST Root,oi=VATSI-17659957,o=Republika Slovenija,c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root, cn=CRL1
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. <i>Authority Information Access</i>	Access Method=OCSP http://ocsp.ca.gov.si Access Method=CA Issuers http://www.ca.gov.si/crt/si-trust-root.crt
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. <i>certificatePolicies</i>	Certificate Policy: PolicyIdentifier=2.5.29.32.0 (»anyPolicy«) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	4C25 278C A82D 729E
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. <i>Certificate Fingerprint – SHA-1</i>	D3C6 C554 C171 F9BA 952C E04C AC2C 1C9B D68B 08D4
Odtis potrdila SHA-256, angl. <i>Certificate Fingerprint – SHA-256</i>	7950 15CA ACA7 4715 D341 120D 3F0E FD19 2A03 2F1C 0039 1797 F54E F998 0804 A175

1.3.2 Prijavna služba

(1) Organizacije, ki opravljajo naloge prijavne službe, pooblasti overitelj na MJU. Izpolnjevati morajo pogoje za opravljanje nalog prijavnih služb overitelja na MJU ter delovati v skladu z veljavnimi predpisi in poslovniki za delo prijavnih služb overitelja na MJU.

(2) Naloge prijavne službe so:

- preverjanje istovetnosti imetnikov oz. bodočih imetnikov, njihovih podatkov in drugih potrebnih podatkov,
- sprejemanje zahtevkov za pridobitev potrdil,
- sprejemanje zahtevkov za preklic potrdil,
- preverjanje podatkov v zahtevkih,
- izdajanje potrebne dokumentacije imetnikom oz. bodočim imetnikom,



- posredovanje zahtevkov in ostalih podatkov na varen način na SIGEN-CA.

(3) Izdajatelj SIGEN-CA ima vzpostavljene prijavnne službe na različnih lokacijah, podatki o tem pa so objavljeni na spletnih straneh SIGEN-CA.

1.3.3 Imetniki potrdil

Imetniki potrdil po tej politiki so vedno fizične osebe (angl. *subject*), glej definicijo v pogl. 1.6.

1.3.4 Tretje osebe

(1) Tretje osebe so pravne ali fizične osebe, ki se zanašajo na izdana potrdila izdajatelja SIGEN-CA.

(2) Tretje osebe se morajo ravnati po navodilih izdajatelja SIGEN-CA in morajo vedno preveriti veljavnost potrdila, namen uporabe potrdila, čas veljavnosti potrdila itd. Podrobnejše obveznosti in odgovornosti tretjih oseb so navedene v podpogl. 4.5.2 in 9.6.4.

(3) Med tretjo osebo in izdajateljem SIGEN-CA oz. overiteljem na MJU se lahko sklene medsebojni pisni dogovor.

1.3.5 Ostali udeleženci

Niso predvideni.

1.4. Namen uporabe potrdil

(1) Spletna potrdila SIGEN-CA izdana po pričujoči politiki se lahko uporabljajo za:

- šifriranje podatkov v elektronski obliki,
- overjanje digitalno podpisanih podatkov v elektronski obliki ter izkazovanje istovetnosti podpisnika,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil overitelja na MJU.

(2) Uporaba potrdil je povezana z namenom pripadajočih ključev. Ločimo naslednji možnosti:

- zasebni ključ za podpisovanje in dešifriranje (v nadaljevanju *zasebni ključ*) ter
- javni ključ za overjanje podpisa in šifriranje (v nadaljevanju *javni ključ*).

(3) Izdajatelj SIGEN-CA izdaja tudi potrdila za sistem OCSP za preverjanje veljavnosti potrdil, ki jih je izdal SIGEN-CA.

1.4.1 Pravilna uporaba potrdil in ključev

(1) Namen potrdil oz. pripadajočih ključev je podan v potrdilu v polju *uporaba ključa* (angl. *Key Usage*).

(2) Vsakemu imetniku potrdila pripada en par ključev, ki ga sestavljata zasebni in javni ključ, ki sta namenjena za podpisovanje/overjanje podpisa in dešifriranje/šifriranje podatkov.

1.4.2 Nedovoljena uporaba potrdil in ključev

(1) Potrdila, ki jih izdaja SIGEN-CA, se morajo uporabljati v skladu s politiko in veljavno zakonodajo, sicer njihova uporaba ni dovoljena.

(2) Drugih prepovedi v zvezi z uporabo potrdil izdajatelja SIGEN-CA ni.

1.5. Upravljanje s politiko

1.5.1 Upravljevec politike

Upravni odbor overitelja na MJU je odgovoren za pripravo, prijavo, objavo, upravljanje in interpretacijo tega dokumenta.

1.5.2 Kontaktne osebe

Kontaktne osebe v zvezi s politiko in ostalo dokumentacijo so pooblašene osebe overitelja na MJU (kontaktni podatki so podani v podpogl. 1.3.).

1.5.3 Odgovorna oseba glede skladnosti delovanja izdajatelja s politiko

Odgovorne osebe glede skladnosti delovanja izdajatelja SIGEN-CA skladno s to politiko so pooblašene osebe overitelja na MJU v skladu z nalogami, ki jih opravljajo znotraj organizacijskih skupin (glej podpogl. 5.2.1).

1.5.4 Postopek za sprejem nove politike

(1) Overitelj na MJU lahko izda tudi amandmaje k politiki, glej podpogl. 9.12.

(2) Upravni odbor overitelja na MJU pripravi predlog nove politike oz. amandmaja.

(3) Novo politiko oz. amandmaje potrdi minister, pristojen za javno upravo.

(4) Skladno z ZEPEP se prijava novosti storitev overitelja na MJU opravi tudi na pristojno ministrstvo za register overiteljev v Republiki Sloveniji.

1.6. Izrazi in okrajšave

1.6.1 Izrazi

(1) Splošni izrazi, ki se uporabljajo v tej politiki, so naslednji.

Digitalni podpis	Varen elektronski podpis, ki izpolnjuje zahteve 2. člena ZEPEP in 25. člena Uredbe.
Digitalno potrdilo (Potrdilo)	Potrdilo v elektronski obliki, ki podaja naslednje ključne informacije: (1) podatek o izdajatelju, (2) podatek o imetniku, (3) imetnikov javni ključ, (4) čas veljavnosti in (5) digitalni podpis izdajatelja, ki je to potrdilo izdal.



Infrastruktura javnih ključev	Nabor vlog, politik in postopkov, ki so potrebni za tvorjenje, upravljanje, distribucijo, uporabo, hrambo in preklic digitalnih potrdil ter za upravljanje šifriranja z javnimi ključi (primerjaj okrajšavo <i>PKI</i>).
Kvalificirano digitalno potrdilo	Digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP in ki ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena ZEPEP in Uredbo (primerjaj okrajšavo <i>ZEPEP</i> in izraz <i>Uredba</i>).
Overitelj	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi in ki izpolnjuje zahteve overiteljev kvalificiranih potrdil v skladu z Uredbo in ZEPEP (primerjaj okrajšavo <i>CA</i> in izraz <i>Potrdila</i>).
Register preklicanih potrdil	Seznam digitalnih potrdil, ki so bila preklicana pred potekom veljavnosti (angl. <i>Certification Revocation List</i>). Izdajatelj SIGEN-CA ta seznam objavlja v svojem repozitoriju (primerjaj okrajšavo <i>CRL</i>).
Poslovni subjekt	Pravna ali fizična oseba, registrirana za opravljanje dejavnosti.
Tretja oseba	Pravna ali fizična osebe, ki se zanaša na izdana digitalna potrdila oz. na digitalni podpis, ki ga lahko verificira s pomočjo javnega ključa, ki se nahaja v digitalnem potrdilu.
Uredba k ZEPEP	Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06).
Zanesljivi seznam overiteljev	Zanesljivi seznam države članice Evropske Unije, ki določa minimalne podatke o nadzorovanih/akreditiranih overiteljih, ki izdajajo kvalificirana potrdila v skladu z veljavno zakonodajo, vključno z informacijami o kvalificiranih potrdilih (angl. <i>QC</i>) za overjanje elektronskega podpisa in informacijami, ali je podpis ustvarjen s sredstvi za varno elektronsko podpisovanje (angl. <i>SSCD</i>).

(2) Drugi izrazi, uporabljeni v tej politiki, so podani v spodaj.

Domena	Neodvisna infrastruktura PKI za potrebe povezovanja overiteljev, ki je vzpostavljena znotraj določene organizacije. Izdajatelji znotraj posamezne domene uporabljajo nabor skupnih politik, ki jih označujemo kot politike domene.
Državni center za storitve zaupanja	Državni center za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo.
Imetnik	Uporabnik, ki mu je izdajatelj izdal digitalno potrdilo. V primeru izdajatelja SIGEN-CA in te politike je to fizična oseba (angl. <i>subject</i>).
Infrastruktura overitelja	Vsi prostori overitelja, njegova strojna in programska oprema ter varnostni mehanizmi, ki so potrebni za varno delovanje njegovih izdajateljev.
Interna politika overitelja na MJU	Zaupni del notranjih pravil delovanja overitelja na Ministrstvu za javno upravo v skladu z Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06).
Izdajatelj	Izdajatelj digitalnih potrdil, ki deluje v okviru overitelja (primerjaj okrajšavo <i>CA</i> in izraza <i>Overitelj</i> in <i>Potrdilo</i>).
Izdajatelj SIGEN-CA	V okviru overitelja na MJU deluje več izdajateljev. Le-ti izdajajo bodisi digitalna potrdila bodisi časovne žige (primerjaj izraz <i>Overitelj na MJU</i>). SIGEN-CA je izdajatelj potrdil za pravne in fizične osebe, angl. <i>Slovenian General Certification Authority</i> , http://www.sigen-ca.si .
Javni imenik	Javni imenik, s katerim upravlja izdajatelj SIGEN-CA, je vzpostavljen na strežniku x500.gov.si , in sicer po standardu X.500. V imeniku se objavljajo kvalificirana digitalna potrdila, ki jih izdaja SIGEN-CA, ter register preklicanih potrdil.



Korenski izdajatelj	V hierarhičnem modelu infrastrukture javnih ključev korenski izdajatelj predstavlja osnovno izhodiščno točko zaupanja znotraj določene domene, njegovo potrdilo se uporablja pri preverjanju veljavnosti potrdil znotraj verige zaupanja.
Korenski izdajatelj SI-TRUST Root	Korenski izdajatelj digitalnih potrdil, ki deluje znotraj overitelja na MJU in izdaja digitalna potrdila za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil (angl. <i>Slovenian Trust Service Root Certification Authority</i>), http://www.ca.gov.si .
Medsebojno povezovanje	Medsebojno povezovanje ali tudi navzkrižno overjanje se uporablja za vzpostavljanje zaupanja tako med izdajatelji znotraj posamezne domene kot tudi za povezovanje izdajateljev iz različnih domen (znotrajdomensko (intra-domain) in meddomensko (inter-domain) overjanje).
Objava SIGEN-CA	Javna objava na spletnih straneh SIGEN-CA oz. na straneh overitelja na MJU, http://www.siggen-ca.si oz. http://www.ca.gov.si .
Obvestila SIGEN-CA	Vsa navodila, pojasnila, sezname, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči SIGEN-CA oz. overitelj na MJU in jih objavi ali kako drugače posreduje imetnikom, organizacijam ali tretjim osebam.
Overitelj na MJU	Glej izraz Državni center za storitve zaupanja.
Podrejeni izdajatelj	V hierarhičnem modelu infrastrukture javnih ključev podrejeni izdajatelj nima samoizdanega potrdila, temveč mu je njegovo osnovno digitalno potrdilo izdal neposredno nadrejeni izdajatelj. Delovanje podrejenega izdajatelja je določeno s pravili nadrejenega izdajatelja. V infrastrukturi javnih ključev, ki jo vzpostavlja korenski izdajatelj SI-TRUST Root, leta v vlogi nadrejenega izdajatelja izdaja digitalna potrdila za podrejene izdajatelje. Hkrati SI-TRUST Root predstavlja osnovno izhodišče zaupanja znotraj domene pod SI-TRUST Root.
Politika	Javni del notranjih pravil overitelja, ki določajo namen, delovanje in metodologijo upravljanja z digitalnimi potrdili, odgovornost overitelja ter zahteve, ki jih morajo izpolnjevati uporabniki in tretje osebe, ki uporabljajo in se zanašajo na digitalna potrdila overitelja.
Potrdilo oz. spletno potrdilo	Spletno kvalificirano digitalno potrdilo v elektronski obliki, ki povezuje podatke iz potrdila z imetnikovim zasebnim ključem ter potrjuje imetnikovo istovetnost (angl. <i>web certificate</i>).
Povezani izdajatelj	Izdajatelj digitalnih potrdil, ki mu je korenski izdajatelj SI-TRUST Root izdal povezovalno potrdilo.
Povezovalno potrdilo	Digitalno potrdilo, ki vzpostavlja zaupanje med dvema izdajateljema.
Prijavna služba SIGEN-CA	Po pooblastilu izdajatelja SIGEN-CA prijavna služba sprejema zahtevke za pridobitev in preklic potrdil ter preverja istovetnosti imetnikov oz. bodočih imetnikov (RA, angl. <i>Registration Authority</i>).
Veriga zaupanja	Nabor potrdil, ki se uporabljajo pri preverjanju veljavnosti potrdila končnega uporabnika. Poleg potrdila končnega uporabnika vključuje še potrdilo korenskega izdajatelja ter potrdila podrejenih ali povezanih izdajateljev.
Zahtevak	Obrazec SIGEN-CA za pridobivanje ali preklic potrdil, ki je dostopen preko spletne strani SIGEN-CA oz. pri pooblaščenih osebah na prijavnih službah.

1.6.2 Okrajšave



CA	Izdajatelj digitalnih potrdil, angl. <i>Certification Authority</i> .
CP _{Name}	Ime politike delovanja overitelja oz. izdajatelja (angl. <i>Certification Policy Name</i>), povezano z enolično oznako politike delovanja (primerjaj okrajšavo CP _{OID}).
CP _{OID}	Enolična oznaka politike delovanja, ki temelji na številki OID, angl. <i>Certification Policy Object Identifier</i> .
CRL	Seznam preklicanih potrdil (CRL, angl. <i>Certification Revocation List</i>) (primerjaj izraz <i>Register preklicanih potrdil</i>).
DNS	Baza imen računalnikov, ki so vključeni v internet. Omogoča povezave imen računalnikov z njihovimi številkami IP (DNS, angl. <i>Domain Name System</i>).
eIDAS	Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (eIDAS; Uradni list EU, št. L 257/73).
ETSI	Mednarodna priporočila za področje telekomunikacij, angl. <i>European Telecommunications Standards Institut</i> , http://www.etsi.org .
FIPS	Nabor standardov ameriške vlade za uporabo v računalniških sistemih, angl. <i>Federal Information Processing Standard</i>
HSM	Strojna oprema za varno shranjevanje zasebnih ključev ali strojni varnostni modul, angl. <i>Hardware Security Module</i> .
LDAP	Protokol, ki določa dostop do imenika in je specficiran po IETF (angl. <i>Internet Engineering Task Force</i>) priporočilu RFC 1777 »Leightweight Directory Access Protocol«.
MJU	Ministrstvo za javno upravo, Tržaška cesta 21, 1000 Ljubljana.
OCSP	Protokol za sprotno preverjanje veljavnosti kvalificiranih digitalnih potrdil po priporočilu RFC 2560 »X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, (angl. <i>Online Certificate Status Protocol</i>).
OI	Polje v digitalnem potrdilu z imenom organizationIdentifier in OID številko 2.5.4.97, ki vsebuje identifikacijsko oznako organizacije, različno od njenega uradnega imena. Overitelj na MJU v skladu s standardi ETSI v ta namen uporablja davčno številko organizacije s predpono VATSI.
OID	Mednarodna številka, ki enolično določa posamezni objekt v skladu z mednarodnim standardom ITU-T X.208 (ASN.1), angl. <i>Object Identifier</i> .
PKCS#7 in PKCS#10	Priporočila (angl. <i>Public Key Cryptography Standards</i>) podjetja RSA Security za razvijalce računalniških sistemov, ki uporabljajo asimetrične kriptografske algoritme. <ul style="list-style-type: none">• PKCS#7 določa sintakso za kriptografsko obdelane podatke, kot so digitalni podpisi in digitalne ovojnice. Uporablja se npr. za pošiljanje digitalnih potrdil in seznamov preklicanih potrdil.• PKCS#10 določa sintakso za zahtevek za overitev javnega ključa, imena in drugih atributov.
PKI	Infrastruktura javnih ključev, angl. <i>Public Key Infrastructure</i> .



PKIX-CMP	Določa postopek za izmenjavo podatkov, ki se nanašajo na digitalna potrdila med entitetami infrastrukture overitelja. Zajema tudi <i>de-facto</i> standarda PKCS#7 in PKCS#10. Objavljen je kot priporočilo RFC 4210 » <i>Public Key Infrastructure (based on) X.509 - Certificate Management Protocols</i> «.
RFC	Mednarodna priporočila za Internet skupine IETF, angl. <i>Internet Engineering Task Force</i> in IESG, angl. <i>Internet Engineering Steering Group</i> , angl. <i>Request for Comments</i> , http://www.ietf.org/rfc.html .
UTF-8	Način kodiranja mednarodnega nabora znakov unicode, pri katerem znaki ASCII ostanejo enozložni, ostali znaki pa lahko zasedajo več zlogov.
X.501	Priporočila za razločevalna imena: »ITU-T Recommendation X.501 - Information technology - Open Systems Interconnection - The Directory: Models«.
X.509	Priporočila za profil digitalnih potrdil in registra preklicanih potrdil: RFC 5280: »Internet X.509 Public Key Infrastructure Certificate and CRL Profile«.
TSA	Izdajatelj varnih časovnih žigov (TSA, angl. <i>Time Stamping Authority</i>).
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14).

2. OBJAVE IN ODGOVORNOSTI GLEDE REPOZITORIJA

2.1. Repozitoriji

Overitelj na MJU dokumente oz. podatke izdajatelja SIGEN-CA javno objavlja v dveh repozitorijih:

- v javnem imeniku na strežniku x500.gov.si ter
- na spletnih straneh <http://www.sigen-ca.si>.

2.2. Objava informacij o potrdilih

(1) Overitelj na MJU javno objavlja naslednje dokumente oz. podatke izdajatelja SIGEN-CA:

- politike delovanja izdajatelja,
- cenik,
- zahtevke za storitve izdajatelja,
- navodila za varno uporabo digitalnih potrdil,
- informacije o veljavni zakonodaji v zvezi z delovanjem overitelja na MJU ter
- ostale informacije v zvezi z delovanjem SIGEN-CA.

(2) V strukturi javnega imenika digitalnih potrdil, ki se nahaja na strežniku x500.gov.si, se objavljajo:

- evidenčni podatki o potrdilu (imetnikov naziv, naslov e-pošte, serijska številka ...),
- veljavna digitalna potrdila (podrobneje podana v podpogl. 7.1) in
- register preklicanih digitalnih potrdil (podrobneje podan v podpogl. 7.2).

(3) Ostali dokumenti oz. ključni podatki o delovanju izdajatelja SIGEN-CA ter splošna obvestila imetnikom in tretjim osebam se objavijo na spletnih straneh <http://www.sigen-ca.si>.

(4) Zaupni del notranjih pravil overitelja na MJU, znotraj katerega deluje izdajatelj SIGEN-CA, ni javno dostopen



dokument.

(5) Overitelj na MJU je odgovoren za pravočasnost in verodostojnost objavljenih dokumentov in ostalih podatkov.

2.3. Pogostnost javne objave

(1) Nove politike so objavljene v skladu z navedbo v podpogl. 9.10.

(2) Javno dostopne informacije oz. dokumenti se objavijo takoj po njihovem nastanku.

(3) Potrdila se objavijo v javnem imeniku takoj po njihovi izdaji, evidenčni podatki o potrdilu (imetnikov naziv, naslov e-pošte, serijska številka ...) pa že ob sami rezervaciji potrdila.

(4) Preklicana potrdila se v registru preklicanih potrdil objavijo takoj (podrobno o tem v podpogl. 4.9.8).

(5) Ostale javno dostopne informacije oz. dokumenti se objavijo po potrebi.

2.4. Dostop do repozitorijev

(1) Javno dostopne informacije oz. dokumenti, digitalna potrdila in register preklicanih potrdil so na razpolago 24ur/7dni/365dni brez omejitev.

(2) Javni imenik, ki hrani potrdila, je javno dostopen na strežniku *x500.gov.si* po protokolu LDAP.

(3) Potrdila so dostopna tudi prek spletne strani SIGEN-CA po protokolu HTTPS:

<https://www.sigen-ca.si/cda-cgi/clientcgi?action=directorySearch>.

(4) Overitelj na MJU oz. izdajatelj SIGEN-CA v skladu z Interno politiko overitelja na MJU skrbi za pooblaščno in varno dodajanje, spreminjanje ali brisanje podatkov v javnem imeniku potrdil.

3. ISTOVETNOST IN VERODOSTOJNOST

3.1. Določanje imen

3.1.1 Oblika imen

(1) Vsako potrdilo vsebuje v skladu s priporočilom RFC 5280 podatke o imetniku ter izdajatelju v obliki razločevalnega imena, ki je oblikovano kot UTF8String oz. PrintableString v skladu s priporočilom RFC 5280 »Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile« in s standardom X.501.

(2) V vsakem izdanem potrdilu je naveden izdajatelj le-tega, in sicer v polju *izdajatelj* (angl. *issuer*), glej tabelo v nadaljevanju.

(3) Razločevalno ime imetnikov vsebuje osnovne podatke o imetniku, in sicer v polju *imetnik* (angl. *subject*), glej tabelo v nadaljevanju.



(4) Vsako razločevalno ime vključuje tudi serijsko številko, ki jo določi izdajatelj SIGEN-CA³ (glej podpogl. 3.1.5).

Vrsta potrdila	Naziv polja	Razločevalno ime ⁴
potrdilo izdajatelja SIGEN-CA	Izdajatelj, angl. <i>Issuer</i> in	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
spletno potrdilo	Imetnik, angl. <i>Subject</i>	c=SI, st=Slovenija, ou=individuals, cn=<ime in priimek>, gn=<ime>, surname=<priimek>, sn=<serijska številka>

3.1.2 Zahteva po smiselnosti imen

- (1) Imetnik potrdila je nedvoumno določen z razločevalnim imenom v skladu s prejšnjim razdelkom.
- (2) Podatki o imetniku oz. nazivu v razločevalnem imenu vsebujejo znake iz kodne tabele UTF-8.

3.1.3 Uporaba anonimnih imen ali psevdonimov

Ni predvidena.

3.1.4 Pravila za interpretacijo imen

Pravila so navedena v podpogl. 3.1.1 in 3.1.2.

3.1.5 Enoličnost imen

- (1) Podeljeno razločevalno ime je enolično za vsako izdano potrdilo.
- (2) Enolična je tudi serijska številka, ki je vključena v razločevalno ime.
- (3) Serijska številka je 13-mestno število in enolično določa imetnika oz. izdano potrdilo. Spodnja tabela natančneje določa pomen in vrednosti posameznih mest serijskega števila:

Serijska številka	Pomen	Vrednost
1. mesto	oznaka za potrdilo, ki ga je izdal izdajatelj SIGEN-CA	2
2.- 8. mesto	enolično število imetnika	/
9. - 10. mesto	oznaka za spletno potrdilo za fizično osebo	12

³ Potrdilo izdajatelja SIGEN-CA ne vsebuje serijske številke.

⁴ Pomen posameznih označb: država (»c«), organizacija (»o«), organizacijska enota (»ou«), ime (»cn«), serijska številka (»sn«).



11. – 12. mesto	zaporedno število istovrstnega potrdila	/
13. mesto	kontrolna številka	/

3.1.6 Priznavanje, verodostojnost in vloga blagovnih znamk

(1) Imetniki ne smejo zahtevati imen, ki bi pripadala nekomu drugemu in bi bile s tem kršene avtorske ali druge pravice tretjih oseb.

(2) Morebitne spore rešujeta izključno prizadeta stran in imetnik.

3.2. Začetno preverjanje istovetnosti

3.2.1 Metoda za dokazovanje lastništva zasebnega ključa

Dokazovanje o posedovanju zasebnega ključa, ki pripada javnemu ključu v potrdilu, je zagotovljeno z varnimi postopki pred in ob prevzemu potrdila ter protokolom PKCS#10. Zahtevki za izdajo potrdila vsebuje javni ključ in je podpisan s pripadajočim zasebnim ključem, npr. v obliki PKCS#10 v skladu z RSA PKCS#10 Certification Request Syntax Standard.

3.2.2 Preverjanje istovetnosti organizacij

Ni predpisano.

3.2.3 Preverjanje istovetnosti fizičnih oseb

(1) Preverjanje istovetnosti imetnikov opravi prijavna služba overitelja na MJU.

(2) Izdajatelj SIGEN-CA preveri osebne podatke o imetniku v ustreznih registrih.

(3) Pri naslovu e-pošte imetnika izdajatelj SIGEN-CA preveri, ali je na zahtevku podani naslov e-pošte veljaven, in sicer na način, da SIGEN-CA pošlje obvestilo bodočemu imetniku ob sprejemu zahtevka. Če je to sporočilo zavrnjeno, prevzem potrdila ni mogoč.

3.2.4 Nепreverjeni podatki pri začetnem preverjanju

Nepreverjenih podatkov v potrdilu ni.

3.2.5 Preverjanje pooblastil

Ni predpisano.

3.2.6 Merila za medsebojno povezovanje



- (1) Izdajatelj SIGEN-CA je medsebojno priznan s strani korenškega izdajatelja SI-TRUST Root.
- (2) Izdajatelj SIGEN-CA se medsebojno ne povezuje z drugimi izdajatelji.
- (3) Overitelj na MJU se preko korenškega izdajatelja SI-TRUST Root lahko povezuje z drugimi overitelji, kar se ureja z medsebojnim dogovorom oz. pogodbo.

3.3. Istovetnost in verodostojnost ob obnovi potrdila

3.3.1 Istovetnost in verodostojnost ob obnovi

- (1) Istovetnost imetnikov pri ponovni izdaji spletnega potrdila se preverja bodisi na prijavnih službah overitelja na MJU ali pa se ugotavlja na podlagi že izdanega veljavnega digitalnega potrdila za fizične osebe, ki ga je izdal izdajatelj SIGEN-CA.
- (2) Izdajatelj SIGEN-CA preveri osebne podatke o imetniku v ustreznih registrih.
- (3) Pri naslovu e-pošte imetnika izdajatelj SIGEN-CA preveri, ali je na zahtevku podani naslov e-pošte veljaven, in sicer na način, da SIGEN-CA pošlje obvestilo bodočemu imetniku ob sprejemu zahtevka. Če je to sporočilo zavrnjeno, prevzem potrdila ni mogoč.

3.3.2 Istovetnost in verodostojnost ob obnovi po preklicu

Preverjanje imetnikov poteka skladno z določili iz podpogl. 3.2.3.

3.4. Istovetnost in verodostojnost ob zahtevi za preklic

- (1) Zahtevek za preklic potrdila imetnik odda:
 - osebno na prijavnih službah, kjer pooblaščenec osebe preverijo istovetnost prosilca,
 - elektronsko, vendar mora biti zahtevek digitalno podpisan z zasebnim ključem, ki pripada digitalnemu potrdilu, ki ga je izdal overitelj na MJU, s tem pa izkazana tudi istovetnost prosilca.
- (2) V primeru preklica preko telefona na dežurno telefonsko številko izdajatelja SIGEN-CA mora imetnik navesti v ta namen izbrano geslo.
- (3) Podroben postopek za preklic je podan v podpogl. 4.9.3.

4. UPRAVLJANJE S POTRDI

4.1. Zahtevek za pridobitev potrdila

4.1.1 Kdo lahko predloži zahtevek za pridobitev potrdila

Bodoči imetniki potrdil so vedno fizične osebe, glej definicijo v podpogl. 1.3.3.

4.1.2 Postopek za pridobitev potrdila in odgovornosti

- (1) Za pridobitev potrdila mora bodoči imetnik pravilno izpolniti in podpisati zahtevek za pridobitev potrdila. Zahtevek lahko odda procesno sposobna oseba, starejša od 15 let.
- (2) V primeru, da je bodoči imetnik invalidna oseba, lahko zahtevek za pridobitev potrdila odda v njegovem imenu druga oseba, ki mora priložiti notarsko ali upravno overjeno pooblastilo ter svoj veljavni osebni dokument s sliko.
- (3) Bodoči imetnik lahko izdajatelju SIGEN-CA po elektronski poti posreduje zahtevek, digitalno podpisan z njegovim veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, ki mu ga je izdal izdajatelj SIGEN-CA.
- (4) Zahtevki za pridobitev so dostopni na prijavnih službah oz. pri drugih pooblaščenih osebah izdajatelja SIGEN-CA in na spletnih straneh SIGEN-CA.
- (5) Bodoči imetnik je za pridobitev potrdila dolžan:
 - izpolniti zahtevek za pridobitev potrdila z resničnimi in pravilnimi podatki,
 - zahtevek oddati na prijavno službo osebno ali izdajatelju SIGEN-CA po elektronski poti posredovati zahtevek, digitalno podpisan z njegovim veljavnim digitalnim potrdilom za fizične osebe, ki mu ga je izdal izdajatelj SIGEN-CA,
 - opraviti prevzem potrdila na varen način po navodilih izdajatelja SIGEN-CA.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

4.2.1 Preverjanje istovetnosti in verodostojnosti bodočega imetnika

- (1) V primeru osebne oddaje zahtevka na prijavni službi pooblaščen oseba na prijavni službi preveri istovetnost bodočega imetnika v skladu z veljavno zakonodajo. Bodoči imetnik mora izkazati svojo istovetnost z veljavnim osebnim dokumentom.
- (2) V primeru oddaje zahtevka na elektronski način pooblaščen oseba izdajatelja SIGEN-CA opravi overjanje elektronskega podpisa. Istovetnost bodočega imetnika se izkaže z veljavnostjo njegovega elektronskega podpisa.
- (3) Preveriti je potrebno istovetnost bodočega imetnika oz. vse tiste podatke, ki so navedeni v zahtevku in so dostopni v uradnih evidencah oz. drugih uradnih veljavnih dokumentih.

4.2.2 Odobritev/zavrnitev zahtevka

- (1) Zahtevek za pridobitev potrdila odobrijo oz. v primeru nepravilnih ali pomanjkljivih podatkov ali neizpolnjevanja obveznosti zavrnejo pooblaščen osebo izdajatelja SIGEN-CA.
- (2) O odobritvi oz. zavrnitvi je bodoči imetnik obveščen po e-pošti.
- (3) V primeru odobritve izdajatelj SIGEN-CA pred izdajo potrdila obvesti bodočega imetnika z vso potrebno dokumentacijo v skladu z veljavno zakonodajo.

4.2.3 Čas za izdajo potrdila

SIGEN-CA na podlagi odobrenega zahtevka bodočemu imetniku digitalnega potrdila avtorizacijsko kodo in referenčno številko posreduje najkasneje v desetih (10) dneh od odobritve zahtevka.

4.3. Izdaja potrdila

4.3.1 Postopek izdajatelja ob izdaji potrdila

(1) V primeru odobrenega zahtevka SIGEN-CA posreduje bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo po dveh ločenih poteh: referenčno številko po elektronski pošti, avtorizacijsko kodo pa s pošto pošiljko, izjemoma pa ju lahko pooblaščen oseb SIGEN-CA preda tudi osebno. Oba podatka bodoči imetnik potrebuje za prevzem digitalnega potrdila.

(2) Potrdila se izdajajo izključno na infrastrukturi overitelja na MJU.

(3) Izdano digitalno potrdilo SIGEN-CA objavi v javnem imeniku in na spletnih straneh (glej podpogl. 4.4.2).

4.3.2 Obvestilo imetniku o izdaji potrdila

(1) Bodoči imetnik je obveščen o odobritvi oz. zavrnitvi zahtevka za pridobitev digitalnega potrdila.

(2) Dva (2) meseca pred potekom potrdila oz. ključev izdajatelj SIGEN-CA imetnika o tem obvesti po e-pošti.

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila

(1) Za prevzem potrdila bodoči imetnik potrebuje referenčno številko in avtorizacijsko kodo, ki mu ju izda SIGEN-CA, glej podpogl. 4.3.

(2) Način in podrobna navodila za prevzem potrdil po tej politiki so opisana na spletni strani <http://www.sigenc.si>. Prav tako so na spletni strani objavljene tudi vse novice v zvezi z načinom prevzema potrdil.

(3) Imetnik mora takoj po prevzemu potrdila preveriti podatke v tem potrdilu. Če izdajatelja SIGEN-CA ne obvesti o morebitnih napakah, se smatra, da se z vsebino strinja in da soglaša s pogoji delovanja in prevzemom obveznosti in odgovornosti.

(4) Bodoči imetnik potrdila mora po prejemu referenčne številke in avtorizacijske kode potrdilo prevzeti v šestdesetih (60) dneh od rezervacije potrdila. Na zahtevo bodočega imetnika je možno čas za prevzem podaljšati za novih šestdesetih (60), sicer SIGEN-CA rezervacijo potrdila prekliče.

(5) Po prevzemu potrdila postaneta referenčna številka in avtorizacijska koda neuporabni.

4.4.2 Objava potrdila

Izdano potrdilo se javno objavi v repozitoriju overitelja na MJU, kot je navedeno v pogl. 2.

4.4.3 Obvestilo o izdaji tretjim osebam

Ni predpisano.

4.5. Uporaba potrdil in ključev

4.5.1 Uporaba potrdila in zasebnega ključa imetnika

- (1) Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnega ključa dolžan:
- podatke za prevzem potrdila skrbno varovati pred nepooblaščenimi osebami,
 - hraniti zasebni ključ in potrdilo v skladu z obvestili in priporočili SIGEN-CA,
 - zasebni ključ in vse druge zaupne podatke ščititi s primernim geslom v skladu s priporočili SIGEN-CA ali na drug način tako, da ima dostop do njih samo imetnik,
 - skrbno varovati gesla za zaščito zasebnega ključa,
 - po preteku veljavnosti oz. preklicu potrdila ravnati v skladu z obvestili SIGEN-CA.
- (2) Imetnik mora varovati zasebni ključ pred nepooblaščenno uporabo.
- (3) Ostale dolžnosti in odgovornosti so določene v podpogl. 9.6.3.

4.5.2 Uporaba potrdila in javnega ključa za tretje osebe

- (1) Tretja oseba, ki se zanaša na potrdilo, mora ravnati in uporabljati potrdila v skladu s politiko in ostalimi veljavnimi predpisi.
- (2) Tretja oseba se lahko zanaša na potrdilo samo za namen, določen v potrdilu (glej podpogl. 6.1.7), in na način, ki je določen s politiko,
- (3) Ob uporabi potrdila mora tretja oseba vedno preveriti veljavnost digitalnega potrdila v skladu z navodili izdajatelja SIGEN-CA:
- v času uporabe potrdila preveriti, če potrdilo ni preklicano,
 - v času uporabe potrdila preveriti, če je bil digitalni podpis kreiran v času veljavnosti in z ustreznim namenom potrdila,
 - v času uporabe potrdila preveriti podpis izdajatelja potrdila SIGEN-CA, ki je objavljen v tej politiki in tudi na morebiten drug način posredovan tretjim osebam,
 - upoštevati druge določbe, če je z overiteljem na MJU oz. izdajateljem SIGEN-CA sklenila dogovor o uporabi potrdil.
- (4) Tretja oseba mora za overjanje podpisa oz. druge kriptografske operacije uporabljati programsko in strojno opremo, s katero lahko na verodostojen način preveri vse zgoraj navedene zahteve za varno uporabo potrdil.
- (5) Ostale dolžnosti in odgovornosti so določene v podpogl. 9.6.4.

4.6. Ponovna izdaja potrdila brez spremembe javnega ključa

Ni podprta.



4.6.1 Razlogi za ponovno izdajo potrdila

Ni podprto.

4.6.2 Kdo lahko zahteva ponovno izdajo

Ni podprto.

4.6.3 Postopek ob ponovni izdaji potrdila

Ni podprto.

4.6.4 Obvestilo imetniku o izdaji novega potrdila

Ni podprto.

4.6.5 Prevzem ponovno izdanega potrdila

Ni podprto.

4.6.6 Objava ponovno izdanega potrdila

Ni podprto.

4.6.7 Obvestilo o izdaji drugim subjektom

Ni podprto.

4.7. Obnova potrdila

4.7.1 Razlogi za obnovo potrdila

Ni podprto.

4.7.2 Kdo lahko zahteva obnovo potrdila

Ni podprto.

4.7.3 Postopek pri obnovi potrdila

Ni podprto.



4.7.4 Obvestilo imetniku o obnovi potrdila

Ni podprto.

4.7.5 Prezem obnovljenega potrdila

Ni podprto.

4.7.6 Objava obnovljenega potrdila

Ni podprto.

4.7.7 Obvestilo o izdaji drugim subjektom

Ni podprto.

4.8. Sprememba potrdila

(1) Če pride do spremembe podatkov, ki vplivajo na veljavnost razločevalnega imena oz. drugih podatkov v potrdilu, je potrebno potrdilo preklicati.

(2) Za pridobitev novega potrdila je potrebno ponoviti postopek za pridobitev novega potrdila, kot je naveden v podpogl. 4.1. Storitev izdajatelja za spremembo potrdil ni podprta.

4.8.1 Razlogi za spremembo potrdila

Ni podprto.

4.8.2 Kdo lahko zahteva spremembo

Ni podprto.

4.8.3 Postopek ob spremembi potrdila

Ni podprto.

4.8.4 Obvestilo imetniku o izdaji novega potrdila

Ni podprto.

4.8.5 Prezem spremenjenega potrdila

Ni podprto.

4.8.6 Objava spremenjenega potrdila

Ni podprto.

4.8.7 Obvestilo o izdaji drugim subjektom

Ni podprto.

4.9. Preklic in začasna razveljavitev potrdila⁵

4.9.1 Razlogi za preklic

(1) Preklic potrdila mora imetnik zahtevati v primeru:

- če je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- če obstaja nevarnost zlorabe zasebnega ključa ali potrdila imetnika,
- če so se spremenili oz. so napačni ključni podatki, navedeni v potrdilu.

(2) Izdajatelj SIGEN-CA prekliče potrdilo tudi brez zahteve imetnika takoj, ko izve:

- da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,
- da je prišlo do napake pri preverjanju istovetnosti podatkov na prijavnici službi,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- za neizpolnjevanje obveznosti imetnika,
- da niso poravnani morebitni stroški za upravljanje digitalnih potrdil,
- da je bila infrastruktura overitelja na MJU ogrožena na način, ki vpliva na zanesljivost potrdila,
- da je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- da bo SIGEN-CA prenehal z izdajanjem potrdil ali da je bilo overitelju na MJU prepovedano upravljanje s potrdili in njegove dejavnosti ni prevzel drug overitelj,
- da je preklic odredilo pristojno sodišče ali upravni organ.

4.9.2 Kdo lahko zahteva preklic

Preklic potrdila lahko zahteva:

- pooblaščen oseba izdajatelja SIGEN-CA,
- imetnik,
- pristojno sodišče ali
- upravni organ.

4.9.3 Postopek za preklic

(1) Preklic lahko imetnik zahteva:

- osebno v času uradnih ur na prijavnici službi,

⁵ Po priporočilu RFC 3647 to podpoglavje vključuje tudi postopek za storitev suspenza, ki jo izdajatelj SIGEN-CA ne omogoča.



- elektronsko štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov,
- telefonsko štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov.

(2) Če se preklic zahteva:

- osebno, je potrebno ustrezen zahtevek za preklic potrdila oddati na prijavno službo;
- elektronsko, mora imetnik poslati na SIGEN-CA elektronsko sporočilo z zahtevkom za preklic, ki mora biti digitalno podpisan z zaupanja vrednim potrdilom za njegovo overjanje. Ob tem mora izdajatelj zahtevka za preklic hkrati o tem telefonsko obvestiti SIGEN-CA na dežurno telefonsko številko za preklice (glej podpogl. 1.3.1);
- telefonsko, mora imetnik poklicati na dežurno telefonsko številko za preklice (glej podpogl. 1.3.1), ob tem mora navesti geslo, ki ga je v ustreznem zahtevku za pridobitev potrdila imetnik podal kot geslo za preklic potrdila oz. ga je drugače varno posredoval SIGEN-CA. Brez gesla za preklic imetnik ne more telefonsko preklicati potrdila.

(3) O datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic je imetnik vedno obveščen.

(4) Če preklic odredi sodišče ali upravni organ, se to izvede po veljavnih postopkih

4.9.4 Čas za izdajo zahtevka za preklic

Zahtevek za preklic je potrebno zahtevati nemudoma, če gre za možnost zlorabe ali nezanesljivosti ipd. nujne primere, sicer pa prvi delovni dan v času, ki velja za poslovni čas državnih organov oz. uradnih ur na prijavnih službah (glej naslednje podpoglavje).

4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica

(1) Overitelj na MJU po prejemu veljavne zahteve za preklic:

- najkasneje v štirih (4) urah preklic potrdilo, če gre za preklic zaradi nevarnosti zlorabe ali nezanesljivosti ipd.,
- sicer pa prvi delovni dan po prejetju zahtevka za preklic.

(2) Po preklicu je tako potrdilo takoj dodano v register preklicanih potrdil in brisano iz javnega imenika potrdil⁶.

4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

(1) Tretje osebe, ki se zanašajo na potrdilo, morajo pred uporabo preveriti najnovejši objavljeni register preklicanih potrdil.

(2) Zaradi verodostojnosti in celovitosti je vedno potrebno preveriti tudi verodostojnost tega registra, ki je digitalno podpisan s strani SIGEN-CA.

(3) Tretja oseba mora za vsako uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja verige zaupanja v skladu z RFC 5280.

⁶ V javnem imeniku ostanejo samo evidenčni podatki o potrdilu.



(4) Če tretja oseba ne more preveriti statusa digitalnega potrdila v registru preklicanih potrdil, lahko zavrne uporabo digitalnega potrdila oz. digitalno potrdilo kljub temu uporabi in zavestno sprejme.

4.9.7 Pogostnost objave registra preklicanih potrdil

Register preklicanih potrdil se osvežuje (za dostop do registra glej podpogl. 7.2.2):

- po vsakem preklicu potrdila,
- enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil, in sicer približno štiriindvajset (24) ur po zadnjem osveževanju.

4.9.8 Čas do objave registra preklicanih potrdil

Objava novega registra preklicanih potrdil se izvede:

- v javnem imeniku na strežniku *x500.gov.si* takoj,
- na spletni strani pa z zakasnitvijo največ desetih (10) minut.

4.9.9 Sprotno preverjanje statusa potrdil

Podprt je protokol za sprotno preverjanje statusa potrdil (OCSP) v skladu s priporočilom RFC 2560 »X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP«. Podrobno o tem glej podpogl. 7.3.

4.9.10 Zahteve za sprotno preverjanje statusa potrdil

Tretje osebe morajo ob uporabi potrdila vedno preveriti, ali je potrdilo, na katerega se zanašajo, preklicano. Glej tudi podpogl. 4.9.6.

4.9.11 Drugi načini za dostop do statusa potrdil

Niso podprti.

4.9.12 Druge zahteve pri zlorabi zasebnega ključa

Niso predpisane.

4.9.13 Razlogi za začasno razveljavitev

Ni podprto.

4.9.14 Kdo lahko zahteva začasno razveljavitev

Ni podprto.

4.9.15 Postopek za začasno razveljavitev

Ni podprto.

4.9.16 Čas začasne razveljavitve

Ni podprto.

4.10. Preverjanje statusa potrdil

4.10.1 Dostop za preverjanje

Register preklicanih potrdil je objavljen v javnem imeniku na strežniku x500.gov.si ter na spletnih straneh <http://www.sigen-ca.si>, sprotno preverjanje statusa potrdila je dostopno na naslovu <http://ocsp.sigen-ca.si>, podrobnosti o dostopu pa so v podpogl. 7.2 in 7.3.

4.10.2 Razpoložljivost

Preverjanje statusa potrdil je na razpolago štiriindvajset (24) ur vse dni v letu.

4.10.3 Druge možnosti

Niso predpisane.

4.11. Prekinitev razmerja med imetnikom in izdajateljem

Razmerje med imetnikom in overiteljem na MJU se prekine, če

- imetnikovo potrdilo preteče in ga le-ta ne podaljša,
- je potrdilo preklicano, imetnik pa ne zaprosi za novega.

4.12. Odkrivanje kopije ključev za dešifriranje

4.12.1 Postopek za odkrivanje ključev za dešifriranje

Ni podprto.

4.12.2 Postopek za odkrivanje ključa seje

Ni podprto.

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

5.1. Fizično varovanje

- (1) Oprema overitelja na MJU je varovana z večnivojskim sistemom fizičnega in elektronskega varovanja.
- (2) Varovanje infrastrukture overitelja na MJU se izvaja v skladu s priporočili stroke za najvišji nivo varovanja.
- (3) Celoten opis infrastrukture overitelja na MJU in postopki upravljanja ter varovanje le-te so določeni z Interno politiko overitelja na MJU.

5.1.1 Lokacija in zgradba overitelja

- (1) Oprema overitelja na MJU je postavljena v posebnih, varovanih, ločenih prostorih v okviru infrastrukture Ministrstva za javno upravo.
- (2) Zavarovana je z večnivojskim sistemom fizičnega in elektronskega varovanja.
- (3) Podrobna določila so v Interni politiki overitelja na MJU.

5.1.2 Fizični dostop do infrastrukture overitelja

- (1) Dostop do infrastrukture overitelja na MJU oz. izdajatelja je omogočen samo pooblaščenim osebam overitelja na MJU skladno z njihovimi nalogami in pooblastili, glej podpogl. 5.2.1.
- (2) Vsi dostopi so varovani v skladu z veljavno zakonodajo in priporočili.
- (3) Podrobna določila so v Interni politiki overitelja na MJU.

5.1.3 Napajanje in prezračevanje

- (1) Infrastruktura overitelja na MJU ima zagotovljeno neprekinjeno napajanje in ustrezne klimatske sisteme.
- (2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.4 Zaščita pred poplavo

- (1) Infrastruktura overitelja na MJU ni izpostavljena nevarnosti poplav.
- (2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.5 Zaščita pred požari

- (1) Prostor overitelja na MJU so varovani pred morebitnim izbruhom požara.
- (2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.6 Hramba nosilcev podatkov

- (1) Podatki v fizični ali elektronski obliki se zapisujejo na nosilce podatkov, ki se varno hranijo v zaščitениh objektih.
- (2) Varnostne kopije programske opreme in šifriranih baz overitelja na MJU se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih, na različnih lokacijah.
- (3) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.7 Odstranjevanje odpadkov

- (1) Overitelj na MJU zagotavlja varno odstranjevanje in uničevanje dokumentov v fizični in elektronski obliki.
- (2) Odstranjevanje odpadkov izvaja posebna komisija v skladu z Interno politiko overitelja na MJU.

5.1.8 Hramba na oddaljeni lokaciji

Glej podpogl. 5.1.6.

5.2. Organizacijska struktura izdajatelja oz. overitelja

5.2.1 Organizacija overitelja in zaupanja vredne vloge

- (1) Operativno, organizacijsko in strokovno pravilno delovanje overitelja na MJU vodi pooblaščen oseb overitelja na MJU, ki jo za opravljanje navedenih nalog pooblasti vodja notranje organizacijske enote v okviru Ministrstva za javno upravo, ki je odgovorna za upravljanje digitalnih potrdil (v nadaljevanju *vodja NOE*).
- (2) Med pooblaščen osebe overitelja na MJU spadajo:
 - zaposleni pri overitelju na MJU in
 - prijavne službe.
- (3) Zaposleni pri overitelju na MJU so razporejeni v šest organizacijskih skupin, ki pokrivajo naslednja vsebinska področja:
 - upravljanje overitelja,
 - upravljanje s potrdili,
 - upravljanje z infrastrukturo,
 - varovanje in kontrola,
 - notranje preverjanje skladnosti,
 - pravno-administrativno.
- (4) Zaupanja vredne vloge opravljajo zaposleni, ki izvajajo naloge s sledečih vsebinskih področij:
 - upravljanje overitelja,
 - upravljanje s potrdili,
 - upravljanje z infrastrukturo,
 - varovanje in kontrola.



Organizacijska skupina	Vloga	Osnovne naloge	Število oseb
Upravljanje overitelja	Upravljevec sistema	– Strategija delovanja overitelja na MJU – Določevanje prvega varnostnega inženirja – Operativno vodenje overitelja na MJU	3
Upravljanje s kvalificiranimi potrdili	Prvi varnostni inženir	– Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil – Določevanje drugih varnostnih inženirjev	1
	Drugi varnostni inženirji	– Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil	2
	Administratorji potrdil	– Upravljanje s potrdili	2
Upravljanje z infrastrukturo	Sistemske administrator	– Upravljanje z operacijskim sistemom (nameščanje, konfiguracija, vzdrževanje...) – Upravljanje s telekomunikacijami (sistem za preprečevanje in odkrivanje vdorov, požarna pregrada, ...)	2
Varovanje in kontrola	Varnostni administrator	– Pregled dnevnikov – Vzdrževanje varnostnih kopij	1
Notranje preverjanje skladnosti	Notranji revizor		1
Pravno-administrativno	Pravnik		1

(5) Upravni odbor overitelja na MJU sestavljajo upravljevec sistema, varnostni inženir, pravnik in vodja NOE.

(6) Naloge upravnega odbora overitelja na MJU so:

- imenovanje zaposlenih, ki izvajajo zaupanja vredne vloge,
- priprava sprememb in novih verzij politike,
- izvajanje ugotavljanja skladnosti v skladu z eIDAS,
- odločanje o izdaji in preklicu potrdil za podrejene in povezane izdajatelje,
- druge naloge upravljanja Državnega centra za storitve zaupanja.

5.2.2 Število oseb za posamezne vloge

(1) Posamezne občutljive naloge mora skladno z veljavno zakonodajo in Interno politiko overitelja na MJU opravljati več oseb hkrati.

(2) Na infrastrukturi je zagotovljeno, da varnostne ali kritične postopke odobrita dve pooblaščenici istočasno.

(3) Navedeno število oseb v tabeli v podpogl. 5.2.1 predstavlja minimalno število oseb.

5.2.3 Izkazovanje istovetnosti za opravljanje posameznih vlog

Izkazovanje istovetnosti in pravice dostopov za opravljanje posameznih nalog skladno z vlogo posamezne organizacijske skupine kot tudi za opravljanje nalog prijavnih služb je zagotovljena z varnostnimi mehanizmi in kontrolnimi postopki na programski opremi overitelja na MJU.

5.2.4 Nezdržljivost vlog

- (1) Vse organizacijske skupine overitelja na MJU, navedene v tabeli podpogl. 5.2.1, so med seboj nezdržljive.
- (2) Ob pomanjkanju ustrezno usposobljenega kadra se lahko zaradi podobne vrste opravil združi osebje določenih skupin z enakimi oz. podobnimi privilegiji delovanja.
- (3) Vloge posameznih organizacijskih skupin so določene z Interno politiko overitelja na MJU.

5.3. Nadzor nad osebjem

V skladu z veljavno zakonodajo so podrobnejša določila glede nadzora osebja določena v Interni politiki overitelja na MJU.

5.3.1 Potrebne kvalifikacije in izkušnje osebja ter njegova primernost

- (1) Osebje overitelja na MJU ima skladno z zahtevami veljavne zakonodaje ustrezne kvalifikacije in izkušnje ter je skladno z zahtevami veljavne zakonodaje primerno za opravljanje svojih nalog.
- (2) Pooblaščen osebe overitelja na MJU pred pričetkom opravljanja nalog za potrebe overitelja na MJU podpišejo izjavo o opravljanju nalog s posebnimi odgovornostmi.
- (3) Zaposleni pri overitelju na MJU, ki opravljajo zaupanja vredne vloge:
 - morajo biti za opravljanje teh vlog imenovani s strani upravnega odbora overitelja na MJU,
 - ne smejo opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog pri overitelju na MJU,
 - ne smejo biti na prejšnjih podobnih dolžnostih (npr. skrbnik kriptografskih naprav, varnostni inženir) razrešeni nalog zaradi malomarnosti ali neizpolnjevanja obveznosti in
 - morajo imeti dovoljenje za dostop do tajnih podatkov najmanj stopnje ZAUPNO.

5.3.2 Preverjanje primernosti osebja

- (1) Preverjanje primernosti zaposlenih pri overitelju na MJU se pred sklenitvijo delovnega razmerja izvede s strani kadrovske službe Ministrstva za javno upravo skladno z veljavno zakonodajo, ki velja za javne uslužbenke.
- (2) Preverjanje primernosti zaposlenih pri overitelju na MJU, ki opravljajo zaupanja vredne vloge, se ob pridobitvi dovoljenja za dostop do tajnih podatkov izvaja s strani organa, pristojnega po Zakonu o tajnih podatkih (ZTP, Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10 in 60/11).

5.3.3 Izobraževanje osebja

Osebam, ki opravljajo naloge zgoraj navedenih organizacijskih skupin in naloge prijavnih služb, se zagotavlja vsa potrebna izobraževanja.

5.3.4 Zahteve za redna usposabljanja

Osebe se usposablja glede na potrebe oz. novosti v zvezi z delovanjem infrastrukture izdajatelja SIGEN-CA.

5.3.5 Menjava nalog

Ni predpisana.

5.3.6 Sankcije

Sankcije v primeru nepooblaščenega ali malomarnega izvajanja nalog se za pooblaščen osebe overitelja na MJU izvajajo skladno z veljavno zakonodajo, ki velja za javne uslužbenke in drugo veljavno zakonodajo.

5.3.7 Zahteve za zunanje izvajalce

Za morebitne zunanje izvajalce veljajo enake zahteve kot za pooblaščen osebe overitelja na MJU.

5.3.8 Dostop osebja do dokumentacije

Pooblaščenim osebam overitelja na MJU je na voljo vsa potrebna dokumentacija skladno z njihovimi zadolžitvami in nalogami.

5.4. Varnostni pregledi sistema

(1) Izdajatelj SIGEN-CA ima skladno z veljavno zakonodajo vzpostavljen stalen nadzor delovanja svoje infrastrukture, v okviru katerega se preverja:

- fizična varnost informacijsko-komunikacijske infrastrukture,
- nemoteno delovanje vseh varnostnih sistemov,
- nemoteno delovanje vseh informacijsko-komunikacijskih sistemov in
- ali je v vmesnem času prišlo do vdora ali poskusa vdora nepooblaščenih oseb do opreme ali podatkov.

(2) Podrobni podatki o tem so skladno z veljavno zakonodajo določeni v Interni politiki overitelja na MJU.

5.4.1 Vrste dnevnikov

(1) Izdajatelj SIGEN-CA skladno z veljavno zakonodajo beleži naslednje vrste dogodkov:

- dogodke na operacijskem sistemu, programski in strojni opremi izdajatelja,
- dogodke na operacijskih sistemih, programski in strojni opremi elementov komunikacijskega sistema,
- dogodke v zvezi s ključi izdajatelja,
- dogodke v zvezi z ključi in digitalnimi potrdili imetnikov (izdaja, prevzem, preklic),
- dogodke v zvezi z varnostno politiko in upravljanjem informacijskega sistema izdajatelja,
- dogodke v zvezi z varnostno politiko in upravljanjem komunikacijskega sistema.

(2) Izdajatelj SIGEN-CA zbira in beleži v elektronski ali pisni obliki tudi podatke, ki vplivajo na varnost, niso pa del informacijsko-komunikacijskega sistema izdajatelja:



- dogodke v zvezi s fizičnim dostopom do sistemov izdajatelja ter fizično lokacijo,
- kadrovske spremembe osebja overitelja na MJU,
- dogodke, povezane z uničevanjem občutljivega materiala (na primer kriptografskega materiala oziroma ključev in nosilcev ključev, aktivacijskih podatkov, osebnih podatkov o imetnikih).

(3) Dnevniki beleženih dogodkov v pisni obliki ali elektronski obliki se hranijo v varovanih prostorih overitelja na MJU.

5.4.2 Pogostost pregledov dnevnikov beleženih dogodkov

(1) Izdajatelj SIGEN-CA opravlja redne varnostne preglede svoje infrastrukture, pri čemer uporablja nadzorne in alarmne sisteme za sprotno obveščanje o dogodkih.

(2) Osebje overitelja na MJU pregleduje dnevnik beleženih dogodkov ob vsakem prejetem opozorilu iz nadzornih sistemov. Pregled vključuje:

- preverjanje integritete dnevnikov,
- pregled zapisov v dnevniku ter
- analizo in poročanje o relevantnih dogodkih - razreševanje problemov.

5.4.3 Čas hrambe dnevnikov beleženih dogodkov

(1) Dnevnik beleženih dogodkov v zvezi s ključi in digitalnimi potrdili se hranijo vsaj sedem (7) let po poteku potrdila, na katerega se dnevniški zapis nanaša.

(2) Ostali dnevnik beleženih dogodkov se hranijo vsaj sedem (7) let po nastanku dogodka.

(3) Dnevnik beleženih dogodkov iz prejšnjega odstavka, ki vsebujejo osebne podatke, se hranijo v skladu z veljavno zakonodajo.

5.4.4 Zaščita dnevnikov beleženih dogodkov

(1) Dnevnik so varovani v skladu z varnostnimi mehanizmi, ki zagotavljajo najvišji nivo varnosti.

(2) Podrobnosti so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.4.5 Varnostne kopije dnevnikov beleženih dogodkov

(1) Varnostne kopije dnevnikov se izvajajo dnevno v okviru rednega varnostnega kopiranja sistemov.

(2) Podrobnosti so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.4.6 Zbiranje podatkov za dnevnik beleženih dogodkov

(1) Podatki se zbirajo bodisi avtomatsko ali pa ročno, odvisno od vrste podatkov.

(2) Podrobnosti so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.4.7 Obveščanje povzročitelja dogodka

Povzročitelja dogodkov ni potrebno obveščati.

5.4.8 Ocena ranljivosti sistema

(1) Analizo dnevnikov in nadzor nad izvajanjem vseh postopkov redno izvajajo pooblaščen osebe overitelja na MJU ali pa se to izvaja avtomatsko z drugimi varnostnimi mehanizmi na vseh računalniško-komunikacijskih napravah v pristojnosti overitelja na MJU.

(2) Ocena ranljivosti se izvaja na podlagi analize dnevnikov in ugotovitev nadzora nad izvajanjem postopkov.

(3) Podrobnosti so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.5. Arhiviranje podatkov

5.5.1 Vrste arhiviranih podatkov

Izdajatelj SIGEN-CA skladno z veljavno zakonodajo hrani naslednje podatke oz. dokumente:

- dnevnike,
- zapisnike,
- vsa dokazila o opravljenem preverjanju istovetnosti imetnikov,
- sklenjene medsebojne dogovore oz. pogodbe,
- vse zahteve,
- izdana potrdila in register preklicanih potrdil,
- politike delovanja,
- objave in obvestila izdajatelja SIGEN-CA,
- zasebne ključe za dešifriranje v skladu z podpogl. 6.1.1 ter
- druge dokumente v skladu z veljavnimi predpisi.

5.5.2 Čas hrambe

(1) Arhivirani podatki v zvezi s ključi in digitalnimi potrdili se hranijo vsaj sedem (7) let po poteku potrdila, na katerega se podatek nanaša.

(2) Ostali arhivirani podatki se hranijo vsaj sedem (7) let po njihovem nastanku.

(3) Arhivirani podatki iz prejšnjega odstavka, ki vsebujejo osebne podatke, se hranijo v skladu z veljavno zakonodajo.

5.5.3 Zaščita arhiviranih podatkov

(1) Arhivirani podatki, ki sodijo v dokumentarno gradivo (zahtevki imetnikov, dogovori in pogodbe ter dnevniki beleženih dogodkov v pisni obliki), se hranijo in arhivirajo v skladu s postopki dela z dokumentarnim gradivom na MJU.

(2) Arhivirani podatki, ki se beležijo v okviru informacijskega sistema (avtomatsko generirani dnevnik beleženih



dogodkov, digitalna potrdila, registri preklicanih potrdil ter zasebni dešifrirni ključi), se nahajajo na vsaj dveh kopijah na ločenih lokacijah.

(3) V skladu z veljavno zakonodajo je podrobno to določeno v Interni politiki overitelja na MJU.

5.5.4 Varnostno kopiranje arhiviranih podatkov

(1) Za podatke, ki sodijo v dokumentarno gradivo (zahtevki imetnikov, dogovori in pogodbe ter dnevnik beleženih dogodkov v pisni obliki), se zagotavlja razpoložljivost v skladu s postopki dela z dokumentarnim gradivom na MJU.

(2) Ob izdelavi arhiva podatkov, ki se beležijo v okviru informacijskega sistema (avtomatsko generirani dnevnik beleženih dogodkov, digitalna potrdila, registri preklicanih potrdil ter zasebni dešifrirni ključi), se izdelava varnostna kopija. Kopija arhiviranih podatkov se varno hrani na dveh fizičnih lokacijah.

(3) Podrobnosti o tem so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.5.5 Zahteva po časovnem žigosanju

Ni predpisana.

5.5.6 Način zbiranja arhiviranih podatkov

(1) Podatki se zbirajo na način, skladen z vrsto dokumenta.

(2) V skladu z veljavno zakonodajo je to podrobno določeno v Interni politiki overitelja na MJU.

5.5.7 Postopek za dostop do arhiviranih podatkov in njihova verifikacija

(1) Dostop do arhiviranih podatkov je dovoljen:

- upravnemu odboru overitelja na MJU,
- pooblaščenim osebam overitelja na MJU in
- za potrebe izvajanja inšpekcijskega nadzora.

(2) V skladu z veljavno zakonodajo je to podrobno določeno v Interni politiki overitelja na MJU.

5.6. Obnova izdajateljevega potrdila

V primeru obnove potrdila izdajatelja SIGEN-CA se postopek objavi na spletnih straneh SIGEN-CA.

5.7. Okrevalni načrt

5.7.1 Postopek v primeru vdorov in zlorabe

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

5.7.2 Postopek v primeru okvare strojne in programske opreme ali podatkov

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

5.7.3 Postopek v primeru ogroženega zasebnega ključa izdajatelja

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

5.7.4 Okrevalni načrt

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

5.8. Prenehanje delovanja izdajatelja

Če bo overitelj na MJU prenehal z opravljanjem svoje dejavnosti ali izdajatelj SIGEN-CA prenehal z izdajanjem potrdil, bo overitelj na MJU ukrepal skladno z veljavno zakonodajo.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitvev ključev

6.1.1 Generiranje ključev

(1) Generiranje para ključev izdajatelja SIGEN-CA za podpisovanje in overjanje je formalen in kontroliran postopek ob namestitvi programske opreme SIGEN-CA, o katerem se vodi poseben zapisnik (dokument »Zapisnik postopka generiranja ključev izdajatelja SIGEN-CA-2«). Zapisnik postopka zagotavlja celovitost in revizijsko sled izvedbe postopka, zato se izvaja po natančno pripravljenih navodilih.

(2) Zapisnik postopka se varno shrani.

(3) Morebitne kasnejše spremembe v avtorizacijah ali pomembne spremembe nastavitve informacijskega sistema SIGEN-CA, ki so opravljene ob vzpostavitvi sistema, se dokumentirajo v posebnem zapisniku oz. v ustreznem dnevniku.

(4) Za generiranje para ključev izdajatelja SIGEN-CA se uporabi strojni varnostni modul (glej podpogl. 6.2.1).

(5) Ključi imetnikov se generirajo pri imetniku.

6.1.2 Dostava zasebnega ključa imetnikom

Zasebni ključ se generira pri imetniku in se ne prenaša.

6.1.3 Dostava javnega ključa izdajatelju potrdil⁷

V postopku prevzema potrdila imetniki svoj javni ključ dostavijo v podpis izdajatelju SIGEN-CA po protokolu PKCS#7.

6.1.4 Dostava izdajateljevega javnega ključa tretjim osebam

(1) Potrdilo z javnim ključem izdajatelja SIGEN-CA je objavljeno v repozitoriju overitelja na MJU (glej podpogl. 2.1).

(2) Potrdilo z javnim ključem izdajatelja SIGEN-CA je imetniku dostavljeno oz. tretjim osebam dostopno:

- v javnem imeniku x500.gov.si po protokolu LDAP (glej podpogl. 2.3),
- preko spletne strani <https://www.sigen-ca.si/cda-cgi/clientcgi?action=caCert> (samo potrdilo št. 2),
- v obliki PEM na naslovu <https://www.sigen-ca.si/sigen-ca.pem> oz <https://www.sigen-ca.si/sigen-ca-g2.pem>,
- v obliki PEM na naslovu <http://www.sigen-ca.si/sigen-ca.pem> oz <http://www.sigen-ca.si/sigen-ca-g2.pem>, pri čemer mora dodatno preveriti verodostojnost potrdila,
- preko protokola PKCS#7.

6.1.5 Dolžina ključev

Potrdilo	Dolžina ključa po RSA [bit]
potrdilo izdajatelja SIGEN-CA	3072
potrdilo za imetnike	2048 ⁸
potrdilo za sistem OCSP	2048

6.1.6 Generiranje in kakovost parametrov javnih ključev

Kvaliteta parametrov ključa izdajatelja SIGEN-CA je zagotovljena s strani proizvajalca strojne opreme za varno shranjevanje zasebnih ključev, ki uporablja generator naključnih števil (angl. *random number generator*) v skladu s standardom FIPS 140-2 Level 3.

6.1.7 Namen ključev in potrdil

(1) Namen uporabe ključev oz. potrdil je v skladu z X.509 v.3 določen v potrdilu v polju *uporaba ključa* (angl. *keyUsage*) in *razširjena uporaba ključa* (angl. *extended keyUsage*)⁹.

(2) Za podpis potrdil in registra preklicanih potrdil je namenjen zasebni ključ izdajatelja SIGEN-CA, za overjanje pa javni ključ v izdajateljevem potrdilu.

(3) Profil potrdil je podan v podpogl. 7.1.

6.2. Zaščita zasebnega ključa in varnostni moduli

⁷ RFC 3647 ne predvideva opisa načina dostave potrdil imetnikom.

⁸ Vrednost pomeni minimalno predpisano dolžino.

⁹ Za potrdila SIGEN-CA se to polje ne uporablja.

6.2.1 Standardi za kriptografski modul

Zasebni ključ izdajatelja SIGEN-CA se generira, uporablja in hrani na strojni opremi za varno shranjevanje zasebnih ključev (strojni varnostni modul, HSM angl. *Hardware Security Module*), ki izpolnjuje zahteve v skladu s standardom FIPS 140-2 Level 3.

6.2.2 Nadzor zasebnega ključa s strani pooblaščenih oseb

Določila glede dostopa do zasebnega ključa izdajatelja SIGEN-CA so v skladu z veljavno zakonodajo določena v Interni politiki overitelja na MJU.

6.2.3 Odkrivanje kopije zasebnega ključa

Ni predpisano.

6.2.4 Varnostna kopija zasebnega ključa

Izdajatelj SIGEN-CA zagotavlja varnostno kopijo svojega zasebnega ključa. Podrobnosti so določene v Interni politiki overitelja na MJU.

6.2.5 Arhiviranje zasebnega ključa

Ni predpisano.

6.2.6 Prenos zasebnega ključa iz/v kriptografski modul

(1) Prenos zasebnega ključa izdajatelja SIGEN-CA iz strojnega varnostnega modula se izvede v šifrirani obliki po generiranju para ključev izdajatelja SIGEN-CA z namenom izdelave varnostne kopije zasebnega ključa (glej podpogl. 6.2.4). Prenos zasebnega ključa v strojni varnostni modul se izvede v šifrirani obliki v primeru zamenjave ali ponastavitve varnostnega modula.

(2) Prenos zasebnega ključa iz oziroma v kriptografski modul se izvede z odobritvijo vsaj dveh pooblaščenih oseb overitelja na MJU.

(3) Podrobnosti o prenosu izdajateljevega zasebnega ključa so določene v Interni politiki overitelja na MJU.

(4) Zasebni ključ imetnika se generira pri imetniku s programsko ali strojno opremo, ki je v pristojnosti imetnika.

6.2.7 Zapis zasebnega ključa v kriptografskem modulu

(1) Zasebni ključ je v strojnem varnostnem modulu varovan z mehanizmi v skladu s standardom FIPS 140-2 Level 3.

(2) Imetniki imajo dostop do svojega zasebnega ključa z geslom z ustreznimi aplikacijami.

6.2.8 Postopek za aktiviranje zasebnega ključa

(1) Aktiviranje zasebnega ključa izdajatelja SIGEN-CA se izvede ob zagonu programske opreme izdajatelja in poteka v skladu z določili Interne politike overitelja na MJU.

(2) Imetniki morajo uporabljati tako programsko okolje, ki za aktiviranje njihovega zasebnega ključa zahteva vnos ustreznega gesla.

6.2.9 Postopek za deaktiviranje zasebnega ključa

(1) Ob zaustavitvi delovanja izdajatelja SIGEN-CA programska oprema SIGEN-CA deaktivira zasebni ključ SIGEN-CA.

(2) Imetniki morajo uporabljati tako programsko okolje, ki ob odjavi ali po določenem pretečenem času onemogoči dostop do njihovega zasebnega ključa brez vnosa ustreznega gesla.

6.2.10 Postopek za uničenje zasebnega ključa

(1) Postopek za uničenje zasebnega ključa izdajatelja SIGEN-CA poteka na varen način skladno z določili Interne politike overitelja na MJU. Zasebni ključ se uniči tako, da ga ni mogoče restavrirati.

(2) Uničenje zasebnih ključev na strani imetnikov je v pristojnosti imetnikov. Uporabiti morajo ustrezne aplikacije za varno brisanje potrdil.

6.2.11 Lastnosti kriptografskega modula

Strojni varnostni modul ustreza standardom, podanim v podpogl. 6.2.1.

6.3. Ostali vidiki upravljanja ključev

6.3.1 Arhiviranje javnega ključa

Izdajatelj SIGEN-CA arhivira svoj javni ključ in javne ključne imetnikov, kot je podano v podpogl. 5.5.

6.3.2 Obdobje veljavnosti potrdila in ključev

(1) Veljavnost potrdil in ključev je podana po spodnji tabeli.

Tip potrdila	Par ključev	Ključ	Veljavnost
spletno potrdilo	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	5 let
		javni ključ	5 let

(2) Veljavnost ključev potrdila za sistem OCSP je tri (3) leta.

6.4. Gesla za dostop do zasebnega ključa

6.4.1 Generiranje gesel

- (1) Pooblaščenec osebe izdajatelja za dostop do zasebnega ključa SIGEN-CA uporabljajo močna gesla, s katerimi ravnajo v skladu z Interno politiko overitelja na MJU.
- (2) Aktivacijska podatka, t.j. referenčna številka in avtorizacijska koda, ki sta potrebna za prevzem potrdila, se ustvarita na strani SIGEN-CA. Podatka sta unikatna.
- (3) Imetniki sami določijo geslo, s katerim zaščitijo dostop do svojih zasebnih ključev.
- (4) SIGEN-CA priporoča uporabo varnih gesel:
 - mešano uporaba velikih in malih črk, števil in posebnih znakov,
 - dolžine vsaj 8 znakov,
 - odsvetuje se uporabo besed, ki so zapisane v slovarjih.

6.4.2 Zaščita gesel

- (1) Gesla pooblaščenih oseb izdajatelja SIGEN-CA za dostop do zasebnega ključa izdajatelja SIGEN-CA se shranijo v skladu z Interno politiko overitelja na MJU.
- (2) Aktivacijska podatka za prevzem potrdila se kreirata varno pri izdajatelju SIGEN-CA.
- (3) SIGEN-CA posreduje bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo po dveh ločenih poteh:
 - referenčno številko po elektronski pošti,
 - avtorizacijsko kodo s pošto pošiljko,
 - izjemoma pa ju preda tudi osebno.
- (4) Do prevzema potrdila mora bodoči imetnik skrbno varovati aktivacijska podatka za prevzem potrdila, po prevzemu potrdila postaneta neuporabna in ju imetnik lahko zavrže.
- (5) SIGEN-CA priporoča, da se geslo za dostop do zasebnega ključa ne shranjuje oz. se shrani na varno mesto in da ima do njega dostop le imetnik.
- (6) SIGEN-CA imetnikom priporoča, da sami poskrbijo za zamenjavo gesla vsaj vsakih šest (6) mesecev.

6.4.3 Drugi vidiki gesel

Niso predpisani.

6.5. Varnostne zahteve za računalniško opremo izdajatelja

6.5.1 Specifične tehnične varnostne zahteve

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

6.5.2 Nivo varnostne zaščite

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1 Nadzor razvoja sistema

(1) Izdajatelj SIGEN-CA uporablja programsko opremo proizvajalca Entrust, ki je certificirana v skladu s Common Criteria EAL4+.

(2) Podrobne tehnične zahteve so določene v Interni politiki overitelja na MJU.

6.6.2 Upravljanje varnosti

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

6.6.3 Nadzor življenjskega cikla

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

6.7. Varnostna kontrola računalniške mreže

(1) Omogočeni so le mrežni protokoli, ki so nujno potrebni za delovanje sistema.

(2) V skladu z veljavno zakonodajo je to podrobneje določeno v Interni politiki overitelja na MJU.

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL POTRDIL, REGISTRA PREKLICANIH POTRDIL IN SPROTNEGA PREVERJANJA STATUSA POTRDIL

7.1. Profil potrdil

(1) Na podlagi pričujoče politike SIGEN-CA izdaja spletna potrdila za fizične osebe.

(2) Vsa potrdila vključujejo podatke, ki so skladno z veljavno zakonodajo določeni za kvalificirana potrdila.

(3) Potrdila izdajatelja SIGEN-CA sledijo standardu X.509.



7.1.1 Različica potrdil

Vsa potrdila izdajatelja SIGEN-CA sledijo standardu X.509, in sicer različici 3, skladno z RFC 5280.

7.1.2 Profil potrdil z razširitvami

7.1.2.1 Profil potrdila SIGEN-CA

Profil potrdila SIGEN-CA je predstavljen v podpogl. 1.3.1.

7.1.2.2 Profil potrdil za imetnike

(1) Podatki v potrdilu so navedeni spodaj.

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. <i>Version</i>	3
Identifikacijska oznaka, angl. <i>Serial Number</i>	enolična interna številka potrdila-celo število
Algoritem za podpis, angl. <i>Signature algorithm</i>	sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. <i>Issuer</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Veljavnost, angl. <i>Validity</i>	Not Before: <pričetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT> v formatu <i>UTCTime</i> <LLMMDDuumssZ>
Imetnik, angl. <i>Subject</i>	razločevalno ime imetnika, ki vključuje ime imetnika in serijsko številko (glej podpogl. 3.1.1), v obliki, primerni za izpis
Algoritem za javni ključ, angl. <i>Subject Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. <i>RSA Public Key</i>	dolžina ključa je min 2048 bitov, glej podpogl. 6.1.5
Razširitve X.509v3	
Alternativno ime OID 2.5.29.17, angl. <i>Subject Alternative Name</i>	elektronski naslov imetnika, glej podpogl. 7.1.2.3



Objava registra preklicanih potrdil, OID 2.5.29.31, angl. <i>CRL Distribution Points</i>	Url: http://www.sigen-ca.si/crl/sigen-ca-g2.crl Url: ldap://x500.gov.si/cn=SIGEN-CA G2,oi=VATSI-17659957,o=Republika Slovenija,c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2, cn=CRL< <i>zaporedna številka registra, glej podpogl. 7.2.2</i> >
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. <i>Authority Information Access</i>	Access Method=OCSP http://ocsp.sigen-ca.si
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Digital Signature, Key Encipherment, ContentCommitment
Razširjena uporaba ključa, OID 2.5.29.37, angl. <i>Extended Key Usage</i>	<i>se ne uporablja</i>
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	4C25 278C A82D 729E
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	<i>identifikator imetnikovega ključa</i>
Politike, pod katerimi je bilo izdano potrdilo, OID 2.5.29.32, angl. <i>certificatePolicies</i>	Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6105.2.2.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/ PolicyIdentifier=0.4.0.1456.1.2
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. <i>qcStatement</i>	QcCompliance statement
Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	CA: FALSE Brez omejitev dolžine (Path Length Constraint: none)
Odtis potrdila (ni del potrdila)	
Odtis potrdila-SHA-1 angl. <i>Certificate Fingerprint – SHA-1</i>	<i>razpoznavni odtis potrdila po SHA-1</i>
Odtis potrdila-SHA-256 angl. <i>Certificate Fingerprint – SHA-256</i>	<i>razpoznavni odtis potrdila po SHA-256</i>

(2) Polje *uporaba ključa* (angl. *Key Usage*) je označeno kot kritično (angl. *critical*).

(3) Imetnik ima lahko eno samo veljavno istovrstno potrdilo, razen v času šestdeset (60) dni pred potekom veljavnosti tega potrdila, ko lahko imetnik pridobi novo potrdilo.

7.1.2.3 Zahteve za elektronski naslov

(1) Elektronski naslov mora izpolnjevati naslednje zahteve:

- mora biti veljaven in
- mora biti pomensko povezan z imetnikom.

(2) SIGEN-CA si pridržuje pravico za zavrnitev zahtevka za pridobitev potrdila, če ugotovi, da je elektronski naslov:

- neprimeren oz. žaljiv,
- da je zavajajoč za tretje stranke,
- predstavlja neko drugo pravno ali fizično osebo,
- je v nasprotju z veljavnimi predpisi in standardi.

7.1.3 Identifikacijske oznake algoritmov

(1) Potrdila, ki jih izdaja SIGEN-CA, so s strani izdajatelja podpisana z algoritmom, določenim v polju *signature algorithm*: vrednost »sha256WithRSAEncryption«, identifikacijska oznaka: OID 1.2.840.113549.1.1.11.

(2) Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri pooblaščenih osebah izdajatelja SIGEN-CA.

7.1.4 Oblika imen

Glej podpogl. 3.1.1.

7.1.5 Omejitve glede imen

Omejitve glede imen (polje v potrdilu angl. *nameConstraints*) niso predpisane.

7.1.6 Oznaka politike potrdila

Glej podpogl. 7.1.2.

7.1.7 Uporaba razširitvenega polja za omejitve uporabe politik

Omejitve uporabe politik (angl. *Policy constraints*) se ne uporabljajo.

7.1.8 Oblika in obravnava specifičnih podatkov o politiki

V potrdilih, ki jih izdaja izdajatelj SIGEN-CA, se uporablja specifični podatek *policyQualifiers*, ki se obravnava v skladu z RFC 5280.

7.1.9 Obravnava kritičnega razširitvenega polja politike

Razširitveno polje politika (angl. *CertificatePolicies*) ni označeno kot kritično.

7.2. Profil registra preklicanih potrdil

7.2.1 Različica

- (1) Register preklicanih potrdil ustreza priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, vključno z ver. 2.
- (2) Register preklicanih potrdil je stalno dostopen v repozitoriju (glej podpogl. 2.1):
- po protokolu LDAP in
 - po protokolu HTTP.

7.2.2 Vsebina registra in razširitve

- (1) Register preklicanih potrdil poleg ostalih podatkov v skladu s priporočilom X.509 vsebuje (osnovna polja in razširitve so podrobneje prikazana v tabeli spodaj):
- identifikacijske oznake preklicanih potrdil in
 - čas in datum preklica.

Naziv polja	Vrednost oz. pomen
Osnovna polja v CRL	
Različica, angl. <i>Version</i>	2
Izdajatelj podpis, angl. <i>Signature</i>	<i>podpis SIGEN-CA</i>
Razločevalno ime izdajatelja, angl. <i>Issuer</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Čas izdaje CRL, angl. <i>thisUpdate</i>	Last Update: <čas izdaje po GMT>
Čas izdaje naslednjega CRL, angl. <i>nextUpdate</i>	Next Update: <čas naslednje izdaje po GMT>
Identifikacijske oznake preklicanih potrdil in čas preklica, angl. <i>revokedCertificate</i>	Serial Number: <identifikacijska oznaka preklicanega dig. potrdila> Revocation Date: <čas preklica po GMT>
Algoritem za podpis, angl. <i>Signature Algorithm</i>	sha256WithRSAEncryption
Razširitve X.509v2 CRL	
Identifikator izdajateljevega ključa, angl. <i>Authority Key Identifier</i> (OID 2.5.29.35)	<i>identifikator izdajateljevega ključa</i>
Številka za posamične registre (CRL1, CRL2,...), angl. <i>CRLnumber</i> (OID 2.5.29.20)	<i>zaporedna številka posamičnega registra</i>
Alternativno ime izdajatelja angl. <i>issuerAltName</i> (OID 2.5.28.18)	<i>se ne uporablja</i>
Oznaka seznama sprememb angl. <i>deltaCRLindicator</i> (OID 2.5.29.27)	<i>se ne uporablja</i>
Objava seznama sprememb angl. <i>issuingDistributionPoint</i> (OID 2.5.29.28)	<i>se ne uporablja</i>

- (2) Preklicana digitalna potrdila, katerih veljavnost je potekla, ostanejo objavljena v posamičnem registru, v celotnem registru pa so objavljena le do poteka veljavnosti.



(3) Polja v CRL niso označena kot kritična.

(4) Register preklicanih digitalnih potrdil je javno objavljen v repozitoriju (glej podpogl. 2.1).

(5) Izdajatelj objavlja tako posamične registre kot tudi celotni register na enem mestu. Dostop po protokolih LDAP in HTTP ter objavo prikazuje spodnja tabela.

	Objava CRL	Dostop do CRL
<i>posamični registri</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2, cn=CRL<zaporedna številka registra>	- ldap://x500.gov.si/cn=CRL<zaporedna številka registra>, cn=SIGEN-CA G2,oi=VATSI-17659957,o=Republika Slovenija,c=SI
<i>celotni register</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2 (v polju "CertificationRevocationList")	- http://www.sigen-ca.si/crl/sigen-ca-g2.crl - ldap://x500.gov.si/cn=SIGEN-CA G2,oi=VATSI-17659957,o=Republika Slovenija,c=SI?certificateRevocationList

7.3. Profil sprotnega preverjanja statusa potrdil

(1) Sprotno preverjanje statusa digitalnih potrdil je dostopno na naslovu <http://ocsp.sigen-ca.si>.

(2) Profil sporočil OCSP (zahtevek/odgovor) storitve za sprotno preverjanje statusa potrdil je v skladu s priporočilom RFC 2560.

7.3.1 Različica

Izdajatelj SIGEN-CA uporablja sporočila OCSP verzije 1 v skladu s priporočilom RFC 2560.

7.3.2 Razširitve sprotnega preverjanje statusa

Sporočila OCSP (zahtevek/odgovor) storitve za sprotno preverjanje statusa potrdil podpirajo razširitev Nonce, ki ni označena kot kritična.

8. INŠPEKCIJSKI NADZOR

8.1. Pogostnost inšpekcijskega nadzora

Pogostnost inšpekcijskega nadzora je v pristojnosti inšpekcijske službe, ki je pristojna v skladu z veljavno zakonodajo.

8.2. Inšpekcijska služba

(1) Izvajanje določb ZEPEP overitelja na MJU skladno z ZEPEP opravlja pristojna inšpekcijska služba v skladu z veljavno zakonodajo za inšpekcijski nadzor.



(2) Notranje preverjanje skladnosti delovanja izvaja notranji revizor in ostale pooblaščne osebe v okviru overitelja na MJU.

8.3. Neodvisnost inšpekcijske službe

Inšpekcijska služba je organ, pristojen v skladu z veljavno zakonodajo.

8.4. Področja inšpekcijskega nadzora

Področja nadzora so določena z veljavno zakonodajo in predpisi.

8.5. Ukrepi overitelja

V primeru ugotovljenih pomanjkljivosti ali napak si izdajatelj SIGEN-CA oz. overitelj na MJU prizadeva za odpravo le-teh v najkrajšem možnem času.

8.6. Objava rezultatov inšpekcijskega nadzora

Overitelj na MJU javno objavi povzetek sklepov inšpekcijskega nadzora na svojih spletnih straneh.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik storitev

9.1.1 Cena izdaje in obnove potrdil

Stroški upravljanja s potrdili se obračunavajo po objavljenem ceniku na spletni strani <http://www.sigen-ca.si/cenik.php>.

9.1.2 Cena dostopa do potrdil

Dostop do imenika izdanih potrdil izdajatelja SIGEN-CA je brezplačen.

9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil

Dostop do statusa potrdila in registra preklicanih potrdil izdajatelja SIGEN-CA je brezplačen.

9.1.4 Cene drugih storitev



Stroške potrebne strojne ali programske opreme, ki jo zahteva oz. priporoča SIGEN-CA za varno shranjevanje in uporabo potrdil, krije imetnik potrdila.

9.1.5 Povrnitev stroškov

Ni predpisana.

9.2. Finančna odgovornost

9.2.1 Zavarovalniško kritje

Ministrstvo za javno upravo ima glede delovanja overitelja na MJU ustrezno zavarovano svojo odgovornost v skladu z veljavno zakonodajo.

9.2.2 Drugo kritje

Ni predpisano.

9.2.3 Zavarovanje imetnikov

Ni predpisano.

9.3. Varovanje poslovnih podatkov

9.3.1 Varovani podatki

(1) Izdajatelj SIGEN-CA kot zaupne obravnava naslednje podatke:

- vse zahtevke za pridobitev potrdila ali druge storitve
- vse morebitne zaupne podatke v zvezi s finančnimi obveznostmi,
- vse morebitne zaupne podatke, ki so predmet medsebojne pogodbe s tretjimi osebami ter
- vse ostale zadeve, ki so v skladu z veljavno zakonodajo zavedene v Interni politiki overitelja na MJU.

(2) Z vsemi morebitnimi zaupnimi podatki o imetnikih in tretjih osebah, ki so nujno potrebni za storitve upravljanja s potrdili, izdajatelj SIGEN-CA ravna v skladu z veljavno zakonodajo.

9.3.2 Nevarovani podatki

Izdajatelj SIGEN-CA javno objavlja samo take poslovne podatke, ki v skladu z veljavno zakonodajo niso zaupne narave.

9.3.3 Odgovornost glede varovanja poslovnih podatkov

Izdajatelj SIGEN-CA posreduje le tiste podatke, ki so navedeni v potrdilu. Drugi podatki se lahko posredujejo le v primeru, če se posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s potrdili. Podatki se



posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

9.4. Varovanje osebnih podatkov

9.4.1 Načrt varovanja osebnih podatkov

Z vsemi osebnimi in zaupnimi podatki o imetnikih potrdil, ki so nujno potrebni za storitve upravljanja s potrdili, izdajatelj SIGEN-CA ravna v skladu z veljavno zakonodajo.

9.4.2 Varovani osebni podatki

Varovani podatki so vsi osebni podatki, ki jih izdajatelj SIGEN-CA pridobi na zahtevkih za svoje storitve ali v ustreznih registrih za dokazovanje istovetnosti imetnika.

9.4.3 Nevarovani osebni podatki

Drugih morebitnih nevarovanih osebnih podatkov, razen teh, ki so navedeni v potrdilu in registru preklicanih potrdil, ni.

9.4.4 Odgovornost glede varovanja osebnih podatkov

Overitelj na MJU je odgovoren v skladu z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo) in drugo veljavno zakonodajo glede varovanja osebnih podatkov.

9.4.5 Pooblastilo glede uporabe osebnih podatkov

Imetnik pooblasti overitelja na MJU oz. izdajatelja SIGEN-CA za uporabo osebnih podatkov na zahtevku za pridobitev potrdila ali kasneje v pisni obliki.

9.4.6 Posredovanje osebnih podatkov na uradno zahtevo

(1) Overitelj na MJU ne posreduje podatkov o imetnikih potrdil, ki niso navedeni v potrdilu, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s potrdili, ter je overitelja na MJU imetnik pooblastil za to (glej prejšnje podpoglavje), ali na zahtevo pristojnega sodišča ali upravnega organa.

(2) Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

9.4.7 Druga določila glede posredovanja osebnih podatkov

Niso predpisana.

9.5. Določbe glede pravic intelektualne lastnine

Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine v zvezi s izdajateljem SIGEN-CA::

- na pričujoči politiki pripadajo vse pravice overitelju na MJU,
- na javnem imeniku potrdil in registru preklicanih potrdil pripadajo vse pravice overitelju na MJU,
- na vseh podatkih v potrdilih pripadajo vse pravice overitelju na MJU,
- na zasebnem ključu za podpisovanje pripadajo vse pravice imetniku potrdila.

9.6. Obveznosti in odgovornosti

9.6.1 Obveznosti in odgovornosti izdajatelja

(1) Izdajatelj SIGEN-CA oz. overitelj na MJU je dolžan:

- delovati v skladu s svojimi notranjimi pravili in ostalimi veljavnimi predpisi in zakonodajo,
- delovati v skladu z mednarodnimi priporočili,
- objavljati vse pomembne dokumente, ki določajo njegovo delovanje (politike delovanja, zahtevke, cenik, navodila za varno uporabo kvalificiranih digitalnih potrdil ipd.),
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti overitelja na MJU, ki kakorkoli vplivajo na imetnike potrdil in tretje osebe,
- zagotoviti delovanje prijavnih služb v skladu z določili SIGEN-CA in ostalimi veljavnimi predpisi,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi podatki o overitelju, imetnikih potrdil ali tretjimi osebami,
- preklicati potrdilo in objaviti preklicano potrdilo v registru preklicanih potrdil, ko ugotovi, da so podani razlogi po tej politiki ali drugih veljavnih predpisih,
- izdajati kvalificirana digitalna potrdila v skladu s to politiko in ostalimi predpisi ter priporočili.

(2) Izdajatelj SIGEN-CA oz. overitelj na MJU je dolžan:

- zagotoviti pravilnost podatkov izdanih potrdil,
- zagotoviti, da ima imetnik potrdila v času izdaje le-tega zasebni ključ, ki pripada v potrdilu navedenemu javnemu ključu (glej podpogl. 3.2.1),
- zagotoviti pravilnost objave registra preklicanih potrdil,
- zagotoviti pravilnost delovanja sprotnega preverjanja statusa potrdil,
- zagotoviti enoličnost razločevalnih imen,
- zagotoviti primerno fizično varnost prostorov in dostopov do samih prostorov izdajatelja,
- kot dober gospodar skrbeti za nemoteno delovanje in čim večjo razpoložljivost storitve,
- kot dober gospodar skrbeti za čim večjo dostopnost storitev,
- kot dober gospodar skrbeti za nemoteno delovanje vseh ostalih spremljajočih storitev,
- poskušati odpraviti nastale probleme po najboljših močeh in v najkrajšem času,
- skrbeti za optimizacijo strojne in programske opreme in
- obveščati vse ustrezne subjekte o pomembnih zadevah ter
- izpolnjevati vse druge zahteve v skladu s to politiko.

(3) Izdajatelj SIGEN-CA oz. overitelj na MJU zagotavlja čim večjo dostopnost svojih storitev, in sicer 24ur/7dni/365dni, pri čemer pa se ne upošteva naslednjih primerov:

- načrtovanih in vnaprej napovedanih tehničnih ali servisnih posegov na infrastrukturi,
- nenačrtovanih tehničnih ali servisnih posegov na infrastrukturi kot posledica nepredvidenih okvar,
- tehničnih ali servisnih posegov zaradi okvare infrastrukture izven pristojnosti izdajatelja SIGEN-CA oz. overitelja na MJU in
- nedostopnost kot posledico višje sile ali izrednih dogodkov.

(4) Vzdrževalna dela ali nadgradnje infrastrukture mora overitelj na MJU oz. SIGEN-CA najaviti vsaj tri (3) dni pred pričetkom del.

(5) Overitelj na MJU je odgovoren za vse navedbe v tem dokumentu in za izvajanje vseh določil iz te politike.

(6) Ostale obveznosti oz. odgovornosti izdajatelja SIGEN-CA oz. overitelja na MJU so določene v interni politiki overitelja na MJU in morebitnem medsebojnem dogovoru s tretjo osebo.

9.6.2 Obveznost in odgovornost prijavne službe

(1) Prijavna služba je dolžna:

- preverjati istovetnost imetnikov oz. bodočih imetnikov,
- sprejemati zahtevke za storitve SIGEN-CA,
- preverjati zahtevke,
- izdajati potrebno dokumentacijo imetnikom oz. bodočim imetnikom,
- posredovati zahtevke in ostale podatke na varen način na SIGEN-CA.

(2) Prijavna služba je odgovorna za izvajanje vseh določil iz teh politik in drugih zahtev, ki jih dogovorita z overiteljem na MJU.

9.6.3 Obveznosti in odgovornost imetnika

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:

- seznaniti se s to politiko pred izdajo potrdila,
- ravnati v skladu s politiko in ostalimi veljavnimi predpisi,
- če po oddaji zahtevka za pridobitev potrdila oz. drugo storitev od izdajatelja SIGEN-CA ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, se mora obrniti na pooblaščen osebe izdajatelja SIGEN-CA,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SIGEN-CA oziroma zahtevati preklic potrdila,
- v kolikor po oddaji zahtevka za pridobitev potrdila oz. drugo storitev od izdajatelja SIGEN-CA ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, potem se mora obrniti na pooblaščen osebe izdajatelja SIGEN-CA,
- spremljati vsa obvestila SIGEN-CA in ravnati v skladu z njimi,
- v skladu z obvestili ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- vse spremembe, ki so povezane s potrdilom, nemudoma sporočiti SIGEN-CA,
- zahtevati preklic potrdila, če so bili zasebni ključi ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe,
- uporabljati potrdilo za namen, določen v potrdilu (glej podpogl. 7.1), in na način, ki je določen s politiko SIGEN-CA,
- skrbeti za originalno podpisane dokumente in arhiv teh dokumentov.

(2) Imetnik odgovarja za:

- nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,
- vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil SIGEN-CA ter veljavnih predpisov.

(3) Obveznosti imetnika glede uporabe potrdil so določene v podpogl. 4.5.1.

9.6.4 Obveznosti in odgovornost tretjih oseb

(1) Tretje osebe morajo proučiti vse zahteve in okoliščine, preden se odločijo za zanašanje na potrdila, ki jih izda SIGEN-CA.

(2) Tretje osebe, ki se zanašajo na izdana potrdila SIGEN-CA, morajo:

- skrbno proučiti vse možnosti tveganja in odgovornosti pri uporabi potrdil in določiti politiko za način uporabe,
- za overjanje podpisa oz. druge kriptografske operacije uporabljati programsko in strojno opremo, s katero lahko na verodostojen način preverijo vse zahteve za varno uporabo potrdil,
- obvestiti izdajatelja SIGEN-CA, če izvedo, da so bili zasebni ključi imetnika potrdila, na katerega se zanašajo, ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, navedeni v potrdilu,
- skrbeti za arhiv dokumentov,
- upoštevati druge določbe iz morebitnih medsebojnih dogovorov,
- upoštevati vsa navodila oz. priporočila SIGEN-CA glede zanesljive uporabe,
- ob morebitnih napakah ali problemih takoj obvestiti izdajatelja SIGEN-CA,
- seznaniti se s to politiko in upoštevati vsa določila glede njihove obveznosti, odgovornosti ter omejitve glede zaupanja in uporabe potrdil,
- spremljati vsa obvestila in objave izdajatelja SIGEN-CA in ravnati v skladu z le-timi,
- upoštevati morebitna druga pravila, ki so izven pristojnosti izdajatelja in so določena drugje.

(3) Tretje osebe nosijo vse posledice, ki bi nastale zaradi morebitnega neupoštevanja določil te politike, morebitnega dogovora z overiteljem na MJU in veljavne zakonodaje.

9.6.5 Obveznosti in odgovornosti drugih subjektov

Niso predpisane.

9.7. Zanikanje odgovornosti

Overitelj na MJU ni odgovoren za škodo, ki bi nastala zaradi:

- uporabe potrdil za namen in na način, ki ni izrecno predviden v tej politiki,
- nepravilnega ali pomanjkljivega varovanja gesel ali zasebnih ključev imetnikov, izdajanja zaupnih podatkov ali ključev tretjim osebam in neodgovornega ravnanja imetnika,
- zlorabe oz. vdora v informacijski sistem imetnika potrdila in s tem do podatkov o potrdilih s strani nepooblaščenih oseb,
- nedelovanja ali slabega delovanja informacijske infrastrukture imetnika potrdila ali tretjih oseb,
- nepreverjanja podatkov in veljavnosti potrdil,
- nepreverjanja časa veljavnosti potrdila,
- ravnanja imetnika potrdila ali tretje osebe v nasprotju z obvestili izdajatelja SIGEN-CA, politiko in drugimi predpisi,
- omogočene uporabe oz. zlorabe imetnikovega potrdila nepooblaščenim osebam,
- izdanega potrdila z napačnimi podatki in neverdostojnimi podatki ali drugih dejanj imetnika,
- uporabe potrdil ter veljavnosti potrdil ob spremembah podatkov iz potrdila, elektronskih naslovov ali spremembah imen imetnikov,
- izpada infrastrukture, ki ni v domeni upravljanja overitelja na MJU,
- podatkov, ki se šifrirajo ali podpisujejo z uporabo potrdil,
- ravnanja imetnikov pri uporabi potrdil, in sicer tudi v primeru, če je imetnik ali tretja oseba spoštoval vsa določila te politike, obvestila izdajatelja SIGEN-CA ali druge veljavne predpise,

- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

9.8. Omejitev odgovornosti

Izdajatelj SIGEN-CA oz. overitelj na MJU jamči za vrednost posameznega pravnega posla glede na vrsto potrdila do vrednosti do višine 1.000 EUR.

9.9. Poravnava škode

Za škodo odgovarja stranka, ki je le-to povzročila zaradi neupoštevanja določil iz te politike in veljavne zakonodaje in morebitnih medsebojnih dogovorov.

9.10. Veljavnost politike

9.10.1 Čas veljavnosti

Nova verzija oz. spremembe politike overitelja na MJU se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na MJU z označenim datumom začetka njene veljavnosti.

9.10.2 Konec veljavnosti politike

(1) Konec veljavnosti politike ni določen in povezan z veljavnostjo potrdil, izdanih na podlagi politike.

(2) Ob objavi nove politike ostanejo za vsa potrdila, izdana na podlagi te politike, v veljavi tista določila, ki se smiselno ne morejo nadomestiti z ustreznimi določili po novi politiki (na primer postopek, ki določa način, po katerem je bilo to potrdilo izdano ipd.).

(3) Izdajatelj lahko za posamezna določila veljavne politike izda amandmaje, kot je to podano v podpogl. 9.12.

9.10.3 Učinek poteka veljavnosti politike

(1) Ob izdaji nove politike se vsa kvalificirana digitalna potrdila izdana po tem datumu obravnavajo po novi politiki.

(2) Nova politika ne vpliva na veljavnost potrdil, ki so bila izdana po prejšnjih politikah. Taka potrdila ostanejo v veljavi do konca preteka veljavnosti, pri čemer se, kjer je to možno, obravnavajo po novi politiki.

9.11. Komuniciranje med subjekti

(1) Kontaktni podatki overitelja oz. izdajatelja so objavljeni na spletnih straneh in podani v podpogl. 1.3.1.

(2) Kontaktni podatki imetnikov so podani v zahtevkih v zvezi s potrdili.

(3) Kontaktni podatki tretjih oseb so podani v morebitnem medsebojnem dogovoru med tretjo osebo in overiteljem na MJU.

(4) Izdajatelj SIGEN-CA ostale subjekte obvešča preko obvestil, objavljenih na spletnih straneh, ter preko e-pošte.

(5) Izdajatelj SIGEN-CA ter tretja oseba lahko določita način komuniciranja z medsebojnim dogovorom oz. pogodbo.

9.12. Spreminjanje dokumenta

9.12.1 Postopek uveljavitve sprememb

(1) Overitelj na MJU si pridržuje pravico do spremembe tega dokumenta brez predhodnega obveščanja imetnikov potrdil SIGEN-CA, v kolikor spremembe ne vplivajo na namen uporabe in postopke upravljanja, ki lahko spremenijo nivo zaupanja.

(2) Spremembe ali dopolnitve k pričujoči politiki lahko izdajatelj objavi v obliki amandmajev k tej politiki, kadar ne gre za bistvene spremembe v delovanju izdajatelja.

(3) Amandmaji se sprejmejo po enakem postopku kot politika.

(4) Imetniki oz. bodoči imetniki lahko na elektronski naslov izdajatelja SIGEN-CA podajo svoje pripombe glede vsebine politike, ki jih obravnavajo pooblaščen osebe overitelja na MJU. Overitelj na MJU si pridružuje pravico, da pripombe upošteva po lastni presoji.

9.12.2 Veljavnost in objava sprememb

Spremembe politike overitelja na MJU se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na MJU z veljavnimi identifikacijskimi oznakami (CP_{OID}) in označenim datumom začetka njene veljavnosti.

9.12.3 Sprememba identifikacijske oznake politike

Če spremembe vplivajo na namen uporabe ali postopke upravljanja, ki lahko spremenijo nivo zaupanja, se nova verzija politike izdajatelja SIGEN-CA označi z novo identifikacijsko oznako (CP_{OID}).

9.13. Postopek v primeru sporov

Stranke si bodo prizadevale za sporazumno reševanje sporov, če pa to ne bi bilo mogoče, je za reševanje sporov pristojno sodišče v Ljubljani. Stranke za reševanje sporov dogovorijo izključno uporabo predpisov Republike Slovenije.

9.14. Veljavna zakonodaja

Overitelj na MJU in izdajatelj SIGEN-CA delujeta v skladu z:

- ZEPEP,
- Uredbo k ZEPEP,

- Uredbo eIDAS,
- evropskimi direktivami,
- Zakonom o varstvu osebnih podatkov,
- Zakonom o tajnih podatkih,
- priporočili ETSI s področja kvalificiranih potrdil in storitev zaupanja,
- priporočili RFC s področja potrdil X.509,
- in drugimi veljavnimi predpisi in priporočili.

9.15. Skladnost z veljavno zakonodajo

Nadzor nad skladnostjo delovanja overitelja na MJU oz. izdajatelja SIGEN-CA z veljavno zakonodajo in predpisi, določenimi v podpogl. 9.14, izvaja pristojna inšpekcijska služba (glej podpogl. 8.2).

9.16. Splošne določbe

9.16.1 Celovit dogovor

Določbe te politike v ničemer ne spreminjajo, omejujejo ali drugače vplivajo na obveznosti, odgovornosti in poročstva, ki overitelja na MJU zavezujejo na podlagi drugih pogodb ali dogovorov oziroma druge veljavne zakonodaje.

9.16.2 Prenos pravic

Potrdilo, ki ga izdajatelj SIGEN-CA izda imetniku ter morebitne pravice, povezane z uporabo potrdila, so namenjene izključno imetniku in niso prenosljive na tretje osebe.

9.16.3 Neodvisnost določil

Če katerokoli od določil politike ali morebitnega dogovora oz. pogodbe je ali postane neveljavno, to ne vpliva na ostala določila. Neveljavno določilo se nadomesti z veljavnim, ki mora čim bolj ustrezati namenu, ki ga je želelo doseči neveljavno določilo.

9.16.4 Terjatve

Niso določene.

9.16.5 Višja sila

Overitelj na MJU ni odgovoren za škodo, ki bi nastala zaradi višje sile, na katero overitelj nima možnosti vpliva kot so npr. vojne, teroristična dejanja, nemiri, naravne nesreče ipd.

9.17. Ostale določbe



9.17.1 Razumevanje določil

V besedilu politike se uporablja moška samostalniška oblika, ki pa se nanaša na oba spola. Vsi izrazi, zapisani v ednini, se nanašajo tudi na množino in obratno.

9.17.2 Nasprotujoča določila

Če so določila te politike v nasprotju z določili katerekoli pogodbe ali dogovora med overiteljem na MJU in organizacijo ali tretjo osebo, veljajo določila pogodbe ali dogovora.

9.17.3 Odstopanje od določil

Če izdajatelj SIGEN-CA v posameznem primeru izjemoma odstopi od upoštevanja posameznega določila te politike, to ne pomeni, da bi ta izjema veljala tudi v bodoče in v vseh ostalih primerih.

9.17.4 Navzkrižno overjanje

Podrobnosti o navzkrižnem overjanju so podane v podpogl. 3.2.6.