POLITIKA SIGOV-CA

za kvalificirana digitalna potrdila za državne organe

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 11. januarja 2016
verzija: 6.0

CP_{Name}: SIGOV-CA

- **Politika za spletna kvalificirana digitalna potrdila za zaposlene**
  CP_{OID}: 1.3.6.1.4.1.6105.1.1.7
- **Politika za spletna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic**
  CP_{OID}: 1.3.6.1.4.1.6105.1.2.7
- **Politika za posebna kvalificirana digitalna potrdila za zaposlene**
  CP_{OID}: 1.3.6.1.4.1.6105.1.3.7
- **Politika za posebna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic**
  CP_{OID}: 1.3.6.1.4.1.6105.1.4.7
- **Politika za spletna kvalificirana digitalna potrdila za splošne nazive**
  CP_{OID}: 1.3.6.1.4.1.6105.1.5.7
- **Politika za spletna kvalificirana digitalna potrdila za splošne nazive z obvezno uporabo pametnih kartic**
  CP_{OID}: 1.3.6.1.4.1.6105.1.6.7
- **Politika za posebna kvalificirana digitalna potrdila za splošne nazive**
  CP_{OID}: 1.3.6.1.4.1.6105.1.7.7
- **Politika za posebna kvalificirana digitalna potrdila za splošne nazive z obvezno uporabo pametnih kartic**
  CP_{OID}: 1.3.6.1.4.1.6105.1.8.7
- **Politika za spletna kvalificirana digitalna potrdila za strežnike**
  CP_{OID}: 1.3.6.1.4.1.6105.1.9.7
- **Politika za spletna kvalificirana digitalna potrdila za podpis kode**
  CP_{OID}: 1.3.6.1.4.1.6105.1.10.7
- **Politika za kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov**
  CP_{OID}: 1.3.6.1.4.1.6105.1.11.7
- **Politika za kvalificirana digitalna potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil**
  CP_{OID}: 1.3.6.1.4.1.6105.1.12.7

Zgodovine politik

Izdaje politik delovanja SIGOV-CA	
verzija: 6.0, veljavnost**:** od 11. januarja 2016	
• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.1.1.7 • Politika za spletna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.2.7 • Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.1.3.7 • Politika za posebna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.4.7 • Politika za spletna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.5.7 • Politika za spletna kvalificirana digitalna potrdila za splošne nazive z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.6.7 • Politika za posebna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.7.7 • Politika za posebna kvalificirana digitalna potrdila za splošne nazive z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.8.7 • Politika za spletna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.1.9.7 • Politika za spletna kvalificirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.1.10.7 • Politika za kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov, CP_{OID}: 1.3.6.1.4.1.6105.1.11.7 • Politika za kvalificirana digitalna potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil, CP_{OID}: 1.3.6.1.4.1.6105.1.12.7 CP_{Name}: SIGOV-CA	*Spremembe z verzijo 6.0:* • *tvorjeno je bilo drugo lastno digitalno potrdilo izdajatelja SIGOV-CA z zasebnim ključem dolžine 3072 bitov, ki se hrani na strojni opremi za varno shranjevanje zasebnih ključev,* • *v potrdilu izdajatelja SIGOV-CA in vseh potrdilih imetnikov se uporablja zgostitveni algoritem SHA-256,* • *spremenjeno je razločevalno ime digitalnega potrdila izdajatelja SIGOV-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.*
verzija: 5.0, veljavnost**:** od 7. novembra 2015	

• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.1.1.6 • Politika za spletna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.2.6 • Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.1.3.6 • Politika za posebna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.4.6 • Politika za spletna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.5.6 • Politika za spletna kvalificirana digitalna potrdila za splošne nazive z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.6.6 • Politika za posebna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.7.6 • Politika za posebna kvalificirana digitalna potrdila za splošne nazive z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.8.6 • Politika za spletna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.1.9.6 • Politika za spletna kvalificirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.1.10.6 • Politika za kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov, CP_{OID}: 1.3.6.1.4.1.6105.1.11.6 • Politika za kvalificirana digitalna potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil, CP_{OID}: 1.3.6.1.4.1.6105.1.12.6 CP_{Name}: SIGOV-CA	*Spremembe z verzijo 5.0:* • *uporaba novega naziva za overitelja na Ministrstvu za notranje zadeve, po novem je to »Državni center za storitve zaupanja«,* • *pri spletnih potrdilih za strežnike se uporablja zgostitveni algoritem SHA-256,* • *veljavnost spletnih potrdil za strežnike je 3 leta,* • *veljavnost potrdila za šifriranje in zasebnega ključa za podpisovanje pri posebnih potrdilih za zaposlene in splošne nazive je 5 let,* • *v razločevalnem imenu posebnih potrdil ni oznake organizacije,* • *omogočeno je izdajanje spletnih potrdil za strežnike z več imeni strežnika,* • *ukinjeno je izdajanje posebnih potrdil za strežnike,* • *novi kontaktni podatki izdajatelja SIGOV-CA.*
amandma k politiki verzije 4.0, veljavnost: od 21. marca 2014	
Amandma k Politiki SIGOV-CA za kvalificirana digitalna potrdila za državne organe št. 2 / 4.0	*Sprememba z amandmajem št. 2 / 4.0:* • *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 SIGOV-CA za kvalificirana digitalna potrdila za državne organe št. 1 / 4.0	*Sprememba z amandmajem št. 1 / 4.0:* • *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 za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.1.5 • Politika za posebna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.2.5 • Politika za spletna kvalificirana digitalna potrdila za strežnike in podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.1.3.3 • Politika za posebna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.1.4.3 • Politika za kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov, CP_{OID}: 1.3.6.1.4.1.6105.1.5.3 • Politika za kvalificirana digitalna potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil, CP_{OID}: 1.3.6.1.4.1.6105.1.6.2 • Politika za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.7.1 • Politika za posebna kvalificirana digitalna potrdila za zaposlene in splošne nazive z obvezno uporabo pametnih kartic, CP_{OID}: 1.3.6.1.4.1.6105.1.8.1 CP_{Name}: SIGOV-CA	*Spremembe z verzijo 4.0:* • *izdajatelj digitalnih potrdil SIGOV-CA izdaja kvalificirana digitalna potrdila s ključi minimalne dolžine 2048 bitov;* • *izdajatelj digitalnih potrdil SIGOV-CA izdaja tudi spletna in posebna kvalificirana digitalna potrdila za zaposlene in splošne nazive brez obvezne uporabe pametnih kartic. Če se bo bodoči imetnik odločil za potrdilo z obvezno uporabo pametne kartice, mu bo le-ta skupaj z digitalnih potrdilom na varen način dostavljena s strani izdajatelja SIGOV-CA;* • *v kvalificiranih digitalnih potrdilih za zaposlene in splošne nazive je dodana ustrezna oznaka za kvalificirana potrdila oziroma potrdila z obvezno uporabo pametnih kartic;* • *spremeni se jamstvo za vrednost posameznega pravnega posla.*
amandma k politiki verzije 3.0, veljavnost**:** od 18. maja 2007	
Amandma k Politiki SIGOV-CA za kvalificirana digitalna potrdila za državne organe št. 1 / 3.0	*Sprememba z amandmajem št. 1 / 3.0:* • *izdajatelj SIGOV-CA bodočemu imetniku potrdila avtorizacijske kode ne posreduje več s priporočeno pošto, temveč z navadno poštno pošiljko.*
verzija: 3.0, veljavnost**:** od 28. februarja 2006	
• Politika SIGOV-CA za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.1.4 • Politika SIGOV-CA za posebna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.2.4 • Politika SIGOV-CA za spletna kvalificirana digitalna potrdila za strežnike in podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.1.3.2 • Politika SIGOV-CA za posebna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.1.4.2 • Politika SIGOV-CA za kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov, CP_{OID}: 1.3.6.1.4.1.6105.1.5.2 • Politika SIGOV-CA za kvalificirana digitalna potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil, CP_{OID}: 1.3.6.1.4.1.6105.1.6.1 CP_{Name}: SIGOV-CA	*Spremembe z verzijo 3.0:* • *uporaba novega naziva za overitelja na Centru Vlade za informatiko, po novem je to »Overitelj na Ministrstvu za javno upravo«;* • *osebna kvalificirana digitalna potrdila se po novem imenujejo »posebna kvalificirana digitalna potrdila«;* • *imetniki potrdila SIGOV-CA so omejeni na državne organe, in sicer neposredne proračunske porabnike;* • *izdaja se tudi kvalificirana digitalna potrdila za sisteme za sprotno preverjanje veljavnosti digitalnih potrdil (OCSP);* • *preklic je po novem mogoč samo v poslovnem času, razen v nujnih primerih;* • *struktura dokumenta je v skladu s priporočili RFC 3647.*
verzija: 2.1, veljavnost: od 28. oktobra 2003	

• Politika SIGOV-CA za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.1.3 • Politika SIGOV-CA za osebna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.2.3 • Politika SIGOV-CA za spletna kvalificirana digitalna potrdila za strežnike in podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.1.3.1 • Politika SIGOV-CA za osebna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.1.4.1 • Politika SIGOV-CA za kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov, CP_{OID}: 1.3.6.1.4.1.6105.1.5.1 CP_{Name}: SIGOV-CA	*Spremembe z verzijo 2.1:* • *izdaja se tudi kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov;* • *politike so po novem ločene za potrdila, za katere so obvezna sredstva za varno hrambo potrdil;* • *struktura dokumenta je v skladu s priporočili RFC 2527.*
verzija: 2, veljavnost: od 15. julija 2002	
• Politika SIGOV-CA za kvalificirana digitalna potrdila za institucije javne uprave, CP_{OID}: 1.3.6.1.4.1.6105.1.1.2 in 1.3.6.1.4.1.6105.1.2.2 CP_{Name}: SIGOV-CA	*Sprememba z verzijo 2:* • *izdaja se tudi kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote institucij;* • *izdaja se tudi kvalificirana digitalna potrdila za podpis kode.*
verzija: 1, veljavnost: od 17. januarja 2001	
• Politika SIGOV-CA za službena spletna kvalificirana digitalna potrdila, CP_{OID}:1.3.6.1.4.1.6105.1.1.1, CP_{Name}: SIGOV-CA-1 • Politika SIGOV-CA za službena osebna kvalificirana digitalna potrdila, CP_{OID}: 1.3.6.1.4.1.6105.1.2.1, CP_{Name}: SIGOV-CA-2	/

VSEBINA

1. UVOD ... 14

1.1. Pregled ... 14

1.2. Identifikacijski podatki politike delovanja ... 15

1.3. Subjekti ... 16
1.3.1 Državni center za storitve zaupanja in izdajatelj SIGOV-CA ... 16
1.3.2 Prijavna služba SIGOV-CA ... 18
1.3.3 Imetniki potrdil in njihove organizacije ... 19
1.3.4 Tretje osebe ... 19
1.3.5 Ostali udeleženci ... 19

1.4. Namen uporabe ... 19
1.4.1 Pravilna uporaba potrdil in ključev ... 20
1.4.2 Nedovoljena uporaba ... 20

1.5. Upravljanje dokumentacije ... 21
1.5.1 Upravljavec politik ... 21
1.5.2 Pooblaščene osebe za politiko ... 21
1.5.3 Odgovorna oseba glede skladnosti delovanja izdajatelja SIGOV-CA s politiko ... 21
1.5.4 Postopek za sprejem nove politike ... 21

1.6. Okrajšave in izrazi ... 21
1.6.1 Okrajšave ... 21
1.6.2 Izrazi ... 23

2. OBJAVE INFORMACIJ IN JAVNI IMENIK POTRDIL ... 24

2.1. Objava dokumentov in javni imenik ... 24

2.2. Pogostnost objav ... 25

2.3. Dostop do informacij in javnega imenika potrdil ... 25

3. ISTOVETNOST IMETNIKOV POTRDIL ... 25

3.1. Dodelitev imen ... 25
3.1.1 Razločevalna imena ... 25
3.1.2 Zahteve pri tvorbi razločevalnega imena ... 27
3.1.3 Uporaba anonimnih imen ali psevdonimov ... 27
3.1.4 Pravila za interpretacijo razločevalnih imen ... 27
3.1.5 Enoličnost razločevalnih imen ... 27
3.1.6 Zaščite imen oz. znamk ... 28

3.2. Preverjanje istovetnosti imetnikov ob prvi izdaji potrdila ... 28
3.2.1 Metoda za posedovanju pripadnosti zasebnega ključa ... 28
3.2.2 Preverjanje istovetnosti organizacije ... 28
3.2.3 Preverjanje istovetnosti imetnikov ... 28
3.2.4 Nepreverjeni podatki v potrdilih ... 28
3.2.5 Preverjanje pooblastil zaposlenih za pridobitev potrdil ... 29
3.2.6 Medsebojno priznavanje ... 29

3.3. Preverjanje imetnikov za ponovno izdajo potrdila ... 29
3.3.1 Preverjanje imetnikov pri podaljšanju potrdil ... 29
3.3.2 Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu ... 29

3.4. Preverjanje istovetnosti ob zahtevi za preklic ... 29

4. UPRAVLJANJE S POTRDILI ... 30

4.1. Pridobitev potrdila 30
4.1.1 Kdo lahko pridobi potrdilo 30
4.1.2 Postopek bodočega imetnika za pridobitev potrdila in odgovornosti 30

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila 30
4.2.1 Preverjanje istovetnosti bodočega imetnika 30
4.2.2 Odobritev/zavrnitev zahtevka 30

4.3. Postopek po odobritvi zahtevka za pridobitev potrdila 31
4.3.1 Postopek izdajatelja SIGOV-CA z obvezno uporabo pametne kartice 31
4.3.2 Postopek izdajatelja SIGOV-CA brez obvezne uporabe pametne kartice 31
4.3.3 Postopek izdajatelja SIGOV-CA - splošno 31
4.3.4 Obvestilo imetnika o izdaji 31

4.4. Prevzem potrdila 31
4.4.1 Postopek prevzema potrdila z obvezno uporabo pametne kartice 31
4.4.2 Postopek prevzema potrdila brez obvezne uporabe pametne kartice 32
4.4.3 Objava potrdila 32

4.5. Obveznosti in odgovornosti uporabnikov glede uporabe potrdil 32
4.5.1 Obveznosti imetnika potrdila oziroma organizacije 32
4.5.2 Obveznosti za tretje osebe 33

4.6. Ponovna izdaja potrdila brez spremembe javnega ključa 33

4.7. Regeneriranje ključev - velja samo za posebna potrdila 34
4.7.1 Razlogi za regeneracijo 34
4.7.2 Kdo zahteva regeneracijo 34
4.7.3 Postopek za izdajo zahtevka za regeneracijo z obvezno uporabo pametne kartice 34
4.7.4 Postopek za izdajo zahtevka za regeneracijo brez obvezne uporabe pametne kartice 34

4.8. Sprememba potrdila 35
4.8.1 Okoliščina za spremembo potrdila 35
4.8.2 Kdo zahteva spremembo 35
4.8.3 Postopek ob zahtevku za spremembo 35
4.8.4 Obvestilo o izdaji novega potrdila 35
4.8.5 Prevzem spremenjenega potrdila 35
4.8.6 Objava spremenjenega potrdila 35
4.8.7 Obvestilo drugih subjektov o spremembi 35

4.9. Preklic in suspenz potrdila 35
4.9.1 Razlogi za preklic 36
4.9.2 Kdo zahteva preklic 36
4.9.3 Postopki za preklic 36
4.9.4 Čas za izdajo zahtevka za preklic 37
4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica 37
4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe 37
4.9.7 Pogostnost objave registra preklicanih potrdil 37
4.9.8 Čas objave registra preklicanih potrdil 37
4.9.9 Sprotno preverjanje statusa potrdil 38
4.9.10 Zahteve za sprotno preverjanje statusa potrdil 38
4.9.11 Drugi načini za dostop do statusa potrdil 38
4.9.12 Posebne zahteve pri zlorabi zasebnega ključa 38
4.9.13 Razlogi za suspenz 38
4.9.14 Kdo zahteva suspenz 38
4.9.15 Postopek za suspenz 38
4.9.16 Čas suspenza 38

4.10. Preverjanje statusa potrdil 38
4.10.1 Dostop za preverjanje 38
4.10.2 Razpoložljivost 38

4.10.3 Druge informacije za preverjanje statusa ... 39

4.11. Prekinitev razmerja med imetnikom in overiteljem ... 39

4.12. Odkrivanje kopije ključev za dešifriranje - velja za posebna potrdila ... 39
4.12.1 Razlogi za odkrivanje kopije ključev za dešifriranje ... 39
4.12.2 Kdo zahteva odkrivanje kopije ključev za dešifriranje ... 39
4.12.3 Postopek ob zahtevku za odkrivanje kopije ključev za dešifriranje ... 39

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE ... 39

5.1. Fizično varovanje ... 39
5.1.1 Lokacija in zgradba overitelja na MJU ... 40
5.1.2 Fizični dostop do infrastrukture overitelja na MJU ... 40
5.1.3 Napajanje in prezračevanje ... 40
5.1.4 Zaščita pred poplavo ... 40
5.1.5 Zaščita pred požari ... 40
5.1.6 Hramba nosilcev podatkov ... 40
5.1.7 Odstranjevanje odpadkov ... 41
5.1.8 Hramba na oddaljeni lokaciji ... 41

5.2. Organizacijska struktura izdajatelja oz. overitelja ... 41
5.2.1 Skupine overitelja na MJU ... 41
5.2.2 Število oseb za posamezne naloge ... 42
5.2.3 Izkazovanje istovetnosti za opravljanje posameznih nalog ... 42
5.2.4 Nezdružljivost nalog ... 42

5.3. Nadzor nad osebjem ... 42
5.3.1 Potrebne kvalifikacije in izkušnje osebja ... 42
5.3.2 Primernost osebja ... 42
5.3.3 Dodatno izobraževanje osebja ... 43
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 ... 43
5.4.3 Čas hrambe dnevnikov ... 43
5.4.4 Zaščita dnevnikov ... 44
5.4.5 Varnostne kopije dnevnikov ... 44
5.4.6 Zbiranje podatkov za dnevnike ... 44
5.4.7 Obveščanje povzročitelja dogodka ... 44
5.4.8 Ocena ranljivosti sistema ... 44

5.5. Arhiviranje podatkov ... 44
5.5.1 Vrste arhivskih podatkov ... 44
5.5.2 Čas hrambe ... 45
5.5.3 Zaščita arhivskih podatkov ... 45
5.5.4 Varnostna kopija arhiva ... 45
5.5.5 Zahteva po časovnem žigosanju ... 45
5.5.6 Način zbiranja podatkov ... 45
5.5.7 Postopek za dostop do arhivskih podatkov in njihova verifikacija ... 45

5.6. Podaljšanje veljavnosti potrdil ... 45
5.6.1 Podaljševanje veljavnosti posebnih potrdil ... 45
5.6.2 Podaljševanje veljavnosti spletnih potrdil ... 46
5.6.3 Podaljšanje veljavnosti potrdila izdajatelja SIGOV-CA ... 46

5.7. Okrevalni načrt ... 46
5.7.1 Postopek v primeru vdorov in zlorabe ... 46
5.7.2 Postopek v primeru okvare programske opreme, podatkov ... 46
5.7.3 Postopek v primeru ogroženega zasebnega ključa izdajatelja SIGOV-CA ... 46
5.7.4 Okrevalni načrt ... 46

5.8. Prenehanje delovanja SIGOV-CA ... 46

6. TEHNIČNE VARNOSTNE ZAHTEVE ... 46

6.1. Generiranje in namestitev ključev ... 46
6.1.1 Generiranje ključev ... 47
6.1.2 Dostava zasebnega ključa imetnikom ... 48
6.1.3 Dostava javnega ključa izdajatelju potrdil ... 48
6.1.4 Dostava izdajateljevega javnega ključa ... 48
6.1.5 Dolžina ključev ... 49
6.1.6 Generiranje in kakovost parametrov javnih ključev ... 49
6.1.7 Namen ključev in potrdil ... 49

6.2. Zaščita zasebnega ključa ... 49
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 (angl. *Key Escrow*) ... 50
6.2.4 Varnostna kopija zasebnega ključa ... 50
6.2.5 Arhiviranje zasebnega ključa ... 50
6.2.6 Zapis zasebnega ključa v kriptografski modul ... 50
6.2.7 Postopek za aktiviranje zasebnega ključa ... 50
6.2.8 Postopek za deaktiviranje zasebnega ključa ... 50
6.2.9 Postopek za uničenje zasebnega ključa ... 50

6.3. Ostali aspekti upravljanja ključev ... 51
6.3.1 Arhiviranje javnega ključa ... 51
6.3.2 Obdobje veljavnosti za javne in zasebne ključe ... 51

6.4. Gesla za dostop do potrdil oz. ključev ... 51
6.4.1 Generiranje gesel ... 51
6.4.2 Zaščita gesel ... 52
6.4.3 Drugi aspekti gesel ... 52

6.5. Varnostne zahteve za računalniško opremo izdajatelja ... 52
6.5.1 Specifične tehnične varnostne zahteve ... 52
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 ... 53

6.7. Varnostne kontrole računalniške mreže ... 53

6.8. Časovno žigosanje ... 53

7. PROFIL POTRDIL IN REGISTRA PREKLICANIH POTRDIL ... 53

7.1. Profil potrdil ... 53
7.1.1 Različica potrdil ... 53
7.1.2 Profil potrdil z razširitvami ... 54
7.1.3 Identifikacijske oznake algoritmov ... 58
7.1.4 Oblika razločevalnih imen ... 58
7.1.5 Omejitve glede imen ... 58
7.1.6 Označba politike potrdila ... 58
7.1.7 Omejitve uporabe ... 58

7.2. Profil registra preklicanih potrdil ... 58

7.2.1 Različica ... 58
7.2.2 Vsebina registra in razširitve ... 59
7.2.3 Objava registra CRL v javnem imeniku in v digitalnih potrdilih ... 59

7.3. Profil sprotnega preverjanja statusa potrdil ... 60
7.3.1 Verzija sprotnega preverjanje statusa ... 60
7.3.2 Razširitve sprotnega preverjanje statusa ... 60

8. INŠPEKCIJSKI NADZOR ... 60

8.1. Pogostnost inšpekcijskega nadzora ... 60

8.2. Inšpekcijska služba ... 60

8.3. Neodvisnost inšpekcijske služba ... 60

8.4. Področja inšpekcijskega nadzora ... 60

8.5. Ukrepi overitelja ... 61

8.6. Objava rezultatov inšpekcijskega nadzora ... 61

9. FINANČNE IN OSTALE PRAVNE ZADEVE ... 61

9.1. Cenik ... 61
9.1.1 Cena izdaje potrdil in podaljšanja ... 61
9.1.2 Cena dostopa do potrdil ... 61
9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil ... 61
9.1.4 Cene drugih storitev ... 61
9.1.5 Povrnitev stroškov ... 61

9.2. Finančna odgovornost ... 61
9.2.1 Zavarovalniško kritje ... 61
9.2.2 Drugo kritje ... 62
9.2.3 Zavarovanje imetnikov ... 62

9.3. Varovanje poslovnih podatkov ... 62
9.3.1 Varovani podatki ... 62
9.3.2 Nevarovani podatki ... 62
9.3.3 Odgovornost glede varovanja ... 62

9.4. Varovanje osebnih podatkov ... 62
9.4.1 Načrt varovanja osebnih podatkov ... 62
9.4.2 Varovani osebni podatki ... 63
9.4.3 Nevarovani osebni podatki ... 63
9.4.4 Odgovornost glede varovanja osebnih podatkov ... 63
9.4.5 Pooblastilo glede uporabe osebnih podatkov ... 63
9.4.6 Posredovanje osebnih podatkov ... 63
9.4.7 Druga določila glede varovanja osebnih podatkov ... 63

9.5. Določbe glede pravic intelektualne lastnine ... 63

9.6. Obveznosti in odgovornosti ... 63
9.6.1 Obveznosti in odgovornosti overitelja na MJU oz. izdajatelja SIGOV-CA ... 63
9.6.2 Obveznost in odgovornost prijavne službe ... 64
9.6.3 Obveznosti in odgovornost imetnika potrdila oziroma organizacije ... 65
9.6.4 Obveznosti in odgovornost tretjih oseb ... 65
9.6.5 Obveznosti in odgovornost drugih oseb ... 65

9.7. Omejitev odgovornosti ... 65

9.8. Omejitev glede uporabe ... 66

9.9. Poravnava škode ... 66

9.10. Veljavnost politike ... 66

9.10.1 Čas veljavnosti 66
9.10.2 Konec veljavnosti politike 66
9.10.3 Učinek poteka veljavnosti politike 67
9.11. Komuniciranje med subjekti 67
9.12. Amandmaji 67
9.12.1 Postopek za sprejem amandmajev 67
9.12.2 Veljavnost in objava amandmajev 67
9.12.3 Sprememba identifikacijske številke politike 67
9.13. Postopek v primeru sporov 67
9.14. Veljavna zakonodaja 68
9.15. Skladnost z veljavno zakonodajo 68
9.16. Druga določila 68

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 oz. overitelj*) 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 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), evropskimi direktivami ter drugimi veljavnimi predpisi in priporočili.

Kvalificirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba digitalnih potrdil overitelja na MJU,
- za varno elektronsko komuniciranje med imetniki kvalificiranih digitalnih potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba digitalnih potrdil overitelja na MJU.

Izdajatelj kvalificiranih digitalnih potrdil SIGOV-CA (angl. *Slovenian Governmental Certification Authority*), http://www.sigov-ca.gov.si, izdaja le-te za državne organe in druge organe, ki po veljavni zakonodaji veljajo za neposredne uporabnike državnega proračuna, in deluje v okviru overitelja na MJU, http://www.ca.gov.si.

Izdajatelj SIGOV-CA je registriran v skladu z veljavno zakonodajo in medsebojno priznan z izdajateljem kvalificiranih digitalnih potrdil SIGEN-CA (angl. *Slovenian General Certification Authority*), http://www.sigen-ca.si.

Pričujoči dokument določa politike izdajatelja SIGOV-CA za več vrst kvalificiranih digitalnih potrdil, ki izpolnjujejo najvišje varnostne zahteve. Na podlagi tega dokumenta SIGOV-CA izdaja posebna in spletna kvalificirana digitalna potrdila po naslednjih politikah: CP_{OID}: 1.3.6.1.4.1.6105.1.1.7, CP_{OID}: 1.3.6.1.4.1.6105.1.2.7, CP_{OID}: 1.3.6.1.4.1.6105.1.3.7, CP_{OID}: 1.3.6.1.4.1.6105.1.4.7, CP_{OID}: 1.3.6.1.4.1.6105.1.5.7, CP_{OID}: 1.3.6.1.4.1.6105.1.6.7, CP_{OID}: 1.3.6.1.4.1.6105.1.7.7, CP_{OID}: 1.3.6.1.4.1.6105.1.8.7, CP_{OID}: 1.3.6.1.4.1.6105.1.9.7, CP_{OID}: 1.3.6.1.4.1.6105.1.10.7, CP_{OID}: 1.3.6.1.4.1.6105.1.11.7 ter CP_{OID}: 1.3.6.1.4.1.6105.1.12.7.

Pričujoči dokument nadomešča prejšnje objavljene politike SIGOV-CA. Vsa kvalificirana 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 kvalificirano digitalno potrdilo izdano (na primer postopek za preklic velja po novi politiki).

Spremembe pričujočega dokumenta so sledeče:
- tvorjeno je bilo drugo lastno digitalno potrdilo izdajatelja SIGOV-CA z zasebnim ključem dolžine 3072 bitov, ki se hrani na strojni opremi za varno shranjevanje zasebnih ključev,
- v potrdilu izdajatelja SIGOV-CA in vseh potrdilih imetnikov se uporablja zgostitveni algoritem SHA-256,
- spremenjeno je razločevalno ime digitalnega potrdila izdajatelja SIGOV-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.

Kvalificirana digitalna potrdila se pridobijo na podlagi zahtevka, ki ga mora podpisati predstojnik organizacije oz. organizacijske enote in bodoči imetniki. V primeru kvalificiranega digitalnega potrdila za splošni naziv, strežnik, podpis kode, izdajatelja časovnih žigov oz. sistema za sprotno preverjanje veljavnosti digitalnih potrdil je bodoči imetnik zaposleni oz. oseba, ki jo predstojnik pooblasti za uporabo tega potrdila. Predstojnik s podpisom zahtevka

jamči za istovetnost bodočega imetnika. Izpolnjen zahtevek se odda na prijavno službo, ki je vzpostavljena na sedežu Overitelja na MJU (kontaktni podatki so objavljeni na spletni strani http://www.sigov-ca.gov.si/prijavne-slu.php).

Spletna in posebna kvalificirana digitalna potrdila SIGOV-CA za zaposlene in splošne nazive se praviloma izdajo kot potrdila z obvezno uporabo pametnih kartic in so na podlagi odobrenega zahtevka prevzeta na imetnikovo pametno kartico na infrastrukturi izdajatelja SIGOV-CA. Izjemoma lahko bodoči imetnik na zahtevku za pridobitev kvalificiranega potrdila zahteva drugače, če uporaba pametne kartice v njegovem okolju s tehničnega vidika ni mogoča. Pri potrdilu z obvezno uporabo pametne kartice je le-ta bodočemu imetniku skupaj z digitalnim potrdilom na varen način dostavljena s strani izdajatelja SIGOV-CA, tako da bodoči imetnik preko kontaktne osebe organizacije prejme pametno kartico z digitalnim potrdilom, prednastavljeno geslo za dostop do digitalnega potrdila pa prejme s poštno pošiljko z oznako »Osebno« na naslov svoje organizacije.

V primeru digitalnih potrdil brez obvezne uporabe pametnih kartic SIGOV-CA na podlagi odobrenega zahtevka pripravi referenčno številko in avtorizacijsko kodo, ki sta unikatni za vsakega bodočega imetnika kvalificiranega digitalnega potrdila in ju le-ta potrebuje za prevzem svojega potrdila, ki ga opravi v skladu z navodili izdajatelja SIGOV-CA. Bodoči imetnik prejme referenčno številko po elektronski pošti, avtorizacijsko kodo pa s poštno pošiljko na naslov svoje organizacije.

Spletno kvalificirano digitalno potrdilo je povezano z enim parom ključev, ki se tvori z imetnikovo programsko ali strojno opremo. SIGOV-CA nikoli ne hrani zasebnega ključa. Javni ključ se pošlje izdajatelju SIGOV-CA, ki izda potrdilo, katerega sestavni del je javni ključ. Spletno potrdilo in pripadajoči ključi se shranijo pri imetniku oz. na imetnikovi pametni kartici, samo potrdilo pa se objavi tudi v javnem imeniku potrdil.

Pri posebnem digitalnem potrdilu sta ločena para ključev za podpisovanje/overjanje in za dešifriranje/šifriranje in s tem tudi dve potrdili. Pri tem velja:

- Par ključev za podpisovanje/overjanje se tvori z imetnikovo programsko ali strojno opremo. SIGOV-CA nikoli ne hrani zasebnega ključa za podpisovanje. Javni ključ za overjanje podpisa se pošlje SIGOV-CA, ki izda potrdilo za overjanje podpisa, katerega sestavni del je javni ključ za overjanje podpisa. Potrdilo za overjanje podpisa se shrani pri imetniku oz. na imetnikovi pametni kartici.
- Par ključev za dešifriranje/šifriranje se tvori na strani izdajatelja SIGOV-CA. Zasebni ključ za dešifriranje se shrani na imetnikovi programski ali strojni opremi. Zaradi možnega dostopa (dešifriranja) do pomembnih zašifriranih podatkov, če zasebni ključ za dešifriranje iz kakršnegakoli razloga ni več dostopen, se ta ključ po posebnem režimu, ki je določen z Interno politiko overitelja na MJU, varno hrani tudi v arhivu SIGOV-CA. SIGOV-CA izda potrdilo za šifriranje, katerega sestavni del je javni ključ za šifriranje. Potrdilo za šifriranje se objavi v javnem imeniku potrdil.

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

Imetnik mora skrbno varovati zasebne ključe, svoje kvalificirano digitalno potrdilo in pametno kartico ter ravnati v skladu s politiko, obvestili izdajatelja SIGOV-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 oz. overitelj*).

(2) Politike overitelja kvalificiranih digitalnih potrdil in varnih časovnih žigov predstavljajo celoten javni del notranjih pravil overitelja 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 imetniki, uporabniki in tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila in 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), evropskimi direktivami ter drugimi veljavnimi predpisi in priporočili.

(4) Kvalificirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba potrdil overitelja na MJU,
- za varno elektronsko komuniciranje med imetniki potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

(5) 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.

(6) Izdajatelj SIGOV-CA (angl. Slovenian Governmental Certification Authority), http://www.sigov-ca.gov.si, izdaja kvalificirana digitalna potrdila za državne organe in druge organe, ki po veljavni zakonodaji veljajo za neposredne uporabnike državnega proračuna (v nadaljevanju *organizacije*), in deluje v okviru overitelja na MJU, http://www.ca.gov.si. Pričujoči dokument določa politike izdajatelja SIGOV-CA za vse vrste kvalificiranih digitalnih potrdil za potrebe neposrednih uporabnikov državnega proračuna.

(7) Izdajatelj SIGOV-CA je registriran v skladu z veljavno zakonodajo in medsebojno priznan z izdajateljem kvalificiranih digitalnih potrdil SIGEN-CA (angl. *Slovenian General Certification Authority*), http://www.sigen-ca.si.

(8) Po pričujoči politiki SIGOV-CA izdaja naslednja kvalificirana digitalna potrdila:
- posebna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- posebna kvalificirana digitalna potrdila za zaposlene v organizacijah z obvezno uporabo pametnih kartic,
- posebna kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote organizacij,
- posebna kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote organizacij z obvezno uporabo pametnih kartic,
- spletna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- spletna kvalificirana digitalna potrdila za zaposlene v organizacijah z obvezno uporabo pametnih kartic,
- spletna kvalificirana digitalna potrdila za splošne nazive organizacij oz. organizacijske enote organizacij,
- spletna kvalificirana digitalna potrdila za splošne nazive organizacij oz. organizacijske enote organizacij z obvezno uporabo pametnih kartic,
- spletna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo organizacije,
- spletna kvalificirana digitalna potrdila za podpis kode za potrebe organizacije,

- kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov[1],
- kvalificirana digitalna potrdila za sisteme za sprotno preverjanje veljavnosti digitalnih potrdil[2],
- za druge izdajatelje digitalnih potrdil.

(9) Kvalificirana digitalna potrdila SIGOV-CA (v nadaljevanju *potrdila*) 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.

(10) Za posebna in spletna potrdila za zaposlene in splošne nazive, na podlagi politike po CP_{OID}: 1.3.6.1.4.1.6105.1.2.7, CP_{OID}: 1.3.6.1.4.1.6105.1.4.7, CP_{OID}: 1.3.6.1.4.1.6105.1.6.7 in CP_{OID}: 1.3.6.1.4.1.6105.1.8.7 je obvezna uporaba pametnih kartic, za druga pa je potrebno upoštevati priporočila izdajatelja SIGOV-CA za zaščito zasebnih ključev oz. uporabo varnih kriptografskih modulov.

(11) Pričujoča politika je pripravljena skladno s priporočilom RFC 3647 »Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework«.

(12) Medsebojna razmerja se lahko izvajajo tudi na podlagi pisnega dogovora med organizacijami in overiteljem na MJU, ali med tretjimi osebami, ki se zanašajo na potrdila izdajatelja SIGOV-CA in overiteljem na MJU.

(13) Overitelj na MJU se lahko povezuje v mrežo overiteljev na horizontalni ali vertikalni ravni, kar se ureja z medsebojnim pisnim dogovorom.

1.2. Identifikacijski podatki politike delovanja

(1) Oznake pričujoče politike delovanja SIGOV-CA so različne glede na vrsto potrdila:
- CP_{OID}: 1.3.6.1.4.1.6105.1.1.7 za spletna kvalificirana digitalna potrdila za zaposlene,
- CP_{OID}: 1.3.6.1.4.1.6105.1.2.7 za spletna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.3.7 za posebna kvalificirana digitalna potrdila za zaposlene,
- CP_{OID}: 1.3.6.1.4.1.6105.1.4.7 za posebna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.5.7 za spletna kvalificirana digitalna potrdila za splošne nazive,
- CP_{OID}: 1.3.6.1.4.1.6105.1.6.7 za spletna kvalificirana digitalna potrdila za splošne nazive z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.7.7 za posebna kvalificirana digitalna potrdila za splošne nazive,
- CP_{OID}: 1.3.6.1.4.1.6105.1.8.7 za posebna kvalificirana digitalna potrdila za splošne nazive z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.9.7 za spletna kvalificirana digitalna potrdila za strežnike,
- CP_{OID}: 1.3.6.1.4.1.6105.1.10.7 za spletna kvalificirana digitalna potrdila za podpis kode,
- CP_{OID}: 1.3.6.1.4.1.6105.1.11.7 za kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov (v nadaljevanju *TSA*, angl. *Time Stamp Authority*),
- CP_{OID}: 1.3.6.1.4.1.6105.1.12.7 za kvalificirana digitalna potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil (v nadaljevanju *OCSP*, angl. *Online Certificate Status Protocol*).

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

[1] Potrdila za izdajatelje časovnih žigov se, kjer ni drugače navedeno, obravnavajo kot posebna kvalificirana digitalna potrdila.
[2] Potrdila za sisteme za sprotno preverjanje veljavnosti digitalnih potrdil se, kjer ni drugače navedeno, obravnavajo kot spletna kvalificirana digitalna potrdila.

1.3. Subjekti

1.3.1 Državni center za storitve zaupanja in izdajatelj SIGOV-CA

(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 podani spodaj:

Naslov:	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
Oznaka:	Republika Slovenija

(3) V okviru overitelja na MJU deluje izdajatelj kvalificiranih digitalnih potrdil SIGOV-CA.

(4) Kontaktni podatki izdajatelja SIGOV-CA so podani spodaj::

Naslov:	SIGOV-CA Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
E-pošta:	sigov-ca@gov.si
Telefon:	01 4788 330
Spletna stran:	http://www.sigov-ca.gov.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

(5) Izdajatelj SIGOV-CA opravlja naslednje naloge:
- izdaja kvalificirana digitalna potrdila,
- določa in objavlja svojo politiko delovanja,
- določa in objavlja 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 prijavne službe,
- za bodoče imetnike opravi prevzem digitalnih potrdil, pri katerih je obvezna uporaba pametnih kartic in
- opravlja vse ostale storitve v skladu s politiko in ostalimi predpisi.

(6) Izdajatelj SIGOV-CA je ob začetku svojega produkcijskega delovanja tvoril svoje lastno digitalno potrdilo, ki je namenjeno overjanju potrdil, ki jih je SIGOV-CA izdal imetnikom ali izdajateljem varnih časovnih žigov.

Potrdilo št. 1 SIGOV-CA vsebuje naslednje podatke[3]:

Polje	Podatki potrdila št.1 izdajatelja SIGOV-CA
Različica, angl. *Version*	2 (*kar pomeni verzijo 3*)
Identifikacijska oznaka, angl. *Serial Number*	3A5C 701A
Algoritem podpis, angl. *Signature Algorithm*	sha1WithRSAEncryption
Izdajatelj, angl. *Issuer*	c=si, o=state-institutions, ou=sigov-ca
Imetnik, angl. *Subject*	c=si, o=state-institutions, ou=sigov-ca
Pričetek veljavnosti, angl. *Validity: Not Before*	Jan 10 14:52:52 2016 GMT
Konec veljavnosti, angl. *Validity: Not After*	Jan 10 15:22:52 2036 GMT
Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 2048 bitov*
Identiteta ključa (po alg. SHA-1), angl. *Subject Key Identifier*	1EF8 D453 6BB3 8306 E904 0657 02F9 A5BF C658 3C72
Odtis potrdila (ni del potrdila)	
Odtis potrdila MD-5, angl. *Certificate Fingerprint – MD5*	739D D35F C63C 95FE C6ED 89E5 8208 DD89
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	7FB9 E2C9 95C9 7A93 9F9E 81A0 7AEA 9B4D 7046 3496
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	74CB 3A4E A791 AFB0 A2D1 A0B1 3301 B3BE E0E5 0AD5 C79A 1A6F 2C66 3E6F 4EE7 A484

(7) Izdajatelj SIGOV-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 SIGOV-CA izdal imetnikom ali izdajateljem varnih časovnih žigov od 11.1.2016 dalje.

Potrdilo št. 2 SIGOV-CA vsebuje naslednje podatke:

Polje	Podatki potrdila št.2 izdajatelja SIGOV-CA
Različica, angl. *Version*	2 (*kar pomeni verzijo 3*)
Identifikacijska oznaka, angl. *Serial Number*	BD1A 837C 0000 0000 567B C70E
Algoritem podpis, angl. *Signature Algorithm*	sha256WithRSAEncryption

[3] Pomen je podan v podpogl. 3.1 in 7.1.

Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, organizationIdentifier=VATSI-17659957, cn=SIGOV-CA
Imetnik, angl. *Subject*	c=SI, o=Republika Slovenija, organizationIdentifier=VATSI-17659957, cn=SIGOV-CA
Pričetek veljavnosti, angl. *Validity: Not Before*	Dec 24 09:51:06 2015 GMT
Konec veljavnosti, angl. *Validity: Not After*	Dec 24 10:21:06 2035 GMT
Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 3072 bitov*
Identiteta ključa, angl. *Subject Key Identifier*	465E 40E5 53ED FEFE
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	4357 B45E 9FF9 0BDA BA78 B532 2EB0 656F D1B7 BA58
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	64DC 4058 1A84 B6F2 93C1 AFFF 63F8 E14A 99B7 EAC4 1D1F DB38 65CA BAA2 FA01 B610

1.3.2 Prijavna služba SIGOV-CA

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

(2) Naloge prijavne službe so:
- preverjanje istovetnosti imetnikov oz. bodočih imetnikov, podatkov o organizacijah in drugih potrebnih podatkov,
- sprejemanje zahtevkov za pridobitev potrdil,
- sprejemanje zahtevkov za preklic potrdil,
- sprejemanje zahtevkov za regeneriranje ključev posebnih potrdil,
- preverjanje podatkov v zahtevkih,
- izdajanje potrebne dokumentacije imetnikom oz. bodočim imetnikom,
- posredovanje zahtevkov in ostalih podatkov na varen način na SIGOV-CA.

(3) Naloge prijavne službe za potrebe izdajatelja SIGOV-CA vrši:
- organizacija za svoje zaposlene osebe opravlja del nalog prijavnih služb po določilih SIGOV-CA, in sicer predstojnik organizacije, kjer je bodoči imetnik potrdila zaposlen, jamči za njegovo istovetnost, ki jo je preverila v skladu z 31. členom in drugimi določili ZEPEP,
- pooblaščena oseba prijavne službe, ki preveri podatke o imetnikih oz. bodočih imetnikih, podatke o organizaciji in druge potrebne podatke ter izvaja ostale naloge v pristojnosti prijavne službe.

(4) Izdajatelj SIGOV-CA ima vzpostavljeno svojo prijavno službo na svojem sedežu (glej razd. 1.3.1), podatki o tem pa so objavljeni na spletnih straneh.

1.3.3 Imetniki potrdil in njihove organizacije

(1) Organizacija oz. predstojnik le-te je naročnik digitalnih potrdil (angl. *subscriber*) za imetnike potrdil, ki so zaposleni v organizaciji ali opravljajo delo za to organizacijo (angl. *subject*).

(2) Predstojnik s podpisom zahtevka za pridobitev potrdila jamči za podatke o organizaciji in istovetnosti bodočih imetnikov in jih pooblašča za uporabo potrdil v imenu opravljanja nalog za organizacijo.

(3) Imetniki potrdil so vedno fizične osebe. V primeru potrdila za strežnike oz. informacijske sisteme, splošne nazive in podpis kode je imetnik takega potrdila pooblaščen s strani predstojnika, v primeru potrdila za izdajatelja varnih časovnih žigov in druge izdajatelje pa predstojnik organizacije izdajatelja varnih časovnih žigov oz. drugega izdajatelja oz. od njega pooblaščena oseba. Imetniki so tako lahko:
- zaposleni,
- zaposleni, pooblaščeni za uporabo splošnih nazivov oz. organizacijske enote organizacij,
- zaposleni, pooblaščeni za upravljanje s strežniki (storitvami oz. aplikacijami),
- zaposleni, pooblaščeni za uporabo programske opreme za podpis kode,
- predstojniki oz. pooblaščene osebe organizacij izdajateljev varnih časovnih žigov,
- predstojniki oz. pooblaščene osebe organizacij sistemov za sprotno preverjanje veljavnosti digitalnih potrdil in
- predstojniki oz. pooblaščene osebe drugih izdajateljev potrdil.

(4) Med organizacijo in izdajateljem SIGOV-CA oz. overiteljem na MJU se lahko sklene medsebojni pisni dogovor.

1.3.4 Tretje osebe

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

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

(3) Tretje osebe niso nujno tudi imetniki potrdil izdajatelja SIGOV-CA oz. digitalnih potrdil drugih izdajateljev.

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

1.3.5 Ostali udeleženci

Niso predvideni.

1.4. Namen uporabe

(1) Posebna in spletna potrdila SIGOV-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) Namen potrdil oz. pripadajočih ključev je podan v potrdilu v polju *namen uporabe* (angl. *key usage*), v primerih potrdil za strežnike, podpis kode, izdajatelje TSA in sisteme za OCSP pa dodatno v polju *razširjena uporaba ključa* (angl. *extended key usage*), glej 7.1.2.

(3) Uporaba potrdil je povezana z namenom pripadajočih ključev. Ločimo naslednje možnosti:

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

1.4.1 Pravilna uporaba potrdil in ključev

(1) Vsakemu imetniku posebnega potrdila pripadata dva ločena para ključev - za digitalno podpisovanje/overjanje podpisa in za dešifriranje/šifriranje podatkov. Oba para imata po en zasebni in javni ključ.

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

(3) Izdajatelju TSA ter sistemu OCSP se podeli samo en par ključev, in sicer par ključev za digitalno podpisovanje/overjanje.

(4) Pregled uporabe potrdil in ključev je podan v tabeli spodaj.

Tip potrdila	Par ključev	Pripadajoči ključi	Namen
posebno za zaposlene in splošne nazive	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	-ključ za podpisovanje -ključ za overjanje podpisa	podpisovanje/overjanje
	par za dešifriranje/šifriranje (potrdilo za šifriranje)	-ključ za dešifriranje -ključ za šifriranje	dešifriranje/šifriranje
spletno za zaposlene in splošne nazive	par digitalno podpisovanje/overjanje in dešifriranje/šifriranje	- zasebni ključ - javni ključ	podpisovanje/overjanje in dešifriranje/šifriranje
spletno za strežnike[4]	par digitalno podpisovanje/overjanje in dešifriranje/šifriranje	- zasebni ključ - javni ključ	podpisovanje/overjanje in dešifriranje/šifriranje varnih povezav
spletno za podpis kode[4]	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	-ključ za podpisovanje -ključ za overjanje podpisa	podpisovanje/overjanje izvršljive programske kode
potrdilo za izdajatelja TSA[5]	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	-ključ za podpisovanje -ključ za overjanje podpisa	podpisovanje/overjanje varnih časovnih žigov
potrdilo za sistem OCSP[4]	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	-ključ za podpisovanje -ključ za overjanje podpisa	podpisovanje/overjanje odzivov OCSP

1.4.2 Nedovoljena uporaba

(1) Potrdila, ki jih izdaja SIGOV-CA, se morajo uporabljati v skladu s politiko in veljavno zakonodajo.

[4] Namen uporabe potrdila za strežnike je dodatno omejen na vzpostavljanje varne povezave.
[5] Namen uporabe potrdila za podpis kode, izdajatelje TSA oz. sisteme OCSP je dodatno omejen na overjanje izvršljive programske kode, varnih časovnih žigov oz. odzivov sistema OCSP.

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

1.5. Upravljanje dokumentacije

1.5.1 Upravljavec politik

Z dokumentacijo upravlja izdajatelj SIGOV-CA oz. overitelj na MJU.

1.5.2 Pooblaščene osebe za politiko

Pooblaščene osebe v zvezi s politiko in ostalo dokumentacijo so pooblaščene osebe overitelja na MJU.

1.5.3 Odgovorna oseba glede skladnosti delovanja izdajatelja SIGOV-CA s politiko

Odgovorne osebe glede skladnosti delovanja so pooblaščene osebe overitelja na MJU v skladu z nalogami, ki jih opravljajo v okviru organizacijskih skupin (glej razd. 5.2.1).

1.5.4 Postopek za sprejem nove politike

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

(2) Spremembe politike overitelja na MJU se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na MJU pod novo identifikacijsko številko (CP_{OID}) in označenim datumom začetka njene veljavnosti. V tem času lahko imetniki oz. bodoči imetniki na elektronski naslov izdajatelja SIGOV-CA podajo svoje pripombe, ki jih obravnavajo pooblaščene osebe overitelja na MJU.

(3) Overitelj lahko izda tudi amandmaje k politiki, glej podpogl. 9.12.

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

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

1.6. Okrajšave in izrazi

1.6.1 Okrajšave

CA	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi, angl. *Certification Authority.*
CP_{Name}	Ime politike delovanja overitelja oz. izdajatelja (angl. *Certification Policy Name*), povezano z mednarodno številko politike delovanja (primerjaj okrajšavo CP_{OID}).

CP_{OID}	Mednarodna številka, ki enolično določa politiko delovanja, v skladu z mednarodnim standardom ITU-T priporočili X.208 (ASN.1), angl. *Certification Policy Object IDentifier.*
CRL	Seznam preklicanih potrdil (CRL, angl. *Certification Revocation List*) (primerjaj izraz *Register preklicanih potrdil*).
DNS	Baza imen računalnikov, ki so vključeni v internet. Omogoča povezave imen računalnikov z njihovimi številkami IP (DNS, angl. *Domain Name System*).
ETSI	Mednarodna priporočila za področje telekomunikacij, angl. *European Telecommunications Standards Institut,* http://www.etsi.org.
LDAP	Protokol, ki določa dostop do imenika in je specificiran po IETF (angl. *Internet Engineering Task Force*) 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. *Online Certificate Status* Protocol).
PKCS#7 in PKCS#10	Priporočila (angl. *Public Key Cryptography Standards*) podjetje RSA Security za razvijalce računalniških sistemov, ki uporabljajo asimetrične kriptografske algoritme. • 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. *Public Key Infrastructure.*
PKIX-CMP	Določa postopek za izmenjavo podatkov, ki se nanašajo na digitalna potrdila med entitetami infrastrukture overitelja. Zajema tudi *de-facto* standarda PKCS#7 in PKCS#10. Trenutno je objavljen kot priporočilo RFC 4210 »*Public Key Infrastructure (based on) X.509 - Certificate Management Protocols*«.
RFC	Mednarodna priporočila za Internet skupine IETF, angl. *Internet Engineering Task Force* in IESG, angl. *Internet Engineering Steering Group*, angl. *Request for Comments*, http://www.ietf.org/rfc.html.
SSCD	Varno sredstvo za elektronsko podpisovanje, ki ustreza zahtevam Aneksa III EU Direktive o elektronskem podpisu 1999/93/EC in 37. členu ZEPEP, (angl. Secure Signature Creation Device)
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 3280: »Internet X.509 Public Key Infrastructure Certificate and CRL Profile«.
TSA	Izdajatelj varnih časovnih žigov (TSA, angl. *Time Stamping Authority*).
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14).

1.6.2 Izrazi

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

EU Direktiva o elektronskem podpisu	Directive 1999/93/EC Of The European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
Digitalni podpis	Varen elektronski podpis, ki izpolnjuje zahteve 2. člena ZEPEP in 25. člena Uredbe.
Državni organ	Ministrstva, organi v sestavi ministrstev, vladne službe in upravne enote, Državni zbor, Državni svet, Ustavno sodišče, Računsko sodišče, Varuh človekovih pravic, pravosodni organi in druge osebe javnega prava, ki so neposredni uporabniki državnega proračuna v skladu z Zakonom o javnih financah (Uradni list RS, št. 11/11 – uradno prečiščeno besedilo, 14/13 – popr., 101/13 in 55/15 – ZFisP).
Kvalificirano digitalno potrdilo	Kvalificirano 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 *ZEPEP* in izraz *Uredba*).
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 *CA* in izraz *Potrdila*).
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	Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06).

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

Državni center za storitve zaupanja	Državni center za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo.
Imetnik	Zaposlena oseba, pooblaščena za uporabo potrdila za zaposlene, za potrdila za splošne nazive, za strežnike, za podpis kode, izdajatelja varnih časovnih žigov, sisteme za preverjanje veljavnosti digitalnih potrdil ali druge overitelje (angl. *subject*) (primerjaj izraz *Zaposlen*).
Infrastruktura overitelja na MJU/ izdajatelja SIGOV-CA	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 SIGOV-CA	V okviru overitelja na MJU deluje več izdajateljev. Le-ti izdajajo bodisi kvalificirana digitalna potrdila bodisi varne časovne žige. (primerjaj izraz *Overitelj na MJU*). SIGOV-CA je izdajatelj potrdil za državne organe, angl. *Slovenian Governmental Certification Authority*, http://www.sigov-ca.gov.si (primerjaj definicijo *Državni organ* in *Overitelj*).
Javni imenik	Javni imenik, s katerim upravlja izdajatelj SIGOV-CA, je vzpostavljen na strežniku *x500.gov.si*, in sicer po standardu X.500. V imeniku se objavljajo kvalificirana digitalna potrdila, ki jih izdaja SIGOV-CA, ter register preklicanih potrdil.
Objava SIGOV-CA	Javna objava na spletnih straneh SIGOV-CA oz. na straneh overitelja na MJU, http://www.sigov-ca.gov.si oz. http://www.ca.gov.si.

Obvestila SIGOV-CA	Vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči SIGOV-CA oz. overitelj na MJU in jih objavi ali kako drugače posreduje imetnikom, organizacijam ali tretjim osebam.
Organizacija	Državni organ, definiran v skladu s to politiko, primerjaj izraz Državni organ.
Overitelj na MJU	Glej izraz Državni center za storitve zaupanja.
Pametna kartica (varno sredstvo za elektronsko podpisovanje)	Varno sredstvo za elektronsko podpisovanje oz. varno hranjenje zasebnih ključev in potrdila (SSCD, angl. *Secure Signature Creation Device*), ki ustreza zahtevam Aneksa III EU direktive o elektronskem podpisu oz. 37. člena ZEPEP. Zasebnega ključa z varnega sredstva za elektronsko podpisovanje ni mogoče izvoziti oz. kopirati. Po tej politiki izdajatelj SIGOV-CA na svoji infrastrukturi za imetnika opravi prevzem kvalificiranega digitalnega potrdila z obvezno uporabo pametnih kartic.
Posebno potrdilo	Posebno kvalificirano digitalno potrdilo v elektronski obliki (posebno potrdilo sestavlja potrdilo za overjanje podpisa in potrdilo za šifriranje), ki povezuje podatke iz potrdila z imetnikovima zasebnima ključema ter potrjuje imetnikovo identiteto (angl. *enterprise certificate*). Prejšnje poimenovanje za to potrdilo je »osebno kvalificirano digitalno potrdilo«.
Potrdilo	Spletno ali posebno potrdilo.
Prijavna služba SIGOV-CA	Po pooblastilu izdajatelja SIGOV-CA prijavna služba sprejema zahtevke za pridobitev in preklic potrdil ter regeneracijo ključev posebnih potrdil in preverja istovetnosti bodočih imetnikov oz. podatkov o organizacijah (RA, angl. *Registration Authority*).
Spletno potrdilo	Kvalificirano digitalno potrdilo v elektronski obliki, ki povezuje podatke iz potrdila z imetnikovim zasebnim ključem ter potrjuje imetnikovo istovetnost (angl. *web certificate*).
Zahtevek	Obrazec SIGOV-CA za pridobivanje ali preklic potrdil, regeneracijo ključev posebnega potrdila, odkrivanje kopije zasebnega ključa za dešifriranje posebnega potrdila, ki je dostopen preko spletne strani SIGOV-CA oz. pri pooblaščenih osebah na prijavnih službah.
Zaposlen	Fizična oseba, ki je v delovnem razmerju z organizacijo ali pa na drugačni pravni podlagi dela za organizacijo in za katero želi odgovorna oseba te organizacije pridobiti potrdilo, ki ga ta oseba potrebuje za opravljanje dela za to organizacijo.

2. OBJAVE INFORMACIJ IN JAVNI IMENIK POTRDIL

2.1. Objava dokumentov in javni imenik

(1) Overitelj na MJU je odgovoren, da vse v zvezi z delovanjem SIGOV-CA, obvestila imetnikom in tretjim osebam SIGOV-CA objavlja javno na spletnih straneh SIGOV-CA, http://www.sigov-ca.gov.si.

(2) Javno dostopni dokumenti so naslednji:
- politike delovanja izdajatelja,
- cenik,
- zahtevki za storitve izdajatelja,
- navodila za varno uporabo digitalnih potrdil,
- informacijo o veljavni zakonodaji v zvezi z delovanjem overitelja ter
- ostale informacije v zvezi z delovanjem SIGOV-CA.

(3) Javno pa niso dostopni dokumenti, ki predstavljajo zaupni del notranjih pravil overitelja na MJU.

(4) V strukturi javnega imenika digitalnih potrdil, ki se nahaja na strežniku *x500.gov.si, s*e 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).

(5) Pri spletnih potrdilih za strežnike se ne objavljajo evidenčni podatki o potrdilih in veljavna digitalna potrdila.

2.2. Pogostnost objav

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

(2) 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.

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

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

2.3. Dostop do informacij in javnega imenika potrdil

(1) Javni imenik, kjer se hranijo potrdila, je javno dostopen na strežniku *x500.gov.si* po protokolu LDAP.

(2) Potrdila so dostopna tudi prek spletne strani SIGOV-CA po protokolu HTTPS:

https://www.sigov-ca.gov.si/cda-cgi/clientcgi?action=directorySearch.

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

3. ISTOVETNOST IMETNIKOV POTRDIL

3.1. Dodelitev imen

3.1.1 Razločevalna imena

(1) Vsako potrdilo vsebuje v skladu z RFC 3280 podatke o imetniku oz. nazivu ter izdajatelju v obliki razločevalnega imena, ki je oblikovano v skladu z RFC 3280 in s standardom *X.501.*

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

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

(4) Naziv, ki je vključen v razločevalno ime, je v primeru potrdila:
- za zaposlene navedeno imetnikovo ime in priimek,
- za splošni naziv oz. organizacijsko enoto organizacije splošni naziv oz. organizacijska enota organizacije,

- za strežnike ime strežnika,
- za podpis kode naziv organizacije ipd.,
- za izdajatelje varnih časovnih žigov naziv izdajatelja,
- za sisteme za preverjanje veljavnosti digitalnih potrdil naziv sistema.

(5) Vsako razločevalno ime vključuje tudi serijsko številko, ki jo določi izdajatelj SIGOV-CA[6] (glej razd. 3.1.5).

(6) Razločevalno ime se glede na vrsto identitete oz. potrdila tvori po naslednjih pravilih[7]

Vrsta potrdila	Naziv polja	Razločevalno ime[8]
potrdilo izdajatelja SIGOV-CA	izdajatelj, angl. *issuer*	c=SI, o=Republika Slovenija, organizationIdentifier=VATSI-17659957, cn=SIGOV-CA
posebna potrdila za zaposlene	imetnik, angl. *subject*	c=SI, o=state authorities, ou=certificates, cn=<ime priimek>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
posebna potrdila za splošne nazive organizacij oz. organizacijske enote organizacij	imetnik, angl. *subject*	c=SI, o=state authorities, ou=certificates, cn=<naziv>, sn=<serijska številka>
spletna potrdila za zaposlene	imetnik, angl. *subject*	c=SI, o=state authorities, ou=web-certificates, cn=<ime priimek>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
spletna potrdila za splošne nazive organizacij oz. organizacijske enote organizacij	imetnik, angl. *subject*	c=SI, o=state authorities, ou=web-certificates, cn=<naziv>, sn=<serijska številka>
spletna potrdila za strežnike	imetnik, angl. *subject*	c=SI, o=state authorities, ou=servers, cn=<naziv>, sn=<serijska številka>
spletna potrdila za podpis kode	imetnik, angl. *subject*	c=SI, o=state authorities, ou=codesign, cn=<naziv>, sn=<serijska številka>
potrdila za izdajatelje varnih časovnih žigov	imetnik,	c=SI, o=state authorities,

[6] Potrdilo izdajatelja SIGOV-CA ne vsebuje serijske številke.
[7] Pravila za tvorbo razločevalnih imen za druge vrste potrdil določi in objavi SIGOV-CA.
[8] Pomen posameznih označb: država (»c«), organizacija (»o«), organizacijska enota (»ou«), ime (»cn«), serijska številka (»sn«).

	angl. *subject*	ou=TSA-certificates, cn=<naziv>, sn=<serijska številka>
potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil	imetnik, angl. *subject*	c=SI, o=state authorities, ou=ocsp-certificates, cn=<naziv>, sn=<serijska številka>

3.1.2 Zahteve pri tvorbi razločevalnega imena

(1) V primeru potrdila za strežnik mora biti za ime strežnika navedeno polno domensko ime (angl. *fully qualified domain name*).

(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 razločevalnih imen

Pravila so navedena v razd. 3.1.1 in 3.1.2.

3.1.5 Enoličnost razločevalnih 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 SIGOV-CA	1	
2.- 8. mesto	enolično število imetnika	/	
9. - 10. mesto	oznaka za posebno potrdilo	zaposlen	20
		splošni naziv	22
		izdajatelj TSA	26
	oznaka za spletno potrdilo	zaposlen	14
		splošni naziv	18
		strežnik	10
		podpis kode	19
		sistem OCSP	11
11. – 12. mesto	zaporedno število istovrstnega potrdila	/	
13. mesto	kontrolna številka	/	

3.1.6 Zaščite imen oz. znamk

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

(2) Odgovornost v zvezi z uporabo imen oz. zaščitenih znamk je izključno na strani organizacije in imetnika. Izdajatelj SIGOV-CA oz. overitelj na MJU ni dolžan preverjati in/ali na to opozoriti imetnika oz. organizacijo.

(3) Morebitne spore rešujeta izključno prizadeta stran in imetnik oz. organizacija.

3.2. Preverjanje istovetnosti imetnikov ob prvi izdaji potrdila

3.2.1 Metoda za posedovanju pripadnosti zasebnega ključa

(1) Dokazovanje o posedovanju zasebnega ključa, ki pripada javnemu ključu v potrdilu, je zagotovljeno z varnimi postopki pred in ob prevzemu potrdila ter protokolom PKIX-CMP in PKCS#10.

(2) Dokazilo o posedovanju sredstva za varno hranjenje zasebnih ključev in potrdil, ki jih podeli izdajatelj imetniku, se hrani pri izdajatelju.

3.2.2 Preverjanje istovetnosti organizacije

(1) Za pravilnost podatkov jamči predstojnik organizacije s podpisom na zahtevku za pridobitev potrdila.

(2) Pri ustreznih službah se preveri pravilnost podatkov o organizaciji in njenem predstojniku.

3.2.3 Preverjanje istovetnosti imetnikov

(1) Organizacija za svoje zaposlene osebe opravlja del nalog prijavnih služb po določilih SIGOV-CA, in sicer predstojnik organizacije jamči:
- za istovetnost bodočega imetnika potrdila, ki ga je preveril v skladu z 31. členom in drugimi določili ZEPEP ter
- da je bodoči imetnik bodisi zaposlen v organizaciji in želi zanj pridobiti potrdilo ali pa za organizacijo opravlja naloge, za katera je potrebno pridobiti to potrdilo.

(2) Izdajatelj SIGOV-CA preveri osebne podatke o imetnikih v ustreznih registrih.

(3) Pri spletnih potrdilih za strežnike izdajatelj SIGOV-CA preveri lastništvo spletne domene v imenu strežnika.

(4) Naslov e-pošte imetnika izdajatelj SIGOV-CA preveri v centralnem imeniku uporabnikov e-pošte za državne organe.

3.2.4 Nepreverjeni podatki v potrdilih

(1) Nepreverjeni podatek v potrdilu je naziv za:
- splošne nazive oz. organizacijske enote ter
- imena strežnikov,
- za podpis kode,

- izdajatelje TSA,
- sisteme OCSP ter
- druge izdajatelje.

(2) Za pravilnost zgoraj navedenih podatkov jamčita organizacija in imetnik.

3.2.5 Preverjanje pooblastil zaposlenih za pridobitev potrdil

Organizacija oz. predstojnik organizacije s podpisom na zahtevku za pridobitev jamči, da želi za določeno osebo, ki je zaposlena ali opravlja naloge za to organizacijo, da le-ta pridobi potrdilo bodisi zase ali za splošni naziv oz. organizacijsko enoto, strežnik, podpis kode, izdajatelja TSA ali sistem OCSP, s katerim bo ta oseba upravljala.

3.2.6 Medsebojno priznavanje

(1) Overitelj na MJU se lahko povezuje in priznava z izdajatelji domačih in tujih overiteljev, vendar ni dolžan priznati drugih izdajateljev tudi, če ima drugi overitelj status akreditiranega overitelja ali overitelja kvalificiranih digitalnih potrdil.

(2) Overitelj na MJU zagotavlja, da bo izvajal medsebojno priznavanje izključno po podpisu pisne pogodbe z drugimi overitelji, ki pa morajo izpolnjevati raven varnostnih zahtev, ki je primerljiva ali višja, kot jo predpiše overitelj na MJU.

(3) Pooblaščene osebe overitelja na MJU pregledujejo notranja pravila drugega overitelja ter njegovo izpolnjevanje varnostnih zahtev.

(4) Stroške potrebne infrastrukture, ki jo zahteva overitelj na MJU za medsebojno priznavanje, krije drugi overitelj.

3.3. Preverjanje imetnikov za ponovno izdajo potrdila

3.3.1 Preverjanje imetnikov pri podaljšanju potrdil

(1) Podaljšanje posebnih potrdil se vrši po protokolu PKIX-CMP, kjer imetnik izkaže svojo istovetnost s posedovanjem še veljavnega zasebnega ključa.

(2) Pri ponovni izdaji spletnega potrdila pa je potrebno ponovno preveriti istovetnost imetnika po postopku, navedenem v razd. 3.2.3.

3.3.2 Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu

Preverjanje imetnikov poteka skladno z določili iz razd. 3.2.3.

3.4. Preverjanje istovetnosti ob zahtevi za preklic

(1) Zahtevek za preklic potrdila imetnik oz. predstojnik odda:
- osebno na prijavno službo, kjer pooblaščene 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 SIGOV-CA mora imetnik navesti v ta namen izbrano geslo.

(3) Podroben postopek za preklic je podan v razd. 4.9.3.

4. UPRAVLJANJE S POTRDILI

4.1. Pridobitev potrdila

4.1.1 Kdo lahko pridobi potrdilo

Bodoči imetniki potrdil so vedno fizične osebe, zaposlene v organizaciji, za katere le-ta želi pridobiti potrdilo. V primeru potrdila za strežnike oz. informacijske sisteme, splošne nazive in podpis kode je imetnik takega potrdila pooblaščen s strani predstojnika, v primeru potrdila za izdajatelja varnih časovnih žigov in druge izdajatelje pa predstojnik organizacije izdajatelja varnih časovnih žigov oz. drugega izdajatelja oz. od predstojnika pooblaščena oseba. Podrobno o tem že v razd. 1.3.3.

4.1.2 Postopek bodočega imetnika za pridobitev potrdila in odgovornosti

(1) Za pridobitev potrdila morata bodoči imetnik in predstojnik pravilno izpolniti in podpisati zahtevek za pridobitev potrdila.

(2) Zahtevki za pridobitev so dostopni na prijavnih službah oz. pri drugih pooblaščenih osebah izdajatelja SIGOV-CA in na spletnih straneh SIGOV-CA.

(3) Bodoči imetnik in predstojnik sta za pridobitev potrdila dolžna:
- izpolniti zahtevek za pridobitev potrdila z resničnimi in pravilnimi podatki,
- ga na varen način posredovati na prijavno službo,
- opraviti prevzem potrdila na varen način po navodilih izdajatelja SIGOV-CA v primeru, da bodoči imetnik sam prevzame digitalno potrdilo.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

4.2.1 Preverjanje istovetnosti bodočega imetnika

(1) Predstojnik organizacije, kjer je bodoči imetnik potrdila zaposlen, jamči za istovetnost bodočega imetnika potrdila, ki ga je preveril v skladu z 31. členom in drugimi določili ZEPEP.

(2) Izdajatelj SIGOV-CA preveri istovetnost bodočega imetnika oz. vse podatke o bodočem imetniku in organizaciji, 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 iz dogovora s strani organizacije zavrnejo pooblaščene osebe overitelja na MJU.

(2) O odobritvi oz. zavrnitvi je bodoči imetnik obveščen po e-pošti.

(3) V primeru odobritve izdajatelj SIGOV-CA pred izdajo potrdila obvesti predstojnika in bodočega imetnika z vso potrebno dokumentacijo v skladu s 36. členom ZEPEP.

4.3. Postopek po odobritvi zahtevka za pridobitev potrdila

4.3.1 Postopek izdajatelja SIGOV-CA z obvezno uporabo pametne kartice

V primeru odobrenega zahtevka SIGOV-CA ravna skladno z Interno politiko delovanja overitelja na MJU.

4.3.2 Postopek izdajatelja SIGOV-CA brez obvezne uporabe pametne kartice

(1) V primeru odobrenega zahtevka SIGOV-CA posreduje bodočemu imetniku potrdila referenčno številko (angl. *reference number*) in avtorizacijsko kodo (angl. *authorization code*) po dveh ločenih poteh: referenčno številko po elektronski pošti, avtorizacijsko kodo pa s poštno pošiljko, izjemoma pa ju lahko pooblaščena oseba SIGOV-CA preda tudi osebno. Oba podatka bodoči imetnik potrebuje za prevzem digitalnega potrdila.

(2) SIGOV-CA bodočemu imetniku avtorizacijsko kodo in referenčno številko posreduje najkasneje v desetih (10) dneh od odobritve zahtevka.

4.3.3 Postopek izdajatelja SIGOV-CA - splošno

Potrdila se izdajajo izključno na infrastrukturi overitelja na MJU.

4.3.4 Obvestilo imetnika o izdaji

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

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila z obvezno uporabo pametne kartice

(1) V primeru odobrenega zahtevka SIGOV-CA za bodočega imetnika na svoji infrastrukturi opravi prevzem kvalificiranega digitalnega potrdila z uporabe pametno kartico. SIGOV-CA nato pametno kartico s prevzetim digitalnim potrdilom preko kontaktne osebe organizacije, ki je zaprosila za imetnikovo potrdilo, posreduje bodočemu imetniku.

(2) Prednastavljeno geslo za dostop do digitalnega potrdila se imetniku posreduje s poštno pošiljko z oznako »Osebno« na naslov njegove organizacije.

(3) Podrobnosti postopka so določene v z Interno politiko delovanja overitelja na MJU.

(4) Imetnik mora takoj po prevzemu pametne kartice, na katerem je že prevzeto potrdilo, preveriti podatke v tem potrdilu. Če izdajatelja SIGOV-CA nemudoma ne obvesti o morebitnih napakah, se smatra, da se z vsebino strinja in da soglaša s pogoji delovanja ter prevzemom obveznosti in odgovornosti.

(5) SIGOV-CA bodočemu imetniku pametno kartico skupaj z digitalnim potrdilom in navodili za ravnanje na varen

način posreduje najkasneje v desetih (10) dneh od odobritve zahtevka.

4.4.2 Postopek prevzema potrdila brez obvezne uporabe pametne kartice

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

(2) Način in podrobna navodila za prevzem vseh vrst potrdil po tej politiki so opisana na spletni strani http://www.sigov-ca.gov.si. Prav tako so na spletni strani objavljene tudi vse novosti v zvezi z načinom prevzema potrdil.

(3) Imetnik mora takoj po prevzemu potrdila preveriti podatke v tem potrdilu. Če izdajatelja SIGOV-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 SIGOV-CA rezervacijo potrdila prekliče.

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

4.4.3 Objava potrdila

Glede objave potrdila glej pogl. 2.

4.5. Obveznosti in odgovornosti uporabnikov glede uporabe potrdil

4.5.1 Obveznosti imetnika potrdila oziroma organizacije

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:
- seznaniti se in ravnati v skladu s politiko in dogovorom med organizacijo in overiteljem na MJU pred izdajo potrdila,
- ravnati v skladu s politiko in določili iz morebitnega dogovora med organizacijo in overiteljem na MJU in ostalimi veljavnimi predpisi,
- če po oddaji zahtevka za pridobitev potrdila oz. drugo storitev od izdajatelja SIGOV-CA ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, se mora obrniti na pooblaščene osebe izdajatelja SIGOV -CA,
- po prejemu oz. po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SIGOV-CA oziroma zahtevati preklic potrdila,
- spremljati vsa obvestila SIGOV-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 SIGOV-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 SIGOV-CA,
- skrbeti za originalno podpisane dokumente in arhiv teh dokumentov.

(2) Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnih ključev dolžan tudi:
- podatke za prevzem potrdila skrbno varovati pred nepooblaščenimi osebami,

- hraniti zasebne ključe in potrdilo na način v skladu z obvestili in priporočili SIGOV-CA,
- zasebne ključe in vse druge zaupne podatke ščititi s primernim geslom v skladu s priporočili SIGOV-CA ali na drug način tako, da ima dostop do njih samo imetnik,
- skrbno varovati gesla za zaščito zasebnih ključev,
- po preteku veljavnosti oz. preklicu potrdila ravnati v skladu z obvestili SIGOV-CA.

(3) Predstojnik oz. organizacija je dolžna:
- skrbno prebrati politiko in določila iz dogovora med organizacijo in overiteljem na MJU pred podpisom zahtevka za pridobitev potrdila,
- zagotoviti, da imetniki potrdil za njegovo organizacijo izpolnjujejo vse zahteve iz te politike in veljavnih predpisov,
- redno spremljati vsa obvestila SIGOV-CA,
- ravnati v skladu z obvestili, politiko in dogovorom med organizacijo in overiteljem na MJU in ostalimi veljavnimi predpisi,
- zagotoviti, da imetniki potrdil ustrezno posodabljajo potrebno strojno in programsko opremo za varno delo s potrdili,
- skrbeti za arhiv elektronskih dokumentov ter potrebnih podatkov za uporabo potrdil,
- vse spremembe glede imetnika in organizacije, ki so povezane s potrdilom imetnika, nemudoma sporočiti SIGOV-CA,
- zahtevati preklic potrdila, če so bili zasebni ključi imetnika potrdila ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

4.5.2 Obveznosti za tretje osebe

(1) Tretja oseba, ki se zanaša na potrdilo, mora:
- ravnati in uporabljati potrdila v skladu in namenom s politiko in ostalimi veljavnimi predpisi,
- skrbno proučiti vse možnosti tveganja in odgovornosti pri uporabi potrdil in določiti politiko za način uporabe,
- obvestiti SIGOV-CA, če izve, da so bili zasebni ključi imetnika potrdila, na katerega se zanaša, 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,
- se zanašati na potrdilo samo za namen, določen v potrdilu (glej razd. 6.1.7), in na način, ki je določen s politiko,
- v času uporabe potrdila preveriti, če potrdilo ni v registru preklicanih potrdil,
- 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 SIGOV-CA, ki je objavljen v tej politiki in tudi na spletnih straneh SIGOV-CA oz. drugih izdajateljev potrdil overitelja na MJU,
- upoštevati druge določbe, če je z overiteljem na MJU oz. izdajateljem SIGOV-CA sklenila dogovor o uporabi potrdil.

(2) 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.

4.6. Ponovna izdaja potrdila brez spremembe javnega ključa

Postopek izdaje novega potrdila brez spremembe javnega ključa oz. drugega podatka v potrdilu s strani izdajatelja SIGOV-CA ni podprta.

4.7. Regeneriranje ključev - velja samo za posebna potrdila

4.7.1 Razlogi za regeneracijo

(1) Regeneriranje ključev za posebno potrdilo se izvede, če imetnik potrdila:
- pozabi geslo za dostop do zasebnih ključev in nima možnosti odklepanja pametne kartice,
- izgubi ali poškoduje nosilce za hrambo ključnih podatkov za uporabo potrdila,
- nima omogočenega avtomatičnega podaljševanja veljavnosti potrdila,
- ni izvedel dostopa do svojega potrdila tako dolgo, da mu je potekla veljavnost ključa za digitalno podpisovanje in s tem dostop do potrdila.

(2) Overitelj na MJU si glede na varnostne okoliščine pridržuje samostojno odločitev med:
- regeneriranjem ključev
- ali preklicem.

(3) Regeneriranje ključev posebnih potrdil, izdanih pred 11.1.2016 in podpisanih s potrdilom št. 1 izdajatelja SIGOV-CA, je dovoljeno le za potrebe dostopa do zgodovine ključev za dešifriranje po predhodnem dogovoru z izdajateljem SIGOV-CA. Postopek se lahko izvaja le do poteka veljavnosti potrdila št. 1 izdajatelja SIGOV-CA tj. do 10.1.2021.

4.7.2 Kdo zahteva regeneracijo

Regeneracijo lahko zahteva imetnik potrdila skupaj predstojnikom.

4.7.3 Postopek za izdajo zahtevka za regeneracijo z obvezno uporabo pametne kartice

(1) Regeneriranje ključev za potrdila se izvede na osnovi izpolnjenega zahtevka za regeneriranje ključev s strani imetnika potrdila ter predstojnika, ki se odda na prijavni službi SIGOV-CA.

(2) Kot pri izdaji novega potrdila prejme imetnik pametno kartico z digitalnim potrdilom, ki ga je na svoji infrastrukturi na podlagi zahtevka za regeneracijo za imetnika regeneriral izdajatelj SIGOV-CA.

(3) Potrdilo za overjanje podpisa, ki se izda zaradi postopka regeneracije, vsebuje enako razločevalno ime kot prvotno potrdilo.

(4) SIGOV-CA posreduje imetniku pametno kartico skupaj z regeneriranim digitalnim potrdilom oz. regeneriranimi ključi ter navodili za ravnanje na varen način najkasneje v desetih (10) dneh od obravnave zahtevka za regeneracijo (razd. 4.7.1).

4.7.4 Postopek za izdajo zahtevka za regeneracijo brez obvezne uporabe pametne kartice

(1) Regeneriranje ključev za potrdila se izvede na osnovi izpolnjenega zahtevka za regeneriranje ključev s strani imetnika potrdila ter predstojnika, ki se odda na prijavni službi SIGOV-CA.

(2) Kot pri izdaji novega potrdila prejme imetnik referenčno številko in avtorizacijsko kodo za dostop do para ključev za šifriranje in generiranje novega para ključev za podpisovanje.

(3) SIGOV-CA imetniku avtorizacijsko kodo in referenčno številko posreduje najkasneje v desetih (10) dneh od obravnave zahtevka za regeneracijo (razd. 4.7.1).

(4) Regeneracijo mora imetnik opraviti v šestdesetih (60) dneh od rezervacije potrdila. Na zahtevo imetnika je možno čas za regeneracijo podaljšati za novih šestdesetih (60), sicer SIGOV-CA rezervacijo potrdila prekliče.

(5) Po opravljeni regeneraciji postaneta referenčna številka in avtorizacijska koda neuporabni.

4.8. Sprememba potrdila

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

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

4.8.1 Okoliščina za spremembo potrdila

Ni podprta.

4.8.2 Kdo zahteva spremembo

Ni podprto.

4.8.3 Postopek ob zahtevku za spremembo

Ni podprt.

4.8.4 Obvestilo o izdaji novega potrdila

Ni podprto.

4.8.5 Prevzem spremenjenega potrdila

Ni podprt.

4.8.6 Objava spremenjenega potrdila

Ni podprta.

4.8.7 Obvestilo drugih subjektov o spremembi

Ni podprto.

4.9. Preklic in suspenz potrdila

4.9.1 Razlogi za preklic

(1) Preklic potrdila morata imetnik ali predstojnik organizacije zahtevati v primeru:
- če so bili zasebni ključi imetnika potrdila ogroženi na način, ki vpliva na zanesljivost uporabe,
- če obstaja nevarnost zlorabe zasebnih ključev ali potrdila imetnika,
- če so se spremenili oz. so napačni ključni podatki, navedeni v potrdilu,
- če imetnik ni več zaposlen v organizaciji ali je prenehal z delom za organizacijo ali ni več pooblaščen za uporabo potrdila.

(2) Izdajatelj SIGOV-CA prekliče potrdilo tudi brez zahteve imetnika ali predstojnika organizacije takoj, ko izve:
- da je imetnik potrdila prenehal delati v ali za organizacijo,
- 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 prijavni službi,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- za neizpolnjevanje obveznosti imetnika oz. organizacije iz te politike in dogovora med organizacijo in overiteljem na MJU,
- da niso poravnani stroški za upravljanje digitalnih potrdil,
- da je bila infrastruktura overitelja na MJU ogrožena na način, ki vpliva na zanesljivost potrdila,
- da so bili zasebni ključi imetnika potrdila ogroženi na način, ki vpliva na zanesljivost uporabe,
- da bo SIGOV-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 zahteva preklic

Preklic potrdila lahko zahteva:
- pooblaščena oseba izdajatelja SIGOV-CA,
- predstojnik organizacije,
- imetnik,
- pristojno sodišče ali
- upravni organ.

4.9.3 Postopki za preklic

(1) Preklic lahko imetnik zahteva:
- osebno v poslovnem času na prijavni službi,
- elektronsko po elektronski pošti štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila sicer v poslovnem času,
- telefonsko štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila, sicer v poslovnem času.

(2) Preklic lahko predstojnik organizacije zahteva:
- osebno v poslovnem času,
- elektronsko po elektronski pošti štiriindvajset (24) ur na dan vse dni v letu.

(3) Če se preklic zahteva:
- osebno, je potrebno izpolniti ustrezen zahtevek za preklic potrdila ter ga oddati na prijavno službo;
- elektronsko, mora imetnik ali predstojnik organizacije poslati na SIGOV-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 SIGOV-CA na dežurno telefonsko

številko za preklice (glej razd. 1.3.1);
- telefonsko, mora imetnik poklicati na dežurno telefonsko številko za preklice (glej razd. 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 SIGOV-CA. Brez gesla za preklic imetnik ne more telefonsko preklicati potrdila.

(4) O datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic morata biti vedno obveščena imetnik in predstojnik.

(5) Sodišča in upravni organi, ki tudi lahko zahtevajo preklic, storijo to 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 poslovnem času (glej naslednji razdelek).

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 prekliče 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 potrdil[9].

4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

Tretje osebe, ki se zanašajo na potrdilo, morajo pred uporabo preveriti najnovejši objavljeni register preklicanih potrdil. Zaradi verodostojnosti in celovitosti je vedno potrebno preveriti tudi verodostojnost tega registra, ki je digitalno podpisan s strani SIGOV-CA.

4.9.7 Pogostnost objave registra preklicanih potrdil

Register preklicanih potrdil se osvežuje (za dostop do registra glej razd. 7.2.3):
- 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 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.

[9] V javnem imeniku ostanejo samo evidenčni podatki o potrdilu.

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.

4.9.11 Drugi načini za dostop do statusa potrdil

Niso podprti.

4.9.12 Posebne zahteve pri zlorabi zasebnega ključa

Niso določene.

4.9.13 Razlogi za suspenz

Ni podprto.

4.9.14 Kdo zahteva suspenz

Ni podprto.

4.9.15 Postopek za suspenz

Ni podprto.

4.9.16 Čas suspenza

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*, podrobnosti o dostopu pa so v podpogl. 7.2 in 7.3.

4.10.2 Razpoložljivost

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

4.10.3 Druge informacije za preverjanje statusa

Niso predpisane.

4.11. Prekinitev razmerja med imetnikom in overiteljem

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 - velja za posebna potrdila

4.12.1 Razlogi za odkrivanje kopije ključev za dešifriranje

(1) SIGOV-CA hrani zgodovino ključev za dešifriranje in odkrije njihovo kopijo le v izjemnih primerih, ko le-ti iz kakršnegakoli razloga niso dostopni, za dostop do službenih podatkov, ki so zašifrirani in dostopni le z imetnikovim ključem za dešifriranje.

(2) SIGOV-CA si pridružuje pravico, da ne odobri odkritja kopije ključev za dešifriranje, če gre za potrdilo, ki je bilo preklicano zaradi napačnih podatkov v potrdilu.

(3) Odkrivanje kopije ključev za dešifriranje za potrdila, izdana pred 11.1.2016 in podpisana s potrdilom št. 1 izdajatelja SIGOV-CA, se lahko izvaja le do poteka veljavnosti potrdila št. 1 izdajatelja SIGOV-CA tj. do 10.1.2021.

4.12.2 Kdo zahteva odkrivanje kopije ključev za dešifriranje

Kopijo ključev za dešifriranje lahko zahteva:
- predstojnik na podlagi zahtevka za odkrivanje kopije ključev za dešifriranje za dostop do podatkov, ki so zašifrirani in dostopni z imetnikovim ključem za dešifriranje,
- če to odredi pristojno sodišče ali upravni organ.

4.12.3 Postopek ob zahtevku za odkrivanje kopije ključev za dešifriranje

(1) Predstojnik mora izpolniti zahtevek za odkrivanje kopije ključev za dešifriranje in ga na varen način posredovati na SIGOV-CA.

(2) SIGOV-CA pred odkrivanjem kopije ključev za dešifriranje:
- po elektronski pošti obvesti imetnika potrdila o datumu ter izdajatelju zahtevka za odkrivanje kopije njegovih ključev za dešifriranje podatkov, in
- prekliče veljavnost potrdila in po elektronski pošti o preklicu obvesti imetnika.

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 na MJU

(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 na MJU

(1) Dostop do infrastrukture overitelja na MJU oz. izdajatelja je omogočen samo pooblaščenim osebam overitelja na MJU skladno z njihovimi nalogami in pooblastili, glej razd. 5.2.1.

(2) Vsi dostopi so varovani v skladu z zakonodajo in priporočili.

(3) Podrobna določila so v Interni politiki overitelja na MJU.

5.1.3 Napajanje in prezračevanje

(1) Infrastruktura overitelja 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, razen v primeru višje sile.

(2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.5 Zaščita pred požari

(1) Prostori overitelja 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) Nosilci podatkov, bodisi v papirnati ali elektronski obliki, se hranijo varno v zaščitenih 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 razd. 5.1.6.

5.2. Organizacijska struktura izdajatelja oz. overitelja

5.2.1 Skupine overitelja na MJU

(1) Operativno, organizacijsko in strokovno pravilno delovanje overitelja na MJU vodi pooblaščena oseba 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.

(2) Med pooblaščene osebe overitelja na MJU spadajo
- zaposleni pri overitelju na MJU in
- prijavne službe.

(3) Zaposleni pri overitelju na MJU so razporejeni v štiri organizacijske skupine, ki pokrivajo naslednja vsebinska področja:
- upravljanje z informacijskim sistemom,
- upravljanje s kvalificiranimi potrdili,
- varovanje in kontrola,
- pravno-administrativno.

Organizacijska skupina	Vloga	Osnovne naloge	Število oseb
Upravljanje z informacijskim sistemom	Upravljavec sistema	– Strategija delovanja overitelja na MJU – Določevanje prvega varnostnega inženirja – Operativno vodenje overitelja na MJU	2
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
Varovanje in kontrola	Varnostni administrator	– Upravljanje s telekomunikacijami (sistem za preprečevanje in odkrivanje vdorov,	1

		požarna pregrada, ...) – Vzdrževanje varnostnih kopij	
Pravno-administrativno	Pravnik		1

5.2.2 Število oseb za posamezne naloge

(1) Posamezne občutljive naloge mora skladno z Uredbo in Interno politiko delovanja overitelja na MJU opravljati več oseb hkrati. Med te spadajo:
- regeneriranje ključev,
- odkrivanje kopije ključev za dešifriranje ter
- druge naloge, določene z Interno politiko delovanja overitelja na MJU.

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

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

5.2.3 Izkazovanje istovetnosti za opravljanje posameznih nalog

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

5.2.4 Nezdružljivost nalog

(1) Vse organizacijske skupine overitelja na MJU, navedene v tabeli razd. 5.2.1, so med seboj nezdružljive.

(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 Uredbo so podrobnejša določila glede nadzora osebja določena v Interni politiki overitelja na MJU.

5.3.1 Potrebne kvalifikacije in izkušnje osebja

Osebje overitelja na MJU ima skladno z zahtevami ZEPEP in Uredbo ustrezne kvalifikacije in izkušnje.

5.3.2 Primernost osebja

Osebje overitelja na MJU ima skladno z zahtevami ZEPEP in Uredbo ustrezne kvalifikacije in izkušnje.

5.3.3 Dodatno izobraževanje osebja

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

5.3.4 Zahteve za redna usposabljanja

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

5.3.5 Menjava nalog

Ni predpisana.

5.3.6 Sankcije

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

5.3.7 Zahteve za zunanje izvajalce

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

5.3.8 Dostop osebja do dokumentacije

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

5.4. Varnostni pregledi sistema

5.4.1 Vrste dnevnikov

(1) Izdajatelj SIGOV-CA skladno z Uredbo preverja vse, kar določa:
- varnost infrastrukture,
- nemoteno delovanje vseh varnostnih 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 Uredbo določeni v Interni politiki overitelja na MJU.

5.4.2 Pogostost pregledov dnevnikov

Izdajatelj SIGOV-CA opravlja varnostne preglede svoje infrastrukture oz. dnevnikov dnevno.

5.4.3 Čas hrambe dnevnikov

Dnevniki se hranijo trajno.

5.4.4 Zaščita dnevnikov

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

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

5.4.5 Varnostne kopije dnevnikov

(1) Varnostne kopije dnevnikov se izvajajo dnevno.

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

5.4.6 Zbiranje podatkov za dnevnike

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

(2) Podrobnosti so v skladu z Uredbo 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) Analiza dnevnikov in nadzor nad izvajanjem vseh postopkov se izvaja redno s strani pooblaščenih oseb overitelja na MJU ali pa avtomatsko z drugimi varnostnimi mehanizmi na vseh računalniško-komunikacijskih napravah v pristojnosti overitelja na MJU.

(2) Ocena ranljivosti se izvaja na podlagi analize dnevnikov.

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

5.5. Arhiviranje podatkov

5.5.1 Vrste arhivskih podatkov

Izdajatelj SIGOV-CA skladno z Uredbo hrani naslednje podatke oz. dokumente:
- dnevnike,
- zapisnike,
- vsa dokazila o opravljenem preverjanju istovetnosti imetnikov in organizacij,
- vse zahtevke,
- potrdila in register preklicanih potrdil,
- politike delovanja,
- objave in obvestila SIGOV-CA,

- zasebne ključe za dešifriranje v skladu z razd. 6.1.1 ter
- druge dokumente v skladu z veljavnimi predpisi.

5.5.2 Čas hrambe

Izdajatelj SIGOV-CA arhivske podatke hrani skladno z veljavno zakonodajo in predpisi.

5.5.3 Zaščita arhivskih podatkov

(1) Arhivski podatki so varno shranjeni.

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

5.5.4 Varnostna kopija arhiva

(1) Kopija arhivskih podatkov se varno hrani.

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

5.5.5 Zahteva po časovnem žigosanju

Ni predpisana.

5.5.6 Način zbiranja podatkov

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

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

5.5.7 Postopek za dostop do arhivskih podatkov in njihova verifikacija

(1) Dostop do arhivskih podatkov je možen samo pooblaščenim osebam.

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

5.6. Podaljšanje veljavnosti potrdil

5.6.1 Podaljševanje veljavnosti posebnih potrdil

(1) Podaljševanje veljavnosti potrdil za posebna potrdila: generiranje novih parov ključev in podaljševanje veljavnosti posebnega potrdila se izvaja avtomatsko po varnem protokolu PKIX-CMP ob prvi uporabi potrdila imetnika z neposrednim dostopom do infrastrukture SIGOV-CA v obdobju stotih (100) dni pred zadnjim dnem veljavnosti potrdila.

(2) Posebno potrdilo, katerega veljavnost se podaljša, vsebuje enako razločevalno ime kot prvotno potrdilo.

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

(4) Podaljševanje veljavnosti posebnih potrdil, izdanih pred 11.1.2016 in podpisanih s potrdilom št. 1 izdajatelja SIGOV-CA, ni podprto.

5.6.2 Podaljševanje veljavnosti spletnih potrdil

(1) Spletna potrdila se ne podaljšujejo avtomatsko. Potrebno je ponoviti postopek za pridobitev novega potrdila.

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

5.6.3 Podaljšanje veljavnosti potrdila izdajatelja SIGOV-CA

V primeru novega izdanega potrdila izdajatelja SIGOV-CA se postopek objavi na spletnih straneh SIGOV-CA.

5.7. Okrevalni načrt

5.7.1 Postopek v primeru vdorov in zlorabe

V skladu z Uredbo je to določeno v Interni politiki delovanja overitelja na MJU.

5.7.2 Postopek v primeru okvare programske opreme, podatkov

V skladu z Uredbo je to določeno v Interni politiki delovanja overitelja na MJU.

5.7.3 Postopek v primeru ogroženega zasebnega ključa izdajatelja SIGOV-CA

V skladu z Uredbo je to določeno v Interni politiki delovanja overitelja na MJU.

5.7.4 Okrevalni načrt

V skladu z Uredbo je to določeno v Interni politiki delovanja overitelja na MJU.

5.8. Prenehanje delovanja SIGOV-CA

Če bo overitelj na MJU prenehal z opravljanjem svoje dejavnosti ali izdajatelj SIGOV-CA prenehal z izdajanjem potrdil, bo overitelj na MJU ukrepal v skladu z ZEPEP.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev ključev

6.1.1 Generiranje ključev

(1) Generiranje para ključev izdajatelja SIGOV-CA za podpisovanje in overjanje je formalen in kontroliran postopek ob namestitvi programske opreme SIGOV-CA, o katerem se vodi poseben zapisnik (dokument »Zapisnik postopka generiranja ključev izdajatelja SIGOV-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 nastavitev informacijskega sistema SIGOV-CA, ki so opravljene ob vzpostavitvi sistema, se dokumentirajo v posebnem zapisniku oz. v ustreznem dnevniku.

(4) Za generiranje para ključev izdajatelja SIGOV-CA se uporabi strojni varnostni modul (glej razd. **Napaka! Vira sklicevanja ni bilo mogoče najti.**).

(2) Ključi imetnikov se generirajo odvisno od vrste potrdila v skladu s spodnjo tabelo.

Tip potrdila	Potrdilo	Ključ se generira
posebno za zaposlene in splošne nazive z obvezno uporabo pametne kartice	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	z uporabo imetnikove pametne kartice na infrastrukturi izdajatelja SIGOV-CA
	par ključev za dešifriranje/šifriranje (potrdilo za šifriranje)	pri izdajatelju SIGOV-CA
posebno za zaposlene in splošne nazive brez obvezne uporabe pametne kartice	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	pri imetniku
	par ključev za dešifriranje/šifriranje (potrdilo za šifriranje)	pri izdajatelju SIGOV-CA
spletno za zaposlene in splošne nazive z obvezno uporabo pametne kartice	par ključev za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	z uporabo imetnikove pametne kartice na infrastrukturi izdajatelja SIGOV-CA
spletno za strežnike ter zaposlene in splošne nazive brez obvezne uporabe pametne kartice	par ključev za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	pri imetniku
potrdilo za podpis kode	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	pri imetniku
potrdilo za izdajatelja TSA	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	pri izdajatelju TSA
potrdilo za sistem OCSP	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	v sistemu OCSP

6.1.2 Dostava zasebnega ključa imetnikom

Način varnega prenosa zasebnega ključa je podan v spodnji tabeli.

Tip potrdila	Potrdilo	Ključ	Dostava
posebno z obvezno uporabo pametne kartice	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	zasebni ključ za podpisovanje	pri generiranju digitalnega potrdila ni prenosa[10]; pametno kartico z digitalnim potrdilom in zasebnim ključem imetnik prejme preko kontaktne osebe svoje organizacije
	par za dešifriranje/šifriranje (potrdilo za šifriranje)	zasebni ključ za dešifriranje	pri generiranju digitalnega potrdila prenos od izdajatelja do imetnikove pametne kartice po PKIX-CMP; pametno kartico z digitalnim potrdilom in zasebnim ključem imetnik prejme preko kontaktne osebe svoje organizacije
posebno brez obvezne uporabe pametne kartice	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	zasebni ključ za podpisovanje	ni prenosa
	par za dešifriranje/šifriranje (potrdilo za šifriranje)	zasebni ključ za dešifriranje	prenos od izdajatelja do imetnika po PKIX-CMP
spletno z obvezno uporabo pametne kartice	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	pri generiranju digitalnega potrdila ni prenosa[11]; pametno kartico z digitalnega potrdilom in zasebnim ključem imetnik prejme preko kontaktne osebe svoje organizacije
spletno brez obvezne uporabe pametne kartice	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	ni prenosa

6.1.3 Dostava javnega ključa izdajatelju potrdil[12]

V postopku prevzema potrdila se javni ključ dostavi izdajatelju SIGOV-CA po protokolu PKIX-CMP za posebna potrdila in protokolu PKCS#7 za spletna potrdila.

6.1.4 Dostava izdajateljevega javnega ključa

Potrdilo z javnim ključem izdajatelja SIGOV-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.sigov-ca.gov.si/cda-cgi/clientcgi?action=caCert,
- v obliki PEM na naslovu https://www.sigov-ca.gov.si/sigov-ca2.pem,
- v obliki PEM na naslovu http://www.sigov-ca.gov.si/sigov-ca2.pem, pri čemer mora dodatno preveriti

[10] Ključ se generira z uporabo imetnikove pametne kartice na infrastrukturi izdajatelja SIGOV-CA.
[11] Ključ se generira z uporabo imetnikove pametne kartice na infrastrukturi izdajatelja SIGOV-CA.
[12] RFC 3647 ne predvideva opisa načina dostave potrdil imetnikom.

verodostojnost potrdila,
- pri potrdilih brez obvezne uporabe pametne kartice preko protokola PKIX-CMP za posebna potrdila in PKCS#7 za spletna potrdila.

6.1.5 Dolžina ključev

Potrdilo	Dolžina ključa po RSA [bit]
potrdilo izdajatelja SIGOV-CA	3072
potrdilo za: • zaposlene • splošne nazive • strežnike • podpis kode • sisteme OCSP	2048[13]
potrdilo za izdajatelje TSA	2048

6.1.6 Generiranje in kakovost parametrov javnih ključev

Kvaliteta parametrov ključa izdajatelja SIGOV-CA je zagotovljena s strani proizvajalca programske opreme z uporabo kvalitetnih generatorjev naključnih števil (angl. *random number generator*).

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)*.

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

(3) Profil različnih vrst potrdil imetnikov je podan v podpogl. 7.1.

6.2. Zaščita zasebnega ključa

6.2.1 Standardi za kriptografski modul

Zasebni ključ izdajatelja SIGOV-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 SIGOV-CA so v skladu z Uredbo določena v Interni politiki overitelja na MJU.

[13] Vrednost pomeni minimalno predpisano dolžino.

6.2.3 Odkrivanje kopije zasebnega ključa (angl. *Key Escrow*)

(1) SIGOV-CA odkriva kopije zasebnega ključa za dešifriranje za posebna potrdila, za katere se skladno z določili iz razd. 6.1.1 generira ključ na strani izdajatelja SIGOV-CA.

(2) Postopek za odkrivanje kopije zasebnega ključa za dešifriranje za posebna potrdila je določen v podpogl. 4.12.

6.2.4 Varnostna kopija zasebnega ključa

Varnostne kopije zasebnih ključev za dešifriranje posebnih potrdil (skladno z določili iz razd. 6.1.1) se hranijo v šifriranih bazah SIGOV-CA, se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih.

6.2.5 Arhiviranje zasebnega ključa

SIGOV-CA arhivira kopije zasebnih ključev za dešifriranje posebnih potrdil (skladno z določili iz razd. 6.1.1), kot je to določeno v podpogl. 5.5.

6.2.6 Zapis zasebnega ključa v kriptografski modul

(1) Zasebni ključi za dešifriranje posebnih potrdil imetnikov se iz mesta, kjer se ustvarijo, t.j. pri izdajatelju SIGOV-CA, prenesejo po protokolu PKIX-CMP:
- k imetniku pri potrdilih brez obvezne uporabe pametne kartice,
- na imetnikovo pametno kartico pri potrdilih z obvezno uporabo pametne kartice.

(2) Ostali zasebni ključi imetnikov se tvorijo:
- pri imetniku pri potrdilih brez obvezne uporabe pametne kartice,
- z uporabo imetnikove pametne kartice na infrastrukturi izdajatelja SIGOV-CA pri potrdilih z obvezno uporabo pametne kartice.

6.2.7 Postopek za aktiviranje zasebnega ključa

(1) Aktiviranje zasebnega ključa izdajatelja SIGOV-CA poteka v skladu z določili Interne politike overitelja na MJU.

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

6.2.8 Postopek za deaktiviranje zasebnega ključa

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

6.2.9 Postopek za uničenje zasebnega ključa

(1) Postopek za uničenje zasebnega ključa izdajatelja SIGOV-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.

6.3. Ostali aspekti upravljanja ključev

6.3.1 Arhiviranje javnega ključa

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

6.3.2 Obdobje veljavnosti za javne in zasebne ključe

Veljavnost potrdil in ključev je podana po spodnji tabeli.

Tip potrdila	Par ključev	Ključi	Veljavnost
posebno potrdilo za zaposlene in splošne nazive	par za digitalno podpisovanje/overjanje (posebno potrdilo – za overjanje podpisa)	zasebni ključ za podpisovanje	5 let
		javni ključ za overjanje podpisa	5 let
	par za dešifriranje/šifriranje (posebno potrdilo – za šifriranje)	zasebni ključ za dešifriranje	5 let
		javni ključ za šifriranje	5 let
spletno potrdilo za zaposlene, splošne nazive in podpis kode	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	5 let
		javni ključ	5 let
spletno potrdilo za strežnike	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	3 leta
		javni ključ	3 leta
potrdilo za izdajatelja TSA	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	zasebni ključ	3 leta
		javni ključ	5 let
potrdilo za sistem OCSP	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	zasebni ključ	5 let
		javni ključ	5 let

6.4. Gesla za dostop do potrdil oz. ključev

6.4.1 Generiranje gesel

(1) Aktivacijska podatka, t.j. referenčna številka in avtorizacijska koda, ki sta potrebna za prevzem potrdila, se ustvarita na strani SIGOV-CA. Podatka sta unikatna.

(2) Potrdila z obvezno uporabo pametne kartice so zaščitena s prednastavljenim geslom, ki se generira ob prevzemu potrdila. Prednastavljeno geslo mora imetnik spremeniti pred prvo uporabo potrdila.

(3) Imetniki sami določijo geslo, s katerim zaščitijo dostop do svojih zasebnih ključev.

(4) SIGOV-CA priporoča uporabo varnih gesel:
- mešano uporaba velikih in malih črk, številk in posebnih znakov,

- dolžine vsaj 8 znakov,
- odsvetuje se uporabo besed, ki so zapisane v slovarjih.

6.4.2 Zaščita gesel

(1) Aktivacijska podatka za prevzem potrdila se kreirata varno pri izdajatelju SIGOV-CA.

(2) Pri potrdilih brez obvezne uporabe pametne kartice SIGOV-CA posreduje bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo po dveh ločenih poteh:
- referenčno številko po elektronski pošti,
- avtorizacijsko kodo s poštno pošiljko,
- izjemoma pa ju preda tudi osebno.

(3) Do prevzema potrdila mora bodoči imetnik skrbno varovati aktivacijska podatka za prevzem potrdila, po prevzemu potrdila postaneta neuporabna in ju imetnik lahko zavrže.

(4) Pri potrdilih z obvezno uporabo pametne kartice SIGOV-CA posreduje bodočemu imetniku potrdila pametno kartico z digitalnim potrdilom in prednastavljeno geslo po dveh ločenih poteh:
- pametno kartico z dig. potrdilom preko kontaktne osebe njegove organizacije,
- prednastavljeno geslo s poštno pošiljko z oznako »Osebno« na naslov njegove organizacije.

(5) Prednastavljeno geslo mora imetnik spremeniti pred prvo uporabo potrdila.

(6) SIGOV-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.

(7) SIGOV-CA imetnikom priporoča, da sami poskrbijo za zamenjavo gesla vsaj vsakih šest (6) mesecev.

6.4.3 Drugi aspekti gesel

Niso predpisani.

6.5. Varnostne zahteve za računalniško opremo izdajatelja

6.5.1 Specifične tehnične varnostne zahteve

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

6.5.2 Nivo varnostne zaščite

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

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1 Nadzor razvoja sistema

SIGOV-CA uporablja programsko opremo proizvajalca Entrust, ki je certificirana v skladu s FIPS 140-1 nivo 2 in

Common Criteria EAL4+.

6.6.2 Upravljanje varnosti

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

6.7. Varnostne kontrole računalniške mreže

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

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL POTRDIL IN REGISTRA PREKLICANIH POTRDIL

7.1. Profil potrdil

(1) Na podlagi pričujoče politike SIGOV-CA izdaja in v tem razdelku obravnava naslednje vrste potrdil za potrebe organizacij[14]:

- posebna potrdila za zaposlene,
- posebna potrdila za zaposlene z obvezno uporabo pametnih kartic,
- spletna potrdila za zaposlene,
- spletna potrdila za zaposlene z obvezno uporabo pametnih kartic,
- posebna potrdila za splošne nazive organizacij oz. organizacijske enote,
- posebna potrdila za splošne nazive organizacij oz. organizacijske enote z obvezno uporabo pametnih kartic,
- spletna potrdila za splošne nazive organizacij oz. organizacijske enote,
- spletna potrdila za splošne nazive organizacij oz. organizacijske enote z obvezno uporabo pametnih kartic,
- spletna potrdila za strežnike,
- spletna potrdila za podpis kode,
- potrdila za izdajatelje TSA,
- potrdila za sisteme OCSP ter
- potrdila za druge izdajatelje[15].

(2) Vsa potrdila vključujejo podatke, ki so skladno z ZEPEP določena za kvalificirana potrdila.

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

7.1.1 Različica potrdil

Vsa potrdila izdajatelja SIGOV-CA sledijo standardu *X.509*, in sicer različici 3.

[14] Potrdilo izdajatelja SIGOV-CA je podrobno podano že v razd. 1.3.1.
[15] Podrobnosti o tem se določijo v medsebojnem dogovoru med SIGOV-CA in drugim izdajateljem.

7.1.2 Profil potrdil z razširitvami

(1) Osnovni podatki v potrdilu so navedeni spodaj, ostali podatki pa so vsebovani glede na vrsto potrdila v nadaljevanju:

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	2 (*kar pomeni verzijo 3*)
Identifikacijska oznaka potrdila, angl. *Serial Number*	*enolična interna številka potrdila-celo število*
Algoritem za podpis, angl. *Signature algorithm*	sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, organizationIdentifier=VATSI-17659957, cn=SIGOV-CA
Veljavnost, angl. *Validity*	Not Before: <*pričetek veljavnosti po GMT*> Not After: <*konec veljavnosti po GMT*> *v formatu UTCTime* <LLMMDDuummssZ>
Imetnik, angl. *Subject*	*razločevalno ime imetnika, odvisno od vrste potrdila (glej razd. 3.1.1), v obliki, primerni za izpis*
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, angl. *Public Key (... bits)*	*modul, eksponent,...*
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. *RSA Public Key*	*dolžina ključa je min 2048 bitov*
Razširitve X.509v3	
Alternativno ime OID 2.5.29.17, angl. *Subject Alternative Name*	*elektronski naslov, glej razd. 7.1.2.3* *ime strežnika pri spletnih potrdilih za strežnike, glej razd. 7.1.2.4*
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	Url: http://www.sigov-ca.gov.si/crl/sigov-ca2.crl Url: ldap://x500.gov.si/cn=SIGOV-CA, organizationIdentifier=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList c=SI, o=Republika Slovenija, organizationIdentifier=VATSI-17659957, cn=SIGOV-CA, cn=CRL<*zaporedna številka registra, glej razd. 7.2.3*>
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. *Authority Information Access*	Access Method=OCSP http://ocsp.sigov-ca.gov.si
Zasebni ključ za podpisovanje velja do, OID 2.5.29.16, angl. *Private Key Usage Period*	*odvisna od vrste potrdila, glej razd. 6.3.2*
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	*odvisna od vrste potrdila, glej razd. 7.1.2.1 in 7.1.2.2*
Razširjena uporaba, OID 2.5.29.37, angl. *Extended Key Usage*	*odvisno od vrste potrdila, glej razd. 7.1.2.1 in 7.1.2.2*

Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	465E 40E5 53ED FEFE
Identifikator imetnikovega ključa, OID 2.5.*29.14,* *angl. Subject Key Identifier*	*identifikator imetnikovega ključa*
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier= *odvisno od vrste potrdila, glej razd. 7.1.2.1 in 7.1.2.2* [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	*odvisna od vrste potrdila, glej razd. 7.1.2.1 in 7.1.2.2*
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	*se ne uporablja*
OID 1.2.840.113533.7.65.0 Verzija Entrust angl. *Entrust version extension*	V8.1
Dodatna identifikacija (ni del digitalnega potrdila)	
razpoznavni odtis potrdila-SHA-1 angl. *Certificate Fingerprint – SHA-1*	*razpoznavni odtis potrdila po SHA-1*
razpoznavni odtis potrdila-SHA-256 angl. *Certificate Fingerprint – SHA-256*	*razpoznavni odtis potrdila po SHA-256*

(2) Pod istimi podatki o nazivu, podatki o organizaciji, elektronskim naslovom ima imetnik lahko eno samo veljavno istovrstno potrdilo.

7.1.2.1 Profil posebnih potrdil

(1) Obe potrdili posebnega potrdila, t.j. potrdilo za šifriranje ter potrdilo za overjanje podpisa, vključujeta podatke, ki so navedene v tabeli zgoraj. Določena polja v potrdilu, ki pa so odvisna od vrste le-tega, pa so podana v nadaljevanju.

(2) Vrednosti polj za *namen uporabe*, *razširjen namen uporabe, politiko ter oznako kvalificiranega potrdila* za potrdilo za šifriranje so podane v spodnji tabeli.

Nazivi polja	Vrednost potrdila za šifriranje			
	zaposlen z obvezno uporabo pametne kartice	splošni naziv z obvezno uporabo pametne kartice	zaposlen	splošni naziv
Namen uporabe, angl. *Key Usage*	Key Encipherment			
Razširjen namen uporabe, angl. *Extended Key Usage*	/			
Politike, pod katerimi je bilo izdano potrdilo (OID), in iz katerih je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.1.4.7 0.4.0.1456.1.1 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.8.7 0.4.0.1456.1.1 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.3.7 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.7.7 0.4.0.1456.1.2

Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	QcCompliance statement QcSSCD statement	QcCompliance statement QcSSCD statement	QcCompliance statement	QcCompliance statement

(3) Vrednosti polj za *namen uporabe, razširjen namen uporabe, politiko ter oznako kvalificiranega potrdila* za potrdilo za overjanje podpisa so podane v spodnji tabeli.

Nazivi polja	Vrednost potrdila za overjanje podpisa				
	zaposlen z obvezno uporabo pametne kartice	splošni naziv z obvezno uporabo pametne kartice	zaposlen	splošni naziv	izdajatelj TSA
Namen uporabe, angl. *Key Usage*	Digital Signature				
Razširjen namen uporabe, angl. *Extended Key Usage*	/				Time Stamping
Politike, pod katerimi je bilo izdano potrdilo (OID), in iz katerih je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.1.4.7 0.4.0.1456.1.1 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.8.7 0.4.0.1456.1.1 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.3.7 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.7.7 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.11.7
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	QcCompliance statement QcSSCD statement	QcCompliance statement QcSSCD statement	QcCompliance statement	QcCompliance statement	

(4) Polja, označena kot kritična (angl. *critical*), so sledeča:
- *namen uporabe* (angl. *Key Usage*) za vse vrste posebnih potrdil,
- *razširjen namen uporabe* (angl. *Extended Key Usage)* za potrdilo za izdajatelja TSA.

7.1.2.2 Profil spletnih potrdil

(1) Spletno potrdilo vključuje podatke, ki so navedeni v tabeli v razd. 7.1.2. Vrednosti polj za *namen uporabe*, *razširjen namen uporabe, politiko ter oznako kvalificiranega potrdila,* ki pa so odvisne od vrste potrdila, so za spletno potrdilo podane v spodnji tabeli.

Nazivi polja	Vrednost spletnega potrdila			
	zaposlen z obvezno uporabo pametne kartice	splošni naziv z obvezno uporabo pametne kartice	zaposlen	splošni naziv
Namen uporabe, angl. *Key Usage*	Digital Signature, Key Encipherment			

Razširjen namen uporabe, angl. *Extended Key Usage*	/			
Politike, pod katerimi je bilo izdano potrdilo (OID), in iz katerih je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.1.2.7 0.4.0.1456.1.1 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.6.7 0.4.0.1456.1.1 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.1.7 0.4.0.1456.1.2	Policy: 1.3.6.1.4.1.6105.1.5.7 0.4.0.1456.1.2
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	QcCompliance statement QcSSCD statement	QcCompliance statement QcSSCD statement	QcCompliance statement	QcCompliance statement

Nazivi polja	Vrednost spletnega potrdila		
	strežnik	podpis kode	sistem OCSP
Namen uporabe, angl. *Key Usage*	Digital Signature, Key Encipherment	Digital Signature	
Razširjen namen uporabe, angl. *Extended Key Usage*	serverAuth, clientAuth	code Signing	OCSP Signing
Politike, pod katerimi je bilo izdano potrdilo (OID), in iz katerih je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.1.9.7	Policy: 1.3.6.1.4.1.6105.1.10.7	Policy: 1.3.6.1.4.1.6105.1.12.7
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*			

(2) Polje za *namen uporabe* (angl. *Key Usage*) je za vse vrste spletnih potrdil označeno kot kritično (angl. *critical*).

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 oz. organizacijo.

(2) SIGOV-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.

7.1.2.4 Zahteve za ime strežnika

(1) Ime strežnika je polno domensko ime, navedeno v razločevalnem imenu (glej 1. odstavek razd. 3.1.2).

(2) Poleg imena strežnika, navedenega v razločevalnem imenu, lahko imetnik doda največ 4 dodatna imena strežnika.

7.1.3 Identifikacijske oznake algoritmov

(1) Potrdila, ki jih izdaja SIGOV-CA, so s strani izdajatelja podpisana z algoritmom, določenim v polju s*ignature 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 SIGOV-CA.

7.1.4 Oblika razločevalnih imen

Glej razd. 3.1.1.

7.1.5 Omejitve glede imen

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

7.1.6 Označba politike potrdila

Glej razd. 7.1.2.

7.1.7 Omejitve uporabe

Omejitve uporabe (polje v potrdilu angl. *Usage policy constraints extension*) niso predpisane.

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 javnem imeniku potrdil (glej podpogl. 2.3):
- 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. *Version*	1 (*kar pomeni verzijo 2*)
Algoritem za podpis, angl. *Signature Algorithm*	sha256WithRSAEncryption
Izdajateljev podpis, angl. *Signature*	*podpis SIGOV-CA*
Razločevalno ime izdajatelja, angl. *Issuer*	c=SI, o=Republika Slovenija, organizationIdentifier=VATSI-17659957, cn=SIGOV-CA
Čas izdaje CRL, angl. *thisUpdate*	Last Update: <*čas izdaje po GMT*>
Čas izdaje naslednjega CRL, angl. *nextUpdate*	Next Update: <*čas naslednje izdaje po GMT*>
identifikacijske oznake preklicanih potrdil in čas preklica, angl. *revokedCertificate*	Serial Number: <*identifikacijska oznaka preklicanega dig. potrdila*> Revocation Date: <*čas preklica po GMT*>
Razširitve X.509v2 CRL	
identifikator izdajateljevega ključa, angl. *Authority Key Identifier* *(OID 2.5.29.35)*	465E 40E5 53ED FEFE
številka za posamične registre (CRL1, CRL2,....), angl. *CRLnumber* *(OID 2.5.29.20)*	*zaporedna številka posamičnega registra*
angl. *issuerAltName* *(OID 2.5.28.18)*	*se ne uporablja*
angl. *deltaCRLindicator* *(OID 2.5.29.27)*	*se ne uporablja*
angl. *issuingDistribuitionPoint* *(OID 2.5.29.28)*	*se ne uporablja*

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

7.2.3 Objava registra CRL v javnem imeniku in v digitalnih potrdilih

(1) SIGOV-CA objavlja register v javnem imeniku na strežniku *X500.gov.si.*

(2) 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

posamični registri	c=SI, o=Republika Slovenija, organizationIdentifier=VATSI-17659957, cn=SIGOV-CA, cn=CRL<*zaporedna številka registra*>	- ldap://x500.gov.si/cn=CRL<*zaporedna številka registra*>, cn=SIGOV-CA,organizationIdentifier=VATSI-17659957,o=Republika Slovenija,c=SI
celotni register	c=SI, o=Republika Slovenija, organizationIdentifier=VATSI-17659957, cn=SIGOV-CA (*v polju "CertificationRevocationList"*)	- http://www.sigov-ca.gov.si/crl/sigov-ca2.crl - ldap://x500.gov.si/cn=SIGOV-CA, organizationIdentifier=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.sigov-ca.gov.si.

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

7.3.1 Verzija sprotnega preverjanje statusa

Izdajatelj SIGOV-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 ZEPEP.

8.2. Inšpekcijska služba

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

8.3. Neodvisnost inšpekcijske služba

Inšpekcijska služba je organ, pristojen v skladu z ZEPEP.

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 SIGOV-CA oz. overitelj 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. FINANČNE IN OSTALE PRAVNE ZADEVE

9.1. Cenik

9.1.1 Cena izdaje potrdil in podaljšanja

Stroški upravljanja s potrdili se obračunavajo organizaciji po objavljenem ceniku na spletni strani http://www.sigov-ca.gov.si/cenik.php.

9.1.2 Cena dostopa do potrdil

Dostop do javnega imenika potrdil je brezplačen, razen če se stranki dogovorita drugače.

9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil

Dostop do statusa potrdila in registra preklicanih potrdil je brezplačen, razen če se stranki dogovorita drugače.

9.1.4 Cene drugih storitev

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

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 po ZEPEP ter Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje.

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 SIGOV-CA ravna zaupno z naslednjimi podatki:
- z vsemi zahtevki za pridobitev potrdila ali druge storitve
- zasebne ključe posebnih potrdil, katerih kopija se hrani tudi pri izdajatelju SIGOV-CA
- vse morebitne zaupne podatke v zvezi s finančnimi obveznostmi,
- vse morebitne zaupne podatke, ki so predmet medsebojne pogodbe z organizacijo ali tretjimi osebami ter
- vse ostale zadeve, ki so v skladu z Uredbo zavedene v Interni politiki delovanja overitelja na MJU.

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

9.3.2 Nevarovani podatki

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

9.3.3 Odgovornost glede varovanja

Izdajatelj SIGOV-CA ne posreduje drugih podatkov o organizacijah, razen teh, ki niso navedeni v potrdilu ali morebitni medsebojni pogodbi, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s potrdili, ter je to na zahtevku za pridobitev potrdila ali kasneje v pisni obliki odobril imetnik potrdila oz. predstojnik organizacije, ali na zahtevo pristojnega sodišča ali upravnega organa. 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 SIGOV-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 medsebojne pogodbe oz. 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 oz. predstojnik organizacije pooblasti overitelja na MJU oz. izdajatelja SIGOV-CA za uporabo osebnih podatkov na zahtevku za pridobitev potrdila ali kasneje v pisni obliki.

9.4.6 Posredovanje osebnih podatkov

(1) Overitelj na MJU ne posreduje drugih 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 oz. predstojnik organizacije pooblastil za to (glej prejšnji razdelek), 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 varovanja osebnih podatkov

Niso predpisana.

9.5. Določbe glede pravic intelektualne lastnine

Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine:
- 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 oz. organizaciji.

9.6. Obveznosti in odgovornosti

9.6.1 Obveznosti in odgovornosti overitelja na MJU oz. izdajatelja SIGOV-CA

(1) Overitelj na MJU oz. izdajatelj SIGOV-CA 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, ki kakorkoli vplivajo na imetnike potrdil, organizacije in tretje osebe,
- zagotoviti delovanje prijavnih služb v skladu z določili SIGOV-CA in ostalimi veljavnimi predpisi,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi podatki o overitelju, imetnikih potrdil, podatkov o organizacijah 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) Overitelj na MJU oz. izdajatelj SIGOV-CA je dolžan:
- zagotoviti pravilnost podatkov izdanih potrdil,
- zagotoviti, da ima imetnik potrdila v času izdaje le-tega zasebni ključ pripadajoč v potrdilu navedenemu javnemu ključu,
- zagotoviti varen prevzem digitalnih potrdil z obvezno uporabo pametnih kartic in poskrbeti za varno posredovanje pametnih kartic z digitalnimi potrdili imetnikom,
- zagotoviti pravilnost objave registra preklicanih 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 uporabnike o pomembnih zadevah ter
- izpolnjevati vse druge zahteve v skladu s to politiko.

(3) Overitelj na MJU oz. izdajatelj SIGOV-CA zagotavlja čim večjo dostopnost svojih storitev, in sicer 24ur/7dni/365dni, pri čemer pa se ne upošteva naslednje primere:
- načrtovane in vnaprej napovedane tehnične ali servisne posege na infrastrukturi,
- nenačrtovane tehnične ali servisne posege na infrastrukturi kot posledica nepredvidenih okvar,
- tehnične ali servisne posege zaradi okvare infrastrukture izven pristojnosti izdajatelja SIGOV-CA in
- nedostopnost kot posledica višje sile ali izrednih dogodkov.

(4) Vzdrževalna dela ali nadgradnje infrastrukture mora overitelj na MJU oz. SIGOV-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 SIGOV-CA oz. overitelja na MJU so določene z morebitnim medsebojnim dogovorom z organizacijo oz. tretjo osebo.

9.6.2 Obveznost in odgovornost prijavne službe

(1) Prijavna služba je dolžna:
- preverjati istovetnost imetnikov oz. bodočih imetnikov in podatkov o organizaciji,
- sprejemati zahtevke za storitve SIGOV-CA,

- preverjati zahtevke,
- izdajati potrebno dokumentacijo imetnikom oz. bodočim imetnikom in organizacijam,
- posredovati zahtevke in ostale podatke na varen način na SIGOV-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 potrdila oziroma organizacije

(1) Organizacija 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 SIGOV-CA ter veljavnih predpisov.

(2) Obveznosti imetnikov oz. organizacije so glede uporabe potrdil določena v razd. 4.5.1.

9.6.4 Obveznosti in odgovornost tretjih oseb

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

(2) Tretje osebe, ki se zanašajo na izdana potrdila SIGOV-CA, morajo:
- upoštevati tudi vsa navodila oz. priporočila SIGOV-CA glede zanesljive uporabe, določene tudi v razd. uporabe oz. zanašanja na potrdila glede uporabe potrdil so določena v razd. 4.5.2,
- ob morebitnih napakah ali problemih takoj obvestiti izdajatelja SIGOV-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 SIGOV-CA in ravnati v skladu z le-temi,
- 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 in veljavne zakonodaje.

9.6.5 Obveznosti in odgovornost drugih oseb

Niso predpisani.

9.7. Omejitev 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 oz. dogovoru med organizacijo in SIGOV-CA,
- 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 v registru preklicanih potrdil,
- nepreverjanja časa veljavnosti potrdila,
- ravnanja imetnika potrdila, njegove organizacije ali tretje osebe v nasprotju z obvestili SIGOV-CA, politiko in drugimi predpisi,
- omogočene uporabe oz. zlorabe imetnikovega potrdila nepooblaščenim osebam,
- izdanega potrdila z napačnimi podatki in neverodostojnimi podatki ali drugih dejanj imetnika ali organizacije ali overitelja,
- uporabe potrdil ter veljavnosti potrdil ob spremembah podatkov iz potrdila, elektronskih naslovov ali spremembah imen organizacij ali 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 SIGOV-CA ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

9.8. Omejitev glede uporabe

Izdajatelj SIGOV-CA oz. overitelj na MJU jamči za vrednost posameznega pravnega posla glede na vrsto potrdila do vrednosti:

- za digitalna potrdila z obvezno uporabo pametnih kartic do višine 5.000 EUR ter
- za potrdila brez obvezne uporabe pametnih kartic 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.

9.10. Veljavnost politike

9.10.1 Čas veljavnosti

(1) Nova verzija oz. spremembe politike overitelja na MJU se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na MJU pod novo identifikacijsko številko (CP_{OID}) in označenim datumom začetka njene veljavnosti.

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

9.10.2 Konec veljavnosti politike

(1) 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.).

(2) 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 oz. podaljšana 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 razd. 1.3.1.

(2) Kontaktni podatki imetnikov in njihovih organizacij pa so podani v zahtevkih v zvezi s potrdili.

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

9.12. Amandmaji

9.12.1 Postopek za sprejem amandmajev

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

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

(3) Če amandma bistveno vpliva na delovanje overitelja, se o tem obvesti pristojno ministrstvo po enakem postopku, kot to velja za politiko.

(4) Način za označevanje amandmajev določi izdajatelj SIGOV-CA.

9.12.2 Veljavnost in objava amandmajev

(1) Izdajatelja SIGOV-CA določi pričetek in konec veljavnosti amandmajev.

(2) Amandma se sedem (7) dni pred pričetkom veljavnosti objavi na spletnih straneh SIGOV-CA.

9.12.3 Sprememba identifikacijske številke politike

Če sprejeti amandma vpliva na uporabo potrdil, potem lahko izdajatelj SIGOV-CA določi novo identifikacijsko oznako politike (CP_{OID}) oz. amandmajev.

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

(1) Overitelj na MJU in izdajatelj SIGOV-CA delujeta v skladu z:
- ZEPEP,
- Uredbo,
- evropskimi direktivami,
- Zakonom o varstvu osebnih podatkov,
- priporočili ETSI in RFC
- in drugimi veljavnimi predpisi.

(2) Oblika in vsebina te politike je usklajena z:
- RFC 3647 »Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework«,
- ETSI TS 101 456 v 1.3.1. »Policy requirements for certification authorities issuing qualified certificates«.

9.15. Skladnost z veljavno zakonodajo

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

(2) Notranje preverjanje skladnosti delovanja izvajajo pooblaščene osebe v okviru overitelja na MJU.

9.16. Druga določila

Niso predpisana.