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

SI-TRUST
SIGEN-CA

POLITIKA SIGEN-CA

za kvalificirana digitalna potrdila za poslovne subjekte

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 20. oktobra 2020
verzija: 7.2

CP_{Name}: SIGEN-CA-1

- **Politika za spletna kvalificirana digitalna potrdila za zaposlene**
  CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.5
- **Politika za posebna kvalificirana digitalna potrdila za zaposlene**
  CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.5
- **Politika za spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom**
  CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.5
- **Politika za posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom**
  CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.5
- **Politika za spletna normalizirana digitalna potrdila za informacijske sisteme**
  CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.5
- **Politika za spletna normalizirana digitalna potrdila za podpis kode**
  CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.5
- **Politika za spletna kvalificirana digitalna potrdila za avtentikacijo spletišč**
  CP_{OID}: 1.3.6.1.4.1.6105.2.1.7.5
- **Politika za spletna kvalificirana digitalna potrdila za elektronski žig**
  CP_{OID}: 1.3.6.1.4.1.6105.2.1.8.5

© Državni center za storitve zaupanja

Zgodovina politik

Izdaje politik delovanja SIGEN-CA	
verzija: 7.2, veljavnost: od 20. oktobra 2020	
• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.5 • Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.5 • Politika za spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.5 • Politika za posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.5 • Politika za spletna normalizirana digitalna potrdila za informacijske sisteme, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.5 • Politika za spletna normalizirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.5 • Politika za spletna kvalificirana digitalna potrdila za avtentikacijo spletišč, CP_{OID}: 1.3.6.1.4.1.6105.2.1.7.5 • Politika za spletna kvalificirana digitalna potrdila za elektronski žig, CP_{OID}: 1.3.6.1.4.1.6105.2.1.8.5 CP_{Name}: SIGEN-CA-1	*Spremembe z verzijo 7.2:* • *pri potrdilih za avtentikacijo spletišč se elektronski naslov ne zapisuje v potrdilo,* • *veljavnost potrdil za avtentikacijo spletišč je 13 mesecev,* • *revizija dokumenta.*
amandma k politiki verzije 7.1, veljavnost: od 15. aprila 2020	
Amandma k Politiki SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte št. 1 / 7.1	*Sprememba z amandmajem št. 1 / 7.1:* • *oddaja zahtevka za pridobitev digitalnega potrdila je omogočena tudi na elektronski način z veljavnim kvalificiranim digitalnim potrdilom za elektronski podpis, izdanim s strani izdajatelja, vpisanega v zanesljivi seznam ponudnikov kvalificiranih storitev zaupanja v Republiki Sloveniji.*
verzija: 7.1, veljavnost: od 1. oktobra 2019	
• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.5 • Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.5 • Politika za spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.5 • Politika za posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.5 • Politika za spletna normalizirana digitalna potrdila za informacijske sisteme, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.5 • Politika za spletna normalizirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.5 • Politika za spletna kvalificirana digitalna potrdila za avtentikacijo spletišč, CP_{OID}: 1.3.6.1.4.1.6105.2.1.7.5 • Politika za spletna kvalificirana digitalna potrdila za elektronski žig, CP_{OID}: 1.3.6.1.4.1.6105.2.1.8.5 CP_{Name}: SIGEN-CA-1	*Sprememba z verzijo 7.1:* • *kvalificirana digitalna potrdila za splošne nazive so preimenovana v kvalificirana digitalna potrdila za zaposlene s splošnim nazivom,* • *revizija dokumenta.*
amandma k politiki verzije 7.0, veljavnost: od 18. februarja 2019	
Amandma k Politiki SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte št. 1 / 7.0	*Sprememba z amandmajem št. 1 / 7.0:* • *pri potrdilih za elektronske žige je spremenjen naziv, ki je vključen v razločevalno ime.*
verzija: 7.0, veljavnost: od 28. maja 2018	

© Državni center za storitve zaupanja

• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.5 • Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.5 • Politika za spletna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.5 • Politika za posebna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.5 • Politika za spletna normalizirana digitalna potrdila za informacijske sisteme, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.5 • Politika za spletna normalizirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.5 • Politika za spletna kvalificirana digitalna potrdila za avtentikacijo spletišč, CP_{OID}: 1.3.6.1.4.1.6105.2.1.7.5 • Politika za spletna kvalificirana digitalna potrdila za elektronski žig, CP_{OID}: 1.3.6.1.4.1.6105.2.1.8.5 CP_{Name}: SIGEN-CA-1	*Spremembe z verzijo 7.0:* • *normalizirana potrdila za strežnike so preimenovana v kvalificirana potrdila za avtentikacijo spletišč,* • *veljavnost potrdil za avtentikacijo spletišč je 27 mesecev,* • *spremenjeno je razločevalno ime potrdil za avtentikacijo spletišč,* • *uvedena so kvalificirana potrdila za elektronski žig in normalizirana potrdila za informacijske sisteme,* • *v potrdilih so navedene oznake politik, kot so določene z novimi standardi,* • *uvedena je Krovna politika SI-TRUST za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja SI-TRUST, zato se pričujoča politika v določenih točkah sklicuje nanjo,* • *izrazi in okrajšave so usklajeni z veljavno zakonodajo.*
verzija: 6.0, veljavnost: od 6. junija 2016	
• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.4 • Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.4 • Politika za spletna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.4 • Politika za posebna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.4 • Politika za spletna normalizirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.4 • Politika za spletna normalizirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.4 CP_{Name}: SIGEN-CA-1	*Spremembe z verzijo 6.0:* • *tvorjeno je bilo drugo lastno digitalno potrdilo izdajatelja SIGEN-CA z zasebnim ključem dolžine 3072 bitov, ki se hrani na strojni opremi za varno shranjevanje zasebnih ključev,* • *v potrdilu izdajatelja SIGEN-CA in vseh potrdilih imetnikov se uporablja zgostitveni algoritem SHA-256,* • *spremenjeno je razločevalno ime digitalnega potrdila izdajatelja SIGEN-CA,* • *spremenjena so razločevalna imena potrdil imetnikov, ki lahko vključujejo znake iz kodne tabele UTF-8,* • *podprto je sprotno preverjanje statusa potrdil po protokolu OCSP,* • *izdajatelj SIGEN-CA je priznan s strani korenskega izdajatelja SI-TRUST Root,* • *pri potrdilih za zaposlene in splošne nazive je v polju uporaba ključa (angl. Key Usage) dodana vrednost ContentCommitment,* • *potrdila za strežnike in podpis kode so preimenovana v normalizirana potrdila.*
verzija: 5.0, veljavnost: od 7. novembra 2015	
• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.3 • Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.3 • Politika za spletna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.3 • Politika za posebna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.3 • Politika za spletna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.3 • Politika za spletna kvalificirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.3 CP_{Name}: SIGEN-CA-1	*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,* • *omogočeno je izdajanje spletnih potrdil za strežnike z več imeni strežnika,* • *ukinjeno je izdajanje posebnih potrdil za strežnike,* • *novi kontaktni podatki izdajatelja SIGEN-CA.*
amandma k politiki verzije 4.0, veljavnost: od 21. marca 2014	
Amandma k Politiki SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte 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	

© Državni center za storitve zaupanja

Amandma k Politiki SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte 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 SIGEN-CA za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.2 • Politika SIGEN-CA za posebna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105. 2.1.2.2 • Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za strežnike in podpis kode, CP_{OID}: 1.3.6.1.4.1.6105. 2.1.3.2 • Politika SIGEN-CA za posebna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.2 CP_{Name}: SIGEN-CA-1	*Spremembe z verzijo 4.0:* • *izdajatelj digitalnih potrdil SIGEN-CA izdaja kvalificirana digitalna potrdila s ključi minimalne dolžine 2048 bitov;* • *v kvalificiranih dig. potrdilih za zaposlene in splošne nazive je dodana ustrezna oznaka za kvalificirana potrdila;* • *spremeni se jamstvo za vrednost posameznega pravnega posla.*
amandma k politiki verzije 3.0, veljavnost: od 18. maja 2007	
Amandma k Politiki SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte št. 1 / 3.0	*Sprememba z amandmajem št. 1 / 3.0:* • *izdajatelj SIGEN-CA bodočemu imetniku potrdila avtorizacijske kode ne posreduje po priporočeni pošti.*
verzija: 3.0, veljavnost: od 28. februarja 2006	
• Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.1 • Politika SIGEN-CA za posebna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105. 2.1.2.1 • Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za strežnike in podpis kode, CP_{OID}: 1.3.6.1.4.1.6105. 2.1.3.1 • Politika SIGEN-CA za posebna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.1 CP_{Name}: SIGEN-CA-1	*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«;* • *preklic je po novem mogoč samo v uradnih urah, razen v nujnih primerih;* • *uporaba novega naziva za imetnike SIGEN-CA, in sicer za imetnike »pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti« uporablja izraz »poslovni subjekti«;* • *struktura dokumenta je v skladu s priporočili RFC 3647.*
verzija: 2.0, veljavnost: od 15. julija 2002	
Politika SIGEN-CA za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti CP_{OID}: 1.3.6.1.4.1.6105.2.1.2 CP_{Name}: SIGEN-CA-1	*Spremembe z verzijo 2.0:* • *izdaja se tudi kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote institucij;* • *izdaja se tudi kvalificirana digitalna potrdila za strežnike in podpis kode.*
verzija: 1.0, veljavnost: od 15. oktobra 2001	
Politika SIGEN-CA za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti CP_{OID}:1.3.6.1.4.1.6105.2.1.1 CP_{Name}: SIGEN-CA-1	/

© Državni center za storitve zaupanja

VSEBINA

© Državni center za storitve zaupanja

© Državni center za storitve zaupanja

© Državni center za storitve zaupanja

© Državni center za storitve zaupanja

© Državni center za storitve zaupanja

© Državni center za storitve zaupanja

POVZETEK

Politike za digitalna potrdila in elektronske časovne žige predstavljajo celoten javni del notranjih pravil Državnega centra za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo (v nadaljevanju *SI-TRUST*) in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi in normaliziranimi digitalnimi potrdili, dodeljevanje kvalificiranih elektronskih časovnih žigov, odgovornost SI-TRUST ter zahteve, ki jih morajo izpolnjevati uporabniki in tretje osebe, ki uporabljajo in se zanašajo na kvalificirana digitalna potrdila in na kvalificirane elektronske časovne žige, in drugi ponudniki storitev zaupanja, ki želijo uporabljati storitve SI-TRUST.

SI-TRUST izdaja kvalificirana digitalna potrdila ter kvalificirane elektronske časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (eIDAS; Uradni list EU, št. L 257/73), standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

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

Normalizirana digitalna potrdila, ki jih izdaja SI-TRUST, so namenjena:
- izdajateljem potrdil, izdajateljem časovnih žigov, sistemom OCSP, informacijskim sistemom, podpisovanju programske kode in registra preklicanih potrdil ter v ostalih primerih, kjer ni možna uporaba kvalificiranih potrdil,
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

Kvalificirana digitalna potrdila, ki jih izdaja SI-TRUST, so namenjena:
- ustvarjanju elektronskih podpisov in elektronskih žig ter avtentikaciji spletišč,
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil,
- za varno elektronsko komuniciranje med imetniki potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

Kvalificirani elektronski časovni žigi SI-TRUST 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 kvalificirani elektronski časovni žig.

Znotraj SI-TRUST deluje izdajatelj kvalificiranih digitalnih potrdil SIGEN-CA (angl. *Slovenian General Certification Authority*), https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/, ki izdaja potrdila za poslovne subjekte in fizične osebe.

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

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

Pričujoči dokument določa politike izdajatelja SIGEN-CA za poslovne subjekte, t.j. pravne in fizične osebe, registrirane za opravljanje dejavnosti (v nadaljevanju *organizacije*) za več vrst kvalificiranih digitalnih potrdil, ki izpolnjujejo najvišje varnostne zahteve. Na podlagi tega dokumenta SIGEN-CA izdaja posebna in spletna digitalna potrdila po naslednjih politikah CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.5, CP_{OID}:

© SI-TRUST

1.3.6.1.4.1.6105.2.1.3.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.7.5 ter CP_{OID}: 1.3.6.1.4.1.6105.2.1.8.5.

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

Spremembi pričujočega dokumenta sta sledeči:
- pri potrdilih za avtentikacijo spletišč se elektronski naslov ne zapisuje v potrdilo,
- veljavnost potrdil za avtentikacijo spletišč je 13 mesecev.

Ker spremembe, ki jih prinaša nova politika, ne vplivajo na namen uporabe ali postopke upravljanja, ki lahko spremenijo nivo zaupanja, se identifikacijske oznake politik (CP_{OID}), ne spremenijo.

Kvalificirana digitalna potrdila se pridobijo na podlagi zahtevka, ki ga morata podpisati odgovorna oseba poslovnega subjekta in bodoči imetniki. V primeru digitalnega potrdila za informacijske sisteme, podpis kode, spletišča in elektronske žige je bodoči imetnik zaposleni oz. oseba, ki jo odgovorna oseba pooblasti za uporabo tega potrdila. Odgovorna oseba s podpisom zahtevka jamči za istovetnost bodočega imetnika. Istovetnost bodočega imetnika se lahko izkaže tudi z veljavnostjo njegovega elektronskega podpisa. Izpolnjen zahtevek se odda na prijavno službo (seznam je objavljen na spletni strani https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/).

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

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

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 opremo. SIGEN-CA nikoli ne hrani in tudi nima dostopa do zasebnega ključa za podpisovanje. Javni ključ za overjanje podpisa se pošlje SIGEN-CA, ki izda potrdilo za overjanje podpisa, katerega sestavni del je javni ključ za overjanje podpisa. Potrdilo za overjanje podpisa se shrani pri imetniku.
- Par ključev za dešifriranje/šifriranje se tvori na strani izdajatelja SIGEN-CA. Zasebni ključ za dešifriranje hrani imetnik. 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 SI-TRUST, varno hrani tudi v arhivu SIGEN-CA. SIGEN-CA izda potrdilo za šifriranje, katerega sestavni del je javni ključ za šifriranje. Potrdilo za šifriranje se objavi v javnem imeniku potrdil.

SIGEN-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 in svoje digitalno potrdilo ter ravnati v skladu s politiko, obvestili izdajatelja SIGEN-CA in veljavno zakonodajo.

© Državni center za storitve zaupanja

1. UVOD

1.1. Pregled

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

(2) Znotraj SI-TRUST deluje izdajatelj SIGEN-CA (angl. *Slovenian General Certification Authority*), https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/, ki izdaja digitalna potrdila za poslovne subjekte in fizične osebe. Pričujoči dokument določa politike izdajatelja SIGEN-CA za vse vrste digitalnih potrdil za potrebe poslovnih subjektov (v nadaljevanju *organizacije*).

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

(4) Po pričujoči politiki SIGEN-CA izdaja naslednja kvalificirana digitalna potrdila:
- posebna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote,
- spletna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote,
- spletna kvalificirana digitalna potrdila za avtentikacijo spletišč, s katerimi upravljajo organizacije,
- spletna kvalificirana digitalna potrdila za elektronske žige organizacij,
- spletna normalizirana digitalna potrdila za informacijske sisteme, s katerimi upravljajo organizacije,
- spletna normalizirana digitalna potrdila za podpis kode za potrebe organizacije.

(5) Digitalna potrdila SIGEN-CA se lahko uporabljajo za:
- šifriranje podatkov v elektronski obliki,
- overjanje digitalno podpisanih podatkov v elektronski obliki ter izkazovanje istovetnosti imetnika,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil SI-TRUST.

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

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

(8) Medsebojna razmerja se izvajajo tudi na podlagi morebitnega pisnega dogovora med organizacijami in SI-TRUST, ali med tretjimi osebami, ki se zanašajo na potrdila izdajatelja SIGEN-CA, in SI-TRUST.

(9) SI-TRUST se preko korenskega izdajatelja SI-TRUST Root lahko povezuje z drugimi ponudniki storitev zaupanja, kar se ureja z medsebojnim dogovorom oz. pogodbo.

1.2. Identifikacijski podatki politike delovanja

© Državni center za storitve zaupanja

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

(2) Oznaka pričujoče politike je CP_{Name}: SIGEN-CA-1, identifikacijske oznake politike SIGEN-CA-1 pa so različne glede na vrsto potrdila:
- CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.5 za spletna kvalificirana potrdila za zaposlene,
- CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.5 za posebna kvalificirana potrdila za zaposlene,
- CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.5 za spletna kvalificirana potrdila za zaposlene s splošnim nazivom,
- CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.5 za posebna kvalificirana potrdila za zaposlene s splošnim nazivom,
- CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.5 za spletna normalizirana potrdila za informacijske sisteme,
- CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.5 za spletna normalizirana potrdila za podpis kode,
- CP_{OID}: 1.3.6.1.4.1.6105.2.1.7.5 za spletna kvalificirana potrdila za avtentikacijo spletišč,
- CP_{OID}: 1.3.6.1.4.1.6105.2.1.8.5 za spletna kvalificirana potrdila za elektronske žige.

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

1.3. Udeleženci infrastrukture javnih ključev

1.3.1 Ponudnik storitev zaupanja

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

(2) V okviru SI-TRUST deluje izdajatelj kvalificiranih digitalnih potrdil SIGEN-CA.

(3) Kontaktni podatki izdajatelja SIGEN-CA so:

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

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

© Državni center za storitve zaupanja

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

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

Naziv polja	Vrednost potrdila izdajatelja SIGEN-CA
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	3B3C F9C9
Algoritem za podpis, angl. *Signature Algorithm*	sha1WithRSAEncryption
Izdajatelj, angl. *Issuer*	c=si, o=state-institutions, ou=sigen-ca
Imetnik, angl. *Subject*	c=si, o=state-institutions, ou=sigen-ca
Pričetek veljavnosti, angl. *Validity: Not Before*	Jun 29 21:27:46 2001 GMT
Konec veljavnosti, angl. *Validity: Not After*	Jun 29 21:57:46 2021 GMT
Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 2048 bitov*
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. *Authority Key Identifier*	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. *Subject Key Identifier*	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
Odtis potrdila (ni del potrdila)	
Odtis potrdila MD-5, angl. *Certificate Fingerprint – MD5*	49EF A6A1 F0DE 8EA7 6AEE 5B7D 1E5F C446
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	3E42 A187 06BD 0C9C CF59 4750 D2E4 D6AB 0048 FDC4
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	12D4 80C1 A3C6 6478 1B99 D9DF 0E9F AF3F 1CAC EE1B 3C30 C312 3A33 7A4A 454F FED2

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

Potrdilo št. 2 SIGEN-CA vsebuje naslednje podatke:

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

© Državni center za storitve zaupanja

Naziv polja	Vrednost potrdila izdajatelja SIGEN-CA
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	CD81 8601 0000 0000 571E 043E
Algoritem za podpis, angl. *Signature Algorithm*	sha256WithRSAEncryption
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Imetnik, angl. *Subject*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Pričetek veljavnosti, angl. *Validity: Not Before*	Apr 25 11:19:25 2016 GMT
Konec veljavnosti, angl. *Validity: Not After*	Apr 25 11:49:25 2036 GMT
Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 3072 bitov*
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	4C25 278C A82D 729E
Identifikator imetnikovega ključa, OID 2.5.*29.14*, *angl. Subject Key Identifier*	4C25 278C A82D 729E
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	335F 27AE EE7A EA9B D4E3 FE59 EB65 B4AC 8926 E0E7
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	C4B9 BB09 EA4E F4A1 37EC 573A EFC1 23C4 B509 62CF B99A E13A 9331 14DB 4A34 274D

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

Nazivi polja Osnovna polja v potrdilu	Vrednost oz. pomen
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	A668 BD51 0000 0000 571D D0E8
Algoritem za podpis, angl. *Signature Algorithm*	sha256WithRSAEncryption
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Imetnik, angl. *Subject*	c=si, o=state-institutions, ou=sigen-ca
Pričetek veljavnosti, angl. *Validity: Not Before*	May 24 11:58:27 2016 GMT

© Državni center za storitve zaupanja

Konec veljavnosti, angl. *Validity: Not After*	Jun 27 22:00:00 2021 GMT
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 2048 bitov*
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	Url: http://www.ca.gov.si/crl/si-trust-root.crl Url: ldap://x500.gov.si/cn=SI-TRUST Root, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root, cn=CRL1
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. *Authority Information Access*	Access Method=OCSP http://ocsp.ca.gov.si Access Method=CA Issuers http://www.ca.gov.si/crt/si-trust-root.crt
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier=2.5.29.32.0 (»anyPolicy«) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.*29.14,* *angl. Subject Key Identifier*	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	EF9B C82D C8B0 F209 4529 447F 3BB6 6AC9 9C25 7C66
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	E016 01D8 F0D6 9434 E699 735C 4F34 8FC1 5FB4 8F2C 2B20 03FE E0F5 4A90 E819 48FD

Nazivi polja Osnovna polja v potrdilu	Vrednost oz. pomen
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	28C3 981D 0000 0000 571D D0E7

© Državni center za storitve zaupanja

Algoritem za podpis, angl. *Signature Algorithm*	sha256WithRSAEncryption
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Imetnik, angl. *Subject*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Pričetek veljavnosti, angl. *Validity: Not Before*	May 24 11:49:41 2016 GMT
Konec veljavnosti, angl. *Validity: Not After*	Apr 23 22:00:00 2036 GMT
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 3072 bitov*
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	Url: http://www.ca.gov.si/crl/si-trust-root.crl Url: ldap://x500.gov.si/cn=SI-TRUST Root, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root, cn=CRL1
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. *Authority Information Access*	Access Method=OCSP http://ocsp.ca.gov.si Access Method=CA Issuers http://www.ca.gov.si/crt/si-trust-root.crt
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier=2.5.29.32.0 (»anyPolicy«) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.*29.14*, *angl. Subject Key Identifier*	4C25 278C A82D 729E
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	D3C6 C554 C171 F9BA 952C E04C AC2C 1C9B D68B 08D4

© Državni center za storitve zaupanja

Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	7950 15CA ACA7 4715 D341 120D 3F0E FD19 2A03 2F1C 0039 1797 F54E F998 0804 A175

1.3.2 Prijavna služba

(1) Organizacije, ki opravljajo naloge prijavne službe, pooblasti SI-TRUST. Izpolnjevati morajo pogoje za opravljanje nalog prijavnih služb SI-TRUST 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 SIGEN-CA.

(3) Naloge prijavne službe za potrebe izdajatelja SIGEN-CA vrši pooblaščena oseba prijavne službe, ki preveri podatke o imetnikih oz. bodočih imetnikih, podatke o organizaciji in druge potrebne podatke ter izvaja ostale zgoraj navedene naloge.

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

1.3.3 Imetniki potrdil

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

(2) Odgovorna oseba 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 informacijske sisteme, podpis kode, spletišča in elektronske žige je imetnik takega potrdila pooblaščen s strani odgovorne osebe. Imetniki so tako lahko:
- zaposleni,
- zaposleni, pooblaščeni za upravljanje z informacijskimi sistemi (storitvami oz. aplikacijami),
- zaposleni, pooblaščeni za uporabo programske opreme za podpis kode,
- zaposleni, pooblaščeni za upravljanje s spletišči,
- zaposleni, pooblaščeni za upravljanje z elektronskimi žigi.

(4) Med organizacijo in izdajateljem SIGEN-CA oz. SI-TRUST se sklene medsebojni pisni dogovor.

1.3.4 Tretje osebe

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

1.3.5 Ostali udeleženci

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.4. Namen uporabe potrdil

(1) Posebna in spletna potrdila SIGEN-CA, izdana po pričujoči politiki, se lahko uporabljajo za:
- šifriranje podatkov v elektronski obliki,
- overjanje digitalno podpisanih podatkov v elektronski obliki ter izkazovanje istovetnosti podpisnika,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil SI-TRUST.

(2) 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*).

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

1.4.1 Pravilna uporaba potrdil in ključev

(1) Namen potrdil oz. pripadajočih ključev je podan v potrdilu v polju *uporaba ključa* (angl. *Key Usage*), v primerih potrdil za avtentikacijo spletišč in podpis kode pa dodatno v polju *razširjena uporaba ključa* (angl. *Extended Key Usage*), glej 7.1.2.

(2) 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.

(3) 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.

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

Tip potrdila	Par ključev	Pripadajoči ključi	Namen
posebno za zaposlene in za zaposlene s splošnim nazivom	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 za zaposlene s splošnim nazivom	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	- zasebni ključ - javni ključ	podpisovanje/overjanje in dešifriranje/šifriranje
spletno za informacijske sisteme	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	- zasebni ključ - javni ključ	podpisovanje/overjanje in dešifriranje/šifriranje

© Državni center za storitve zaupanja

spletno za podpis kode[2]	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	- ključ za podpisovanje - ključ za overjanje podpisa	podpisovanje/overjanje izvršljive programske kode
spletno za avtentikacijo spletišč[3]	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	- zasebni ključ - javni ključ	podpisovanje/overjanje in dešifriranje/šifriranje varnih povezav
spletno za elektronski žig	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	- ključ za podpisovanje - ključ za overjanje podpisa	podpisovanje/overjanje

1.4.2 Nedovoljena uporaba potrdil in ključev

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.5. Upravljanje s politiko

1.5.1 Upravljavec politik

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.5.2 Kontaktne osebe

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.5.3 Odgovorna oseba glede skladnosti delovanja izdajatelja s politiko

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.5.4 Postopek za sprejem nove politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.6. Izrazi in okrajšave

1.6.1 Izrazi

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.6.2 Okrajšave

[2] Namen uporabe potrdila za podpis kode je dodatno omejen na overjanje izvršljive programske kode.
[3] Namen uporabe potrdila za avtentikacijo spletišč je dodatno omejen na vzpostavljanje varne povezave.

© Državni center za storitve zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

2. OBJAVE IN ODGOVORNOSTI GLEDE REPOZITORIJA

2.1. Repozitoriji

Določbe so opredeljene v Krovni politiki SI-TRUST.

2.2. Objava informacij o potrdilih

(1) SI-TRUST javno objavlja naslednje dokumente oz. podatke izdajatelja SIGEN-CA:
- politike delovanja izdajatelja,
- cenik,
- zahtevke za storitve izdajatelja,
- navodila za varno uporabo digitalnih potrdil,
- informacije o veljavni zakonodaji v zvezi z delovanjem SI-TRUST ter
- ostale informacije v zvezi z delovanjem SIGEN-CA.

(2) 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).

(3) Ostali dokumenti oz. ključni podatki o delovanju izdajatelja SIGEN-CA ter splošna obvestila imetnikom in tretjim osebam se objavijo na spletnih straneh https://www.si-trust.gov.si.

(4) Zaupni del notranjih pravil SI-TRUST, znotraj katerega deluje izdajatelj SIGEN-CA, ni javno dostopen dokument.

(5) SI-TRUST je odgovoren za pravočasnost in verodostojnost objavljenih dokumentov in ostalih podatkov.

2.3. Pogostnost javne objave

Določbe so opredeljene v Krovni politiki SI-TRUST.

2.4. Dostop do repozitorijev

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

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

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

https://www.si-trust.gov.si/sl/ss-obrazci/iskanje-digitalnih-potrdil-si-trust/.

(4) SI-TRUST oz. izdajatelj SIGEN-CA v skladu z Interno politiko SI-TRUST skrbi za pooblaščeno in varno

© Državni center za storitve zaupanja

dodajanje, spreminjanje ali brisanje podatkov v javnem imeniku potrdil.

3. ISTOVETNOST IN VERODOSTOJNOST

3.1. Določanje imen

3.1.1 Oblika imen

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

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

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

(4) Naziv, ki je vključen v razločevalno ime, je v primeru potrdila:
- za zaposlene navedeno imetnikovo ime in priimek,
- za zaposlene s splošnim nazivom organizacije oz. organizacijske enote splošni naziv oz. organizacijska enota organizacije ter imetnikovo ime in priimek,
- za informacijske sisteme naziv sistema,
- za podpis kode naziv organizacije oz. njene organizacijske enote,
- za avtentikacijo spletišč registrirano ime spletišča,
- za elektronske žige oznaka, ki nedvoumno predstavlja organizacijo oz. njeno storitev.

(5) Podatki o organizaciji so v razločevalnem imenu podani v obliki oznake organizacije in njene davčne številke (glej o tem tudi naslednje podpoglavje).

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

(7) Razločevalno ime se glede na vrsto identitete oz. potrdila tvori po naslednjih pravilih[5].

Vrsta potrdila	Naziv polja	Razločevalno ime[6]
potrdilo izdajatelja SIGEN-CA	izdajatelj, angl. *issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
posebna potrdila za zaposlene	imetnik, angl. *subject*	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>, cn=<ime in priimek>, gn=<ime>, surname=<priimek>,

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

© Državni center za storitve zaupanja

		sn=<serijska številka>
posebna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote	imetnik, angl. *subject*	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>, cn=<naziv>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
spletna potrdila za zaposlene	imetnik, angl. *subject*	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>, cn=<ime in priimek>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
spletna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote	imetnik, angl. *subject*	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>, cn=<naziv>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
spletna potrdila za informacijske sisteme	imetnik, angl. *subject*	c=SI , st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>
spletna potrdila za podpis kode	imetnik, angl. *subject*	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>
spletna potrdila za avtentikacijo spletišč	imetnik, angl. *subject*	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>, l=<kraj organizacije>, bc=<vrsta organizacije>, jur=<nivo registracije>, cn=<naziv>, sn=NTRSI-<matična št. organizacije>/SITRUST-<serijska številka>
spletna potrdila za elektronske žige	imetnik, angl. *subject*	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>, cn=<naziv>,

© Državni center za storitve zaupanja

		sn=<serijska številka>

3.1.2 Zahteva po smiselnosti imen

(1) Oznaka organizacije, ki je v skladu z določili podpogl. 3.1.1 vključena v razločevalno ime, mora izpolnjevati naslednje zahteve:
- mora biti registrirana v poslovnem ali drugem uradnem registru[7],
- največja dolžina je lahko šestdeset (60) znakov[8].

(2) SIGEN-CA si pridržuje pravico do zavrnitve naziva, če ugotovi:
- da je le-ta neprimeren oz. žaljiv,
- da je zavajajoč za tretje stranke oz. pripada neki drugi pravni ali fizični osebi,
- da je v nasprotju z veljavnimi predpisi.

(3) V primeru potrdila za avtentikacijo spletišč mora biti za ime spletišča navedeno polno domensko ime (angl. *fully qualified domain name*).

(4) Podatki o imetniku oz. nazivu v razločevalnem imenu vsebujejo znake iz kodne tabele UTF-8.

3.1.3 Uporaba anonimnih imen ali psevdonimov

Ni predvidena.

3.1.4 Pravila za interpretacijo imen

Pravila so navedena v podpogl. 3.1.1 in 3.1.2.

3.1.5 Enoličnost imen

(1) Podeljeno razločevalno ime je enolično za vsako izdano potrdilo.

(2) Enolična je tudi serijska številka, ki je vključena v razločevalno ime.

(3) Serijska številka je 13-mestno število in enolično določa imetnika oz. izdano potrdilo. Spodnja tabela natančneje določa pomen in vrednosti posameznih mest serijskega števila:

Serijska številka	Pomen	Vrednost	
1. mesto	oznaka za potrdilo, ki ga je izdal izdajatelj SIGEN-CA	2	
2.- 8. mesto	enolično število imetnika	/	
9. - 10. mesto	oznaka za posebno potrdilo	zaposlen	20
		zaposlen s splošnim nazivom	22
	oznaka za spletno potrdilo	zaposlen	16
		zaposlen s splošnim nazivom	18

[7] Oznaka mora biti izpeljana iz registriranega skrajšanega ali polnega imena organizacije.
[8] Pri registriranem imenu, daljšem od 60 znakov, se oznako določi kot prvih 60 znakov imena.

© Državni center za storitve zaupanja

		informacijski sistem	10
		podpis kode	19
		spletišče	13
		elektronski žig	15
11. – 12. mesto	zaporedno število istovrstnega potrdila	/	
13. mesto	kontrolna številka	/	

3.1.6 Priznavanje, verodostojnost in vloga blagovnih znamk

Določbe so opredeljene v Krovni politiki SI-TRUST.

3.2. Začetno preverjanje istovetnosti

3.2.1 Metoda za dokazovanje lastništva zasebnega ključa

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

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

3.2.2 Preverjanje istovetnosti organizacij

(1) Podatki o organizaciji so navedeni v obliki oznake organizacije in njene davčne številke, glej podpogl. 3.1.1 in 3.1.2.

(2) Za pravilnost podatkov jamči odgovorna oseba organizacije s podpisom na zahtevku za pridobitev potrdila.

(3) Izdajatelj SIGEN-CA pri ustreznih službah oz. v uradnih evidencah preveri pravilnost podatkov o organizaciji in istovetnosti odgovorne osebe.

(4) Pri spletnih potrdilih za avtentikacijo spletišč izdajatelj SIGEN-CA preveri lastništvo oz. nadzor nad spletno domeno v osnovnem in vseh dodatnih imenih spletišč na enega od naslednjih načinov:

- izdajatelj SIGEN-CA pošlje sporočilo z enkratno oznako na elektronske naslove »admin«, »administrator«, »webmaster«, »hostmaster« in »postmaster« spletne domene v imenu spletišča; izdajo potrdila omogoči, ko za vsako spletno domeno prejme potrditev,
- izdajatelj SIGEN-CA pošlje sporočilo z enkratno oznako na elektronski naslov, določen v oznaki *contactemail* zapisa DNS CAA; izdajo potrdila omogoči, ko za vsako spletno domeno prejme potrditev,
- za spletne domene, registrirane pri Ministrstvu za javno upravo, izdajatelj SIGEN-CA preveri lastništvo domene pri kontaktni osebi lastnika domene; izdajo potrdila omogoči, ko za vsako spletno domeno prejme potrditev.

(5) Pri spletnih potrdilih za avtentikacijo spletišč izdajatelj SIGEN-CA preveri zapise DNS CAA za spletno domeno v osnovnem in vseh dodatnih imenih spletišč in omogoči izdajo potrdila, če za vsako spletno domeno:

- ne obstaja nobena oznaka *issue* zapisa DNS CAA ali

© Državni center za storitve zaupanja

- obstaja oznaka *issue* zapisa DNS CAA z vrednostjo »si-trust.gov.si«.

3.2.3 Preverjanje istovetnosti fizičnih oseb

(1) Organizacija za svoje zaposlene osebe preverja njihovo istovetnost po določilih SIGEN-CA in sicer odgovorna oseba organizacije jamči:
- za istovetnost bodočega imetnika potrdila, ki ga je preveril v skladu z veljavno zakonodajo 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 SIGEN-CA preveri osebne podatke o imetnikih v ustreznih registrih.

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

3.2.4 Nepreverjeni podatki pri začetnem preverjanju

(1) Nepreverjeni podatek v potrdilu je naziv za:
- splošne nazive,
- informacijske sisteme in
- podpis kode ter
- imena spletišč.

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

3.2.5 Preverjanje pooblastil

Organizacija oz. odgovorna oseba organizacije s podpisom jamči, da želi za določeno osebo, ki je zaposlena ali opravlja naloge za to organizacijo, da le-ta pridobi potrdilo bodisi zase ali za informacijski sistem, podpis kode, spletišče ali elektronski žig, s katerim bo ta oseba upravljala.

3.2.6 Merila za medsebojno povezovanje

(1) Izdajatelj SIGEN-CA je medsebojno priznan s strani korenskega izdajatelja SI-TRUST Root.

(2) Izdajatelj SIGEN-CA se medsebojno ne povezuje z drugimi izdajatelji.

(3) SI-TRUST se preko korenskega izdajatelja SI-TRUST Root lahko povezuje z drugimi ponudniki storitev zaupanja, kar se ureja z medsebojnim dogovorom oz. pogodbo.

3.3. Istovetnost in verodostojnost ob obnovi potrdila

3.3.1 Istovetnost in verodostojnost ob obnovi

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

© Državni center za storitve zaupanja

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

3.3.2 Istovetnost in verodostojnost ob obnovi po preklicu

Preverjanje imetnikov poteka skladno z določili iz podpogl. 3.2.3.

3.4. Istovetnost in verodostojnost ob zahtevi za preklic

(1) Zahtevek za preklic potrdila imetnik oz. odgovorna oseba 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 SI-TRUST, s tem pa izkazana tudi istovetnost prosilca.

(2) V primeru preklica preko telefona na dežurno telefonsko številko izdajatelja SIGEN-CA mora imetnik navesti v ta namen izbrano geslo.

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

4. UPRAVLJANJE S POTRDILI

4.1. Zahtevek za pridobitev potrdila

4.1.1 Kdo lahko predloži zahtevek za pridobitev potrdila

Bodoči imetniki potrdil so vedno fizične osebe, zaposlene v organizaciji, za katere le-ta želi pridobiti potrdilo. V primeru potrdila za informacijske sisteme, podpis kode, avtentikacijo spletišč in elektronske žige je imetnik takega potrdila pooblaščen s strani odgovorne osebe. Podrobno o tem že v podpogl. 1.3.3.

4.1.2 Postopek za pridobitev potrdila in odgovornosti

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

(2) Bodoči imetnik lahko izdajatelju SIGEN-CA po elektronski poti posreduje zahtevek, digitalno podpisan z njegovim veljavnim kvalificiranim digitalnim potrdilom za elektronski podpis za poslovne subjekte, ki mu ga je izdal izdajatelj SIGEN-CA. V izjemnih primerih je zahtevek lahko digitalno podpisan z veljavnim kvalificiranim digitalnim potrdilom za elektronski podpis, ki ga je izdal izdajatelj, vpisan v zanesljivi seznam ponudnikov kvalificiranih storitev zaupanja v Republiki Sloveniji. Elektronski podpis, ustvarjen s tovrstnim potrdilom, se lahko uporabi tudi pri podpisu odgovorne osebe.

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

(4) Odgovorna oseba s svojim podpisom lahko pooblasti drugo osebo, da le-ta zahtevek prinese na prijavno službo.

© Državni center za storitve zaupanja

(5) Bodoči imetnik in odgovorna oseba 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 SIGEN-CA.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

4.2.1 Preverjanje istovetnosti in verodostojnosti bodočega imetnika

(1) Odgovorna oseba organizacije, kjer je bodoči imetnik potrdila zaposlen, jamči za istovetnost bodočega imetnika potrdila, ki ga je preverila v skladu z veljavno zakonodajo.

(2) V primeru oddaje zahtevka na elektronski način pooblaščena oseba izdajatelja SIGEN-CA opravi overjanje elektronskega podpisa. Istovetnost bodočega imetnika se izkaže z veljavnostjo njegovega elektronskega podpisa.

(3) Izdajatelj SIGEN-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) Pred oddajo zahtevka izdajatelj SIGEN-CA seznani odgovorno osebo in bodočega imetnika z vso potrebno dokumentacijo v skladu z veljavno zakonodajo.

(2) Zahtevek za pridobitev potrdila odobrijo oz. v primeru nepravilnih ali pomanjkljivih podatkov ali neizpolnjevanja obveznosti iz dogovora s strani organizacije zavrnejo pooblaščene osebe SI-TRUST.

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

4.2.3 Čas za izdajo potrdila

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

4.3. Izdaja potrdila

4.3.1 Postopek izdajatelja ob izdaji potrdila

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

(2) Potrdila se izdajajo izključno na infrastrukturi SI-TRUST.

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

© Državni center za storitve zaupanja

4.3.2 Obvestilo imetniku o izdaji potrdila

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

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

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila

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

(2) Način in podrobna navodila za prevzem vseh vrst potrdil po tej politiki so opisana na spletni strani https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/. 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. V kolikor izdajatelja SIGEN-CA ne obvesti o morebitnih napakah, se smatra, da se z vsebino strinja in da soglaša s pogoji delovanja in prevzemom obveznosti in odgovornosti.

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

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

4.4.2 Objava potrdila

Izdano potrdilo se javno objavi v repozitoriju SI-TRUST, kot je navedeno v pogl. 2.

4.4.3 Obvestilo o izdaji tretjim osebam

Ni predpisano.

4.5. Uporaba potrdil in ključev

4.5.1 Uporaba potrdila in zasebnega ključa imetnika

(1) Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnih ključev dolžan:

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

© Državni center za storitve zaupanja

(2) Imetnik mora varovati zasebni ključ za podpisovanje podatkov pred nepooblaščeno uporabo.

(3) Ostale dolžnosti in odgovornosti so določene v podpogl. 9.6.3.

4.5.2 Uporaba potrdila in javnega ključa za tretje osebe

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6. Ponovna izdaja potrdila brez spremembe javnega ključa

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.1 Razlogi za ponovno izdajo potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.2 Kdo lahko zahteva ponovno izdajo

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.3 Postopek ob ponovni izdaji potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.4 Obvestilo imetniku o izdaji novega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.5 Prevzem ponovno izdanega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.6 Objava ponovno izdanega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.7 Obvestilo o izdaji drugim subjektom

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.7. Obnova potrdila (velja samo za posebna potrdila)

© Državni center za storitve zaupanja

(1) Pri posebnih potrdilih je omogočena obnova potrdila, ki se lahko izvaja samodejno pred potekom potrdila ali kot regeneriranje ključev na zahtevo imetnika.

(2) Posebno potrdilo, ki se obnovi, vsebuje enako razločevalno ime kot prvotno potrdilo.

(2) Samodejno 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 SIGEN-CA v obdobju stotih (100) dni pred zadnjim dnem veljavnosti potrdila.

(4) Samodejno podaljševanje veljavnosti posebnih potrdil, izdanih pred 6.6.2016 in podpisanih s potrdilom št. 1 izdajatelja SIGEN-CA, ni podprto.

4.7.1 Razlogi za regeneriranje ključev

(1) Regeneriranje ključev za posebno potrdilo se izvede, če imetnik potrdila:
- pozabi geslo za dostop do zasebnih ključev,
- 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) SI-TRUST si glede na varnostne okoliščine pridržuje samostojno odločitev med:
- regeneriranjem ključev
- ali preklicem.

(3) Regeneriranje ključev posebnih potrdil, izdanih pred 6.6.2016 in podpisanih s potrdilom št. 1 izdajatelja SIGEN-CA, je dovoljeno le za potrebe dostopa do zgodovine ključev za dešifriranje po predhodnem dogovoru z izdajateljem SIGEN-CA. Postopek se lahko izvaja le do poteka veljavnosti potrdila št. 1 izdajatelja SIGEN-CA tj. do 29.6.2021.

4.7.2 Kdo lahko zahteva regeneriranje ključev

Regeneracijo lahko zahteva imetnik potrdila skupaj z odgovorno osebo.

4.7.3 Postopek pri regeneriranju ključev

(1) Regeneriranje ključev za potrdila se izvede na osnovi izpolnjenega zahtevka za regeneriranje ključev s strani imetnika potrdila in odgovorne osebe, ki se odda na prijavni službi SIGEN-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) SIGEN-CA imetniku avtorizacijsko kodo in referenčno številko posreduje najkasneje v desetih (10) dneh od obravnave zahtevka za regeneracijo (podpogl. 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 SIGEN-CA rezervacijo potrdila prekliče.

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

© Državni center za storitve zaupanja

4.7.4 Obvestilo imetniku o regeneriranju ključev

Postopek je enak kot pri prvi izdaji potrdila, glej podpogl. 4.3.2.

4.7.5 Prevzem regeneriranega potrdila

Postopek je enak kot pri prvem prevzemu potrdila, glej podpogl, 4.4.1.

4.7.6 Objava obnovljenega potrdila

Postopek je enak kot pri prvem prevzemu potrdila, glej podpogl, 4.4.2.

4.7.7 Obvestilo o izdaji drugim subjektom

Postopek je enak kot pri prvem prevzemu potrdila, glej podpogl, 4.4.3.

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 Razlogi za spremembo potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.2 Kdo lahko zahteva spremembo

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.3 Postopek ob spremembi potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.4 Obvestilo imetniku o izdaji novega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.5 Prevzem spremenjenega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

4.8.6 Objava spremenjenega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.7 Obvestilo o izdaji drugim subjektom

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9. Preklic in začasna razveljavitev potrdila[9]

4.9.1 Razlogi za preklic

(1) Preklic potrdila morata imetnik ali odgovorna oseba 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 SIGEN-CA prekliče potrdilo tudi brez zahteve imetnika ali odgovorna oseba 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 SI-TRUST,
- da niso poravnani stroški za upravljanje digitalnih potrdil,
- da je bila infrastruktura SI-TRUST 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 SIGEN-CA prenehal z izdajanjem potrdil ali da je bilo SI-TRUST prepovedano upravljanje s potrdili in njegove dejavnosti ni prevzel drug ponudnik storitev zaupanja,
- da je preklic odredilo pristojno sodišče ali upravni organ.

4.9.2 Kdo lahko zahteva preklic

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

(2) Preklic potrdila lahko zahteva tudi odgovorna oseba organizacije.

4.9.3 Postopek za preklic

(1) Preklic lahko imetnik zahteva:

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

© Državni center za storitve zaupanja

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

(2) Preklic lahko odgovorna oseba organizacije zahteva:
- osebno v času uradnih ur na prijavni službi,
- elektronsko po elektronski pošti štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe potrdila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov.

(3) Če je delovanje SI-TRUST zaradi nepredvidenih dogodkov bistveno okrnjeno, lahko imetnik ali odgovorna oseba preklic zahteva zgolj osebno v času uradnih ur na prijavni službi.

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

(5) O datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic sta imetnik in odgovorna oseba obveščena po elektronski pošti.

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

4.9.4 Čas za izdajo zahtevka za preklic

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

4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica

(1) SI-TRUST 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) Če je delovanje SI-TRUST zaradi nepredvidenih dogodkov bistveno okrnjeno, se preklic zaradi nevarnosti zlorabe ali nezanesljivosti ipd. izvede najkasneje v štiriindvajsetih (24) urah po prejemu veljavne zahteve za preklic.

(3) Po preklicu je potrdilo takoj dodano v register preklicanih potrdil in brisano iz javnega imenika potrdil[10].

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

© Državni center za storitve zaupanja

4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.7 Pogostnost objave registra preklicanih potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.8 Čas do objave registra preklicanih potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.9 Sprotno preverjanje statusa potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.10 Zahteve za sprotno preverjanje statusa potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.11 Drugi načini za dostop do statusa potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.12 Druge zahteve pri zlorabi zasebnega ključa

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.13 Razlogi za začasno razveljavitev

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.14 Kdo lahko zahteva začasno razveljavitev

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.15 Postopek za začasno razveljavitev

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.16 Čas začasne razveljavitve

© Državni center za storitve zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.10. Preverjanje statusa potrdil

4.10.1 Dostop za preverjanje

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

4.10.2 Razpoložljivost

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.10.3 Druge možnosti

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.11. Prekinitev razmerja med imetnikom in izdajateljem

Razmerje med imetnikom in SI-TRUST se prekine, če
- imetnikovo potrdilo preteče in ga le-ta ne podaljša,
- je potrdilo preklicano, imetnik pa ne zaprosi za novega.

4.12. Odkrivanje kopije ključev za dešifriranje

4.12.1 Postopek za odkrivanje ključev za dešifriranje (velja samo za posebna potrdila)

(1) SIGEN-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) SIGEN-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 6.6.2016 in podpisana s potrdilom št. 1 izdajatelja SIGEN-CA, se lahko izvaja le do poteka veljavnosti potrdila št. 1 izdajatelja SIGEN-CA tj. do 29.6.2021.

4.12.1.1 Kdo zahteva odkrivanje kopije ključev za dešifriranje

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

© Državni center za storitve zaupanja

4.12.1.2 Postopek ob zahtevku za odkrivanje kopije ključev za dešifriranje

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

(2) SIGEN-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.

4.12.2 Postopek za odkrivanje ključa seje

Določbe so opredeljene v Krovni politiki SI-TRUST.

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

5.1. Fizično varovanje

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.1 Lokacija in zgradba ponudnika storitev zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.2 Fizični dostop do infrastrukture ponudnika storitev zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.3 Napajanje in prezračevanje

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.4 Zaščita pred poplavo

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.5 Zaščita pred požari

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.6 Hramba nosilcev podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

5.1.7 Odstranjevanje odpadkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.8 Hramba na oddaljeni lokaciji

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.2. Organizacijska struktura izdajatelja oz. ponudnika storitev zaupanja

5.2.1 Organizacija ponudnika storitev zaupanjain zaupanja vredne vloge

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.2.2 Število oseb za posamezne vloge

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.2.3 Izkazovanje istovetnosti za opravljanje posameznih vlog

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.2.4 Nezdružljivost vlog

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3. Nadzor nad osebjem

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.1 Potrebne kvalifikacije in izkušnje osebja ter njegova primernost

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.2 Preverjanje primernosti osebja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.3 Izobraževanje osebja

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

5.3.4 Zahteve za redna usposabljanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.5 Menjava nalog

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.6 Sankcije

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.7 Zahteve za zunanje izvajalce

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.8 Dostop osebja do dokumentacije

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4. Varnostni pregledi sistema

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.1 Vrste beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.2 Pogostost pregledov dnevnikov beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.3 Čas hrambe dnevnikov beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.4 Zaščita dnevnikov beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

5.4.5 Varnostne kopije dnevnikov beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.6 Zbiranje podatkov za dnevnike beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.7 Obveščanje povzročitelja dogodka

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.8 Ocena ranljivosti sistema

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5. Arhiviranje podatkov

5.5.1 Vrste arhiviranih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.2 Čas hrambe

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.3 Zaščita arhiviranih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.4 Varnostno kopiranje arhiviranih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.5 Zahteva po časovnem žigosanju

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.6 Način zbiranja arhiviranih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

5.5.7 Postopek za dostop do arhiviranih podatkov in njihova verifikacija

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.6. Obnova izdajateljevega potrdila

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

5.7. Okrevalni načrt

5.7.1 Postopek v primeru vdorov in zlorabe

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.7.2 Postopek v primeru okvare strojne in programske opreme ali podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.7.3 Postopek v primeru ogroženega zasebnega ključa izdajatelja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.7.4 Okrevalni načrt

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.8. Prenehanje delovanja izdajatelja

Določbe so opredeljene v Krovni politiki SI-TRUST.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev ključev

6.1.1 Generiranje ključev

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

(2) Zapisnik postopka se varno shrani.

(3) Morebitne kasnejše spremembe v avtorizacijah ali pomembne spremembe nastavitev informacijskega sistema

© Državni center za storitve zaupanja

SIGEN-CA, ki so opravljene ob vzpostavitvi sistema, se dokumentirajo v posebnem zapisniku oz. v ustreznem dnevniku.

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

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

Tip potrdila	Potrdilo	Ključ se generira
posebno za zaposlene in za zaposlene s splošnim nazivom	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	pri imetniku
	par ključev za dešifriranje/šifriranje (potrdilo za šifriranje)	pri izdajatelju SIGEN-CA
spletno za zaposlene, za zaposlene s splošnim nazivom, informacijske sisteme in avtentikacijo spletišč	par ključev za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	pri imetniku
potrdilo za podpis kode in elektronske žige	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	pri imetniku

6.1.2 Dostava zasebnega ključa imetnikom

Način varnega prenosa zasebnega ključa je podan v spodnji tabeli.

Tip potrdila	Potrdilo	Ključ	Dostava
posebno	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	zasebni ključ za podpisovanje	ni prenosa[11]
	par za dešifriranje/šifriranje (potrdilo za šifriranje)	zasebni ključ za dešifriranje	prenos od izdajatelja do imetnika po PKIX-CMP
spletno	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 imetniki svoj javni ključ dostavijo v podpis izdajatelju SIGEN-CA po protokolu PKIX-CMP za posebna potrdila in protokolu PKCS#7 za spletna potrdila.

6.1.4 Dostava izdajateljevega javnega ključa tretjim osebam

(1) Potrdilo z javnim ključem izdajatelja SIGEN-CA je objavljeno v repozitoriju SI-TRUST (glej podpogl. 2.1).

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

[11] Ključ se generira pri imetniku in se nikoli ne hrani pri izdajatelju SIGEN-CA.
[12] RFC 3647 ne predvideva opisa načina dostave potrdil imetnikom.

© Državni center za storitve zaupanja

- v javnem imeniku *x500.gov.si* po protokolu LDAP (glej podpogl. 2.3),
- v obliki PEM na naslovu https://www.si-trust.gov.si/assets/si-trust-root/povezovalni-podrejeni/sigenca/sigen-ca.xcert.pem oz. https://www.si-trust.gov.si/assets/si-trust-root/povezovalni-podrejeni/sigenca-g2/sigen-ca-g2.xcert.pem,
- 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 SIGEN-CA	3072
potrdilo za: • zaposlene • zaposlene s splošnim nazivom • informacijske sisteme • podpis kode • avtentikacijo spletišč • elektronske žige	2048[13]
potrdilo za sistem OCSP	2048

6.1.6 Generiranje in kakovost parametrov javnih ključev

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.1.7 Namen ključev in potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.2. Zaščita zasebnega ključa in varnostni moduli

6.2.1 Standardi za kriptografski modul

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.2.2 Nadzor zasebnega ključa s strani pooblaščenih oseb

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.2.3 Odkrivanje kopije zasebnega ključa

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

[13] Vrednost pomeni minimalno predpisano dolžino.

© Državni center za storitve zaupanja

(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

(1) Izdajatelj SIGEN-CA zagotavlja varnostno kopijo svojega zasebnega ključa. Podrobnosti so določene v Interni politiki SI-TRUST.

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

6.2.5 Arhiviranje zasebnega ključa

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

6.2.6 Prenos zasebnega ključa iz/v kriptografski modul

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

(2) Zasebni ključi za dešifriranje posebnih potrdil imetnikov se iz mesta, kjer se ustvarijo, tj. pri izdajatelju SIGEN-CA, prenesejo na imetnikovo stran po protokolu PKIX-CMP.

(3) Ostali zasebni ključi imetnikov se generirajo pri imetniku.

6.2.7 Zapis zasebnega ključa v kriptografskem modulu

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

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

6.2.8 Postopek za aktiviranje zasebnega ključa

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

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

6.2.9 Postopek za deaktiviranje zasebnega ključa

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

(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.

© Državni center za storitve zaupanja

6.2.10 Postopek za uničenje zasebnega ključa

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

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

6.2.11 Lastnosti kriptografskega modula

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.3. Ostali vidiki upravljanja ključev

6.3.1 Arhiviranje javnega ključa

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.3.2 Obdobje veljavnosti potrdila in ključev

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

Tip potrdila	Par ključev	Ključi	Veljavnost
posebno potrdilo za zaposlene in za zaposlene s splošnim nazivom	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, za zaposlene s splošnim nazivom in za informacijske sisteme	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	5 let
		javni ključ	5 let
spletno potrdilo za avtentikacijo spletišč	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	13 mesecev
		javni ključ	13 mesecev
spletno potrdilo za podpis kode in elektronske žige	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	zasebni ključ za podpisovanje	5 let
		javni ključ za overjanje podpisa	5 let

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

6.4. Gesla za dostop do zasebnega ključa

6.4.1 Generiranje gesel

(1) Pooblaščene osebe izdajatelja za dostop do zasebnega ključa SIGEN-CA uporabljajo močna gesla, s katerimi ravnajo v skladu z Interno politiko SI-TRUST.

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

© Državni center za storitve zaupanja

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

(4) SIGEN-CA priporoča uporabo varnih gesel:
- mešano uporaba velikih in malih črk, števil in posebnih znakov,
- dolžine vsaj 8 znakov,
- odsvetuje se uporabo besed, ki so zapisane v slovarjih.

6.4.2 Zaščita gesel

(1) Gesla pooblaščenih oseb izdajatelja SIGEN-CA za dostop do zasebnega ključa izdajatelja SIGEN-CA se shranijo v skladu z Interno politiko SI-TRUST.

(2) Aktivacijska podatka za prevzem potrdila se kreirata varno pri izdajatelju SIGEN-CA.

(3) SIGEN-CA posreduje bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo po dveh ločenih poteh:
- referenčno številko po elektronski pošti,
- avtorizacijsko kodo po pošti,
- 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) SIGEN-CA priporoča, da se geslo za dostop do zasebnega ključa ne shranjuje oz. se shrani na varno mesto in da ima do njega dostop le imetnik.

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

6.4.3 Drugi vidiki gesel

Niso predpisani.

6.5. Varnostne zahteve za računalniško opremo izdajatelja

6.5.1 Specifične tehnične varnostne zahteve

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.5.2 Nivo varnostne zaščite

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1 Nadzor razvoja sistema

© Državni center za storitve zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.6.2 Upravljanje varnosti

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.6.3 Nadzor življenjskega cikla

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.7. Varnostna kontrola računalniške mreže

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

(2) V skladu z veljavno zakonodajo je to podrobneje določeno v Interni politiki SI-TRUST.

6.8. Časovno žigosanje

Določbe so opredeljene v Krovni politiki SI-TRUST.

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

7.1. Profil potrdil

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

- posebna potrdila za zaposlene,
- spletna potrdila za zaposlene,
- posebna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote,
- spletna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote,
- spletna potrdila za informacijske sisteme,
- spletna potrdila za podpis kode,
- spletna potrdila za avtentikacijo spletišč ter
- spletna potrdila za elektronske žige.

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

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

7.1.1 Različica potrdil

[14] Potrdilo izdajatelja SIGEN-CA je podrobno podano že v .podpogl. 1.3.1.

© Državni center za storitve zaupanja

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

7.1.2 Profil potrdil z razširitvami

7.1.2.1 Profil potrdila SIGEN-CA

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

7.1.2.2 Profil potrdil za imetnike

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*	3
Identifikacijska oznaka, 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, oi=VATSI-17659957, cn=SIGEN-CA G2
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 podpogl. 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)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*dolžina ključa je min. 2048 bitov, glej podpogl. 6.1.5*
Razširitve X.509v3	
Alternativno ime, OID 2.5.29.17, angl. *Subject Alternative Name*	*ime spletišča pri spletnih potrdilih za avtentikacijo spletišč, glej podpogl. 7.1.2.4* *elektronski naslov imetnika pri ostalih potrdilih, glej podpogl. 7.1.2.3*
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	Url: http://www.sigen-ca.si/crl/sigen-ca-g2.crl Url: ldap://x500.gov.si/cn=SIGEN-CA G2, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2, cn=CRL<*zaporedna številka registra, glej podpogl. 7.2.2*>

© Državni center za storitve zaupanja

Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. *Authority Information Access*	Access Method: OCSP (OID 1.3.6.1.5.5.7.48.1) Access Location: URL=http://ocsp.sigen-ca.si Access Method: CaIssuer (OID 1.3.6.1.5.5.7.48.2) Access Location: URL=http://www.sigen-ca.si/crt/sigen-ca-g2-certs.p7c
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	*odvisna od vrste potrdila, glej podpogl. 7.1.2.2.1 in 7.1.2.2.2*
Razširjena uporaba ključa, OID 2.5.29.37, angl. *Extended Key Usage*	*odvisno od vrste potrdila, glej podpogl. 7.1.2.2.1 in 7.1.2.2.2*
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	4C25 278C A82D 729E
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 podpogl. 7.1.2.2.1 in 7.1.2.2.2* [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*	*odvisno od vrste potrdila, glej podpogl. 7.1.2.2.1 in 7.1.2.2.2*
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	CA: FALSE Brez omejitev dolžine (Path Length Constraint: none)
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1 angl. *Certificate Fingerprint – SHA-1*	*razpoznavni odtis potrdila po SHA-1*
Odtis potrdila SHA-256 angl. *Certificate Fingerprint – SHA-256*	*razpoznavni odtis potrdila po SHA-256*

7.1.2.2.1 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 so odvisna od vrste le-tega, pa so podana v nadaljevanju.

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

Naziv polja	Vrednost pri potrdilu za šifriranje	
	zaposlen	zaposlen s splošnim nazivom
Uporaba ključa, angl. *Key Usage*	Key Encipherment	
Razširjena uporaba ključa, 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: 1.3.6.1.4.1.6105.2.1.2.5	Policy: 1.3.6.1.4.1.6105.2.1.4.5

© Državni center za storitve zaupanja

Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	/

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

Naziv polja	Vrednost pri potrdilu za overjanje podpisa	
	zaposlen	zaposlen s splošnim nazivom
Uporaba ključa, angl. *Key Usage*	Digital Signature, ContentCommitment	
Razširjena uporaba ključa, 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: 1.3.6.1.4.1.6105.2.1.2.5 0.4.0.194112.1.0	Policy: 1.3.6.1.4.1.6105.2.1.4.5 0.4.0.194112.1.0
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	QcCompliance statement QcType: esign PdsLocation: https://www.ca.gov.si/cps/sigenca1_pds_en.pdf, https://www.ca.gov.si/cps/sigenca1_pds_sl.pdf	

(4) Polje *uporaba ključa* (angl. *Key Usage*) je za vse vrste posebnih potrdil označeno kot kritično (angl. *critical*).

7.1.2.2.2 Profil spletnih potrdil

(1) Spletno potrdilo vključuje podatke, ki so navedeni v tabeli v podpogl. 7.1.2. Vrednosti polj za *uporabo ključa, razširjeno uporabo ključa, politiko ter oznako kvalificiranega potrdila,* ki pa so odvisne od vrste potrdila, so za spletno potrdilo podane v spodnji tabeli.

Naziv polja	Vrednost pri spletnem potrdilu			
	zaposlen	zaposlen s splošnim nazivom	informacijski sistem	podpis kode
Uporaba ključa, angl. *Key Usage*	Digital Signature, Key Encipherment, ContentCommitment		Digital Signature, Key Encipherment	Digital Signature
Razširjena uporaba ključa, angl. *Extended Key Usage*	/		/	code Signing
Politike, pod katerimi je bilo izdano potrdilo (OID), in iz katerih je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.2.1.1.5 0.4.0.194112.1.0	Policy: 1.3.6.1.4.1.6105.2.1.3.5 0.4.0.194112.1.0	Policy: 1.3.6.1.4.1.6105.2.1.5.5	Policy: 1.3.6.1.4.1.6105.2.1.6.5
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	QcCompliance statement QcType: esign PdsLocation: https://www.ca.gov.si/cps/sigenca1_pds_en.pdf, https://www.ca.gov.si/cps/sigenca1_pds_sl.pdf		/	

Naziv polja	Vrednost pri spletnem potrdilu	
	avtentikacija spletišč	elektronski žig

© Državni center za storitve zaupanja

Uporaba ključa, angl. *Key Usage*	Digital Signature, Key Encipherment,	Digital Signature, ContentCommitment
Razširjena uporaba ključa, angl. *Extended Key Usage*	serverAuth, clientAuth	/
Politike, pod katerimi je bilo izdano potrdilo (OID), in iz katerih je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.2.1.7.5 0.4.0.194112.1.4	Policy: 1.3.6.1.4.1.6105.2.1.8.5 0.4.0.194112.1.1
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	QcCompliance statement QcType: web PdsLocation: https://www.ca.gov.si/cps/sigenca2_pds_en.pdf, https://www.ca.gov.si/cps/sigenca2_pds_sl.pdf	QcCompliance statement QcType: eseal PdsLocation: https://www.ca.gov.si/cps/sigenca2_pds_en.pdf, https://www.ca.gov.si/cps/sigenca2_pds_sl.pdf

(2) Polje *uporaba ključa* (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) SIGEN-CA si pridržuje pravico za zavrnitev zahtevka za pridobitev potrdila, če ugotovi, da je elektronski naslov:
- neprimeren oz. žaljiv,
- da je zavajajoč za tretje stranke,
- predstavlja neko drugo pravno ali fizično osebo,
- je v nasprotju z veljavnimi predpisi in standardi.

7.1.2.4 Zahteve za ime spletišča

(1) Ime spletišča je polno domensko ime, navedeno v razločevalnem imenu (glej 2. odstavek podpogl. 3.1.2).

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

7.1.3 Identifikacijske oznake algoritmov

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.4 Oblika imen

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

7.1.5 Omejitve glede imen

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.6 Oznaka politike potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.7 Uporaba razširitvenega polja za omejitev uporabe politik

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.8 Oblika in obravnava specifičnih podatkov o politiki

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.9 Obravnava kritičnega razširitvenega polja politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.2. Profil registra preklicanih potrdil

7.2.1 Različica

Določbe so opredeljene v Krovni politiki SI-TRUST.

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*	2
Izdajateljev podpis, angl. *Signature*	p*odpis SIGEN-CA*
Razločevalno ime izdajatelja, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Čas izdaje CRL, angl. *thisUpdate*	Last Update: <*čas izdaje po GMT*>
Čas izdaje naslednjega CRL, angl. *nextUpdate*	Next Update: <*čas naslednje izdaje po GMT*>

© Državni center za storitve zaupanja

Identifikacijske oznake preklicanih potrdil in čas preklica, angl. *revokedCertificate*	Serial Number: <*identifikacijska oznaka preklicanega dig. potrdila*> Revocation Date: <*čas preklica po GMT*>
Algoritem za podpis, angl. *Signature Algorithm*	sha256WithRSAEncryption
Razširitve X.509v2 CRL	
Identifikator izdajateljevega ključa, angl. *Authority Key Identifier* *(OID 2.5.29.35)*	*identifikator izdajateljevega ključa*
Številka za posamične registre (CRL1, CRL2,....), angl. *CRLnumber* *(OID 2.5.29.20)*	*zaporedna številka posamičnega registra*
Alternativno ime izdajatelja angl. *issuerAltName* *(OID 2.5.28.18)*	*se ne uporablja*
Oznaka seznama sprememb angl. *deltaCRLindicator* *(OID 2.5.29.27)*	*se ne uporablja*
Objava seznama sprememb 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.

(3) Polja v CRL niso označena kot kritična.

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

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

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

7.3. Profil sprotnega preverjanja statusa potrdil

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

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

7.3.1 Različica

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

7.3.2 Razširitve sprotnega preverjanje statusa

Določbe so opredeljene v Krovni politiki SI-TRUST.

8. INŠPEKCIJSKI NADZOR

8.1. Pogostnost inšpekcijskega nadzora

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.2. Inšpekcijska služba

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.3. Neodvisnost inšpekcijske službe

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.4. Področja inšpekcijskega nadzora

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.5. Ukrepi ponudnika storitev zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.6. Objava rezultatov inšpekcijskega nadzora

Določbe so opredeljene v Krovni politiki SI-TRUST.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik storitev

9.1.1 Cena izdaje in obnove potrdil

Stroški upravljanja s potrdili se obračunavajo organizaciji po objavljenem ceniku na spletni strani https://www.si-trust.gov.si/sl/digitalna-potrdila/poslovni-subjekti/.

© Državni center za storitve zaupanja

9.1.2 Cena dostopa do potrdil

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

9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil

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

9.1.4 Cene drugih storitev

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.1.5 Povrnitev stroškov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.2. Finančna odgovornost

9.2.1 Zavarovalniško kritje

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.2.2 Drugo kritje

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.2.3 Zavarovanje imetnikov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.3. Varovanje poslovnih podatkov

9.3.1 Varovani podatki

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.3.2 Nevarovani podatki

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.3.3 Odgovornost glede varovanja poslovnih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

9.4. Varovanje osebnih podatkov

9.4.1 Načrt varovanja osebnih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.4.2 Varovani osebni podatki

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.4.3 Nevarovani osebni podatki

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.4.4 Odgovornost glede varovanja osebnih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.4.5 Pooblastilo glede uporabe osebnih podatkov

Imetnik oz. odgovorna oseba organizacije pooblasti SI-TRUST oz. izdajatelja SIGEN-CA za uporabo osebnih podatkov na zahtevku za pridobitev potrdila ali kasneje v pisni obliki.

9.4.6 Posredovanje osebnih podatkov na uradno zahtevo

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

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

9.4.7 Druga določila glede posredovanja osebnih podatkov

Niso predpisana.

9.5. Določbe glede pravic intelektualne lastnine

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.6. Obveznosti in odgovornosti

© Državni center za storitve zaupanja

9.6.1 Obveznosti in odgovornosti izdajatelja

Določbe so opredeljene v Krovni politiki SI-TRUST.

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 SIGEN-CA,
- preverjati zahtevke,
- izdajati potrebno dokumentacijo imetnikom oz. bodočim imetnikom in organizacijam,
- posredovati zahtevke in ostale podatke na varen način na SIGEN-CA.

(2) Prijavna služba je odgovorna za izvajanje vseh določil iz teh politik in drugih zahtev, ki jih dogovorita z SI-TRUST.

9.6.3 Obveznosti in odgovornost imetnika oziroma organizacije

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

(2) Odgovorna oseba oz. organizacija je dolžna:
- skrbno prebrati politiko in določila iz dogovora med organizacijo in SI-TRUST 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 izdajatelja SIGEN-CA,
- ravnati v skladu z obvestili, politiko in dogovorom med organizacijo in SI-TRUST 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 SIGEN-CA,

© Državni center za storitve zaupanja

- 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.

(3) 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 SIGEN-CA ter veljavnih predpisov.

(4) Obveznosti imetnika oz. organizacije glede uporabe potrdil so določene v .podpogl. 4.5.1.

9.6.4 Obveznosti in odgovornost tretjih oseb

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.6.5 Obveznosti in odgovornosti drugih subjektov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.7. Zanikanje odgovornosti

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.8. Omejitev odgovornosti

Izdajatelj SIGEN-CA oz. SI-TRUST jamči za vrednost posameznega pravnega posla do vrednosti 1.000 EUR.

9.9. Poravnava škode

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.10. Veljavnost politike

9.10.1 Čas veljavnosti

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.10.2 Konec veljavnosti politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.10.3 Učinek poteka veljavnosti politike

© Državni center za storitve zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.11. Komuniciranje med subjekti

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.12. Spreminjanje dokumenta

9.12.1 Postopek uveljavitve sprememb

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.12.2 Veljavnost in objava sprememb

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.12.3 Sprememba identifikacijske oznake politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.13. Postopek v primeru sporov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.14. Veljavna zakonodaja

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.15. Skladnost z veljavno zakonodajo

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.16. Splošne določbe

9.16.1 Celovit dogovor

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.16.2 Prenos pravic

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja

9.16.3 Neodvisnost določil

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.16.4 Terjatve

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.16.5 Višja sila

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.17. Ostale določbe

9.17.1 Razumevanje določil

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.17.2 Nasprotujoča določila

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.17.3 Odstopanje od določil

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.17.4 Navzkrižno overjanje

Določbe so opredeljene v Krovni politiki SI-TRUST.

© Državni center za storitve zaupanja