



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



# **POLITIKA SIGEN-CA**

## **za spletna kvalificirana digitalna potrdila za fizične osebe**

*Javni del notranjih pravil Državnega centra za storitve zaupanja*

veljavnost: od 28. maja 2018  
verzija: 7.0

CP<sub>Name</sub>: SIGEN-CA-2

CP<sub>OID</sub>: 1.3.6.1.4.1.6105.2.2.3.5



## Zgodovina politik

Izdaje politik delovanja SIGEN-CA	
verzija: 7.0, veljavnost: od 28. maja 2018	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP <sub>OID</sub> : 1.3.6.1.4.1.6105.2.2.3.5 CP <sub>Name</sub> : SIGEN-CA-2	<b>Spremembe z verzijo 7.0:</b> <ul style="list-style-type: none"><li>v potrdilih so navedene oznake politik, kot so določene z novimi standardi,</li><li>uvredena 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,</li><li>izrazi in okrajšave so usklajeni z veljavno zakonodajo.</li></ul>
verzija: 6.0, veljavnost: od 6. junija 2016	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP <sub>OID</sub> : 1.3.6.1.4.1.6105.2.2.3.4 CP <sub>Name</sub> : SIGEN-CA-2	<b>Spremembe z verzijo 6.0:</b> <ul style="list-style-type: none"><li>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,</li><li>v potrdilu izdajatelja SIGEN-CA in vseh potrdilih imetnikov se uporablja zagostitveni algoritem SHA-256,</li><li>spremenjeno je razločevalno ime digitalnega potrdila izdajatelja SIGEN-CA,</li><li>spremenjena so razločevalna imena potrdil imetnikov, ki lahko vključujejo znake iz kodne tabele UTF-8,</li><li>podprto je sprotno preverjanje statusa potrdil po protokolu OCSP,</li><li>izdajatelj SIGEN-CA je priznan s strani korenskega izdajatelja SI-TRUST Root,</li><li>pri potrdilih imetnikov je v polju uporaba ključa (angl. Key Usage) dodana vrednost ContentCommitment</li></ul>
verzija: 5.0, veljavnost: od 7. novembra 2015	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP <sub>OID</sub> : 1.3.6.1.4.1.6105.2.2.3.3 CP <sub>Name</sub> : SIGEN-CA-2	<b>Spremembe z verzijo 5.0:</b> <ul style="list-style-type: none"><li>uporaba novega naziva za overitelja na Ministrstvu za notranje zadeve, po novem je to »Državni center za storitve zaupanja«,</li><li>kvalificirano potrdilo lahko pridobi procesno sposobna oseba, starejša od 15 let,</li><li>novi kontaktni podatki izdajatelja SIGEN-CA.</li></ul>
amandma k politiki verzije 4.0, veljavnost: od 21. marca 2014	
Amandma k Politiki SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe št. 2 / 4.0	<b>Sprememba z amandmajem št. 2 / 4.0:</b> <ul style="list-style-type: none"><li>uporaba novega naziva za overitelja na Ministrstvu za pravosodje in javno upravo, po novem je to »Overitelj na Ministrstvu za notranje zadeve«.</li></ul>
amandma k politiki verzije 4.0, veljavnost: od 23. julija 2012	
Amandma k Politiki SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe št. 1 / 4.0	<b>Sprememba z amandmajem št. 1 / 4.0:</b> <ul style="list-style-type: none"><li>uporaba novega naziva za overitelja na Ministrstvu za javno upravo, po novem je to »Overitelj na Ministrstvu za pravosodje in javno upravo«.</li></ul>
verzija: 4.0, veljavnost: od 14. septembra 2009	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP <sub>OID</sub> : 1.3.6.1.4.1.6105.2.2.3.2 CP <sub>Name</sub> : SIGEN-CA-2	<b>Spremembe z verzijo 4.0:</b> <ul style="list-style-type: none"><li>izdajatelj digitalnih potrdil SIGEN-CA izdaja kvalificirana digitalna potrdila s ključi minimalne dolžine 2048 bitov;</li><li>v kvalificiranih dig. potrdilih za fizične osebe je dodana ustrezna oznaka za kvalificirana potrdila.</li></ul>



<b>verzija: 3.1, veljavnost: od 18. maja 2007</b>	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP <sub>OID</sub> : 1.3.6.1.4.1.6105.2.2.3.1 CP <sub>Name</sub> : SIGEN-CA-2	<b>Spremembe z verzijo 3.1:</b> <ul style="list-style-type: none"><li>• <i>izdajatelj SIGEN-CA bodočemu imetniku potrdila avtorizacijske kode ne posreduje več po priporočeni pošti temveč z navadno pošto pošiljko;</i></li><li>• <i>oddaja zahtevka za pridobitev digitalnega potrdila je omogočena tudi na elektronski način z veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, izdanim s strani izdajatelja SIGEN-CA;</i></li><li>• <i>omogočena je predhodna pridobitev novega potrdila pred potekom veljavnosti prejšnjega;</i></li><li>• <i>prijavne službe overitelja morajo pri svojem delu upoštevati poslovniške za delo prijavnih služb.</i></li></ul>
<b>verzija: 3.0, veljavnost: od 28. februarja 2006</b>	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP <sub>OID</sub> : 1.3.6.1.4.1.6105.2.2.3 CP <sub>Name</sub> : SIGEN-CA-2	<b>Spremembe z verzijo 3.0:</b> <ul style="list-style-type: none"><li>• <i>uporaba novega naziva za overitelja na Centru Vlade za informatiko, po novem je to »Overitelj na Ministrstvu za javno upravo«;</i></li><li>• <i>osebna kvalificirana digitalna potrdila se po novem imenujejo »posebna kvalificirana digitalna potrdila«;</i></li><li>• <i>preklic je po novem mogoč samo v času uradnih ur, razen v nujnih primerih;</i></li><li>• <i>uporaba novega naziva za imetnike SIGEN-CA, in sicer za imetnike »pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti« uporablja izraz »poslovni subjekti«;</i></li><li>• <i>struktura dokumenta je v skladu s priporočili RFC 3647.</i></li></ul>
<b>verzija: 2, veljavnost: od 15. julija 2002</b>	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP <sub>OID</sub> : 1.3.6.1.4.1.6105.2.2.2 CP <sub>Name</sub> : SIGEN-CA-2	/
<b>verzija: 1, veljavnost: od 9. julija 2001</b>	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP <sub>OID</sub> : 1.3.6.1.4.1.6105.2.2.1 CP <sub>Name</sub> : SIGEN-CA-2	/



## VSEBINA

<b>1.</b>	<b>UVOD</b> .....	<b>12</b>
1.1.	Pregled.....	12
1.2.	Identifikacijski podatki politike delovanja .....	12
1.3.	Udeleženci infrastrukture javnih ključev .....	12
1.3.1	Ponudnik storitev zaupanja.....	13
1.3.2	Prijavna služba.....	17
1.3.3	Imetniki potrdil.....	18
1.3.4	Tretje osebe .....	18
1.3.5	Ostali udeleženci.....	18
1.4.	Namen uporabe potrdil.....	18
1.4.1	Pravilna uporaba potrdil in ključev .....	18
1.4.2	Nedovoljena uporaba potrdil in ključev .....	19
1.5.	Upravljanje s politiko .....	19
1.5.1	Upravljaavec politike .....	19
1.5.2	Kontaktne osebe .....	19
1.5.3	Odgovorna oseba glede skladnosti delovanja izdajatelja s politiko .....	19
1.5.4	Postopek za sprejem nove politike .....	19
1.6.	Izrazi in okrajšave .....	19
1.6.1	Izrazi .....	19
1.6.2	Okrajšave.....	19
<b>2.</b>	<b>OBJAVE IN ODGOVORNOSTI GLEDE REPOZITORIJA</b> .....	<b>19</b>
2.1.	Repozitoriji.....	19
2.2.	Objava informacij o potrdilih .....	19
2.3.	Pogostnost javne objave.....	20
2.4.	Dostop do repozitorijev .....	20
<b>3.</b>	<b>ISTOVETNOST IN VERODOSTOJNOST</b> .....	<b>20</b>
3.1.	Določanje imen.....	20
3.1.1	Oblika imen .....	20
3.1.2	Zahteva po smiselnosti imen .....	21
3.1.3	Uporaba anonimnih imen ali psevdonimov .....	21
3.1.4	Pravila za interpretacijo imen.....	21
3.1.5	Enoličnost imen.....	21
3.1.6	Priznavanje, verodostojnost in vloga blagovnih znamk .....	22
3.2.	Začetno preverjanje istovetnosti .....	22
3.2.1	Metoda za dokazovanje lastništva zasebnega ključa .....	22
3.2.2	Preverjanje istovetnosti organizacij.....	22
3.2.3	Preverjanje istovetnosti fizičnih oseb .....	22
3.2.4	Nepreverjeni podatki pri začetnem preverjanju.....	23
3.2.5	Preverjanje pooblastil.....	23
3.2.6	Merila za medsebojno povezovanje.....	23
3.3.	Istovetnost in verodostojnost ob obnovi potrdila.....	23
3.3.1	Istovetnost in verodostojnost ob obnovi.....	23
3.3.2	Istovetnost in verodostojnost ob obnovi po preklicu .....	23
3.4.	Istovetnost in verodostojnost ob zahtevi za preklic .....	23



<b>4.</b>	<b>UPRAVLJANJE S POTRDILI.....</b>	<b>24</b>
<b>4.1.</b>	<b>Zahtevek za pridobitev potrdila .....</b>	<b>24</b>
4.1.1	Kdo lahko predloži zahtevek za pridobitev potrdila .....	24
4.1.2	Postopek za pridobitev potrdila in odgovornosti .....	24
<b>4.2.</b>	<b>Postopek ob sprejemu zahtevka za pridobitev potrdila .....</b>	<b>24</b>
4.2.1	Preverjanje istovetnosti in verodostojnosti bodočega imetnika.....	24
4.2.2	Odobritev/zavrnitev zahtevka.....	25
4.2.3	Čas za izdajo potrdila.....	25
<b>4.3.</b>	<b>Izdaja potrdila.....</b>	<b>25</b>
4.3.1	Postopek izdajatelja ob izdaji potrdila .....	25
4.3.2	Obvestilo imetniku o izdaji potrdila.....	25
<b>4.4.</b>	<b>Prevzem potrdila .....</b>	<b>25</b>
4.4.1	Postopek prevzema potrdila .....	25
4.4.2	Objava potrdila.....	26
4.4.3	Obvestilo o izdaji tretjim osebam .....	26
<b>4.5.</b>	<b>Uporaba potrdil in ključev .....</b>	<b>26</b>
4.5.1	Uporaba potrdila in zasebnega ključa imetnika .....	26
4.5.2	Uporaba potrdila in javnega ključa za tretje osebe .....	26
<b>4.6.</b>	<b>Ponovna izdaja potrdila brez spremembe javnega ključa.....</b>	<b>26</b>
4.6.1	Razlogi za ponovno izdajo potrdila .....	26
4.6.2	Kdo lahko zahteva ponovno izdajo .....	27
4.6.3	Postopek ob ponovni izdaji potrdila .....	27
4.6.4	Obvestilo imetniku o izdaji novega potrdila.....	27
4.6.5	Prevzem ponovno izdanega potrdila.....	27
4.6.6	Objava ponovno izdanega potrdila .....	27
4.6.7	Obvestilo o izdaji drugim subjektom .....	27
<b>4.7.</b>	<b>Obnova potrdila.....</b>	<b>27</b>
4.7.1	Razlogi za obnovo potrdila.....	27
4.7.2	Kdo lahko zahteva obnovo potrdila .....	27
4.7.3	Postopek pri obnovi potrdila.....	27
4.7.4	Obvestilo imetniku o obnovi potrdila .....	27
4.7.5	Prevzem obnovljenega potrdila.....	28
4.7.6	Objava obnovljenega potrdila .....	28
4.7.7	Obvestilo o izdaji drugim subjektom .....	28
<b>4.8.</b>	<b>Sprememba potrdila .....</b>	<b>28</b>
4.8.1	Razlogi za spremembo potrdila .....	28
4.8.2	Kdo lahko zahteva spremembo .....	28
4.8.3	Postopek ob spremembi potrdila .....	28
4.8.4	Obvestilo imetniku o izdaji novega potrdila .....	28
4.8.5	Prevzem spremenjenega potrdila .....	28
4.8.6	Objava spremenjenega potrdila .....	28
4.8.7	Obvestilo o izdaji drugim subjektom .....	29
<b>4.9.</b>	<b>Preklic in začasna razveljavitev potrdila.....</b>	<b>29</b>
4.9.1	Razlogi za preklic.....	29
4.9.2	Kdo lahko zahteva preklic.....	29
4.9.3	Postopek za preklic.....	29
4.9.4	Čas za izdajo zahtevka za preklic.....	30
4.9.5	Čas od prejetega zahtevka za preklic do izvedbe preklica .....	30
4.9.6	Zahteve po preverjanju registra preklicanih potrdil za tretje osebe.....	30
4.9.7	Pogostnost objave registra preklicanih potrdil .....	30



4.9.8	Čas do objave registra preklicanih potrdil .....	30
4.9.9	Sprotno preverjanje statusa potrdil .....	31
4.9.10	Zahteve za sprotno preverjanje statusa potrdil .....	31
4.9.11	Drugi načini za dostop do statusa potrdil .....	31
4.9.12	Druge zahteve pri zlorabi zasebnega ključa .....	31
4.9.13	Razlogi za začasno razveljavitev .....	31
4.9.14	Kdo lahko zahteva začasno razveljavitev .....	31
4.9.15	Postopek za začasno razveljavitev .....	31
4.9.16	Čas začasne razveljavitve.....	31
<b>4.10.</b>	<b>Preverjanje statusa potrdil .....</b>	<b>31</b>
4.10.1	Dostop za preverjanje .....	31
4.10.2	Razpoložljivost .....	32
4.10.3	Druge možnosti .....	32
<b>4.11.</b>	<b>Prekinitev razmerja med imetnikom in izdajateljem .....</b>	<b>32</b>
<b>4.12.</b>	<b>Odkrivanje kopije ključev za dešifriranje.....</b>	<b>32</b>
4.12.1	Postopek za odkrivanje ključev za dešifriranje.....	32
4.12.2	Postopek za odkrivanje ključa seje .....	32
<b>5.</b>	<b>UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE.....</b>	<b>32</b>
<b>5.1.</b>	<b>Fizično varovanje .....</b>	<b>32</b>
5.1.1	Lokacija in zgradba ponudnika storitev zaupanja .....	32
5.1.2	Fizični dostop do infrastrukture ponudnika storitev zaupanja .....	32
5.1.3	Napajanje in prezračevanje .....	32
5.1.4	Zaščita pred poplavo.....	33
5.1.5	Zaščita pred požari .....	33
5.1.6	Hramba nosilcev podatkov.....	33
5.1.7	Odstranjevanje odpadkov .....	33
5.1.8	Hramba na oddaljeni lokaciji.....	33
<b>5.2.</b>	<b>Organizacijska struktura izdajatelja oz. ponudnika storitev zaupanja.....</b>	<b>33</b>
5.2.1	Organizacija ponudnika storitev zaupanja in zaupanja vredne vloge .....	33
5.2.2	Število oseb za posamezne vloge .....	33
5.2.3	Izkazovanje istovetnosti za opravljanje posameznih vlog.....	33
5.2.4	Nezdružljivost vlog .....	33
<b>5.3.</b>	<b>Nadzor nad osebjem .....</b>	<b>33</b>
5.3.1	Potrebne kvalifikacije in izkušnje osebja ter njegova primernost .....	34
5.3.2	Preverjanje primernosti osebja .....	34
5.3.3	Izobraževanje osebja .....	34
5.3.4	Zahteve za redna usposabljanja .....	34
5.3.5	Menjava nalog.....	34
5.3.6	Sankcije .....	34
5.3.7	Zahteve za zunanje izvajalce.....	34
5.3.8	Dostop osebja do dokumentacije.....	34
<b>5.4.</b>	<b>Varnostni pregledi sistema .....</b>	<b>34</b>
5.4.1	Vrste dnevnikov .....	34
5.4.2	Pogostost pregledov dnevnikov beleženih dogodkov .....	35
5.4.3	Čas hrambe dnevnikov beleženih dogodkov .....	35
5.4.4	Zaščita dnevnikov beleženih dogodkov .....	35
5.4.5	Varnostne kopije dnevnikov beleženih dogodkov .....	35
5.4.6	Zbiranje podatkov za dnevnik beleženih dogodkov .....	35
5.4.7	Obveščanje povzročitelja dogodka .....	35
5.4.8	Ocena ranljivosti sistema .....	35



<b>5.5.</b>	<b>Arhiviranje podatkov .....</b>	<b>35</b>
5.5.1	Vrste arhiviranih podatkov .....	35
5.5.2	Čas hrambe.....	35
5.5.3	Zaščita arhiviranih podatkov .....	35
5.5.4	Varnostno kopiranje arhiviranih podatkov.....	36
5.5.5	Zahteva po časovnem žigosanju .....	36
5.5.6	Način zbiranja arhiviranih podatkov .....	36
5.5.7	Postopek za dostop do arhiviranih podatkov in njihova verifikacija .....	36
<b>5.6.</b>	<b>Obnova izdajateljevega potrdila .....</b>	<b>36</b>
<b>5.7.</b>	<b>Okrevalni načrt.....</b>	<b>36</b>
5.7.1	Postopek v primeru vdorov in zlorabe.....	36
5.7.2	Postopek v primeru okvare strojne in programske opreme ali podatkov .....	36
5.7.3	Postopek v primeru ogroženega zasebnega ključa izdajatelja .....	36
5.7.4	Okrevalni načrt.....	36
<b>5.8.</b>	<b>Prenehanje delovanja izdajatelja .....</b>	<b>36</b>
<b>6.</b>	<b>TEHNIČNE VARNOSTNE ZAHTEVE.....</b>	<b>37</b>
<b>6.1.</b>	<b>Generiranje in namestitvev ključev .....</b>	<b>37</b>
6.1.1	Generiranje ključev .....	37
6.1.2	Dostava zasebnega ključa imetnikom.....	37
6.1.3	Dostava javnega ključa izdajatelju potrdil .....	37
6.1.4	Dostava izdajateljevega javnega ključa tretjim osebam.....	37
6.1.5	Dolžina ključev .....	37
6.1.6	Generiranje in kakovost parametrov javnih ključev.....	38
6.1.7	Namen ključev in potrdil.....	38
<b>6.2.</b>	<b>Zaščita zasebnega ključa in varnostni moduli .....</b>	<b>38</b>
6.2.1	Standardi za kriptografski modul.....	38
6.2.2	Nadzor zasebnega ključa s strani pooblaščenih oseb .....	38
6.2.3	Odkrivanje kopije zasebnega ključa.....	38
6.2.4	Varnostna kopija zasebnega ključa .....	38
6.2.5	Arhiviranje zasebnega ključa .....	38
6.2.6	Prenos zasebnega ključa iz/v kriptografski modul .....	38
6.2.7	Zapis zasebnega ključa v kriptografskem modulu .....	39
6.2.8	Postopek za aktiviranje zasebnega ključa .....	39
6.2.9	Postopek za deaktiviranje zasebnega ključa .....	39
6.2.10	Postopek za uničenje zasebnega ključa .....	39
6.2.11	Lastnosti kriptografskega modula .....	39
<b>6.3.</b>	<b>Ostali vidiki upravljanja ključev .....</b>	<b>39</b>
6.3.1	Arhiviranje javnega ključa .....	39
6.3.2	Obdobje veljavnosti potrdila in ključev .....	39
<b>6.4.</b>	<b>Gesla za dostop do zasebnega ključa.....</b>	<b>40</b>
6.4.1	Generiranje gesel.....	40
6.4.2	Zaščita gesel .....	40
6.4.3	Drugi vidiki gesel.....	40
<b>6.5.</b>	<b>Varnostne zahteve za računalniško opremo izdajatelja .....</b>	<b>40</b>
6.5.1	Specifične tehnične varnostne zahteve .....	41
6.5.2	Nivo varnostne zaščite .....	41
<b>6.6.</b>	<b>Tehnični nadzor življenjskega cikla izdajatelja .....</b>	<b>41</b>
6.6.1	Nadzor razvoja sistema .....	41
6.6.2	Upravljanje varnosti .....	41
6.6.3	Nadzor življenjskega cikla.....	41



6.7.	Varnostna kontrola računalniške mreže .....	41
6.8.	Časovno žigosanje.....	41
<b>7.</b>	<b>PROFIL POTRDIL, REGISTRA PREKLICANIH POTRDIL IN SPROTNEGA PREVERJANJA STATUSA POTRDIL.....</b>	<b>41</b>
7.1.	Profil potrdil.....	41
7.1.1	Različica potrdil.....	42
7.1.2	Profil potrdil z razširitvami .....	42
7.1.3	Identifikacijske oznake algoritmov .....	44
7.1.4	Oblika imen .....	44
7.1.5	Omejitve glede imen .....	44
7.1.6	Oznaka politike potrdila.....	44
7.1.7	Uporaba razširitvenega polja za omejitev uporabe politik.....	44
7.1.8	Oblika in obravnava specifičnih podatkov o politiki.....	44
7.1.9	Obravnava kritičnega razširitvenega polja politike.....	44
7.2.	Profil registra preklicanih potrdil.....	44
7.2.1	Različica.....	45
7.2.2	Vsebina registra in razširitve.....	45
7.3.	Profil sprotnega preverjanja statusa potrdil.....	46
7.3.1	Različica.....	46
7.3.2	Razširitve sprotnega preverjanje statusa.....	46
<b>8.</b>	<b>INŠPEKCIJSKI NADZOR.....</b>	<b>46</b>
8.1.	Pogostnost inšpekcijskega nadzora .....	46
8.2.	Inšpekcijska služba.....	46
8.3.	Neodvisnost inšpekcijske službe .....	46
8.4.	Področja inšpekcijskega nadzora .....	46
8.5.	Ukrepi ponudnika storitev zaupanja .....	47
8.6.	Objava rezultatov inšpekcijskega nadzora.....	47
<b>9.</b>	<b>OSTALE POSLOVNE IN PRAVNE ZADEVE.....</b>	<b>47</b>
9.1.	Cenik storitev .....	47
9.1.1	Cena izdaje in obnove potrdil.....	47
9.1.2	Cena dostopa do potrdil.....	47
9.1.3	Cena dostopa do statusa potrdila in registra preklicanih potrdil .....	47
9.1.4	Cene drugih storitev.....	47
9.1.5	Povrnitev stroškov.....	47
9.2.	Finančna odgovornost .....	47
9.2.1	Zavarovalniško kritje .....	47
9.2.2	Drugo kritje.....	48
9.2.3	Zavarovanje imetnikov .....	48
9.3.	Varovanje poslovnih podatkov .....	48
9.3.1	Varovani podatki .....	48
9.3.2	Nevarovani podatki .....	48
9.3.3	Odgovornost glede varovanja poslovnih podatkov .....	48
9.4.	Varovanje osebnih podatkov .....	48
9.4.1	Načrt varovanja osebnih podatkov.....	48
9.4.2	Varovani osebni podatki.....	48
9.4.3	Nevarovani osebni podatki.....	48
9.4.4	Odgovornost glede varovanja osebnih podatkov.....	48





9.4.5	Pooblastilo glede uporabe osebnih podatkov .....	48
9.4.6	Posredovanje osebnih podatkov na uradno zahtevo .....	49
9.4.7	Druga določila glede posredovanja osebnih podatkov .....	49
<b>9.5.</b>	<b>Določbe glede pravic intelektualne lastnine .....</b>	<b>49</b>
<b>9.6.</b>	<b>Obveznosti in odgovornosti.....</b>	<b>49</b>
9.6.1	Obveznosti in odgovornosti izdajatelja.....	49
9.6.2	Obveznost in odgovornost prijavnne službe .....	49
9.6.3	Obveznosti in odgovornost imetnika .....	49
9.6.4	Obveznosti in odgovornost tretjih oseb .....	50
9.6.5	Obveznosti in odgovornosti drugih subjektov .....	50
<b>9.7.</b>	<b>Zanikanje odgovornosti.....</b>	<b>50</b>
<b>9.8.</b>	<b>Omejitev odgovornosti .....</b>	<b>50</b>
<b>9.9.</b>	<b>Poravnava škode.....</b>	<b>50</b>
<b>9.10.</b>	<b>Veljavnost politike.....</b>	<b>50</b>
9.10.1	Čas veljavnosti .....	51
9.10.2	Konec veljavnosti politike .....	51
9.10.3	Učinek poteka veljavnosti politike .....	51
<b>9.11.</b>	<b>Komuniciranje med subjekti .....</b>	<b>51</b>
<b>9.12.</b>	<b>Spreminjanje dokumenta .....</b>	<b>51</b>
9.12.1	Postopek uveljavitve sprememb .....	51
9.12.2	Veljavnost in objava sprememb .....	51
9.12.3	Sprememba identifikacijske oznake politike.....	51
<b>9.13.</b>	<b>Postopek v primeru sporov.....</b>	<b>51</b>
<b>9.14.</b>	<b>Veljavna zakonodaja .....</b>	<b>51</b>
<b>9.15.</b>	<b>Skladnost z veljavno zakonodajo.....</b>	<b>51</b>
<b>9.16.</b>	<b>Splošne določbe .....</b>	<b>52</b>
9.16.1	Celovit dogovor .....	52
9.16.2	Prenos pravic .....	52
9.16.3	Neodvisnost določil .....	52
9.16.4	Terjatve .....	52
9.16.5	Višja sila .....	52
<b>9.17.</b>	<b>Ostale določbe .....</b>	<b>52</b>
9.17.1	Razumevanje določil .....	52
9.17.2	Nasprotujoča določila .....	52
9.17.3	Odstopanje od določil.....	52
9.17.4	Navzkrižno overjanje.....	52



## 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*), <http://www.siggen-ca.si>, ki izdaja potrdila za poslovne subjekte in fizične osebe.

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

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

Pričujoči dokument določa politiko izdajatelja SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe. Na podlagi tega dokumenta SIGEN-CA izdaja spletna kvalificirana digitalna potrdila, ki izpolnjujejo najvišje varnostne zahteve, po politiki CP<sub>OID</sub>: 1.3.6.1.4.1.6105.2.2.3.5.



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

Spremembe, ki jih prinaša nova politika, so sledeče:

- 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.

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

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

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

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

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



## 1. UVOD

### 1.1. Pregled

- (1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.
- (2) Znotraj SI-TRUST deluje izdajatelj SIGEN-CA (angl. *Slovenian General Certification Authority*), <http://www.sigen-ca.si>, ki izdaja digitalna potrdila za poslovne subjekte in fizične osebe. Pričujoči dokument določa politike izdajatelja SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe.
- (3) Izdajatelj SIGEN-CA je registriran v skladu z veljavno zakonodajo in priznan s strani korenškega izdajatelja SI-TRUST Root (angl. *Slovenian Trust Service Root Certification Authority*).
- (4) Po pričujoči politiki SIGEN-CA izdaja spletna kvalificirana digitalna potrdila za fizične osebe po CP<sub>OID</sub>: 1.3.6.1.4.1.6105.2.2.3.4.
- (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 med tretjimi osebami, ki se zanašajo na potrdila izdajatelja SIGEN-CA, in SI-TRUST se izvajajo tudi na podlagi morebitnega pisnega dogovora.
- (9) SI-TRUST se preko korenškega 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

- (1) Pričujoči dokument je Politika SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe (v nadaljevanju *politika SIGEN-CA*).
- (2) Oznaka pričujoče politike je CP<sub>Name</sub>: SIGEN-CA-2, identifikacijska oznaka politike SIGEN-CA-2 pa CP<sub>OID</sub>: 1.3.6.1.4.1.6105.2.2.3.5.
- (3) V vsakem potrdilu je navedba ustrezne politike v obliki oznake CP<sub>OID</sub>, 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:	<a href="http://www.sigen-ca.si">http://www.sigen-ca.si</a>
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 zahteve za svoje storitve,
  - določa in objavlja navodila in priporočila za varno uporabo svojih storitev,
  - skrbi za javni imenik potrdil,
  - objavlja register preklicanih potrdil,
  - skrbi za nemoteno delovanje svojih storitev v skladu s politiko in ostalimi predpisi,
  - obvešča svoje uporabnike,
  - skrbi za delovanje svoje prijavnne službe in,
  - opravlja vse ostale storitve v skladu s to politiko in ostalimi predpisi.
- (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<sup>1</sup>:

Naziv polja	Vrednost potrdila izdajatelja SIGEN-CA
Osnovna polja v potrdilu	
Različica, angl. <i>Version</i>	3
Identifikacijska oznaka, angl. <i>Serial Number</i>	3B3C F9C9
Algoritem podpis, angl. <i>Signature Algorithm</i>	sha1WithRSAEncryption
Izdajatelj, angl. <i>Issuer</i>	c=si, o=state-institutions, ou=sigen-ca
Imetnik, angl. <i>Subject</i>	c=si, o=state-institutions, ou=sigen-ca

<sup>1</sup> Pomen je podan v podpogl. 3.1 in 7.1.



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

(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:

Naziv polja	Vrednost potrdila izdajatelja SIGEN-CA
Različica, angl. <i>Version</i>	3
Identifikacijska oznaka, angl. <i>Serial Number</i>	CD81 8601 0000 0000 571E 043E
Algoritem za podpis, angl. <i>Signature Algorithm</i>	sha256WithRSAEncryption
Izdajatelj, angl. <i>Issuer</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Imetnik, angl. <i>Subject</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Pričetek veljavnosti, angl. <i>Validity: Not Before</i>	Apr 25 11:19:25 2016 GMT
Konec veljavnosti, angl. <i>Validity: Not After</i>	Apr 25 11:49:25 2036 GMT
Algoritem za javni ključ, angl. <i>Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)



Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. <i>RSA Public Key</i>	<i>ključ dolžine 3072 bitov</i>
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	4C25 278C A82D 729E
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	4C25 278C A82D 729E
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. <i>Certificate Fingerprint – SHA-1</i>	335F 27AE EE7A EA9B D4E3 FE59 EB65 B4AC 8926 E0E7
Odtis potrdila SHA-256, angl. <i>Certificate Fingerprint – SHA-256</i>	C4B9 BB09 EA4E F4A1 37EC 573A EFC1 23C4 B509 62CF B99A E13A 9331 14DB 4A34 274D

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

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



Objava registra preklicanih potrdil, OID 2.5.29.31, angl. <i>CRL Distribution Points</i>	Url: <a href="http://www.ca.gov.si/crl/si-trust-root.crl">http://www.ca.gov.si/crl/si-trust-root.crl</a>  Url: <a href="ldap://x500.gov.si/cn=SI-TRUST%20Root,oi=VATSI-17659957,o=Republika%20Slovenija,c=SI?certificateRevocationList">ldap://x500.gov.si/cn=SI-TRUST Root,oi=VATSI-17659957,o=Republika Slovenija,c=SI?certificateRevocationList</a>  c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root, cn=CRL1
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. <i>Authority Information Access</i>	Access Method=OCSP <a href="http://ocsp.ca.gov.si">http://ocsp.ca.gov.si</a>  Access Method=CA Issuers <a href="http://www.ca.gov.si/crt/si-trust-root.crt">http://www.ca.gov.si/crt/si-trust-root.crt</a>
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. <i>certificatePolicies</i>	Certificate Policy: PolicyIdentifier=2.5.29.32.0 (»anyPolicy«) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.ca.gov.si/cps/">http://www.ca.gov.si/cps/</a>
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
<b>Odtis potrdila (ni del potrdila)</b>	
Odtis potrdila SHA-1, angl. <i>Certificate Fingerprint – SHA-1</i>	EF9B C82D C8B0 F209 4529 447F 3BB6 6AC9 9C25 7C66
Odtis potrdila SHA-256, angl. <i>Certificate Fingerprint – SHA-256</i>	E016 01D8 F0D6 9434 E699 735C 4F34 8FC1 5FB4 8F2C 2B20 03FE E0F5 4A90 E819 48FD

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. <i>Version</i>	3
Identifikacijska oznaka, angl. <i>Serial Number</i>	28C3 981D 0000 0000 571D D0E7
Algoritem za podpis, angl. <i>Signature Algorithm</i>	sha256WithRSAEncryption
Izdajatelj, angl. <i>Issuer</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Imetnik, angl. <i>Subject</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Pričetek veljavnosti, angl. <i>Validity: Not Before</i>	May 24 11:49:41 2016 GMT





Konec veljavnosti, angl. <i>Validity: Not After</i>	Apr 23 22:00:00 2036 GMT
Algoritem za javni ključ, angl. <i>Subject Public Key Algorithm</i>	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. <i>RSA Public Key</i>	ključ dolžine 3072 bitov
<b>Razširitve X.509v3</b>	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. <i>CRL Distribution Points</i>	Url: <a href="http://www.ca.gov.si/crl/si-trust-root.crl">http://www.ca.gov.si/crl/si-trust-root.crl</a>  Url: <a href="ldap://x500.gov.si/cn=SI-TRUST Root, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList">ldap://x500.gov.si/cn=SI-TRUST Root, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList</a>  c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root, cn=CRL1
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. <i>Authority Information Access</i>	Access Method=OCSP <a href="http://ocsp.ca.gov.si">http://ocsp.ca.gov.si</a>  Access Method=CA Issuers <a href="http://www.ca.gov.si/crt/si-trust-root.crt">http://www.ca.gov.si/crt/si-trust-root.crt</a>
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. <i>certificatePolicies</i>	Certificate Policy: PolicyIdentifier=2.5.29.32.0 (»anyPolicy«) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.ca.gov.si/cps/">http://www.ca.gov.si/cps/</a>
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	4C25 278C A82D 729E
<b>Odtis potrdila (ni del potrdila)</b>	
Odtis potrdila SHA-1, angl. <i>Certificate Fingerprint – SHA-1</i>	D3C6 C554 C171 F9BA 952C E04C AC2C 1C9B D68B 08D4
Odtis potrdila SHA-256, angl. <i>Certificate Fingerprint – SHA-256</i>	7950 15CA ACA7 4715 D341 120D 3F0E FD19 2A03 2F1C 0039 1797 F54E F998 0804 A175

### 1.3.2 Prijavna služba

(1) Organizacije, ki opravljajo naloge prijavne službe, pooblasti SI-TRUST. Izpolnjevati morajo pogoje za



opravljanje nalog prijavnih služb SI-TRUST ter delovati v skladu z veljavnimi predpisi in poslovniki za delo prijavnih služb SI-TRUST.

(2) Naloge prijavne službe so:

- preverjanje istovetnosti imetnikov oz. bodočih imetnikov, njihovih podatkov in drugih potrebnih podatkov,
- sprejemanje zahtevkov za pridobitev potrdil,
- sprejemanje zahtevkov za preklic potrdil,
- preverjanje podatkov v zahtevkih,
- izdajanje potrebne dokumentacije imetnikom oz. bodočim imetnikom,
- posredovanje zahtevkov in ostalih podatkov na varen način na SIGEN-CA.

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

### 1.3.3 Imetniki potrdil

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

### 1.3.4 Tretje osebe

Določbe so opredeljene v Krovni politiki SI-TRUST.

### 1.3.5 Ostali udeleženci

Določbe so opredeljene v Krovni politiki SI-TRUST.

## 1.4. Namen uporabe potrdil

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

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

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

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

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

### 1.4.1 Pravilna uporaba potrdil in ključev

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

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

#### **1.4.2 Nedovoljena uporaba potrdil in ključev**

Določbe so opredeljene v Krovni politiki SI-TRUST.

### **1.5. Upravljanje s politiko**

#### **1.5.1 Upravljaivec politike**

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**

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*, se objavljajo:
  - evidenčni podatki o potrdilu (imetnikov naziv, naslov e-pošte, serijska številka ...),
  - veljavna digitalna potrdila (podrobneje podana v podpogl. 7.1) in
  - register preklicanih digitalnih potrdil (podrobneje podan v podpogl. 7.2).
  
- (3) Ostali dokumenti oz. ključni podatki o delovanju izdajatelja SIGEN-CA ter splošna obvestila imetnikom in tretjim osebam se objavijo na spletnih straneh <http://www.sigen-ca.si>.
  
- (4) Zaupni del notranjih pravil 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.sigen-ca.si/cda-cgi/clientcgi?action=directorySearch>.
  
- (4) SI-TRUST oz. izdajatelj SIGEN-CA v skladu z Interno politiko SI-TRUST skrbi za pooblaščen in varno dodajanje, spreminjanje ali brisanje podatkov v javnem imeniku potrdil.

## **3. ISTOVETNOST IN VERODOSTOJNOST**

### **3.1. Določanje imen**

#### **3.1.1 Oblika imen**

- (1) Vsako potrdilo vsebuje v skladu s priporočilom RFC 5280 podatke o imetniku ter izdajatelju v obliki razločevalnega imena, ki je oblikovano kot UTF8String oz. PrintableString v skladu s priporočilom RFC 5280



»Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile« in s standardom X.501.

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

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

(4) Vsako razločevalno ime vključuje tudi serijsko številko, ki jo določi izdajatelj SIGEN-CA<sup>2</sup> (glej podogl. 3.1.5).

(5) Razločevalno ime se tvori po naslednjih pravilih<sup>3</sup>.

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

### 3.1.2 Zahteva po smiselnosti imen

(1) Imetnik potrdila je nedvoumno določen z razločevalnim imenom v skladu s prejšnjim razdelkom.

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

### 3.1.3 Uporaba anonimnih imen ali psevdonimov

Ni predvidena.

### 3.1.4 Pravila za interpretacijo imen

Pravila so navedena v podogl. 3.1.1 in 3.1.2.

### 3.1.5 Enoličnost imen

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

<sup>2</sup> Potrdilo izdajatelja SIGEN-CA ne vsebuje serijske številke.

<sup>3</sup> Pravila za tvorbo razločevalnih imen za druge vrste potrdil določi in objavi SIGEN-CA.

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



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

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

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

*Ni predpisano.*

### 3.2.3 Preverjanje istovetnosti fizičnih oseb

(1) Preverjanje istovetnosti imetnikov opravi prijavna služba SI-TRUST.

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

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



### **3.2.4 Nепреverjeni podatki pri začetnem preverjanju**

Nepreverenih podatkov v potrdilu ni.

### **3.2.5 Preverjanje pooblastil**

*Ni predpisano.*

### **3.2.6 Merila za medsebojno povezovanje**

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

### **3.3.2 Istovetnost in verodostojnost ob obnovi po preklicu**

Preverjanje imetnikov poteka skladno z določili iz podpogl. 3.2.3.

## **3.4. Istovetnost in verodostojnost ob zahtevi za preklic**

- (1) Zahtevek za preklic potrdila imetnik odda:
  - osebno na prijavnih službah, kjer pooblaščenec osebe preverijo istovetnost prosilca,
  - elektronsko, vendar mora biti zahtevek digitalno podpisan z zasebnim ključem, ki pripada digitalnemu potrdilu, ki ga je izdal 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, glej definicijo v podpogl. 1.3.3.

#### 4.1.2 Postopek za pridobitev potrdila in odgovornosti

(1) Za pridobitev potrdila mora bodoči imetnik pravilno izpolniti in podpisati zahtevek za pridobitev potrdila. Zahtevek lahko odda procesno sposobna oseba, starejša od 15 let.

(2) V primeru, da je bodoči imetnik invalidna oseba, lahko zahtevek za pridobitev potrdila odda v njegovem imenu druga oseba, ki mora priložiti notarsko ali upravno overjeno pooblastilo ter svoj veljavni osebni dokument s sliko.

(3) Bodoči imetnik lahko izdajatelju SIGEN-CA po elektronski poti posreduje zahtevek, digitalno podpisan z njegovim veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, ki mu ga je izdal izdajatelj SIGEN-CA.

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

(5) Bodoči imetnik je za pridobitev potrdila dolžan:

- izpolniti zahtevek za pridobitev potrdila z resničnimi in pravilnimi podatki,
- zahtevek oddati na prijavno službo osebno ali izdajatelju SIGEN-CA po elektronski poti posredovati zahtevek, digitalno podpisan z njegovim veljavnim digitalnim potrdilom za fizične osebe, ki mu ga je izdal izdajatelj SIGEN-CA,
- opraviti prevzem potrdila na varen način po navodilih izdajatelja SIGEN-CA.

### 4.2. *Postopek ob sprejemu zahtevka za pridobitev potrdila*

#### 4.2.1 Preverjanje istovetnosti in verodostojnosti bodočega imetnika

(1) V primeru osebne oddaje zahtevka na prijavnih službah pooblaščen oseba na prijavnih službah preveri istovetnost bodočega imetnika v skladu z veljavno zakonodajo. Bodoči imetnik mora izkazati svojo istovetnost z veljavnim osebnim dokumentom.

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

(3) Preveriti je potrebno istovetnost bodočega imetnika oz. vse tiste podatke, ki so navedeni v zahtevku in so dostopni v uradnih evidencah oz. drugih uradnih veljavnih dokumentih.



#### **4.2.2 Odobritev/zavrnitev zahtevka**

- (1) Pred oddajo zahtevka izdajatelj SIGEN-CA seznaní 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 zavrnejo pooblašćene osebe izdajatelja SIGEN-CA.
- (3) O odobritvi oz. zavrnitvi je bodoči imetnik obvešćen po e-pošti.

#### **4.2.3 Čas za izdajo potrdila**

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

### **4.3. Izdaja potrdila**

#### **4.3.1 Postopek izdajatelja ob izdaji potrdila**

- (1) V primeru odobrenega zahtevka SIGEN-CA posreduje bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo po dveh ločenih poteh: referenčno številko po elektronski pošti, avtorizacijsko kodo pa s pošto pošiljko, izjemoma pa ju lahko pooblašćena 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).

#### **4.3.2 Obvestilo imetniku o izdaji potrdila**

- (1) Bodoči imetnik je obvešćen o odobritvi oz. zavrnitvi zahtevka za pridobitev digitalnega potrdila.
- (2) Dva (2) meseca pred potekom potrdila oz. ključev izdajatelj SIGEN-CA imetnika o tem obvesti po e-pošti.

### **4.4. Prevzem potrdila**

#### **4.4.1 Postopek prevzema potrdila**

- (1) Za prevzem potrdila bodoči imetnik potrebuje referenčno številko in avtorizacijsko kodo, ki mu ju izda SIGEN-CA, glej podpogl. 4.3.
- (2) Način in podrobna navodila za prevzem potrdil po tej politiki so opisana na spletni strani <http://www.sigenc.si>. Prav tako so na spletni strani objavljene tudi vse novosti v zvezi z načinom prevzema potrdil.
- (3) Imetnik mora takoj po prevzemu potrdila preveriti podatke v tem potrdilu. Če izdajatelja SIGEN-CA ne obvesti o morebitnih napakah, se smatra, da se z vsebino strinja in da soglašá 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 prekliche.

(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 zasebnega ključa dolžan:

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

(2) Imetnik mora varovati zasebni ključ pred nepooblaščenno uporabo.

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

#### **4.5.2 Uporaba potrdila in javnega ključa za tretje osebe**

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**

#### **4.7.1 Razlogi za obnovo potrdila**

*Ni podprto.*

#### **4.7.2 Kdo lahko zahteva obnovo potrdila**

*Ni podprto.*

#### **4.7.3 Postopek pri obnovi potrdila**

*Ni podprto.*

#### **4.7.4 Obvestilo imetniku o obnovi potrdila**

*Ni podprto.*

#### **4.7.5 Prezem obnovljenega potrdila**

*Ni podprto.*

#### **4.7.6 Objava obnovljenega potrdila**

*Ni podprto.*

#### **4.7.7 Obvestilo o izdaji drugim subjektom**

*Ni podprto.*

### **4.8. Sprememba potrdila**

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

(2) Za pridobitev novega potrdila je potrebno ponoviti postopek za pridobitev novega potrdila, kot je naveden v podpogl. 4.1. Storitve 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 Prezem spremenjenega potrdila**

Določbe so opredeljene v Krovni politiki SI-TRUST.

#### **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<sup>5</sup>

#### 4.9.1 Razlogi za preklic

(1) Preklic potrdila mora imetnik zahtevati v primeru:

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

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

- da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,
- da je prišlo do napake pri preverjanju istovetnosti podatkov na prijavni službi,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- za neizpolnjevanje obveznosti imetnika,
- da niso poravnani morebitni stroški za upravljanje digitalnih potrdil,
- da je bila infrastruktura SI-TRUST ogrožena na način, ki vpliva na zanesljivost potrdila,
- da je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- da bo SIGEN-CA prenehal z izdajanjem potrdil ali da je bilo 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

#### 4.9.3 Postopek za preklic

(1) Preklic lahko imetnik zahteva:

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

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

(3) Če se preklic zahteva:

---

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



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

(4) O datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic je imetnik obveščen po elektronski pošti.

(5) 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 preklic 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<sup>6</sup>.

#### **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.

<sup>6</sup> V javnem imeniku ostanejo samo evidenčni podatki o potrdilu.

#### **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**

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](http://x500.gov.si) ter na spletnih straneh <http://www.sigen-ca.si>, sprotno preverjanje statusa potrdila je dostopno na naslovu <http://ocsp.sigen-ca.si>, podrobnosti o dostopu pa so v podpogl. 7.2 in 7.3.

#### **4.10.2 Razpoložljivost**

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**

*Ni podprto.*

#### **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.

#### **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 zaupanja in 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.

### **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 dnevnikov**

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.

#### **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.

#### **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 namestitvev ključev

#### 6.1.1 Generiranje ključev

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

(2) Zapisnik postopka se varno shrani.

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

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

(5) Ključi imetnikov se generirajo pri imetniku.

#### 6.1.2 Dostava zasebnega ključa imetnikom

Zasebni ključ se generira pri imetniku in se ne prenaša.

#### 6.1.3 Dostava javnega ključa izdajatelju potrdil<sup>7</sup>

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

#### 6.1.4 Dostava izdajateljevega javnega ključa tretjim osebam

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

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

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

#### 6.1.5 Dolžina ključev

---

<sup>7</sup> RFC 3647 ne predvideva opisa načina dostave potrdil imetnikom.



Potrdilo	Dolžina ključa po RSA [bit]
potrdilo izdajatelja SIGEN-CA	3072
potrdilo za imetnike	2048 <sup>8</sup>
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

*Ni podprto.*

### 6.2.4 Varnostna kopija zasebnega ključa

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

### 6.2.5 Arhiviranje zasebnega ključa

*Ni podprto.*

### 6.2.6 Prenos zasebnega ključa iz/v kriptografski modul

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

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

<sup>8</sup> Vrednost pomeni minimalno predpisano dolžino.

### 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.

### 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	Ključ	Veljavnost
spletno	par za digitalno	zasebni ključ	5 let



potrdilo	podpisovanje/overjanje in dešifriranje/šifriranje	javni ključ	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) Pooblaščenec 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.

(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 s pošto pošiljko,
- izjemoma pa ju preda tudi osebno.

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

(5) SIGEN-CA priporoča, da se geslo za dostop do zasebnega ključa ne shranjuje oz. se shrani na varno mesto in da ima do njega dostop le imetnik.

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

### 6.4.3 Drugi vidiki gesel

*Niso predpisani.*

## 6.5. Varnostne zahteve za računalniško opremo izdajatelja



### **6.5.1 Specifične tehnične varnostne zahteve**

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**

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 spletna potrdila za fizične osebe.
- (2) Vsa potrdila vključujejo podatke, ki so skladno z veljavno zakonodajo določeni za kvalificirana potrdila.
- (3) Potrdila izdajatelja SIGEN-CA sledijo standardu X.509.

### 7.1.1 Različica potrdil

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

### 7.1.2 Profil potrdil z razširitvami

#### 7.1.2.1 Profil potrdila SIGEN-CA

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

#### 7.1.2.2 Profil potrdil za imetnike

(1) Podatki v potrdilu so navedeni spodaj.

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



Objava registra preklicanih potrdil, OID 2.5.29.31, angl. <i>CRL Distribution Points</i>	Url: <a href="http://www.sigen-ca.si/crl/sigen-ca-g2.crl">http://www.sigen-ca.si/crl/sigen-ca-g2.crl</a>  Url: <code>ldap://x500.gov.si/cn=SIGEN-CA G2, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList</code>  <code>c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2, cn=CRL&lt;zaporedna številka registra, glej podpogl. 7.2.2&gt;</code>
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. <i>Authority Information Access</i>	Access Method: OCSP (OID 1.3.6.1.5.5.7.48.1) Access Location: URL= <a href="http://ocsp.sigen-ca.si">http://ocsp.sigen-ca.si</a>  Access Method: Calssuer (OID 1.3.6.1.5.5.7.48.2) Access Location: URL= <a href="http://www.sigen-ca.si/crt/sigen-ca-g2-certs.p7c">http://www.sigen-ca.si/crt/sigen-ca-g2-certs.p7c</a>
Uporaba ključa, OID 2.5.29.15, angl. <i>Key Usage</i>	Digital Signature, Key Encipherment, ContentCommitment
Razširjena uporaba ključa, OID 2.5.29.37, angl. <i>Extended Key Usage</i>	<i>se ne uporablja</i>
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. <i>Authority Key Identifier</i>	4C25 278C A82D 729E
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. <i>Subject Key Identifier</i>	<i>identifikator imetnikovega ključa</i>
Politike, pod katerimi je bilo izdano potrdilo, OID 2.5.29.32, angl. <i>certificatePolicies</i>	Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6105.2.2.3.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.ca.gov.si/cps/">http://www.ca.gov.si/cps/</a> PolicyIdentifier=0.4.0.194112.1.0
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. <i>qcStatement</i>	QcCompliance statement QcType: esign PdsLocation: <a href="https://www.ca.gov.si/cps/sigenca2_pds_en.pdf">https://www.ca.gov.si/cps/sigenca2_pds_en.pdf</a> , <a href="https://www.ca.gov.si/cps/sigenca2_pds_sl.pdf">https://www.ca.gov.si/cps/sigenca2_pds_sl.pdf</a>
Osnovne omejitve, OID 2.5.29.19, angl. <i>Basic Constraints</i>	CA: FALSE Brez omejitev dolžine (Path Length Constraint: none)
<b>Odtis potrdila (ni del potrdila)</b>	
Odtis potrdila-SHA-1 angl. <i>Certificate Fingerprint – SHA-1</i>	<i>razpoznavni odtis potrdila po SHA-1</i>
Odtis potrdila-SHA-256 angl. <i>Certificate Fingerprint – SHA-256</i>	<i>razpoznavni odtis potrdila po SHA-256</i>

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

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

### 7.1.2.3 *Zahteve za elektronski naslov*

(1) Elektronski naslov mora izpolnjevati naslednje zahteve:

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

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

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

### **7.1.3 Identifikacijske oznake algoritmov**

Določbe so opredeljene v Krovni politiki SI-TRUST.

### **7.1.4 Oblika imen**

Določbe so opredeljene v Krovni politiki SI-TRUST.

### **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 omejitve 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. <i>Version</i>	2
Izdajateljev podpis, angl. <i>Signature</i>	podpis SIGEN-CA
Razločevalno ime izdajatelja, angl. <i>Issuer</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Čas izdaje CRL, angl. <i>thisUpdate</i>	Last Update: <čas izdaje po GMT>
Čas izdaje naslednjega CRL, angl. <i>nextUpdate</i>	Next Update: <čas naslednje izdaje po GMT>
Identifikacijske oznake preklicanih potrdil in čas preklica, angl. <i>revokedCertificate</i>	Serial Number: <identifikacijska oznaka preklicanega dig. potrdila> Revocation Date: <čas preklica po GMT>
Algoritem za podpis, angl. <i>Signature Algorithm</i>	sha256WithRSAEncryption
Razširitve X.509v2 CRL	
Identifikator izdajateljevega ključa, angl. <i>Authority Key Identifier</i> (OID 2.5.29.35)	identifikator izdajateljevega ključa
Številka za posamične registre (CRL1, CRL2,...), angl. <i>CRLnumber</i> (OID 2.5.29.20)	zaporedna številka posamičnega registra
Alternativno ime izdajatelja angl. <i>issuerAltName</i> (OID 2.5.28.18)	se ne uporablja
Oznaka seznama sprememb angl. <i>deltaCRLindicator</i> (OID 2.5.29.27)	se ne uporablja
Objava seznama sprememb angl. <i>issuingDistributionPoint</i> (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
<i>posamični registri</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2, cn=CRL<zaporedna številka registra>	- ldap://x500.gov.si/cn=CRL<zaporedna številka registra>, cn=SIGEN-CA G2,oi=VATSI-17659957,o=Republika Slovenija,c=SI
<i>celotni register</i>	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2 (v polju "CertificateRevocationList")	- 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.

#### **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 po objavljenem ceniku na spletni strani <http://www.sigen-ca.si/cenik.php>.

#### **9.1.2 Cena dostopa do potrdil**

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

#### **9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil**

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

#### **9.1.4 Cene drugih storitev**

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.

## **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 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 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**

#### **9.6.1 Obveznosti in odgovornosti izdajatelja**

Določbe so opredeljene v Krovni politiki SI-TRUST.

#### **9.6.2 Obveznost in odgovornost prijavnne službe**

(1) Prijavna služba je dolžna:

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

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

#### **9.6.3 Obveznosti in odgovornost imetnika**

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:

- seznaniti se s to politiko pred izdajo potrdila,
- ravnati v skladu s politiko in ostalimi veljavnimi predpisi,
- če po oddaji zahtevka za pridobitev potrdila oz. drugo storitev od izdajatelja SIGEN-CA ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, se mora obrniti na pooblaščen osebe izdajatelja SIGEN-CA,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti

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

(2) Imetnik odgovarja za:

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

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

#### **9.6.4 Obveznosti in odgovornost tretjih oseb**

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**

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.

### **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.