



**Zavod za zdravstveno  
zavarovanje Slovenije**  
Miklošičeva cesta 24  
1507 Ljubljana  
[www.zzzs.si](http://www.zzzs.si)



# **Infrastruktura javnih ključev ZZZS za potrebe sistema kartice zdravstvenega zavarovanja**

**Politika overitelja digitalnih potrdil ZZZS-CA**

---

### Stanje dokumenta

<b>Verzija</b>	<b>Veljavnost</b>	<b>Opis</b>
Verzija 1	04. 09. 2008 do 26. 09. 2013	Politika ZZZS-CA izdana za potrebe sistema kartice zdravstvenega zavarovanja
Verzija 1.1	27. 09. 2013 do 16. 01. 2018	Politika ZZZS-CA izdana za potrebe sistema kartice zdravstvenega zavarovanja
Verzija 2.0	17. 01. 2018 do 24. 03. 2021	Politika ZZZS-CA izdana za potrebe sistema kartice zdravstvenega zavarovanja (G2)
Verzija 2.1	25. 03. 2021 dalje	Politika ZZZS-CA izdana za potrebe sistema kartice zdravstvenega zavarovanja (ECC)

---

## Vsebina

1.	UVOD.....	7
1.1.	Pregled .....	7
1.2.	Naziv dokumenta in identifikacijska oznaka.....	7
1.3.	Udeleženci infrastrukture javnih ključev .....	8
1.3.1.	Overitelj.....	8
1.3.2.	Prijavna služba .....	11
1.3.3.	Imetniki digitalnih potrdil .....	11
1.3.4.	Tretje osebe.....	11
1.4.	Namen uporabe digitalnih potrdil .....	12
1.4.1.	Dovoljena uporaba digitalnih potrdil .....	12
1.5.	Upravljanje s pravili delovanja.....	12
1.5.1.	Organ, ki upravlja s pričujočim dokumentom .....	12
1.5.2.	Kontaktne podatki .....	12
1.5.3.	Odgovorni organ za odobritev skladnosti pravil delovanja upravitelja infrastrukture overitelja s Politiko ZZZS-CA.....	12
1.5.4.	Postopek odobritve pravil delovanja overitelja .....	12
2.	ODGOVORNOST ZA OBJAVE IN REPOZITORIJ.....	13
2.1.	Repozitorij .....	13
2.2.	Objave informacij o digitalnih potrdilih.....	13
2.3.	Čas in pogostost objav .....	13
2.4.	Dostop do podatkov v repozitoriju.....	13
3.	PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI .....	14
3.1.	Določanje imen.....	14
3.1.1.	Vrste imen.....	14
3.1.2.	Potreba po smiselnosti imen .....	14
3.1.3.	Anonimnost imetnikov in uporaba psevdonimov .....	14
3.1.4.	Pravila za interpretacijo različnih oblik imen.....	14
3.2.	Prva registracija.....	14
3.2.1.	Metode dokazovanja lastništva zasebnega ključa .....	14
3.2.2.	Preverjanje istovetnosti za fizične osebe .....	15
3.2.3.	Podatki o imetnikih digitalnih potrdil, ki se ne preverjajo .....	15
3.2.4.	Merila za medsebojno povezovanje .....	15
3.3.	Preverjanje istovetnosti pri obnovi digitalnega potrdila .....	15
3.3.1.	Preverjanje istovetnosti pri rutinski obnovi digitalnih potrdil .....	15
3.3.2.	Preverjanje istovetnosti pri obnovi digitalnega potrdila po preklicu.....	15
3.4.	Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila .....	15
4.	UPRAVLJANJE Z DIGITALNIMI POTRDILI .....	15
4.1.	Prošnja za izdajo digitalnega potrdila.....	15
4.2.	Izdaja digitalnega potrdila .....	16
4.2.1.	Postopki overitelja ob izdaji digitalnega potrdila .....	16
4.2.2.	Obvestilo imetniku o izdaji digitalnega potrdila.....	16
4.3.	Prevzem digitalnega potrdila .....	16
4.3.1.	Postopek potrditve prevzema digitalnega potrdila .....	16
4.3.2.	Objava digitalnega potrdila .....	16
4.3.3.	Obveščanje drugih udeležencev o izdaji digitalnega potrdila.....	16
4.4.	Uporaba ključev in digitalnih potrdil.....	16
4.4.1.	Uporaba ključev in digitalnih potrdil s strani imetnikov .....	16
4.4.2.	Uporaba digitalnih potrdil s strani tretjih oseb .....	17
4.5.	Obnova digitalnih potrdil brez spremembe ključev .....	17
4.6.	Obnova digitalnih potrdil.....	17
4.7.	Sprememba digitalnega potrdila .....	17
4.8.	Začasna ukinitve veljavnosti in preklic digitalnega potrdila.....	17
4.8.1.	Okoliščine preklica.....	17
4.8.2.	Kdo lahko zahteva preklic.....	17

4.8.3.	Postopki za preklic.....	18
4.8.4.	Čas za posredovanje vloge za preklic.....	18
4.8.5.	Čas od vloge za preklic do preklica.....	18
4.8.6.	Obveza preverjanja registra preklicanih potrdil.....	18
4.8.7.	Pogostost objav registrov preklicanih potrdil.....	18
4.8.8.	Storitev sprotnega preverjanje statusa digitalnih potrdil.....	18
4.8.9.	Ostale oblike objavljanja preklicanih digitalnih potrdil.....	18
4.8.10.	Posebne zahteve glede zlorabe ključa.....	18
4.9.	Storitve objavljanja statusa digitalnih potrdil.....	18
4.9.1.	Tehnične lastnosti storitve.....	18
4.9.2.	Razpoložljivost storitve.....	19
4.10.	Predčasna ukinitve veljavnosti digitalnih potrdil.....	19
4.11.	Varnostno kopiranje in odkrivanje zasebnega ključa.....	19
4.11.1.	Postopki povrnitve zgodovine ključev in odkrivanje kopije zasebnega ključa za dešifriranje.....	19
5.	FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE.....	19
5.1.	Fizično varovanje.....	19
5.2.	Organizacijski varnostni ukrep.....	19
5.3.	Zahteve za osebe overitelja.....	20
5.4.	Postopki zbiranja in upravljanja revizijskih sledi.....	20
5.5.	Arhiviranje podatkov.....	21
5.6.	Obnova digitalnih potrdil overiteljev.....	21
5.7.	Postopki v primeru ogrožanja zasebnega ključa in okrevalni načrt.....	21
5.7.1.	Postopki v primeru okvar in zlorab.....	21
5.7.2.	Uničenje programske, strojne opreme ali podatkov.....	21
5.7.3.	Ogrožanje zasebnega ključa overitelja.....	22
5.7.4.	Neprekinjenost poslovanja ob naravnih in drugih nesrečah.....	22
5.8.	Prenehanje delovanja overitelja.....	22
6.	TEHNIČNE VARNOSTNE ZAHTEVE.....	22
6.1.	Generiranje in namestitvev para ključev.....	22
6.1.1.	Generiranje para ključev.....	22
6.1.2.	Dostava zasebnega ključa imetniku.....	22
6.1.3.	Dostava imetnikovega javnega ključa overitelju.....	23
6.1.4.	Dostava overiteljevega javnega ključa tretjim osebam.....	23
6.1.5.	Dolžina ključev.....	23
6.1.6.	Parametri za generiranje javnih ključev in preverjanje parametrov.....	23
6.1.7.	Namen uporabe ključev.....	23
6.2.	Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov.....	24
6.2.1.	Standardi za kriptografski modul.....	24
6.2.2.	Nadzor zasebnega ključa overitelja s strani pooblaščenih oseb.....	24
6.2.3.	Odkrivanje zasebnega ključa.....	24
6.2.4.	Varnostno kopiranje zasebnih ključev.....	24
6.2.5.	Arhiviranje zasebnega ključa.....	25
6.2.6.	Prenos zasebnega ključa v kriptografski modul in iz njega.....	25
6.2.7.	Hranjenje overiteljevega zasebnega ključa v kriptografskem modulu.....	25
6.2.8.	Postopek za aktiviranje zasebnega ključa.....	25
6.2.9.	Postopek za deaktiviranje zasebnega ključa.....	25
6.2.10.	Postopek za uničenje zasebnega ključa.....	25
6.2.11.	Stopnja varnosti kriptografskih modulov.....	25
6.3.	Ostali vidiki upravljanja s pari ključev.....	25
6.3.1.	Arhiviranje javnega ključa.....	25
6.3.2.	Obdobje veljavnosti ključev in digitalnih potrdil.....	25
6.4.	Aktivacijski podatki.....	26
6.4.1.	Generiranje in instalacija aktivacijskih podatkov.....	26
6.4.2.	Zaščita aktivacijskih podatkov.....	26
6.4.3.	Drugi vidiki aktivacijskih podatkov.....	26

6.5.	Varnostne zahteve za računalnike .....	26
6.5.1.	Specifične tehnične varnostne zahteve za računalnike .....	26
6.5.2.	Nivo varnostne zaščite računalnikov .....	26
6.6.	Tehnični nadzor življenjskega cikla overitelja .....	27
6.6.1.	Nadzor razvoja sistema .....	27
6.6.2.	Upravljanje varnosti .....	27
6.7.	Varnostne kontrole na ravni računalniškega omrežja .....	27
7.	PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL .....	27
7.1.	Profil digitalnih potrdil .....	27
7.1.1.	Verzija digitalnih potrdil.....	27
7.1.2.	Razširitvena polja .....	28
7.1.2.1	Standardna X.509 v3 razširitvena polja .....	28
7.1.2.2	Razširitvena polja za potrebe Zavoda.....	28
7.1.3.	Identifikacijske oznake algoritmov .....	29
7.1.4.	Oblike imen.....	29
7.1.5.	Omejitve imen.....	29
7.1.6.	Identifikacijska oznaka politik .....	29
7.1.7.	Način uporabe razširitvenega polja <i>policyConstraints</i> za omejitev uporabe politik 29	
7.1.8.	Specifični podatki o politiki (angl. Policy Qualifiers extension) .....	29
7.1.9.	Procesiranje oznake kritičnosti razširitvenih polj .....	30
7.2.	Profil registrov preklicanih potrdil .....	30
7.2.1.	Verzija registrov preklicanih potrdil.....	30
7.2.2.	Razširitvena polja registrov preklicanih potrdil .....	30
7.3.	Profil OSCP .....	30
8.	PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA.....	30
8.1.	Pogostost ali okoliščine izvajanja nadzornih pregledov .....	30
8.2.	Pogoji za izvajalca nadzora.....	30
8.3.	Relacija med izvajalcem nadzora in overiteljem .....	31
8.4.	Področja nadzora .....	31
8.5.	Postopki po opravljenem nadzornem pregledu.....	31
8.6.	Prejemniki in objava ugotovitev.....	31
9.	OSTALE POSLOVNE IN PRAVNE ZADEVE .....	31
9.1.	Finančna odgovornost.....	31
9.2.	Zaupnost poslovnih informacij.....	31
9.3.	Zaupnost osebnih podatkov .....	31
9.4.	Zaščita intelektualne lastnine .....	31
9.5.	Odgovornosti in jamstva.....	32
9.5.1.	Odgovornosti in jamstva overitelja .....	32
9.5.2.	Odgovornost in jamstva imetnikov digitalnih potrdil .....	32
9.5.3.	Odgovornost in jamstva tretjih oseb .....	32
9.6.	Zanikanje odgovornosti overitelja.....	32
9.7.	Omejitve odgovornosti overitelja .....	32
9.8.	Poravnava škode.....	32
9.9.	Začetek in prenehanje veljavnosti .....	33
9.9.1.	Začetek veljavnosti .....	33
9.9.2.	Prenehanje veljavnosti .....	33
9.9.3.	Učinek in posledice prenehanja veljavnosti.....	33
9.10.	Obvestila in komuniciranje z udeleženci .....	33
9.11.	Spreminjanje dokumenta .....	33
9.11.1.	Postopek uveljavitve sprememb.....	33
9.11.2.	Postopek obveščanja in rok za pripombe.....	33
9.11.3.	Spremembe, ki zahtevajo novo identifikacijsko oznako politike .....	33
9.12.	Reševanje sporov.....	33
9.13.	Veljavna zakonodaja .....	33
9.14.	Skladnost s pravnimi akti .....	34

---

9.15.	Splošne določbe.....	34
9.15.1.	Ostali obvezujoči dokumenti.....	34
9.15.2.	Prenos pravic in obveznosti.....	34
9.15.3.	Spremembe okoliščin delovanja.....	34
9.15.4.	Uveljavljanje (povračila stroškov v primeru sporov in izjeme).....	34
9.15.5.	Višje sile.....	34
9.16.	Ostale določbe .....	35
10.	Priloge.....	36
10.1.	Transformacija znakov za zapis imena in priimka v digitalnih potrdilih (polje CN) .....	36
10.2.	Osnovni nabor - znaki slovenske abecede: .....	36
10.3.	Dodatni nabor – znaki, ki se pogosto uporabljajo v lastnoimenskem besedju .....	36
10.4.	Nabor znakov s pravorečnimi znamenji .....	36
10.5.	Transformacija posebnih znakov .....	37
10.6.	Pojmi in kratice .....	37

---

# 1. UVOD

---

## 1.1. Pregled

Zavod za zdravstveno zavarovanje Slovenije (Zavod) ima vzpostavljeno zasebno infrastrukturo javnih ključev (ZZZS-PKI) v okviru katere deluje overitelj digitalnih potrdil ZZZS-CA za potrebe delovanja sistema kartice zdravstvenega zavarovanja. Overitelj ZZZS-CA deluje kot zaprt sistem in izdaja standardna (nekvalificirana oziroma normalizirana) digitalna potrdila za kartice zdravstvenega zavarovanja (KZZ), profesionalne kartice (PK) in spletne strežnike (SSL). Digitalna potrdila se uporabljajo za preverjanje istovetnosti imetnikov KZZ in PK ter spletnih strežnikov SSL ob dostopu do on-line sistema zdravstvenega zavarovanja.

Zavod ima v okviru zasebne infrastrukture overitelja ZZZS-CA vzpostavljene tri korenske izdajatelje, ki izdajajo potrdila imetnikom potrdil. Potrdila korenskih izdajateljev imajo sledeča razločevalna imena:

- CN=ZZZS-CA ,OU=PKI,O=ZZZS,C=SI
- CN=ZZZS-CA G2,OU=PKI,O=ZZZS,C=SI
- CN=ZZZS-CA ECC,OU=PKI,O=ZZZS,C=SI

Korenski izdajatelj CN=ZZZS-CA ,OU=PKI,O=ZZZS,C=SI uporablja asimetrične ključe RSA in zgoščevalni algoritem SHA-1.

Korenski izdajatelj CN=ZZZS-CA G2,OU=PKI,O=ZZZS,C=SI uporablja asimetrične ključe RSA in zgoščevalni algoritem SHA-256.

Korenski izdajatelj CN=ZZZS-CA ECC,OU=PKI,O=ZZZS,C=SI uporablja asimetrične ključe, ki temeljijo na eliptičnih krivuljah (Elliptic Curve Cryptosystems - ECC) in zgoščevalni algoritem SHA-384.

---

## 1.2. Naziv dokumenta in identifikacijska oznaka

Naziv pričujočega dokumenta je Politika delovanja overitelja digitalnih potrdil Zavoda za zdravstveno zavarovanje Slovenije za sistem kartice zdravstvenega zavarovanja. Skrajšan naziv dokumenta je Politika ZZZS-CA.

Politika ZZZS-CA velja za digitalna potrdila označena z naslednjimi identifikacijskimi oznakami politik (angl. Policy Object Identifiers):

Tip digitalnega potrdila	Identifikacijska oznaka politike
PK-NDP in PK-NDP-EC	1.3.6.1.4.1.29715.1.2.1
KZZ-ODP in KZZ-ODP-EC	1.3.6.1.4.1.29715.1.2.2
KZZ-NDP in KZZ-NDP-EC	1.3.6.1.4.1.29715.1.2.3
SSL-NDP	1.3.6.1.4.1.29715.1.2.4

V nadaljevanju dokumenta se oznaka PK-NDP uporablja tudi za potrdila PK-NDP-EC. Oznaka PK-NDP-EC se uporabi kadar je potrebno razlikovanje med tipoma potrdil.

V nadaljevanju dokumenta se oznaka KZZ-ODP uporablja tudi za potrdila KZZ-ODP-EC. Oznaka PK-ODP-EC se uporabi kadar je potrebno razlikovanje med tipoma potrdil.

V nadaljevanju dokumenta se oznaka KZZ-NDP uporablja tudi za potrdila KZZ-NDP-EC. Oznaka PK-NDP-EC se uporabi kadar je potrebno razlikovanje med tipoma potrdil.

---

## 1.3. Udeleženci infrastrukture javnih ključev

### 1.3.1. Overitelj

Overitelja sestavlja osebje odgovorno za upravljanje politike delovanja in celotnega delovanja overitelja (angl. Policy Management Authority – PMA) ter osebje za upravljanje in vzdrževanje infrastrukture overitelja, zasebnih kriptografskih ključev overitelja ter strojne in programske opreme (angl. Operations Authority – OA).

Overitelj ZZS-CA upravlja tri korenske izdajatelje digitalnih potrdil, ki so v postopku tvorjenja ključev sami sebi izdali digitalno potrdilo (angl. self-signed certificate).

Naloge upravitelja politike overitelja (ZZS-CA PMA, ali kratko PMA), ki jih opravlja osebje Zavoda so:

- izdelava in vzdrževanje Politike ZZS-CA;
- predložitev Politike ZZS-CA, ter sprememb v pregled in odobritev odgovorni oziroma pooblaščenim osebam Zavoda v skladu z notranjimi pravili Zavoda;
- nadzor in revizija skladnosti delovanja upravitelja infrastrukture overitelja (ZZS-CA OA) s Politiko ZZS-CA;
- reševanje sporov med imetniki potrdil in ZZS-CA.
- Naloge upravitelja infrastrukture overitelja (ZZS-CA OA, ali kratko OA), ki jih opravlja osebje izvajalca personalizacije kartic so:
  - generiranje para ključev overitelja, varno upravljanje zasebnega ključa overitelja ter distribucija javnega ključa overitelja;
  - vzpostavitev okolja in postopka za obdelavo zahtevkov za izdajo digitalnih potrdil ter podpisovanje in izdaja digitalnih potrdil;
  - objava in distribucija digitalnih potrdil;
  - izvedba preklica digitalnih potrdil, vključno z objavo registra preklicanih potrdil (angl. Certificate Revocation List – CRL);
  - upravljanje infrastrukture overitelja v skladu s Politiko ZZS-CA;
  - izdelava in vzdrževanje Pravil delovanja overitelja ZZS-CA ter predložitev v odobritev in potrditev Zavodu (glej poglavje 1.5.3 Odgovorni organ za odobritev skladnosti pravil delovanja upravitelja infrastrukture overitelja s Politiko ZZS-CA).

V nadaljevanju dokumenta, kjer ni potrebno razločevati med specifičnimi nalogami ali korenskim izdajatelji, se za overitelja kot celoto uporabljata tudi izraza overitelj ZZS-CA in overitelj.

Tabela 1: Podatki potrdila CN=ZZS-CA ,OU=PKI,O=ZZS,C=SI

Naziv polja	Vrednost
Različica, angl. Version	3
Serijska številka potrdila angl. Serial Number	6E94F8FC855E48C3
Algoritem za podpis angl. Signature algorithm	sha1WithRSAEncryption
Izdajatelj angl. Issuer	C=si,O=ZZS,OU=PKI,CN=ZZS-CA
Imetnik angl. Subject	C=si,O=ZZS,OU=PKI,CN=ZZS-CA



Pričetek veljavnosti, angl. Validity: Not Before	4. september 2008 10:58:24
Konec veljavnosti angl. Validity: Not After	30. avgust 2028 10:58:24
Algoritem javnega ključa angl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ RSA Public Key	Ključ RSA dolžine 2048 bitov
Name uporabe ključa angl. Key Usage	Kritično (Critical) Podpis potrdil (keyCertSign) Podpis CRL (cRLSign)
Osnovne omejitve angl. Basic Constraints	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa angl. Authority Key Identifier	A1A617AE07645D72A4D0ADD769A988736AE54052
Identifikator imetnikovega ključa angl. Subject Key Identifier	A1A617AE07645D72A4D0ADD769A988736AE54052
Odtis potrdila	
Odtis potrdila SHA-1 angl. Certificate Fingerprint – SHA1	8B61F7B2950EE1F11C04ABE9D61701CD763D1CE9
Odtis potrdila SHA-256, angl. Certificate Fingerprint – SHA256	12DAF111796350D21956B1C98BEED66B 10BD3E11F0581AACDE3C0DA68D5FD3B6

Tabela 2: Podatki potrdila CN=ZZZS-CA G2 ,OU=PKI,O=ZZZS,C=SI

Naziv polja	Vrednost
Različica, angl. Version	3
Serijska številka potrdila angl. Serial Number	04B4616768CA93CD
Algoritem za podpis angl. Signature algorithm	Sha256WithRSAEncryption
Izdajatelj angl. Issuer	C=SI,O=ZZZS,OU=PKI,CN=ZZZS-CA G2
Imetnik angl. Subject	C=SI,O=ZZZS,OU=PKI,CN=ZZZS-CA G2
Pričetek veljavnosti, angl. Validity: Not Before	17. januar 2018 18:08:52
Konec veljavnosti angl. Validity: Not After	17. januar 2038 18:08:52

Algoritem javnega ključa angl. Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ RSA Public Key	Ključ RSA dolžine 3072 bitov
Name uporabe ključa angl. Key Usage	Kritično (Critical) Podpis potrdil (keyCertSign) Podpis CRL (cRLSign)
Osnovne omejitve angl. Basic Constraints	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa angl. Authority Key Identifier	E5FD859BD5E18BC7C0599D6A89089B089154AA28
Identifikator imetnikovega ključa angl. Subject Key Identifier	E5FD859BD5E18BC7C0599D6A89089B089154AA28
Odtis potrdila	
Odtis potrdila SHA-1 angl. Certificate Fingerprint – SHA1	B7C4890C8D9D3D200B26578532EB1E3D1EF03FFC
Odtis potrdila SHA-256, angl. Certificate Fingerprint – SHA256	6312EBFEEEE6DE5505977DD6F94C5F1DB3E411AB8 3FF07A7A578499A384EDC58B

Tabela 3: Podatki v potrdilu CN=ZZZS-CA ECC ,OU=PKI,O=ZZZS,C=SI

Naziv polja	Vrednost
Različica, angl. Version	3
Serijska številka potrdila angl. Serial Number	481C34BBE1E9A83D
Algoritem za podpis angl. Signature algorithm	ecdsa-with-SHA384
Izdajatelj angl. Issuer	C=SI,O=ZZZS,OU=PKI,CN=ZZZS-CA ECC
Imetnik angl. Subject	C=SI,O=ZZZS,OU=PKI,CN=ZZZS-CA ECC
Pričetek veljavnosti, angl. Validity: Not Before	25. marec 2021 11:28:14
Konec veljavnosti angl. Validity: Not After	25. junij 2046 11:28:14
Algoritem javnega ključa angl. Subject Public Key Algorithm	secp384r1 (1.3.132.0.34)
Imetnikov javni ključ RSA Public Key	Ključ EC dolžine 384 bitov

Name uporabe ključa angl. Key Usage	Kritično (Critical) Podpis potrdil (keyCertSign) Podpis CRL (cRLSign)
Osnovne omejitve angl. Basic Constraints	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa angl. Authority Key Identifier	058BB69990CA03A4AFF4297B1B4DA7012296CB6D
Identifikator imetnikovega ključa angl. Subject Key Identifier	058BB69990CA03A4AFF4297B1B4DA7012296CB6D
Odtis potrdila	
Odtis potrdila SHA-1 angl. Certificate Fingerprint – SHA1	8CFC95D7EB63067EE463ED7548D30292978A30ED
Odtis potrdila SHA-256, angl. Certificate Fingerprint – SHA256	92FCB0534CFDD0E467B52D7A3A45A26D4C855681 A97C10F9D856E9B49D48CD50

### 1.3.2. Prijavna služba

Prijavna služba se ne uporablja. Overitelj ZZS-CA izdaja:

- digitalna potrdila samo imetnikom KZZ in PK na osnovi podatkov o zavarovanih osebah in izvajalcih zdravstvenih storitev v obstoječih evidencah Zavoda in
- digitalna potrdila za spletne strežnike in naprave SSL, ki jih upravlja Zavod, ali pa se povezujejo s strežniki Zavoda.

### 1.3.3. Imetniki digitalnih potrdil

Overitelj ZZS-CA izdaja digitalna potrdila:

- fizičnim osebam, ki so upravičene do KZZ na podlagi Pravilnika o KZZ (v nadaljevanju imetniki KZZ);
- fizičnim osebam, ki so upravičene do PK na podlagi Pravilnika o KZZ (v nadaljevanju imetniki PK) ter
- skrbnikom sistemov IT v okviru Zavoda in z Zavodom povezanih organizacij za uporabo na spletnih strežnikih in napravah SSL.

### 1.3.4. Tretje osebe

Tretje osebe so fizične ali pravne osebe, ki zaupajo digitalnemu potrdilu, oziroma povezavi med imenom imetnika in javnim ključem v digitalnem potrdilu. Tretje osebe so tako osebe, ki imajo digitalno potrdilo overitelja ZZS-CA, kot tudi subjekti, ki takšnega potrdila nimajo in zaupajo podatkom v digitalnem potrdilu na podlagi zaupanja v overitelja ZZS-CA.

---

## 1.4. Namen uporabe digitalnih potrdil

### 1.4.1. Dovoljena uporaba digitalnih potrdil

Digitalna potrdila PK-NDP in KZZ-NDP izdana po pričujoči politiki se prvenstveno uporabljajo za preverjanje istovetnosti imetnikov KZZ in PK ob dostopu do vstopne točke on-line sistema zdravstvenega zavarovanja.

Digitalna potrdila KZZ-ODP izdana po pričujoči politiki so prvenstveno namenjena za preverjanje istovetnosti imetnikov KZZ ob prijavi v spletne aplikacije za dostop do lastnih zdravstveno-zavarovalniških in medicinskih podatkov.

Digitalna potrdila SSL-NDP izdana po pričujoči politiki so prvenstveno namenjena preverjanju istovetnosti strežnikov in naprav, ki se povezujejo preko protokola SSL v računalniškem omrežju Zavoda in na njega povezanih zunanjih sistemov.

Digitalna potrdila overitelja ZZZS-CA se lahko neomejeno uporabljajo tudi za druge namene v okviru zdravstvenega varstva in zdravstvenega zavarovanja. Uporaba izven tega okolja je dovoljena le po dogovoru z Zavodom.

---

## 1.5. Upravljanje s pravili delovanja

### 1.5.1. Organ, ki upravlja s pričujočim dokumentom

Pričujoči dokument (Politika ZZZS-CA) in overitelja ZZZS-CA kot celoto, upravlja Zavod.

### 1.5.2. Kontaktni podatki

Naslov:	Zavod za zdravstveno zavarovanje Slovenije Oddelek za operativo Miklošičeva cesta 24 1507 Ljubljana
Telefon:	01 3077548
Spletni naslov:	<a href="https://ca.zzss.si/">https://ca.zzss.si/</a>
Elektronska pošta:	ca-info@zzss.si

### 1.5.3. Odgovorni organ za odobritev skladnosti pravil delovanja upravitelja infrastrukture overitelja s Politiko ZZZS-CA

Skladnost pravil delovanja overitelja (angl. Certification Practice Statement – CPS) potrjuje odgovorna oziroma pooblaščen oseba Zavoda v skladu z notranjimi pravili Zavoda.

### 1.5.4. Postopek odobritve pravil delovanja overitelja

Postopek odobritve in preverjanje skladnosti pravil delovanja overitelja s Politiko ZZZS-CA preverja ZZZS-CA PMA. V okviru postopka odobritve se izvede:

- preverjanje skladnosti dokumenta Pravila delovanja overitelja ZZZS-CA z zahtevami Politike ZZZS-CA in
- preverjanje infrastrukture ter vzpostavljene postopke glede na določila Politike ZZZS-CA in priporočila dobre prakse (po potrebi).

ZZZS-CA PMA po izvedenem postopku preverjanja predloži Pravila delovanja overitelja ZZZS-CA v odobritev odgovorni osebi navedeni v poglavju 1.5.3.

---

## 2. ODGOVORNOST ZA OBJAVE IN REPOZITORIJ

---

### 2.1. Repozitorij

Overitelj ZZS-CA objavlja informacije o digitalnih potrdilih in svojih storitvah na spletnem naslovu <https://ca.zzs.si/>.

### 2.2. Objave informacij o digitalnih potrdilih

Overitelj ZZS-CA objavlja sledeče informacije:

Informacija	Lokacija objave
Digitalno potrdilo overitelja ZZS-CA	<a href="https://ca.zzs.si/zzs-ca.cer">https://ca.zzs.si/zzs-ca.cer</a> <a href="https://ca.zzs.si/zzs-ca-g2.cer">https://ca.zzs.si/zzs-ca-g2.cer</a> <a href="https://ca.zzs.si/zzs-ca-ecc.cer">https://ca.zzs.si/zzs-ca-ecc.cer</a>  Digitalna potrdila overitelja je možno pridobiti tudi na zahtevo poslano na naslov naveden v 1.5.2
Register preklicanih potrdil	HTTP in LDAP naslov registra preklicanih potrdil, kot navedeno v razširitvenem polju digitalnega potrdila (glej poglavje 7.1.2): Za ZZS-CA: HTTP URL: <a href="http://ca.zzs.si/crl/zzs-ca.crl">http://ca.zzs.si/crl/zzs-ca.crl</a> LDAP URL: <a href="ldap://ca.zzs.si/cn=ZZS-CA,ou=PKI,o=ZZS,c=SI?certificateRevocationList">ldap://ca.zzs.si/cn=ZZS-CA,ou=PKI,o=ZZS,c=SI?certificateRevocationList</a> Za ZZS-CA-G2: HTTP URL: <a href="http://ca.zzs.si/crl/zzs-ca-g2.crl">http://ca.zzs.si/crl/zzs-ca-g2.crl</a> LDAP URL: <a href="ldap://ca.zzs.si/cn=ZZS-CA%20G2,ou=PKI,o=ZZS,c=SI?certificateRevocationList%3Bbinary">ldap://ca.zzs.si/cn=ZZS-CA%20G2,ou=PKI,o=ZZS,c=SI?certificateRevocationList%3Bbinary</a> Za ZZS-CA-ECC: HTTP URL: <a href="http://ca.zzs.si/crl/zzs-ca-ecc.crl">http://ca.zzs.si/crl/zzs-ca-ecc.crl</a> LDAP URL: <a href="ldap://ca.zzs.si/cn=ZZS-CA%20ECC,ou=PKI,o=ZZS,c=SI?certificateRevocationList%3Bbinary">ldap://ca.zzs.si/cn=ZZS-CA%20ECC,ou=PKI,o=ZZS,c=SI?certificateRevocationList%3Bbinary</a>
Politika ZZS-CA	<a href="https://ca.zzs.si/dokumenti/">https://ca.zzs.si/dokumenti/</a>
Obrazec za preklic KZZ-OPD digitalnih potrdil in ostale informacije glede delovanja overitelja	<a href="https://ca.zzs.si/dokumenti/">https://ca.zzs.si/dokumenti/</a>

### 2.3. Čas in pogostost objav

Overitelj uvrsti preklicano digitalno potrdilo v register preklicanih potrdil takoj po opravljenem preklicu. Objava registra preklicanih potrdil se izvaja, kot je navedeno v poglavjih 4.8.5 in 4.8.7.

Ostale informacije so objavljene sproti ob njihovi spremembi ali ko postanejo dostopne overitelju.

### 2.4. Dostop do podatkov v repozitoriju

Vse informacije v repozitorijih so dostopne za branje brez omejitev. Repozitoriji imajo vzpostavljene ustrezne tehnične kontrole za zaščito pred nepooblaščenimi spremembami.

---

## 3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

---

### 3.1. Določanje imen

#### 3.1.1. Vrste imen

Vsako digitalno potrdilo vsebuje edinstveno razločevalno ime X.501 DN (angl.: Distinguished Name, DN) v skladu z RFC3280. Splošno ime (angl. Common Name, CN) vsebuje oznako potrdila, ime, priimek in ZZZS številko osebe oziroma imetnika ter številko izvoda kartice, kot je navedeno v tabeli v poglavju 3.1.4. Razločevalno ime je praviloma zapisano v obliki UTF8String in ne sme biti prazno.

#### 3.1.2. Potreba po smiselnosti imen

Nabor atributov v kratkem razločevalnem imenu (angl. Relative Distinguished Name, RDN) mora enolično določati imetnika digitalnega potrdila. Edinstvenost razločevalnega imena je dosežena z uporabo ZZZS številke in številke izvoda kartice, ki sta dodani imenu in priimku v splošnem imenu.

#### 3.1.3. Anonimnost imetnikov in uporaba psevdonimov

Anonimnost imetnikov in uporaba psevdonimov se ne uporablja.

#### 3.1.4. Pravila za interpretacijo različnih oblik imen

Transformacija znakov za zapis imena in priimka v digitalnih potrdilih (polje CN) je podana v prilogi 10.1.

Razločevalno ime (angl. Distinguished Name) v digitalnih potrdilih vsebuje sledeča polja:

Atribut razločevalnega imena	Vrednost
Country (C=)	SI
Organization (O=)	ZZZS
Organizational Unit (OU=)	PKI
Organizational Unit (OU=)	PK-NDP (digitalna potrdila na PK); ali KZZ-NDP (digitalna potrdila brez PIN-a na KZZ); ali KZZ-ODP (digitalna potrdila s PIN-om na KZZ)
Common Name (CN=)	V potrdilih s ključi RSA: "[KZZ-NDP KZZ-ODP PK-NDP] ime in priimek imetnika" "ZZZS številka" "številka izvoda kartice" ali polno ime strežnika SSL. V potrdilih s ključi EC: "[KZZ-NDP-EC KZZ-ODP-EC PK-NDP-EC] ime in priimek imetnika" "ZZZS številka" "številka izvoda kartice" ali polno ime strežnika SSL.

---

### 3.2. Prva registracija

#### 3.2.1. Metode dokazovanja lastništva zasebnega ključa

Kriptografski pari ključev in digitalno potrdilo se generirajo v okviru postopka personalizacije kartic, zato dokazovanje lastništva zasebnega ključa s strani imetnika ni potrebno. V okviru postopka izdelave kartic se za kontrolo povezave med zasebnim in javnim ključem vsebovanim

---

v zahtevku za izdajo digitalnega potrdila uporablja PKCS#10 oblika zahtevka v skladu z RSA PKCS#10 Certification Request Syntax Standard.

### **3.2.2. Preverjanje istovetnosti za fizične osebe**

Overitelj ZZS-CA izdaja:

- digitalna potrdila imetnikom KZZ in PK na osnovi podatkov o zavarovanih osebah in izvajalcih zdravstvenih storitev v obstoječih evidencah Zavoda;
- digitalna potrdila za strežnike SSL na osnovi podatkov v inertnih evidencah Zavoda in zahtevka upravitelja strežnika.

Podatki imetnikov KZZ in PK se pridobijo in preverijo skladno z ZZVZZ in Pravili OZZ.

### **3.2.3. Podatki o imetnikih digitalnih potrdil, ki se ne preverjajo**

Vsi podatki vsebovani v digitalnih potrdilih so preverjeni, ali pa jih določi Zavod.

### **3.2.4. Merila za medsebojno povezovanje**

Merila za medsebojno povezovanje se ne uporabljajo.

---

## **3.3. Preverjanje istovetnosti pri obnovi digitalnega potrdila**

### **3.3.1. Preverjanje istovetnosti pri rutinski obnovi digitalnih potrdil**

Rutinska obnova potrdil imetnikov KZZ in PK se izvede ob koncu veljavnosti potrdila, ki se zgodi vedno le z izdajo nove kartice (KZZ, PK).

Rutinska obnova potrdil strežnikov SSL se izvede ob koncu veljavnosti potrdila na zahtevo skrbnika strežnika.

### **3.3.2. Preverjanje istovetnosti pri obnovi digitalnega potrdila po preklicu**

Kartico prekliche imetnik ali Zavod v primeru izgube, uničenja, nedelovanja ali drugih razlogov. Izdajo nove kartice opredeljuje Pravilnik o KZZ, preverjanje podatkov je enako kot določa poglavje 3.2.2.

---

## **3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila**

Glej poglavje 3.2.2.

---

# **4. UPRAVLJANJE Z DIGITALNIMI POTRDILI**

---

## **4.1. Prošnja za izdajo digitalnega potrdila**

Imetnikom ni potrebno vlagati posebne prošnje za izdajo oziroma pridobitev digitalnega potrdila overitelja ZZS-CA. Digitalna potrdila se izdajo imetnikom KZZ in PK hkrati s kartico na osnovi zahtevka za izdajo kartice, razen pri rutinski obnovi digitalnih potrdil, ki je navedena v poglavju 3.2.2, kjer zahtevka za izdajo kartice ni potreben.

Skrbniki sistemov IT posredujejo pisni zahtevek za pridobitev potrdila strežnika SSL na kontaktni naslov naveden v poglavju 1.5.2.

---

## **4.2. Izdaja digitalnega potrdila**

### **4.2.1. Postopki overitelja ob izdaji digitalnega potrdila**

Postopek izdaje digitalnih potrdil imetnikov KZZ in PK je integriran s postopkom personalizacije KZZ in PK. Izvajalec personalizacije v okviru postopka:

- registrira digitalno potrdilo v bazi sistema za overjanje in upravljanje digitalnih potrdil;
- generira par asimetričnih ključev (glej poglavji 6.1 in 6.2 );
- generira PKCS#10 zahtevek za izdajo digitalnega potrdila;
- posreduje PKCS#10 zahtevek sistemu za overjanje in upravljanje digitalnih potrdil, ki preveri zahtevek, ter overi in izda digitalno potrdilo.

Prosilci za izdajo digitalnega potrdila strežnika SSL posredujejo overitelju zahtevek v obliki PKCS#10. Osebe izvajalca personalizacije posreduje zahtevek sistemu za overjanje in upravljanje digitalnih potrdil, ki preveri zahtevek, ter overi in izda digitalni potrdilo. Osebe izvajalca personalizacije posreduje izdano digitalno potrdilo prosilcu po elektronski pošti.

Celoten postopek se izvaja v zaprtem, fizično ločenem in strogo varovanem okolju.

### **4.2.2. Obvestilo imetniku o izdaji digitalnega potrdila**

Imetnik KZZ ali PK prejme obvestilo o izdaji digitalnega potrdila hkrati s kartico.

PIN za uporabo digitalnega potrdila PK-NDP na PK se pošlje imetniku s priporočeno pošiljko in časovnim zamikom.

PIN za uporabo digitalnega potrdila KZZ-ODP na KZZ se pošlje imetniku s priporočeno pošiljko na zahtevo.

Za uporabo digitalnega potrdila KZZ-NDP na KZZ PIN ni potreben.

Imetnik potrdila strežnika SSL prejme potrdil o izdaji hkrati z digitalnim potrdilom. Overitelj ne generira zasebnih ključev strežnikov SSL, zato posredovanje PIN-a ni potrebno.

---

## **4.3. Prevzem digitalnega potrdila**

### **4.3.1. Postopek potrditve prevzema digitalnega potrdila**

Imetniki KZZ in PK potrdijo prevzem digitalnega potrdila s prevzemom poštno pošiljke, s katero mu je poslana kartica.

Imetniki potrdil strežnikov SSL potrdijo prevzem digitalnega potrdila s povratnim sporočilom preko elektronske pošte.

### **4.3.2. Objava digitalnega potrdila**

Digitalna potrdila PK-NDP, KZZ-NDP, KZZ-ODP in SSL-NDP niso javno objavljena.

### **4.3.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila**

Ni predvideno.

---

## **4.4. Uporaba ključev in digitalnih potrdil**

### **4.4.1. Uporaba ključev in digitalnih potrdil s strani imetnikov**

Imetniki lahko uporabljajo ključe in digitalna potrdila za namene označene v razširitvenem polju keyUsage digitalnega potrdila (glej poglavje 6.1.7) in namene opredeljene v poglavju 1.41.4.



---

Imetnik mora skrbno varovati kartico in PIN, da prepreči razkritje zasebnih ključev ali nedovoljeno uporabo kartice.

#### **4.4.2. Uporaba digitalnih potrdil s strani tretjih oseb**

Tretje osebe so dolžne omejiti uporabo digitalnih potrdil PK-NDP, KZZ-NDP, KZZ-ODP in SSL\_NDP le na namene opredeljene v poglavju 1.4. Tretje osebe morajo poleg tega:

- upoštevati določila in omejitve Politike ZZZS-CA;
- pred vsako uporabo digitalnega potrdila preveriti status potrdila v registru preklicanih potrdil;
- obvestiti overitelja v primeru suma zlorabe ali napačne uporabe digitalnega potrdila.

---

#### **4.5. Obnova digitalnih potrdil brez spremembe ključev**

Obnova digitalnih potrdil brez spremembe ključev se ne uporablja.

---

#### **4.6. Obnova digitalnih potrdil**

Digitalna potrdila PK-NDP, KZZ-NDP in KZZ-ODP in pripadajoči ključi so zapisani na PK oziroma KZZ kartico v okviru personalizacije kartice. Njihova obnova oziroma zamenjava brez zamenjave kartice ni možna. Postopek zamenjave kartice se izvaja v skladu s Pravilnikom o KZZ.

Obnova digitalnih potrdil SSL-NDP se izvaja po istem postopku, kot pridobitev prvega potrdila.

---

#### **4.7. Sprememba digitalnega potrdila**

Sprememba digitalnega potrdila se ne uporablja.

---

#### **4.8. Začasna ukinitve veljavnosti in preklic digitalnega potrdila**

##### **4.8.1. Okoliščine preklica**

Preklic KZZ-NDP in PK-NDP digitalnih potrdil se izvede samodejno ob preklicu kartice.

Preklic KZZ-ODP digitalnih potrdil se izvede samodejno ob preklicu kartice ali na zahtevo imetnika.

Okoliščine za preklic kartic so navedene v Pravilniku o KZZ.

Dodatni razlogi za preklic KZZ-ODP so:

- podatki vsebovani v digitalnem potrdilu so napačni ali obstaja sum da so napačni;
- zloraba zasebnega ključa, ali utemeljen sum da je prišlo do razkritja zasebnega ključa;
- kršenje določil Politike ZZZS-CA.

Overitelj lahko prekliče potrdilo iz naslednjih razlogov:

- dejansko ali domnevno razkritje zasebnih ključev;
- spremembe podatkov v potrdilu, ki zahtevajo izdajo novega;
- prenehanje delovanja strežnika SS;
- na zahtevo skrbnika strežnika SSL ali Zavoda.

##### **4.8.2. Kdo lahko zahteva preklic**

Preklic digitalnih potrdil KZZ in PK lahko zahteva imetnik kartice, ali Zavod, kadar uvrsti kartico na seznam neveljavnih skladno s Pravilnikom o KZZ in v primeru zlorab.

---

Preklic SSL-NDP digitalnega potrdila lahko zahtevo skrbnik strežnika SSL, ali Zavod.

#### **4.8.3. Postopki za preklic**

Preklic KZZ in PK se izvaja avtomatsko ob preklicu veljavnosti kartice v skladu s Pravilnikom o KZZ.

Preklic KZZ-ODP ali SSL-NDP se izvede na osnovi zahtevka imetnika. Imetnik mora izpolniti obrazec objavljen na spletni strani overitelja (glej poglavje 2.2 Objave informacij o digitalnih potrdilih) za preklic KZZ-ODP in ga osebno oddati na okencu Zavoda.

Ob preklicu KZZ-ODP, tudi zaradi zlorabe pripadajočega zasebnega ključa, ostane kartica še vedno veljavna.

#### **4.8.4. Čas za posredovanje vloge za preklic**

Imetnik mora zahtevati preklic kartice, ali digitalnega potrdila SSL-NDP v najkrajšem možnem času po nastopu okoliščin za preklic (glej poglavje 4.8.1).

#### **4.8.5. Čas od vloge za preklic do preklica**

Preklic digitalnih potrdil se izvrši istega dne kot je prejet zahtevek za preklic, če je zahtevek prejete najkasneje do 12.00 ure. Če je zahtevek prejet po 12.00 uri, se preklic izvrši naslednjega dne.

#### **4.8.6. Obveza preverjanja registra preklicanih potrdil**

Vsi subjekti, ki se zanašajo na digitalna potrdila overitelja ZZS-CA, morajo pred uporabo javnega ključa vsebovanega v digitalnem potrdilu preveriti register preklicanih digitalnih potrdil. Za preverjanje veljavnosti potrdil je merodajen najnovejši objavljeni register preklicanih digitalnih potrdil objavljen na spletnem naslovu navedem v razširitvenem polju vsakega potrdila in na spletni strani overitelja (glej poglavje 2.2 Objave informacij o digitalnih potrdilih). Register preklicanih digitalnih potrdil je podpisan z istim overiteljevim zasebnim ključem, kot se uporablja za podpis digitalnih potrdil.

#### **4.8.7. Pogostost objav registrov preklicanih potrdil**

Veljavnost CRL je 10 dni. Overitelj objavi nov CRL po izvedbi preklica digitalnih potrdil, ali vsaj 3 dni pred iztekom veljavnosti.

#### **4.8.8. Storitev sprotnega preverjanje statusa digitalnih potrdil**

Storitev sprotnega preverjanje statusa digitalnih potrdil se ne uporablja.

#### **4.8.9. Ostale oblike objavljanja preklicanih digitalnih potrdil**

Ostale oblike objavljanja preklicanih digitalnih potrdil se ne uporabljajo.

#### **4.8.10. Posebne zahteve glede zlorabe ključa**

Glej 4.8.2.

---

### **4.9. Storitve objavljanja statusa digitalnih potrdil**

#### **4.9.1. Tehnične lastnosti storitve**

Status digitalnih potrdil je objavljen z uporabo registra preklicanih potrdil v skladu z (X.509 Certificate Revocation List ) v skladu z RFC3280. Register preklicanih potrdil je dostopen preko LDAP in http protokola. Točen naslov objave registra preklicanih potrdil mora biti vsebovan v

---

razširitvenem polju vsakega izdanega digitalnega potrdila, kot je navedeno v poglavju 7.1.2 Razširitvena polja.

#### **4.9.2. Razpoložljivost storitve**

Overitelj mora zagotavljati razpoložljivost storitve 24 ur 7 dni v tednu.

---

#### **4.10. Predčasna ukinitve veljavnosti digitalnih potrdil**

Predčasna ukinitve veljavnosti digitalnih potrdil se ne uporablja.

---

#### **4.11. Varnostno kopiranje in odkrivanje zasebnega ključa**

Overitelj ne izvaja varnostnega kopiranja in odkrivanja zasebnega ključa.

##### **4.11.1. Postopki povrnitve zgodovine ključev in odkrivanje kopije zasebnega ključa za dešifriranje**

Postopki povrnitve zgodovine ključev in odkrivanje kopije zasebnega ključa za dešifriranje se ne uporabljajo.

## **5. FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE**

Overiteljevo infrastrukturo za izdajanje in upravljanje digitalnih potrdil upravlja izvajalec personalizacije kartic, ki mora zagotavljati varnostne ukrepe opredeljene v nadaljevanju poglavja.

---

### **5.1. Fizično varovanje**

Upravitelj infrastrukture (ZZZS-CA OA) mora zagotoviti:

- varne prostore za izvajanje dejavnosti povezanih z izdajo in upravljanjem digitalnih potrdil;
- nadzor in beleženje dostopov do prostorov, ter da ima dostop samo osebje overitelja, ki upravlja kriptografske ključe in sisteme overitelja;
- ustrezno napajanje in sisteme za vzdrževanje okolja;
- tehnične in varnostne ukrepe za zaščito pred ognjem;
- hranjenje medijev na način, ki preprečuje nedovoljeno ali nenamerno uporabo, dostop, razkritje, ali uničenje s strani fizičnih oseb, ali drugih groženj (npr. ogenj, voda);
- odstranjevanje odpadkov na način, ki preprečuje nedovoljeno ali nenamerno uporabo, dostop, ali razkritje podatkov;
- hranjenje varnostnih kopij in drugih kritičnih podatkov na rezervni lokaciji.

---

### **5.2. Organizacijski varnostni ukrep**

Upravitelj infrastrukture (ZZZS-CA OA) mora imeti:

- jasno opredeljeno organizacijsko strukturo, razdelitev nalog, ter pooblastil za dostop do infrastrukture in podatkov overitelja glede na potrebo po vedenju;
- vzpostavljen sistem avtorizacije dveh oseb za fizični dostop do kritičnih elementov sistema, ter uporabo in upravljanje overiteljevih zasebnih ključev;
- vzpostavljene postopke dodeljevanja, preverjanja, nadzora in ukinitve pravic upraviteljevega osebja za dostop do prostorov, sistemov in posameznih funkcij sistema;

- 
- zagotoviti, da je dostop do prostorov, sistemov in posameznih funkcij sistema omejen na pooblaščen osebe, ter da vzpostavljena infrastruktura omogoča ločevanje, oziroma omejevanje pravic na sistemu glede na funkcije, kot so skrbnik operacijskega sistema, skrbnik zasebnih ključev overitelja in skrbnik varnosti sistema.

---

### **5.3. Zahteve za osebje overitelja**

Upravitelj infrastrukture overitelja mora zaposlovati ustrezno usposobljeno in izkušeno osebje. Izpolnjene morajo biti sledeče zahteve in pogoji:

- Vsaka oseba mora biti ustrezno usposobljena za nalog, ki jih opravlja in ne sme opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog v okviru infrastrukture overitelja;
- Upravitelj infrastrukture overitelja mora imeti opredeljene in vzpostavljene postopke preverjanja primernosti oseb;
- Osebe morajo imeti poleg ustrezne formalne izobrazbe opravljena tudi opravljena dodatna izobraževanja glede na specifičnost njihov nalog;
- Upravitelj infrastrukture overitelja mora imeti opredeljena področja, pogostost in okoliščine dodatnih usposabljanj operativnega osebja;
- Naloge posameznega člana operativnega osebja morajo biti opredeljene v opisu njegovega delovnega mesta;
- Opredeljeni morajo biti pogoji in postopki imenovanja na posamezno funkcijo v okviru operativnega osebja, ter morebitne menjave oziroma kroženje med delovnimi mesti;
- Upravitelj infrastrukture overitelja mora imeti opredeljene ukrepe ob kršitvah pooblastil in nalog s strani operativnega osebja;
- Upravitelj infrastrukture overitelja mora imeti z morebitnimi zunanjimi izvajalci sklenjeno pogodbo v kateri morajo biti opredeljene zahteve in pogoji za izvajalce, ter ukrepi oziroma posledice ob kršitvah;
- Upravitelj infrastrukture overitelja mora zagotoviti da ima operativno osebje dostop do vse potrebne tehnične ter ostale dokumentacije, kot so opisi nalog posameznega člana operativnega oseba, notranji varnostni in ostali pravilniki, ukrepi ob kršitvah pooblastil, ter ostala relevantna dokumentacija.

---

### **5.4. Postopki zbiranja in upravljanja revizijskih sledi**

Upravitelj infrastrukture overitelja mora imeti vzpostavljene postopke zbiranja revizijskih sledi dovoljene in nedovoljene uporabe, ter dostopov do infrastrukture overitelja. Zagotoviti mora:

- Zaupnost in integriteto aktualnih in arhiviranih beležk oziroma zapisov dogodkov v zvezi z digitalnimi potrdili;
- Redno in zanesljivo arhiviranje arhiviranih beležk oziroma zapisov dogodkov v zvezi z digitalnimi potrdili;
- Zanesljivo označevanja časa posameznih dogodkov zapisanih v beležkah;
- Beleženje vseh dogodkov povezanih z upravljanjem ključev;
- Beleženje vseh dogodkov povezanih z upravljanjem digitalnih potrdil;
- Beleženje vseh dogodkov povezanih z zahtevki za izdajo, preklic, ali obnovo digitalnih potrdil;
- Evidenco oziroma spisek beleženih dogodkov, ter načina zbiranja;
- Beleženje na način ki preprečuje enostavno namerno ali nenamerno brisanje revizijskih sledi, razen v primeru prenosa na drug medij, ali po izteku predpisanega obdobja hranjena.
- Redno pregledovanje beleženih dogodkov, ter izdelavo ocene ranljivosti.

---

## 5.5. Arhiviranje podatkov

Upravitelj infrastrukture overitelja mora vzpostaviti postopke arhiviranja za vse sisteme v okviru infrastrukture overitelja. Zagotoviti, oziroma vzpostaviti mora:

- Evidenco oziroma spisek arhiviranih podatkov in načina arhiviranja;
- Postopke arhiviranja, ki zagotavljajo integriteto, verodostojnost in zaupnost arhiviranih podatkov.
- Arhiviranje na način, ki preprečuje enostavno namerno, ali nenamerno brisanje arhivskih kopij, razen v primeru prenosa na drug medij, ali po izteku predpisanega obdobja hranjena.
- Prenos na drug medij, če uporabljeni mediji ne zagotavljajo hranjenja za predpisano obdobje;
- Hraniti arhivirane podatke vsaj še 5 let po izteku veljavnosti relevantnega ključa, ali digitalnega potrdila;
- Omogočiti vpogled v arhivirane podatke, opredeliti okoliščine in pogoje za vpogled, ter način preverjanja verodostojnosti podatkov.

---

## 5.6. Obnova digitalnih potrdil overiteljev

Overitelj mora ob vsaki obnovi lastnega digitalnega potrdila generirati nov par ključev. Postopek mora biti izveden nadzorovano v varnih prostorih in ob upoštevanju ostalih določil poglavja 5 FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE, ter določil poglavja 6 TEHNIČNE VARNOSTNE ZAHTEVE.

---

## 5.7. Postopki v primeru ogrožanja zasebnega ključa in okrevalni načrt

Upravitelj infrastrukture overitelja mora imeti vzpostavljene potrebne ukrepe za zagotavljanje kontinuitete delovanja, vključno z:

- Ukrepi za minimizacijo vpliva izpada električnega omrežja;
- Ukrepi za minimizacijo vpliva nesreč kot sta poplava, ali požar;
- Ukrepi za minimizacijo vpliva ob nerazpoložljivosti zadostnega števila operativnega osebja.

### 5.7.1. Postopki v primeru okvar in zlorab

Upravitelj infrastrukture overitelja zagotoviti vzpostavitev delovanja po okvarah v najkrajšem možnem času. Izdelati mora načrt, oziroma postopke vsaj za:

- Zagotavljanje kontinuitete poslovanja ob naravnih in drugih nesrečah (glej poglavje 5.7.4);
- Obnovo delovanja ob ogrožanju zasebnih ključev overitelja;
- Izdelavo in varno hranjenje varnostnih kopij za obnovitev delovanja in podatkov v primeru okvar ali nesreč.

### 5.7.2. Uničenje programske, strojne opreme ali podatkov

V primeru uničenja zasebnega ključa overitelja brez ogrožanja, mora upravitelj infrastrukture overitelja postopati kot je opredeljeno v poglavju 5.6 Obnova digitalnih potrdil overiteljev.

V primeru okvare, ali uničenja enega od sistemov infrastrukture, more upravitelj infrastrukture overitelja obnoviti delovanje sistema in povrniti podatke iz varnostne kopije v čim krajšem možnem času.

---

### 5.7.3. Ogrožanje zasebnega ključa overitelja

Ob ogrožanju, ali sumu ogrožanja zasebnega ključa overitelja, mora upravitelj infrastrukture overitelja obvestiti Zavod, zaustaviti izdajanje digitalnih potrdil, preklicati ključe overitelja in vseh imetnikov, ter obnoviti ključe in digitalno potrdilo overitelja kot je opredeljeno v poglavju 5.6 Obnova digitalnih potrdil overiteljev.

### 5.7.4. Neprekinjenost poslovanja ob naravnih in drugih nesrečah

V primeru naravnih in drugih nesreč mora overitelj zagotoviti izvajanje storitve na nadomestnem sistemu, ali rezervni lokaciji. Pri vzpostavitvi delovanja na nadomestnem sistemu, ali rezervni lokaciji morajo biti upoštevani vsi varnostni kriteriji in zahteve Politike ZZZS-CA in ne sme biti ogroženo zaupanje v overitelja.

V primeru, da to ne bo izvedljivo v roku 30 dni, mora overitelj postopati v skladu s poglavjem 5.8.

---

## 5.8. Prenehanje delovanja overitelja

V primeru prenehanja delovanja, bo overitelj obvestil Zavod in vse imetnike digitalnih potrdil, ter izvedel naslednje postopke:

- Preklical vsa digitalna potrdila;
- Zagotavljal razpoložljivost registrov preklicanih digitalnih potrdil vsaj še devetdeset (90) dni od preklica overiteljevega potrdila;
- Objavil preklic overiteljevega potrdila na spletnih straneh Zavoda in v registru preklicanih potrdil.

---

## 6. TEHNIČNE VARNOSTNE ZAHTEVE

---

### 6.1. Generiranje in namestitvev para ključev

#### 6.1.1. Generiranje para ključev

Ključni overitelja ZZZS-CA se generirajo po formalnem, podrobno predpisanem in nadzorovanem postopku, v varnih prostorih in ob upoštevanju ostalih določil poglavja 5 FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE. Ključni overitelja morajo biti generirani v strojnem varnostnem kriptografskem modulu, ki ima potrdilo o skladnosti z enim od standardov navedenih v poglavju 6.2.1 Standardi za kriptografski modul.

Imetniški pari ključev se generirajo pri izvajalcu personalizacije kartic v strojnem varnostnem kriptografskem modulu in nato skupaj z digitalnim potrdilom in ostalimi podatki uvozijo na kartico. Strojni varnostni kriptografski modul, imetniške kartice, zaščita ključev med prenosom na kartico in postopke kot celota, so skladni z EAL4+ PP.

Pare ključev strežnikov SSL generirajo skrbniki strežnikov v strojnem ali programskem kriptografskem modulu strežnika. Pri tem morajo upoštevati navodila proizvajalca programske opreme strežnika in varnostna priporočila dobre prakse.

#### 6.1.2. Dostava zasebnega ključa imetniku

Digitalna potrdila izdana po pričujoči politiki in pripadajoči zasebni ključ, se prenesejo do uporabnika na pametni kartici na katero so bili zapisani v postopku personalizacije kartice (glej poglavje 6.1.1 Generiranje para ključev). Pametna kartica je dostavljena imetniku s priporočeno pošiljko.

### 6.1.3. Dostava imetnikovega javnega ključa overitelju

Dostava javnega ključa imetnikov KZZ in PK ni potrebna.

Javni ključ strežnikov SSL je vsebovan v zahtevku PKCS#10, ki ga prosilec posreduje overitelju v postopku izdaje potrdila.

### 6.1.4. Dostava overiteljevega javnega ključa tretjim osebam

Overiteljev javni ključ je vsebovan v samo-podpisanem digitalnem potrdilu overitelja ZZS-CA in objavljen, ter dostopen na spletnih straneh overitelja (glej poglavje 2.2 Objave informacij o digitalnih potrdilih). Tretje osebe so dolžne preveriti istovetnost overitelja in celovitost njegovega digitalnega potrdila.

### 6.1.5. Dolžina ključev

Overitelj ZZS-CA uporablja za podpisovanje digitalnih potrdil imetnikov in registrov preklicanih potrdil asimetrične ključne RSA dolžine 2048 bitov.

Kriptografski ključni imetnikov, generirani v postopku personalizacije, so asimetrični ključni RSA. Dolžina ključev glede na vrsto potrdila je:

Tabela 4: Dolžina ključev v potrdilih izdanih do 25. 03. 2021

Vrsta potrdila	Dolžina ključev
PK-NDP	2048
KZZ-NDP	1024
KZZ-ODP	2048
SSL-NDP	1024 ali več

Tabela 5: Dolžina ključev v potrdilih izdanih po 25. 03. 2021

Vrsta potrdila	Dolžina ključev RSA	Dolžina ključev ECC
PK-NDP	2048	256
KZZ-NDP	2048	256
KZZ-ODP	2048	256
SSL-NDP	2048 ali več	256 ali več

### 6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

Vsi RSA ključni so generirani v skladu s standardom PKCS #1 V1.5.

### 6.1.7. Namen uporabe ključev

Namen uporabe ključev je označen v razširitvenem polju vsakega izdanega digitalnega potrdila v skladu s priporočilom RFC 3280.

Overiteljevi zasebni ključni se uporabljajo samo za podpisovanje digitalnih potrdil in registrov preklicanih potrdil. Overiteljevi javni ključni se uporabljajo samo za preverjanje veljavnosti

---

digitalnih potrdil in registrov preklicanih potrdil. Namen ključev je v overiteljevih digitalnih potrdilih je v skladu z RFC 3280 označen v razširitvenem polju *keyUsage* z bitoma *keyCertSign* in *cRLSign*.

Imetniški zasebni ključji se lahko uporabljajo za podpisovanje in dešifriranje. Imetniški javni ključji se lahko uporabljajo za preverjanje podpisa in šifriranje. Namen ključev v imetniških digitalnih potrdilih s ključji RSA je označen v razširitvenem polju *keyUsage* z bitoma *digitalSignature* in *keyEncipherment*. Namen ključev v imetniških digitalnih potrdilih s ključji ECC je označen v razširitvenem polju *keyUsage* z bitoma *digitalSignature* in *keyAgreement*.

Zasebni ključji strežnikov SSL se lahko uporabljajo za kriptografske operacije znotraj seje SLL. Namen ključev v digitalnih potrdilih strežnikov je v skladu z RFC3280 in splošno prakso označen v razširitvenem polju *keyUsage* z bitoma *digitalSignature* in *keyEncipherment*, ter v razširitvenem polju *extendedKeyUsage* z bitom *id-kp-serverAuth* (*TLS WWW server authentication*).

---

## **6.2. Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov**

### **6.2.1. Standardi za kriptografski modul**

Generiranje overiteljevih ključev in njihova uporaba se izvaja v strojnem varnostnem kriptografskem modulu, ki mora biti skladnem vsaj z enim od sledečih standardov:

- FIPS 140-2 Level 3 ali višji;
- CEN CWA 14167-2, 14167-3 ali 14167-4;
- ISO/IEC 15408 level EAL4 ali višji.

Generiranje imetniških ključev se izvaja v strojnem varnostnem kriptografskem modulu skladnem z Protection Profile for Secure Signature Creation Device (SSCD-PP) Type-1 nivoja EAL4+. Imetniški ključji se uporabljajo na pametni kartici skladni s specifikacijo Protection Profile for Secure Signature Creation Device (PP-SSCD) Type-2 nivoja EAL4+. Prenos ključev iz varnostnega kriptografskega modula na pametno kartico se izvaja v skladu s specifikacijo Protection Profile for Secure Signature Creation Device (PP-SSCD).

Generiranje zasebnih ključev strežnikov SSL se izvaja v strojnem, ali programskem kriptografskem modulu strežnika SSL.

### **6.2.2. Nadzor zasebnega ključa overitelja s strani pooblaščenih oseb**

V postopkih upravljanja s strojnem varnostnim kriptografskim modulom, ali zasebnih ključev overitelja je vedno potrebna prisotnost dveh oseb z pooblastili skrbnika kriptografskega modula, oziroma skrbnika overiteljevih ključev, ki izkažeta svojo istovetnost s pametno kartico kriptografskega modula in geslom kartice.

### **6.2.3. Odkrivanje zasebnega ključa**

Odkrivanje zasebnega ključa se ne uporablja.

### **6.2.4. Varnostno kopiranje zasebnih ključev**

Varnostna kopija overiteljevega zasebnega ključa se izdelava na strojnem kriptografskem modulu in se pred izvozom iz modula in zapisom kopije na medij v modulu šifrira z AES šifrirnim algoritmom. Dešifrirni ključ je zaščiten s ključji porazdeljenimi na pametnih karticah strojnega kriptografskega modula.

Overitelj ne hrani varnostnih kopij zasebnih ključev imetnikov.



---

### **6.2.5. Arhiviranje zasebnega ključa**

Glej 6.2.4 Varnostno kopiranje zasebnih ključev.

### **6.2.6. Prenos zasebnega ključa v kriptografski modul in iz njega**

Zasebni ključ overitelja se prenese v nov strojni kriptografski modul v prisotnosti vsaj dveh pooblaščenih oseb, ki se morata identificirati s pametno kartico strojnega kriptografskega modula in geslom kartice, ter odobriti prenos, oziroma uporabo an novem strojnem kriptografskem modulu.

### **6.2.7. Hranjenje overiteljevega zasebnega ključa v kriptografskem modulu**

Overiteljevi ključi se uporabljajo v strojnem kriptografskem modulu v katerem so bili tvorjeni, oziroma na katerem je bila odobrena in omogočena uporaba kod določeno v poglavju 6.2.6 Prenos zasebnega ključa v kriptografski modul in iz njega.

### **6.2.8. Postopek za aktiviranje zasebnega ključa**

Overiteljev zasebni ključ se aktivira ob vsakem zagonu programske opreme overitelja posebej z odobritvijo dveh pooblaščenih oseb v skladu s poglavjem 6.2.2 Nadzor zasebnega ključa overitelja s strani pooblaščenih oseb.

### **6.2.9. Postopek za deaktiviranje zasebnega ključa**

Overiteljev zasebni ključ se deaktivira in samodejno izbriše iz spomina strojnega kriptografskega modula ob zaustavitvi programske opreme overitelja.

### **6.2.10. Postopek za uničenje zasebnega ključa**

Po preteku obdobja veljavnosti overiteljevih ključev, oziroma uporabe, se uničijo vsi ključi, ki se nahajajo v kriptografskem modulu za upravljanje ključev overitelja, kar onemogoči uporabo overiteljevi ključev, kakor tudi njihovo povrnitev iz varnostne kopije.

### **6.2.11. Stopnja varnosti kriptografskih modulov**

Glej 6.2.1 Standardi za kriptografski modul.

---

## **6.3. Ostali vidiki upravljanja s pari ključev**

### **6.3.1. Arhiviranje javnega ključa**

Overitelj arhivira svoj javni ključ vsebovan v samo podpisanem potrdilu v okviru postopka arhiviranja ostalih podatkov (glej poglavje 5.5 Arhiviranje podatkov)

### **6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil**

Veljavnost javnih in zasebnih ključev overitelja je dvajset (20) let ali petindvajset (25) let in tri (3) mesece.

Veljavnost javnih in zasebnih ključev imetnikov KZZ je deset (10) let.

Veljavnost javnih in zasebnih ključev imetnikov PK je deset (10) let.

Veljavnost javnih in zasebnih ključev strežnikov SSL je deset (10) let.

---

## 6.4. Aktivacijski podatki

Upravitelj infrastrukture overitelja mora zagotoviti varno generiranje in uporabo aktivacijskih podatkov kot so:

- Gesla skrbnikov operacijskih sistemov;
- Gesla pametnih kartic strojnih kriptografskih modulov;
- Identifikacijske oznake, oziroma prstni odtisi (angl. hash code) medijev, oziroma podatkov na medijih za varnostno kopiranje in arhiviranje;
- Začetna gesla uporabniških računov na sistemih;
- Kode za dostop do varnostnih omar;
- Kode za kontrolo vstopa v prostore.

Izvajalec personalizacije kartic imetnikov mora zagotoviti varno generiranje in hranjenje gesel kartic, ter njihovo dostavo imetnikom.

### 6.4.1. Generiranje in instalacija aktivacijskih podatkov

Gesla imetniških pametnih kartic se varno ustvarijo v aplikativni programski opremi za personalizacijo kartic in shranijo v šifrirani obliki. Gesla PK se dostavijo imetnikom z ločeno priporočeno pošiljko. Gesla KZZ se dostavijo imetnikom na njihovo zahtevo. Gesla imetniških pametnih kartic se dešifrirajo v varnem okolju, ter tiskajo na slepe kuverte, ki se dostavijo imetniku s priporočeno pošiljko.

Gesla za dostop določijo, varujejo in upravljajo skrbniki strežnikov SSL.

### 6.4.2. Zaščita aktivacijskih podatkov

Gesla skrbnikov sistemov in gesla pametnih kartic strojnega kriptografskega modula se morajo hraniti v ločenih varnostnih ovojnicah. Ob vsakem dostopu do gesel in PIN kod shranjenih v ovojnicah se mora preveriti in zabeležiti upravičenost dostopa.

Gesla imetniških pametnih kartic se hranijo v šifrirani obliki v bazi sistema za personalizacijo kartic. Dešifrirni ključ se hrani in uporablja na strojnem kriptografskem modulu.

Gesla za zaščito zasebnih ključev strežnikov SSL morajo biti v skladu s priporočili dobre prakse. Minimalna zahteva je, da vsebujejo velike črke (vsaj eno), male črke (vsaj eno), številke (vsaj eno) in da niso krajša od 8 znakov. V primeru, da programska oprema strežnika SSL ne omogoča uporabe gesel za zaščito zasebnega ključa, morajo biti strežniki ustrezno fizično in logično varovani, tako da se prepreči nepooblaščen dostop. V primeru da se v okviru izdelave varnostne kopije strežnika kopirajo tudi zasebni ključa, morajo biti uporabljeni podatkovni mediji ustrezno zaščiteni, da se prepreči nepooblaščen uporaba zasebnega ključa.

### 6.4.3. Drugi vidiki aktivacijskih podatkov

Gesla skrbnikov sistemov, ter gesla pametnih kartic strojnega kriptografskega modula se morajo menjati vsaj enkrat na dve leti in ob vsaki menjavi osebe zadolžene za izvajanje funkcije.

Kode varnostnih omar, kjer je to izvedljivo, se morajo menjati vsaj vsakih 5 let.

---

## 6.5. Varnostne zahteve za računalnike

### 6.5.1. Specifične tehnične varnostne zahteve za računalnike

Specifične tehnične varnostne zahteve za računalnike niso predpisane.

### 6.5.2. Nivo varnostne zaščite računalnikov

Nivo varnostne zaščite računalnikov ni predpisan.

---

## 6.6. Tehnični nadzor življenjskega cikla overitelja

### 6.6.1. Nadzor razvoja sistema

Strojna oprema, operacijski sistemi ter programska oprema overitelja so komercialni proizvodi.

### 6.6.2. Upravljanje varnosti

Izdajatelj evidentira postopke pregledov, sprememb nastavitev in nadgradnje za vse komponente sistema.

Operativno osebje izdajatelja periodično in ob vsaki namestitvi nove verzije ali popravka preverja celovitost operacijskega sistema in aplikativne programske opreme.

Zunanji izvajalec, ki je dobavil informacijsko in komunikacijsko opremo in izvedel začetno inštalacijo, jamči, da oprema:

Izdajatelj evidentira postopke pregledov, sprememb nastavitev in nadgradnje za vse komponente sistema.

Operativno osebje izdajatelja periodično in ob vsaki namestitvi nove verzije ali popravka preverja celovitost operacijskega sistema in aplikativne programske opreme.

Zunanji izvajalec, ki je dobavil informacijsko in komunikacijsko opremo in izvedel začetno inštalacijo, jamči, da:

- oprema dejansko izvira od proizvajalca;
- v obdobju med proizvodnjo in inštalacijo ni prišlo do spreminjanja in posegov v opremo;
- je namestil opremo prave verzije in s predvidenim namenom uporabe.

Programska koda programske opreme overitelja je zaščitena na način, da se da preveriti njen izvor in celovitost. Programska koda programske opreme overitelja je zaščitena na način, da se da preveriti njen izvor in celovitost.

---

## 6.7. Varnostne kontrole na ravni računalniškega omrežja

Overiteljeva infrastruktura sistemi za personalizacijo kartic so fizično ločeni od ostalih omrežij. Overiteljeva infrastruktura je dodatno ločena od ostalih mrežnih segmentov, pri čemer je varnost na mrežnem nivoju zagotovljena z:

- delitvijo sistemov in naprav v ločene komunikacijske segmente, glede na nivo varnostne občutljivosti podatkov, ki se obdelujejo na posameznem sistemu in glede na potrebo dostopnosti;
- uporabo požarnih zidov med posameznimi komunikacijskimi segmenti.

---

## 7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

---

### 7.1. Profil digitalnih potrdil

#### 7.1.1. Verzija digitalnih potrdil

ZZZS-CA izdaja X.509 v3 digitalna potrdila skladna z RFC 3280. Digitalna potrdila vsebujejo naslednja osnovna polja:

X.509 polje	Opis
<i>signature</i>	Overiteljev podpis

<i>issuer</i>	Edinstveno razločevalno ime overitelja
<i>validity</i>	Datum aktiviranja in poteka veljavnosti potrdila
<i>subject</i>	Edinstveno razločevalno ime imetnika potrdila
<i>subjectPublicKeyInformation</i>	Oznaka algoritma ključa
<i>version</i>	Različica potrdila X.509
<i>serialNumber</i>	Edinstvena serijska številka potrdila

## 7.1.2. Razširitvena polja

Razširitvena polja so namenjena uporabi dodatnih atributov v X.509 v3 potrdilih. Standardna razširitvena polja so definirana v skladu z RFC 3280, ki dovoljuje tudi uporabo lastnih razširitvenih polj za potrebe overiteljev. Dodana posebna razširitvena polja za potrebe Zavoda so definirana v 7.1.2.2.

### 7.1.2.1 Standardna X.509 v3 razširitvena polja

Digitalna potrdila, ki jih izdaja ZZS-CA vsebujejo sledeča standardna X.509 v3 razširitvena polja:

X.509 razširitveno polje	Opis
<i>authorityKeyIdentifier</i>	Zgoščena vrednost overiteljevega javnega ključa
<i>subjectKeyIdentifier</i>	Zgoščena vrednost imetnikovega javnega ključa
<i>keyUsage</i>	Namen uporabe javnega ključa, kot opredeljeno v 6.1.7 Namen uporabe ključev
<i>privateKeyUsagePeriod</i>	Veljavnost zasebnega ključa, kot opredeljeno v 6.3.2 Obdobje veljavnosti ključev in digitalnih potrdil
<i>certificatePolicies:</i>	Overiteljeva identifikacijska oznaka politike potrdila, v skladu s poglavjem 1.2 Naziv dokumenta in identifikacijska oznaka in 2.2 Objave informacij o digitalnih potrdilih
<i>CertPolicyID</i>	
<i>CPS URI</i>	
<i>CRLDistributionPoints</i>	Naslovi na katerih je objavljen register preklicanih potrdil, kot je določen v 2.2 Objave informacij o digitalnih potrdilih
<i>basicConstraints</i>	Osnovne omejitve
<i>extKeyUsage</i>	Namen uporabe potrdil strežnikov SSL, kot opredeljeno v 6.1.7 Namen uporabe ključev

Razširitveni polji *keyUsage* in *basicConstraints* sta v vseh izdanih potrdilih označeni kot kritični.

### 7.1.2.2 Razširitvena polja za potrebe Zavoda

Digitalna potrdila PK-NDP, KZZ-NDP in KZZ-ODP, ki jih izdaja ZZS-CA vsebujejo sledeča razširitvena polja za potrebe Zavoda:

Identifikacijska oznaka	Oblika zapisa	Ime podatka vsebovanega v razširitvenem polju
1.3.6.1.4.1.29715.1.1.1	IA5STRING	ZZS številka
1.3.6.1.4.1.29715.1.1.2	IA5STRING	Številka izvoda KZZ/PK
1.3.6.1.4.1.29715.1.1.3	UTF8STRING	Priimek 1
1.3.6.1.4.1.29715.1.1.4	UTF8STRING	Vezaj priimek
1.3.6.1.4.1.29715.1.1.5	UTF8STRING	Priimek 2
1.3.6.1.4.1.29715.1.1.6	UTF8STRING	Ime 1

Identifikacijska oznaka	Oblika zapisa	Ime podatka vsebovanega v razširitvenem polju
1.3.6.1.4.1.29715.1.1.7	UTF8STRING	Vezaj ime
1.3.6.1.4.1.29715.1.1.8	UTF8STRING	Ime 2
1.3.6.1.4.1.29715.1.1.9	IA5STRING	Datum rojstva
1.3.6.1.4.1.29715.1.1.10	IA5STRING	Spol
1.3.6.1.4.1.29715.1.1.11	IA5STRING	IVZ številka imetnika
1.3.6.1.4.1.29715.1.1.12	IA5STRING	EMŠO imetnika
1.3.6.1.4.1.29715.1.1.13	IA5STRING	Identifikacijska št. nosilca (OE)
1.3.6.1.4.1.29715.1.1.14	IA5STRING	Številka izdajatelja kartice
1.3.6.1.4.1.29715.1.1.15	IA5STRING	Vrsta digitalnega potrdila*
1.3.6.1.4.1.15284.10.2.1	IA5STRING	Davčna številka imetnika

\* polje vrsta digitalnega potrdila lahko vsebuje PK-NDP, KZZ-NDP, KZZ-ODP, --, SSL-NDP

### 7.1.3. Identifikacijske oznake algoritmov

Digitalna potrdila, ki jih izdaja ZZZS-CA, vsebujejo nesimetrične kriptografske algoritme s sledečimi identifikacijskimi oznakami:

Algoritem	Identifikacijska oznaka
RSA Encryption	1.2.840.113549.1.1.1
RSA with SHA-1signature	1.2.840.113549.1.1.5
RSA with SHA-256 signature	1.2.840.113549.1.1.11
ECDSA with SHA-384 signature	1.2.840.10045.4.3.3
NIST P-256 prime256v1  secp256r1	1.2.840.10045.3.1.7
NIST P-384 secp384r1	1.3.132.0.34

### 7.1.4. Oblike imen

Kot opredeljeno v poglavju 3.1.1 Vrste imen.

### 7.1.5. Omejitve imen

Omejitve za razločevalna imena so opisana v poglavju 3.1.2 Potreba po smiselnosti imen.

### 7.1.6. Identifikacijska oznaka politik

Vsako potrdilo vsebuje eno ali več identifikacijskih oznak politik. Overitelj uporablja polje »certificatePolicies« za razločevanje med tipi digitalnih potrdil, ki jih izdaja.

### 7.1.7. Način uporabe razširitvenega polja *policyConstraints* za omejitve uporabe politik

Način uporabe razširitvenega polja *policyConstraints* za omejitve uporabe politik se ne uporablja.

### 7.1.8. Specifični podatki o politiki (angl. *Policy Qualifiers extension*)

Specifični podatki o politiki se ne uporabljajo.

---

### 7.1.9. Procesiranje oznake kritičnosti razširitvenih polj

Aplikacije morajo procesirati razširitvena polja digitalnega potrdila, označena kot kritična, v skladu s priporočili RFC 3280.

---

## 7.2. Profil registrov preklicanih potrdil

### 7.2.1. Verzija registrov preklicanih potrdil

Registri preklicanih potrdil morajo so v skladu s priporočili RFC 3280: Certificate and CRL Profile, verzija 2.

Registri preklicanih potrdil vsebujejo naslednja osnovna polja:

X.509 polje	Opis
<i>Version</i>	Verzija profila
<i>Signature</i>	Overiteljev podpis
<i>Issuer</i>	Edinstveno razločevalno ime overitelja
<i>thisUpdate</i>	Čas izdaje registra
<i>nextUpdate</i>	Čas izdaje naslednjega registra
<i>revokedCertificate</i>	Serijske številke preklicanih potrdil

### 7.2.2. Razširitvena polja registrov preklicanih potrdil

Overitelj uporablja X.509 Version 2 CRL razširitvena polja v skladu s priporočili RFC 3280, navedena v naslednji tabeli:

X.509 polje	Opis
<i>CRLNumber</i>	Serijska številka registra
<i>reasonCode</i>	Koda razloga za preklic : (0) Unspecified (1) Key compromise (3) Affiliation change (4) Superseded (5) Cessation of operation
<i>invalidityDate</i>	Čas kompromitiranja ključa

---

## 7.3. Profil OSCP

Profil OSCP se ne uporablja.

## 8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

---

### 8.1. Pogostost ali okoliščine izvajanja nadzornih pregledov

Zavod izvaja nadzor delovanja overitelja enkrat letno v skladu s pogoji določenimi v pogodbi z izvajalcem.

---

### 8.2. Pogoji za izvajalca nadzora

Zavod določi izvajalca nadzora po svoji presoji.

---

### **8.3. Relacija med izvajalcem nadzora in overiteljem**

#### **8.4. Področja nadzora**

V obsegu posameznega nadzornega pregleda, se preverja vsaj eno od področij:

- Generiranje zasebnih ključi imetnikov kartic.
- Generiranje PIN-ov.
- Hranjenje PIN-ov za KZZ-ODP.
- Postopek izdaje digitalnih potrdil.
- Postopek preklica in storitev objavljanja statusa potrdil.
- Varovanje zasebnega ključa overitelja.
- Dostop do varnih prostorov kjer je nameščena infrastruktura overitelja.

---

#### **8.5. Postopki po opravljenem nadzornem pregledu**

V primeru ugotovljenih nepravilnosti, mora upravitelj infrastrukture overitelja pripraviti načrt za odpravo pomanjkljivosti in po izvedbi poročilo o odpravi pomanjkljivosti. Načrt in poročilo mora posredovati inšpektorju, ki je opravil pregled in Zavodu.

---

#### **8.6. Prejemniki in objava ugotovitev**

Zapisnik o opravljenem nadzornem pregledu je vročen overitelju in Zavodu. Zavod objavi povzetek ugotovitev na spletnem naslovu navedenem v poglavju 2.1.

---

## **9. OSTALE POSLOVNE IN PRAVNE ZADEVE**

---

### **9.1. Finančna odgovornost**

Finančna odgovornost upravitelja infrastruktur overitelja do Zavoda je opredeljena v pogodbi med izvajalcem personalizacije kartic in Zavodom.

Zavod ne odgovarja za nikakršno škodo katerekoli vrste, ki bi utegnila nastati zaradi uporabe ali nezmožnosti uporabe digitalnih potrdil na KZZ in PK, ali digitalnih potrdil strežnikov SSL.

---

### **9.2. Zaupnost poslovnih informacij**

Zaupnost poslovnih informacij med overiteljem in Zavodom je opredeljena v pogodbi med izvajalcem personalizacije kartic in upravitelju politike overitelja na Zavodom.

---

### **9.3. Zaupnost osebnih podatkov**

Zavod izdaja digitalna potrdila samo imetnikom KZZ in PK na osnovi obstoječih podatkov o zavarovanih osebah in izvajalcih zdravstvenih storitev v bazi Zavoda in ne zbira, ali hrani dodatnih podatkov za potrebe izdaje in upravljanja digitalnih potrdil.

Zaupnost osebnih podatkov je opredeljena v pogodbi med Zavodom in izvajalcem personalizacije kartic.

---

### **9.4. Zaščita intelektualne lastnine**

Zaščita intelektualne lastnine je opredeljena v pogodbi med Zavodom in izvajalcem personalizacije kartic.

---

## **9.5. Odgovornosti in jamstva**

### **9.5.1. Odgovornosti in jamstva overitelja**

Overitelj jamči, da izdaja digitalna potrdila, izvaja ostale postopke upravljanja digitalnih potrdil, ter upravlja infrastrukturo overitelja v skladu z določili Politike ZZZS-CA, ter veljavne zakonodaje. Overitelj je odgovoren za skladnost tudi kadar določene naloge izvaja zunanji izvajalec.

Overitelj ZZZS-CA:

- zagotavlja, da so podatki o imetniku iz izdajatelju vsebovani v digitalnem potrdilu točni,
- preveri verodostojnost podatkov o imetniku preden izda digitalno potrdilo,
- zagotavlja, da so informacije objavljene v repozitorijih točne in celovite,
- zagotavlja dostop do objavljenih informacij v skladu z določili Politike ZZZS-CA,
- izvaja preklic digitalnih potrdil, po prejemu veljavnega zahtevka, v skladu z določili Politike ZZZS-CA,
- pravočasno izda in objavi register preklicanih potrdil.

### **9.5.2. Odgovornost in jamstva imetnikov digitalnih potrdil**

Imetnik je poleg izpolnjevanja obveznosti, ki izhajajo iz Pravilnika o KZZ, odgovoren da:

- varuje svoje zasebne ključe in kartico, ter upošteva vse ukrepe, da se prepreči izguba, razkritje, sprememba ali nepooblaščen uporaba;
- varuje PIN za uporabo kartice,
- uporablja digitalna potrdila izključno skladno z določili poglavja 1.4 Politike ZZZS-CA,
- nemudoma obvesti overitelja o vsakršni nepravilnosti, ali spremembi podatkov vsebovanih v digitalnem potrdilu,
- nemudoma obvesti o zlorabi, ali sumu zlorabe oziroma razkritja zasebnega ključa,
- nemudoma obvesti overitelja o vsaki zlorabi, ali sumu zlorabe katerega koli digitalnega potrdila, ki ga je izdal overitelj ZZZS-CA.

### **9.5.3. Odgovornost in jamstva tretjih oseb**

Tretje osebe, ki uporabljajo digitalna potrdila overitelja ZZZS-CA v svojih sistemih in aplikacijah, morajo upoštevati vse zahteve Politike ZZZS-CA, ter prevzemajo polno odgovornost in jamstva do imetnikov digitalnih potrdil.

---

## **9.6. Zanikanje odgovornosti overitelja**

Zavod ne odgovarja za nikakršno škodo katerekoli vrste, ki bi utegnila nastati zaradi uporabe ali nezmožnosti uporabe digitalnih potrdil na KZZ in PK.

---

## **9.7. Omejitve odgovornosti overitelja**

V primeru nepravilnega delovanja kartice, jo mora imetnik vrniti Zavodu s priporočeno pošiljko, ali predati osebno. V primeru, da je za nepravilno delovanje kartice kriva tehnična napaka, bo izdajatelj kartico brezplačno zamenjal.

Glej tudi 9.6.

---

## **9.8. Poravnava škode**

Glej 9.1.



---

## **9.9. Začetek in prenehanje veljavnosti**

### **9.9.1. Začetek veljavnosti**

Politika overitelja digitalnih potrdil ZZZS-CA začne veljati naslednji dan po podpisu.

### **9.9.2. Prenehanje veljavnosti**

Veljavnost Politike overitelja digitalnih potrdil ZZZS-CA ni časovna omejena in velja do uveljavitve nove verzije, oziroma do prenehanja delovanja overitelja.

### **9.9.3. Učinek in posledice prenehanja veljavnosti**

Po prenehanju veljavnosti Politike overitelja digitalnih potrdil ZZZS-CA zaradi objave nove verzije imetniki praviloma uporabljajo obstoječa potrdila v skladu z določili Politike overitelja digitalnih potrdil ZZZS-CA, po kateri so bila izdana. V primeru, da zaradi spremenjenih okoliščin to ne bo več mogoče, bo overitelj ob izdaji nove verzije Politike overitelja digitalnih potrdil ZZZS-CA o tem obvestil imetnike.

---

## **9.10. Obvestila in komuniciranje z udeleženci**

Obvestila imetnikom so objavljena na spletni strani <https://ca.zzs.si>, če ni drugače določeno.

---

## **9.11. Spreminjanje dokumenta**

### **9.11.1. Postopek uveljavitve sprememb**

Upravitelj politike overitelja ZZZS-CA pripravi spremembe in jih predloži odgovorni osebi Zavoda (glej poglavje 1.5) v odobritev in podpis.

### **9.11.2. Postopek obveščanja in rok za pripombe**

Imetniki bodo o spremembah obveščeni vsaj osem dni pred uveljavitvijo sprememb Politike overitelja digitalnih potrdil ZZZS-CA na način, določen v poglavju 9.10. Izjema so uredniški in tipografski popravki, ki smiselno ne vplivajo na vsebino Politike overitelja digitalnih potrdil ZZZS-CA.

### **9.11.3. Spremembe, ki zahtevajo novo identifikacijsko oznako politike**

Upravitelj politike overitelja ZZZS-CA po lastni presoji odloči, ali so spremembe vsebine Politike overitelja digitalnih potrdil ZZZS-CA takšne, da zahtevajo objavo nove Politike overitelja digitalnih potrdil ZZZS-CA z novo identifikacijsko oznako.

---

## **9.12. Reševanje sporov**

Pogodbeni stranki si bosta prizadevali vse morebitne spore rešiti sporazumno, izhajajoč iz načela vestnosti in poštenja.

Če do sporazumne rešitve spora ne pride, je za vse spore, ki izvirajo iz tega dogovora, ali so v zvezi z njo, pristojno sodišče v Ljubljani.

---

## **9.13. Veljavna zakonodaja**

Overitelj ZZZS-CA deluje v skladu z zakonodajo Republike Slovenije navedeno v poglavju 9.15. Skladnost s pravnimi akti.

---

## 9.14. Skladnost s pravnimi akti

Overitelj ZZS-CA deluje skladno z:

- Zakonom o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 s spremembami);
- Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00 s spremembami);
- Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 86/04); in
- ostalimi predpisi, ki veljajo na območju RS.

---

## 9.15. Splošne določbe

### 9.15.1. Ostali obvezujoči dokumenti

Navodilo o profesionalni kartici

Pravila OZZ

Pravilnik o KZZ

Pravilnik o zavarovanju osebnih podatkov

### 9.15.2. Prenos pravic in obveznosti

Pravica uporabe KZZ, PK in digitalnih potrdil ni prenosljiva.

### 9.15.3. Spremembe okoliščin delovanja

Če postane zaradi spremenjenih okoliščin delovanja ali spremembe zakonodaje del pričujočega dokumenta nepravilen ali neveljaven, ostanejo ostali deli veljavni vse dokler se ne objavi sprememba. Postopek uveljavitve spremembe je opisan v poglavju 9.11.1 Postopek uveljavitve sprememb.

### 9.15.4. Uveljavljanje (povračila stroškov v primeru sporov in izjeme)

Zahtevki povračila stroškov v primeru sporov so obravnavajo v skladu z veljavnimi predpisi na območju Republike Slovenije.

### 9.15.5. Višje sile

Višja sila so izredne nepremagljive in nepredvidljive okoliščine, ki nastopijo po sklenitvi pogodbe in so zunaj volje ali sfere pogodbenih strank (v celoti tuje pogodbenim strankam), kot na primer požar, potres, druge elementarne nezgode in podobno.

Za višjo silo štejejo tudi predpisi, posamični akti in dejanja ter drugi ukrepi organov Evropske skupnosti, ki izpolnjujejo pogoje iz prejšnjega odstavka. Za višjo silo štejejo tudi predpisi, posamični akti ali ukrepi organov RS, ki pomenijo vključitev obveznih določb predpisov Evropske skupnosti v pravni red Republike Slovenije ali ki pomenijo izvrševanje neposredno uporabljivih pravil prava te skupnosti, ki izpolnjujejo pogoje za višjo silo iz prejšnjega odstavka.

Nobena stranka ne more uveljavljati zahtevkov, ki ji po tem dokumentu, pogodbi ali po zakonu pripadajo zaradi kršitve druge stranke, če je do ravnanja v nasprotju s pogodbo prišlo zaradi višje sile.

Če je zaradi višje sile začasno onemogočeno izvrševanje kakšne obveznosti po tem dokument, ali dogovoru, se rok za izvršitev ustrezno podaljša.

---

## **9.16. Ostale določbe**

Oblika in vsebina dokumenta Politika overitelja digitalnih potrdil ZZS-CA je usklajena z RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

---

## 10. PRILOGE

---

### 10.1. Transformacija znakov za zapis imena in priimka v digitalnih potrdilih (polje CN)

#### 10.2. Osnovni nabor - znaki slovenske abecede:

A, B, C, Č, D, E, F, G, H, I, J, K, L, M, N, O, P, R, S, Š, T, U, V, Z, Ž

a, b, c, č, d, e, f, g, h, i, j, k, l, m, n, o, p, r, s, š, t, u, v, z, ž

---

### 10.3. Dodatni nabor – znaki, ki se pogosto uporabljajo v lastnoimenskem besedju

Q, W, X, Y, Ä, Ö, Ü, Č, Đ

q, w, x, y, ä, ö, ü, č, đ

---

### 10.4. Nabor znakov s pravorečnimi znamenji

Ostrivec: á, é, í, ó, ú, Á, É, Í, Ó, Ú

Krativec: à, è, ì, ò, ù, À, È, Ì, Ò, Ù

Strešica: ê, ô, Ê, Ô

Dvojni ostrivec: ő, ű, Ő, Ű

---

## 10.5. Transformacija posebnih znakov

Č = C

Š = S

Ž = Z

Ä = AE

Ö = OE

Ü = UE

Ć = C

Đ = D

Á = A

É = E

Í = I

Ó = O

Ú = U

À = A

È = E

Ì = I

Ò = O

Ù = U

Ê = E

Ô = O

Õ = O

Ŭ = U

---

## 10.6. Pojmi in kratice

Kratice

Kratice	Opis
CRL	Register preklicanih potrdil (angl.: Certificate Revocation List).
FIPS	Standardi za informacijske tehnologije, ki so v uporabi v ameriških zveznih institucijah. Izdaja jih ameriški nacionalni inštitut za standarde in tehnologijo (angl.: Federal Information Processing Standards).
FIPS 140-2	Serija standardov FIPS za kriptografske module.
IETF	Združenje strokovnjakov s področja Internetnih tehnologij. Izdelujejo serije priporočil (angl.: Internet Engineering Task Force).

Kratica	Opis
ISO	Mednarodna organizacija za standardizacijo (angl.: International Standardization Organization).
ITU-T	Mednarodna organizacija za standardizacijo na področju telekomunikacij (angl.: International Telecommunications Union - Telecommunication Standardization Sector).
OA	Upravitelj infrastrukture overitelja (angl. Operations Authority)
PKCS	Priporočila podjetja RSA Security za uporabo asimetričnih kriptografskih algoritmov (angl.: Public Key Cryptographic Standards).
PKCS#1	Osnovna pravila za formatiranje podatkov ob implemetaciji RSA funkcij. Predpisuje, kako se izračuna digitalni podpis, kako se formatirajo podatki, ki se podpisujejo in format podpisa. Predpisuje tudi sintakso javnega in zasebnega RSA ključa.
PMA	Upravitelj politike overitelja (angl. Policy Management Authority)
RFC	Priporočila, ki jih izdaja IETF.
RFC 3647	Priporočilo, ki določa elemente, ki naj bodo zajeti v politiki overitelja (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). veljavno od novembra 2003 (je nadomestil RFC 2527).
RSA	Eden prvih nesimetričnih kriptografskih sistemov, patentiran leta 1983, imenovan po odkriteljih: Rivest, Shamir in Adelman.
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/2004).
ZVOP-1	Zakon o varstvu osebnih podatkov (Uradni list RS, št.86/2004)
ZTP	Zakon o tajnih podatkih (Uradni list rs, št. 135/03 – UPB1)

#### Pojmi

Izraz	Definicija
Digitalno potrdilo	Je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.
Elektronski podpis	Je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.
Elektronsko sporočilo	Je niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto.

Izraz	Definicija
Imenik	Je podatkovna struktura, ki vsebuje objekte z določenimi lastnosti in pripadajočimi vrednostmi. Imenik, ki vsebuje digitalna potrdila je običajno v skladu s standardom X.500 oziroma razširjenim standardom X.509 ver.3.
Imetnik potrdila	Je določena fizična oseba, navedena v digitalnem potrdilu v polju »Subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, vsebovanem v digitalnem potrdilu oziroma pooblaščen oseba za uporabo potrdila za splošne nazive ter poveljniške dolžnosti v Slovenski vojski.
Informacijski sistem	Je skupek naprav in postopkov, ki omogočajo obdelavo informacij oziroma nudijo informacijske storitve. Združuje računalniško strojno in programsko opremo, računalniške nosilce podatkov, podatkovne zbirke in druge naprave ter identifikacijske, avtorizacijske, upravljalne in nadzorne postopke v funkcionalno celoto.
Pravila delovanja (angl. Practice Statement)	Po Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje vsebuje javni del notranjih pravil overitelja "bistvene določbe, ki vplivajo na odnos med overiteljem in imetniki od njega izdanih potrdil ter tretjimi osebami, ki se zanašajo na ta potrdila". Javni del notranjih pravil overitelja in Politika overitelja digitalnih potrdil sta v konkretnem primeru overitelja na MO isti dokument. [RFC 3647]
Komunikacijski sistem	Je skupek naprav in postopkov, ki omogočajo prenos informacij. Primeri takih sistemov so telekomunikacijski sistemi in računalniška omrežja.
Komunikacijsko informacijski sistem	Je skupen izraz za komunikacijski in informacijski sistem.
Naslovnik elektronskega sporočila	Je oseba, ki ji je pošiljatelj namenil elektronsko sporočilo.
Ogrožanje	Je dejanska ali domnevna možnost razkritja tajnih podatkov, izgube celovitosti ali razpoložljivosti podatkov.
Oprema za elektronsko podpisovanje	Je strojna ali programska oprema ali njune specifične sestavine, ki jo overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov.
Overitelj digitalnih potrdil	Je fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem javnih ključev.
Podatki v elektronski obliki	So podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način.
Politika	Je nabor pravil, ki posledično definira zahteve in pravila v določeni skupini uporabnikov in/ali za določen nabor aplikacij s skupnimi varnostnimi zahtevami [RFC 3647, ETSI].
Pošiljatelj elektronskega sporočila	Je oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila.
Prejemnik elektronskega sporočila	Je oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila.

<b>Izraz</b>	<b>Definicija</b>
Prijavna služba	Je služba oziroma organizacija, ki po pooblastilu izdajatelja kartic sprejema vloge in preverja istovetnosti bodočih imetnikov.
Repozitorij	Je skladišče oziroma odlagališče objektov, vključno z digitalnimi potrdili. Repozitorij sestavljata imenik in spletne strani.
Sredstvo za preverjanje elektronskega podpisa	Je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa.
Sredstvo za elektronsko podpisovanje	Je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa.
Sredstvo za varno elektronsko podpisovanje	Je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena ZEPEP.
Tretja oseba	Je subjekt, ki ni aktivno udeležen v storitev, vendar zaupa izvajalcu in rezultatu storitve.
Uporabnik	Imetnik digitalnega potrdila.
Vloge	So obrazci za pridobitev, preklic, zamenjavo, nadomestitev, podaljšanje kartice.
Zloraba	Je razkritje zaupnega podatka, izguba celovitosti ali razpoložljivosti podatka.
Zunanji izvajalec	Je fizična ali pravna oseba, ki opravlja dela po pogodbi.
Selektivno omejevanje dostopa	Ločevanje dostopa glede na upravičen interes.
Tajnost	Zaupnost v smislu ZTP.
Tajni podatek	Dejstvo ali sredstvo iz delovnega področja organa, ki se nanaša na javno varnost, obrambne zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v ZTP zaščititi pred nepoklicanimi osebami, in ki je v skladu s ZTP določeno in označeno kot tajno.



---

Pripravil: \_\_\_\_\_

Ljubljana, 25. 3. 2021

Številka dokumenta: \_\_\_\_\_

Zavod za zdravstveno zavarovanje Slovenije

---

Generalna direktorica  
doc.dr. Tatjana Mlakar