



AMANDMA k POLITIKI SIGEN-CA

za kvalificirana digitalna potrdila za poslovne subjekte

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 18. februarja 2019

verzija: 1 / 7.0

Podatki o politiki:

CP_{Name}: SIGEN-CA-1

- **Politika za spletna kvalificirana digitalna potrdila za zaposlene**
CPOID: 1.3.6.1.4.1.6105.2.1.1.5
- **Politika za posebna kvalificirana digitalna potrdila za zaposlene**
CPOID: 1.3.6.1.4.1.6105.2.1.2.5
- **Politika za spletna kvalificirana digitalna potrdila za splošne nazive**
CPOID: 1.3.6.1.4.1.6105.2.1.3.5
- **Politika za posebna kvalificirana digitalna potrdila za splošne nazive**
CPOID: 1.3.6.1.4.1.6105.2.1.4.5
- **Politika za spletna normalizirana digitalna potrdila za informacijske sisteme**
CPOID: 1.3.6.1.4.1.6105.2.1.5.5
- **Politika za spletna normalizirana digitalna potrdila za podpis kode**
CPOID: 1.3.6.1.4.1.6105.2.1.6.5
- **Politika za spletna kvalificirana digitalna potrdila za avtentikacijo spletišč**
CPOID: 1.3.6.1.4.1.6105.2.1.7.5
- **Politika za spletna kvalificirana digitalna potrdila za elektronski žig**
CPOID: 1.3.6.1.4.1.6105.2.1.8.5

veljavnost: od 28. maja 2018

verzija: 7.0



Zgodovina politik

Izdaje politik delovanja SIGEN-CA	
amandma k politiki verzije 7.0, veljavnost: od 18. februarja 2019	
Amandma k Politiki SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte št. 1 / 7.0	<i>Sprememba z amandmajem št. 1 / 7.0:</i> <ul style="list-style-type: none">• pri potrdilih za elektronske žige je spremenjen naziv, ki je vključen v razločevalno ime.
verzija: 7.0, veljavnost: od 28. maja 2018	
<ul style="list-style-type: none">• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.5• Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.5• Politika za spletna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.5• Politika za posebna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.5• Politika za spletna normalizirana digitalna potrdila za informacijske sisteme, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.5• Politika za spletna normalizirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.5• Politika za spletna kvalificirana digitalna potrdila za avtentikacijo spletišč, CP_{OID}: 1.3.6.1.4.1.6105.2.1.7.5• Politika za spletna kvalificirana digitalna potrdila za elektronski žig, CP_{OID}: 1.3.6.1.4.1.6105.2.1.8.5 CP _{Name} : SIGEN-CA-1	<i>Spremembe z verzijo 7.0:</i> <ul style="list-style-type: none">• normalizirana potrdila za strežnike so preimenovana v kvalificirana potrdila za avtentikacijo spletišč,• veljavnost potrdil za avtentikacijo spletišč je 27 mesecev,• spremenjeno je razločevalno ime potrdil za avtentikacijo spletišč,• uvedena so kvalificirana potrdila za elektronski žig in normalizirana potrdila za informacijske sisteme,• v potrdilih so navedene oznake politik, kot so določene z novimi standardi,• uvedena je Krovna politika SI-TRUST za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja SI-TRUST, zato se pričujoča politika v določenih točkah sklicuje nanjo,• izrazi in okrajšave so usklajeni z veljavno zakonodajo.
verzija: 6.0, veljavnost: od 6. junija 2016	
<ul style="list-style-type: none">• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.4• Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.4• Politika za spletna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.4• Politika za posebna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.4• Politika za spletna normalizirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.4• Politika za spletna normalizirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.4 CP _{Name} : SIGEN-CA-1	<i>Spremembe z verzijo 6.0:</i> <ul style="list-style-type: none">• tvorjeno je bilo drugo lastno digitalno potrdilo izdajatelja SIGEN-CA z zasebnim ključem dolžine 3072 bitov, ki se hrani na strojni opremi za varno shranjevanje zasebnih ključev,• v potrdilu izdajatelja SIGEN-CA in vseh potrdilih imetnikov se uporablja zagostitveni algoritem SHA-256,• spremenjeno je razločevalno ime digitalnega potrdila izdajatelja SIGEN-CA,• spremenjena so razločevalna imena potrdil imetnikov, ki lahko vključujejo znake iz kodne tabele UTF-8,• podprto je sprotno preverjanje statusa potrdil po protokolu OCSP,• izdajatelj SIGEN-CA je priznan s strani korenkega izdajatelja SI-TRUST Root,• pri potrdilih za zaposlene in splošne nazive je v polju uporaba ključa (angl. Key Usage) dodana vrednost ContentCommitment,• potrdila za strežnike in podpis kode so preimenovana v normalizirana potrdila.
verzija: 5.0, veljavnost: od 7. novembra 2015	



<ul style="list-style-type: none">• Politika za spletna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.3• Politika za posebna kvalificirana digitalna potrdila za zaposlene, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.3• Politika za spletna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.3• Politika za posebna kvalificirana digitalna potrdila za splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.3• Politika za spletna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.3• Politika za spletna kvalificirana digitalna potrdila za podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.3 <p>CP_{Name}: SIGEN-CA-1</p>	<p><i>Spremembe z verzijo 5.0:</i></p> <ul style="list-style-type: none">• uporaba novega naziva za overitelja na Ministrstvu za notranje zadeve, po novem je to »Državni center za storitve zaupanja«,• pri spletnih potrdilih za strežnike se uporablja zgostitveni algoritem SHA-256,• veljavnost spletnih potrdil za strežnike je 3 leta,• veljavnost potrdila za šifriranje in zasebnega ključa za podpisovanje pri posebnih potrdilih za zaposlene in splošne nazive je 5 let,• omogočeno je izdajanje spletnih potrdil za strežnike z več imeni strežnika,• ukinjeno je izdajanje posebnih potrdil za strežnike,• novi kontaktni podatki izdajatelja SIGEN-CA.
amandma k politiki verzije 4.0, veljavnost: od 21. marca 2014	
<p>Amandma k Politiki SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte št. 2 / 4.0</p>	<p><i>Sprememba z amandmajem št. 2 / 4.0:</i></p> <ul style="list-style-type: none">• uporaba novega naziva za overitelja na Ministrstvu za pravosodje in javno upravo, po novem je to »Overitelj na Ministrstvu za notranje zadeve«.
amandma k politiki verzije 4.0, veljavnost: od 23. julija 2012	
<p>Amandma k Politiki SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte št. 1 / 4.0</p>	<p><i>Sprememba z amandmajem št. 1 / 4.0:</i></p> <ul style="list-style-type: none">• uporaba novega naziva za overitelja na Ministrstvu za javno upravo, po novem je to »Overitelj na Ministrstvu za pravosodje in javno upravo«.
verzija: 4.0, veljavnost: od 14. septembra 2009	
<ul style="list-style-type: none">• Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.2• Politika SIGEN-CA za posebna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.2• Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za strežnike in podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.2• Politika SIGEN-CA za posebna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.2 <p>CP_{Name}: SIGEN-CA-1</p>	<p><i>Spremembe z verzijo 4.0:</i></p> <ul style="list-style-type: none">• izdajatelj digitalnih potrdil SIGEN-CA izdaja kvalificirana digitalna potrdila s ključi minimalne dolžine 2048 bitov;• v kvalificiranih dig. potrdilih za zaposlene in splošne nazive je dodana ustrezna oznaka za kvalificirana potrdila;• spremeni se jamstvo za vrednost posameznega pravnega posla.
amandma k politiki verzije 3.0, veljavnost: od 18. maja 2007	
<p>Amandma k Politiki SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte št. 1 / 3.0</p>	<p><i>Sprememba z amandmajem št. 1 / 3.0:</i></p> <ul style="list-style-type: none">• izdajatelj SIGEN-CA bodočemu imetniku potrdila avtorizacijske kode ne posreduje po priporočeni pošti.
verzija: 3.0, veljavnost: od 28. februarja 2006	
<ul style="list-style-type: none">• Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.1• Politika SIGEN-CA za posebna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.1• Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za strežnike in podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.1• Politika SIGEN-CA za posebna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.1 <p>CP_{Name}: SIGEN-CA-1</p>	<p><i>Spremembe z verzijo 3.0:</i></p> <ul style="list-style-type: none">• uporaba novega naziva za overitelja na Centru Vlade za informatiko, po novem je to »Overitelj na Ministrstvu za javno upravo«;• osebna kvalificirana digitalna potrdila se po novem imenujejo »posebna kvalificirana digitalna potrdila«;• preklic je po novem mogoč samo v uradnih urah, razen v nujnih primerih;• uporaba novega naziva za imetnike SIGEN-CA, in sicer za imetnike »pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti« uporablja izraz »poslovni subjekt«;• struktura dokumenta je v skladu s priporočili RFC 3647.
verzija: 2.0, veljavnost: od 15. julija 2002	



Politika SIGEN-CA za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti CP _{OID} : 1.3.6.1.4.1.6105.2.1.2 CP _{Name} : SIGEN-CA-1	<i>Spremembe z verzijo 2.0:</i> <ul style="list-style-type: none">• izdaja se tudi kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote institucij;• izdaja se tudi kvalificirana digitalna potrdila za strežnike in podpis kode.
verzija: 1.0, veljavnost: od 15. oktobra 2001	
Politika SIGEN-CA za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti CP _{OID} :1.3.6.1.4.1.6105.2.1.1 CP _{Name} : SIGEN-CA-1	/



1. UVOD

(1) Amandma št. 1 / 7.0 k politiki delovanja SIGEN-CA-1 izdajatelja SIGEN-CA dopolnjuje obstoječo verzijo Politike SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte (CP_{OID}: 1.3.6.1.4.1.6105.2.1.1.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.2.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.3.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.4.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.5.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.6.5, CP_{OID}: 1.3.6.1.4.1.6105.2.1.7.5 ter CP_{OID}: 1.3.6.1.4.1.6105.2.1.8.5). Vse storitve in novo izdana kvalificirana digitalna potrdila izdajatelja SIGEN-CA se obravnavajo po politiki, dopolnjeni s tem amandmajem.

(2) Pri potrdilih za elektronske žige je spremenjen naziv, ki je vključen v razločevalno ime in sicer je naziv po novem oznaka, ki nedvoumno predstavlja organizacijo oz. njeno storitev. Naziv mora biti povezan z organizacijo, kateri bo potrdilo izdano, ni pa nujno, da je enak uradnemu nazivu organizacije.

2. SPREMEMBE POLITIKE SIGEN-CA ZA KVALIFICIRANA DIGITALNA POTRDILA ZA POSLOVNE SUBJEKTE

V obstoječi verziji Politike SIGEN-CA za kvalificirana digitalna potrdila za poslovne subjekte se v razdelku 3.1.1 »Oblika imen« šesta alineja četrtega odstavka nadomesti z naslednjo:

»- za elektronske žige oznaka, ki nedvoumno predstavlja organizacijo oz. njeno storitev,«.