

## Kvalificirana digitalna potrdila overitelja Halcom-CA

tehnična dokumentacija

## 1 Namen dokumenta

Namen pričujočega dokumenta je osvetlitev nekaterih tehničnih podrobnosti, povezanih z digitalnimi potrdili overitelja Halcom-CA.

Dokument v grobem obravnava naslednja področja:

- [vrste digitalnih potrdil overitelja Halcom-CA](#); pojasnila v zvezi z vrstami in terminologijo, ki jo pri izdaji digitalnih potrdil uporablja overitelj,
- [korenska digitalna potrdila \(angl. »root certificates«\) overitelja Halcom-CA](#); pojasnila v zvezi z lokacijo in vsebino korenskih overiteljevih potrdil,
- [spiski preklicanih digitalnih potrdil \(angl. »certificate revocation lists« oziroma s kratico: CRL\)](#); pojasnila v zvezi s preklicanimi digitalnimi potrdili,
- [LDAP imenik digitalnih potrdil](#); pojasnila v zvezi z javnim imenikom digitalnih potrdil, ki jih je izdal overitelj Halcom-CA,
- [informacije, vsebovane v digitalnih potrdilih](#); pojasnila v zvezi s podatki, ki so vsebovana v digitalnih potrdilih ter podatki, ki jih v lokalnih podatkovnih zbirkah hrani overitelj,
- [spletni servisi overitelja Halcom-CA](#); pojasnila v zvezi s spletnimi servisi, s katerimi je možno pridobiti dodatne informacije o digitalnih potrdilih ter digitalna potrdila vseh slovenskih overiteljev obravnavati na univerzalen način,
- [obveščanje o spremembah, povezanih z digitalnimi potrdili](#); pojasnila o možnostih obveščanja o spremembah, ki bi lahko vplivale na delovanje sistemov, ki uporabljajo digitalna potrdila overitelja Halcom-CA.

## 2 Vrste digitalnih potrdil overitelja Halcom-CA

Overitelj Halcom-CA izdaja kvalificirana digitalna potrdila za različne namene uporabe oziroma vrste imetnikov potrdil:

- za fizične osebe,
- za pravne osebe oziroma pooblaščenke pravnih oseb,
- strežniška digitalna potrdila.

Poleg namenov uporabe digitalnih potrdil se le-ta razlikujejo še po načinu hranjenja pripadajočih osebnih ključev:

- **napredna digitalna potrdila** (za fizične in pravne osebe) - osebni ključi se izdelajo in hranijo na varnih pametnih karticah,
- **standardna digitalna potrdila** (za fizične osebe) - osebni ključi se izdelajo in hranijo na disku osebnega računalnika,
- **strežniška digitalna potrdila** - osebni ključi se izdelajo in hranijo na strežnikih v varovanem okolju ali v namenskih kriptografskih napravah HSM (angl. »*hardware security module*«).

V grobem velja, da je možno kvalificirana digitalna potrdila overitelja Halcom-CA glede na vrsto uporabe (fizična oseba, pravna oseba) ločiti po polju **izdajatelj** (angl. »*issuer*«), način hranjenja pripadajočih osebnih ključev (pametna kartica, disk) po **oznaki politike** (angl. »*policy identifier*«) ter digitalna potrdila za strežnike od ostalih digitalnih potrdil po polju **organizacijska enota** (angl. »*organizational unit*« oziroma s kratico: **OU**) imetnika potrdila (angl. »*subject*«).

Za standardna kvalificirana digitalna potrdila (digitalna potrdila na disku) za fizične osebe velja:

- **izdajatelj potrdila:** *CN = Halcom CA FO, O = Halcom, C = SI,*
- **oznaka politike potrdila:** *1.3.6.1.4.1.5939.1.5.x* (kjer je *x* poljubno število).

Za napredna kvalificirana digitalna potrdila (digitalna potrdila na pametni kartici) za fizične osebe velja:

- **izdajatelj potrdila:** *CN = Halcom CA FO, O = Halcom, C = SI,*
- **oznaka politike potrdila:** *1.3.6.1.4.1.5939.1.4.x* (kjer je *x* poljubno število).

Za napredna kvalificirana digitalna potrdila za pravne osebe oziroma pooblaščenke pravnih oseb velja:

- **izdajatelj potrdila** (stari ključ): *CN = Halcom CA PO, O = Halcom, C = SI*

- ali izdajatelj potrdila (novi ključ): *CN = Halcom CA PO 2, O = Halcom, C = SI*

Za strežniška potrdila velja:

- izdajatelj potrdila: *CN = Halcom CA PO 2, O = Halcom, C = SI*
- atribut **organizacijska enota (OU)** v polju **imetnik potrdila** (angl. »*subject*«):  
*OU=server certificates*

### 3 Korenska digitalna potrdila overitelja Halcom-CA

Ker overitelj Halcom-CA kvalificirana digitalna potrdila glede na vrsto uporabe podpisuje z različnimi osebnimi ključi, je za preverjanje potrdil potrebno uporabiti različna korenska potrdila overitelja.

**Korensko digitalno potrdilo za fizične osebe** (*CN = Halcom CA FO, O = Halcom, C = SI*) se nahaja na spletnem naslovu:

[http://www.halcom.si/images/uploads/files/CRLji/HALCOM\\_CA\\_FO.CRT](http://www.halcom.si/images/uploads/files/CRLji/HALCOM_CA_FO.CRT)

- Enolično ime: *C=SI, O=Halcom, CN= HALCOM CA FO*
- Serijska številka: *113253 (01 BA 65)*
- Overitelj potrdila: *HALCOM CA FO, Halcom, SI*
- Imetnik potrdila: *HALCOM CA FO, Halcom, SI*
- Veljavnost potrdila: *5. junij 2005 - 5. junij 2020*
- Javni ključ: *RSA (2048 bitov)*
- SHA-1 odtis potrdila: *04 09 56 5B 77 DA 58 2E 64 95 AC 00 60 A7 23 54 EB 4B 01 92*

**Korensko digitalno potrdilo s starim ključem za pravne osebe** (*CN = Halcom CA PO, O = Halcom, C = SI*) se nahaja na spletnem naslovu:

[http://www.halcom.si/images/uploads/files/CRLji/HALCOM\\_CA\\_PO.CRT](http://www.halcom.si/images/uploads/files/CRLji/HALCOM_CA_PO.CRT)

- Enolično ime: *C=SI, O=Halcom, CN= HALCOM-CA PO*
- Serijska številka: *22060 (56 2C)*
- Overitelj potrdila: *HALCOM CA PO, Halcom, SI*
- Imetnik potrdila: *HALCOM CA PO, Halcom, SI*
- Veljavnost potrdila: *28. januar 2002 - 28. januar 2007*
- Javni ključ: *RSA (1024 bitov)*
- SHA-1 odtis potrdila: *6229 5831 0961 4CE7 06AE 5B57 3D44 9528 97A9 99DA*

**Korensko digitalno potrdilo z novim ključem za pravne osebe** (*CN = Halcom CA PO 2, O = Halcom, C = SI*) se nahaja na spletnem naslovu:

[http://www.halcom.si/images/uploads/files/CRLji/HALCOM\\_CA\\_PO\\_2.CRT](http://www.halcom.si/images/uploads/files/CRLji/HALCOM_CA_PO_2.CRT)

- Enolično ime: *C=SI, O=Halcom, CN= HALCOM-CA PO 2*
- Serijska številka: *79074 (01 34 E2)*
- Overitelj potrdila: *HALCOM CA PO 2, Halcom, SI*
- Imetnik potrdila: *HALCOM CA PO 2, Halcom, SI*

- Veljavnost potrdila: *7. februar 2004 - 7. februar 2019*
- Javni ključ: *RSA (1024 bitov)*
- SHA-1 odtis potrdila: *7FBB 6ACD 7E0A B438 DAAF 6FD5 0210 D007 C6C0 829C*

## 4 Spiski preklicanih digitalnih potrdil

Vsa digitalna potrdila overitelja Halcom-CA, ki so bila zaradi kakršnega koli razloga preklicana, so navedena v ustreznem spisku preklicanih digitalnih potrdil (CRL).

Takoj po preklicu digitalnega potrdila se osveži spisek preklicanih digitalnih potrdil v javnem LDAP imeniku overitelja. Z nekajminutnim zamikom se ta spisek prenese tudi na spletne strani.

V LDAP imeniku se spiski preklicanih potrdil nahajajo v binarni DER obliki, na spletnih straneh pa tako v binarni DER kot tudi v berljivi PEM obliki. Binarna DER oblika je primerna za uvoz spiskov npr. v Microsoft Certificate Store (za spletni strežnik IIS), berljiva PEM oblika pa za uporabo v spletnem strežniku Apache.

**Spisek preklicanih digitalnih potrdil fizičnih oseb** (*CN = Halcom CA FO, O = Halcom, C = SI*) se nahaja na naslovih:

<ldap://ldap.halcom.si/cn=Halcom CA FO,o=Halcom,c=SI?certificaterevocationlist;binary>

[http://domina.halcom.si/crls/binary/halcom\\_ca\\_fo.crl](http://domina.halcom.si/crls/binary/halcom_ca_fo.crl) (binarna DER oblika)

[http://domina.halcom.si/crls/halcom\\_ca\\_fo.crl](http://domina.halcom.si/crls/halcom_ca_fo.crl) (berljiva PEM oblika)

**Spisek preklicanih digitalnih potrdil pravnih oseb s starim ključem** (*CN = Halcom CA PO, O = Halcom, C = SI*) se nahaja na naslovih:

<ldap://ldap.halcom.si/cn=Halcom CA PO,o=Halcom,c=SI?certificaterevocationlist;binary>

[http://domina.halcom.si/crls/binary/halcom\\_ca\\_po.crl](http://domina.halcom.si/crls/binary/halcom_ca_po.crl) (binarna DER oblika)

[http://domina.halcom.si/crls/halcom\\_ca\\_po.crl](http://domina.halcom.si/crls/halcom_ca_po.crl) (berljiva PEM oblika)

**Spisek preklicanih digitalnih potrdil pravnih oseb z novim ključem** (*CN = Halcom CA PO 2, O = Halcom, C = SI*) se nahaja na naslovih:

<ldap://ldap.halcom.si/cn=Halcom CA PO 2,o=Halcom,c=SI?certificaterevocationlist;binary>

[http://domina.halcom.si/crls/binary/halcom\\_ca\\_po\\_2.crl](http://domina.halcom.si/crls/binary/halcom_ca_po_2.crl) (binarna DER oblika)

[http://domina.halcom.si/crls/halcom\\_ca\\_po\\_2.crl](http://domina.halcom.si/crls/halcom_ca_po_2.crl) (berljiva PEM oblika)

## 5 LDAP imenik digitalnih potrdil

Vsa kvalificirana digitalna potrdila overitelja Halcom-CA so shranjena v LDAP imeniku digitalnih potrdil.

Imenik digitalnih potrdil je javen. Strežnik se oglašča na naslovu *ldap.halcom.si*, TCP vratih **389**.

Digitalna potrdila so shranjena pod vejami, ki ustrezajo razločevalnim imenom (angl. »*distinguished name*« oziroma s kratico: DN) posameznih izdajateljev. Znotraj teh vej je vsako potrdilo shranjeno v objektu z relativnim razločevalnim imenom, ki je sestavljeno iz atributa ***eidCertificateSerialNumber*** in vrednosti, ki ustreza serijski številki digitalnega potrdila v desetiški obliki. Vsako digitalno potrdilo je shranjeno kot atribut objekta razreda ***eidCertificate***. Ime atributa z digitalnim potrdilom v binarni DER obliki je ***usercertificate***. Za prenos je potrebno uporabiti binarni način (atributu pripeti »;***binary***«) - torej »***usercertificate;binary***«.

Primer - digitalno potrdilo pooblaščenca pravne osebe z novim ključem (*CN=Halcom CA PO 2*) s serijsko številko 158915 (v šestnajstiški obliki 026C C3) je tako shranjeno v atributu *usercertificate;binary* pod razločevalnim imenom *eidCertificateSerialNumber=158915, cn=Halcom CA PO 2, o=Halcom, c=SI*, oziroma pod LDAP URL naslovom:

<ldap://ldap.halcom.si:389/eidCertificateSerialNumber=158915,cn=Halcom CA PO 2,o=Halcom,c=SI?usercertificate;binary>

## 6 Informacije, vsebovane v digitalnih potrdilih

Kvalificirana digitalna potrdila overitelja Halcom-CA poleg različnih podatkov o vrsti in veljavnosti potrdila ter javnega ključa imetnika potrdila vsebujejo še podatke o samem imetniku potrdila. Le-ti so navedeni v polju imetnik (angl. »*subject*«).

Kvalificirana digitalna potrdila za fizične osebe (Halcom CA FO) vsebujejo v polju imetnik naslednje podatke:

- atribut CN (*common name*): ime in priimek imetnika,
- atribut G (*given name*): ime imetnika,
- atribut SN (*surname*): priimek imetnika,
- atribut C (*country*): država imetnika,
- atribut E (*e-mail*): elektronski naslov imetnika,
- atribut z OID oznako 1.3.6.1.4.1.5939.2.2: osebna davčna številka imetnika.

Kvalificirana digitalna potrdila za pooblaščenca pravnih oseb (Halcom CA PO in Halcom CA PO 2) vsebujejo v polju imetnik naslednje podatke:

- atribut CN (*common name*): ime in priimek pooblaščenca,
- atribut G (*given name*): ime pooblaščenca,
- atribut SN (*surname*): priimek pooblaščenca,
- atribut O (*organization*): naziv podjetja pooblaščenca,
- atribut C (*country*): država podjetja,
- atribut E (*e-mail*): elektronski naslov pooblaščenca ali podjetja.

Od začetka julija 2006 kvalificirana digitalna potrdila za pooblaščenca pravnih oseb (novejša Halcom CA PO 2) vsebujejo še podatke o davčni številki pooblaščenca ter podjetja. Podatki so shranjeni v:

- atributu z OID oznako 1.3.6.1.4.1.5939.2.2: osebna davčna številka pooblaščenca,
- atributu z OID oznako 1.3.6.1.4.1.5939.2.3: davčna številka podjetja.

Starejša potrdila za pooblaščenca pravnih oseb (izdana pred julijem 2006) teh podatkov ne vsebujejo - le-te je možno pridobiti preko namenskega spletnega servisa (glej razdelek [o spletnih servisih overitelja Halcom-CA](#)).

## 7 Spletni servisi overitelja Halcom-CA

### 7.1 O spletnih servisih

Overitelj kvalificiranih digitalnih potrdil Halcom-CA je eden od štirih v Sloveniji uradno registriranih overiteljev digitalnih potrdil (SIGEN-CA/SIGOV-CA, AC NLB, POŠTA®CA, Halcom-CA).

Kot najstarejši overitelj v Sloveniji ima veliko izkušenj pri vpeljavi podpore digitalnim potrdilom v različnih informacijskih sistemih. Plod teh izkušenj so tudi spletni servisi (angl. »*web services*«), ki so namenjeni uporabi v programski opremi in aplikacijah, ki za delovanje ali ločevanje uporabnikov uporabljajo digitalna potrdila. Ti spletni servisi ponujajo univerzalen vmesnik za obravnavo digitalnih potrdil vseh štirih v Sloveniji registriranih overiteljev in omogočajo:

- **preverjanje veljavnosti digitalnih potrdil** (podpis potrdila, časovna veljavnost, status v spisku preklicanih potrdil),
- **preverjanje osebne davčne številke in davčne številke podjetja imetnika potrdila** (vpisana davčna številka se ujema/ne ujema z davčno številko imetnika potrdila),
- **pridobivanje informacij o digitalnem potrdilu** (podatki o potrdilu, lastniku, davčnih številkah, ipd.).

Univerzalen vmesnik, ki ga ponujajo ti spletni servisi, tako skriva posebnosti posameznih izdajateljev digitalnih potrdil (npr. lokacije in vrste CRL spiskov, lokacije korenskih digitalnih potrdil, lokacije hranjenja davčnih števil, ipd.)

Več informacij (tehnična navodila, opisi servisov, primeri uporabe, WSDL datoteke, ipd.) se nahaja na spletnem strežniku spletnih servisov <https://ws.halcom.si>.

### 7.2 Spletni servis za preverjanje davčnih števil

Spletni servis za preverjanje davčnih števil *CertificateTaxNumbers* je namenjen preverjanju davčnih števil imetnikov digitalnih potrdil.

Programska oprema, ki servis uporablja, le-temu pošlje digitalno potrdilo, osebno davčno številko imetnika ter davčno številko podjetja, spletni servis pa za vsako davčno številko vrne status le-te (pravilna, napačna, status neznan).

### **7.3 Spletni servis za pridobivanje informacij o potrdilu**

Spletni servis za pridobivanje informacij o digitalnem potrdilu *CertificateInfo* je namenjen branju informacij iz digitalnega potrdila.

Programska oprema, ki servis uporablja, le-temu pošlje digitalno potrdilo, spletni servis pa klicatelju vrne podatke o potrdilu (naziv izdajatelja, časovno veljavnost, serijsko številko) ter podatke o imetniku potrdila (ime, priimek, podjetje, država, davčna številka podjetja ter osebna davčna številka imetnika, kadar ta podatek ni tajen).

### **7.4 Spletni servis za preverjanje veljavnosti potrdila**

Spletni servis *CertificateStatus* je namenjen preverjanju veljavnosti digitalnega potrdila v skladu z veljavno zakonodajo in mednarodno uveljavljenimi standardi.

Programska oprema, ki servis uporablja, le-temu pošlje digitalno potrdilo, spletni servis pa za digitalno potrdilo sporoči, ali je le-to veljavno ali ne. Preverjanje veljavnosti obsega preverjanje digitalnega podpisa potrdila, preverjanje časovne veljavnosti potrdila (od - do) ter preverjanje statusa potrdila v spisku preklicanih digitalnih potrdil.

## 8 Obveščanje o spremembah

Tako kot ves preostali svet, se tudi računalniški svet digitalnih potrdil nenehno spreminja. Če v svojem informacijskem sistemu uporabljate digitalna potrdila overitelja Halcom-CA in bi želeli biti obveščeni o vseh spremembah ali novostih, povezanih z digitalnimi potrdili tega overitelja, nam prosimo na elektronski naslov [ca@halcom.si](mailto:ca@halcom.si) sporočite kontaktni naslov za prejemanje obvestil o spremembah.

Obvestila bo overitelj Halcom-CA razposlal, le kadar bo prišlo v sistemu izdaje kvalificiranih digitalnih potrdil do kake spremembe ali novosti, ki bi lahko vplivala na delovanje obstoječih informacijskih sistemov, ki uporabljajo digitalna potrdila tega overitelja. Komerčnih obvestil ali reklam overitelj na kontaktne naslove ne bo razpošiljal.