Pripravil: Andrej KOMELJ Številka: 80082523-7-0/4 Datum: 18.6.2004

Spletni servisi za podporo pri vpeljavi uporabe digitalnih potrdil različnih overiteljev

Različica	Datum	Opis	Odgovorna oseba
1.0	18.6.2004	Osnovna izdaja	Andrej Komelj
1.1	21.6.2004	Prva faza vpeljave spletnih servisov	Andrej Komelj
1.2	30.8.2004	Dopolnitev izhodnih podatkov; WSDL opisi	Andrej Komelj
1.3	15.10.2004	Popravki zapisov imen overiteljev; povezava na predstavitveno stran servisov	Andrej Komelj
1.4.	6.6.2023	Ažurirana imena izdajateljev	Matej Hrovat

1. SPLETNI SERVISI ZA PODPORO PRI VPELJAVI UPORABE DIGITALNIH POTRDIL RAZLIČNIH OVERITELJEV

Halcom informatika ponuja v uporabo tri spletne servise, ki omogočajo lažjo integracijo digitalnih potrdil različnih slovenskih overiteljev v različne informacijske sisteme ali spletne storitve. Spletni servisi so namenjeni poenoteni obravnavi digitalnih potrdil vseh v Sloveniji registriranih overiteljev, saj ponujajo univerzalen vmesnik za:

- preverjanje statusa digitalnega potrdila (veljaven, preklican, ...),
- preverjanje podatkov o lastniku ter podjetju digitalnega potrdila (davčna številka lastnika, podjetja, ...),
- pridobitev informacij o lastniku ter podjetju digitalnega potrdila.

Spletni servisi so dostopni le preko zavarovane (SSL) povezave in niso odprti za nepooblaščeno javno uporabo. Dostop do servisov je mogoč z uporabo ustreznega odjemalčevega digitalnega potrdila na podlagi predhodnega dogovora.

Več informacij o spletnih servisih, WSDL datoteke le-teh ter posamezne primere uporabe je moč dobiti na: https://ws.halcom.si/.

2. VHODNI PODATKI SPLETNIH SERVISOV

Ker vsi spletni servisi obravnavajo različna digitalna potrdila različnih overiteljev, je del nabora vhodnih podatkov zanje poenoten.

Tabela 1: Obvezni podatki o digitalnem potrdilu v zahtevku

POLJE	TIP	OPIS
certificate	base64Binary	X.509 digitalno potrdilo v DER obliki

Tabela 2: Ostali obvezni podatki v zahtevku

POLJE	TIP	OPIS
actionPolicy	string	polje, ki določa obnašanje strežnika (npr. preverjanje v testni ali živi bazi, ipd.)
other	string	rezervirano

3. SPLETNI SERVIS ZA PREVERJANJE VELJAVNOSTI DIGITALNIH POTRDIL (*CERTIFICATESTATUS*)

Spletni servis za preverjanje veljavnosti digitalnih potrdil na podlagi podatkov o digitalnem potrdilu iz zahtevka preveri veljavnost digitalnega potrdila.

Preverjanje veljavnosti vključuje naslednje korake:

1. preverjanje veljavnosti digitalnega podpisa potrdila,
2. preverjanje časovne veljavnosti digitalnega potrdila,
3. preverjanje statusa digitalnega potrdila z uporabo spiska preklicanih potrdil (*CRL – Certificate Revocation List*) ali »on-line« preko OCSP (*Online Certificate Status Protocol*) servisa.

Tabela 3: Izhodni podatki spletnega servisa za preverjanje veljavnosti digitalnih potrdil

POLJE	TIP	OPIS
returnCode	integer	rezultat obravnave zahtevka: • 0 (obravnava uspela), • 100 – 199 (napaka v zahtevku; napačni podatki, ipd.), • 200 – 299 (napaka na strežniku).
returnText	string	opis napake ali razlaga vrnjenega rezultata
certificateStatus	integer	status digitalnega potrdila: • 0 (veljaven), • 303 (status neznan), • 304 (potekel čas veljavnosti), • 305 (potrdilo še ni veljavno), • 306 (preklican), • 307 (podpis potrdila neveljaven).
producedAt	dateTime	čas preverjanja statusa digitalnega potrdila
thisUpdate	dateTime	čas, za katerega je znano, da je vrnjeni status potrdila ažuren[1]

[1] Čas, za katerega ima spletni servis še sveže podatke o preklicanih potrdilih. Kadar se preverjanje statusa vrši preko CRL spiskov, je to čas nastanka CRL spiska, kadar pa se vrši preko OCSP servisa, je to vrednost, ki jo vrne OCSP strežnik.

nextUpdate	dateTime	čas, najkasneje ob katerem bo imel spletni servis novejše informacije o preklicanih digitalnih potrdilih[2]
revocationReason	integer	razlog preklica digitalnega potrdila, kadar je le-to preklicano ali začasno preklicano: • 500 (razlog preklica neznan – *unknown*), • 501 (zloraba ključa – *key compromise*), • 502 (vdor v agencijo izdajateljico – *CA compromise*), • 503 (sprememba pripadnosti – *affiliation changed*), • 504 (digitalno potrdilo nadomeščeno – *superseeded*), • 505 (konec opravljanja funkcije – *cessation of operation*), • 506 (digitalno potrdilo začasno preklicano – *on hold*), • 509 (ukinitev privilegijev – *privilege whithdrawn*), • 510 (vdor v agencijo izdajateljico - *AA compromise*).
revocationDate	dateTime	čas preklica digitalnega potrdila
other	string	rezervirano

WSDL opis spletnega servisa *CertificateStatus* je dosegljiv na spletnem naslovu https://ws.halcom.si/CertificateStatus/CertificateStatus.wsdl.

4. SPLETNI SERVIS ZA PREVERJANJE DAVČNIH ŠTEVILK IMETNIKA TER PODJETJA DIGITALNEGA POTRDILA (*CERTIFICATETAXNUMBERS*)

Spletni servis za preverjanje davčnih številk imetnika ter podjetja digitalnega potrdila je namenjen hitri poizvedbi, ali davčni številki osebe ter podjetja pripadata imetniku digitalnega potrdila.

Funkcionalno spletni servis deluje na enak način kot spletni servis, ki ga za namene preverjanja digitalnih potrdil v sistemu eDavki Davčni upravi Republike Slovenije nudi agencija Halcom-CA; Davčna uprava servisu posreduje podatke o digitalnem potrdilu, davčno številko osebe, ki želi potrdilo uporabiti, ter davčno številko podjetja te osebe, servis pa odgovori, ali digitalno potrdilo dejansko pripada tej osebi (oz. njeni davčni

[2] Čas, do katerega bo spletni servis osvežil informacije o preklicanih potrdilih. Kadar se preverjanje statusa vrši preko CRL spiskov, je to čas izdaje naslednjega CRL spiska, kadar pa se preverjanje vrši preko OCSP servisa, je to čas, ki ga vrne OCSP strežnik. Kadar je vrednost polja 0, ali polje v odgovoru ni navedeno, ima spletni servis v vsakem trenutku dostop do svežih informacij o statusu digitalnih potrdil izdajatelja podtrdila iz zahtevka.

številki) ter podjetju (davčni številki podjetja).

Poleg obveznih vhodnih podatkov, navedenih v razdelku 2 (Vhodni podatki spletnih servisov), spletni servis pričakuje še dva obvezna podatka o davčnih številkah.

Tabela 4: Dodatni obvezni vhodni podatki spletnega servisa za preverjanje davčnih številk imetnika ter podjetja digitalnega potrdila

POLJE	TIP	OPIS
taxNumber	string	davčna številka imetnika digitalnega potrdila
companyTaxNumber	string	davčna številka podjetja imetnika digitalnega potrdila

Spletni servis preveri, ali podani davčni številki pripadata imetniku ter podjetju digitalnega potrdila.

Tabela 5: Izhodni podatki spletnega servisa za preverjanje davčnih številk imetnika ter podjetja digitalnega potrdila

POLJE	TIP	OPIS
returnCode	integer	rezultat obravnave zahtevka: • 0 (obravnava uspela), • 100 – 199 (napaka v zahtevku; napačni podatki, ipd.), • 200 – 299 (napaka na strežniku).
returnText	string	opis napake ali razlaga vrnjenega rezultata
taxNumberStatus	integer	status davčne številke iz zahtevka: • 0 (davčna številka pripada imetniku potrdila), • 700 (davčna številka iz zahtevka ne pripada imetniku potrdila), • 701 (status davčne številke iz zahtevka neznan).
companyTaxNumberStatus	integer	status davčne številke podjetja iz zahtevka: • 0 (davčna številka pripada podjetju imetnika potrdila), • 700 (davčna številka podjetja iz zahtevka ne pripada podjetju imetnika potrdila), • 701 (status davčne številke podjetja iz zahtevka neznan).

WSDL opis spletnega servisa *CertificateTaxNumbers* je dosegljiv na spletnem naslovu https://ws.halcom.si/CertificateTaxNumbers/CertificateTaxNumbers.wsdl.

5. SPLETNI SERVIS ZA PRIDOBITEV INFORMACIJ O DIGITALNEM POTRDILU (*CERTIFICATEINFO*)

Spletni servis za pridobitev informacij o digitalnem potrdilu vrača podatke, ki vsebujejo informacije o potrdilu, imetniku potrdila, podjetju imetnika potrdila ter rezultatu obravnave zahtevka. Če nekaterih od spodaj navedenih informacij o potrdilu ni mogoče pridobiti, so ustrezna polja prazna ali jih v odgovoru ni.

Tabela 6: Izhodni podatki spletnega servisa za pridobitev informacij o digitalnem potrdilu

POLJE	TIP	OPIS
returnCode	integer	rezultat obravnave zahtevka: • 0 (obravnava uspela), • 100 – 199 (napaka v zahtevku; napačni podatki, ipd.), • 200 – 299 (napaka na strežniku).
returnText	string	opis napake ali razlaga vrnjenega rezultata
issuerCN	string	naziv izdajatelja digitalnega potrdila: • ACNLB, ACNLB SubCA • Halcom CA PO 3, Halcom CA FO, Halcom CA PO e-signature 1, Halcom CA FO e-signature 1, Halcom CA PO e-signature 2, Halcom CA FO e-signature 2 • POSTArCA, • SIGEN-CA, SIGOV-CA.
serialNumber	string	serijska številka digitalnega potrdila v šestnajstiški obliki brez vodilnih ničel
validFrom	dateTime	čas začetka veljavnosti digitalnega potrdila
validTo	dateTime	čas poteka veljavnosti digitalnega potrdila
commonName	string	splošni naziv imetnika digitalnega potrdila
firstName	string	ime imetnika digitalnega potrdila
lastName	string	priimek imetnika digitalnega potrdila
company	string	podjetje imetnika digitalnega potrdila
taxNumber	string	davčna številka imetnika digitalnega potrdila
companyTaxNumber	string	davčna številka podjetja imetnika digitalnega potrdila
companyID	string	matična številka podjetja imetnika digitalnega potrdila
other	string	rezervirano

WSDL opis spletnega servisa *CertificateInfo* je dosegljiv na spletnem naslovu https://ws.halcom.si/CertificateInfo/CertificateInfo.wsdl.