

CDA0051**Usluga izdavanja poslužiteljskih certifikata - TCS**

Kategorija: ODLUKA Trajanje: do opoziva Verzija: 1.0 (05.11.2009.)	Klasa: 500-200/09-01/01 Ur. broj: 650-19-09-24 Datum nastanka: 05.11.2009.
URL: ftp://ftp.carnet.hr/pub/CARNet/docs/rules/CDA0051.pdf	

Uvod

Ovim dokumentom definira se servis izdavanja poslužiteljskih elektroničkih certifikata (TERENA Certificate Service – u daljnjem tekstu TCS), korisnici servisa te njihova prava i obaveze.

1. Servis izdavanja poslužiteljskih certifikata

Danas postoji sve veća potreba za poslužiteljskim elektroničkim certifikatima potrebnim za uspostavu sigurnih kanala komunikacije. Da bi korisnici prilikom spajanja na poslužitelj (web poslužitelj, mail poslužitelj i sl.) preuzeli podatke, pristupili osjetljivim podacima ili dali na uvid osjetljive podatke (npr. korisnička imena) moraju biti sigurni da su pristupili pravom poslužitelju te da je komunikacija s poslužiteljem sigurna (nitko ne može presresti/pročitati i/ili promijeniti podatke), odnosno kriptirana.

Korištenje SSL tehnologije omogućava nam traženu sigurnost, ali se zahtjeva da poslužitelji imaju odgovarajuće elektroničke certifikate.

Elektronički certifikati moraju biti izdani od tijela kome krajnji korisnik i/ili proizvođači programske podrške vjeruju, to jest tijela čiji su verifikacijski (*eng.* root) certifikati ugrađeni u korisničke preglednike i druge klijente putem kojih pristupaju poslužiteljima. Tako izdanim elektroničkim certifikatima izbjegavaju se pop-up poruke kojima se korisnik obavještava da je pristupio poslužitelju za čiji elektronički certifikat njegov klijent nema uspostavljen lanac povjerenja.

CARNet je u suradnji s TERENA-om, a u svrhu povećavanja sigurnosti korisnika prilikom pristupa servisima koje nude CARNet članice, uspostavio servis izdavanja poslužiteljskih elektroničkih certifikata za koje u većini klijenata već postoji lanac povjerenja kojim se može provjeriti valjanost elektroničkog certifikata i time izbjeći pojavljivanja pop-up poruke.

2. Stjecanja statusa korisnika usluge - predregistracija

Servis izdavanja poslužiteljskih elektroničkih certifikata namijenjen je isključivo punopravnim CARNet članicama iz akademske i istraživačke zajednice, a to su pravne osobe prema Zakonu o znanstvenoj djelatnosti i visokom obrazovanju (punopravne CARNet članice prema točki 2.1.1. Odluke o stjecanju statusa i pravima korisnika CARNeta Ministarstva znanosti obrazovanja i športa – URL: http://www.carnet.hr/dokumenti?dm_document_id=157&dm_dnl=1 – u daljnjem tekstu punopravna CARNet članica).

Punopravna CARNet članica stječe pravo korisnika servisa predregistracijom. Postupak predregistracije započinje ispunjavanjem, od odgovorne osobe potpisanog i pečatom ustanove ovjerenog dokumenta kojim se imenuju ovlaštene osobe za postupke zahtijevanja, opozivanja, obnavljanja i dobivanja poslužiteljskih elektroničkih certifikata (u daljnjem tekstu: TCS imenovanje). Postupkom predregistracije provjerava se status punopravne CARNet članice odobren od Ministarstva znanosti obrazovanja i športa, točnost navedenih podataka o ustanovi kao i pravo zastupanja ustanove potpisnika TCS imenovanja pri odgovarajućem sudskom registru.

Ustanove korisnice CARNetove usluge SCS definirane u dokumentu [CDA0041](#) ne moraju popunjavati nova imenovanja. Osobe imenovane u pripadajućem SCS proxy dokumentu smatraju se ovlaštenim predstavnicima ustanove za poslove zahtijevanja, opozivanja, obnavljanja i dobivanja poslužiteljskih elektroničkih certifikata u TCS-u.

3. Prava korisnika usluge

Korisnici usluge, to jest njihovi ovlašteni predstavnici, imaju pravo:

- zatražiti neograničeni broj poslužiteljskih certifikata za poslužitelje koji se nalaze u domenama u vlasništvu punopravne CARNet članice;
- zatražiti opoziv kompromitiranih (certifikati za koje se sumnja ili se sa sigurnošću zna da su došli u posjed neovlaštenim osobama) poslužiteljskih elektroničkih certifikata;
- zatražiti obnovu certifikata kojima ističe valjanost.

Punopravna CARNet članica, korisnik servisa, ima pravo tražiti, opozivati ili obnavljati elektroničke certifikate poslužitelja samo za one poslužitelje čiji se jednoznačan naziv poslužitelja (FQDN - fully qualified domain name) koji se nalazi u nazivu elektroničkog certifikata (CN – CommonName atribut Subjecta elektroničkog certifikata), to jest u alternativnom nazivu elektroničkog certifikata (DNS zapisi u SubjectAlternativeName polju elektroničkog certifikata) nalazi u domeni čiji je ona vlasnik.

4. Obaveze korisnika usluge

Korisnici usluge obavezni su:

- imenovati najmanje jednu ovlaštenu osobu koja će u ime ustanove koju predstavlja imati ovlasti obavljanja svih poslova u svrhu zahtijevanja i dobivanja poslužiteljskih elektroničkih certifikata. Imenovanje ovlaštene osobe podnosi se putem obrasca TCS imenovanje (URL: <ftp://ftp.carnet.hr/pub/CARNet/forms/tcs/tcs-imenovanje.doc>). Imenovanje mora sadržavati točne i aktualne informacije te mora biti ovjereno potpisom službenog predstavnika ustanove (dekan, ravnatelj) uz odgovarajući pečat ustanove;
- pisanim putem odmah izvijestiti CARNet o prestanku/promjeni statusa ovlaštene(ih) osobe(a) ili bilo kojeg drugog podatka iz TCS imenovanja;
- poduzeti sve potrebne radnje u cilju zaštite tajnosti privatnog ključa poslužiteljskog elektroničkog certifikata;
- u slučaju kompromitiranja ili gubitka privatnog ključa poslužiteljskog elektroničkog certifikata imenovana ovlaštena osoba dužna je u što kraćem roku podnijeti zahtjev za njegov opoziv;
- poštivati pravila i procedure definirane u temeljnom dokumentu „TCS Certificate Practice Statement“ (u daljnjem tekstu: TCS CPS) koji definira politiku izdavanja i upravljanja poslužiteljskim certifikatima u usluzi TCS (URL: <http://www.terena.org/tcs/repository/>);
- koristiti certifikate isključivo u legalne svrhe i to u skladu s definiranim pravilima korištenja koji su navedeni u dokumentu TCS CPS. Ponajviše, certifikati izdani u sklopu usluge TCS ne smiju se koristiti za osiguranje bilo kojeg oblika financijskih transakcija;
- izdani certifikati mogu biti opozvani od strane CARNeta ili TERENA-e u skladu s uvjetima definiranim u dokumentu TCS CPS;
- certifikati kojima je istekao rok trajanja ili su opozvani ne smiju se koristiti.

U slučaju da se korisnik servisa ne pridržava bilo koje od navedenih obaveza CARNet ima pravo privremeno ili trajno obustaviti pružanje usluge izdavanja poslužiteljskih elektroničkih certifikata. Odluku o privremenoj ili trajnoj obustavi pružanja usluge izdavanja poslužiteljskih elektroničkih certifikata potpisuje ravnatelj CARNeta, to jest njegovi pomoćnici i u odluci se navode razlozi i vrijeme trajanja zabrane. Punopravna CARNet članica, korisnica servisa, ima pravo žalbe na tako donesenu odluku koju podnosi u pisanom obliku.

Više informacija o servisu izdavanja poslužiteljskih elektroničkih certifikata, kao i pripadajući obrasci mogu se naći na web stranicama servisa http://www.carnet.hr/sc_servis.