Hrvatska akademska i istraživačka mreža - CARNet

CDA0059

Usluga izdavanja elektroničkih certifikata - TCS

Kategorija: ODLUKA	**Klasa: 500-200/15/92**
Trajanje: do opoziva	**Ur. broj: I26319-650-53-15-36**
Verzija: 1.0 (18.06.2015.)	**Datum nastanka: 18.06.2015.**
URL: ftp://ftp.carnet.hr/pub/CARNet/docs/rules/CDA0059.pdf	

Uvod

Ovim dokumentom definira se usluga izdavanja elektroničkih certifikata (Trusted Certificate Service – u daljnjem tekstu TCS), korisnici usluge te njihova prava i obaveze.

1. Usluga izdavanja elektroničkih certifikata

Danas postoji sve veća potreba za elektroničkim certifikatima potrebnim za uspostavu sigurnih kanala komunikacije te potpisivanje i/ili kriptiranje datoteka i provjeru autentičnosti programskog kôda.

Bez obzira na vrstu certifikata, elektronički certifikati moraju biti izdani od tijela kome krajnji korisnik i/ili proizvođači programske podrške vjeruju, to jest tijela čiji su verifikacijski (root) certifikati ugrađeni u korisničke preglednike i druge klijente putem kojih pristupaju poslužiteljima. Tako izdanim elektroničkim certifikatima izbjegavaju se sigurnosne poruke kojima se korisnika obavještava da je pristupio poslužitelju za čiji elektronički certifikat njegov klijent nema uspostavljen lanac povjerenja ili programski kôd nije autentičan.

CARNet je u suradnji s GEANT-om (europska asocijacija nacionalnih edukacijskih i istraživačkih mreža, čija je CARNet članica), a u svrhu povećavanja sigurnosti korisnika prilikom pristupa uslugama koje nude članice CARNeta, uspostavio uslugu izdavanja elektroničkih certifikata za koje u većini klijenata već postoji lanac povjerenja kojim se može provjeriti valjanost elektroničkog certifikata i time izbjeći pojavljivanja sigurnosnih poruka.

GEANT je za izdavanje elektroničkih certifikata sklopio ugovor s tvrtkom DigiCert.

TCS uslugom CARNet omogućuje korištenje nekoliko tipova certifikata:

Poslužiteljski certifikati (SSL/TLS certifikati)

Ova vrsta certifikata se najčešće koristi u elektroničkoj komunikaciji. 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 i lozinke) 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/TLS tehnologije omogućava nam traženu sigurnost, ali se zahtijeva da poslužitelji imaju odgovarajuće elektroničke certifikate.

Klijentski certifikati

Klijentski certifikati omogućuju korisnicima identificiranje prema udaljenim uslugama. Na taj način omogućeno je slanje autentičnih zahtjeva prema poslužiteljima (web poslužitelju, mail poslužitelju i sl.). Klijentskim certifikatima omogućeno je korisnicima potpisivanje i/ili kriptiranje e-mail poruka te potpisivanje dokumenata osobnim digitalnim potpisom.

Code Signing certifikati

Jednostavno objavljivanje računalnih programa donosi za sobom i veliku opasnost od lažiranja gotovih rješenja legitimnih programa koje korisnici koriste. Za zaštitu tih programa, oni se mogu digitalno potpisati i time osigurati autentičnost. Vrsta certifikata kojima se osigurava autentičnost programskog kôda i programa su code signing certifikati.

Grid certifikati

Skup certifikata koji omogućuju siguran pristup korisnicima ili automatiziranim alatima (robotima) do resursa u računalnim gridovima, provjeru autentičnosti pojedinih klijenata i sigurnu razmjenu podataka unutar grida s drugim sustavima.

Document Signing certifikati

Ova vrsta certifikata namijenjena je potpisivanju dokumenta na razini ustanove. Potpisivanje dokumenata Document Signing certifikatom nudi veću sigurnost od potpisa Client certifikatom jer se prilikom njegovog izdavanja provodi temeljitija provjera nositelja certifikata, a autorizacija se vrši hardverskim tokenom izdanim od izdavatelja certifikata, tvrtke DigiCert.

Extended Validation certifikati (EV Certificates)

U sklopu TCS usluge moguće je dobiti poslužiteljski EV certifikat i Code Signing EV certifikat. Prilikom izdavanja certifikata tvrtka DigiCert, izdavatelj certifikata, provodi temeljitiju provjeru tražitelja certifikata. Ovi certifikati nude najveći stupanj sigurnosti.

Cijena certifikata

Sve vrste certifikata dostupni su krajnjim korisnicima bez naknade osim Code Signing EV certifikata za kojeg se plaća trošak izdavanja i dostave hardverskog tokena u iznosu od 50 USD.

2. Stjecanja statusa korisnika usluge

Usluga izdavanja elektroničkih certifikata namijenjena je svim članicama CARNeta bez obzira na vrstu članstva. Članica CARNeta stječe pravo korisnika usluge ispunjavanjem, od odgovorne osobe potpisanog i pečatom ustanove ovjerenog, dokumenta kojim se imenuju ovlaštene osobe za postupke zahtijevanja i opozivanja certifikata te odobravanja zahtjeva upućenih od ostalih korisnika u njihovoj ustanovi. CARNet provjerava status članice CARNeta, točnost navedenih podataka o ustanovi kao i pravo zastupanja ustanove potpisnika dokumenta pri odgovarajućem sudskom registru. Imenovanje osobe vrijedi do njezinog opoziva.

3. Prava korisnika usluge

Korisnici usluge imaju pravo korištenja sljedećih certifikata bez naknade, osim EV Code Signing certifikata:

Vrsta certifikata	**Trajanje**
Poslužiteljski certifikati	
SSL Plus Certificate (SSL certifikat za jednu domenu)	1-3 godine
UC Certificate (SSL certifikat za više domena)	1-3 godine
Wildcard Plus (SSL certifikat za sve poddomene)	1-3 godine
EV SSL Certificate (za jednu domenu)	1-2 godine
EV UC Certificate (za više domena)	1-2 godine
Klijentski certifikati	
Digital Signature Plus	1-3 godine
Email Security Plus	1-3 godine
Premium	1-3 godine
Grid certifikati	
Grid Premium	13 mjeseci
Grid Robot Email	13 mjeseci
Grid Robot FQDN	13 mjeseci
Grid Robot Name	13 mjeseci
Grid Host SSL	13 mjeseci
Grid Host SSL UC	13 mjeseci

Vrsta certifikata	Trajanje
Code signing certifikati	
Code Signing Certificate	1-3 godine
EV Code Signing Certificate*	1-3-godine
Document Signing certifikati	
Document Signing Certificate (2000 dokumenata)	1-3 godine
Document Signing Certificate (5000 dokumenata)	1-3 godine

*Za korištenje EV Code Signing certifikata plaća se naknada od 50 USD po certifikatu tvrtki DigiCert.

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

- zatražiti neograničen broj bilo kojeg od navedenih certifikata;
- izdati elektroničke certifikate samo u ime svoje ustanove i za domene koje ustanova koristi.

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 elektroničkih certifikata. Ovlaštene osobe imenuju se do opoziva. Imenovanje ovlaštene osobe podnosi se putem za to predviđenog obrasca dostupnog na web stranicama usluge: https://certifikati.carnet.hr/. Imenovanje mora biti ovjereno potpisom službenog predstavnika ustanove uz odgovarajući pečat ustanove;
- osigurati točnost i ažurnost svih podataka koji se koriste prilikom izdavanja certifikata;
- pročitati i prihvatiti dokumente u TCS repozitoriju (https://www.terena.org/activities/tcs/repository-g3/) kojima se definira način upravljanja certifikatima, posebice dokumente TCS Terms of Use i TCS Consolidated Required Contractual Terms;
- prihvaćanjem ovih dokumenata članica na sebe preuzima sve odgovornosti vezane uz korištenje elektroničkih certifikata.

Korisnici usluge posebno trebaju obratiti pažnju i reagirati u sljedećim slučajevima:

- prestati koristiti certifikat ukoliko je isti opozvan;
- pisanim putem odmah izvijestiti CARNet o prestanku/promjeni statusa ovlaštene(ih) osobe(a);
- poduzeti sve potrebne radnje u cilju zaštite tajnosti privatnog ključa elektroničkog certifikata;
- u slučaju kompromitiranja privatnog ključa elektroničkog certifikata imenovana ovlaštena osoba dužna je u što kraćem roku podnijeti zahtjev za njegov opoziv.

U slučaju da se korisnik usluge ne pridržava navedenih obaveza CARNet ima pravo privremeno ili trajno obustaviti pružanje usluge izdavanja elektroničkih certifikata te opozvati certifikate za koje sumnja da su kompromitirani ili da se koriste u svrhu za koju nisu izdani. Odluku o privremenoj ili trajnoj obustavi pružanja usluge izdavanja elektroničkih certifikata potpisuje ravnatelj CARNeta ili njegovi pomoćnici, i u odluci se navode razlozi i vrijeme trajanja zabrane. Članica CARNeta, korisnica usluge, ima pravo žalbe CARNetu na tako donesenu odluku koju podnosi u pisanom obliku u roku od osam dana od primitka odluke o obustavi usluge.

Odluku o obustavi pružanja usluge i opoziv certifikata mogu donijeti GEANT ili DigiCert ukoliko se usluga ili certifikati koriste protivno pravilima navedenima u dokumentima u TCS repozitoriju (https://www.terena.org/activities/tcs/repository-g3/).

Više informacija o usluzi izdavanja elektroničkih certifikata, kao i pripadajući obrasci mogu se naći na web stranicama: http://certifikati.carnet.hr.

5. Odricanje od odgovornosti

Korisnik je odgovoran za bilo kakvu nastalu štetu nastalu kao posljedicu ili preduvjet korištenja usluge.

6. Završne odredbe

Stupanjem na snagu ove verzije dokumenta, prestaje vrijediti CDA0051, Verzija 2.0, Klasa:500-200/12-92, Ur.br:I8606-650-109-12-1 od 1.2.2012.