Hrvatska akademska i istraživačka mreža - CARNET

CDA0059

Usluga izdavanja elektroničkih certifikata - TCS

Kategorija: ODLUKA	**Klasa: 600-200/20/276**
Trajanje: do opoziva	**Ur. broj: I58412-650-53-20-2**
Verzija: 2.0 (20.04.2020.)	**Datum nastanka: 18.6.2015.**
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 obveze.

1. Usluga izdavanja elektroničkih certifikata

Elektronički certifikati potrebni za uspostavu sigurnih kanala komunikacije te potpisivanje i/ili kriptiranje datoteka i provjeru autentičnosti programskog kôda predstavljaju jedan od najznačajnijih sigurnosnih mehanizama u suvremenim poslovnim procesima.

Bez obzira na vrstu, elektroničke certifikate moraju izdavati tijela koje krajnji korisnici i/ili proizvođači programske podrške smatraju pouzdanima. Detaljnije, tijela čiji su verifikacijski certifikati (*eng. root certificate*) ugrađeni u korisničke preglednike i druge klijente putem kojih krajnji korisnici pristupaju poslužiteljima. Korištenjem elektroničkih certifikata pouzdanih tijela izbjegava se prikazivanje sigurnosnih poruka 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 GÉANT-om, europskim udruženjem nacionalnih edukacijskih i istraživačkih mreža u čijem je CARNET sastavu, u svrhu povećavanja sigurnosti korisnika prilikom pristupa uslugama koje nude ustanove članice CARNET-a, uspostavio uslugu izdavanja elektroničkih certifikata pouzdanih tijela za koje u većini klijenata već postoji lanac povjerenja kojim se može provjeriti valjanost elektroničkog certifikata i time izbjeći pojavljivanje sigurnosnih poruka.

GÉANT je za izdavanje elektroničkih certifikata sklopio ugovor s tvrtkom Sectigo Limited.

2. Vrste elektroničkih certifikata

CARNET TCS uslugom omogućuje korištenje sljedećih tipova elektroničkih certifikata:

Poslužiteljski certifikati (SSL/TLS certifikati)

Ova vrsta elektroničkih certifikata se najčešće koristi u elektroničkoj komunikaciji. Kako 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, odnosno kriptirana te da nitko ne može presresti/pročitati i/ili promijeniti podatke.

Korištenje SSL/TLS tehnologije omogućava nam traženu sigurnost koja se može ostvariti korištenjem odgovarajućih poslužiteljskih elektroničkih certifikata. Dodatno, korisnik može zatražiti i poslužiteljski *Extended Validation* certifikat (*EV Certificates*). Ovi elektronički certifikati nude najveći stupanj sigurnosti, a specifično je da prilikom izdavanja elektroničkog certifikata tvrtka Sectigo Limited, izdavatelj, provodi temeljitiju provjeru tražitelja elektroničkog certifikata.

Klijentski elektronički certifikati

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

Code Signing elektronički certifikati

Jednostavno objavljivanje računalnih programa donosi za sobom i veliku opasnost od lažiranja gotovih rješenja legitimnih programa koje korisnici koriste. Digitalnim potpisivanjem legitimni računalni programi dodatno se štite, a elektronički certifikati jamče njihovu autentičnosti. Vrsta elektroničkih certifikata kojima se osigurava autentičnost programskog kôda i programa su *code signing* elektronički certifikati. Dodatno, korisnik može zatražiti i *Extended Validation* certifikat (*EV Certificates*). Ovi elektronički certifikati nude najveći stupanj sigurnosti, a specifično je da prilikom izdavanja certifikata tvrtka Sectigo Limited, izdavatelj, provodi temeljitiju provjeru tražitelja elektroničkog certifikata.

IGTF elektronički certifikati

Skup elektroničkih certifikata koji omogućuju siguran pristup korisnicima ili automatiziranim alatima (robotima) do resursa u računalnoj grid infrastrukturi, provjeru autentičnosti pojedinih klijenata i sigurnu razmjenu podataka unutar grid infrastrukture s drugim sustavima. Specifikacije elektroničkih certifikata i njihovo korištenje detaljnije je objašnjeno na stranicama organizacije EUGridPMA (https://www.eugridpma.org/).

Document Signing Certifikati

Ova vrsta elektroničkih certifikata namijenjena je potpisivanju dokumenta na razini ustanove. Potpisivanje dokumenata *Document Signing* elektroničkim certifikatom nudi veću sigurnost od potpisa klijentskim elektroničkim certifikatom jer se prilikom njegovog izdavanja provodi opsežnija provjera nositelja elektroničkog certifikata, a sam elektronički certifikat je kreiran sukladno zahtjevima *Adobe Approved Trust List* (AATL) programa.
Više informacija o samom programu i *Document signing* elektroničkim certifikatima nalazi se na

stranicama tvrtke Adobe: (https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html).

***Extended Validation* elektronički certifikati (*EV Certificates*)**

Kako je prethodno navedeno u opisu poslužiteljskih (SSL/TLS) i *Code Signing* elektroničkih certifikata, u sklopu TCS usluge moguće je dobiti poslužiteljski EV elektronički certifikat i *Code Signing* EV elektronički certifikat. Prilikom izdavanja elektroničkih certifikata tvrtka Sectigo Limited, izdavatelj, provodi temeljitiju provjeru tražitelja elektroničkog certifikata. Ovi elektronički certifikati nude najveći stupanj sigurnosti.

Korisnici usluge imaju pravo korištenja sljedećih certifikata:

Vrsta certifikata	**Trajanje**
Poslužiteljski Certifikati	
SSL Certificate (SSL certifikat za jednu domenu)	1-2 godine
Multi domain SSL (SSL certifikat za više domena)	1-2 godine
Wildcard SSL (SSL certifikat za sve poddomene)	1-2 godine
UC SSL (Unified Communication Certificate za više hostova)	1-2 godine
EV SSL Certificate (za jednu domenu)	1-2 godine
EV UC Certificate (za više domena)	1-2 godine
Klijentski Certifikati	
Personal Certificate	1-3 godine
IGTF Certifikati	
SSL	13 mjeseci
MICS Personal	13 mjeseci
MICS-Robot Personal	13 mjeseci
Classic-Robot Email	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	1-2 godine

Tablica 1. Prikaz vrste certifikata i vrijeme trajanja

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

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

3. Cijena elektroničkih certifikata

CARNET kao neprofitna organizacija sve svoje usluge krajnjim korisnicima pruža besplatno. Sukladno tome, sve vrste elektroničkih certifikata dostupne su krajnjim korisnicima za slobodno korištenje bez naknade.

4. Stjecanja statusa korisnika usluge

Usluga izdavanja elektroničkih certifikata namijenjena je svim članicama CARNET-a bez obzira na vrstu članstva. Članica CARNET-a stječe pravo korisnika usluge ispunjavanjem i ovjerom Zahtjeva za imenovanjem ovlaštene osobe za korištenje CARNET-ove usluge Elektroničkih certifikata (TCS) (u daljnjem tekstu Zahtjev) kojim se imenuje odgovorna osoba... Dokument može biti ovjeren digitalnim potpisom zakonskog zastupnika ustanove članice (ravnatelj, dekan, i sl.). Ako prethodno spomenuti dokument nije moguće digitalno potpisati, isti je potrebno ovjeriti potpisom i pečatom.

Digitalno potpisane Zahtjeve u .pdf formatu potrebno je dostaviti putem elektroničke pošte na adresu: tcs-ra@carent.hr.

Zahtjeve ovjerene potpisom i pečatom potrebno je dostaviti u .pdf formatu na adresu elektroničke pošte na adresu tcs-ra@carent.hr, a ustanova je dužna čuvati original tijekom cijelog trajanja korištenja usluge.

Pri svakom zahtjevu za izdavanjem elektroničkih certifikata CARNET provjerava status članice ustanove, točnost navedenih podataka o ustanovi kao i pravo zastupanja ustanove potpisnika Zahtjeva pri odgovarajućem sudskom registru.

Imenovanje osobe vrijedi do njezinog opoziva.

5. Obveze korisnika usluge

Korisnici usluge obvezni su:

- imenovati jednu ovlaštenu osobu koja će u ime ustanove koju predstavlja imati ovlasti obavljanja svih poslova u svrhu zahtijevanja, dobivanja i upravljanja elektroničkim certifikatima. Ovlaštena osoba imenuju se do opoziva. Imenovanje ovlaštene osobe podnosi se putem za to predviđenog Zahtjeva dostupnog na web stranicama usluge: https://certifikati.carnet.hr/;
- osigurati točnost i ažurnost svih podataka koji se koriste prilikom izdavanja elektroničkog certifikata;
- prihvaćanjem ovog 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 elektronički certifikat ako je isti opozvan;
- pisanim putem odmah izvijestiti CARNET o prestanku/promjeni statusa ovlaštene osobe;
- 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 obveza 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 CARNET-a ili njegovi pomoćnici, i u odluci se navode razlozi i vrijeme trajanja zabrane. Članica CARNET-a, korisnica usluge, ima pravo žalbe CARNET-u 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 GÉANT ili Sectigo Limited ako se usluga ili elektronički certifikati koriste protivno pravilima navedenima u dokumentima u TCS repozitoriju (https://wiki.geant.org/display/TCSNT/TCS+Repository/).

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

6. Odricanje od odgovornosti

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

7. Završne odredbe

Stupanjem na snagu ove verzije dokumenta, prestaje vrijediti CDA0059, Klasa:500-200/15-92, Ur.br: : I26319-650-53-15-36 od 18.06.2015.