




AMPEC

Академска мрежа Србије



Правилник коришћења услуге издавања TCS
сертификата

Историја верзија документа

Верзија	Датум	Иницијали аутора	Опис промене
4.0		АТ	Четврта верзија овог документа

Садржај

1	УВОД	4
2	ОПИС УСЛУГЕ ИЗДАВАЊА TCS СЕРТИФИКАТА	5
3	СТИЦАЊЕ СТАТУСА КОРИСНИКА - РЕГИСТРАЦИЈА	6
4	ПРАВА КОРИСНИКА УСЛУГЕ	7
5	ОБАВЕЗЕ КОРИСНИКА УСЛУГЕ	8
6	ОГРАНИЧЕЊЕ ОДГОВОРНОСТИ	10
7	ДОДАТНЕ ИНФОРМАЦИЈЕ	11

1 Увод

У овом документу дефинишу се правила и општи услови коришћења услуге издавања TCS (*Trusted Certificate Service*) сертификата од стране AMRES-а, начин на који AMRES корисник остварује своје право на коришћење ове услуге, као и права и обавезе корисника ове услуге.

2 Опис услуге издавања TCS сертификата

Данас постоји све већа потреба за дигиталним серверским сертификатима који омогућавају успостављање сигурних канала комуникације. Да би корисници приликом приступа серверу (веб-сервер, имејл-сервер и сл.) преузели податке, приступили осетљивим подацима или дали на увид осетљиве податке (нпр. корисничка имена) морају бити сигурни да су приступили правом серверу, те да је комуникација са сервером сигурна (да нико не може да пресретне/прочита и/или промени податке), односно криптована.

Коришћење SSL/TLS технологије омогућава тражену сигурност, али захтева да сервери имају одговарајуће дигиталне сертификате.

Дигитални сертификати морају бити издати од стране тела коме крајњи корисници и/или произвођачи софтвера верују, то јест тела чији су сертификати уграђени у корисничке претраживаче и друге клијенте путем којих крајњи корисници комуницирају међусобно или са серверима.

Академска мрежа Републике Србије (AMPEC) потписала је Уговор са организацијом GÉANT по коме може издавати дигиталне SSL/TLS сертификате за научно-истраживачке и образовне институције у Републици Србији које су AMPEC корисници, док ће се сертификати издавати само за домене регистроване под „.ac.rs“ доменом. GÉANT има улогу сертификационог тела (CA – *Certification Authority*), а AMPEC регистрационог тела (RA – *Registration Authority*).

Сви сертификати издати у оквиру TCS услуге се потписују сертификатом који припада сертификационом телу GÉANT CA 4. Овај прелазни сертификат је потписан од стране USERTrust RSA/ECC CA кореног (*root*) сертификационог тела. Тај корени (*root*) сертификат је преинсталиран у већини SSL/TLS клијената чиме се успоставља ланац поверења (на пример, приликом приступања сајту преко *https* конекције, који се налази на веб серверу који има TCS сертификат, није потребна интервенција корисника како би сертификат био прихваћен јер се одговарајући корени сертификат већ налази преинсталиран у већини често коришћених Интернет прегледача: Internet Explorer, Mozilla Firefox, Google Chrome, Opera и др.).

3 Стицање статуса корисника - регистрација

Према преузетим правима и обавезама за TCS услугу, право на коришћење TCS сертификата, имају само научно-истраживачке и образовне институције које су AMRES корисници.

AMRES корисник стиче право корисника услуге регистрацијом свог домена унутар „.ac.rs“ домена на Порталу Регистра домена „.ac.rs“ <http://registar.ac.rs>. Особа која је при томе именована за административни контакт институције као одговорна за обављање послова у вези са „.ac.rs“ доменом, сматраће се одговорном и за обављање послова у вези са TCS сертификатима у том домену. Институција доставља документ о сагласности за коришћење услуге издавања TCS сертификата и именовању административног контакта у папирној форми на српском и енглеском језику. Овај документ потписује и оверава печатом установе овлашћено лице институције. Тиме се институција, њено овлашћено лице и административни контакт обавезују на поштовање права и обавеза дефинисаних у овом документу.

По достављању документа, AMRES корисник завршава процес регистрације у коме су проверени његов статус, тачност наведених података о институцији и именована особа овлашћена за обављање послова у вези са TCS сертификатима. Овим AMRES корисник стиче статус корисника TCS услуге и уједно право да пријави организацију за TCS портал и захтева TCS сертификате.

4 Права корисника услуге

Административни контакт AMRES корисника, у име институције корисника услуге, има право:

- ❖ затражити неограничени број TCS сертификата за своје сервере; примарни FQDN (*Fully Qualified Domain Name*) једнозначни назив сервера у низу имена која припадају серверу мора да буде из домена који је та институција регистровала у „ac.rs“;
- ❖ затражити неограничен број TCS сертификата за своје кориснике при чему све имејл адресе наведене у сертификату морају бити из домена који је та институција регистровала у „ac.rs“;
- ❖ затражити опозив (повлачење) компромитованих TCS сертификата (сертификата за које се сумња или се са сигурношћу зна да су дошли у посед неовлашћеним особама);
- ❖ затражити обнову сертификата којима истиче период важења.

Сертификат може да садржи једно или више имена која су дефинисана и користе се на серверу, као и једну или више имејл адреса крајњих корисника.

AMRES корисник, корисник TCS услуге, има право тражити, опозивати или обнављати TCS сертификате само за оне сервере који користе бар један назив сервера (FQDN - *Fully Qualified Domain Name*) из домена који је та институција регистровала у „ac.rs“. FQDN из „ac.rs“ домена мора се налазити у називу TCS сертификата (CN – CommonName атрибут Subject поља TCS сертификата). Ако сервер има више FQDN имена, у алтернативном називу дигиталног сертификата (DNS записи у SubjectAlternativeName пољу TCS сертификата) може се наћи FQDN име из „ac.rs“ домена.

5 Обавезе корисника услуге

У оквиру TCS услуге, AMRES корисник је у обавези да:

- ✦ прихвати опште услове и правила коришћења AMRES услуге издавања TCS сертификата описаних у овом документу, потписивањем документа „Сагласност за коришћење услуге издавања TCS сертификата“.
- ✦ именује једног службеног представника (административни контакт) који ће представљати институцију у TCS сервису. Именовање административног контакта врши се преко документа „Сагласност за коришћење услуге издавања TCS сертификата“. Именовање мора да садржи тачне и актуелне информације, усклађене са подацима о институцији на порталу Регистра домена „ac.rs“ и мора бити потписано од стране овлашћеног лица институције (декана, директора), уз одговарајући печат установе;
- ✦ одмах обавести AMRES о престанку/промени статуса административног контакта или било којег другог податка из TCS именовања тако што ће те информације унети преко Портала Регистра домена „ac.rs“. У случају престанка/промене статуса особе која врши послове административног контакта унете промене се морају потврдити писменим путем преко документа „Сагласност за коришћење услуге издавања TCS сертификата“ потписаног од стране овлашћеног лица институције (декана, директора), уз одговарајући печат установе;
- ✦ у свим захтевима и радњама према AMRES-у пружи тачне и прецизне податке. Уколико у периоду важења сертификата дође до промене било ког податка на основу кога је издат, институција је дужна да о овоме обавести AMRES тако што ће измене унети коришћењем Портала Регистра домена „ac.rs“;
- ✦ не инсталира и не користи издати сертификат све док не прегледа и потврди тачност података у сертификату. Институција је у обавези да прекине са коришћењем сертификата уколико било која информација у њему постане нетачна, застарела или неважећа;
- ✦ предузме све потребне мере да би се спречило компромитовање, губитак, разоткривање, мењање и на било који начин неауторизовано коришћење приватног кључа TCS сертификата;
- ✦ у случају компромитовања или губитка приватног кључа TCS сертификата, именовани административни контакт институције је дужан да у што краћем року поднесе захтев за његов опозив;
- ✦ да осигура да су представници AMRES корисника и особље укључено у рад са TCS услугом прочитали, разумели и сложили се са условима коришћења TCS услуге описаним у овом документу, затим условима наведеним у TCS документима о практичним правилима рада сертификационог тела „**TCS Certificate Practice Statement**“ (у даљем тексту TCS CPS), као и пропратних докумената који су објављени у TCS репозиторијуму који је доступан на веб-адреси: <https://wiki.geant.org/display/TCSNT/TCS+Repository>;
- ✦ поштује правила и процедуре дефинисане у TCS CPS документу који дефинише политику издавања и управљања дигиталним сертификатима у оквиру TCS услуге;
- ✦ користи сертификате искључиво у легалне сврхе и то у складу са дефинисаним правилима коришћења која су наведена у документу TCS CPS. Сертификати издати у склопу услуге TCS не смеју да се користе за осигурање било каквог облика финансијских трансакција (нпр. трансакција путем платних картица, *online* плаћања и други облици новчаних трансакција);
- ✦ издати сертификати могу бити опозвани од стране AMRES-а или GÉANT-а у складу са условима наведеним у TCS CPS документу;
- ✦ не сме да користи сертификате којима је истекао датум важења или су опозвани.

У случају да се корисник услуге не придржава било које од наведених обавеза AMRES има право да донесе одлуку у којој се привремено или трајно обуставља пружање услуге издавања TCS сертификата.

У одлуци се наводе разлози и време трајања забране. Корисник TCS услуге има право жалбе на тако донешену одлуку коју подноси у писаном облику.

6 Ограничење одговорности

AMRES не сноси никакву одговорност за било какве губитке који могу да настану као последица сметњи, прекида у раду или било каквих других проблема при коришћењу или издавању TCS сертификата.

7 Додатне информације

Више информација о услузи издавања TCS сертификата, као и припадајући обрасци и документа могу се наћи на веб-страници <https://www.amres.ac.rs/institucije/digitalni-sertifikati/>.

За све додатне информације корисници се могу обратити путем имејл адресе tcs@amres.ac.rs.