AMPEC
Академска мрежа Србије

Упутство за регистрацију AMPEC корисника за коришћење TCS услуге и пријаву организације за SCM портал

Историја верзија документа

Верзија	Датум	Иницијали аутора	Опис промене
2.0		АТ	Друга верзија овог документа

Садржај

1 Увод

Да би проверу података о AMPEC кориснику учинили транспаретном за GÉANT, подаци о AMPEC кориснику у захтеву за издавање сертификата, морају бити доступни и усклађени са подацима наведеним на порталу Регистра. Услови, права и обавезе за коришћење дигиталних сертификата (дефинисани од стране организације GÉANT) прописују да са основним предусловима коришћења дигиталних сертификата мора бити упознат AMPEC корисник, односно његов именовани административни контакт. Именовани административни контакт заступа AMPEC корисника, корисника TCS услуге, у поступцима захтевања, добијања, обнављања и опозивања дигиталних сертификата. Због тога сви AMPEC корисници који желе да користе ово право, морају претходно да прођу кроз процес регистрације за коришћење TCS услуге. Регистрација за коришћење TCS услуге се врши преко портала Регистар.

Регистрација AMPEC корисника за коришћење TCS услуге се врши само једанпут. Након успешне регистрације, AMPEC корисник мора пријавити организацију и добити приступ TCS CSM порталу, а затим може захтевати неограничен број дигиталних сертификата за своје кориснике и сервере. Уколико дође до промене података који су наведени у оригиналном документу Сагласност за коришћење услуге издавања TCS сертификата, AMPEC корисник је дужан да о томе обавести AMPEC, промени податке на порталу Регистра и пошаље нови документ Сагласност за коришћење услуге издавања TCS сертификата са ажурираним подацима.

Регистрација за коришћење TCS услуге је врло једноставна и врши се у неколико корака који су описани у наставку документа.

2 Поступак регистације за коришћење TCS услуге

Захтев за регистрацију AMPEC корисника за коришћење TCS услуге може поднети административни контакт у неколико једноставних корака.

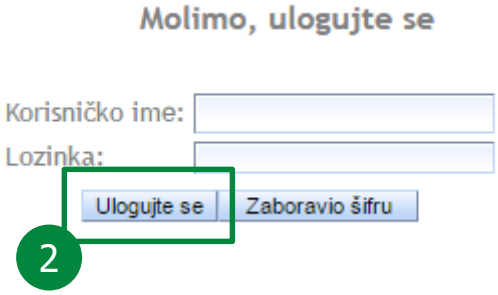
КОРАК 1

Потребно је да административни контакт институције преко Интернет прегледача приступи порталу Регистра и на почетној страни одабере опцију „Улогујте се" (1) .

Слика 1

КОРАК 2

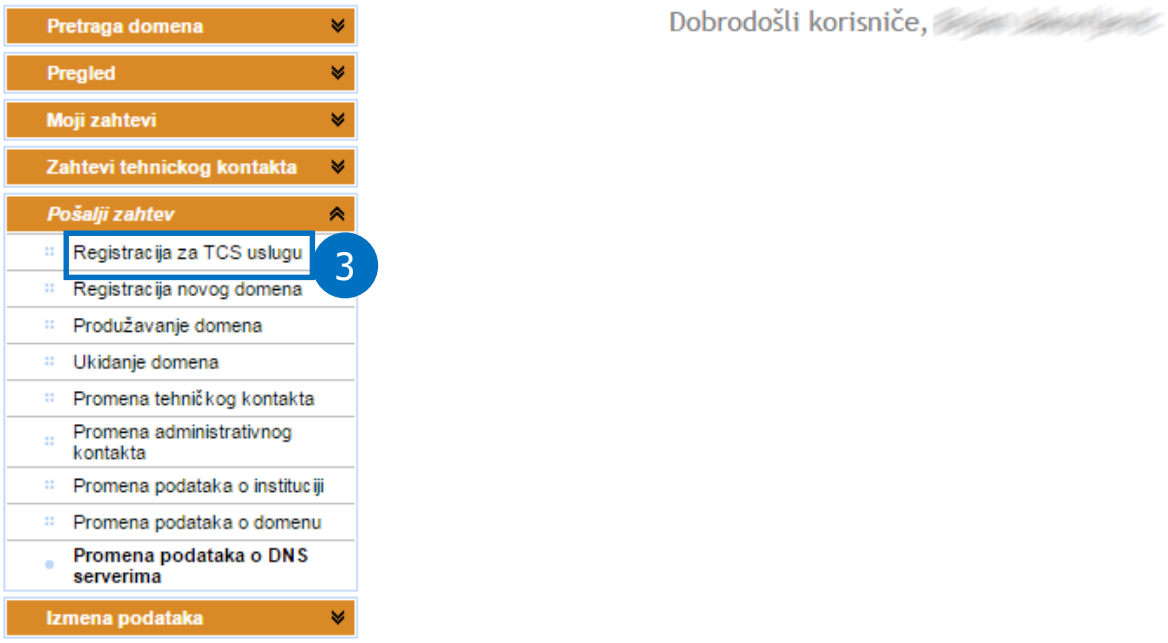
На страници за пријаву корисника, потребно је у одговарајућа поља унети креденцијале налога који административни корисник има на порталу, а потом притиснути дугме „Улогујте се" (2) .



Слика 2

КОРАК 3

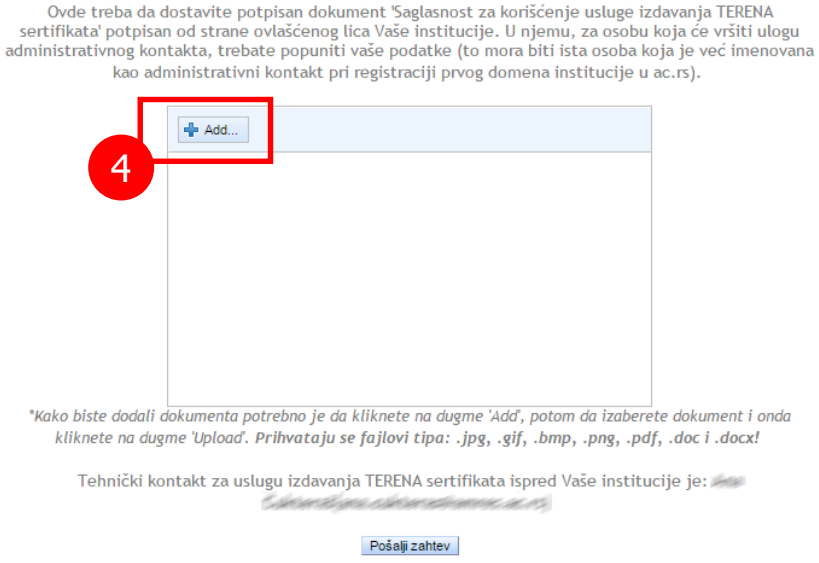
Након успешног приступа порталу, кориснику ће се приказати главна страница Регистра намењена административном контакту. Потребно је у менију са леве стране, у секцији „Пошаљи захтев" одабрати опцију „Регистрација за TCS услугу" (3).



Слика 3

КОРАК 4

На новој страници корисник има могућност да у оквиру свог захтева пошаље скениран, попуњен, оверен и потписан документ Сагласност за коришћење услуге издавања TCS сертификата. Да би административни контакт одабрао документ на свом рачунару који треба послати у захтеву, неопходно је да притисне дугме „Add…" (4) и потом одабере одговарајући документ на локалном рачунару.

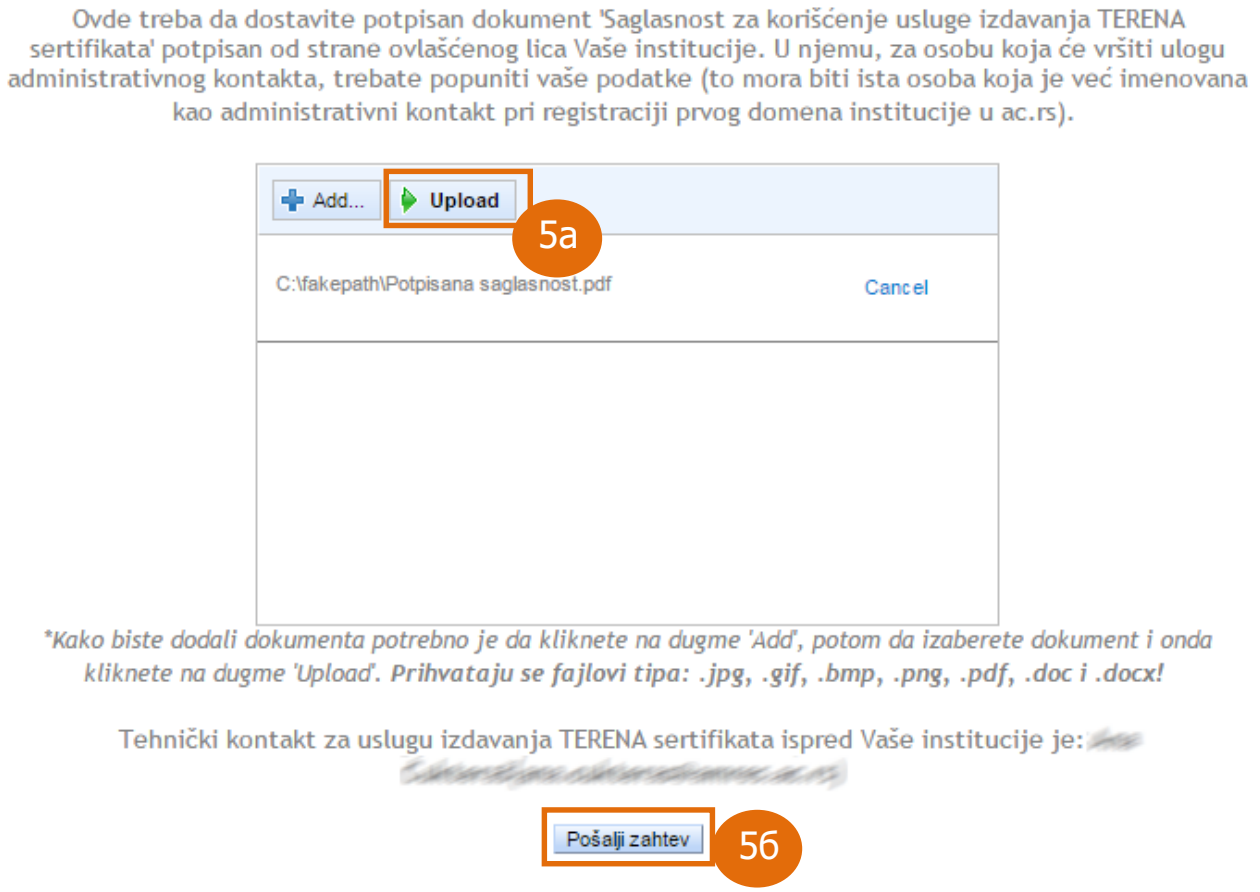


Слика 4

КОРАК 5

Након одабира документа са локалног рачунара потребно је извршити слање документа са локалног рачунара на портал Регистра. Неопходно је да административни контакт притисне дугме „Upload" (5а).

Након што портал обавести корисника да је документ успешно послат, потребно је притиснути дугме „Пошаљи захтев" (5б) како би захтев AMPEC корисника био прослеђен AMPEC-у на проверу.



Слика 5

Након слања захтева, AMPEC ће у најкраћем року прегледати захтев AMPEC корисника и уколико су сви подаци у документу Сагласност за коришћење услуге издавања TCS сертификата у складу са подацима излистаним на порталу Регистра, AMPEC ће имејл поруком потврдити пријем AMPEC корисника у TCS сервис.

3 Поступак пријаве организације за SCM портал

Након успешне регистрације AMPEC корисника за TCS услугу, корисник TCS услуге, тј. TCS администратор треба да пријави организацију и добије приступ SCM порталу, тако што попуни образац Пријава организације AMPEC корисника за SCM портал и пошаље на адресу tcs@amres.ac.rs. Образац садржи:

- податке о организацији - основној јединици TCS портала, која треба да буде креирана на порталу и која представља правно лице које има право да захтева и прибавља TCS дигиталне сертификате,
- податке о TCS административном контакту, коме ће бити креиран налог на порталу и коме ће ова организација бити делегирана, а који се морају поклапати са подацима из документа Сагласност за коришћење услуге издавања TCS сертификата.

3.1 Подаци о организацији

Како би пријавио организацију за SCM портал, AMPEC корисник, корисник TCS услуге попуњава основне податке о својој организацији и то: званичан назив, адресу, град, поштански број, државу, ПИБ и матични број. Корисник може да одабере на ком ће језику и у којој форми пријавити организацију, све док она може да буде валидирана успешно.

Како би на порталу било омогућено захтевање и издавање Grid сертификата, потребно је специфицирати и валидирати и додатно име организације у ASCII формату. Ова функционалност може бити додата накнадно.

Додатно, потребно је одлучити да ли AMPEC корисник жели могућност обнављања приватног кључа S/MIME клијентског сертификата. У оквиру SCM портала клијентски сертификати се издају и преузимају у *PKCS#12* формату, а екстензија фајла је *.p12*. Процес генерисања пара кључева клијентског сертификата се одвија на страни сервера, кликом на линк за преузимање сертификата и након преузимања фајла, процес је завршен и SCM нема више приступ приватном кључу. Међутим, може постојати потреба да се обнови и поврати приватни кључ крајњег корисника како би се декриптовали подаци ако је, на пример, оригинални клијентски сертификат који је припадао крајњем кориснику изгубљен или је крајњи корисник напустио институцију.

Из тог разлога, уколико се за организацију омогући опција "*Allow Key Recovery by Organization Administrators*", сваки креирани приватни кључ клијентског сертификата се енкриптује мастер јавним кључем администратора (сви нивои администратора имају ову могућност), док се приликом иницијализације енкрипције за организацију на самом порталу извршава сама активност генерисања пара мастер кључева, а мастер приватни кључ се мора сачувати на сигурној локацији. Поступак иницијализације енкрипције за организацију извршава се само једном, извршава је први администратор током првог приступа порталу и он је одговоран за мастер приватни кључ. У овом случају није могуће захтевати клијентске сертификате док се овај процес не заврши.

Сви приватни кључеви клијентских сертификата крајњих корисника сада су енкриптовани мастер јавним кључем администратора који је започео овај процес. За декрипцију, тј. за поновно преузимање приватног кључа крајњег корисника са портала, потребан је мастер приватни кључ администратора који је претходно сачуван. У случају преузимања клијентског сертификата са портала до тада активни сертификат постаје опозван и тиме неважећи.

Уколико се мастер приватни кључ администратора компромитује, могуће је поново енкриптовати постојећи пар кључева крајњих корисника новим мастер јавним кључем администратора, при чему је потребно поново сачувати мастер приватни кључ.

Ова опција се дефинише у тренутку креирања организације, као и сектора, и више се не може мењати.

Више детаља о овој функционалности достуно је у SECTIGO бази знања.

НАПОМЕНА: Уколико је ова опција омогућена на RAO нивоу, биће омогућена за све RAO администраторе и сви ће имати приступ приватним кључевима сертификата, уколико имају приступ мастер приватном кључу. У случају креирања сектора (Departments), потребно је искључити, тј. онемогућити ову опцију за MRAO и DRAO администраотре, тј. само RAO администратор треба да има ову могућност, уколико се одлучи за ову опцију. Додатно, постоје корисници који желе да избегну да се њихов приватни кључ генерише и чува на страни сервера. Уколико је RAO администратор сигуран да то није случај и сигуран у начин чувања свог мастер приватног кључа, може да користи ову функционалност, у супротном је препорука да се ова опција не користи из сигурносних разлога. Такође, ова функционалност се није користила ни у претходним фазама пружања TCS услуге.

3.2 Подаци о TCS администратору (RAO)

Како би пријавио RAO администратора за CSM портал, TCS администратор попуњава основне податке: име, презиме, имејл, жељено корисничко име и организације које су му делегиране на порталу уколико постоје.

Административни контакт може да захтева креирање и валидацију једне или више организација. Додатне организације могу се захтевати и накнадно, користећи исту процедуру. У овом случају је потребно специфицирати администратора који је већ креиран на порталу, специфицирати организацију или организације које су му већ додељене и њему ће бити дозвољен приступ додатној новокреираној организацији.

Административни контакт ће путем имејла бити обавештен о креираном налогу и параметрима за приступ SCM порталу.

4 Закључак

Након успешне пријаве организације и отварања администраторског налога (RAO) на SCM порталу, AMPEC корисник:

1. мора да дефинише нову лозинку приликом првог логовања на портал;
2. ОПЦИОНО: може да иницира процес енкрипције и сачува мастер приватни кључ уколико одабере ову могућност у току пријаве;
3. мора да прође кроз процедуру креирања и валидације домена;
4. може да креира друге администраторе своје организације (RAO), секторе (Departments) у оквиру организације и администраотре сектора (DRAO);
5. може да подеси нотификације на порталу;
6. може да захтева сертификате, након што прође процедуру креирања и валидације домена и након што је организација валидирана од стране MRAO администратора.

Детаљније информације о овим корацима налазе се у Упутству за RAO и DRAO администраторе.