



Упутство за RAO и DRAO администраторе

Историја верзија документа

Верзија	Датум	Иницијали аутора	Опис промене
3.0		АТ	Трећа верзија овог документа

Садржај

1	УВОД	4
2	ПРИСТУП SCM ПОРТАЛУ	5
2.1	ПРИСТУП SCM ПОРТАЛУ - DRAO.....	10
3	ПОСТУПАК КРЕИРАЊА И ВАЛИДАЦИЈЕ ДОМЕНА	11
3.1	ОДОБРЕЊЕ ДОМЕНА КОЈЕ ЈЕ ЗАХТЕВАО DRAO АДМИНИСТРАТОР.....	16
3.2	ПОСТУПАК КРЕИРАЊА И ВАЛИДАЦИЈЕ ДОМЕНА - DRAO.....	16
4	ПОСТУПАК КРЕИРАЊА ДРУГИХ АДМИНИСТРАТОРА И СЕКТОРА.....	16
4.1	ПОСТУПАК КРЕИРАЊА СЕКТОРА.....	16
4.2	ПОСТУПАК КРЕИРАЊА RAO АДМИНИСТРАТОРА	18
4.3	ПОСТУПАК КРЕИРАЊА DRAO АДМИНИСТРАТОРА.....	19
4.3.1	ПОСТУПАК КРЕИРАЊА ДРУГИХ АДМИНИСТРАТОРА И СЕКТОРА – DRAO	20
5	ПОСТУПАК ПОДЕШАВАЊА ОБАВЕШТЕЊА НА ПОРТАЛУ	20
5.1	ПОСТУПАК ПОДЕШАВАЊА ОБАВЕШТЕЊА НА ПОРТАЛУ – DRAO	21
6	ПОСТУПАК ЗАХТЕВАЊА И ПРИБАВЉАЊА СЕРТИФИКАТА.....	21
6.1	ПОСТУПАК ЗАХТЕВАЊА SSL СЕРТИФИКАТА	22
6.2	ПОСТУПАК ЗАХТЕВАЊА КЛИЈЕНТСКИХ СЕРТИФИКАТА.....	28
6.3	ПОСТУПАК ЗАХТЕВАЊА И ПРИБАВЉАЊА СЕРТИФИКАТА – DRAO	34
7	ЗАКЉУЧАК	35
	ДОДАТАК А – КРЕИРАЊЕ ЗАХТЕВА ЗА СЕРТИФИКАТ.....	35
1	КРЕИРАЊЕ ЗАХТЕВА ЗА СЕРТИФИКАТ ЗА ЈЕДНО ДОМЕНСКО ИМЕ (SSL) И ЗА СВА ПОДДОМЕНСКА ИМЕНА ЈЕДНОГ ДОМЕНА СА ВАЛИДАЦИЈОМ ОРГАНИЗАЦИЈЕ (WILDCARD)	35
2	КРЕИРАЊЕ ЗАХТЕВА ЗА СЕРТИФИКАТ ЗА ВИШЕ ДОМЕНСКИХ ИМЕНА СА ВАЛИДАЦИЈОМ ОРГАНИЗАЦИЈЕ	36

1 Увод

AMPEC је у сарадњи са организацијом GÉANT успоставио услугу издавања дигиталних сертификата TCS (*Trusted Certificate Service*), у коме регистровани AMPEC корисници имају право на прибављање неограниченог броја SSL/TLS дигиталних сертификата за потребе својих сервера и крајњих корисника.

Услуга издавања TCS сертификата се обавља преко централног SECTIGO портала (Sectigo Certificate Manager - SCM) који се налази на следећој веб-адреси:

» <https://cert-manager.com/customer/AMRES>

Портал је под контролом SECTIGO провајдера и користе га само AMPEC корисници, који су корисници TCS услуге. Преко портала се обављају све акције везане за администрацију, валидацију, захтевање и издавање TCS сертификата.

Како би AMPEC корисник добио приступ TSC **SCM порталу** потребно је испунити следеће предуслове:

1. AMPEC корисник има регистрован домен у оквиру домена „ac.rs“;
2. AMPEC корисник се регистровао за коришћење TCS услуге;
3. AMPEC корисник је комплетирао процедуру пријаве организације за SCM портал;
4. Административни контакт је примио обавештење о креираном RAO налогу и организацији.

SCM портал разликује следеће улоге администратора:

- » **Master Registration Authority Officer (MRAO)** - Администратор највишег нивоа који може приступити свим областима и функционалностима SCM. Има контролу над сертификатима, доменима и обавештењима свих организација и сектора. MRAO администратори могу да креирају и постављају привилегије RAO и DRAO администраторима. AMPEC има MRAO улогу на порталу.
- » **Registration Authority Officer (RAO)** - Администратор кога је креирао MRAO или други RAO у циљу управљања сертификатима и администраторима организације или сектора. Може да креира секторе и DRAO администраторе за своју организацију. Ова привилегија мора бити одобрена од стране MRAO администратора у процесу креирања налога. RAO администратори не могу креирати нове организације нити уређивати опште податке организације чак и ако им је делегирана контрола над том организацијом.
- » **Department Registration Authority Officer (DRAO)** – Администратор кога је креирао RAO или други DRAO у циљу управљања сертификатима и администраторима сектора. Може да креира DRAO администраторе за свој сектор. DRAO администратори могу имати приступ и захтевати сертификате само за сектор који им је делегиран.

TCS административни контакт чији су подаци достављени у документу **Пријава организације AMPEC корисника за TCS портал** аутоматски постаје RAO администратор. Он има могућност да креира налоге за администраторе свог или нижег нивоа. Како би RAO администратор имао могућност захтевања дигиталних сертификата, неопходно је да прође следеће кораке:

1. Приликом првог логовања на портал потребно је дефинисати нову лозинку;
2. ОПЦИОНО: иницирати процес енкрипције и сачувати мастер приватни кључ на сигурном месту, уколико се одабере ова могућност у току процедуре пријаве;
3. Проћи кроз процедуру креирања и валидације домена;
4. ОПЦИОНО: креирати друге администраторе своје организације (RAO), секторе (Departments) у оквиру организације и администраторе сектора (DRAO);

5. ОПЦИОНО: подесити обавештења на порталу;
6. Захтевати сертификате, након што је организација валидирана од стране MRAO администратора и након што прође процедуру креирања и валидације домена.

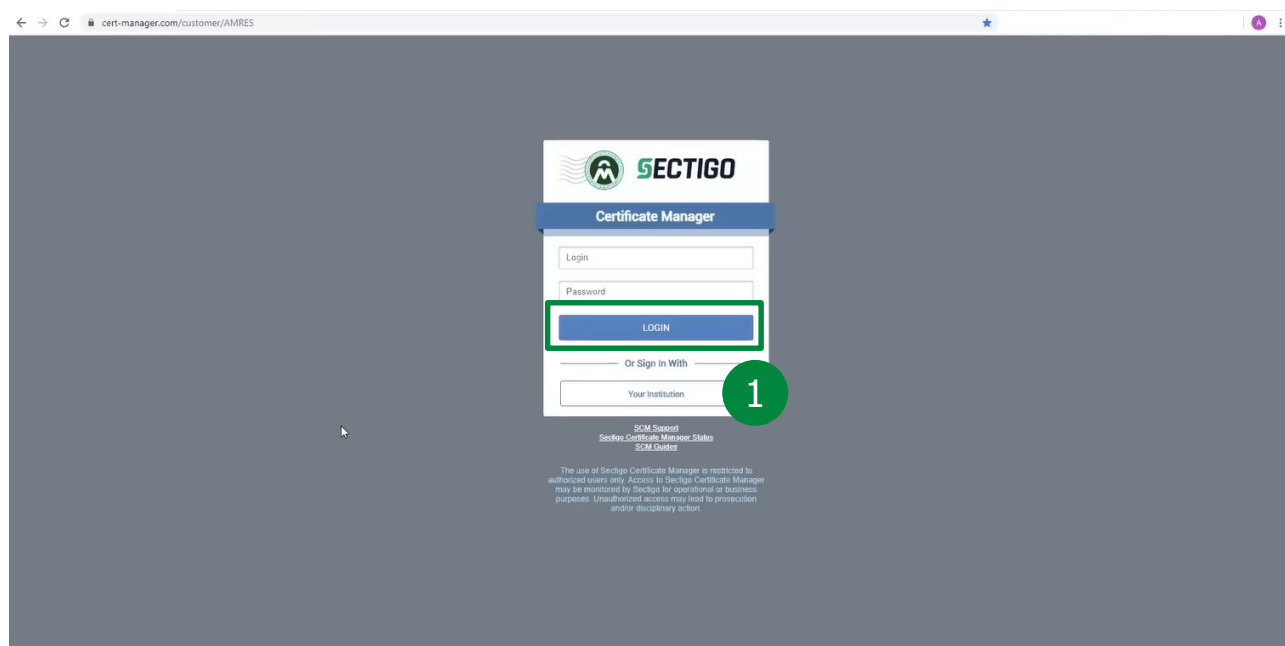
У наставку документа детаљно су описани наведени кораци.

2 Приступ SCM порталу

Након успешне регистрације AMRES корисника за коришћење TCS услуге и завршене процедуре пријаве организације, TCS администратор добија улогу RAO администратора на SCM порталу и добија корисничко име и шифру, за приступање порталу.

КОРАК 1

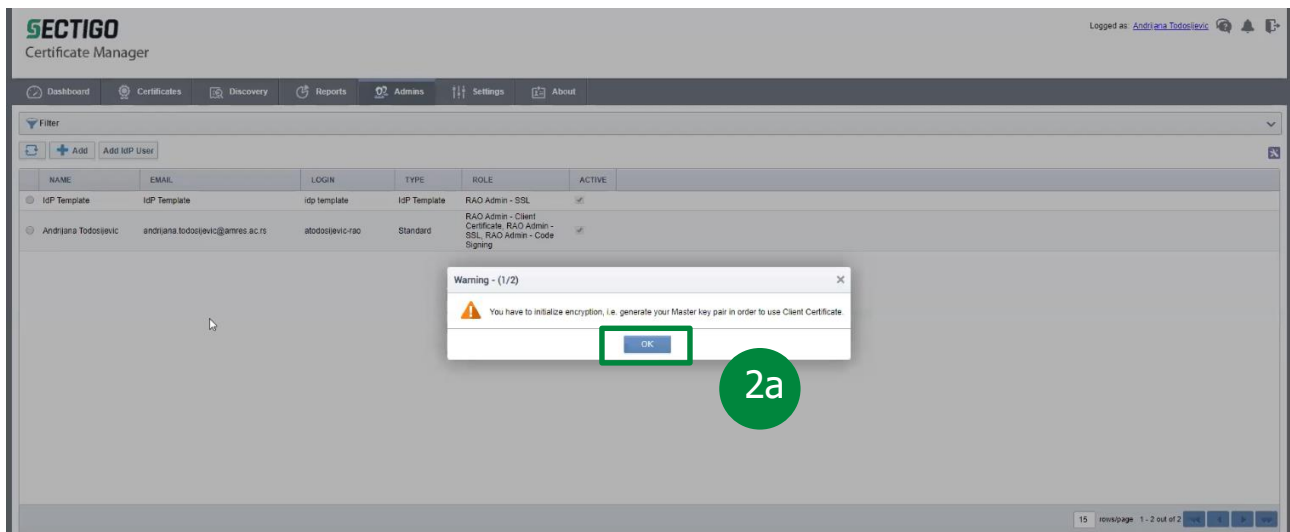
RAO администратор приступа порталу који је доступан на адреси <https://cert-manager.com/customer/AMRES>.



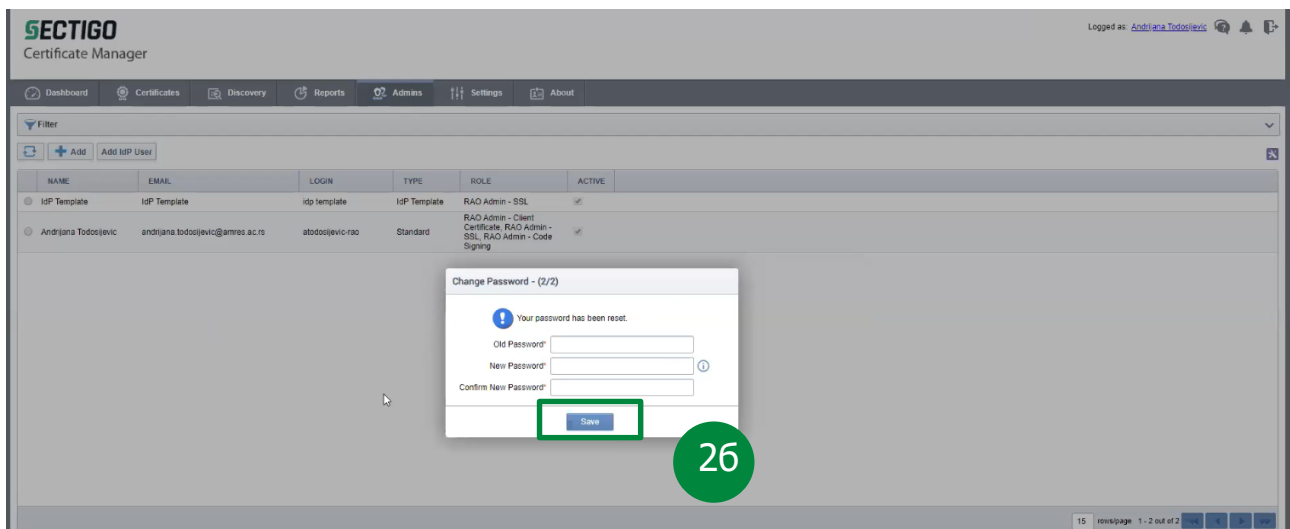
Након уноса корисничког имена и шифре која је добијена од стране MRAO, потребно је кликнути на дугме **LOGIN** (1).

КОРАК 2

ОПЦИОНО: Када RAO први пут уђе на портал, уколико је омогућена опција преузимања кључа клијентског сертификата за RAO, појавиће се упозорење да је потребно иницијализовати енкрипцију.



Након што RAO кликне на дугме **OK (2a)**, појавиће се прозор који захтева дефинисање нове шифре:

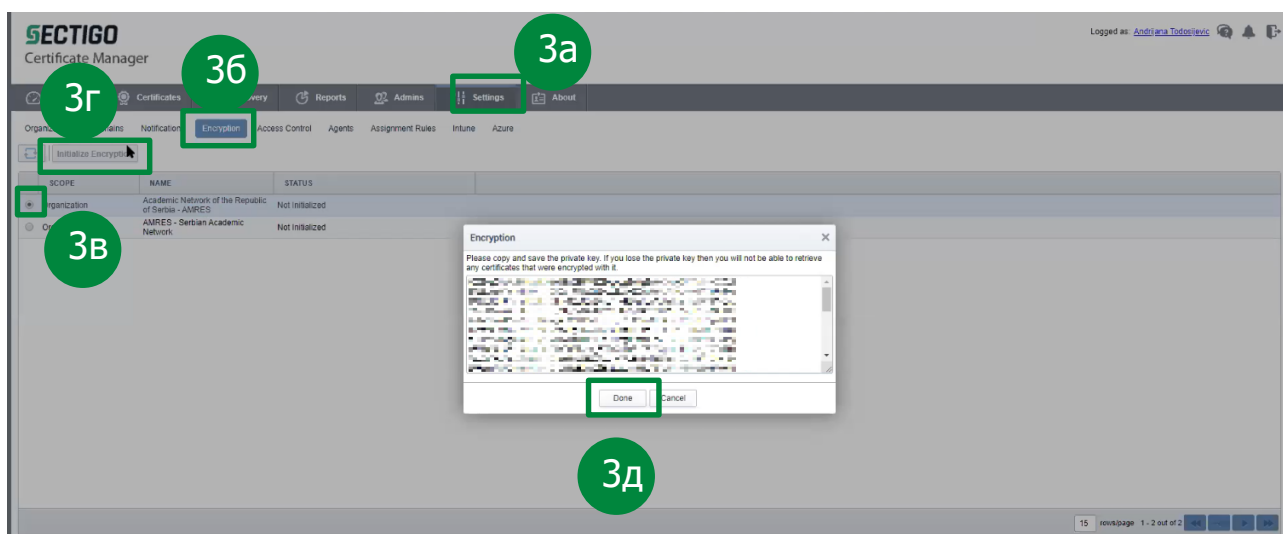


RAO треба да ресетује шифру и затвори прозор кликом на дугме **SAVE (26)**, а затим на **OK**.

КОРАК 3

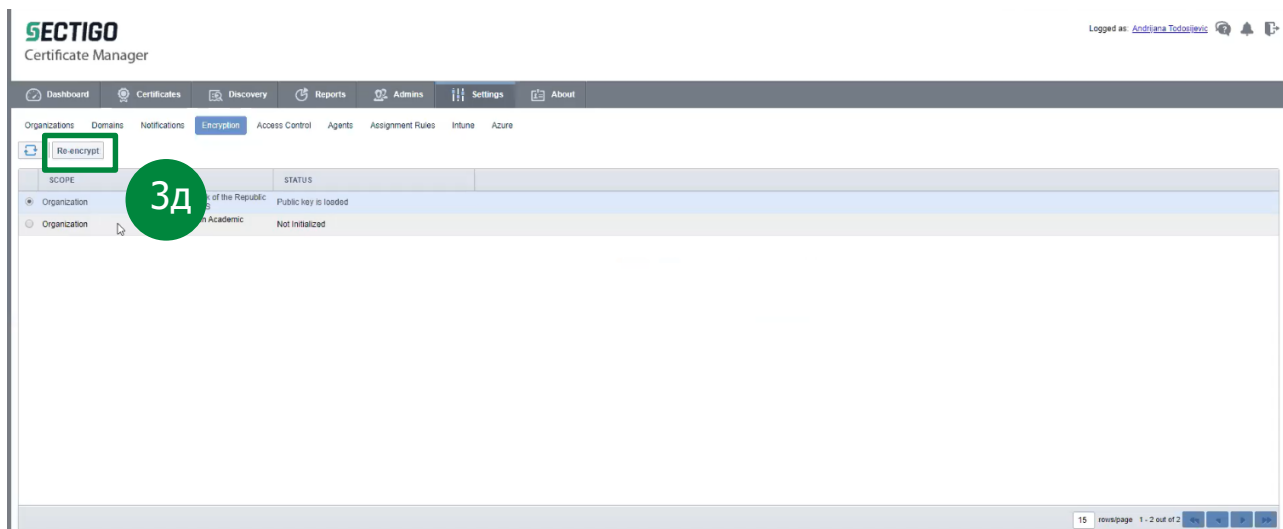
ОПЦИОНО: Уколико је омогућена опција преузимања кључа клијентског сертификата, потребно је иницијализовати енкрипцију и генерисати пар мастер кључева. Потребно је у главном менију одабрати опцију **Settings (3a)**, затим у менију другог нивоа опцију **Encryption (36)**, затим кликнути на организацију **(3в)** па на дугме **Initialize Encryption (3г)**. Појавиће се *pop-up* прозор који садржи мастер приватни кључ који је у овом тренутку потребно копирати и сачувати на сигурној локацији. Након тога потребно је завршити овај процес кликом на **Done (3д)**.

Исти поступак пролази и DRAO администратор када приступа сектору коју му је додељен.



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

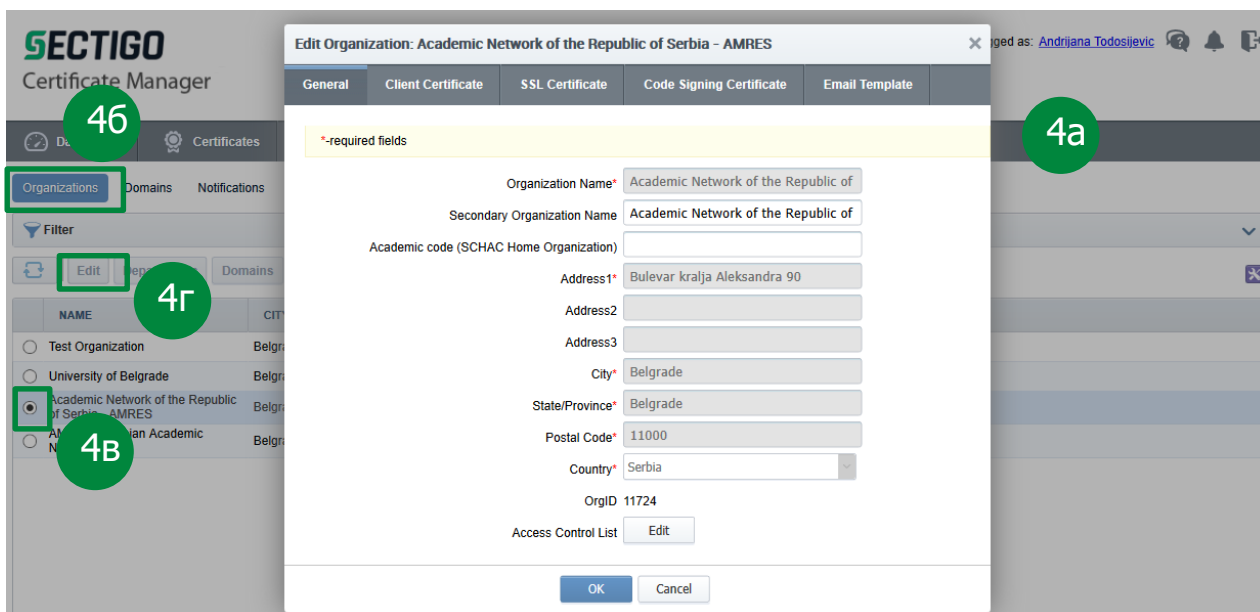
Сада је пар мастер кључева креиран и RAO има приступ само опцији *Re-encrypt* (3д).



У случају преузимања приватног кључа клијентског сертификата са портала до тада активни сертификат постаје опозван и тиме неважећи.

КОРАК 4

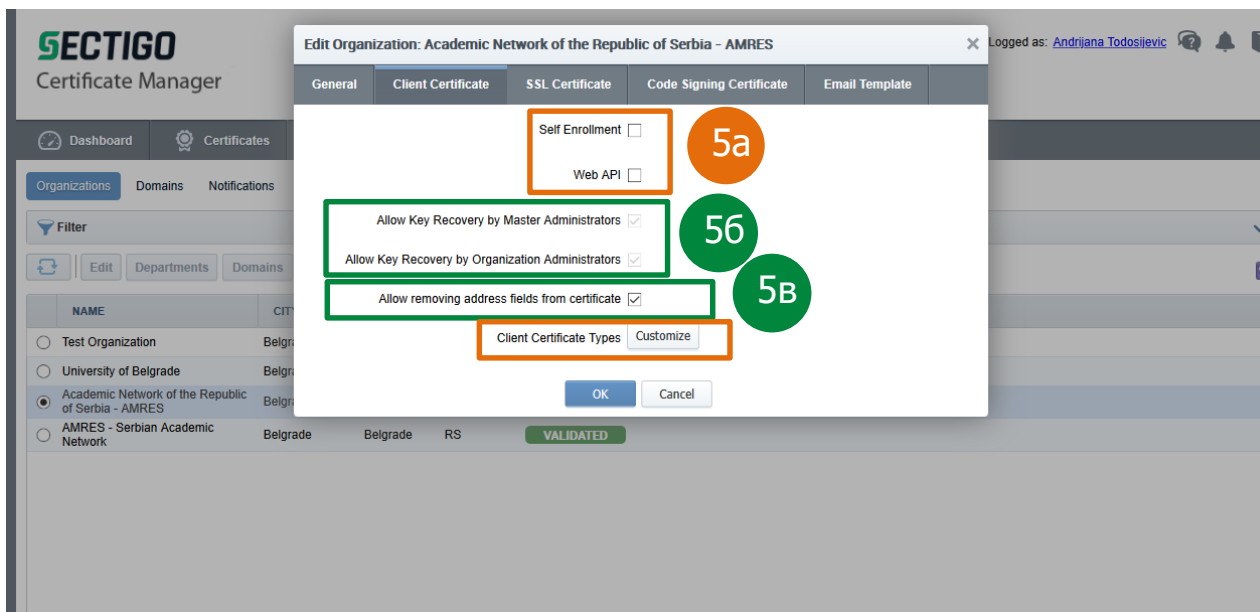
RAO администратор сада има приступ организацији која му је делегирана. RAO администратор може да приступи организацији тако што у главном менију одабере опцију *Settings* (4а), затим у менију другог нивоа прву у низу опцију *Organizations* (4б), затим кликне на организацију (4в) па на дугме *Edit* (4г).



Након овог корака отвара се прозор у коме се налазе подаци и подешавања организације. Први таб *General* приказује опште информације о организацији. Њих дефинише MRAO и они се не могу мењати:

- ❖ Званичан назив организације;
- ❖ Додатни назив организације – званичан назив у ACSII формату, који је услов за захтевање и издавање *Grid* сертификата;
- ❖ Академски код организације – атрибут потребан за пријаву путем SAML протокола, чија је имплементација у припреми, углавном садржи домен институције и може се додати накнадно;
- ❖ Адреса, Град, Поштански број, Држава;
- ❖ Поље *State* – обавезно поље у сертификату, за државе које немају *State/Country* уређење уноси се назив града.
- ❖ *ACL* - листе за контролу приступа која може бити подешена на нивоу организације.

Затим следи таб *Client Certificate*.



КОРАК 5

У оквиру табла *Client Certificate* подешавају се опције у вези са издавањем клијентских сертификата за организацију. *Self Enrollment* и *Web API* (5a) су опције захтевања клијентских сертификата од стране крајњих корисника. Уколико је омогућена *Self Enrollment* опција RAO може да подеси Приступни код који крајњи корисници користе приликом захтевања сертификата путем линка <https://cert-manager.com/customer/AMRES/smime>. Додатно, RAO може да одабере који типови клијентских сертификата и ког трајања ће бити дозвољени у случају коришћења *Self Enrollment* форме. Такође, уколико је омогућена *Web API* опција RAO може да подеси шифру која се користи приликом употребе Web API. Ове функционалности су објашњене у **SECTIGO бази знања** и нису предмет овог упутства.

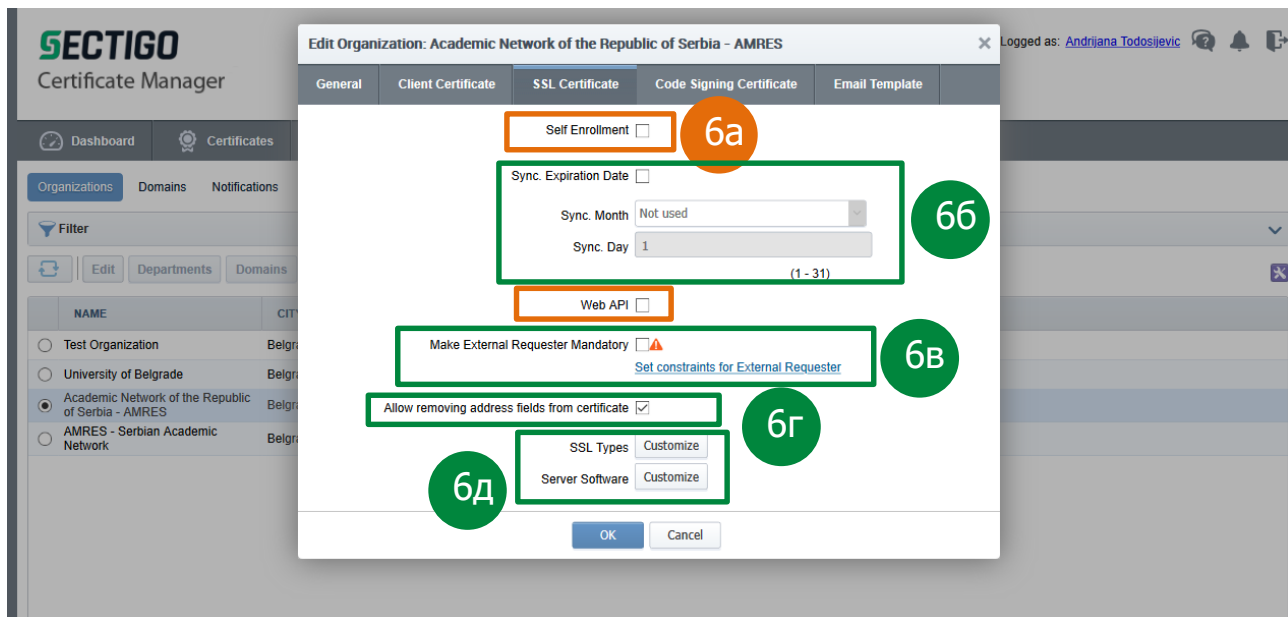
НАПОМЕНА: Уколико се омогући *Self Enrollment* опција сви корисници који имају Приступни код и приступ имејлу у домену институције моћи ће да захтевају сертификате, без додатне контроле. Препорука је да се ова опција не користи. Аутоматска контрола је могућа коришћењем SAML протокола који тренутно није подржан за AMRES и у плану је његова имплементација.

У оквиру табла *Client Certificate* налазе се и опције у вези са могућношћу опоравка и преузимања кључева клијентских сертификата (5б). Ове опције су подешене од стране MRAO администратора у зависности од изабране опције током пријаве организације на SCM портал. Ове опције се не могу накнадно мењати.

Затим, ту је и опција којом се дозвољава да се током креирања из самог сертификата уклони поље које садржи адресу (5в). Ова опција је правила проблеме приликом издавања сертификата и препорука је да се поље које садржи адресу не уклања, иако ова могућност постоји.

КОРАК 6

У оквиру табла *SSL Certificate* подешавају се опције у вези са издавањем серверских сертификата за организацију.



Self Enrollment и *Web API* (6a) су опције захтевања SSL сертификата од стране крајњих корисника. Уколико је омогућена *Self Enrollment* опција RAO може да подеси Приступни код који крајњи корисници користе приликом захтевања сертификата путем линка <https://cert-manager.com/customer/AMRES/ssl>.

НАПОМЕНА: Приликом захтевања сертификата, имејл адреса корисника се не проверава и свако ко има Приступни код може захтевати сертификат. Уколико се ова опција користи потребна је контрола сваког захтева. Препорука је да се ова опција не користи. Аутоматска контрола је могућа коришћењем SAML протокола који тренутно није подржан за AMRES и у плану је његова имплементација.

Такође, уколико је омогућена *Web API* опција RAO може да подеси шифру која се користи приликом употребе *Web API*. Ове функционалности су објашњене у **SECTIGO бази знања** и нису предмет овог упутства.

У оквиру овог таба за организацију може се подесити датум истека свих сертификата, што је значајно за администраторе уколико желе да синхронизују све сертификате на порталу. Важно је напоменути да се овом опцијом не може продужити период валидности сертификата, већ само може да се скрати. Сертификати издати пре укључивања ове опције нису обухваћени овом опцијом, опција важи само уколико се сертификати обнове након тог момента (66).

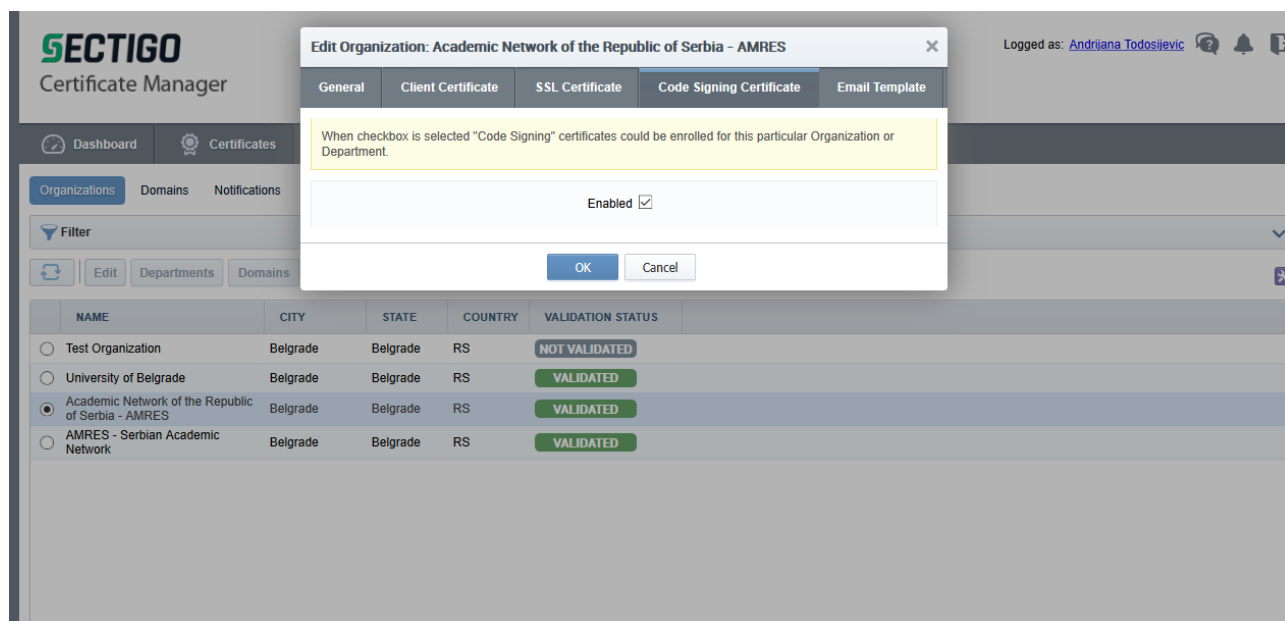
Препорука је да опција *Make External Requester Mandatory* (6в) буде искључена пошто онемогућава функционисање појединих опција за захтевања сертификата.

Затим, ту је и опција којом се дозвољава да се током креирања из самог сертификата уклони поље које садржи адресу (6г). Ова функционалност је правила проблеме приликом издавања сертификата и препорука је да се вредности ових поља не уклањају, иако ова могућност постоји.

Додатно, RAO може да одабере типове *SSL* сертификата, опције трајања и типове платформе који ће бити дозвољени за организацију када се сертификати захтевају преко портала директно (*Admin UI*) и путем *Self Enrollment* форме (6д).

КОРАК 7

У оквиру таба *Code Signing Certificate* дозвољава се захтевање и издавање сертификата за потписивање кода за организацију.



SECTIGO Certificate Manager

Logged as: [Andriana Todosijevic](#)

When checkbox is selected "Code Signing" certificates could be enrolled for this particular Organization or Department.

Enabled ☒

OK Cancel

NAME	CITY	STATE	COUNTRY	VALIDATION STATUS
<input type="radio"/> Test Organization	Belgrade	Belgrade	RS	NOT VALIDATED
<input type="radio"/> University of Belgrade	Belgrade	Belgrade	RS	VALIDATED
<input checked="" type="radio"/> Academic Network of the Republic of Serbia - AMRES	Belgrade	Belgrade	RS	VALIDATED
<input type="radio"/> AMRES - Serbian Academic Network	Belgrade	Belgrade	RS	VALIDATED

КОРАК 8

Таб *Email Templates* администратору даје могућност да подеси имејл шаблоне који ће се затим користити приликом слања обавештења од стране портала.

2.1 Приступ SCM порталу - DRAO

Све опције и подешавања организације која су доступна RAO администратору такође садржи и сваки креирани сектор (Department) на порталу. Када се DRAO администратор улогује на портал може да приступи делегираном сектору и управља свим подешавањима.

3 Поступак креирања и валидације домена

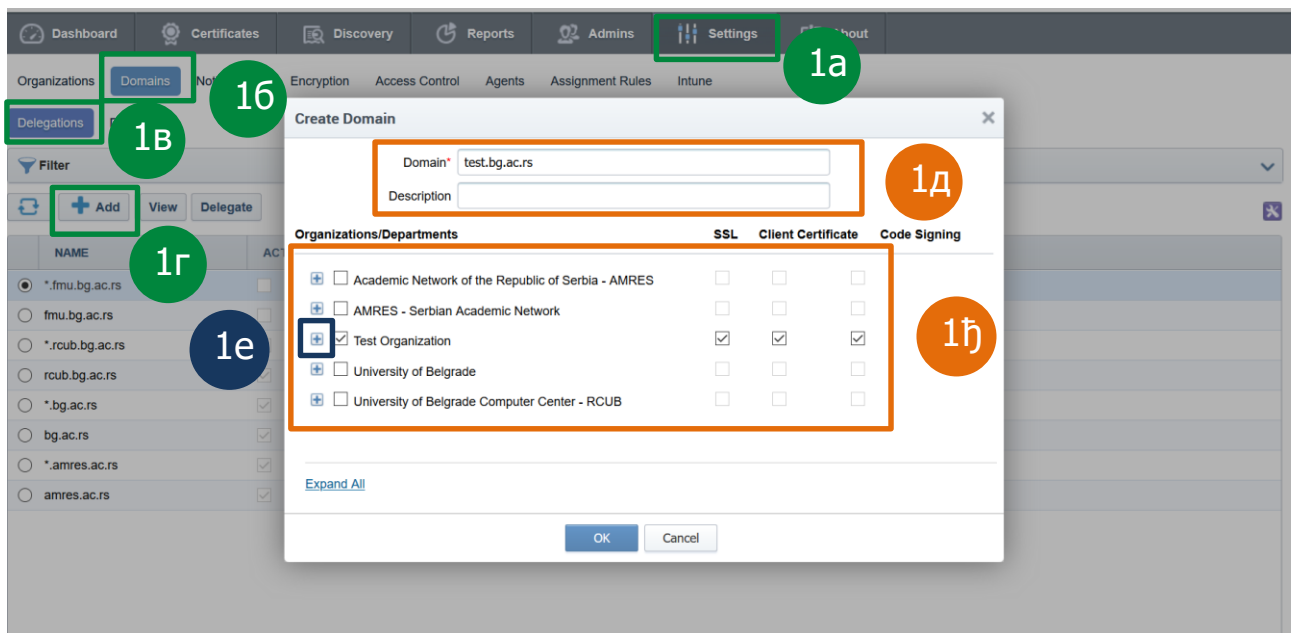
RAO може да креира и управља доменима за организацију која му је додељена. Додатно, може да делегира домене секторима (Departments).

Све креиране домене на порталу мора прво да одобри AMRES.

Како би успешно додао тј. креирао домен, портебно је да RAO креира и домен и *wildcard* домен.

КОРАК1

Како би RAO администратор додао нови домен потребно је да у главном менију одабере опцију *Settings* (1а), затим у менију другог нивоа опцију *Domains* (1б), затим кликне на *Delegations* (1в) па на дугме *Add* (1г).



Појавиће се прозор у коме је потребно унети назив домена (1д) и делегирати домен Организацији (1ђ). Када се кликне на дугме „+“ испред назива организације (1е) појавиће се сви сектори (Departments) организације, који такође могу да буду означени и на тај начин им је делегиран домен.

Администратор може да одабере које ће типове сертификата (SSL, Client, Code Signing) организација или сектор моћи да захтевају за специфицирани домен.

Након клика на дугме *OK*, новокреирани домен приказан је црвеном бојом и има Статус *Requested*. У овом моменту портебно је да MRAO одобри овај домен.

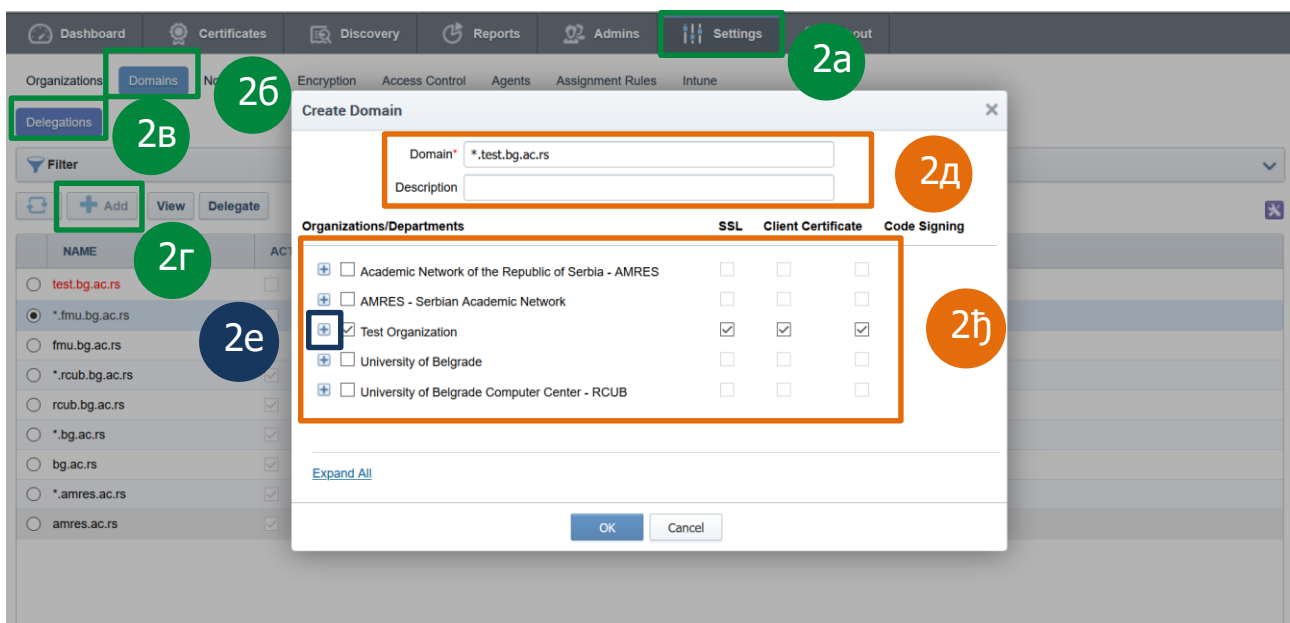
NAME	ACTIVE	DELEGATION STATUS	DATE REQUESTED	VALIDATION STATUS	DCV EXPIRATION
<input type="radio"/> test.bg.ac.rs	<input type="checkbox"/>	Requested	04/03/2020	Validated	04/03/2021
<input checked="" type="radio"/> *.fmu.bg.ac.rs	<input type="checkbox"/>	Approved	04/03/2020	Validated	04/03/2021
<input type="radio"/> fmu.bg.ac.rs	<input type="checkbox"/>	Approved	04/03/2020	Validated	04/03/2021
<input type="radio"/> *.rcub.bg.ac.rs	<input checked="" type="checkbox"/>	Approved	04/03/2020	Not Validated	
<input type="radio"/> rcub.bg.ac.rs	<input checked="" type="checkbox"/>	Approved	04/03/2020	Not Validated	
<input type="radio"/> *.bg.ac.rs	<input checked="" type="checkbox"/>	Approved	04/03/2020	Not Validated	
<input type="radio"/> bg.ac.rs	<input checked="" type="checkbox"/>	Approved	04/03/2020	Validated	04/03/2021
<input type="radio"/> *.amres.ac.rs	<input checked="" type="checkbox"/>	Approved	03/05/2020	Validated	03/06/2021
<input type="radio"/> amres.ac.rs	<input checked="" type="checkbox"/>	Approved	03/05/2020	Validated	03/06/2021

Уколико је домен институције поддомен домена који је већ валидиран на порталу, нпр. додаје се домен *test.bg.ac.rs*, а домен *bg.ac.rs* је већ креиран и валидиран, домен ће бити аутоматски валидиран.

КОРАК 2

Када се креира и делегира нови домен на SCM порталу, потребно је креирати и делегирати и *wildcard* домен истом процедуром како би све функционалности биле омогућене.

Како би RAO администратор додао *wildcard* домен, у овом примеру **.test.bg.ac.rs* потребно је да у главном менију одабере опцију *Settings* (2а), затим у менију другог нивоа опцију *Domains* (2б), затим кликне на *Delegations* (2в) па на дугме *Add* (2г).



Потребно је унети назив *wildcard* домена (2д) и делегирати домен организацији или сектору (2ђ).

Администратор може да одабере које ће типове сертификата (SSL, Client, Code Signing) организација или сектор моћи да захтевају за специфицирани домен (2e).

Након клика на дугме *OK*, новокреирани домен приказан је црвеном бојом и има Статус *Requested*. У овом моменту потребно је да MRAO одобри примарни домен.

Dashboard

Certificates

Discovery

Reports

Admins

Settings

About

Organizations

Domains

Notifications

Encryption

Access Control

Agents

Assignment Rules

Intune

Delegations

DCV

Filter

+

Add

View

Delegate

	NAME	ACTIVE	DELEGATION STATUS	DATE REQUESTED	VALIDATION ST.	DCV EXPIRATION
<input type="radio"/>	*.test.bg.ac.rs	<input type="checkbox"/>	Requested	04/03/2020	Validated	04/03/2021
<input type="radio"/>	test.bg.ac.rs	<input type="checkbox"/>	Requested	04/03/2020	Validated	04/03/2021
<input checked="" type="radio"/>	*.fmu.bg.ac.rs	<input type="checkbox"/>	Approved	04/03/2020	Validated	04/03/2021
<input type="radio"/>	fmu.bg.ac.rs	<input type="checkbox"/>	Approved	04/03/2020	Validated	04/03/2021
<input type="radio"/>	*.rcub.bg.ac.rs	<input checked="" type="checkbox"/>	Approved	04/03/2020	Not Validated	
<input type="radio"/>	rcub.bg.ac.rs	<input checked="" type="checkbox"/>	Approved	04/03/2020	Not Validated	
<input type="radio"/>	*.bg.ac.rs	<input checked="" type="checkbox"/>	Approved	04/03/2020	Not Validated	
<input type="radio"/>	bg.ac.rs	<input checked="" type="checkbox"/>	Approved	04/03/2020	Validated	04/03/2021
<input type="radio"/>	*.amres.ac.rs	<input checked="" type="checkbox"/>	Approved	03/05/2020	Validated	03/06/2021
<input type="radio"/>	amres.ac.rs	<input checked="" type="checkbox"/>	Approved	03/05/2020	Validated	03/06/2021

Након што MRAO администратор одобри примарни домен, његов статус ће се променити у *Approved*. Може се догодити да након неког времена *wildcard* домен и домени креирани у овом периоду и даље буду приказани као невалидирани. Након одређеног времена SCM ће променити њихов статус.

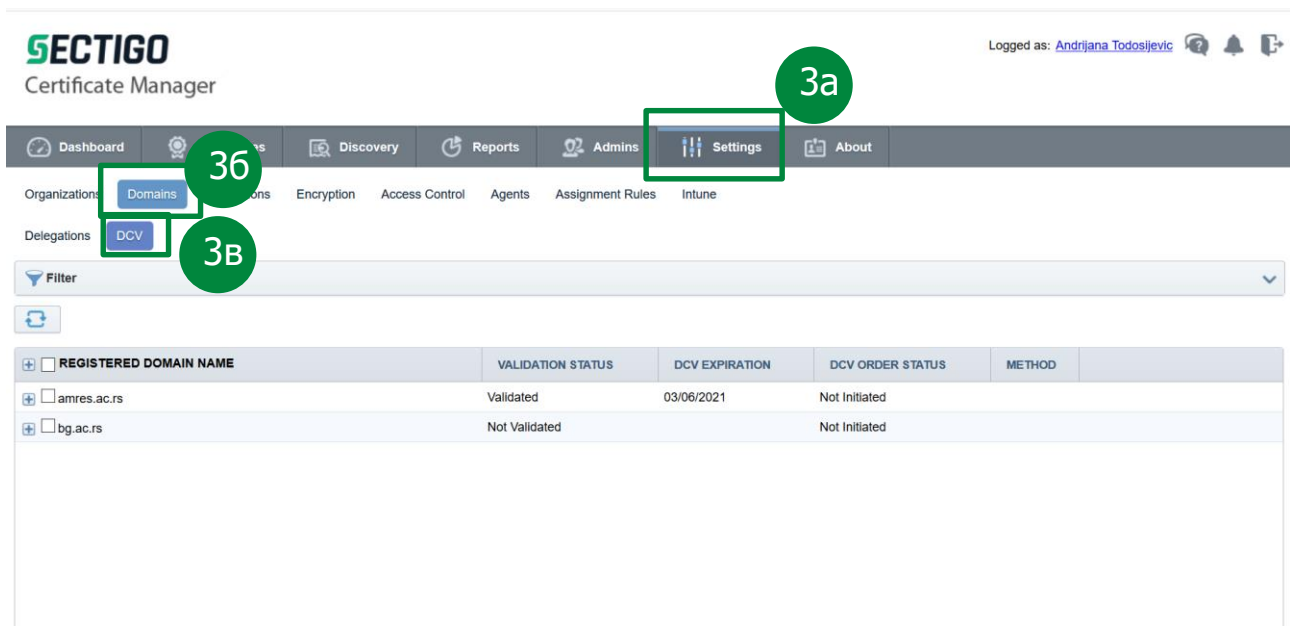
Уколико је примарни домен организације нови домен, а не поддомен неког од постојећих валидираних на порталу, RAO администратор мора да валидира домен.

КОРАК 3: ВАЛИДАЦИЈА ДОМЕНА

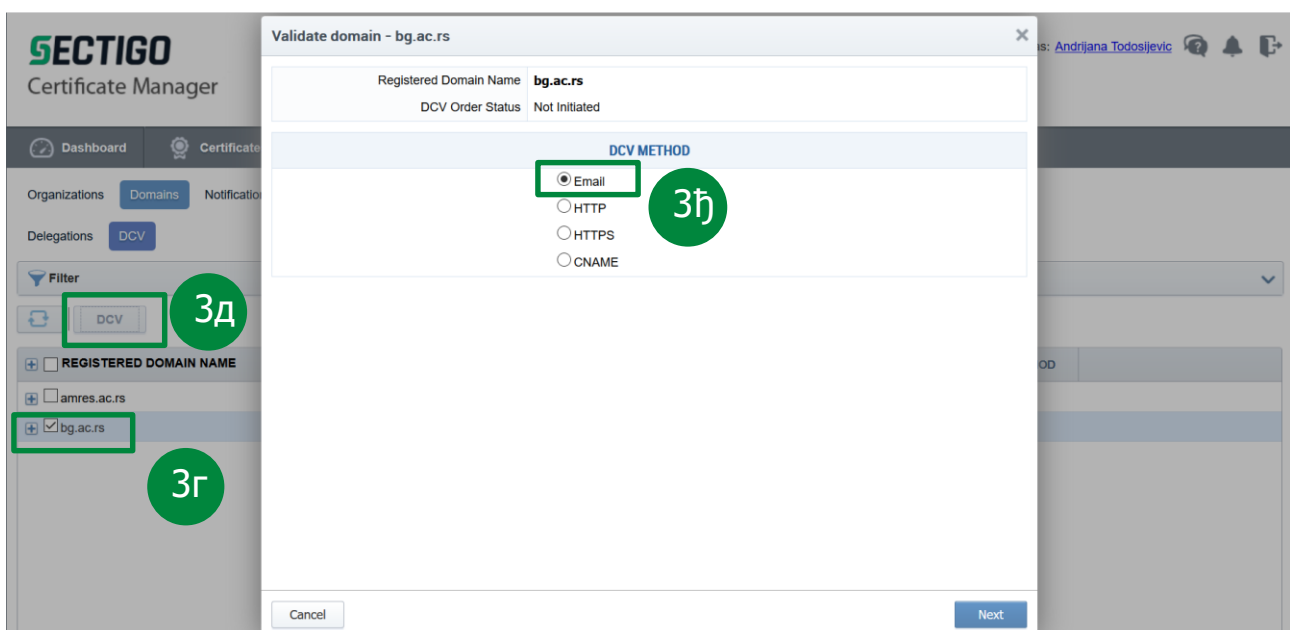
Процесом валидације домена, SECTIGO сертификациона кућа проверава да ли AMRES корисник контролише домене за које жели да прибавља сертификате. Домен се валидира на годину дана.

Као што је већ поменуто, уколико је примарни домен организације нови домен, а не поддомен неког од постојећих валидираних на порталу, RAO администратор мора да валидира домен. SECTIGO сертификациона кућа се референцира на *Public Suffix List (PSL)* листу која је доступна на https://publicsuffix.org/list/public_suffix_list.dat, што је у складу са препорукама *CAB форума* (документ BR v1.7.0 доступан на <https://cabforum.org/baseline-requirements-documents/>, секција 3.2.2.6). Наиме, уколико се на порталу додаје домен који није директан поддомен (поддомен првог нивоа) TLD домена наведених на PSL, већ поддомен вишег нивоа, портал ће аутоматски креирати поддомен првог нивоа. Само овај домен може да се валидира на порталу. Нпр. уколико корисник на порталу дода *test.bg.ac.rs* домен, аутоматски ће бити креиран домен *bg.ac.rs*, а RAO администратор ће моћи да покрене валидацију само *bg.ac.rs* домена. Уколико корисник дода домен *test.ac.rs*, моћи ће да га валидира и неће се креирати *ac.rs* домен, пошто се он налази на PSL листи, у *ICANN DOMAINS* секцији.

Како би започео валидацију домена, потребно је да RAO администратор у главном менију одабере опцију *Settings* (3a), затим у менију другог нивоа опцију *Domains* (36), а затим кликне на *DCV (Domain Control Validation)* (3b).



Затим је потребно да одабере домен који жели да валидира (3г) и кликне **DCV** (3д).

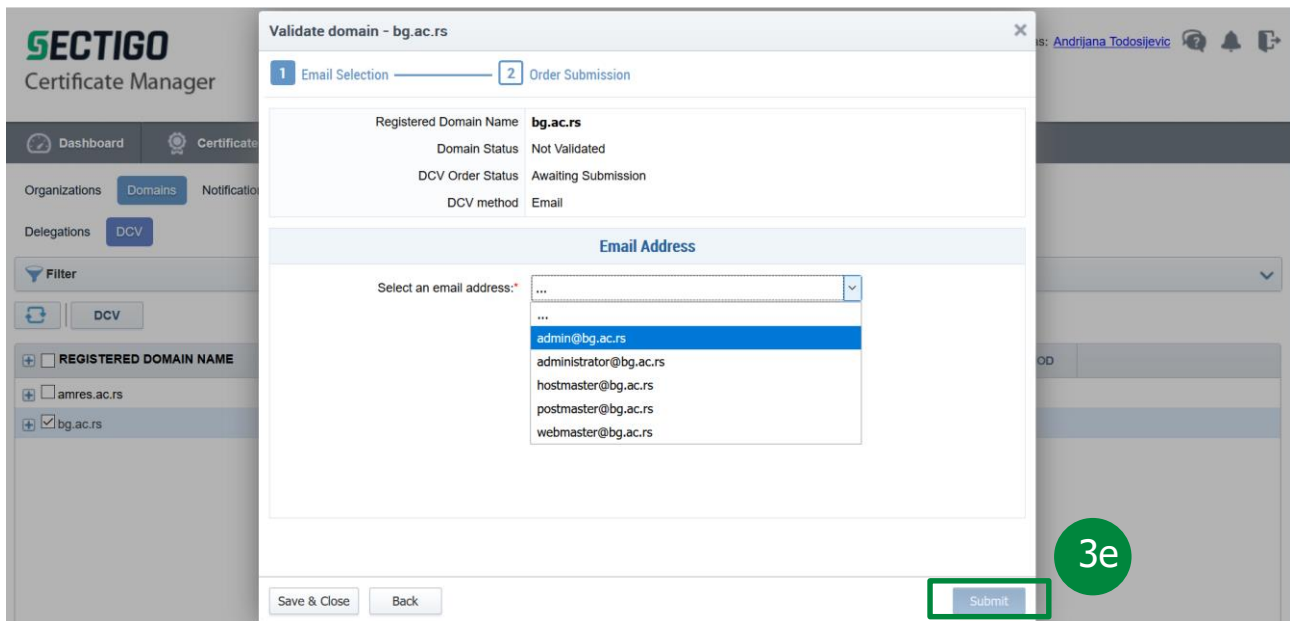


Појавиће се прозор који нуди одабир начина валидације:

- ✦ Email - ова опција подразумева слање имејла са линком за валидацију на једну од пет адреса, нпр. "admin@bg.ac.rs", "administrator@bg.ac.rs", "hostmaster@bg.ac.rs", "postmaster@bg.ac.rs" или "webmaster@bg.ac.rs";
- ✦ HTTP/HTTPS – ова опција подразумева да се .txt фајл одређене садржине коју дефинише SCM постави у *root* директоријум веб-сервера;
- ✦ CNAME - ова опција подразумева додавање CNAME записа у облику *hash* вредности у DNS зону домена који се валидира. SCM систем ће дефинисати ову вредност.

У овом упутству биће објашњена валидација путем имејла (3ђ).

Након што се одабере опција *Email* (3f) и кликне на *Next*, RAO администратор ће имати могућност да одабере имејл адресу на коју жели да пошаље линк за валидацију домена.



Након што се одабере имејл адреса за валидацију домена, потребно је кликнути на *Submit* дугме (3e) чиме се аутоматски шаље имејл на жељену адресу.

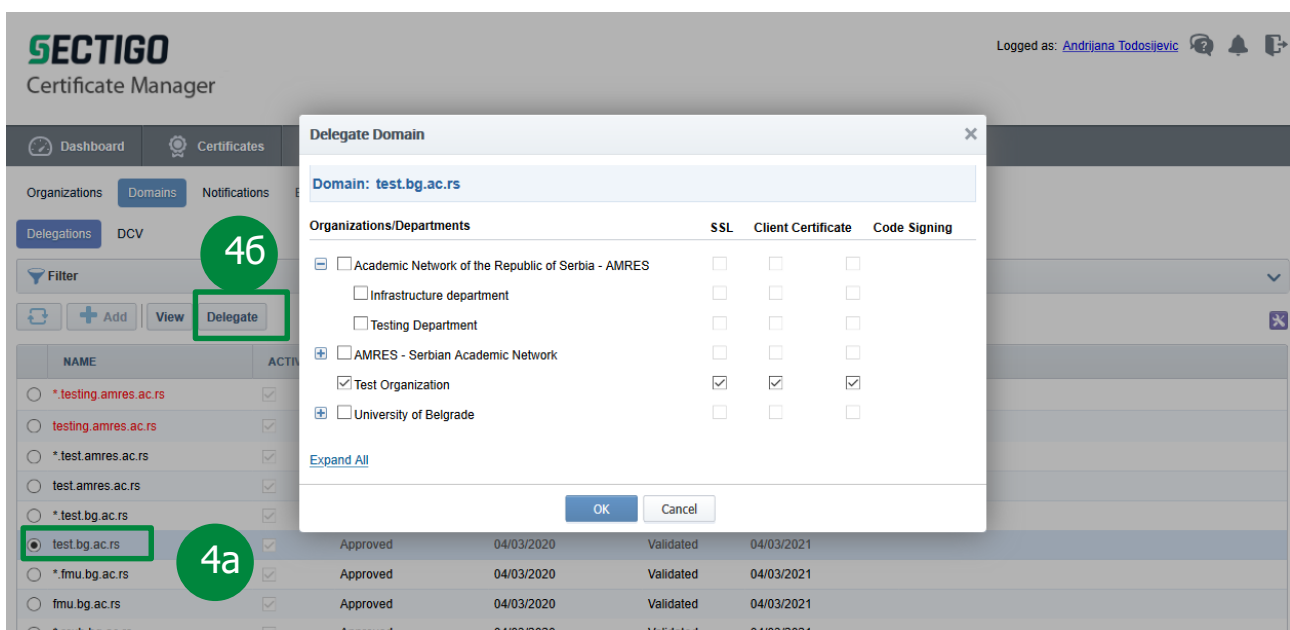
Кликом на линк из имејла (досупан кликом на реч *here*), отвориће се страница на којој је потребно унети валидациони код наведен у имејлу.

НАПОМЕНА: Након овог корака, страница може да прикаже грешку, али ће домен свакако бити валидиран.

ОПЦИОНО: КОРАК 4

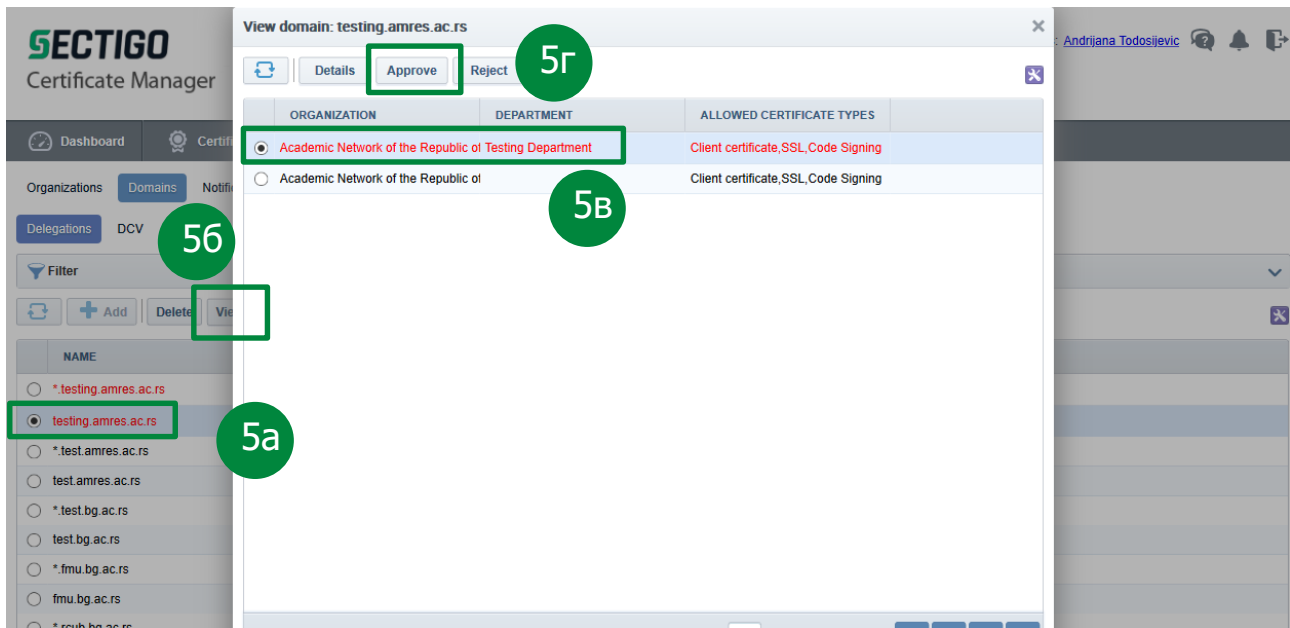
Уколико постоји потреба домен може бити накнадно делегиран нпр. другом сектору.

Потребно је да RAO администратор кликне на домен (4a), затим на *Delegate* (46) и у новом прозору одабере коме жели да делегира домен.



3.1 Одобрење домена које је захтевао DRAO администратор

DRAO администратор може да креира домен и делегира га секторима који су му додељени. У овом случају потребно је одобрење од стране RAO администратора. Како би одобрио захтевани домен, потребно је да RAO администратор кликне на домен (5a), па на *View* (5б). Након што се појави нови прозор одабере се сектор на који се захтев односи (5в) и кликне *Approve* (5г).



3.2 Поступак креирања и валидације домена - DRAO

DRAO администратор пролази исте кораке у поступку додавања, валидације и делегирања домена на порталу. Домене које је додато DRAO администратор мора да одобри RAO администратор.

4 Посупак креирања других администратора и сектора

RAO администратор у оквиру своје организације може да креира:

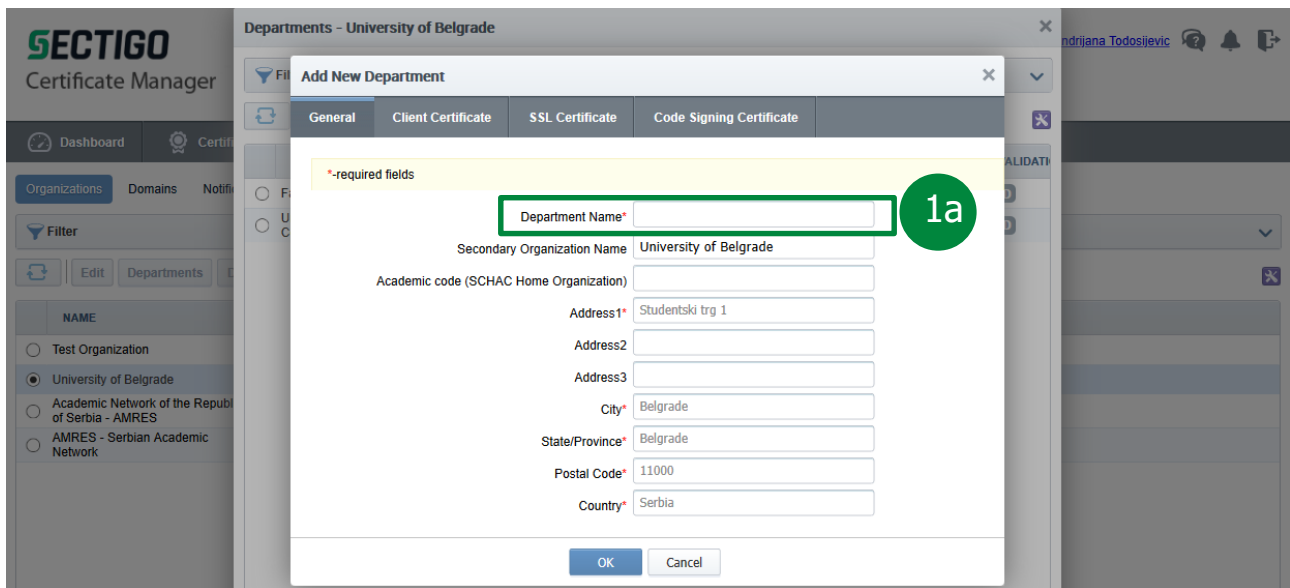
- ⌘ Друге RAO администраторе;
- ⌘ Секторе (Departments);
- ⌘ DRAO администраторе.

4.1 Поступак креирања сектора

Сваки сектор на порталу има све особине, а тиме и подешавања организације. То значи да се на исти начин дефинишу подешавања за поједине типове сертификата.

Како би креирао нови сектор на порталу, потребно је да RAO администратор у главном менију одабере опцију *Settings*, затим у менију другог нивоа прву у низу опцију *Organizations*, потом означи организацију и кликне на *Departments* а затим на *Add*.

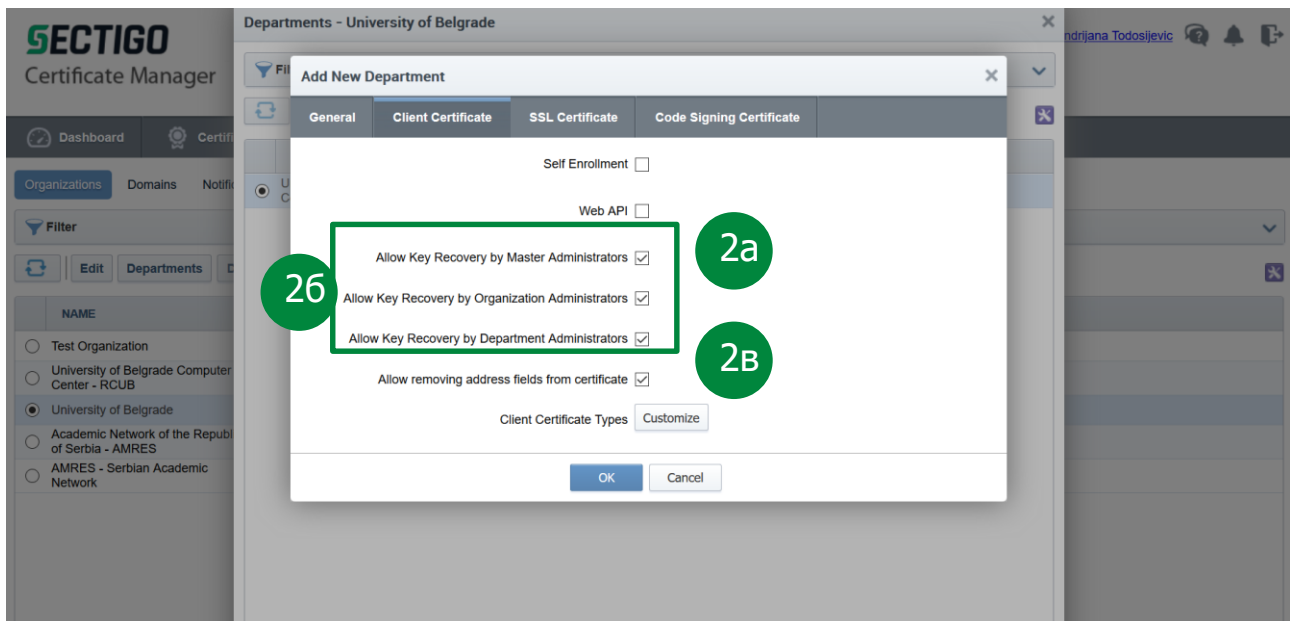
КОРАК 1



Како би RAO администратор додао нови сектор потребно је да дефинише назив сектора (1a). Остала поља су већ попуњена подацима организације.

КОРАК 2

У оквиру таба *Client Certificate* могуће је дефинисати подешавања у вези са захтевањем и издавањем клијентских сертификата.



Важно је напоменути опцију преузимања кључа клијентских сертификата. Уколико је организација креирана са искљученом опцијом за обнову кључа клијентских сертификата, друга по реду опција *Allow Key Recovery by Organization Administrators* (26) биће аутоматски онемогућена.

НАПОМЕНА: Потребно је искључити прву и трећу опцију *Allow Key Recovery by Master Administrators* (2a) и *Allow Key Recovery by Department Administrators* (2b) пошто је потребно избећи да MRAO и DRAO администратори преузимају клијентске сертификате за специфицирани сектор.

Друга по реду опција, уколико је омогућена, може опционо остати укључена уколико RAO администратор жели да додели себи и другим RAO администраторима ову привилегију. Препорука је да се ова опција не користи из сигурносних разлога.

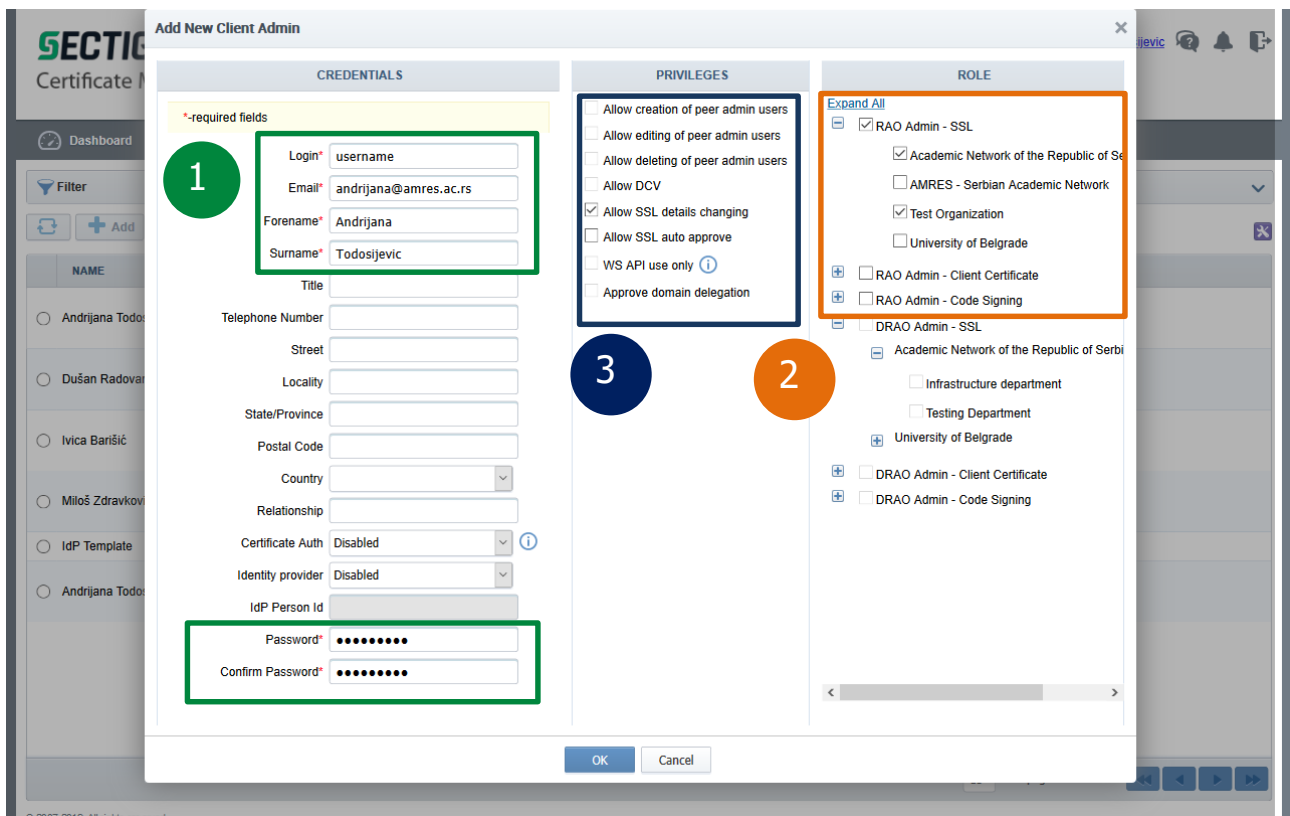
Наведене опције су обавезне приликом креирања сектора и оне се не могу накнадно мењати. Све остале опције могу се накнадно подешавати и оне су додатно описане у КОРАКУ 4 поглавља 2 Приступ SCM порталу.

4.2 Поступак креирања RAO администратора

RAO администратор може да креира RAO и DRAO администраторе. Поступак додавања је исти.

Како би додао новог администратора потребно је да RAO администратор у главном менију одабере опцију *Admins* и затим кликне на дугме *Add*.

НАПОМЕНА: Опција *Add IdP User* служи за додавање администратора који ће приступати порталу путем SAML протокола. Ова опција још увек није у функцији за AMRES.



Прво је потребно унети креденцијале и корисничке податке (1):

- ✦ Корисничко име;
- ✦ Имејл;
- ✦ Име и презиме;
- ✦ Шифру (администратор мења ову шифру након што се први пут улогује на портал);
- ✦ НАПОМЕНА: *Identity Provider* опцију оставити *Disabled*.

Затим је потребно означити улогу новог администратора на порталу тако што ће се означити организација којој је администратор делегиран, за сваки тип сертификата (2).

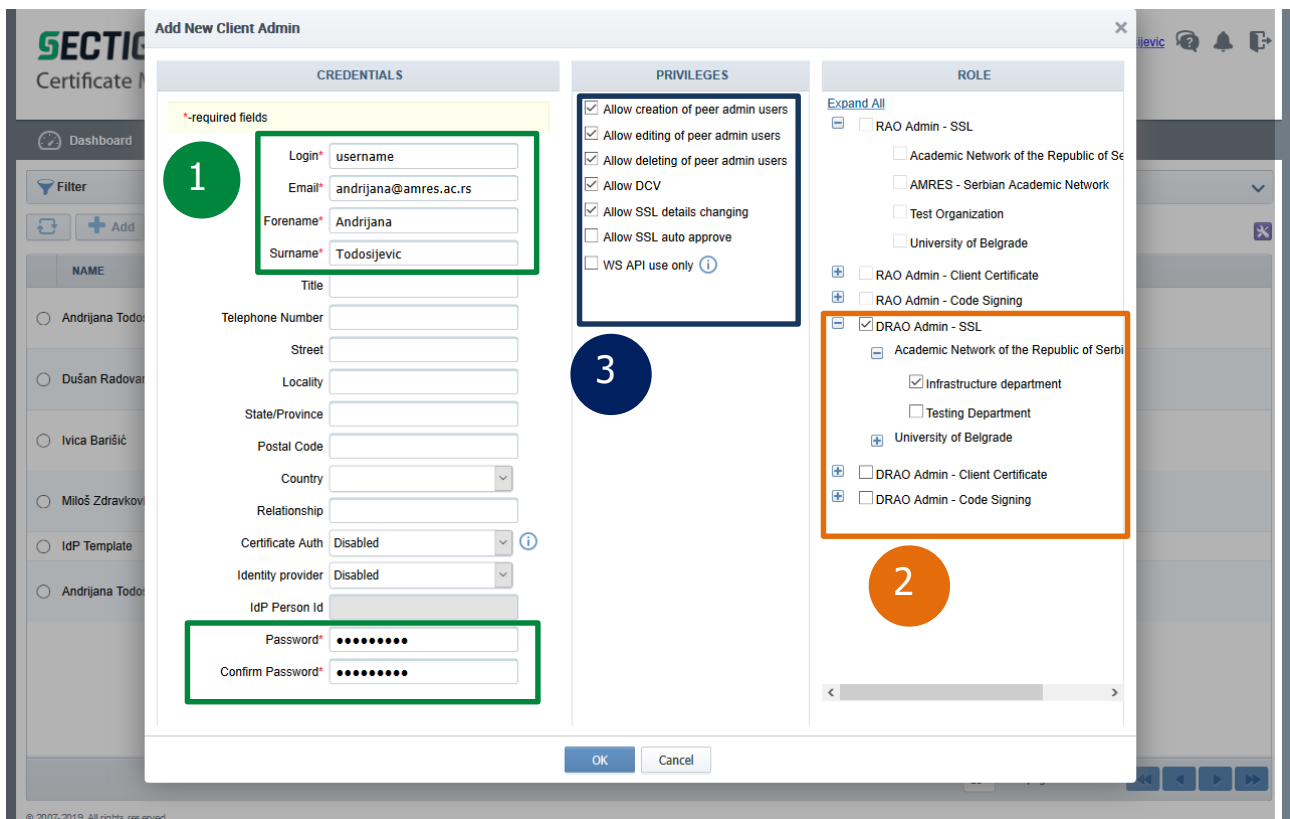
Након доделе RAO улоге, може се приметити да се аутоматски онемогућавају поједине привилегије (3). Разлог је тај што RAO администратор може да креира RAO администраторе истог нивоа, али не може да им додели исти скуп привилегија. Само налог креиран од стране MRAO администратора може добити све привилегије. Уколико постоји потреба за додатним привилегијама за новокреираног RAO администратора, потребно је послати захтев на tcs@amres.ac.rs. Опција *Allow SSL details changing* може бити укључена, док је препорука да опција *Allow SSL auto approve* увек остане искључена. Она означава обавезу да се захтев за сертификатом прво одобри пре него што се сертификат изда. То оставља могућност контроле и накнадне промене детаља сертификата, нпр. период трајања сертификата. Опција *Approve domain delegation* даје могућност RAO администраторима да дозволе додавање домена. Ову могућност на порталу ће за сада имати само MRAO, тако да је потребно да ово опција остане искључена.

4.3 Поступак креирања DRAO администратора

RAO администратор може да креира RAO и DRAO администраторе. Поступак додавања је исти.

Како би RAO администратор додао новог DRAO администратора потребно је да у главном менију одабере опцију *Admins* и затим кликне на дугме *Add*.

НАПОМЕНА: Опција *Add IdP User* служи за додавање администратора који ће приступати порталу путем SAML протокола. Ова опција још увек није у функцији за AMRES.



Прво је потребно унети креденцијале и корисничке податке (1):

- ✎ Корисничко име;
- ✎ Имејл;
- ✎ Име и презиме;
- ✎ Шифру (администратор мења ову шифру након што се први пут улогује на портал);

⌘ **НАПОМЕНА:** *Identity Provider* опцију оставити *Disabled*.

Затим је потребно означити улогу новог администратора на порталу тако што ће се означити сектори којима је администратор делегиран, за сваки тип сертификата (2).

Након доделе DRAO улоге, може се приметити да су све привилегије доступне (3). Разлог је тај што RAO администратор може да креира DRAO администраторе са целим скупом привилегија. Препорука је да опција *Allow SSL auto approve* увек остане искључена. Она означава обавезу да се захтев за сертификатом одобри пре него што се сертификат изда. То оставља могућност контроле и накнадне промене детаља сертификата, нпр. период трајања сертификата.

4.3.1 Поступак креирања других администратора и сектора – DRAO

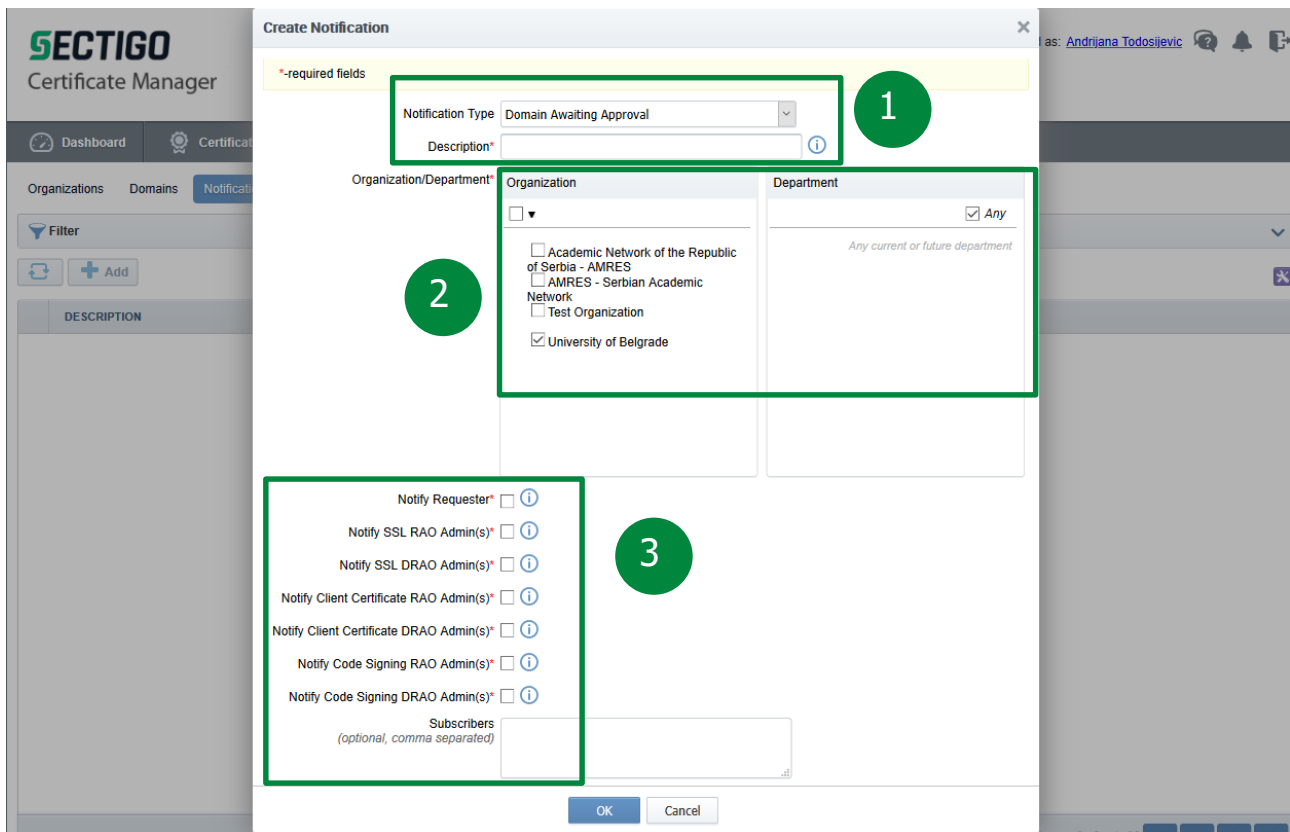
DRAO администратор може да креира друге DRAO администраторе за свој сектор. Поступак додавања нових администратора поклапа се са поступком креирања других RAO администратора од стране RAO администратора. DRAO администратор може да креира DRAO администраторе истог нивоа, али не може да им додели исти скуп привилегија.

5 Поступак подешавања обавештења на порталу

Нотификације на порталу нису обавезне, али су веома корисне. Све нотификације контролише MRAO. Препорука је да се подесе најмање следећа обавештења:

- ⌘ *Domain Awaiting Approval* – обавештење администратору да је креиран и делегиран нови домен од стране DRAO администратора, који чека одобрење. Обавештење је већ подешено од стране MRAO администратора за све организације.
- ⌘ *SSL Awaiting Approval* – обавештење администратору да је захтеван нови SSL сертификат, који чека одобрење;
- ⌘ *Certificate Expiration* – упозорење о истеку сертификата. Обавештење о истеку сертификата је већ подешено од стране MRAO администратора за све типове сертификата, али се могу креирати додатна обавештења по потреби. Обавештења ће стизати једном 60., 30. и 15. дана пре истека сертификата, а затим сваки дан почевши од 7. дана пре истека сертификата;
- ⌘ *DCV Expiration* – истек периода валидности домена. Домен се валидира на годину дана. Обавештење о истеку домена је већ подешено од стране MRAO администратора за све домене, али се могу креирати додатна обавештења по потреби. Обавештења ће стизати једном 60., 30. и 15. дана пре истека валидности домена, а затим сваки дан почевши од 7. дана пре истека валидности домена.

Како би RAO администратор подесио обавештење, потребно је да у главном менију одабере опцију *Settings*, затим у менију другог нивоа опцију *Notifications*, потом кликне на дугме *Add*.



Потребно је одабрати тип обавештења и дефинисати његов опис (1). RAO администратор потом треба да одабере организацију на коју ће се обавештење односити, и да специфицира да ли жели да сви сектори буду укључени (2). Затим је потребно означити администраторе којима ће се слати обавештења (3). Скуп понуђених администратора се разликује у зависности од обавештења.

Кликом на дугме ОК обавештење је креирано.

5.1 Поступак подешавања обавештења на порталу – DRAO

Поступак подешавања нотификација на порталу за DRAO администратора не разликује се од претходно наведеног поступка за RAO администратора. DRAO има могућност да подешава обавештења само за секторе који су му додељени и да одабере само DRAO администраторе као особе које је потребно обавестити.

6 Поступак захтевања и прибављања сертификата

Да би RAO администратор могао да захтева дигиталне сертификате неопходно је да претходно буду испуњени следећи предуслови:

- ❖ AMPEC корисник мора имати регистрован домен у оквиру "ac.rs" домена,
- ❖ AMPEC корисник мора бити регистрован за коришћење TCS услуге и мора имати креирану организацију и RAO налог на SCM порталу,
- ❖ MRAO администратор је комплетирао процедуру валидације организације,
- ❖ RAO администратор је успешно креирао и делегирао домен, и комплетирао процедуру валидације домена,

- ❖ ОПЦИОНО: RAO администратор је иницирао процес енкрипције и сачувао мастер приватни кључ на сигурној локацији, уколико је одабрао ову могућност током пријаве организације за портал.

Уколико су сву предуслови испуњени, администратори AMRES корисника могу преко SCM портала захтевати неограничен број серверских и клијентских сертификата за потребе својих сервера и крајњих корисника.

SCM подржава више начина захтевања и прибављања сертификата:

- ❖ Путем аутоматских захтева и инсталација од стране Агената различитог типа, подржаних од стране SCM;
- ❖ Путем *Self-enrollment* форме која је доступна крајњим корисницима уколико је ова опција омогућена у подешавањима организације;
- ❖ Путем корисничког интерфејса SCM портала.

У упутству ће бити описан начин прибављања сертификата путем корисничког интерфејса SCM портала. Остале функционалности детаљно су објашњене у [SECTIGO бази знања](#).

Поступак захтевања сертификата на порталу се разликује у зависности од типа сертификата, а на порталу се могу захтевати сертификати за три основна типа:

- ❖ *SSL Certificates*;
- ❖ *Client Certificates*;
- ❖ *Code Signing Certificates*.

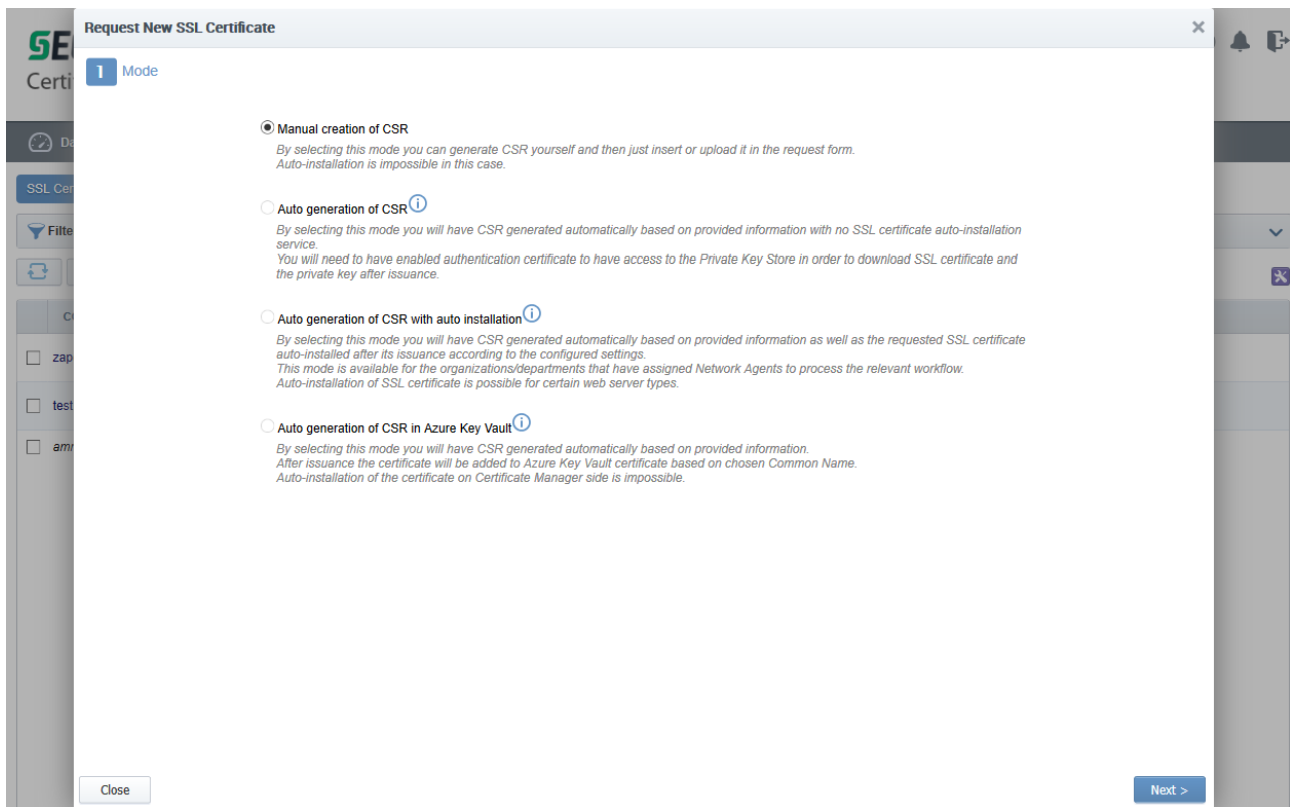
У документу ће бити описани само поступци захтевања и издавања прва два типа сертификата.

6.1 Поступак захтевања **SSL** сертификата

Препоручује се да AMRES корисници, корисници TCS услуге, креирају пар приватни/јавни кључ и захтев за сертификатом на серверу на ком планирају да употребе сертификат. Предност креирања кључева на серверу на коме ће сертификат бити употребљен је тај што приватни кључ неће морати да се пребацује са једног сервера/рачунара на други. Поступак креирања пара приватног/јавног кључа и захтева за сертификат за *Linux* платформу описан је у Додатку А, а додатне информације могу се пронаћи у [SECTIGO бази знања](#).

Како би RAO администратор започео сам процес захтевања сертификата, потребно је да у главном менију одабере опцију *Certificates*, затим у менију другог нивоа опцију *SSL Certificates*, потом кликне на дугме *Add*.

КОРАК 1



Request New SSL Certificate

1 Mode

☒ **Manual creation of CSR**
By selecting this mode you can generate CSR yourself and then just insert or upload it in the request form.
Auto-installation is impossible in this case.

☐ **Auto generation of CSR** ⓘ
By selecting this mode you will have CSR generated automatically based on provided information with no SSL certificate auto-installation service.
You will need to have enabled authentication certificate to have access to the Private Key Store in order to download SSL certificate and the private key after issuance.

☐ **Auto generation of CSR with auto installation** ⓘ
By selecting this mode you will have CSR generated automatically based on provided information as well as the requested SSL certificate auto-installed after its issuance according to the configured settings.
This mode is available for the organizations/departments that have assigned Network Agents to process the relevant workflow.
Auto-installation of SSL certificate is possible for certain web server types.

☐ **Auto generation of CSR in Azure Key Vault** ⓘ
By selecting this mode you will have CSR generated automatically based on provided information.
After issuance the certificate will be added to Azure Key Vault certificate based on chosen Common Name.
Auto-installation of the certificate on Certificate Manager side is impossible.

Close Next >

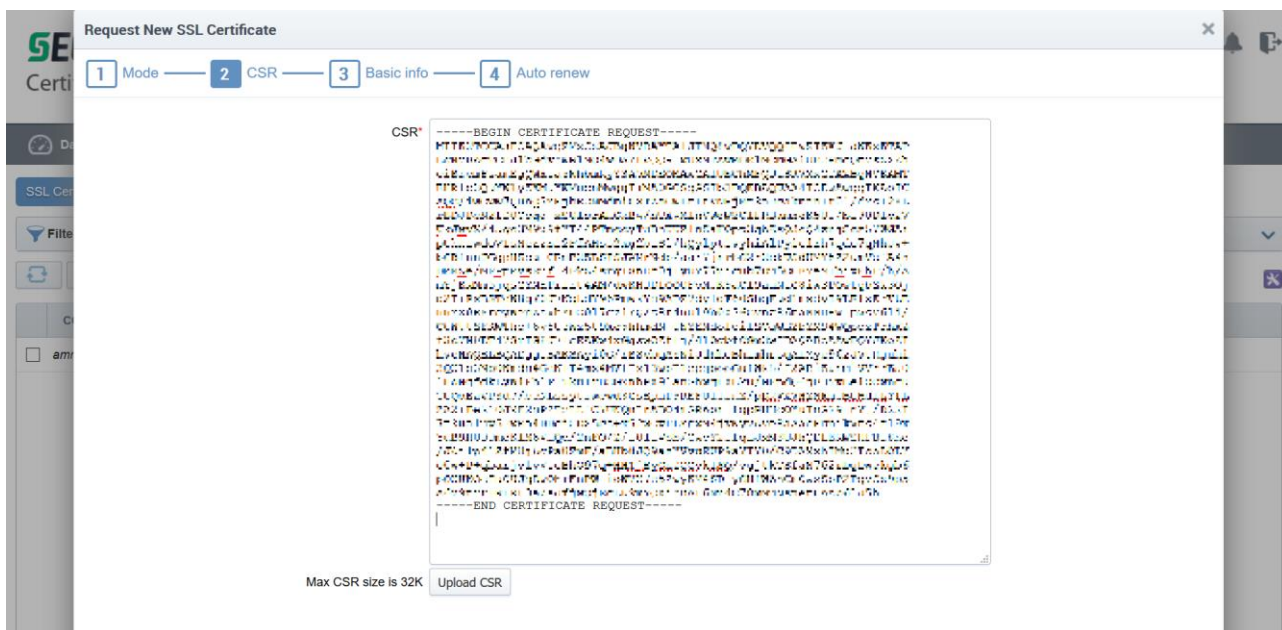
Отвориће се прозор који захтева спецификацију начина креирања захтева:

- ✎ *Manual creation of CSR* – захтев за сертификат претходно је креиран и потребно га је копирати у наредном кораку;
- ✎ *Auto generation of CSR* – ова опција није подржана;
- ✎ *Auto generation of CSR with auto installation* – ова опција је подржана и може се користити уколико постоји бар један Агент конфигуисан у овом моду;
- ✎ *Auto generation of CSR in Azure Key Vault* – ова опција је подржана уколико се *Azure* подеси самостално.

RAO администратор ће најчешће користити прву опцију. Након одабира и клика на дугме *Next* прелази се на други корак.

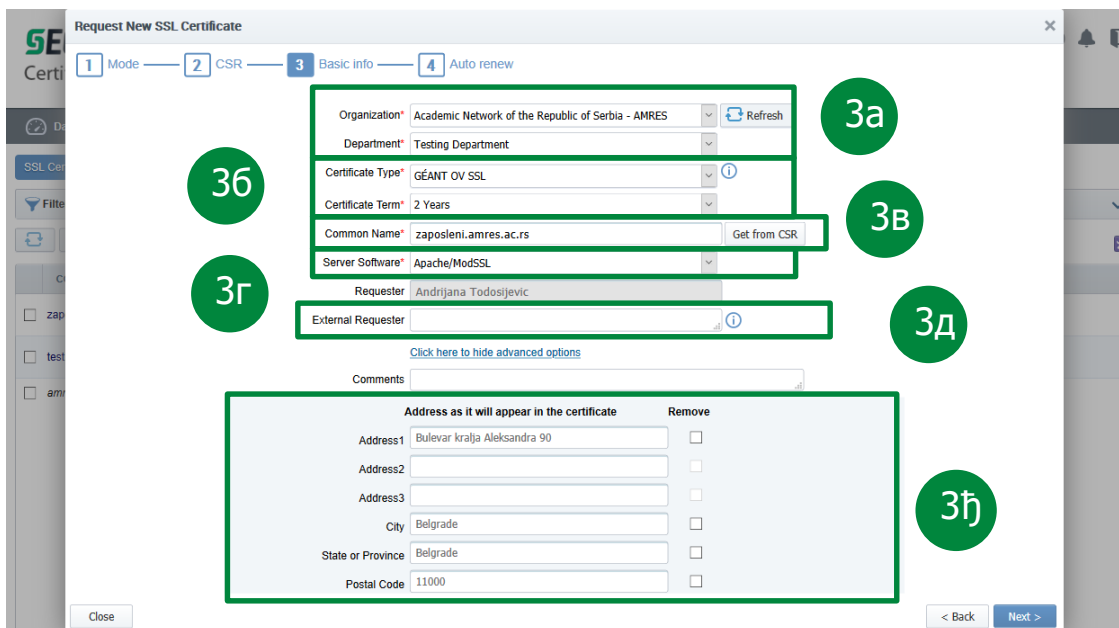
КОРАК 2

У наредном прозору потребно је копирати захтев за сертификат и кликнути на дугме *Next*.



КОПАК 3

Овај корак подразумева подешавање и унос основних информација о сертификату.



RAO администратор бира организацију и сектор за који захтева сертификат (3а). Доступне вредности за ова поља су организације и сектори који су делегирани администратору. Додатно, у овом кораку се специфицира тип сертификата који се захтева и период важења сертификата (36).

НАПОМЕНА: У случају да се одабере *GEANT OV SSL* тип за прибављање сертификата за нпр. *mail.sample.example.ac.rs*, у оквиру SAN поља добија се и вредност *www.mail.sample.example.ac.rs*. Уколико не желите ову опцију, препорука је да се користи тип сертификата за више доменских имена (*Multi-Domain* тип). У случају да се одабере *Wildcard* сертификат, потребно је навести број (количину) сервера на којима је планирана инсталација сертификата. Уколико нисте сигурни, препорука је да се користи тип сертификата за више доменских имена (*Multi-Domain* тип), где ће се као једно додатно, алтернативно доменско име наћи и жељени *Wildcard* домен.

Поље *Common name* (3в) може да садржи:

- ✘ Домен за сертификат за једно доменско име;
- ✘ *Wildcard* домен за сертификат за сва поддоменска имена једног домена;
- ✘ Примарни домен за сертификат за више доменских имена. Приликом захтевања овог сертификата и одабира овог типа у пољу изнад (3б) аутоматски се додаје поље где је потребно специфицирати додатна, алтернативна доменска имена.

Домени се могу уписати ручно или аутоматски попунити из захтева кликом на дугме *Get from CSR*.

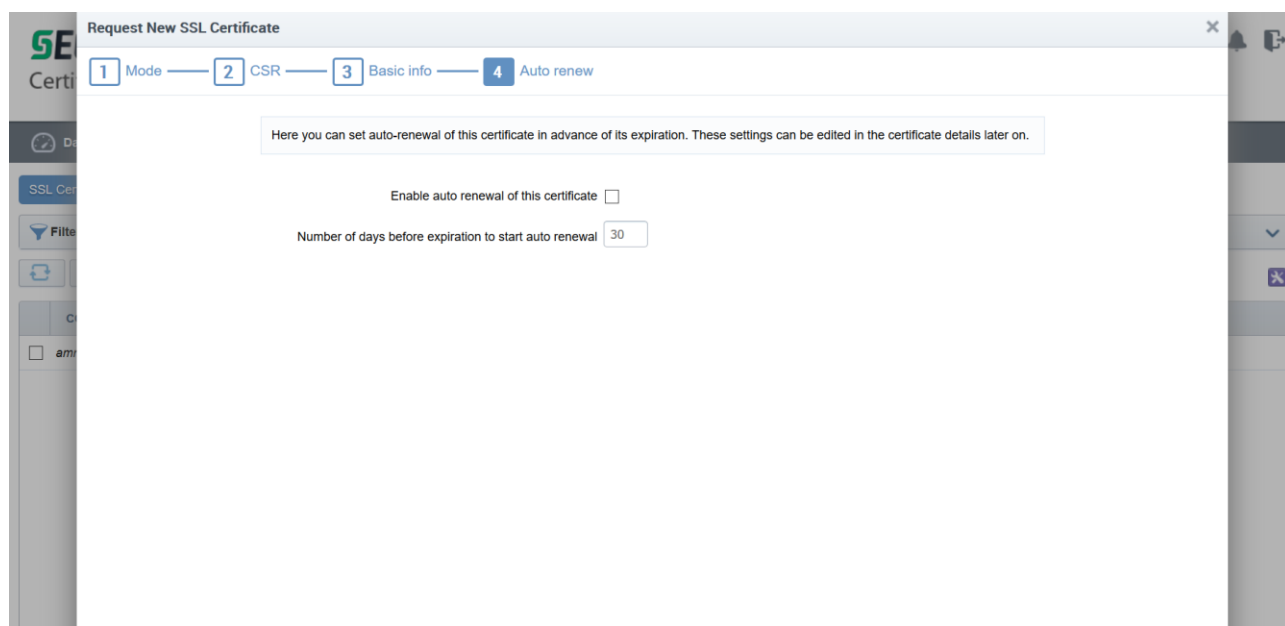
Потребно је и прецизирати на којој серверској платформи је планирано да се инсталира сертификат након што буде издат. Информација о серверској платформи се прецизира да би се сертификат испоручио у потребној форми за жељену серверску платформу (3г).

У оквиру овог корака могуће је специфицирати адресу корисника (3д) у име кога се захтева сертификат. На наведену адресу буће послат мејл који садржи издати сертификат.

Када се кликне на линк за додатне опције приказују се поља дефинисана у оквиру организације (3ђ). Уколико је опција *Allow removing address fields from certificate* у подешавањима организације за коју се захтева сертификат укључена, администратор ће моћи да uklони вредности ових поља. Препорука је да се то не ради пошто у неким случајевима узрокује проблеме са самим сертификатом.

КОРАК 4

Након клика на дугме *Next* приказаће се прозор који преставља четврти корак поступка захтевања сертификата и односи се на опцију аутоматске обнове сертификата.



Ова опција је опциона и функционална само у случају *Apache* веб-сервера. У овом поступку се користи CSR претходног захтева, а *Apache* је једина платформа која дозвољава да исти приватни кључ буде употребљен за различите сертификате.

Кликом на дугме *OK* процедура захтевања сертификата је завршена.

КОРАК 5

Сертификат у овом тренутку има статус *Requested* (5а).

SECTIGO
Certificate Manager

Logged as: [Andrijana Todosijevic](#)

Dashboard Certificates Discovery Reports Admins Settings About

SSL Certificates Client Certificates Code Signing Certificates

Filter

+ Add Export Edit Details Approve Decline

	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
<input checked="" type="checkbox"/>	zaposleni.amres.ac.rs	Academic Network of the Republic of Serbia - AMRES		Requested		Not scheduled	Not scheduled
<input type="checkbox"/>	test.amres.ac.rs	Academic Network of the Republic of Serbia - AMRES	Testing Department	Issued	04/04/2022	Not scheduled	Not scheduled
<input type="checkbox"/>	amres.ac.rs *	AMRES - Serbian Academic Network		External	07/23/2021	Not scheduled	Not scheduled

Како би се одобрио захтев за сертификатом потребно је кликнути на сертификат (56), затим на дугме Approve (5B) и у новом прозору унети жељену поруку. Пре потврде могуће је изменити детаље сертификата кликом на опцију *Details*.

SECTIGO
Certificate Manager

Logged as: [Andrijana Todosijevic](#)

Dashboard Certificates Discovery Reports Admins Settings About

SSL Certificates Client Certificates Code Signing Certificates

Filter

+ Add Export Edit Details Approve Decline

Approval Message


*required fields

Message*

OK

OK Cancel

Захтев се затим шаље СА на валидацију и има статус *Applied*.


SECTIGO
 Certificate Manager

Logged as: [Andrijana Todosijevic](#)

Dashboard Certificates Discovery Reports Admins Settings About

SSL Certificates Client Certificates Code Signing Certificates

Filter

Add Export Details

	COMMON NAME	ORGANIZATION	DEPARTMENT	STATUS	EXPIRES	INSTALL STATE	RENEWAL STATE
<input checked="" type="checkbox"/>	zaposleni.amres.ac.rs	Academic Network of the Republic of Serbia - AMRES		Applied		Not scheduled	Not scheduled
<input type="checkbox"/>	test.amres.ac.rs	Academic Network of the Republic of Serbia - AMRES	Testing Department	Issued	04/04/2022	Not scheduled	Not scheduled
<input type="checkbox"/>	amres.ac.rs*	AMRES - Serbian Academic Network		External	07/23/2021	Not scheduled	Not scheduled

Када се сертификат изда и администратор прими одговарајући мејл, статус прелази у *Issued*.

Сертификати који имају статус *External* су аутоматски детектовани путем *Discovery* сервиса који пружа SCM портал.

Кликом на сертификат, па на опцију *Details* отвара се прозор у коме се могу видети све информације о сертификату, као и преузети сам сертификат у изабраном формату.

SSL Certificate: zaposleni.amres.ac.rs

Certificate (w/ chain), PEM encoded
 Certificate only, PEM encoded
 PKCS#7, PEM encoded
 PKCS#7
 Root/Intermediate(s) only, PEM encoded
 Intermediate(s)/Root only, PEM encoded

Common Name Root/Intermediate(s) only, PEM encoded
 Status Intermediate(s)/Root only, PEM encoded
 Download The Certificate Select

Order Number 337916589
 Vendor Sectigo Limited
 Discovery Status Not deployed
 Self-Enrollment Certificate ID 1718554
 Type GÉANT OV SSL
 Server Software AOL Edit
 Server Software State
 Term 2 years
 Owner Andrijana Todosijevic Resend Edit
 Requested by Andrijana Todosijevic Resend Edit
 External Requester Edit
 Requested 04/03/2020

CERTIFICATE CHAIN DETAILS

Root Intermediate End Entity

Common Name AddTrust External CA Root
 Vendor Self-Signed
 Term 20 years
 Valid From 05/30/2000
 Expires 05/30/2020
 Serial Number 01
 Signature Algorithm SHA1WITHRSA
 Public Key Algorithm RSA
 Public Key Size 2048
 MD5 Hash 1d3554048578b03f42424dbf20730a3f
 SHA1 Hash 02faf3e291435468607857694df5e45b68851868
 Issuer CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
 Subject CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
 Address 1

Close

Са десне стране прозора су подаци о сертификатима који чине ланац поверења, два прелазна и један корени сертификат. *AddTrust External CA Root* сертификат истиче у мају 2020. године, али је безбедно инсталирати сертификате потписане овим кореним сертификатом. Више информација доступно је у [SECTIGO обавештењу и питањима](#).

НАПОМЕНА: Приликом испоруке сертификата, администратор ће примити имејл који садржи линкове за преузимање захтеваног сертификата и прелазних сертификата у [различитим форматима](#) у зависности од одабране платформе.

Сертификати прелазног и кореног сертификационог тела доступни су и на адресама:

- ❖ GÉANT прелазно CA тело: <https://crt.sh/?CAName=%25GEANT+Vereniging%25>
- ❖ Нови корени сертификати: USERTrust RSA CA тело - <https://crt.sh/?id=1199354> , USERTrust ECC CA тело - <https://crt.sh/?id=2841410>

У оквиру сертификата прелазног сертификационог тела преузетог из мејла, налази се група, тј. ланац сертификата, због подршке за старе верзије појединих клијената, као и истека старог кореног сертификата:

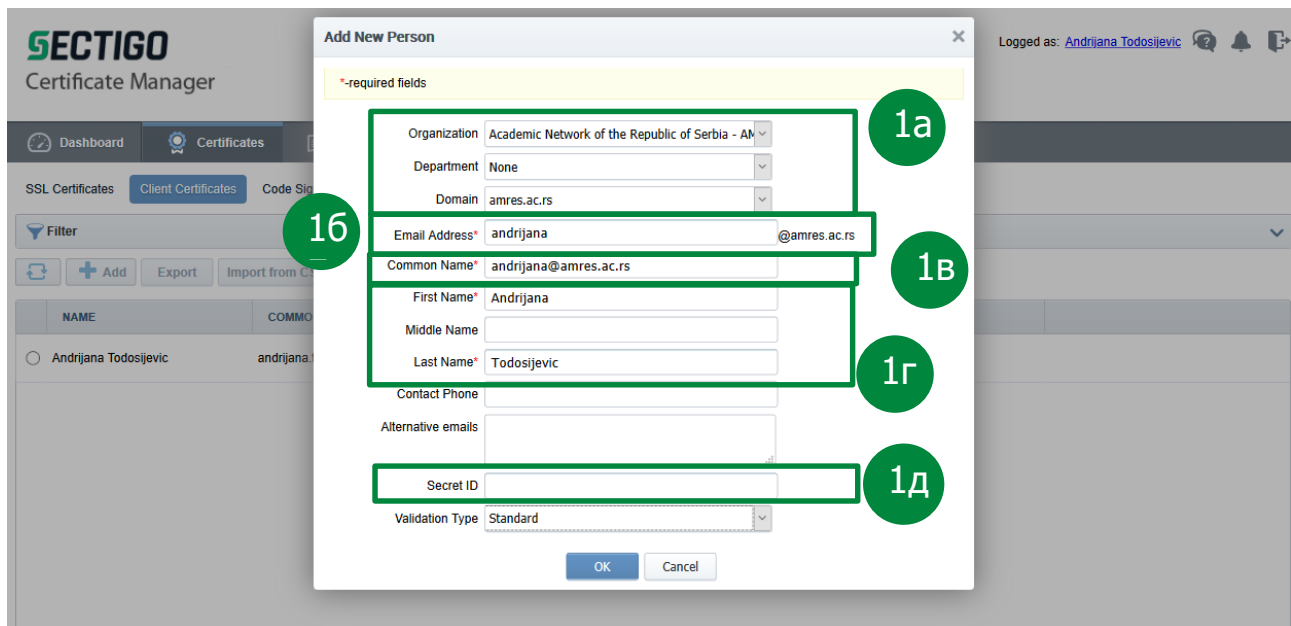
- ❖ https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000rgSZ
- ❖ https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA03I00000117LT

НАПОМЕНА: Није обавезно укључити све прелазне сертификате који се могу преузети са линкова у мејлу, у ланац прелазних сертификата на серверу. Довољно је поставити сертификат GÉANT прелазног сертификационог тела (CN = GEANT OV RSA CA 4 или други) као прелазни. Као што је већ наведено, овај сертификат доступан је на локацији <https://crt.sh/?CAName=%25GEANT+Vereniging%25> , или се може изоловати из групног сертификата из мејла.

6.2 Поступак захтевања клијентских сертификата

Како би RAO администратор започео сам процес захтевања клијентског сертификата, потребно је да дода корисника у систему, тако што у главном менију одабере опцију *Certificates*, затим у менију другог нивоа опцију *Client Certificates*, потом кликне на дугме *Add*.

КОРАК 1



Отвориће се прозор у коме је потребно унети податке о особи за коју се захтева клијентски сертификат. Обавезно је:

- ❖ Одабрати организацију, сектор и домен (1a);
- ❖ Унети први део имејл адресе (16);
- ❖ Унети *Common Name*, што може да буде или имејл адреса корисника или име и презиме (1b);
- ❖ Унети име и презиме корисника (1r).

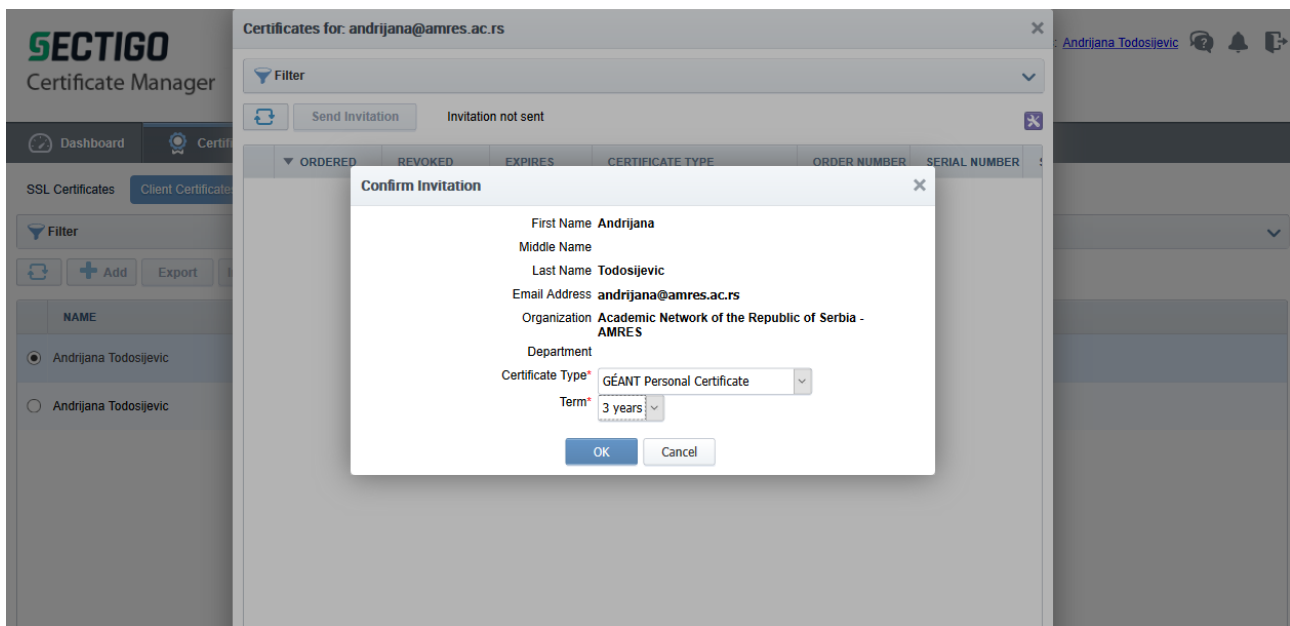
Поље *Secret ID* (1d) користи се за *Self enrollment* форму и може се дефинисати за сваког корисника.

НАПОМЕНА: Ово је други начин коришћења *Self enrollment* форме и нема већих предности у односу на поступак који се тренутно описује, пошто се корисник свакако ручно креира на порталу. Ово поље је јединствено за сваког корисника и то је разлика у односу на употребу *Self enrollment* форме у случају када се дефинише један Приступни код за целу организацију или сектор. *Self enrollment* форма је доступна на линку <https://cert-manager.com/customer/AMRES/smime>.

Опционо се могу унети додатне имејл адресе и контакт телефон корисника. Кликом на дугме *OK* корисник је креиран.

КОРАК 2

Сада је потребно послати позивницу кориснику како би преузео сертификат. Потребно је кликнути на корисника, а затим на *Certificates*. Појавиће се прозор у коме је потребно кликнути на *Send Invitation*.



Да би се позивница послала, одаберу се тип и период важења сертификата и кликне на дугме *OK*. Након овог корака, корисник је примио имејл који садржи линк за валидацију имејла и код захтева.

НАПОМЕНА: За сваког корисника се могу захтевати максимално два клијентска сертификата. Уколико је потребно прибавити нови, један од претходна два мора да буде опозван.

НАПОМЕНА 2: Линк за валидацију у имејлу није више прилагођен нашим корисницима. Потребно је у претраживачу унети вештачки направљен линк следеће форме: <https://cert-manager.com/customer/AMRES/smime?action=invite&requestCode=xxxxxxxxxxxxxxxxxxxxxxxx&email=andrijana%40amres%2eac%2ers>, где је потребно променити код xxxxxxxxxxxxxxxxxxxxxxxxxxx кодом из имејла, као и имејл адресу корисника, где се **тачка** мења скупом карактера **%2e**, а **@** скупом карактера **%40** (део линка на крају `andrijana%40amres%2eac%2ers` представља имејл адресу `andrijana@amres.ac.rs`, а `npr. andrijana%2etodosijevic%40amres%2eac%2ers` представља имејл адресу `andrijana.todosijevic@amres.ac.rs`).

У случају клијентских сертификата, корисник може да отвори линк у било ком претраживачу, пошто се кључеви креирају тренутно на страни сервера, и преузима се .p12 фајл, док се цео процес поништава заједно са приватним кључем и систем више нема приступ приватном кључу сертификата, осим уколико је омогућена опција повратка, тј. поновног преузимања приватног кључа за организацију или сектор. Овај формат фајла садржи и приватни и јавни кључ сертификата.

НАПОМЕНА: Поступак издавања *Code Signing* сертификата се разликује од поступка издавања клијентских сертификата. За генерисање сертификата користи се валидациони линк, а сам процес

генерисања кључа и захтева могућ је једино у Internet Explorer прегледачу, пошто једино он подржава „keugen“ функционалност. Овај процес генерише приватни кључ локално и упућује захтев на систем за креирање сертификата. Кориснику ће стићи још један имејл из кога ће моћи да преузме сертификат, путем истог претраживача који је користио за генерисање приватног кључа.

КОРАК 3

Кликом на валидациони линк из мејла кориснику се отвара веб-форма. Код захтева, имејл и тип сертификата су аутоматски попуњени.



SECTIGO
Certificate Manager

User Registration

Code: *

Email: * andrijana@amres.ac.rs

Certificate Type: GEANT Personal Certificate

Password: *

Re-type Password: *

Passphrase: *

Re-type passphrase: *

3a

36

3b

IMPORTANT* PLEASE READ THIS SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE OR BEFORE CLICKING ON ACCEPT. YOU AGREE THAT BY APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO ITS TERMS. IF YOU ARE APPLYING FOR, ACCEPTING, OR USING A SECTIGO CERTIFICATE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU ARE AN AUTHORIZED REPRESENTATIVE OF SUCH ENTITY AND HAVE THE AUTHORITY TO ACCEPT THIS AGREEMENT ON SUCH ENTITY'S BEHALF. IF YOU DO NOT HAVE SUCH AUTHORITY OR IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A SECTIGO CERTIFICATE AND DO NOT CLICK ACCEPT

SECTIGO CERTIFICATE SUBSCRIBER AGREEMENT

This Sectigo Certificate Subscriber Agreement (this Agreement) is between the individual or legal entity identified on the issued Certificate(s) resulting from this

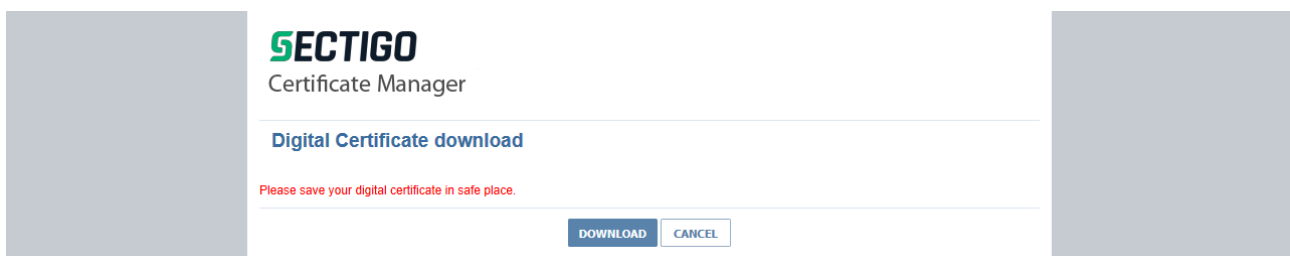
PRINT

☐ I accept the terms and conditions.*
Scroll to bottom of the agreement to activate check box.

SUBMIT CANCEL

Крајњи корисник може да дефинише и унесе шифру (3a), која ће се користити приликом импортовања тј. инсталације сертификата.

Поље *Passphrase* ће се користити приликом опозива сертификата (36). Након што унесе ове две шифре, потребно је да прихвати услове након што прође цео *Subscriber Agreement* и кликом на *SUBMIT*, крајњем кориснику се приказује страница са које може да преузме сертификат.



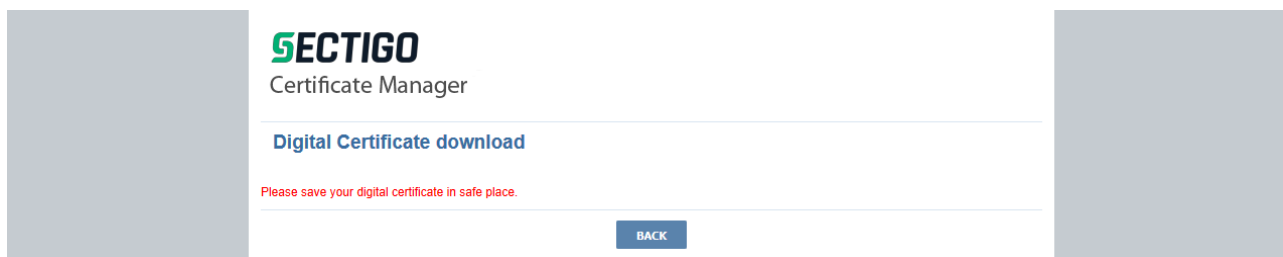
SECTIGO
Certificate Manager

Digital Certificate download

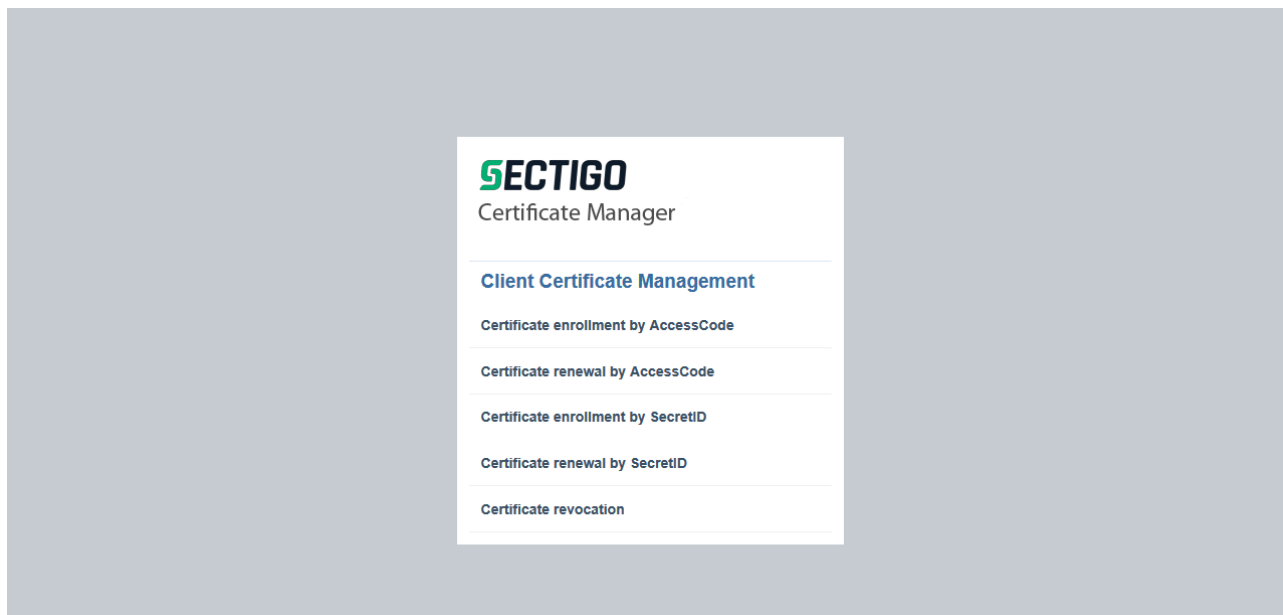
Please save your digital certificate in safe place.

DOWNLOAD CANCEL

Кликом на Download корисник преузима сертификат, и приказује му се завршна страница.



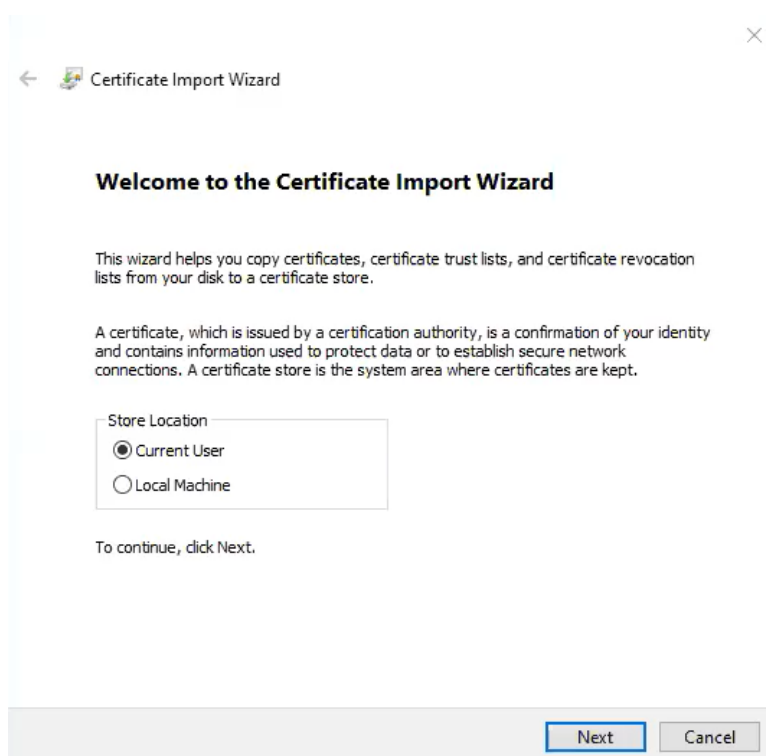
Кликом на дугме *Back* кориснику се приказује *Self-enrollment* форма доступна на <https://cert-manager.com/customer/AMRES/smime> линку.



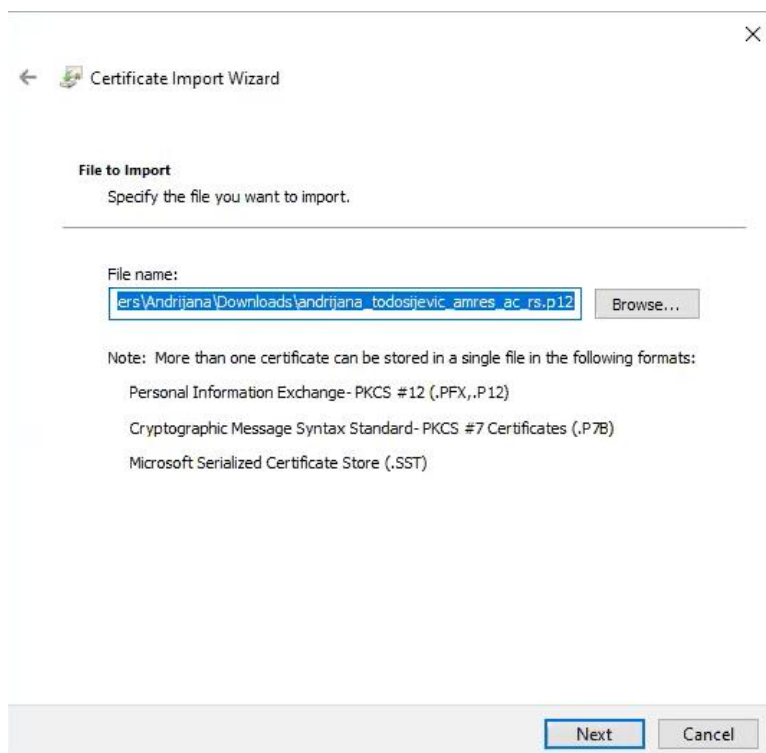
Крајњи корисници могу путем ове форме захтевати сертификате или користећи Приступни код дефинисан у подешавањима организације или сектора, или користећи *SecretID* дефинисан за сваког корисника посебно приликом креирања корисника на порталу.

КОРАК 4

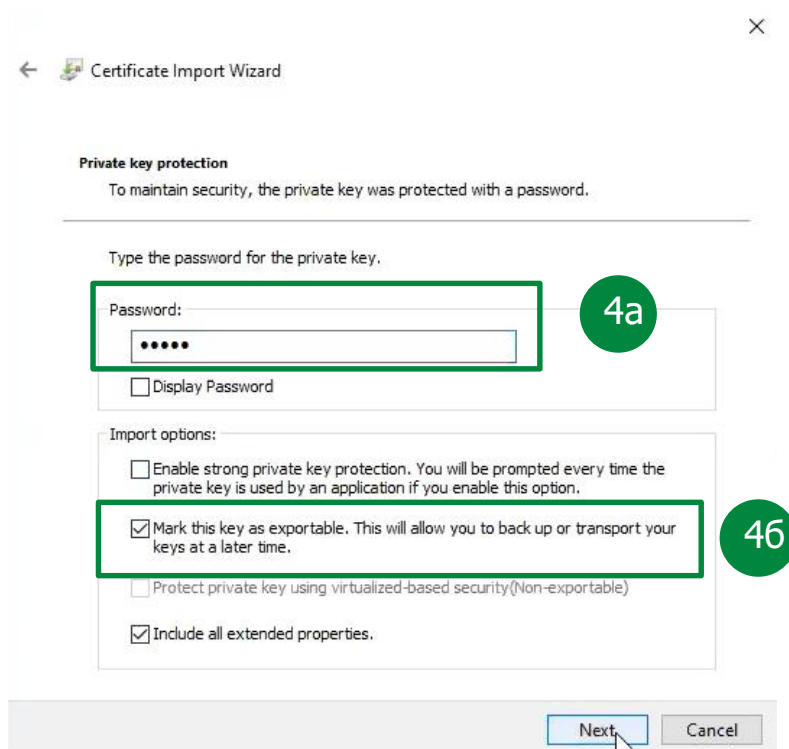
У наредном кораку описан је поступак импортовања сертификата у Windows систем корисничког рачунара, који подразумева покретање самог поступка дуплим кликом на .p12 фајл, након чега се кориснику приказује почетни прозор.



Потребно је да корисник одабере опцију *Current User* и кликне на *Next*.



Фајл је већ одабран, тако да је потребно кликнути на *Next*.



← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: **4a**

☐ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

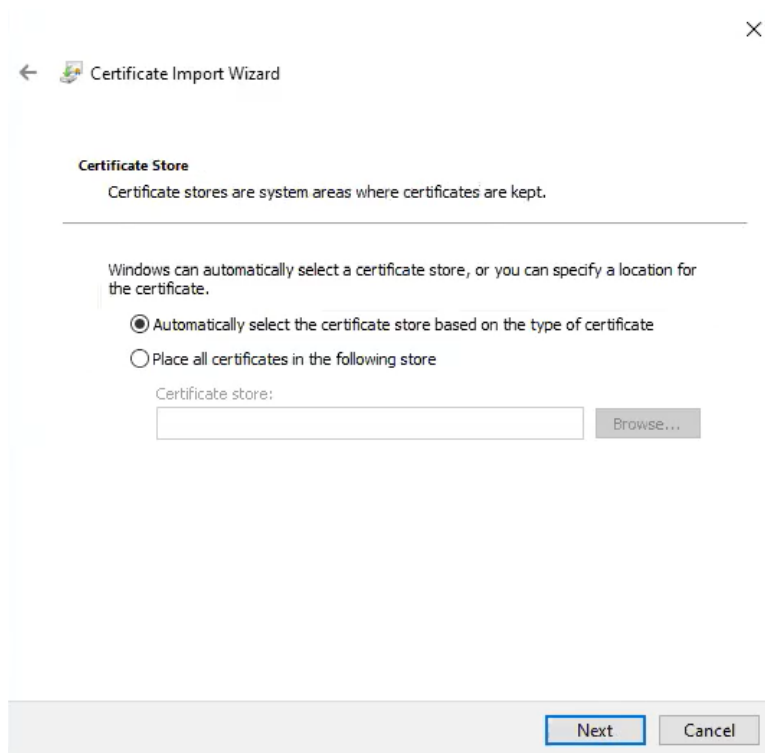
☒ Mark this key as exportable. This will allow you to back up or transport your keys at a later time. **46**

☐ Protect private key using virtualized-based security(Non-exportable)

☒ Include all extended properties.

Next Cancel

У овом прозору потребни је унети шифру **(4a)** дефинисану у КОРАКУ 3 овог поглавља и дозволити опцију за извоз **(46)**, затим кликнути на *Next*.



← Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

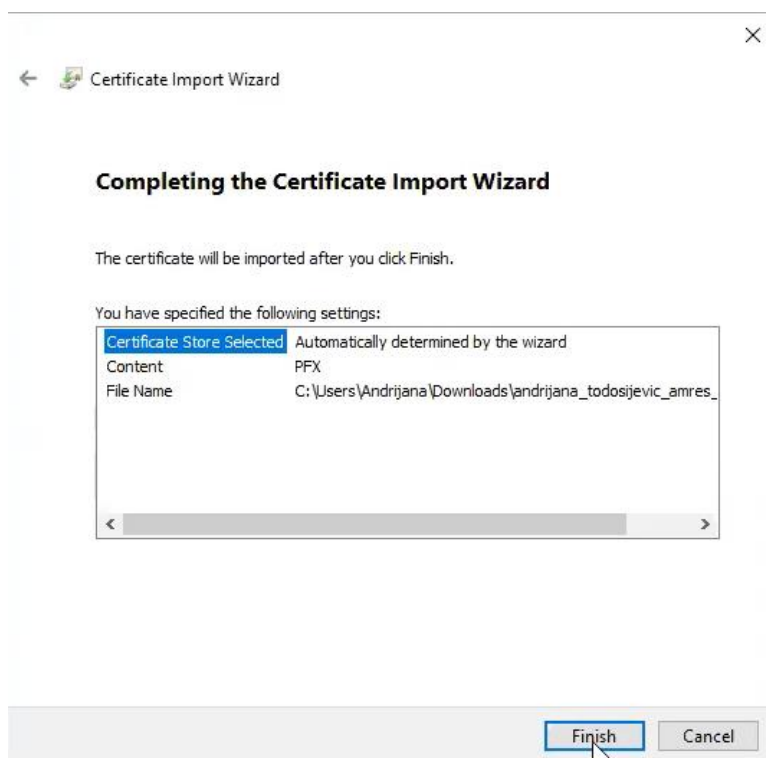
☒ Automatically select the certificate store based on the type of certificate

☐ Place all certificates in the following store

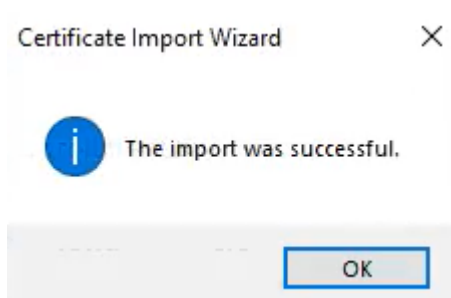
Certificate store: Browse...

Next Cancel

У овом кораку потребно је оставити одабрану опцију *Automatically select the certificate store based on the type of certificate* затим кликнути на *Next*.



Кликом на дугме *Finish* сертификат је успешно инсталиран.



Након овог момента, чак и ако се преузети .p12 фајл обрише са корисничког уређаја, може се поново извести, нпр. користећи *MMC* на Windows платформи.

Када је процес импорта сертификата успешно извршен, сертификат се може даље користити, нпр. од стране Microsoft Outlook апликације.

6.3 Поступак захтевања и прибављања сертификата – DRAO

Поступак прибављања сертификата од стране DRAO администратора у потпуности се поклапа са корацима које пролази RAO администратор.

7 Закључак

Поред наведених процеса, постоје додатне функционалности које пружа SCM, а које нису предмет овог упутства:

- ❖ Коришћење *ACME* налога;
- ❖ Аутоматско детектовање сертификата (*Discovery Service*) - сервис који омогућава да се аутоматски претражују/скенирају специфицирани мрежни опсези или домени, детектују постојећи сертификати и импортују на портал ради даљег управљања. За поступак откривања и детекције сертификата у интерној мрежи организације може да се инсталира и конфигурише Агент;
- ❖ Агенти, који се преузимају са портала и служе да скенирају мрежу организације и по потреби аутоматизују инсталацију сертификата;
- ❖ Извештаји;
- ❖ *WEB API*.

Наведене функционалности SCM портала, као и све остале детаљно су описане у **SECTIGO бази знања**.

Додатак А – Креирање захтева за сертификат

1 Креирање захтева за сертификат за једно доменско име (SSL) и за сва поддоменска имена једног домена са валидацијом организације (wildcard)

Препоручује се да АМРЕС корисници креирају пар приватни/јавни кључ и захтев за сертификат на серверу на ком планирају да употребе сертификат. Предност креирања кључева на серверу на коме ће сертификат бити употребљен је што приватни кључ неће морати да се пребацује са једног сервера/рачунара на други.

Препоручује се употреба **OpenSSL** софтверског алата на Unix/Linux оперативним системима, док се за друге системе препоручују упутства из SECTIGO базе знања:

- ❖ https://support.sectigo.com/Com_KnowledgeProductPage?c=CSR_Generation&k=&lang=
- ❖ https://support.sectigo.com/Com_KnowledgeProductPageFaq?c=CSR_Generation&k=&lang=
- ❖ https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000zFU6

КОРАК 1

Да би АМРЕС корисник креирао пар приватног/јавног кључа и захтев за сертификат у OpenSSL софтверском алату, неопходно је коришћење шаблонског (*template*) конфигурационог фајла. За креирање захтева за сертификат са једним доменским именом потребно је са АМРЕС веб-сајта преузети шаблонски конфигурациони фајл **SCSreq.cnf** и пребацити га на сервер/рачунар на коме ће се креирати пар кључева и захтев за сертификат. Препоручује се да шаблонски конфигурациони буде постављен у посебан директоријум који ће бити намењен за креирање пара приватног/јавног кључа и захтева.

КОРАК 2

На серверу на коме се планира употреба сертификата потребно је позиционирати се у директоријуму где се планира креирање пара приватног/јавног кључа и захтева за сертификат. За Unix/Linux оперативне системе, за почетак потребно је извршити следећу команду:

```
[server]#umask 0377
```

Посматраном командом се постављају адекватне пермисије на свим фајловима који ће бити креирани у поступку креирања пара приватног/јавног кључа.

КОРАК 3

У командној линији сервера са Unix/Linux оперативним системом, потребно је покренути команду за генерисање приватног кључа и захтева за сертификат у коме ће бити садржан јавни кључ:

```
[server]# openssl req -new -config SCSreq.cnf -utf8 -sha256 -keyout myserver.key -out myserver.csr
```

НАПОМЕНА: у оквиру команде могуће је подесити и додатне параметре, као што је нпр. величина кључа, опцијом *-newkey rsa:4096*, или променити нпр. *sha* алгоритам опцијом *-sha512*.

Након покретања команде администратор ће добити низ питања на које је потребно да одговори у складу са подацима који треба да буду уписани у сертификату (Ознака земље, Локација-град, Институција, Назив организационе јединице, FQDN име сервера). FQDN име сервера представља име домена које ће бити заштићено SSL/TLS сертификатом.

НАПОМЕНА: Поље *stateOrProvinceName*, тј. *Пун назив државе* потребно је оставити празно.

НАПОМЕНА: У случају креирања захтева за *wildcard* сертификат, приликом уписивања FQDN имена потребно је испред домена за који се сертификат захтева навести тзв. *wildcard* карактер *, на пример *.amres.ac.rs. Домен *.amres.ac.rs представља сва могућа поддоменска имена домена amres.ac.rs.

Након попуњавања свих неопходних података, у директоријуму ће бити креирана два нова фајла:

- ✎ myserver.key – приватни кључ сертификата;
- ✎ myserver.csr – захтев за сертификат у коме се налази јавни кључ сертификата.

Приватни кључ остаје на серверу и не сме бити јавно доступан. Фајл myserver.csr представља захтев за сертификат и садржај овог фајла треба прекопирати на SCM портал у КОРАКУ 2 за захтевање сертификата. Садржај .csr фајла се може прочитати било којим текст едитором (vi, nano, joe, итд.).

2 Креирање захтева за сертификат за више доменских имена са валидацијом организације

Препоручује се да АМРЕС корисници креирају пар приватни/јавни кључ и захтев за сертификат на серверу на ком планирају да употребе сертификат. Предност креирања кључева на серверу на коме ће сертификат бити употребљен је што приватни кључ неће морати да се пребацује са једног сервера/рачунара на други.

Препоручује се употреба **OpenSSL** софтверског алата на Unix/Linux оперативним системима, док се за друге системе препоручују упутства из SECTIGO базе знања:

- https://support.sectigo.com/Com_KnowledgeProductPage?c=CSR_Generation&k=&lang=
- https://support.sectigo.com/Com_KnowledgeProductPageFaq?c=CSR_Generation&k=&lang=
- https://support.sectigo.com/Com_KnowledgeDetailPage?Id=kA01N000000zFU6

КОРАК 1

Да би AMRES корисник креирао пар приватног/јавног кључа и захтев за сертификат у OpenSSL софтверском алату, неопходно је коришћење шаблонског (*template*) конфигурационог фајла. За креирање захтева за сертификат са више доменских имена потребно је са AMRES веб-сајта преузети шаблонски конфигурациони фајл **MultiSCSreq.cnf** и пребацити га на сервер/рачунар на коме ће се креирати пар кључева и захтев за сертификат. Препоручује се да шаблонски конфигурациони буде постављен у посебан директоријум који ће бити намењен за креирање пара приватног/јавног кључа и захтева за сертификатом.

Конфигурациони фајл **MultiSCSreq.cnf** је потребно изменити у складу са доменским именима које администратор жели да заштити сертификатом. Конфигурациони фајл се може отворити било којим текст едитором (vi, nano, joe, итд.) и изменити. Садржај шаблонског конфигурационог фајла **MultiSCSreq.cnf** је дат у наставку:

```
[ req ]
default_bits          = 2048
default_keyfile       = keyfile.pem
distinguished_name    = req_distinguished_name
encrypt_key           = no
req_extensions        = v3_req

[ req_distinguished_name ]
countryName           = Oznaka zemlje (2 znaka)
countryName_default   = RS
countryName_min       = 2
countryName_max       = 2

stateOrProvinceName   = Pun naziv drzave
localityName           = Lokacija (mesto)
postalCode             = Poštanski broj
streetAddress          = Ulica i broj

organizationName       = Zvanični naziv institucije

0.commonName           = FQDN adresa servera
```

```
0.commonName_max    = 64
```

```
[ v3_req ]
```

```
subjectAltName      = @alt_names
```

```
[ alt_names ]
```

```
DNS.1              =
```

```
DNS.2              =
```

```
DNS.3              =
```

Сваки сертификат за више доменских имена штити једно главно доменско име сервера и потом више алтернативних имена. У конфигурациони фајл **MultiSCSreq.cnf** се приликом измене додају само алтернативна имена, док ће се главно доменско име додати у наредном кораку, приликом креирања пара приватног/јавног кључа и захтева за сертификатом.

Измене конфигурационог фајла је потребно извршити само у делу испод „[alt_names]“. Уколико нпр. администратор жели да заштити укупно 6 доменских имена у једном сертификату, једно име се одређује за главно доменско име, а осталих 5 доменских имена је потребно уписати у конфигурациони фајл **MultiSCSreq.cnf** у делу испод „[alt_names]“ пратећи дати шаблон (DNS.1, DNS.2, DNS.3, DNS.4 и DNS.5). Уколико администратор жели да заштити нпр. 2 доменска имена, једно име се одређује за главно, а друго се уписује у конфигурациони фајл **MultiSCSreq.cnf** у делу испод „[alt_names]“ под променљивом DNS.1, док је остале уносе (DNS.2 и DNS.3) потребно обрисати јер не постоји више од једног алтернативног доменског имена које се штити. Дакле, у конфигурационом фајлу је потребно да постоји X уноса алтернативних имена при чему сваки унос има променљиву DNS.X.

Измењени конфигурациони фајл **MultiSCSreq.cnf** је потребно сачувати и користити у наредном кораку.

КОРАК 2

На серверу на коме се планира употреба сертификата потребно је позиционирати се у директоријуму где се планира креирање пара приватног/јавног кључа и захтева за сертификатом. За Unix/Linux оперативне системе, за почетак потребно је извршити следећу команду:

```
[server]#umask 0377
```

Посматраном командом се постављају адекватне пермисије на свим фајловима који ће бити креирани у поступку креирања пара приватног/јавног кључа.

КОРАК 3

У командној линији сервера са Unix/Linux оперативним системом, потребно је покренути команду за генерисање приватног кључа и захтева за сертификат у коме ће бити садржан јавни кључ:

```
[server]# openssl req -new -config MultiSCSreq.cnf -utf8 -sha256 -keyout myserver.key -out myserver.csr
```

НАПОМЕНА: у оквиру команде могуће је подесити и додатне параметре, као што је нпр. величина кључа, опцијом **-newkey rsa:4096**, или променити нпр. **sha** алгоритам опцијом **-sha512**.

Након покретања команде администратор ће добити низ питања на које је потребно да одговори у складу са подацима који треба да буду уписани у сертификату (Ознака земље, Локација-град, Институција, Назив организационе јединице, FQDN име сервера). FQDN име сервера представља главно доменско име које ће бити заштићено SSL/TLS сертификатом. Алтернативна доменска имена су већ

уписана у конфигурациони фајл **MultiSCSreq.cnf** у делу испод „[alt_names]“ и биће аутоматски унета у захтев за сертификат.

НАПОМЕНА: Поље *stateOrProvinceName*, тј. *Пун назив државе* потребно је оставити празно.

Након попуњавања свих неопходних података, у директоријуму ће бити креирана два нова фајла:

- ⌘ myserver.key – приватни кључ сертификата;
- ⌘ myserver.csr – захтев за сертификат у коме се налази јавни кључ сертификата.

Приватни кључ остаје на серверу и не сме бити јавно доступан. Фајл myserver.csr представља захтев за сертификат и садржај овог фајла треба прекопирати на SCM портал у КОРАКУ 2 за захтевање сертификата. Садржај .csr фајла се може прочитати било којим текст едитором (vi, nano, jое, итд.).