



Упутство за TCS администраторе

Историја верзија документа

Верзија	Датум	Иницијали аутора	Опис промене
1.0	2020.	АТ	Прва верзија овог документа
2.0	2025.	АТ, КС	Друга верзија овог документа

Садржај

УПУТСТВО ЗА TCS АДМИНИСТРАТОРЕ	0
1 УВОД	4
2 ПРИСТУП HARICA ПОРТАЛУ	5
2.1 Приступ HARICA ПОРТАЛУ - <i>ENTERPRISE ADMIN</i>	5
2.2 Приступ HARICA ПОРТАЛУ - <i>ENTERPRISE APPROVER</i>	9
3 ПОСУПАК КРЕИРАЊА ДРУГИХ АДМИНИСТРАТОРА	9
3.1 Поступак доделе улога <i>ENTERPRISE ADMIN</i> и <i>ENTERPRISE APPROVER</i>	9
4 ПОСТУПАК КРЕИРАЊА И ВАЛИДАЦИЈЕ ДОМЕНА	11
4.1 Додавање домена	11
4.2 Валидација домена	12
5 ПОСТУПАК ЗАХТЕВАЊА И ПРИБАВЉАЊА СЕРТИФИКАТА	15
5.1 Поступак захтевања <i>SSL</i> СЕРТИФИКАТА	15
5.1.1 <i>Auto-generate CSR – аутоматско креирање</i> захтева за сертификат у претраживачу	18
5.1.2 <i>Manual creation of CSR – копирање</i> захтева за сертификат који је претходно креиран ..	20
5.2 Поступак захтевања клијентских <i>S/MIME</i> СЕРТИФИКАТА	20
5.2.1 Поступак креирања локалног налога за крајње кориснике	21
5.2.2 Поступак захтевања и преузимања клијентских <i>E-mail only</i> сертификата	29
5.2.3 Поступак захтевања клијентских (<i>IV+OV</i>) email сертификата	33
5.3 Поступак одобравања <i>SSL</i> СЕРТИФИКАТА	36
5.3.1 Поступак одобравања <i>SSL</i> сертификата	36
5.3.2 Поступак одобравања клијентских (<i>IV+OV</i>) email сертификата	38
5.4 Поступак ПРЕУЗИМАЊА СЕРТИФИКАТА	39
5.4.1 Поступак преузимања <i>SSL</i> сертификата	39
5.4.2 Поступак преузимања клијентских (<i>IV+OV</i>) email сертификата	40
ДОДАТАК А – КРЕИРАЊЕ ЗАХТЕВА ЗА СЕРТИФИКАТ	42
1 КРЕИРАЊЕ ЗАХТЕВА ЗА СЕРТИФИКАТ ЗА ЈЕДНО ДОМЕНСКО ИМЕ (SSL) И ЗА СВА ПОДДОМЕНСКА ИМЕНА ЈЕДНОГ ДОМЕНА СА ВАЛИДАЦИЈОМ ОРГАНИЗАЦИЈЕ (WILDCARD)	42
2 КРЕИРАЊЕ ЗАХТЕВА ЗА СЕРТИФИКАТ ЗА ВИШЕ ДОМЕНСКИХ ИМЕНА СА ВАЛИДАЦИЈОМ ОРГАНИЗАЦИЈЕ	43

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 HARICA портала који се налази на следећој веб-адреси:

<https://cm.harica.gr/>

Преко портала се обављају све акције у вези са администрацијом, валидацијом, захтевањем и издавањем TCS сертификата.

Како би AMPEC корисник добио приступ TCS HARICA порталу потребно је испунити следеће предуслове:

1. AMPEC корисник има регистрован домен у оквиру "ac.rs", "edu.rs" и "gov.rs" домена;
2. AMPEC корисник се регистровао за коришћење TCS услуге;
3. Администратор AMPEC корисника (TCS администратор) има један од налога за федеративни приступ порталу:
 - а) администраторски налог у AMPEC Админ бази података коју хостује AMPEC или
 - б) налог за запослене у оквиру Даваоца идентитета своје институције који је регистрован у иAMPEC Федерацији Идентитета, а који је придружен *eduGAIN* интерфедерацији;
4. TCS администратор је добио потврду од AMPEC о успешној регистрацији и валидацији организације у оквиру TCS HARICA портала.

HARICA портал разликује следеће улоге:

Обичан корисник – Корисник који је регистрован на HARICA порталу и препознат да припада својој институцији на основу домена своје мејл адресе. Нема додатне привилегије и може да захтева сертификате.

Enterprise Manager - Администратор највишег нивоа HARICA портала. Има контролу над свим организацијама, сертификатима, доменима и обавештењима свих организација. Шаље захтеве за додавање нових организација на портал и врши валидацију организација. *Enterprise Manager* додељује улогу *Enterprise Admin* администраторима. **AMPEC има Enterprise Manager улогу на порталу.**

Enterprise Admin - Администратор коме је та улога додељена од стране *Enterprise Manager* администратора или другог *Enterprise Admin* администратора, у циљу управљања сертификатима и администраторима организације. Може да додели *SSL and S/MIME Approver* улогу кориснику у оквиру своје организације. *Enterprise Admin* може да упути захтев за нове домene и да врши валидацију домена за своју организацију, али не може креирати нове организације нити уређивати опште податке организације чак и ако им је делегирана контрола над том организацијом. Такође може и захтевати сертификате које *Enterprise Approver* мора да одобри.

Enterprise Approver – Администратор који има *SSL and S/MIME Approver* улогу. Врши утврђивање и одобравање SSL и S/MIME захтева за сертификатима у оквиру организације којој припада. Има приступ свим сертификатима у оквиру организације којој припада.

TCS администратори ће добити *Enterprise Admin* улогу у оквиру своје организације. Да би то постали неопходно је да региструју налоге на HARICA порталу. Након регистрације, *Enterprise Manager (AMPEC)* ће им доделити *Enterprise Admin* улогу у оквиру њихове организације.

Како би *Enterprise Admin* имао могућност захтевања дигиталних сертификата, неопходно је да прође следеће кораке:

1. Приликом првог логовања на портал потребно је одобрити 2FA и проверити да ли се у бази налази **eduPersonEntitlement** атрибут са дефинисаном вредношћу **urn:mace:amres.ac.rs:amres:entitlement:tcs:admin**;
Омогућавање 2FA је обавезно и без тога није могуће доделити било какву улогу Вашем корисничком налогу.
2. ОПЦИОНО: доделити и другим корисницима у оквиру исте организације *Enterprise Admin* или *Enterprise Approver* улогу.
3. Проћи кроз процедуру креирања и валидације домена;
4. Захтевати сертификате, након што је организација валидирана од стране *Enterprise Manager* (AMPEC) и након што су домени креирани и валидирани од стране *Enterprise Admin* администратора.

У наставку документа детаљно су описани наведени кораци.

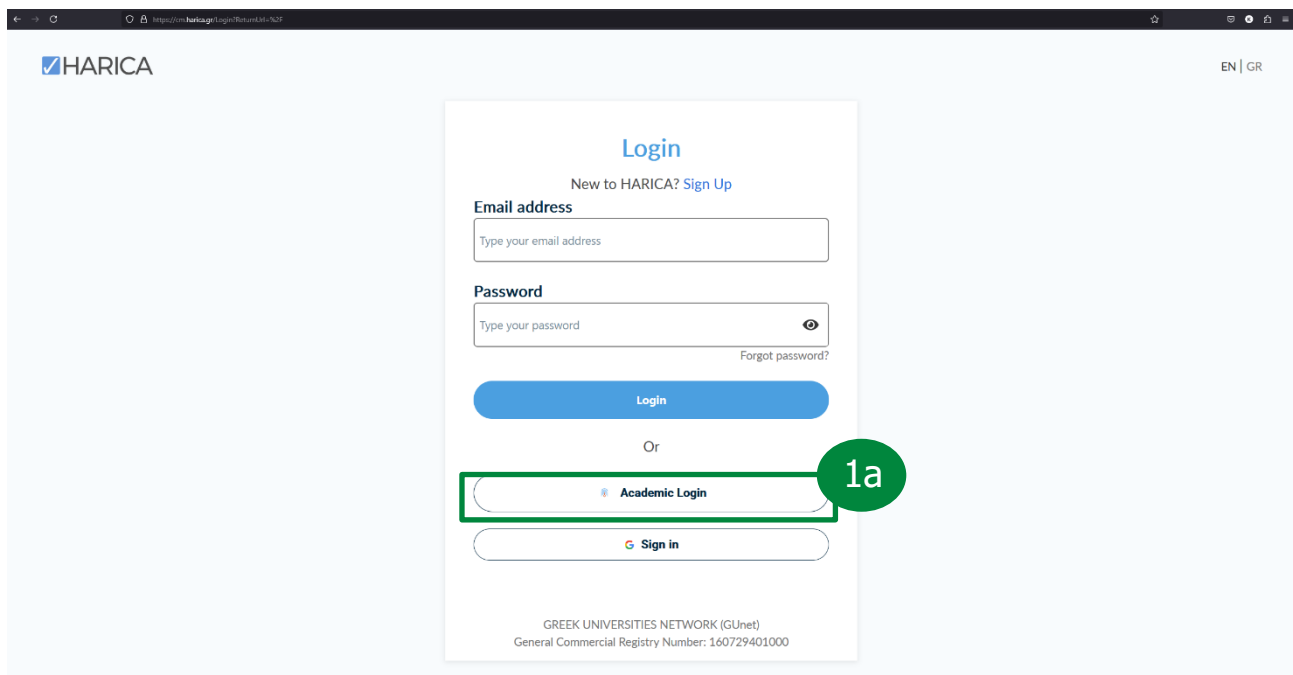
2 Приступ HARICA порталу

Након успешне регистрације AMPEC корисника за коришћење TCS услуге и завршене процедуре пријаве организације и њене валидације од стране AMPEC-а, TCS администратор добија могућност пријаве на HARICA портал.

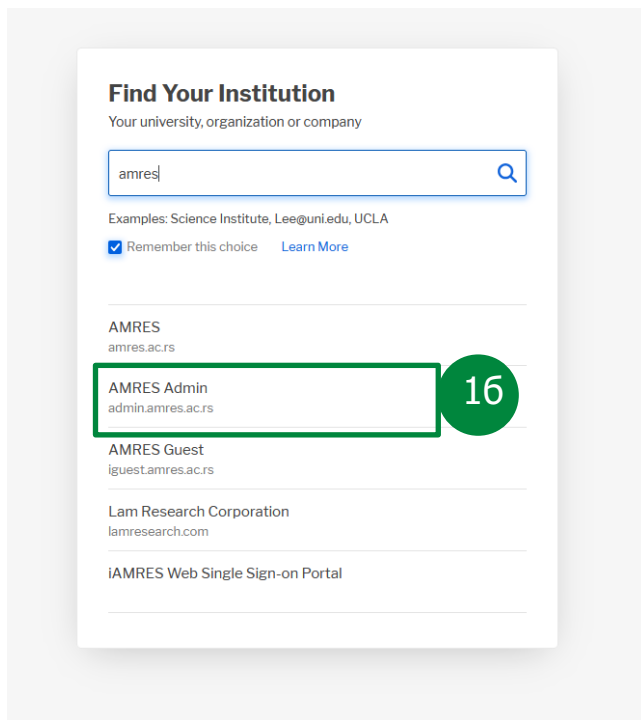
2.1 Приступ HARICA порталу - *Enterprise Admin*

Корисник приступа порталу који је доступан на адреси <https://cm.harica.gr/>.

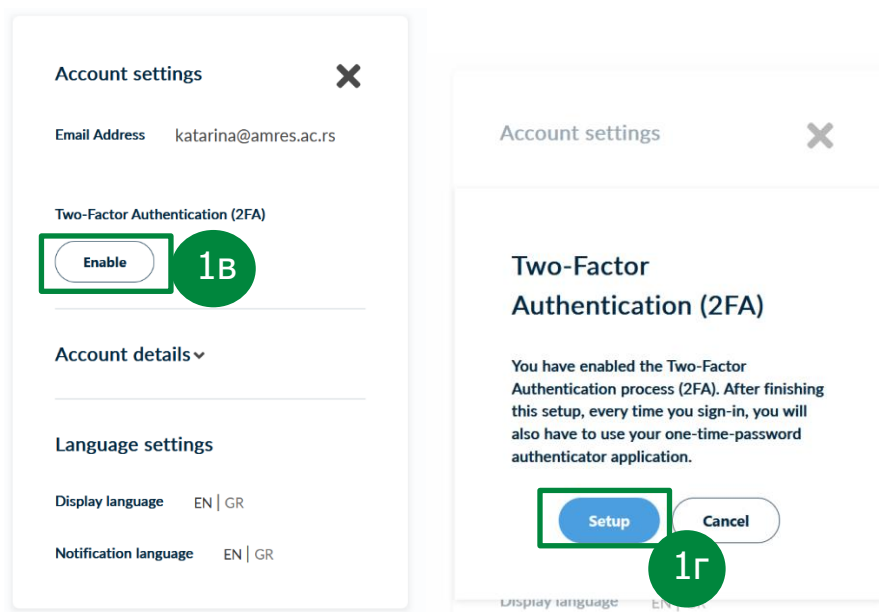
Потребно је изабрати *Academic Login* опцију. (1a).



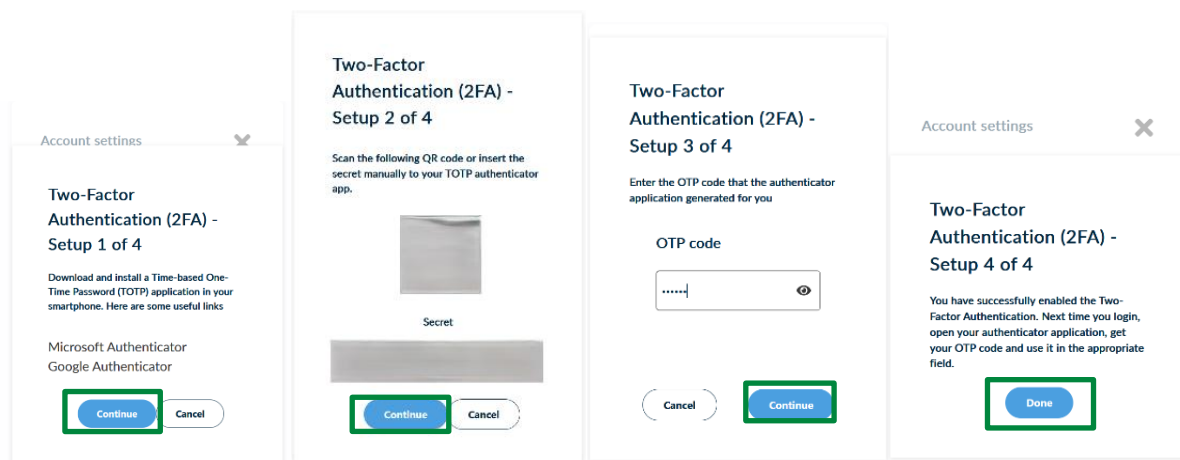
- Уколико институција којој администратор припада има регистрован Давалац идентитета у оквиру иАМРЕС Федерације Идентитета, који је придружен eduGAIN интерфедерацији, може се улоговати коришћењем те опције.
- Уколико то није случај, администратор мора имати свој налог за АМРЕС администраторе у бази која је повезана са АМРЕС Админ Давоцем идентитета и коју хостује АМРЕС. (16)



Након успешне аутентификације неопходно је одобрити 2FA аутентификацију. У горњем десном углу, кликните на Ваше име, а затим изабрати *Profile* и омогућите 2FA (1в), након тога ће се прозор са подешавањима сам покренути (1г).



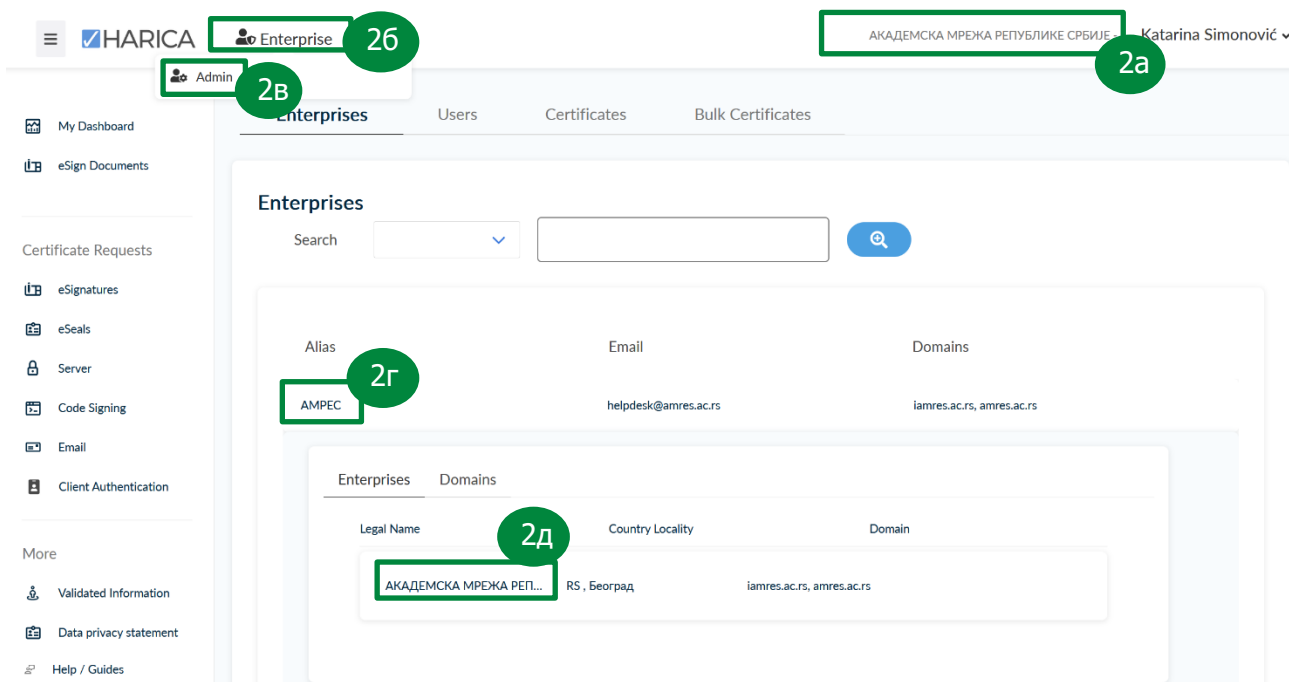
Затим ће се појавити мало упутство од пар корака које је потребно испратити, за то вам је потребан *smart* телефон. Неопходно је да инсталирате *Google Authenticator*, TOTP или сличну апликацију на вашем телефону и скенирате одговарајући QR код, затим ћете на телефону добити генерисан шестоцифрени број који ћете користити за аутентификацију.



Корисник сада има приступ организацији којој припада (2a), а да би постао администратор неопходно је да се јави на tcs@amres.ac.rs. Након што му се додели улога *Enterprise Admin*, администратор може да приступи организацији тако што у главном менију одабере опцију *Enterprise* (26), затим у менију другог нивоа опцију *Admin* (2в), затим кликне на назив своје организације (2г).

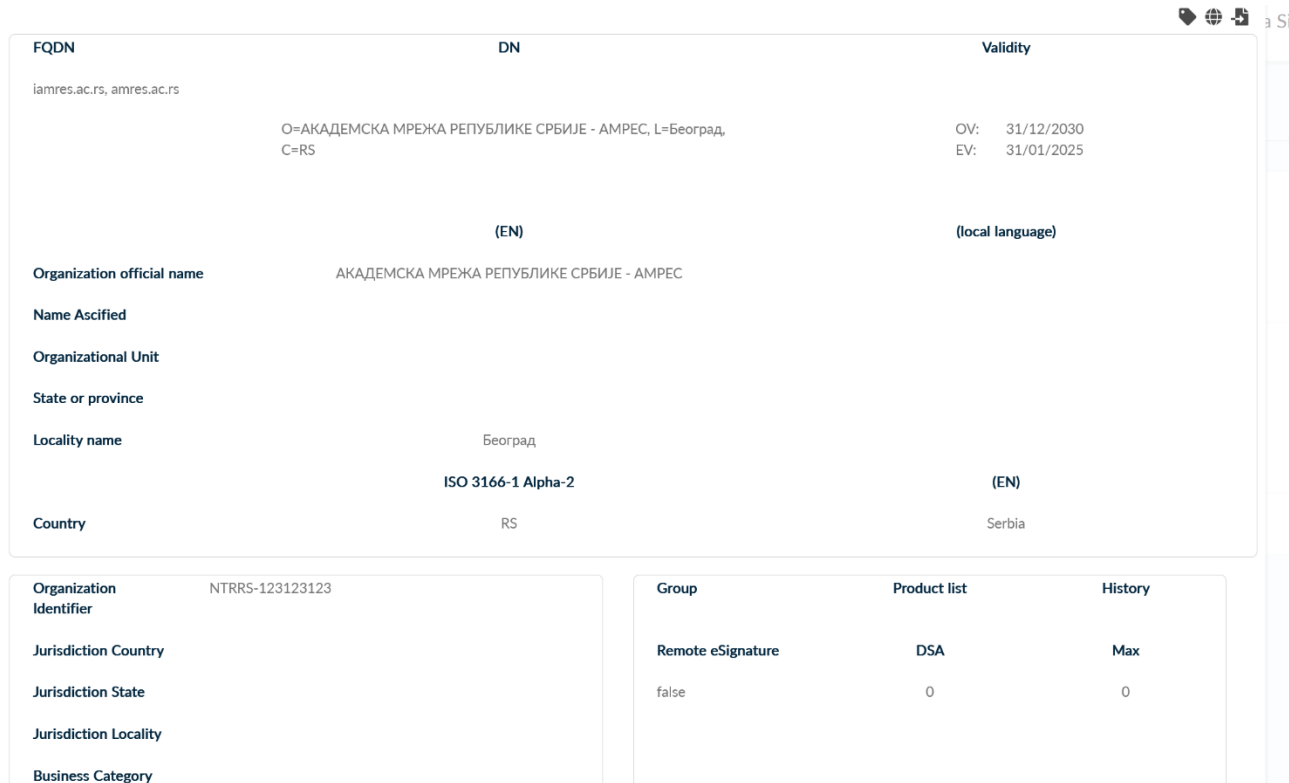
Након овог корака отвара се прозор у коме се налазе подаци и подешавања организације. Први таб *Enterprises* приказује опште информације о организацији. Њих дефинише *Enterprise Manager* и оне се не могу мењати:

- Званичан назив организације;
- Град, Држава;
- Додати домени.



The screenshot shows the HARICA portal interface. The top navigation bar includes the HARICA logo, a user profile dropdown (Katarina Simonović), and a language selector (2a). The left sidebar contains various menu items like 'My Dashboard', 'eSign Documents', 'Certificate Requests', 'eSignatures', 'eSeals', 'Server', 'Code Signing', 'Email', 'Client Authentication', 'Validated Information', 'Data privacy statement', and 'Help / Guides'. The main content area is titled 'Enterprises' and features a search bar. Below the search bar, there is a table with columns: Alias (2г), Email, and Domains. The first row shows 'AMPEC' as the alias, 'helpdesk@amres.ac.rs' as the email, and 'iamres.ac.rs, amres.ac.rs' as domains. Below this table, there is a modal window with tabs for 'Enterprises' and 'Domains'. The 'Enterprises' tab is active, showing a table with columns: Legal Name (2д), Country Locality, and Domain. The first row shows 'АКАДЕМСКА МРЕЖА РЕПУБЛИКЕ СРБИЈЕ - АМРЕС' as the legal name, 'RS, Београд' as the country locality, and 'iamres.ac.rs, amres.ac.rs' as the domain.

Кликом на званичан назив организације (2д) отвара се прозор са наведеним детаљним подацима о организацији, као што је приказано на слици испод:



The screenshot shows the detailed view of the 'AMPEC' organization. The top section displays the FQDN (iamres.ac.rs, amres.ac.rs), DN (O=АКАДЕМСКА МРЕЖА РЕПУБЛИКЕ СРБИЈЕ - АМРЕС, L=Београд, C=RS), and Validity (OV: 31/12/2030, EV: 31/01/2025). Below this, there is a section for the organization's name in English (EN) and local language. The 'Organization official name' is 'АКАДЕМСКА МРЕЖА РЕПУБЛИКЕ СРБИЈЕ - АМРЕС'. The 'Name Ascified' is 'AMPEC'. The 'Organizational Unit' is 'AMPEC'. The 'State or province' is 'Београд'. The 'Locality name' is 'Београд'. The 'Country' is 'RS' (Serbia). Below this, there is a section for the organization's identifier and jurisdiction. The 'Organization Identifier' is 'NTRRS-123123123'. The 'Jurisdiction Country' is 'RS'. The 'Jurisdiction State' is 'RS'. The 'Jurisdiction Locality' is 'RS'. The 'Business Category' is 'RS'. The bottom section displays the 'Group' (Remote eSignature), 'Product list' (DSA), and 'History' (Max). The 'Remote eSignature' is 'false'. The 'DSA' is '0'. The 'Max' is '0'.

Наредни табови приказани су следећим редоследом:

- *Users* – садржи податке о свим корисницима у оквиру организације
- *Certificates* – садржи податке о свим сертификатима који су поднети у оквиру организације
- *Bulk Certificates* - садржи податке о свим *Bulk* сертификатима који су захтевани у оквиру организације

2.2 Приступ HARICA порталу - *Enterprise Approver*

Enterprise Approver на HARICA порталу региструје свој налог на исти начин на који то чини и *Enterprise Admin*, с тим што ће њему *Enterprise Approver* улогу доделити *Enterprise Admin* (у даљем тексту: Админ) те организације, што ће бити објашњено у наставку.

3 Посупак креирања других администратора

Админ у оквиру своје организације може да додели улоге:

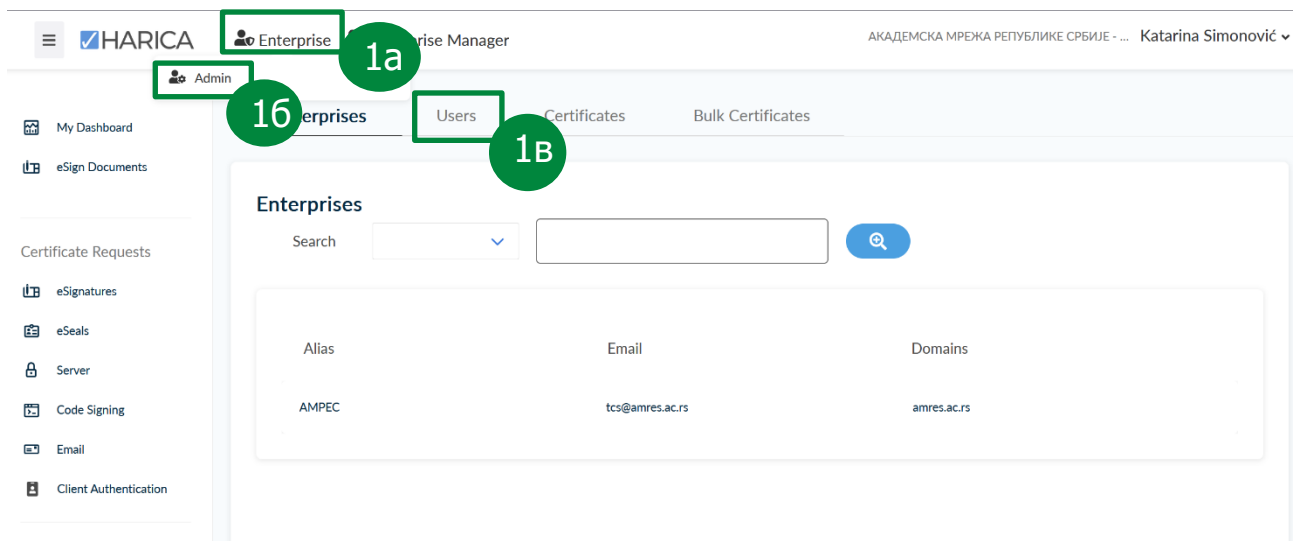
- *Enterprise Admin* за друге кориснике;
- *Enterprise Approver* – *SSL Enterprise Approver*;
- *Enterprise Approver* – *SMIME Enterprise Approver*;
- *Enterprise Approver* за све типове сертификата.

3.1 Поступак доделе улога *Enterprise Admin* и *Enterprise Approver*

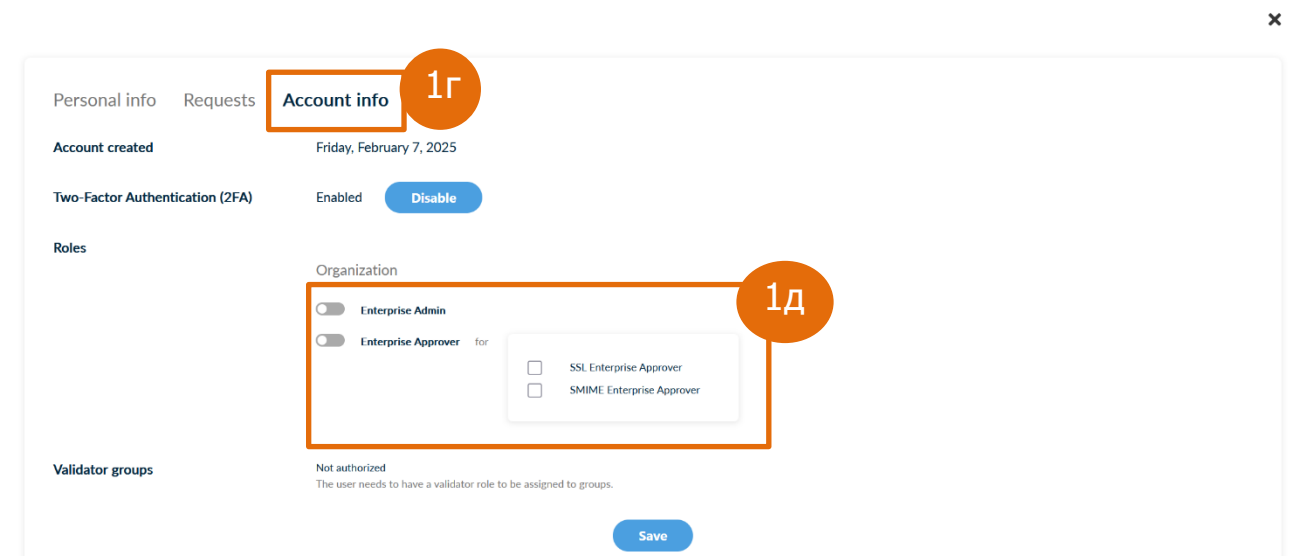
Админ може да додели улогу и *Enterprise Admin* и *Enterprise Approver*. Поступак додељивања је исти.

Како би админ доделио кориснику улогу админа било ког типа, неопходно је да је тај корисник већ регистрован на HARICA порталу и да има омогућену 2FA у оквиру свог налога. Приликом логовања својим федеративним налогом, корисник као један од атрибута шаље и мејл, чија вредност садржи и домен институције којој припада. Ако се овај домен у оквиру вредности мејл атрибута поклапа са доменом институције регистрованој на HARICA порталу, корисник ће аутоматски постати део те организације и биће видљив Админу.

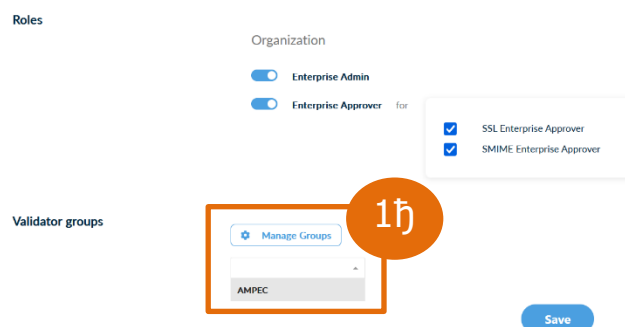
Како би додао новог администратора потребно је да Админ у главном менију одабере опцију *Enterprise (1a)*, а затим у менију другог нивоа опцију *Admin (16)*, и да потражи таб *Users (1b)*, у оквиру кога су излистани сви крајњи корисници који су креирали налог.



Кликом на корисника, отвориће се ново поље са његовим информацијама, и оквиру кога је неопходно кликнути на таб *Account info* (1г). У оквиру овог прозора у секцији *Roles* дефинисане су улоге које могу бити додељене кориснику (1д). Корисник истовремено може имати више улога.



Приликом доделе улоге, *Validators Group* поље ће постати активно и онда ће администратор дефинисати за коју организацију је улога додељена (1ђ).



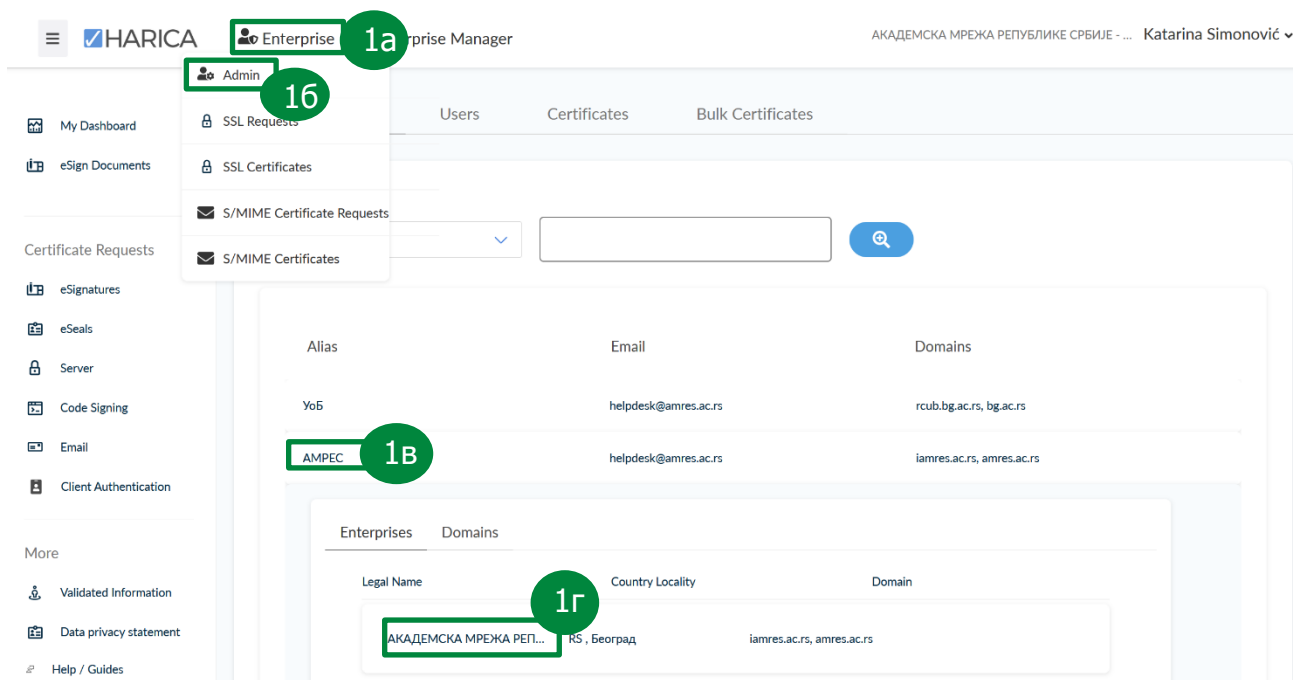
НАПОМЕНА: За одабир ће бити доступне само организације највишег нивоа, тј. групе. У оквиру портала могу се додати и подорганизације (*Affiliate Enterprise*) у оквиру исте групе. Један Админ може да управља већим бројем организација у истој групи.

4 Поступак креирања и валидације домена

Админ може да креира и управља доменима за организацију која му је додељена.

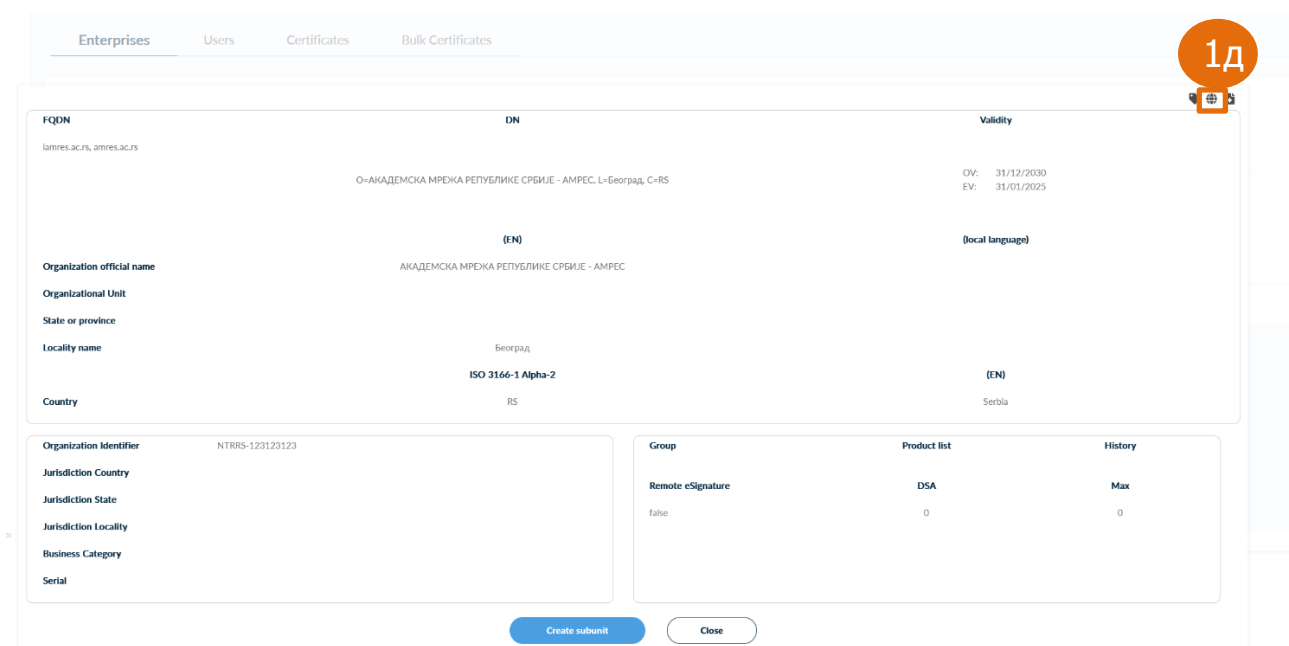
4.1 Додавање домена

Како би Админ додао нови домен, потребно је да у главном менију одабере опцију *Enterprise* (1a), затим у менију другог нивоа опцију *Admin* (16), затим у листи кликне на своју организацију (1в), па кликне на *Legal Name* (1г).



The screenshot shows the HARICA Enterprise Manager interface. The left sidebar contains a menu with items like 'My Dashboard', 'eSign Documents', 'Certificate Requests', 'eSignatures', 'eSeals', 'Server', 'Code Signing', 'Email', 'Client Authentication', and 'More'. The main area shows the 'Enterprise Manager' section with tabs for 'Users', 'Certificates', and 'Bulk Certificates'. A dropdown menu is open under the 'Enterprise' header, showing 'Admin' (16), 'SSL Requests', 'SSL Certificates', 'S/MIME Certificate Requests', and 'S/MIME Certificates'. Below this, a table lists organizations. The 'AMRES' entry (1в) is highlighted. A modal window is open for the 'AMRES' organization, showing the 'Enterprises' tab. The 'Legal Name' field (1г) is highlighted, containing the text 'АКАДЕМСКА МРЕЖА РЕПУБЛИКЕ СРБИЈЕ'.

Појавиће се прозор у коме је потребно да кликнете на иконицу *Add Domains* (1д).



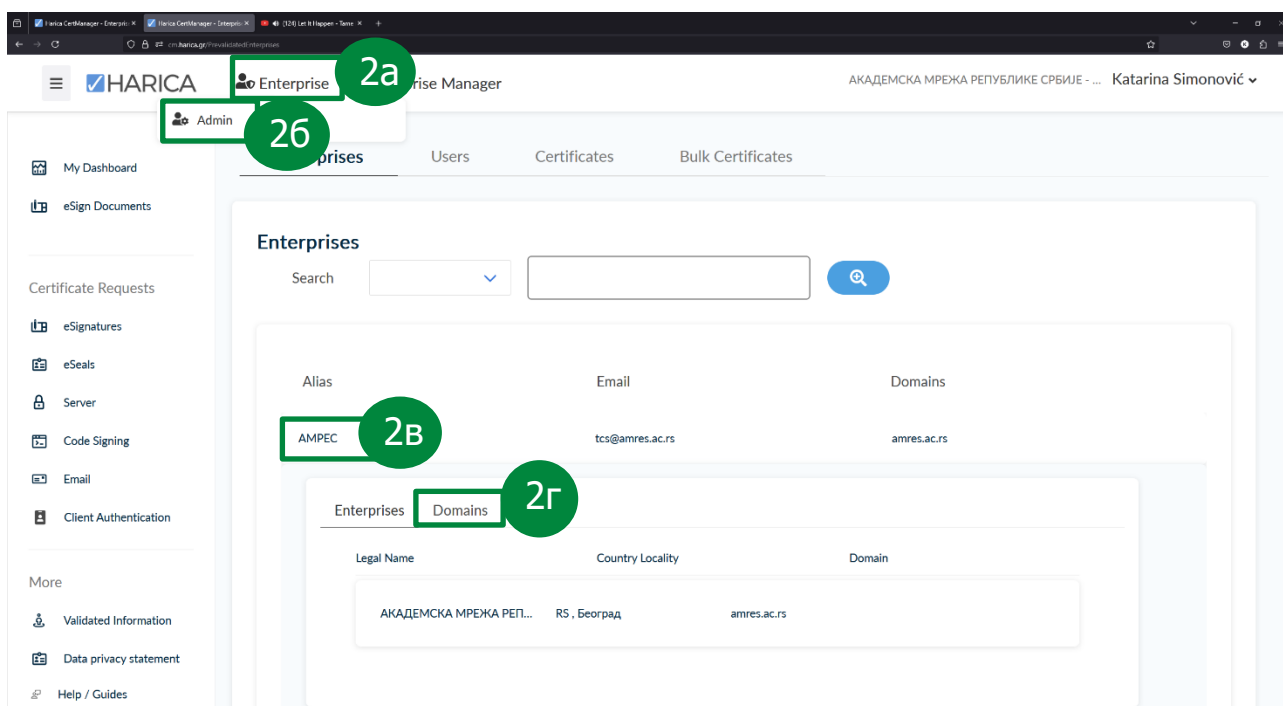
Након тога ће се појавити нови прозор где је потребно прво да скинете *CSV Sample file* (1ђ), у оквиру кога избришете домене који су наведени као пример и додате своје, по истом шаблону. Затим, додате ваш CSV фајл на портал (1е), и онда кликнете *upload* (1ж). Нови домени ће постати видљиви обично у року једног радног дана, након што HARICA ревидира и одобри фајл.



4.2 Валидација домена

Процесом валидације домена, HARICA проверава да ли АМРЕС корисник контролише домене за које жели да прибавља сертификате. Домен се валидира на годину дана.

Како би започео валидацију домена, потребно је да Админ у главном менију одабере опцију *Enterprise* (2а), затим у менију другог нивоа опцију *Admin* (2б), затим кликне на своју организацију (2в) и *Domains* таб (2г).



У оквиру поља *Domains* може бити више домена за валидацију, валидира се сваки посебно кликом на *Validate Domain* (2д).

Enterprises		Domains
Domain	Validity	
iamres.ac.rs	10/03/2026	Validate Domain
amres.ac.rs	10/03/2026	Validate Domain

Појавиће се прозор који нуди одабир начина валидације:

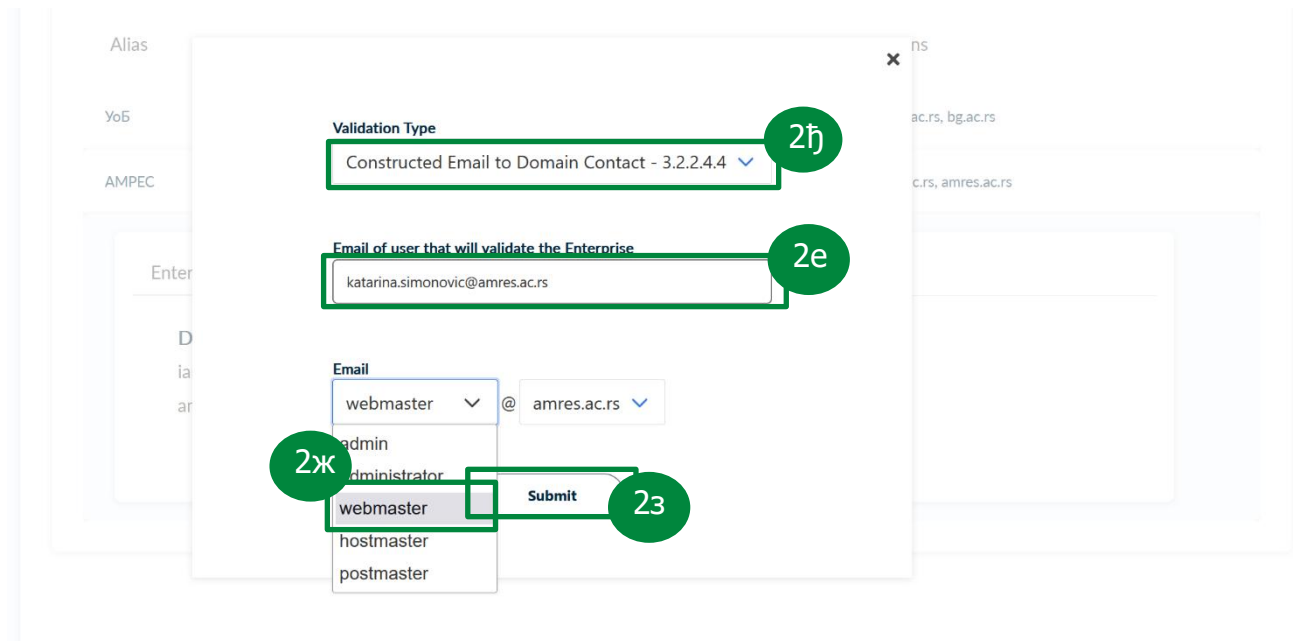
- *Constructed Email to Domain Contact* - ова опција подразумева слање мејла са линком за валидацију на једну од пет адреса, нпр. "admin@bg.ac.rs", "administrator@bg.ac.rs", "hostmaster@bg.ac.rs", "postmaster@bg.ac.rs" или "webmaster@bg.ac.rs";
- *DNS Change* - ова опција подразумева додавање CNAME записа у облику *hash* вредности у DNS зону домена који се валидира.

У овом упутству биће објашњена валидација путем мејла (2ђ).

Након што се одабере опција *Email* (2ђ), **неопходно је да админ унесе свој мејл или мејл особе која је такође регистрована на HARICA порталу за потребе валидације домена (2е), из свог домена, и затим одабере мејл адресу на коју жели да пошаље линк за валидацију домена (2ж).**

НАПОМЕНА: Уколико Админ у пољу (2е) не наведе исправну мејл адресу која постоји на порталу, мејл за валидацију неће бити послат.

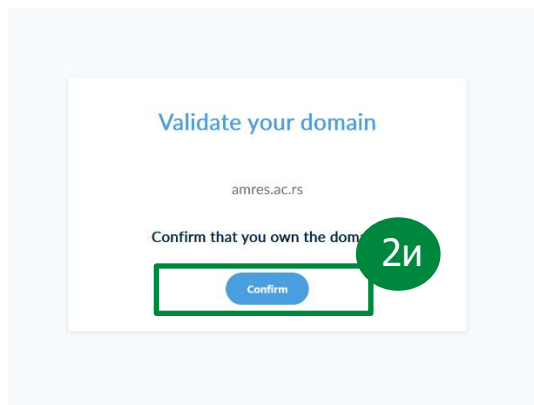
Након што се одабере мејл адреса за валидацију домена (2ж), потребно је кликнути на *Submit* дугме (2з) чиме се аутоматски шаље мејл на одабрану адресу.



The screenshot shows a web form for domain validation. Annotations highlight the following elements:

- 2ђ:** Points to the "Validation Type" dropdown menu, which is currently set to "Constructed Email to Domain Contact - 3.2.2.4.4".
- 2е:** Points to the "Email of user that will validate the Enterprise" text input field, containing the email address "katarina.simonovic@amres.ac.rs".
- 2ж:** Points to the "Email" dropdown menu, which is open and shows a list of email addresses including "webmaster", "admin", "administrator", "webmaster", "hostmaster", and "postmaster".
- 2з:** Points to the "Submit" button, which is located next to the "Email" dropdown menu.

Кликом на линк из примљеног мејла (досупан кликом на реч *Confirm*), отвориће се страница на којој је потребно потврдити да администратор контролише домен и да је домен валидан, кликом на *Confirm* дугме (2и).



The screenshot shows a confirmation page titled "Validate your domain". The domain "amres.ac.rs" is displayed. Below the domain name, there is a text prompt "Confirm that you own the domain" and a blue "Confirm" button. Annotation **2и** points to the "Confirm" button.

Након неког времена, на мејл који је дефинисан приликом регистрације организације стићи ће потврда да је домен валидиран.

НАПОМЕНА: Често је потребно копирати линк у оквиру претраживача или чак користити *Incognito* прозор, како би се избегла колизија са активном сесијом. Уколико дође до колизије, нећете видети страницу приказану изнад и домен неће бити валидан.

5 Поступак захтевања и прибављања сертификата

Да би било могуће захтевати дигиталне сертификате неопходно је да претходно буду испуњени следећи предуслови:

1. AMRES корисник мора имати регистрован домен у оквиру "ac.rs", "edu.rs" и "gov.rs" домена ,
2. AMRES корисник мора бити регистрован за коришћење TCS услуге и мора имати креирану организацију и регистрован и додељен *Enterprise Admin* налог на HARICA порталу,
3. *Enterprise Admin* је успешно креирао и делегирао домен, и комплетирао процедуру валидације домена.

Уколико су сву предуслови испуњени, преко HARICA портала може се захтевати неограничен број сертификата.

Поступак захтевања сертификата на порталу се разликује у зависности од типа сертификата, а на порталу се може захтевати неколико типова сертификата:

- *eSignatures;*
- *eSeals;*
- **Server – доступан бесплатно у оквиру TCS услуге;**
- *Code Signing;*
- **Email - доступан бесплатно у оквиру TCS услуге;**
- *Client Authentication;*

У упутству ће бити описан начин прибављања сертификата путем корисничког интерфејса HARICA портала.

НАПОМЕНА: У документу ће бити описани само поступци захтевања и издавања **серверских** и **S/MIME** сертификата, сви остали се тренутно додатно наплаћују.

5.1 Поступак захтевања **SSL** сертификата

Препоручује се да AMRES корисници, корисници TCS услуге, креирају приватни 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 приватног кључа и захтева за сертификат за *Linux* платформу описан је у Додатку А.

Како би админ започео сам процес захтевања сертификата, потребно је да у главном менију одабере опцију *Server* и попуни основне информације о будућем сертификату.

У овом кораку је опционо да ли ћете попунити *Friendly name* поље, оно је видљиво само на HARICA порталу (1a), али оно што јесте важно је да у овом кораку дефинишете домен за сертификат (16) или више домена уколико вам је потребно (1b). Након тога идете на поље *Next* (1r).

НАПОМЕНА: Уколико захтевате мултидоменски сертификат, алтернативна доменска имена додајете у овом кораку, пошто неће бити касније аутоматски додата из CSR захтева. Уколико прескочите овај корак, сертификат ће обухватити само једно доменско име које наведете.

 My Dashboard

 eSign Documents

Certificate Requests

 eSignatures

 eSeals

 **Server**

 Code Signing

 Email

 Client Authentication

More

 Validated Information

 Data privacy statement

 Help / Guides

Server Certificates / Request new certificate

1. Request

2. Validate

3. Retrieve

Domains Product Details Authorization Summary Submit

Friendly name (optional)

A custom label to help you identify this certificate in your dashboard

testni sertifikat

Add Domains Manually or via [Import](#)

supported: onion v3, Wildcard, Internationalized Domain Name (IDN)

test.amres.ac.rs

☒ Include **www.test.amres.ac.rs** without additional cost.

+ Add more domains

The maximum number of domains allowed per request is 100.

Next

У овом упутству ћемо изабрати OV сертификат (1д).

НАПОМЕНА: Потребно је одабрати опцију која је означена као **Free**.

 My Dashboard

 eSign Documents

Certificate Requests

 eSignatures

 eSeals

 **Server**

 Code Signing

 Email

 Client Authentication

More

 Validated Information

 Data privacy statement

 Help / Guides

GREEK UNIVERSITIES NETWORK (GUNet)
General Commercial Registry Number: 10072942000

Server Certificates / Request new certificate

1. Request

2. Validate

3. Retrieve

Domains Product Details Authorization Summary Submit

Select the type of your certificate

Domain-only (DV)

SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:

- One or more domains

Select

Free

For enterprises or organizations (OV)

SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:

- One or more domains
- Information of your organization that owns/controls the domains

Select

Free

For enterprises or organizations (EV)

SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:

- One or more domains
- Information of your organization that owns/controls the domains
- Official registry information of your organization

Select

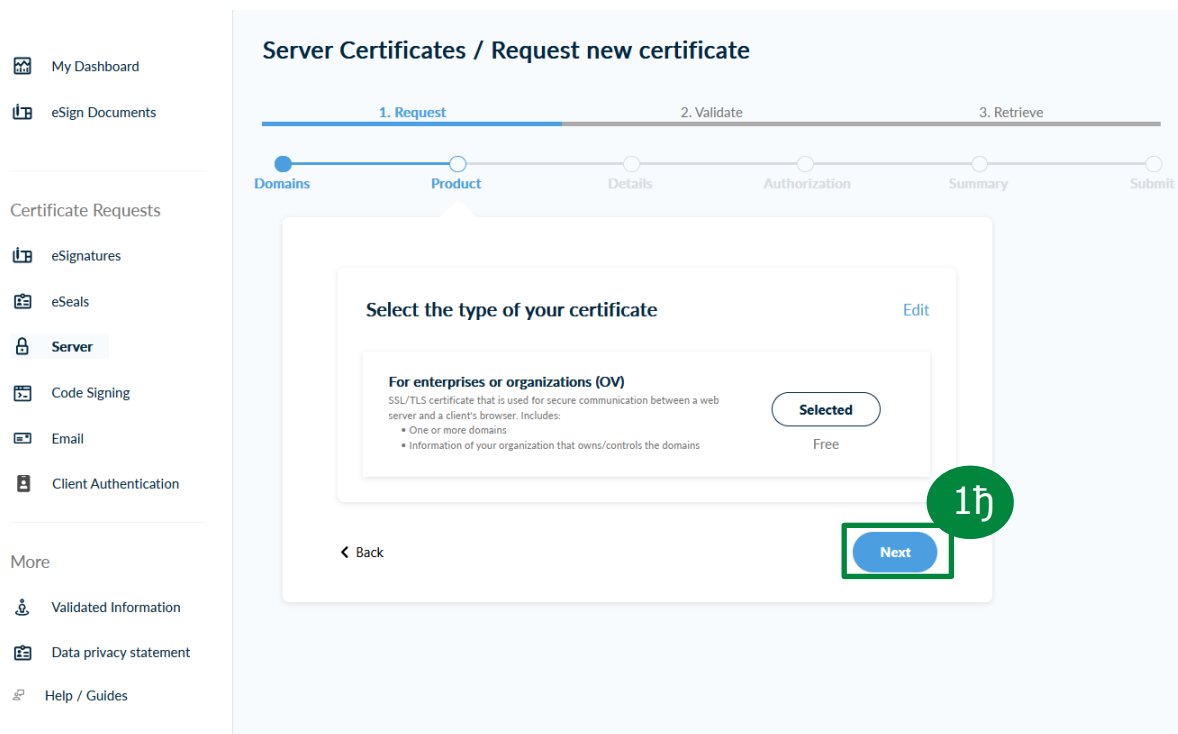
from

275€ year

Back

Next

Након тога ће вас портал преbacити на следеће поље где ћете потврдити ваш избор сертификата кликом на поље *Next* (1ђ).



Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

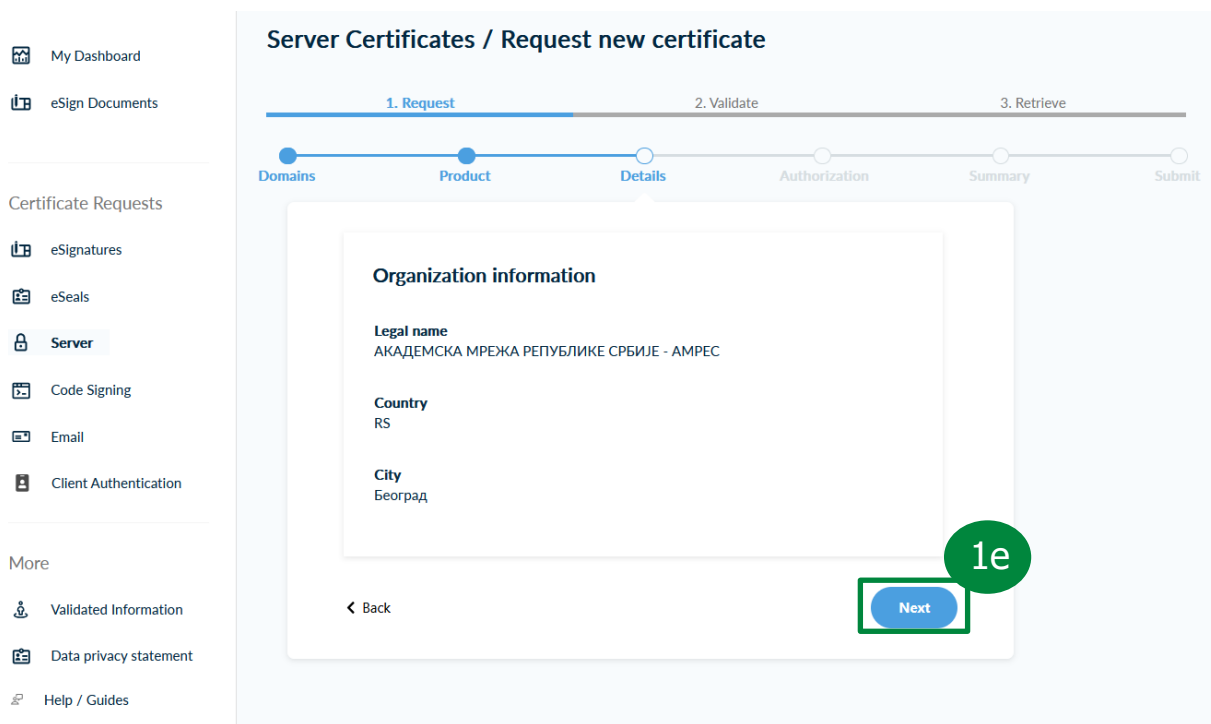
Select the type of your certificate [Edit](#)

For enterprises or organizations (OV)
 SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:
 • One or more domains
 • Information of your organization that owns/controls the domains

Selected Free

[Back](#) [Next](#)

Затим је потребно да потврдите информације о организацији које су достављене приликом регистрације, кликом на поље *Next* (1е).



Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Organization information

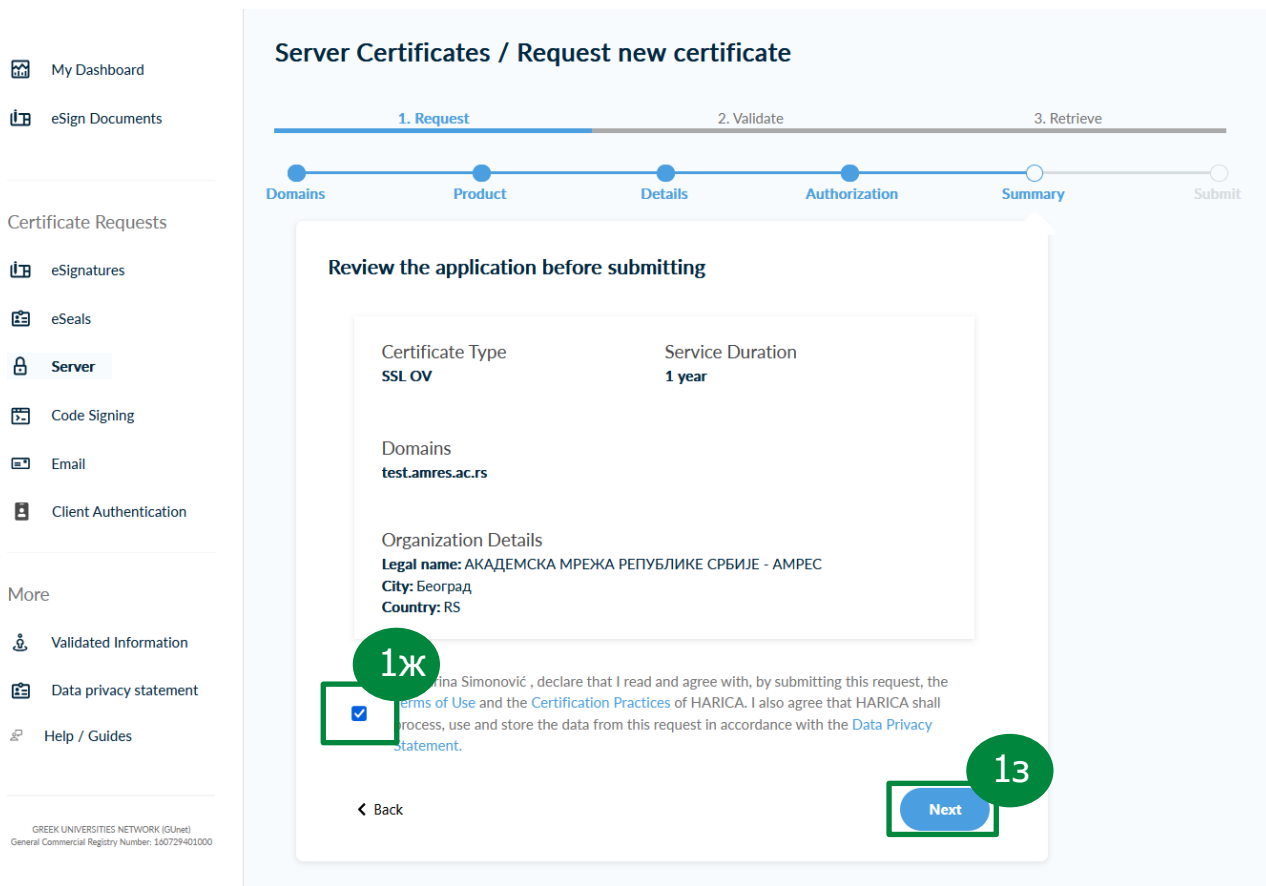
Legal name
 АКАДЕМСКА МРЕЖА РЕПУБЛИКЕ СРБИЈЕ - АМРЕС

Country
 RS

City
 Београд

[Back](#) [Next](#)

На крају ће се појавити прозор као преглед вашег захтева за сертификат, где је потребно да штиклирате да се слажете са условима коришћење (1ж) и кликнете на поље *Next* (13).



Отвориће се прозор који захтева спецификацију начина креирања захтева:

- *Auto-generate CSR* – захтев за сертификат се креира у самом претраживачу;
- *Manual creation of CSR* – захтев за сертификат претходно је креиран и потребно га је копирати у наредном кораку.

Админ може користити било коју опцију и обе ће бити објашњене у наставку.

5.1.1 ***Auto-generate CSR*** – аутоматско креирање захтева за сертификат у претраживачу

У случају да се одлучите за *Auto-generate CSR* (1и) отвориће се нови мени где је потребно изабрати алгоритам енкрипције и величину кључа (1ј), а затим поставити *passphrase* (1к). Запамтите ову шифру она ће вам бити потребна када будете постављали сертификат на сервер. Затим је неопходно сложити се са условима коришћења (1л), и кликнути на поље *Generate Private Key, CSR, and submit order* (1љ).

Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Submit Request

What is a CSR?

1и or

You will create a Private Key in your browser and your CSR will be auto-generated.

1j **1к**

1л

☒ I understand that this passphrase is under my sole knowledge and HARICA does not have access to it.

☒ I, Katarina Simonović, declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

[< Back](#) **1љ**

Након тога, отвориће се нови прозор где је неопходно да преузмете генерисани приватни кључ (**1м**), то је обавезан корак јер се кључ може само тада преузети. Када преузмете кључ, штиклирате опцију да сте га преузели и затворите прозор (**1н**).

Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Request submitted successfully

You have generated a Private Key and your certificate order has been submitted.

You must :

1м

ATTENTION: This is the **ONLY TIME** you can perform this action, you cannot download the Private Key later.

As you have selected OV Certificate in the next steps you have to wait our validators to review your request.

After that you can continue with the certificate issuance process.

1н

☒ I have downloaded my private Key

5.1.2 *Manual creation of CSR* – копирање захтева за сертификат који је претходно креиран

У случају да изаберете *Submit CSR manually* (1n) потребно је да копирати захтев за сертификат (1j), сложити се са условима коришћења сервиса (1k) и кликнути на дугме *Submit request* (1n).

[illegible]

5.2 Поступак захтевања клијентских S/MIME сертификата

Мејл сертификат је дигитални фајл који се инсталира на мејл апликацију како би се осигурала безбедна мејл комуникација. Технологија која то омогућава позната је као S/MIME (*Secure/Multipurpose Internet Mail Extensions*).

S/MIME криптује мејлове и тако их штити од нежељеног приступа. Ова технологија такође омогућава да дигитално потписујете мејлове, односно пружа уверење да сте ви легитиман пошиљалац поруке.

У оквиру HARICA портала могуће је захтевати две врсте ових сертификата:

- *E-mail only* - сертификат који потврђује валидацију мејл адресе
- *For enterprises or organizations (IV+OV)* – сертификат који потврђује валидацију идентитета и валидацију организације

НАПОМЕНА: Битно је напоменути да је пожељно да институција којој крајњи корисник припада има регистрован Давалац идентитета у оквиру иАМРЕС Федерације Идентитета, који је придружен *eduGAIN*

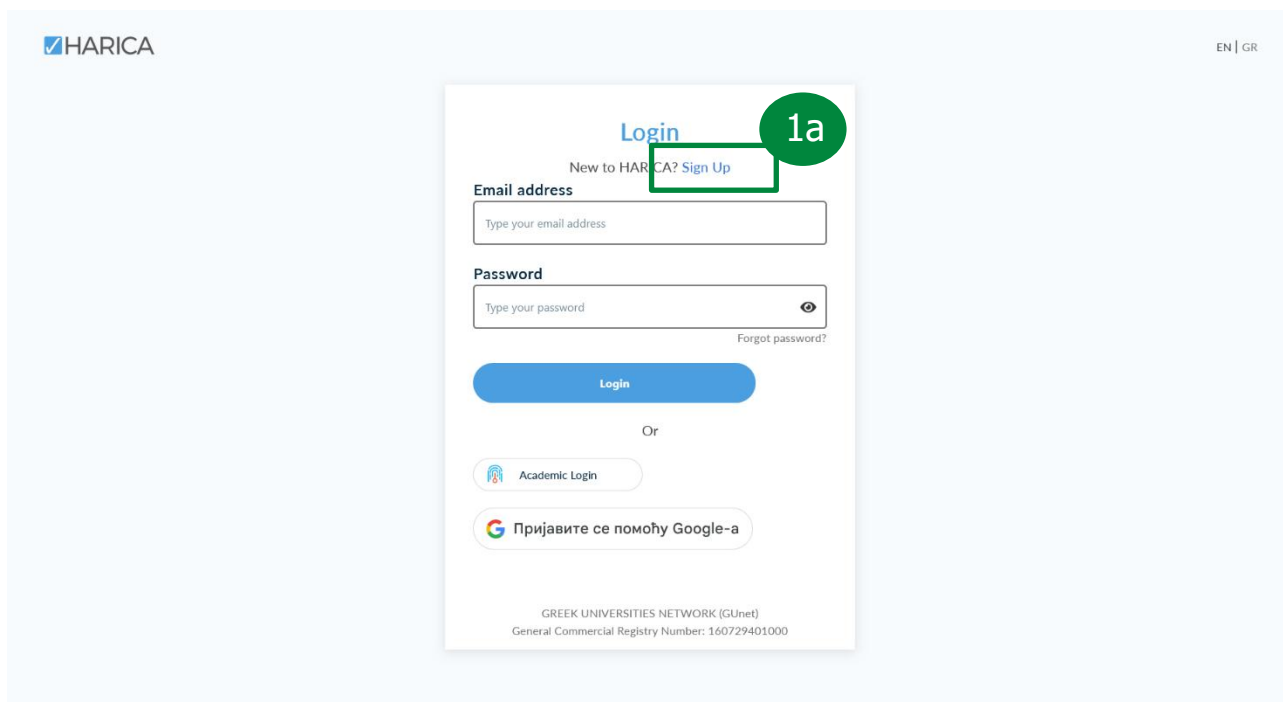
интерфедерацији, као и да крајњи корисник има налог у тој корисничкој бази. Потребно је и подесити **eduPersonEntitlement** атрибут са дефинисаном вредношћу **urn:mace:amres.ac.rs:amres:entitlement:tcs:user** за крајњег корисника.

НАПОМЕНА: Уколико институција није део иАМРЕС Федерације Идентитета, потребно је да крајњи корисник креира локални налог. Локални налог ће бити дозвољен само за крајње кориснике којима је потребан клијентски сертификат. У супротном, биће деактивиран на порталу.

5.2.1 Поступак креирања локалног налога за крајње кориснике

Уколико институција којој крајњи корисник припада нема регистрован Давалац идентитета у оквиру иАМРЕС Федерације Идентитета, који је придружен *eduGAIN* интерфедерацији, крајњи корисник може регистровати свој налог на HARICA порталу локално, а за потребе захтевања и коришћења клијентских S/MIME сертификата.

У том случају неопходно је изабрати *Sign Up* опцију (1a).



Затим ће се отворити портал за регистрацију где је неопходно унети обавезне податке у поља обележена звездицом (*), као што је приказано на слици испод.

 EN | GR

[< Back](#)

Sign Up

Email address *

Given name *

Surname *

Given name (Local language)

Surname (Local language)

Date of birth

Mobile phone

Password *

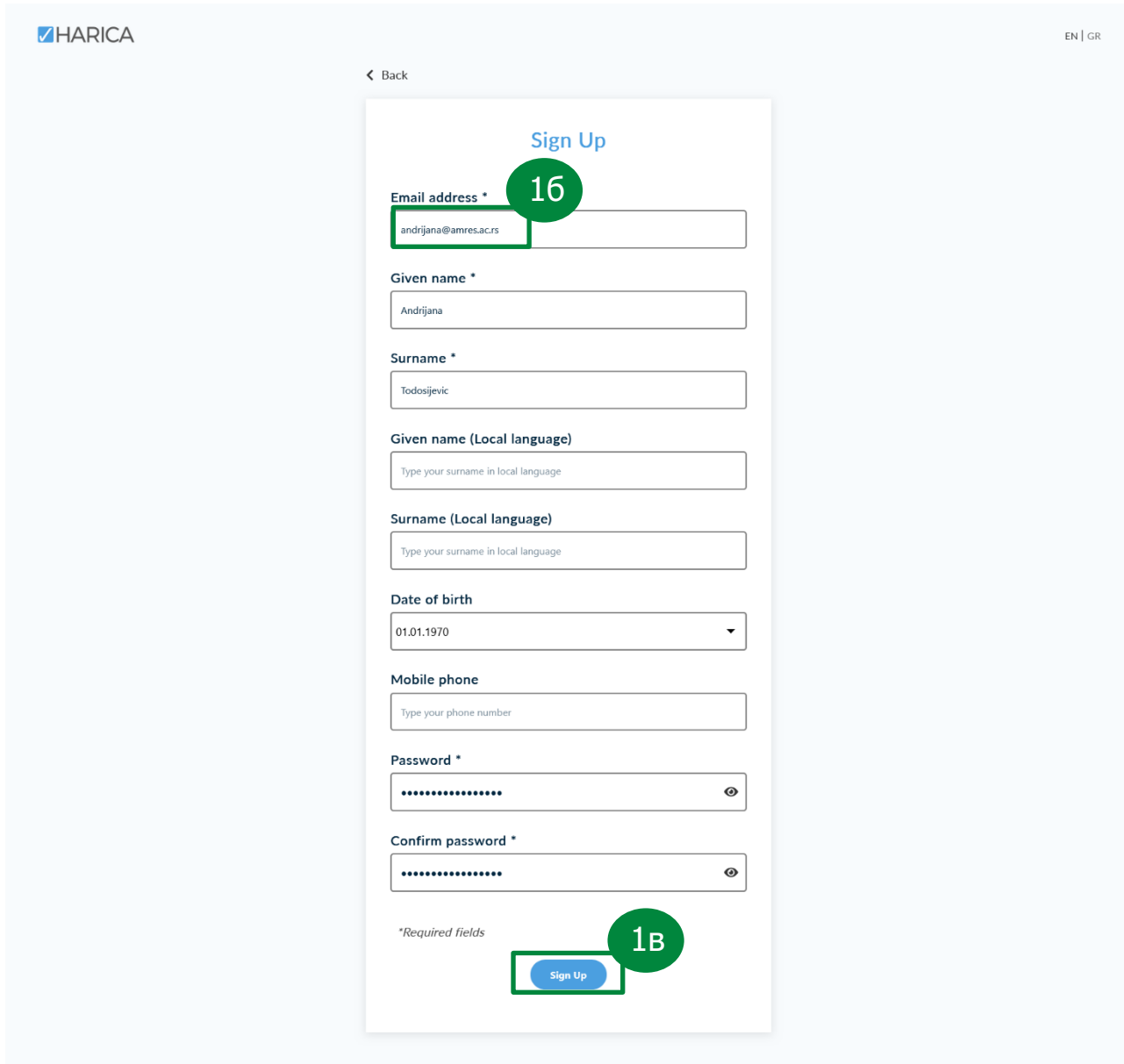
Confirm password *

**Required fields*

Sign Up

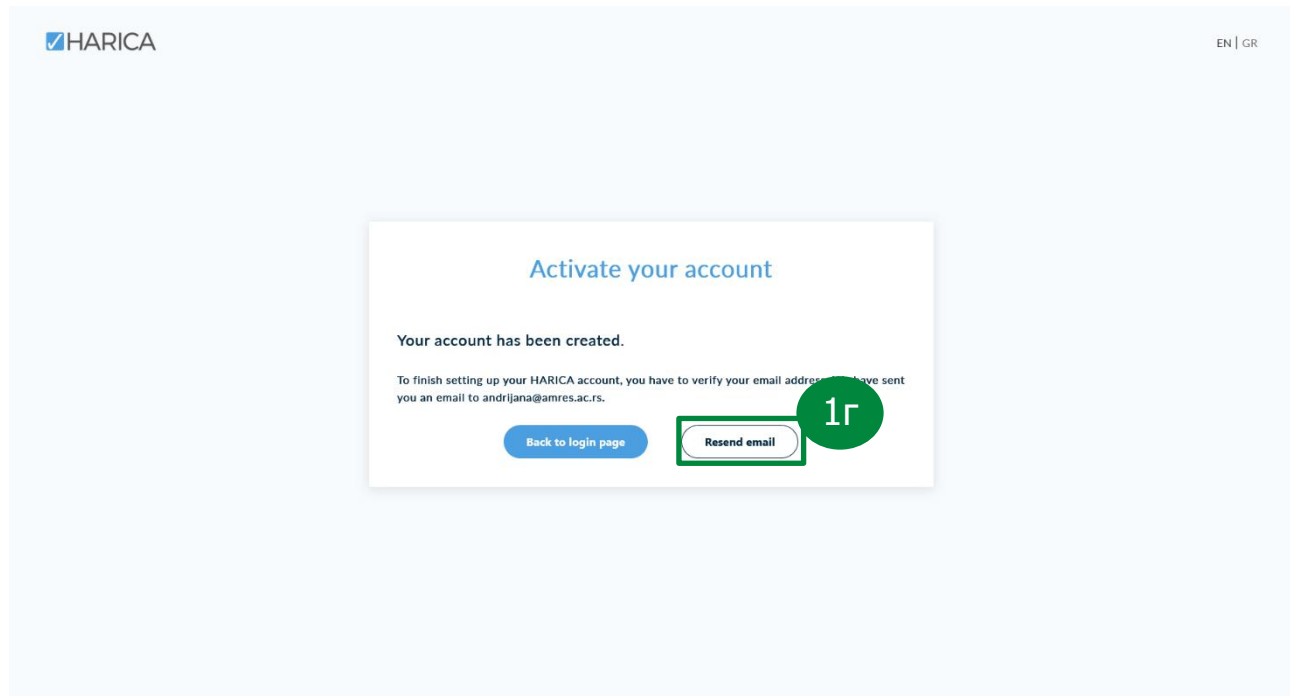
Најважнији податак је Ваш мејл. **Домен мејла се мора поклапати са примарним доменом Ваше организације која је пријављена на HARICA порталу (16).**

Када завршите са попуњавањем података кликнете *Sign Up* (1B).



The screenshot shows the HARICA Sign Up form. At the top left is the HARICA logo. At the top right is the text "EN | GR". Below the logo is a "< Back" link. The form title is "Sign Up". The first field is "Email address *" with the value "andrijana@amres.ac.rs" and a green circle annotation "16" pointing to it. The second field is "Given name *" with the value "Andrijana". The third field is "Surname *" with the value "Todosijevic". The fourth field is "Given name (Local language)" with the placeholder "Type your surname in local language". The fifth field is "Surname (Local language)" with the placeholder "Type your surname in local language". The sixth field is "Date of birth" with the value "01.01.1970" and a dropdown arrow. The seventh field is "Mobile phone" with the placeholder "Type your phone number". The eighth field is "Password *" with a masked password "....." and an eye icon. The ninth field is "Confirm password *" with a masked password "....." and an eye icon. At the bottom left is the text "*Required fields". At the bottom right is a blue "Sign Up" button with a green circle annotation "1B" pointing to it.

Након регистрације налога појавиће Вам се порука да је ваш налог креиран и да је неопходно извршити валидацију мејла који сте користили за регистрацију локалног налога. Проверите Ваше електронско сандуче, у случају да Вам мејл валидације још увек није стигао можете користити опцију *Resend email* (1г).



У Ваше електронско сандуче ће стићи мејл где је потребно кликнути на *Confirm email* како бисте валидирали Вашу мејл адресу (1д).

Welcome to HARICA - Activate your account

 HARICA Certificate Manager (CM) <noreply@harica.gr>
To andrijana@amres.ac.rs

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



Welcome to HARICA!

To activate your account and confirm that you control the email address andrijana@amres.ac.rs, please click the link below and follow the instructions.

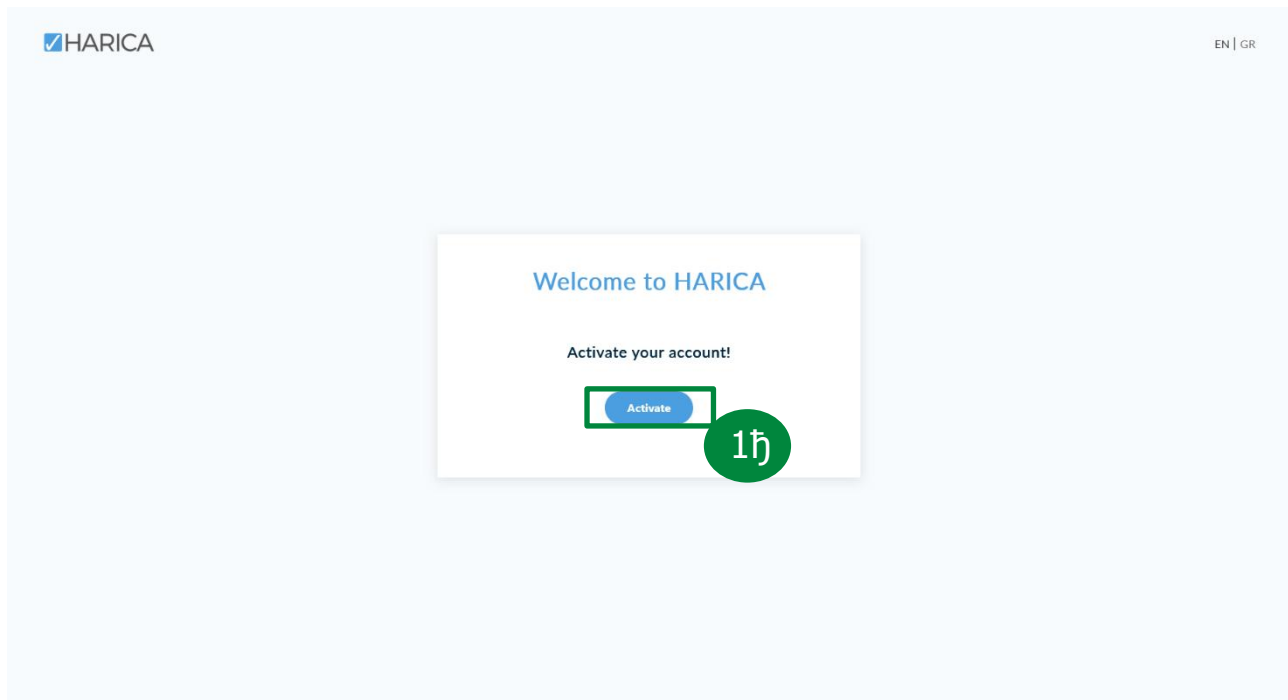
1д

Confirm email

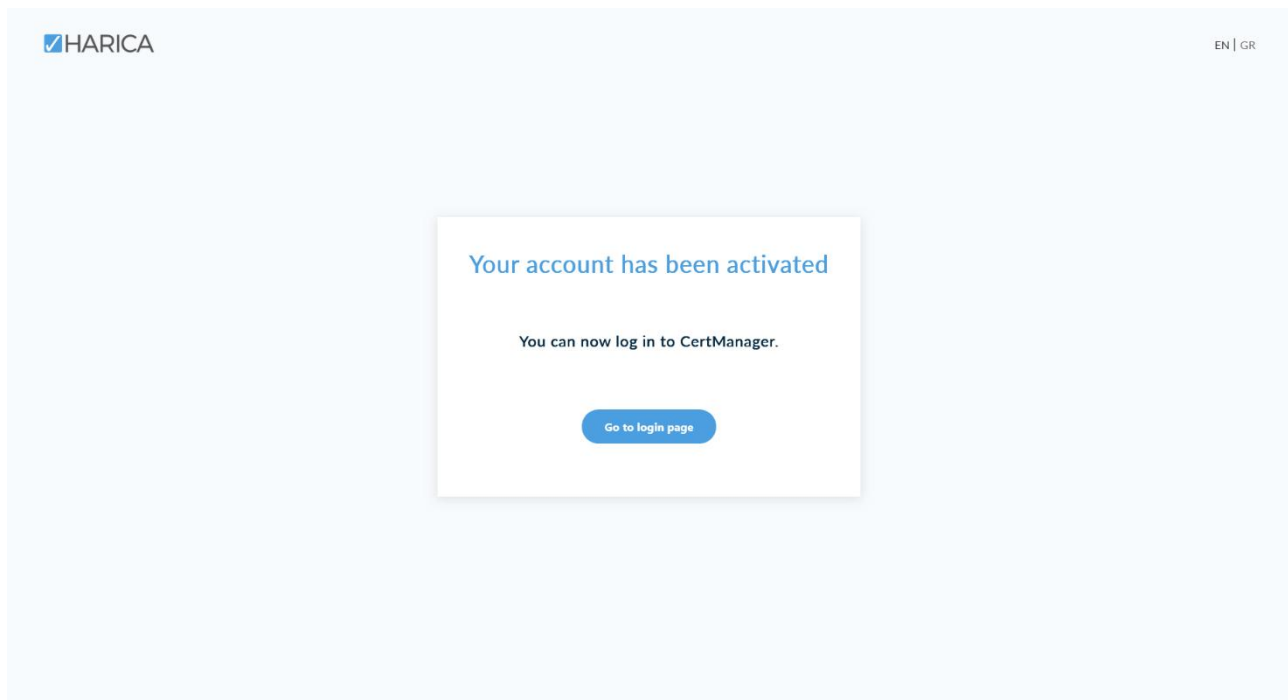
If you didn't sign up with this email address at [Harica CertManager \(https://cm.harica.gr\)](https://cm.harica.gr), you can ignore this message or contact us at support@harica.gr.

Do you need any assistance? Please contact us here!

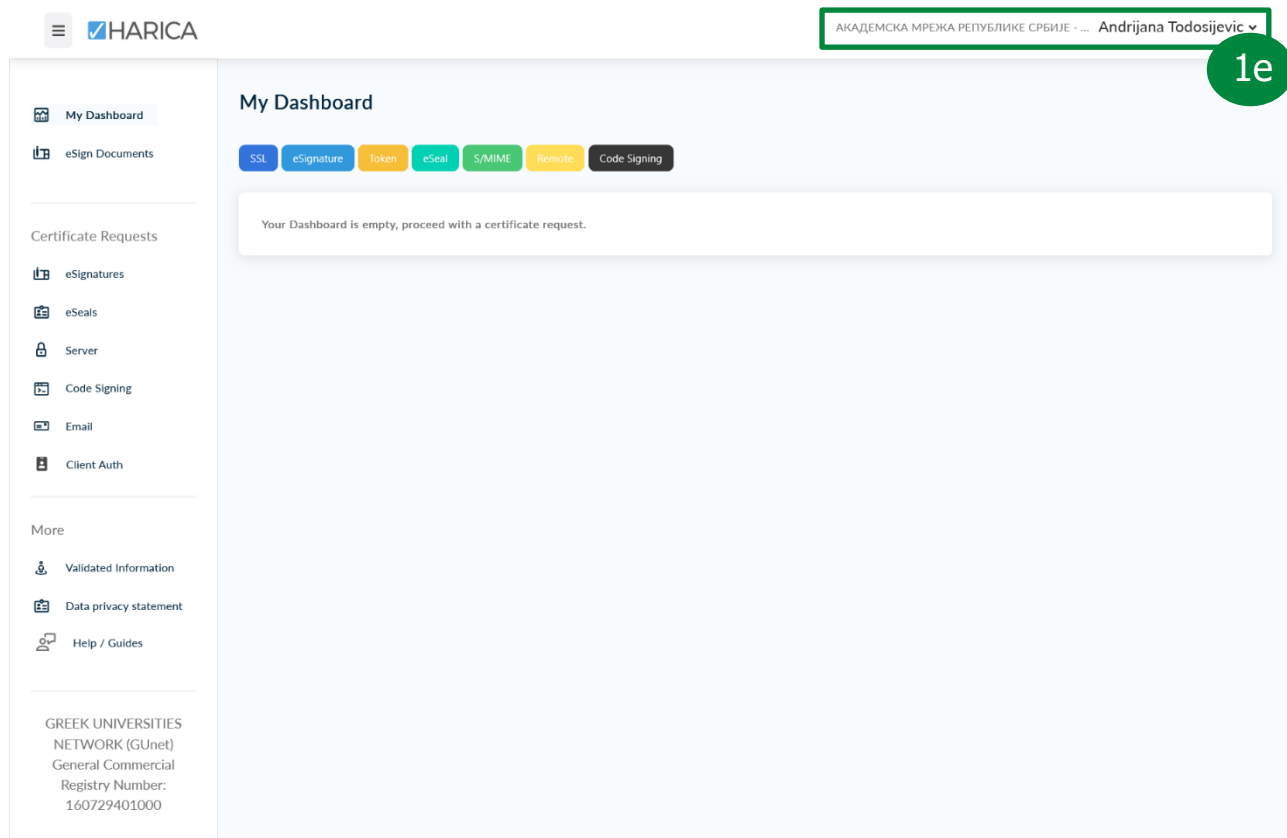
Затим ће се у претраживачу отворити нови прозор, где је неопходно да кликнете на *Activate*, како бисте активирали налог (1ђ).



Појавиће се нова порука потврде да је Ваш налог сада активан.



Након активације, приликом првог логовања, неопходно је да проверите у десном углу да је Ваш налог препознат као део институције којој припадате (1e).



My Dashboard

SSL eSignature Token eSeal S/MIME Remote Code Signing

Your Dashboard is empty, proceed with a certificate request.

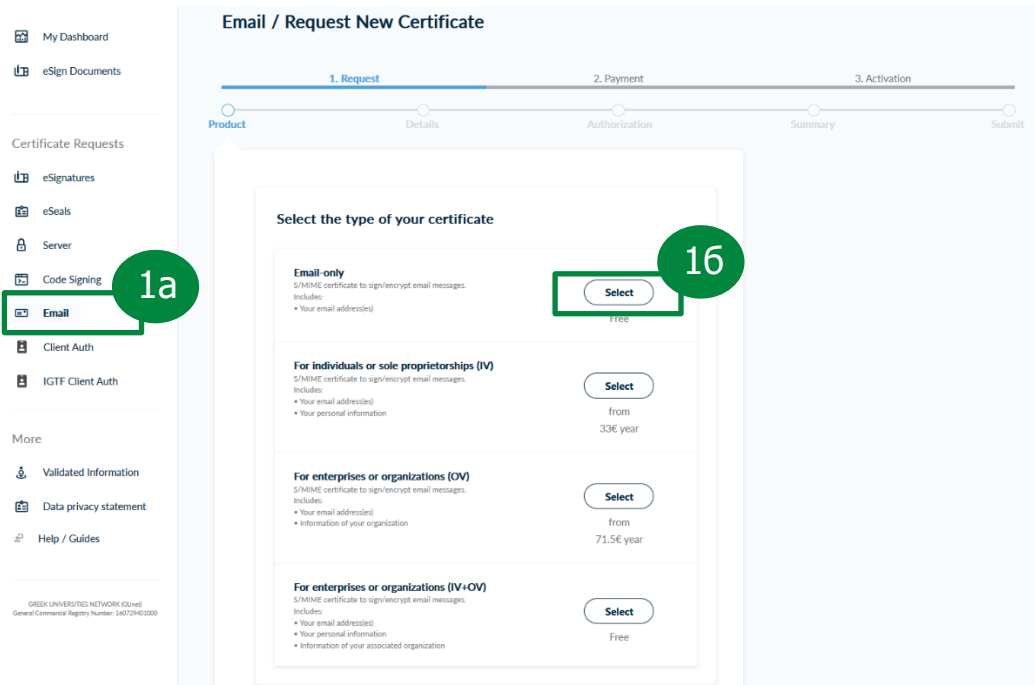
АКАДЕМСКА МРЕЖА РЕПУБЛИКЕ СРБИЈЕ - ... Andrijana Todosijevic

1e

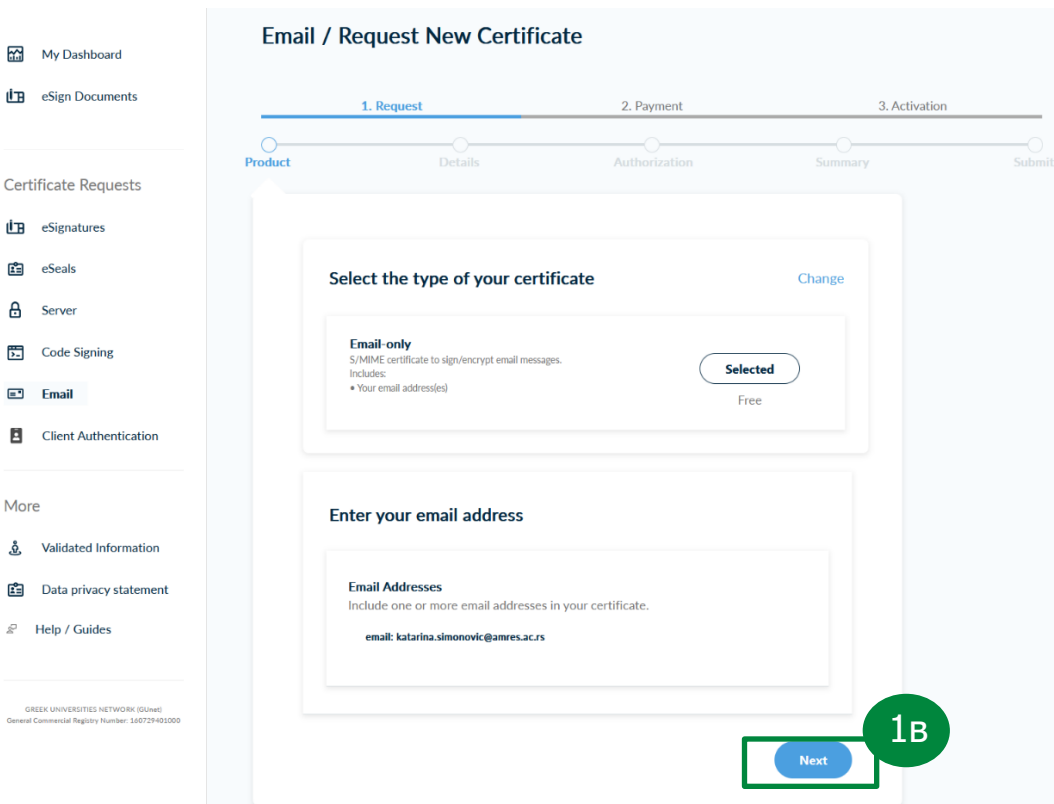
Сада несметано можете да захтевате и преузимате своје клијентске сертификате.

5.2.2 Поступак захтевања и преузимања клијентских *E-mail only* сертификата

За захтевање *e-mail only* сертификата неопходно је да у главном менију изаберете опцију *Email (1a)*, а затим *E-mail only (16)*.



Затим се кликне на *Next* поље (1b).



И опет, Next (1г), чиме потврђујете да ћете валидирати мејл адресу за коју захтевате сертификат.

Email / Request New Certificate

1. Request

2. Payment

3. Activation

Product

Details

Authorization

Summary

Submit

Select a method to validate your email address(es)

Validate via email to selected email address

Validate via email to selected email address

Selected

[Back](#)
[Next](#)

Након тога се шаље захтев, кликом на дугме *Submit* (1д). Захтев ће бити послат на мејл.

Email / Request New Certificate

1. Request

2. Payment

3. Activation

Product

Details

Authorization

Summary

Submit

Review the application before submitting

Certificate Type
S/MIME email-only

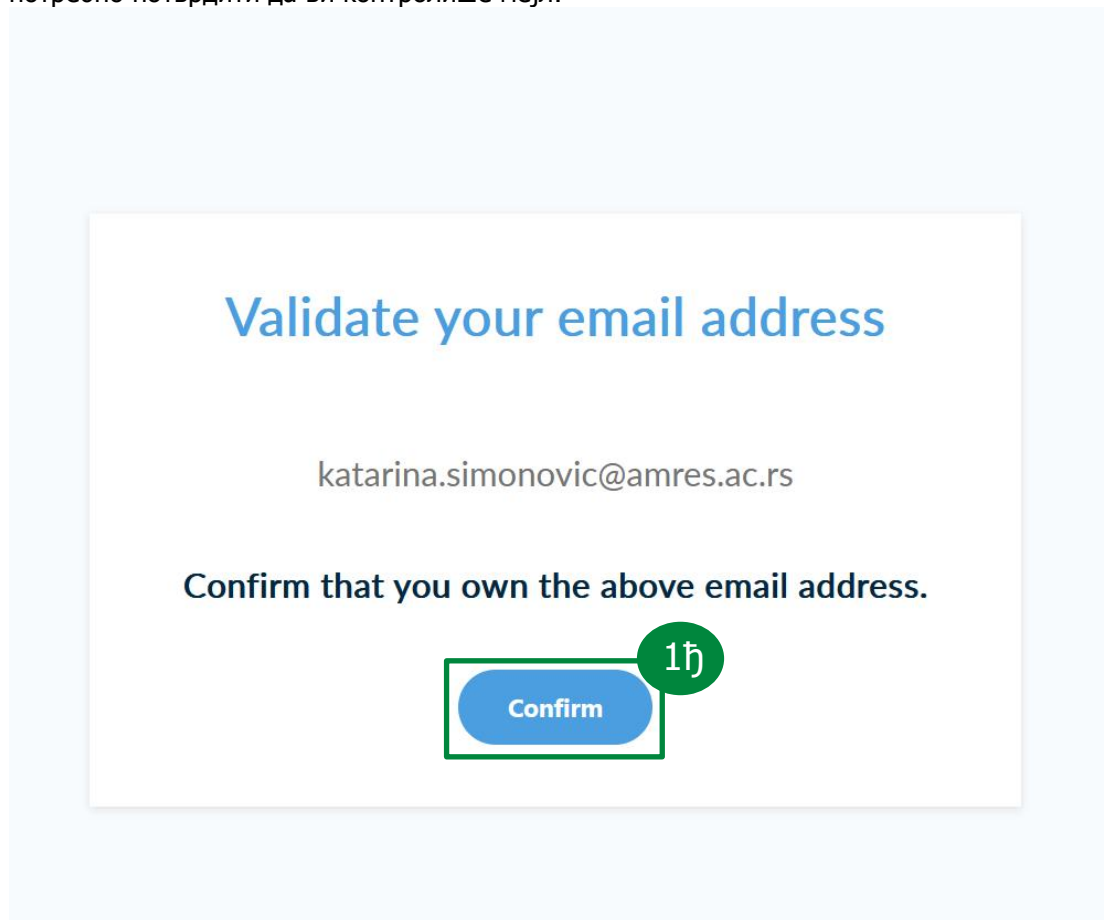
Service Duration
2 years

Emails
1. katarina.simonovic@amres.ac.rs

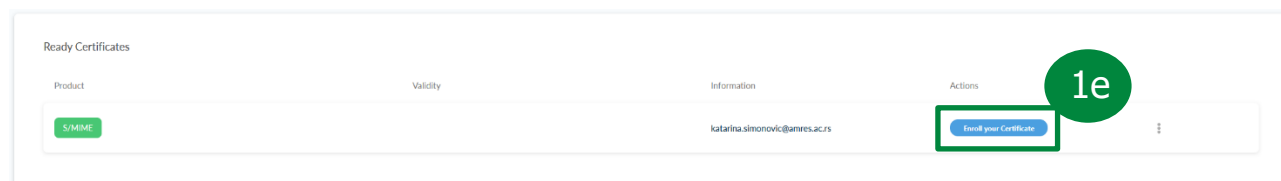
☒ I, Katarina Simonović, declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

[Back](#)
[Submit](#)

Кликом на линк из мејла (доступан кликом на реч *Confirm* (1ђ)), отвориће се страница на којој је потребно потврдити да ви контролишете мејл.



Након валидације мејла, на главном HARICA порталу, у секцији *Dashboard* ћете наћи захтев за сертификат. Потребно га је покренути (1е).



Затим ће вам се појавити прозор са опцијама за креирање сертификата. Овде је дат пример како то можете урадити директно коришћењем *passphrase* (1ж), али можете то урадити и коришћењем CSR фајла.

Потребно је изабрати алгоритам енкрипције и величину кључа (1з), а затим поставити *passphrase* (1и). Запамтите ову шифру она ће вам бити потребна када будете користили сертификат. Затим је неопходно сложити се са условима коришћења (1ј) и кликнути на поље *Enroll Certificate* (1к).

24/03/2026 sertifikat za proveru

Certificate Enrollment

1ж

Generate Certificate

Generate your certificate in .p12 format.

or

Submit CSR manually

Use your (already created) CSR and submit it here.

Set a passphrase to protect your certificate. Please note that the passphrase is required to use the certificate and should therefore be secured and not forgotten.

13

Algorithm

RSA (default) ▾

Key size

2048 (default) ▾

Set a passphrase

1и

.....

👁

Confirm passphrase

.....

👁

1j

☒ I understand that this passphrase is under my sole knowledge and HARICA does not have access to it.

Close

1к

Enroll Certificate

Details Information

Након тога ће се појавити прозор где можете да преузмете сертификат (1л).

Get your certificate

✓

Your certificate is ready. Press the Download button to retrieve it.

1л

Download

ATTENTION: This is the ONLY TIME you can perform this action, you cannot download the certificate later.

Close

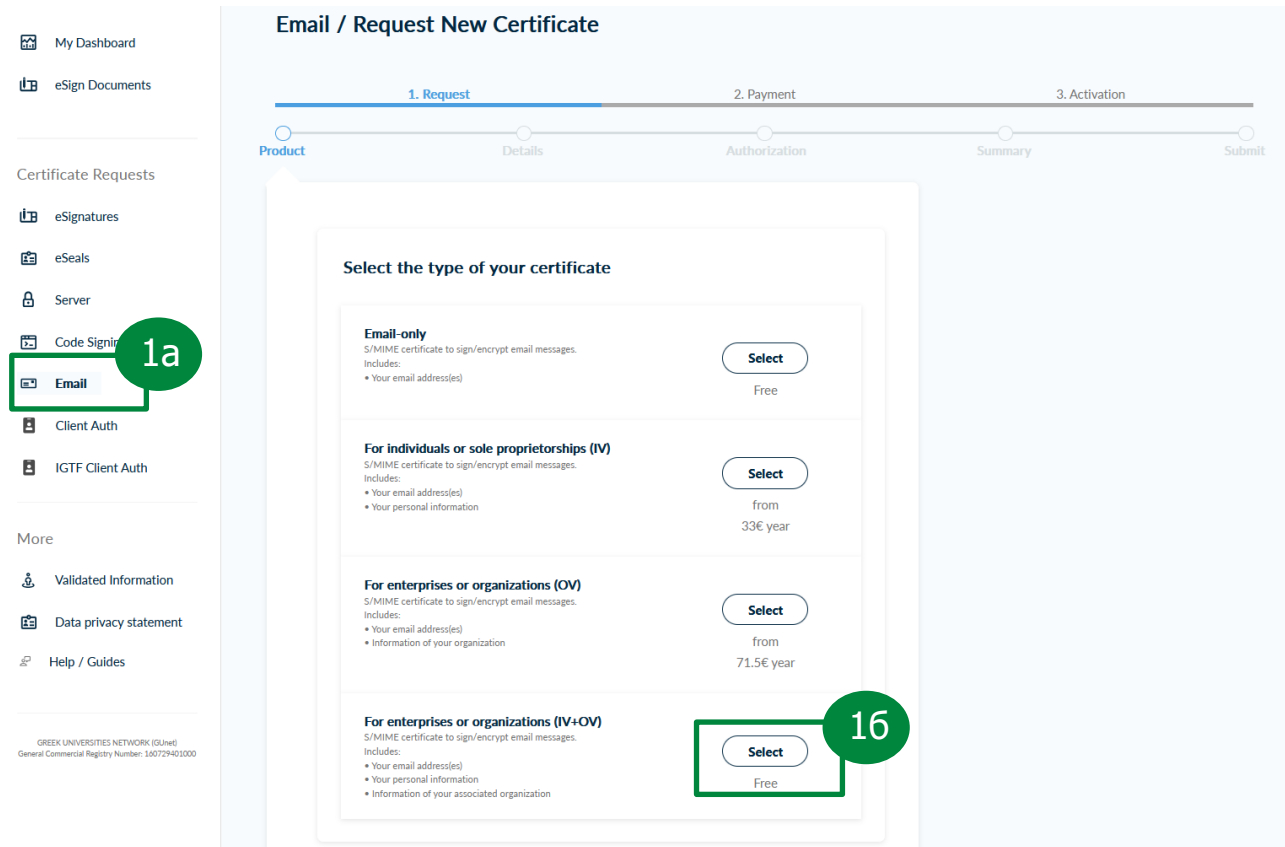
Такође, у *My Dashboard* секцији на HARICA порталу налазе се панели са информацијама о стању свих сертификата које је корисник потраживао. Ту се налазе сви серверским и клијентски сертификати који се могу преузети у сваком тренутку.

www.amres.ac.rs

Страна 32 од 45

5.2.3 Поступак захтевања клијентских (IV+OV) email сертификата

За захтевање *S/MIME IV+OV* сертификата неопходно је да у главном менију изаберете опцију *Email* (1a), а затим *For enterprises or organizations (IV+OV)* (1b).



Email / Request New Certificate

1. Request 2. Payment 3. Activation

Product Details Authorization Summary Submit

Select the type of your certificate

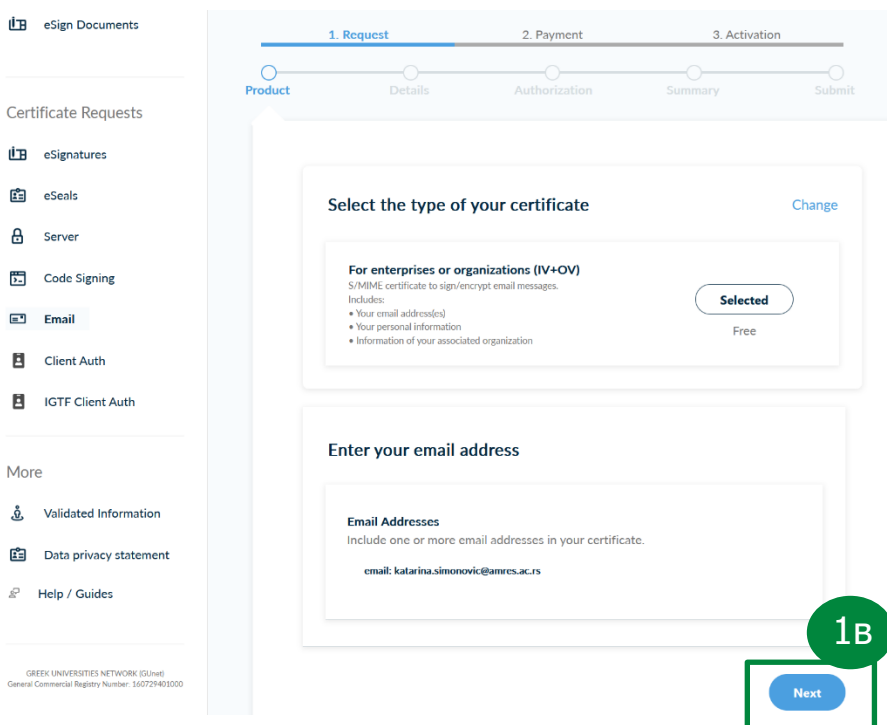
Email-only
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
Select
Free

For individuals or sole proprietorships (IV)
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
• Your personal information
Select
from
33€ year

For enterprises or organizations (OV)
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
• Information of your organization
Select
from
71.5€ year

For enterprises or organizations (IV+OV)
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
• Your personal information
• Information of your associated organization
Select
Free

Затим се кликне на *Next* поље (1b).



eSign Documents

Certificate Requests

eSignatures
eSeals
Server
Code Signing
Email
Client Auth
IGTF Client Auth

More

Validated Information
Data privacy statement
Help / Guides

GREEK UNIVERSITIES NETWORK (GUnet)
General Commercial Registry Number: 160729401000

1. Request 2. Payment 3. Activation

Product Details Authorization Summary Submit

Select the type of your certificate [Change](#)

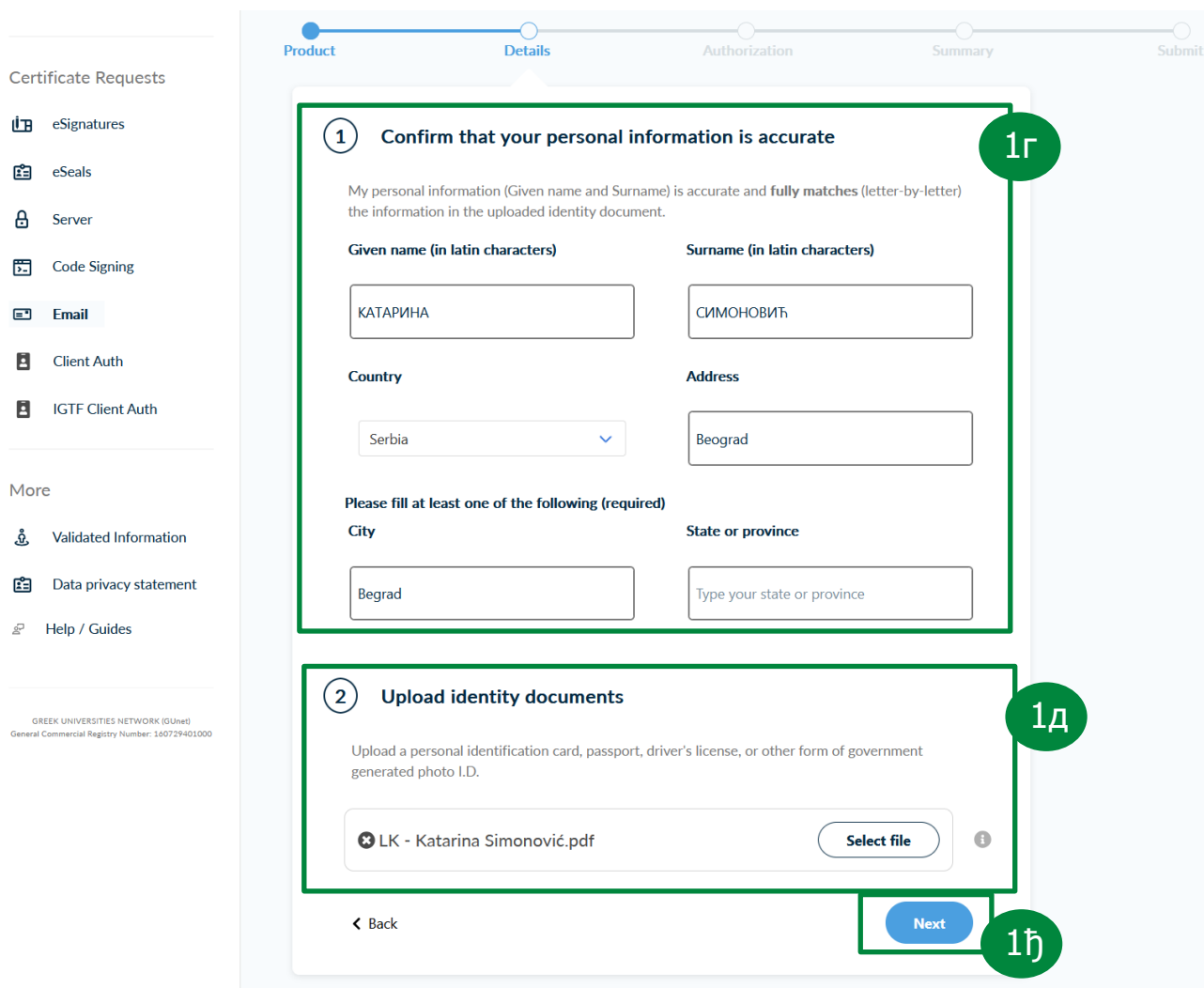
For enterprises or organizations (IV+OV)
S/MIME certificate to sign/encrypt email messages.
Includes:
• Your email address(es)
• Your personal information
• Information of your associated organization
Selected
Free

Enter your email address

Email Addresses
Include one or more email addresses in your certificate.
email: katarina.simonovic@amres.ac.rs

Next

У овом кораку је потребно да попуните податке о себи (1г), који се морају поклопити са подацима у идентификационим документу који ћете приложити (1д). Након тога се кликне на *Next* поље (1ђ).



1 Confirm that your personal information is accurate (1г)

My personal information (Given name and Surname) is accurate and **fully matches** (letter-by-letter) the information in the uploaded identity document.

Given name (in latin characters) KATARINA **Surname (in latin characters)** СИМОНОВИЋ

Country Serbia **Address** Beograd

Please fill at least one of the following (required)

City Begrad **State or province** Type your state or province

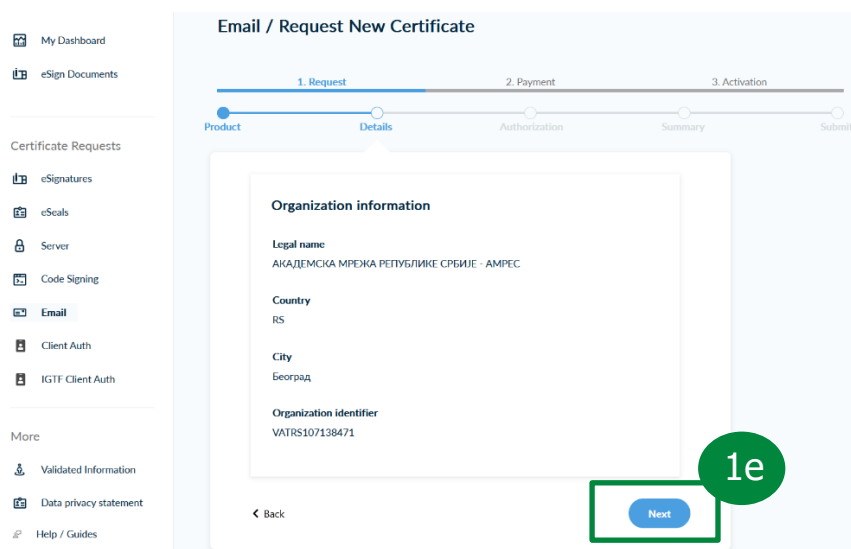
2 Upload identity documents (1д)

Upload a personal identification card, passport, driver's license, or other form of government generated photo I.D.

LK - Katarina Simonović.pdf **Select file**

Next (1ђ)

Потврђујете податке о организацији кликом на *Next* поље (1е).



Email / Request New Certificate

1. Request 2. Payment 3. Activation

Organization information

Legal name: АКАДЕМСКА МРЕЖА РЕПУБЛИКЕ СРБИЈЕ - АМРЕС

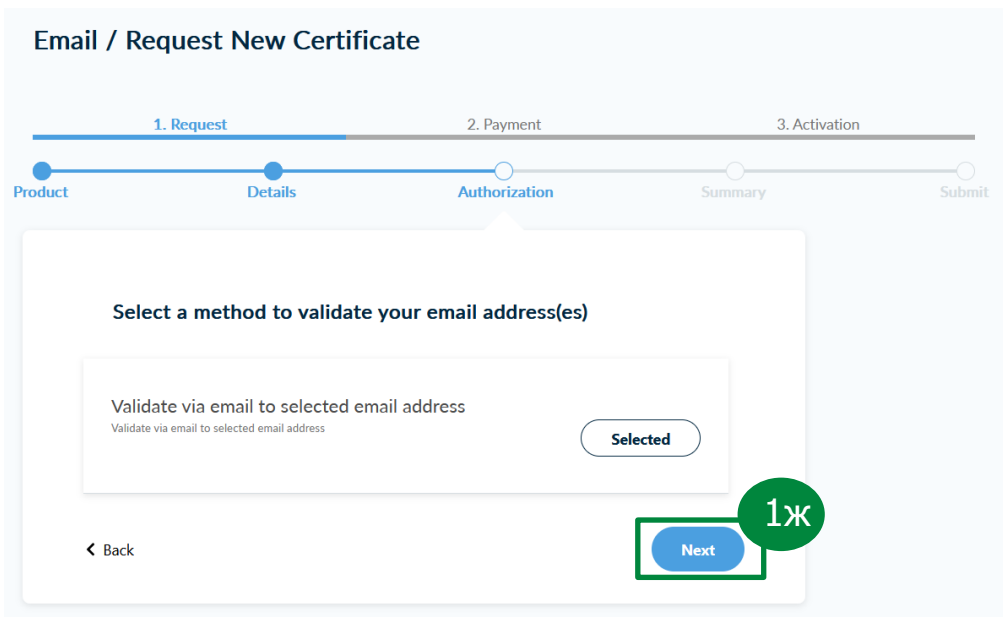
Country RS

City Београд

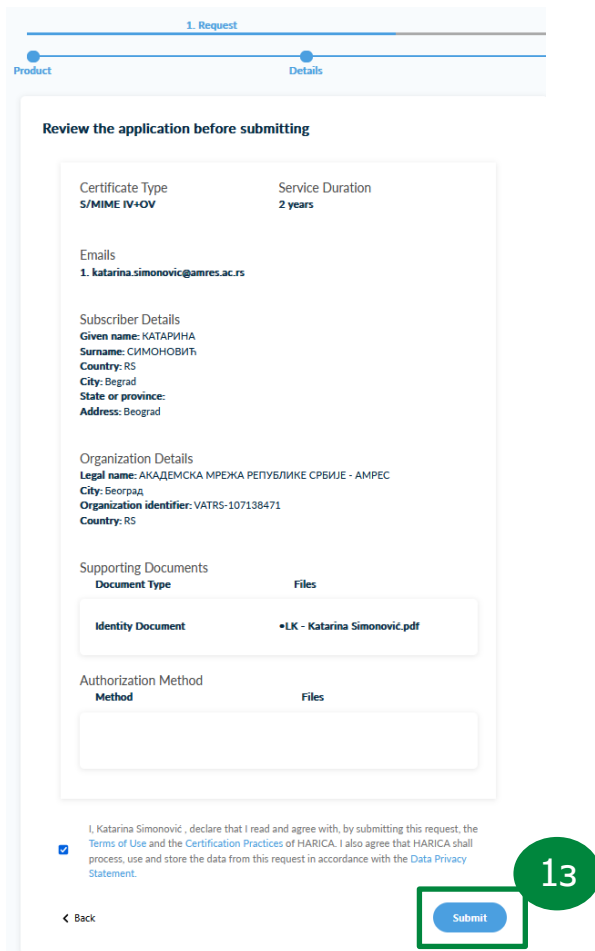
Organization identifier VATRS107138471

Next (1е)

И опет, *Next* (1ж), чиме започињете поступак валидације мејл адресе.



Након тога се шаље захтев, кликом на дугме *Submit* (13), и чека се одобрење сертификата.



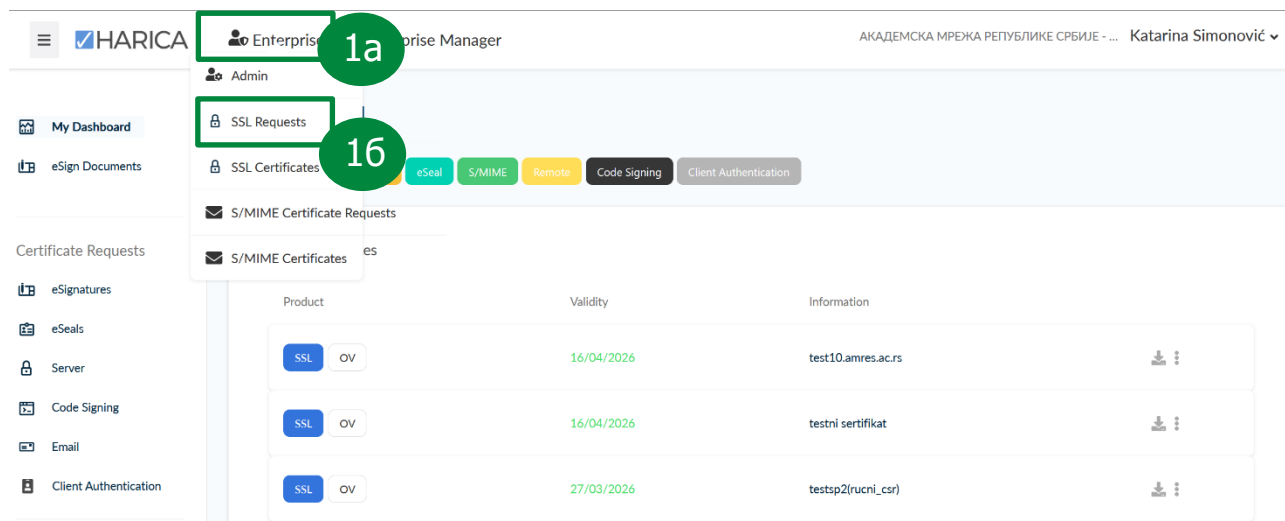
5.3 Поступак одобравања **SSL** сертификата

Да би сертификат био одобрен неопходно је да то одобрење дође од корисника који има *Enterprise Approver* улогу. Поступак додељивања *Enterprise Approver* улоге је објашњен у делу 3.1.

НАПОМЕНА: Није могуће да корисник сам себи одобри сертификат.

5.3.1 Поступак одобравања **SSL** сертификата

Како би *Enterprise Approver* одобрио сертификат потребно је да у главном менију одабере опцију *Enterprise* (1a), затим у менију другог нивоа опцију *SSL Requests* (16).

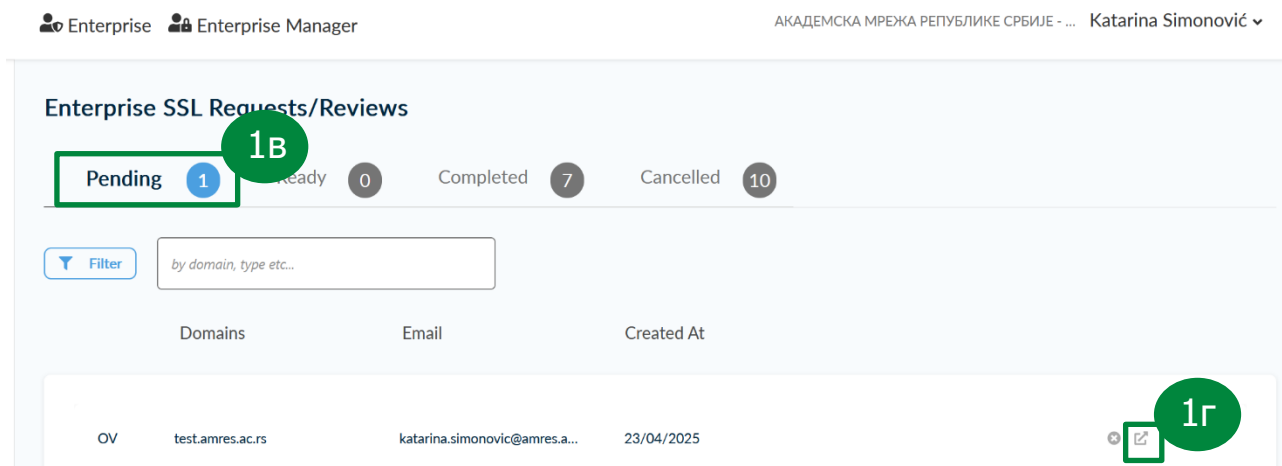


The screenshot shows the HARICA Enterprise Manager interface. The top navigation bar includes the HARICA logo, the user 'Katarina Simonović', and the role 'Enterprise Manager'. The left sidebar contains a menu with options like 'My Dashboard', 'eSign Documents', 'Certificate Requests', 'eSignatures', 'eSeals', 'Server', 'Code Signing', 'Email', and 'Client Authentication'. The main content area shows a dropdown menu for 'Enterprise' (labeled 1a) with 'Admin' selected. Under 'Admin', 'SSL Requests' is highlighted (labeled 16). Below this, there are tabs for 'eSeal', 'S/MIME', 'Remote', 'Code Signing', and 'Client Authentication'. The 'S/MIME' tab is active, showing a table of certificate requests.

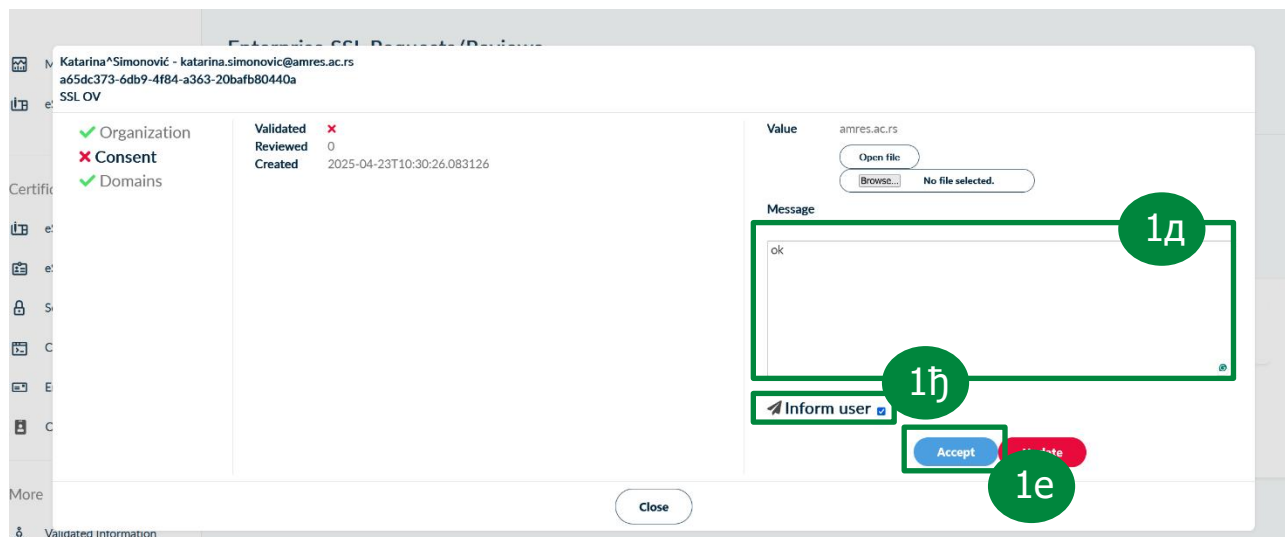
Product	Validity	Information
SSL OV	16/04/2026	test10.amres.ac.rs
SSL OV	16/04/2026	testni sertifikat
SSL OV	27/03/2026	testsp2(rucni_csr)

Отвориће се прозор са статистикама сертификата за ту организацију. *Pending* таб (1в) се односи на сертификате који чекају одобрење. У оквиру исте секције могу се наћи подаци о свим одобреним сертификатима, као и одбијеним.

Неопходно је да се у оквиру *Pending* сертификата, кликне на иконицу у продужетку сертификата који желимо да одобримо (1г).

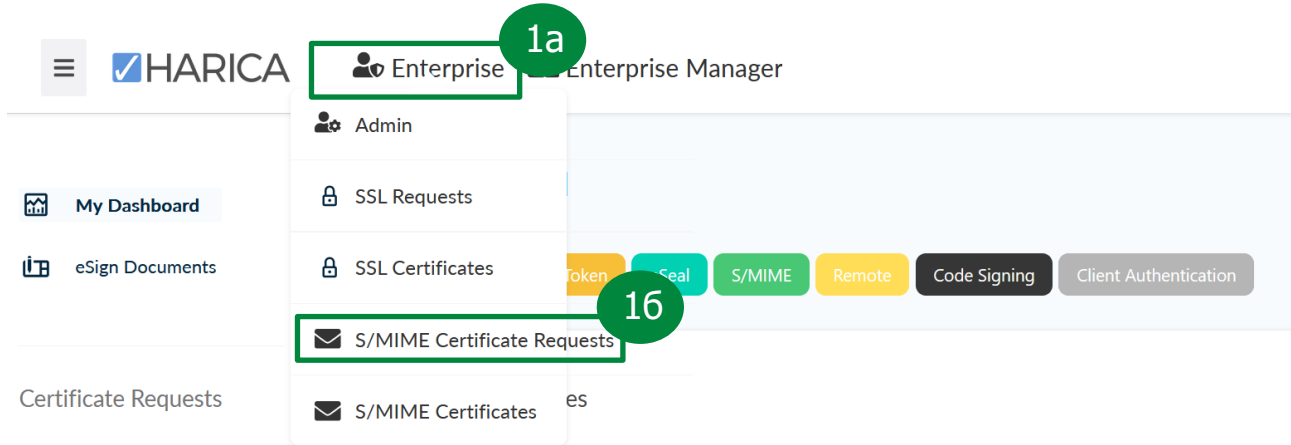


На екрану ће се појавити нови прозор, где је неопходно да у *Message* делу ставите неки текст, овде у примеру је то „ок“ (1д). Можете и корисника да обавестите да му је захтев за сертификат одобрен (1ђ), а на крају кликнете *Accept* (1е). На овај начин је сертификат одобрен, и корисник ће добити мејл о томе.



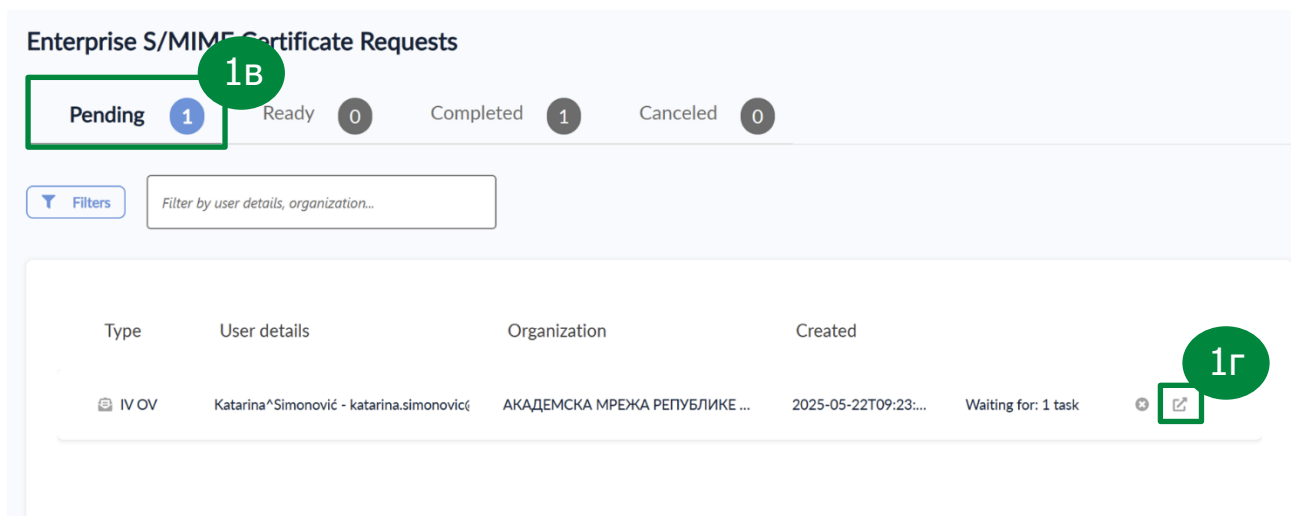
5.3.2 Поступак одобравања клијентских (IV+OV) email сертификата

Како би *Enterprise Approver* одобрио сертификат потребно је да у главном менију одабере опцију *Enterprise* (1a), затим у менију другог нивоа опцију *S/MIME Certificate Requests* (16).



Отвориће се прозор са статистикама сертификата за ту организацију. *Pending* таб (1b) се односи на сертификате који чекају одобрење. У оквиру исте секције могу се наћи подаци о свим одобреним сертификатима, као и одбијеним.

Неопходно је да се у оквиру *Pending* сертификата, кликне на иконицу у продужетку сертификата који желимо да одобримо (1r).



На екрану ће се појавити нова страница, где је неопходно да у *Message* делу ставите неки текст, овде у примеру је то „ок“ (1d). Можете и корисника да обавестите да му је захтев за сертификат одобрен (1ђ), а на крају кликнете *Accept* (1e). На овај начин је сертификат одобрен, и корисник ће добити мејл о томе.

S/MIME IV+OV

- ✗ Natural Person
- ✓ Organization
- ✓ Emails

Validated	✖
Reviewed	0
Created	2025-05-22T09:23:59.454063

Country

Serbia

Email
katarina.simonovic@amres.ac.rs

First name

КАТАРИНА

Locality

Beograd

Last name

СИМОНОВИЋ

State or province

Address

Beograd

Value

Open file

Choose File No file chosen

FN:KATARINA
LN:SIMONOVIC
C:RS
L:Beograd
ADD:Beograd
E:katarina.simonovic@amres.ac.rs

There are non acceptable characters

Message box with 'ok' and a green circle with '1Д' next to it.

Inform user 

11)

1e

Close

5.4 Поступак преузимања сертификата

Како би корисник могао да преузме и користи свој сертификат неопходно је да на HARICA порталу одабере опцију *My Dashboard* (1a). Ту се налазе панели са информацијама о стању свих сертификата које је корисник потраживао.

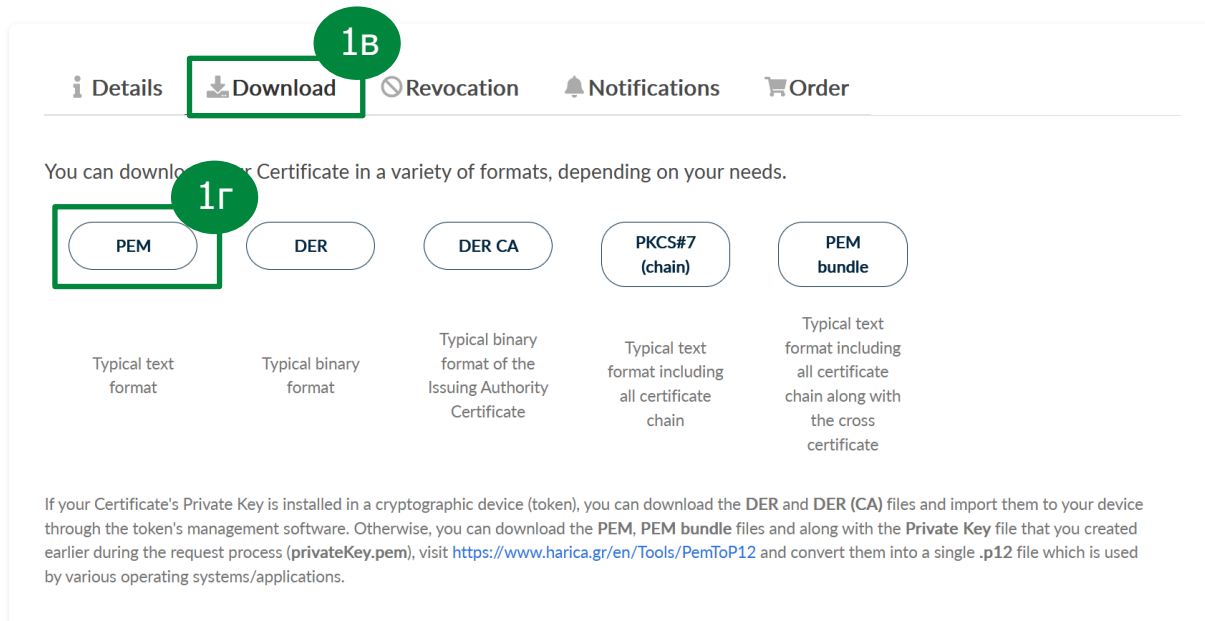
5.4.1 Поступак преузимања SSL сертификата

Да би корисник преузео серверски сертификат, неопходно је да кликне на *Download* иконицу, са десне стране сертификата (16).

The screenshot shows the HARICA Enterprise dashboard. At the top, there's a navigation bar with the HARICA logo, user profile 'Katarina Simonović', and language settings. The main header area includes a sidebar menu on the left with options like 'My Dashboard' (highlighted with a green box and labeled '1a'), 'eSign Documents', 'Certificate Requests', 'eSignatures', 'eSeals', 'Server', 'Code Signing', 'Email', and 'Client Authentication'. Below the sidebar is a 'More' section with links to 'Validated Information' and 'Data privacy statement'. The main content area features a row of tabs: 'SSL', 'eSignature', 'Token', 'eSeal', 'S/MIME', 'Remote', 'Code Signing', and 'Client Authentication'. Under the 'SSL' tab, there are two sections: 'Valid Certificates' and 'Cancelled Requests'. The 'Valid Certificates' section contains a table with columns 'Product', 'Validity', and 'Information'. It lists one certificate with product type 'SSL' (via a dropdown), validity date '10/03/2026', and information 'grafana1.amres.ac.rs'. A download icon (labeled '16') is next to the certificate entry. The 'Cancelled Requests' section has a similar table with columns 'Product', 'Details', 'Information', and 'Actions'. It shows one cancelled request with product type 'SSL' (via a dropdown), details 'ni', and information 'test sertifikat (csr manual)'. A three-dot menu icon is visible at the end of the row.

Отвориће се нови прозор са информацијама о самом сертификату. За преузимање сертификата неопходно је кликнути на *Download* поље (1в), у оквиру кога је могуће преузети сертификат у одговарајућем формату. AMRES корисници најчешће користе *PEM* формат (1г).

Certificate

You can download your Certificate in a variety of formats, depending on your needs.

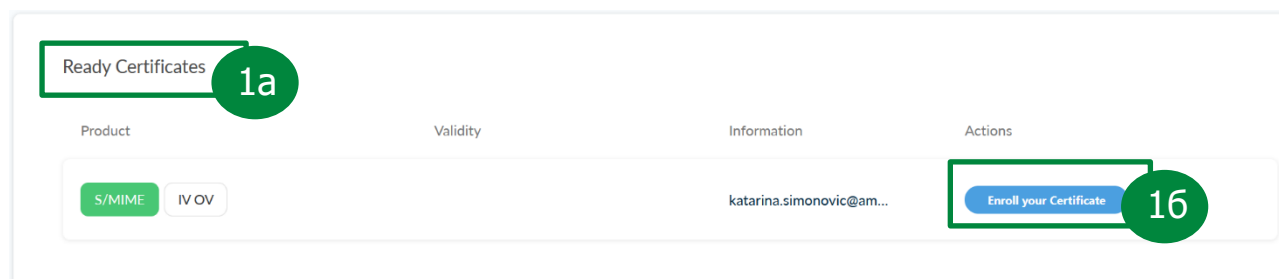
Format	Description
PEM	Typical text format
DER	Typical binary format
DER CA	Typical binary format of the Issuing Authority Certificate
PKCS#7 (chain)	Typical text format including all certificate chain
PEM bundle	Typical text format including all certificate chain along with the cross certificate

If your Certificate's Private Key is installed in a cryptographic device (token), you can download the DER and DER (CA) files and import them to your device through the token's management software. Otherwise, you can download the PEM, PEM bundle files and along with the Private Key file that you created earlier during the request process (*privateKey.pem*), visit <https://www.harica.gr/en/Tools/PemToP12> and convert them into a single .p12 file which is used by various operating systems/applications.

НАПОМЕНА: Поље *Notifications* служи да се у случају да је потребно да се промени мејл адреса на коју ће стизати подсетници пред истек сертификата. Посетник о истеку сертификата ће бити послат 15, 5 и последњег дана пред истек.

5.4.2 Поступак преузимања клијентских (IV+OV) email сертификата

Након што *Enterprise Approver* одобри клијентски (IV+OV) email сертификат, он ће се наћи на HARICA порталу (*My Dashboard*) у *Ready* панелу. (1а). Неопходно је покренути команду *Enroll your Certificate* (16).



Product	Validity	Information	Actions
S/MIME IV OV		katarina.simonovic@am...	Enroll your Certificate

Затим ће вам се појавити прозор са опцијама за креирање сертификата. Овде је дат пример како то можете урадити директно коришћењем *passphrase* (1в), али можете то урадити и коришћењем CSR фајла.

Потребно је изабрати алгоритам енкрипције и величину кључа (1г), а затим поставити *passphrase* (1д). Запамтите ову шифру, она ће вам бити потребна када будете користили сертификат. Затим је неопходно сложити се са условима коришћења (1ђ), и кликнути на поље *Enroll Certificate* (1е).

Certificate Enrollment

1в

Generate Certificate

Generate your certificate in .p12 format.

or

Submit CSR manually

Use your (already created) CSR and submit it here.

Set a passphrase to protect your certificate. Please note that the passphrase is required to use the certificate and should therefore be secured and not forgotten.

1г

Algorithm

RSA (default) ▾

Key size

2048 (default) ▾

1д

Set a passphrase

.....

👁

Confirm passphrase

.....

👁

1ђ

☒ I understand that this passphrase is under my sole knowledge and HARICA does not have access to it.

Close

1е

Enroll Certificate

Након тога ће се појавити прозор где можете да преузмете сертификат (1ж). Такође, у *My Dashboard* секцији на HARICA порталу налазе се панели са информацијама о стању свих сертификата које је корисник потраживао. Ту се налазе сви серверским и клијентски сертификати који се могу преузети у сваком тренутку.

Get your certificate

✓

Your certificate is ready. Press the Download button to retrieve it.

1ж

Download

ATTENTION: This is the ONLY TIME you can perform this action, you cannot download the certificate later.

Close

www.amres.ac.rs

Страна 41 од 45

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.

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: 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 КОПАКУ 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.

КОПАК 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 више доменских имена потребно је са АМРЕС 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.

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.).