AMPEC
Академска мрежа Србије

Упутство за прибављање TCS сертификата преко DigiCert портала

Историја верзија документа

Верзија	Датум	Иницијали аутора	Опис промене
1.0	29.1.2016.	МК	Прва верзија овог документа

Садржај

1 Увод

Да би корисници приликом преузимања или слања осетљивих података на неки сервер имали заштићену комуникацију, морају да буду сигурни да су приступили заиста оном серверу којем су имали намеру да приступе и да нико не може да прочита/промени податке који се шаљу или примају. Употреба дигиталних сертификата у комбинацији са SSL/TLS (*Secure Socket Layer / Transport Layer Security*) технологијом омогућава поменуту сигурност.

AMPEC је у сарадњи са организацијом GEANT успоставио сервис издавања SSL/TLS сертификата - TCS (*Trusted Certificate Service*), где GEANT има улогу сертификационог тела (*CA – Certification Authority*), а AMPEC регистрационог тела (RA – Registration Authority). Право на коришћење ових сертификата за потребе својих сервера, сервиса и крајњих корисника имају сви AMPEC корисници који претходно прођу кроз процес регистрације.

Сви сертификати издати у оквиру TCS услуге се потписују TERENA SSL CA 3 сертификатом који припада сертификационом телу које је креирао GEANT. Сертификат TERENA SSL CA 3 је потписан од стране DigiCert Assured ID Root CA кореног (*root)* сертификационог тела. Тај корени (*root)* сертификат је преинсталиран у већини SSL/TLS клијената (на пример, приликом приступања сајту преко *https* конекције, који се налази на веб серверу који има TCS сертификат, није потребна интервенција корисника како би сертификат био прихваћен јер се одговарајући корени сертификат већ налази преинсталиран у већини често коришћених Интернет прегледача: Internet Explorer, Mozilla Firefox, Google Chrome, Opera).

Да би AMPEC корисник има право да се пријави за коришћење услуге издавања TCS сертификата неопходно је да испуни следећи предуслов:

- AMPEC корисник мора да има регистровани домен у оквиру „ac.rs" домена

Уколико AMPEC корисник испуњава предуслов за пријаву на услугу издавања TCS сертификата, потребно је испратити следеће кораке да би дошао до могућности да захтева и прибавља TCS сертификате:

1. AMPEC корисник треба да се пријави за коришћење услуге издавања TCS сертификата
2. AMPEC корисник треба да креира администраторски налог на DigiCert порталу
3. AMPEC корисник треба да креира организацију на DigiCert порталу и потом успешно прође кроз процедуру валидације организације и валидације домена за који жели да прибавља сертификате

Валидацију организације и валидацију домена је потребно урадити само једном за сваки тип сертификата који AMPEC корисник жели да прибави. Након валидације AMPEC корисник може захтевати неограничен број сертификата за валидирани домен.

Кораци које је потребно испунити како би сертификат био издат су:

1. Креирање пара кључева и захтева за сертификатом
2. Подношење захтева
3. Инсталација сертификата и конфигурација сервера

У наставку Упутства дате су смернице за испуњавање сваког од поменутих корака у процесу прибављања сертификата преко DigiCert портала.

2 Захтевање и прибављање сертификата

У оквиру TCS сервиса, AMPEC корисник може захтевати следеће типове сертификата:

- Серверски сертификати за једно доменско име са валидацијом организације (*SSL plus*)
- Серверски сертификати за више доменских имена са валидацијом организације (*Multi-Domain SSL*)
- Серверски сертификати за сва поддоменска имена једног домена са валидацијом организације (*Wildcard Plus*)
- Серверски сертификати за једно доменско име са проширеном валидацијом (*EV SSL Plus*)
- Серверски сертификати за више доменских имена са проширеном валидацијом (*EV Multi-Domain*)
- Клијентски сертификат за потписивање (*Digital Signature Plus*)
- Клијентски сертификат за енкрипцију (*Email Security Plus*)
- Клијентски (S/MIME) имејл сертификат за енкрипцију и потписивање (*Premium*)
- Сертификат организације за потписивање Adobe докумената (*Document Signing – Organization 2000/5000*)
- Сертификат за потписивање програмског кода са валидацијом организације (*Code signing*)
- Сертификат за потписивање програмског кода са проширеном валидацијом (*EV Code signing*)
- Грид сертификати (*Grid Host/Client/Robot*)

Сви сертификати се прибављају преко централног DigiCert портала. У наставку су дати кораци које је потребно предузети како би AMPEC корисник прибавио жељени сертификат.

2.1 Прибављање серверског сертификата за једно доменско име са валидацијом организације (*SSL plus*)

Прибављање серверског сертификата за једно доменско име са валидацијом организације захтева да је AMPEC корисник претходно пријављен за коришћење TCS услуге, има регистрован домен у оквиру „ac.rs" домена и да је извршио валидацију организације и валидацију домена на DigiCert порталу.

Процедура прибављања сертификата захтева следеће акције AMPEC корисника:

- Креирање пара приватног/јавног кључа и захтева за сертификатом
- Подношење захтева за сертификат на DigiCert порталу
- Преузимање сертификата путем имејла или DigiCert портала

У наставку је дат детаљан опис свих потребних корака у процесу прибављања серверских сертификата.

Препоручује се да AMPEC корисници 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 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 Windows оперативне системе препоручује коришћење DigiCert алата.

КОРАК 1

Да би AMPEC 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 AMPEC 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 за сертификатом.

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 SCSreq.cnf -utf8 –sha256 -keyout myserver.key –out myserver.csr
```

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.

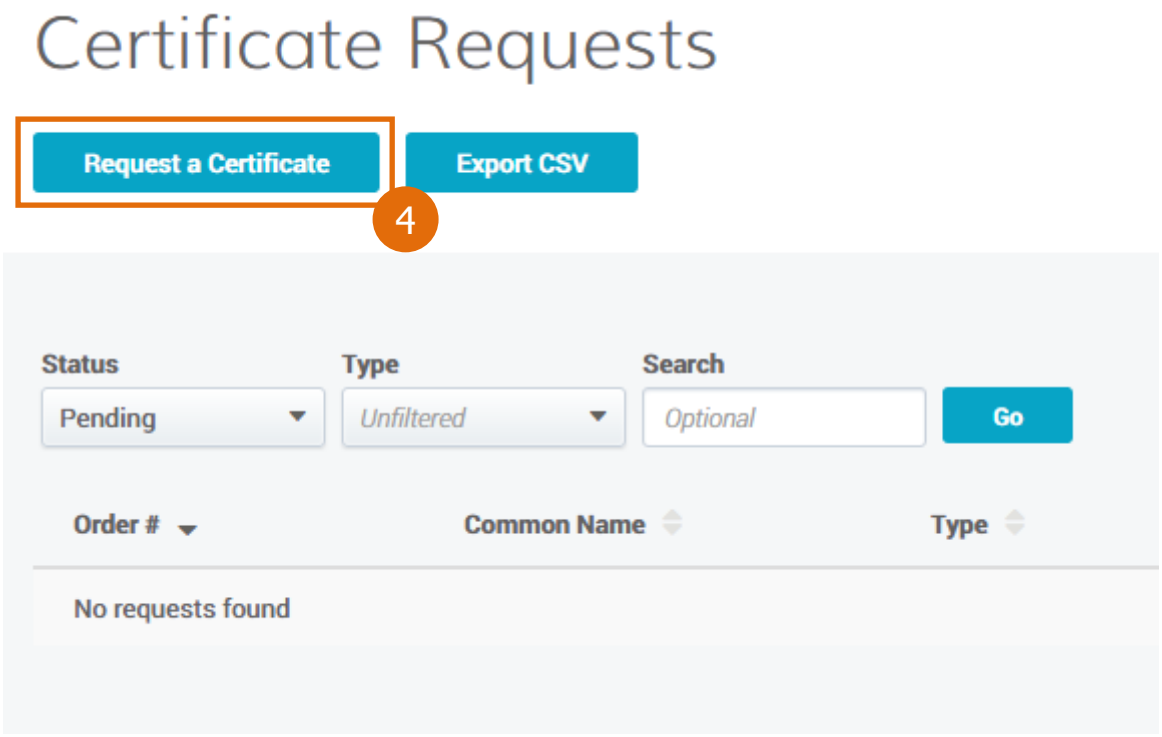
Након попуњавања свих неопходних података, у директоријуму ће бити креирана два нова фајла:

- 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 у наредним корацима прекопирати на DigiCert портал. Садржај .csr фајла се може прочитати било којим текст едитором (vi, nano, joe итд.)

КОРАК 4

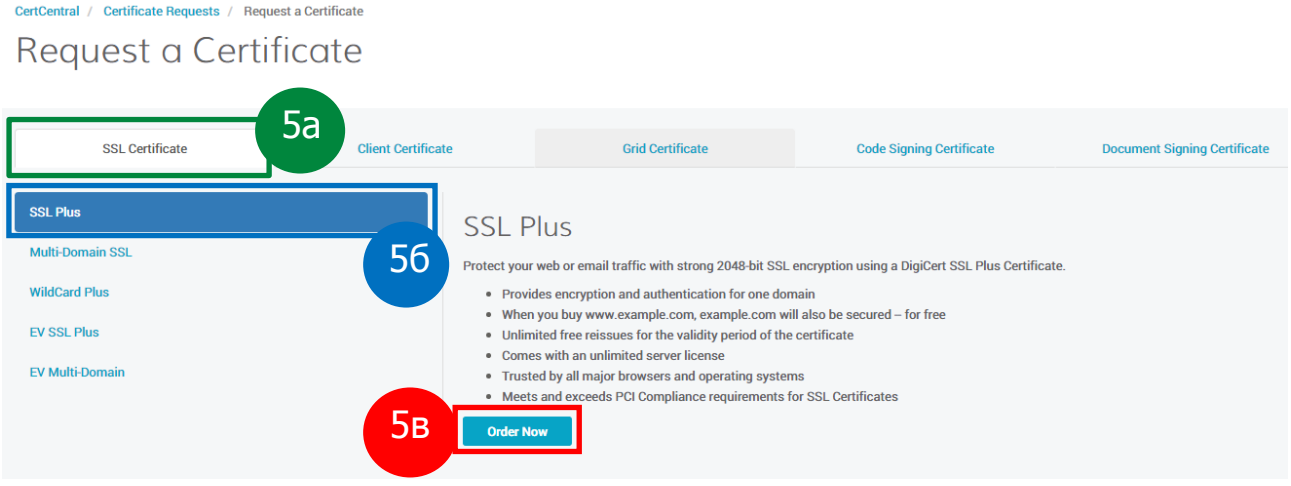
На DigiCert порталу потребно је у менију са леве стране притиснути опцију „CERTIFICATES“. У новоотвореном прозору потребно је притиснути дугме „Request a Certificate“ (4).



Слика 1

КОРАК 5

У новоотвореном прозору потребно је одабрати жељени сертификат - таб „SSL Certificate" (5а) , опција „SSL Plus" (5б) са леве стране прозора. У средини прозора приказаће се општи опис одабраног типа сертификата. Потребно је притиснути дугме „Order Now" (5в) како би се захтевао жељени сертификат.

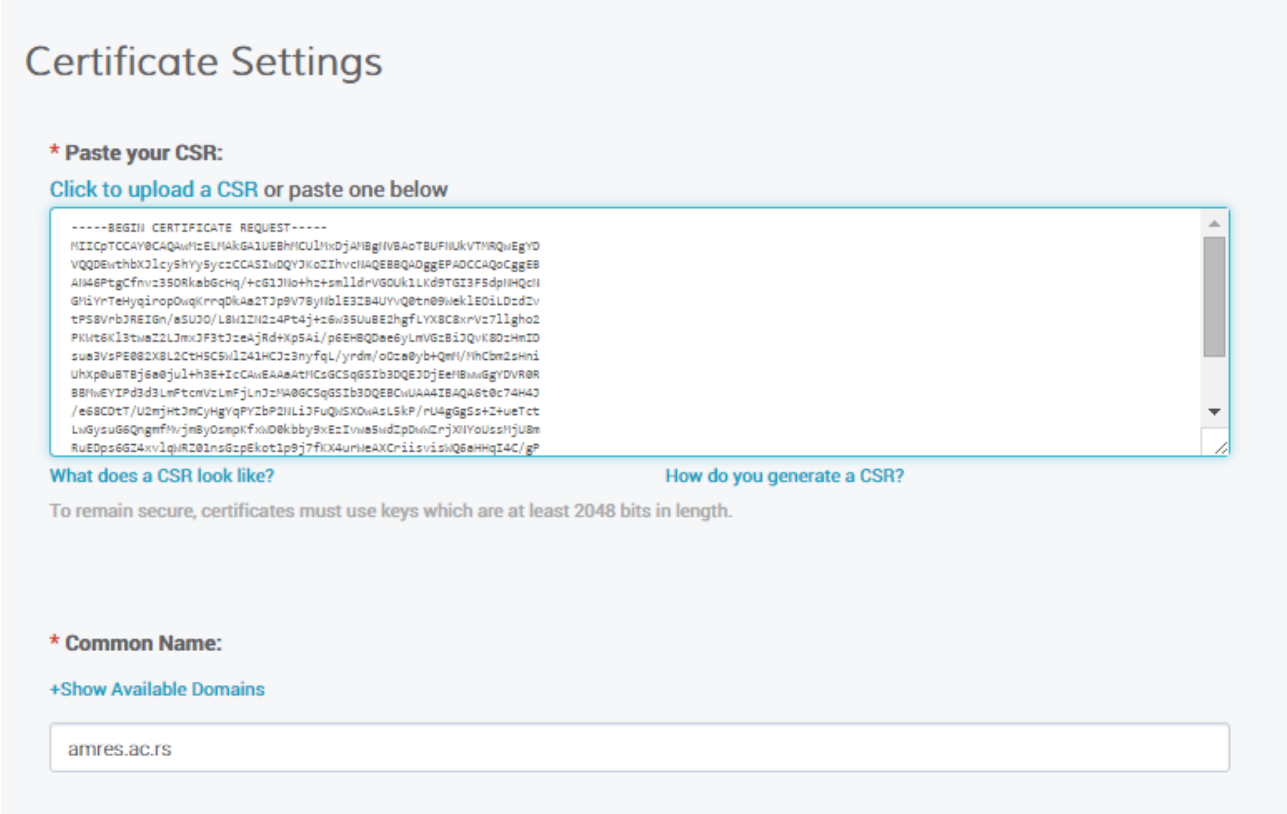


Слика 2

КОРАК 6

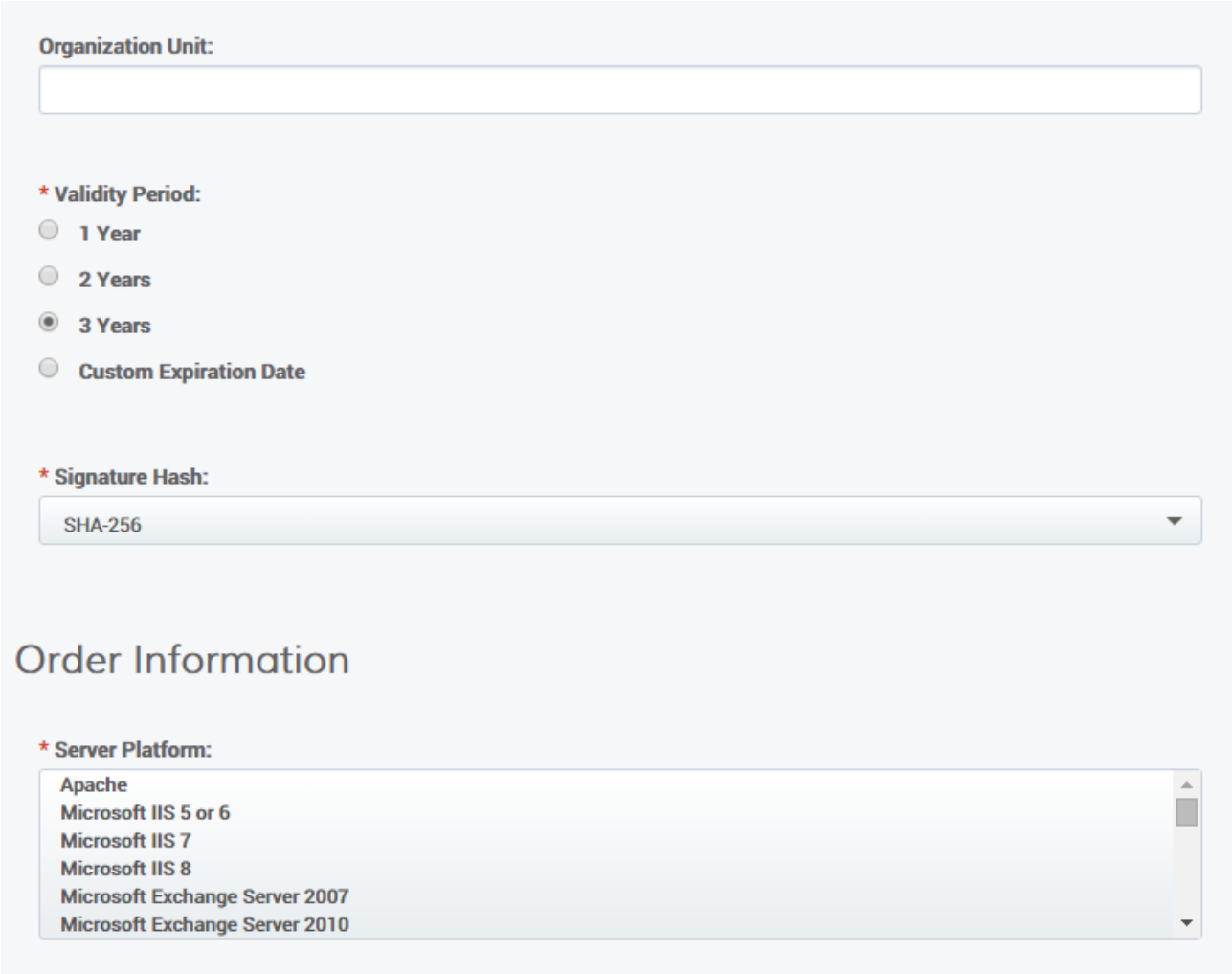
Администратору ће се приказати формулар који је потребно попунити како би захтев за сертификат био прослеђен DigiCert провајдеру. У пољу испод „Paste your CSR:" је потребно прекопирати садржај .csr фајла који је добијен у кораку 3. Алтернативно, администратор може притиснути опцију „Click to upload a CSR" која се налази тик изнад поменутог поља како би послао серверу .csr фајл. Након

прекопирања садржаја .csr фајла, у пољу „Common Name:" ће се аутоматски исписати FQDN име које ће бити заштићено SSL/TLS сертификатом. FQDN имена се читају из .csr фајла и аутоматски уписују у поменуто поље.



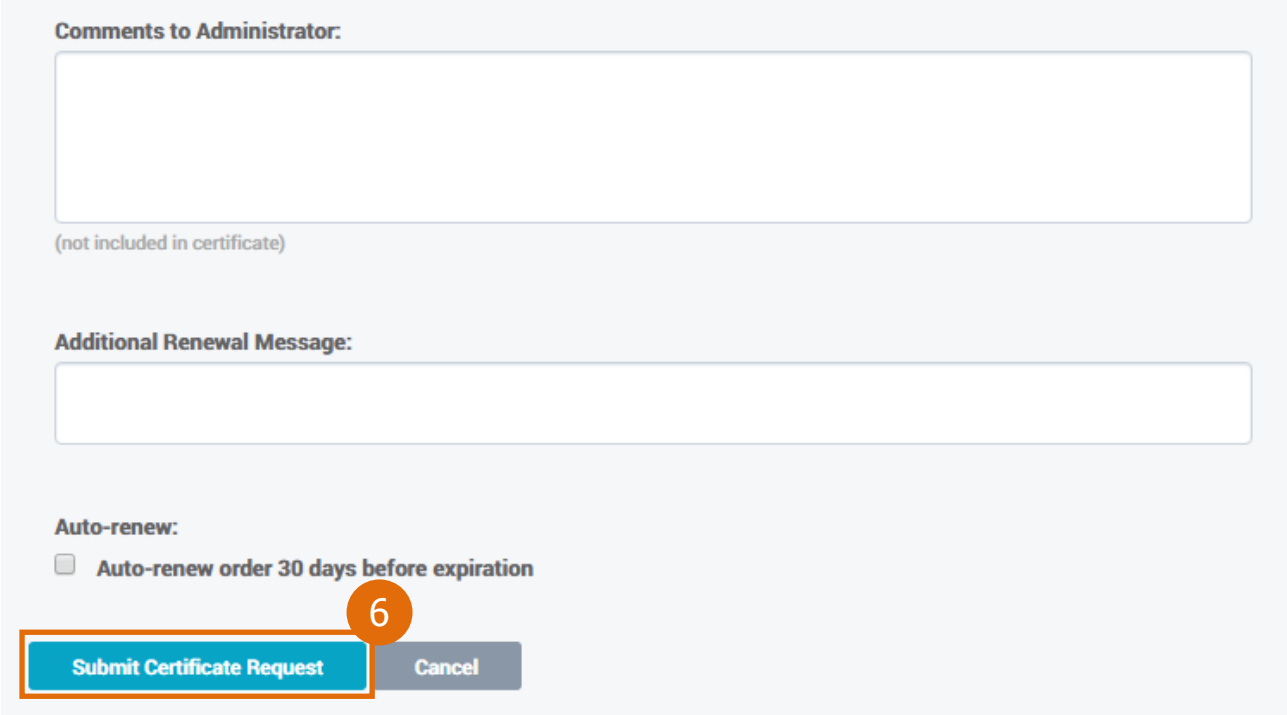
Слика 3

У наставку формулара потребно је одабрати период важења сертификата (1,2 или 3 године), потом изабрати хеш алгоритам који се користи у сертификату (одабрати исти хеш алгоритам који се користио и приликом генерисања захтева у кораку 3 – SHA256) и на крају прецизирати на којој серверској платформи је планирано да се инсталира сертификат након што буде издат. Информација о серверској платформи се прецизира да би DigiCert провајдер заједно са сертификатом испоручио и кратко упутство за инсталацију сертификата на жељеној серверској платформи. Опционо, администратор може прецизирати и организациону јединицу у оквиру своје институције за коју се захтева сертификат.



Слика 4

На крају формулара је администраторима остављена могућност да оставе поруку осталим администраторима везану за издавање сертификата или да прецизирају поруку коју ће добити приликом будуће нотификације о истеку сертификата и потреби да се исти обнови. Администратори могу обележити опцију „Auto-renew" којом се аутоматски покреће процедура обнове сертификата 30 дана пре истека постојећег сертификата. Све ове опције су опционе и администратори их не морају користити.



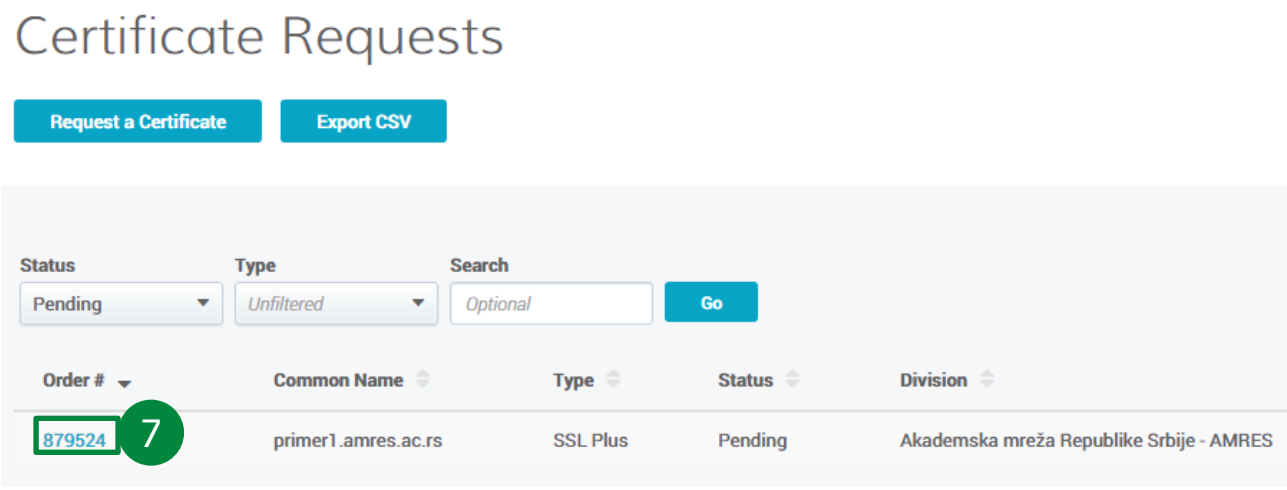
Слика 5

Након попуњавања наведених поља потребно је притиснути дугме „Submit Certificate Request" (6).

КОРАК 7

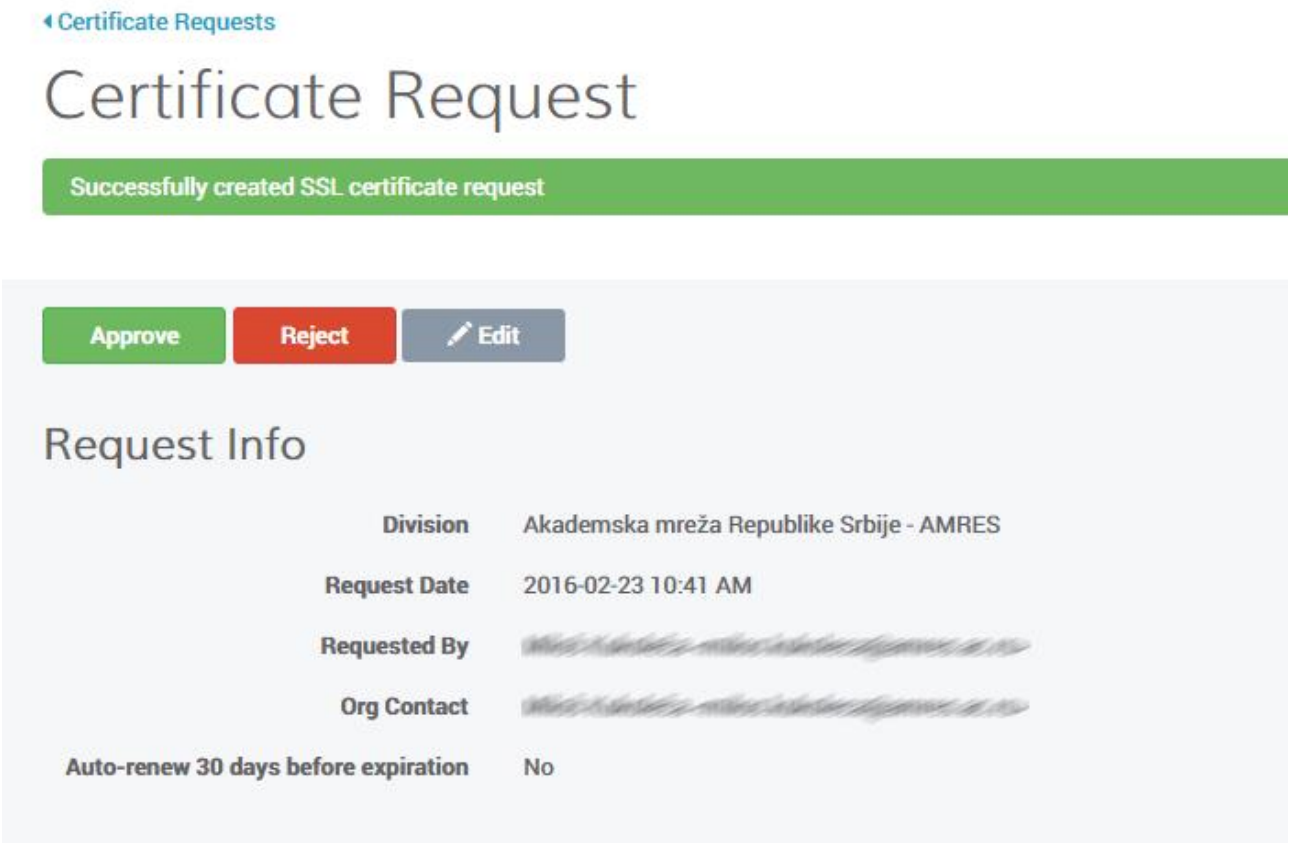
На централном DigiCert порталу је могуће у оквиру једне институције креирати кориснике са привилегијама обичног корисника (User) или администратора (Admin, SAML Admin). Било да је захтев поднео обичан корисник или администратор, захтев мора бити потврђен од стране администратора.

У складу са тим, након слања захтева преко портала, администратору ће се приказати прозор у оквиру кога ће морати да потврди поруџбину сертификата. Администратор може потврдити поруџбину одмах или може то урадити касније. Тражени сертификат неће бити издат док поруџбина не буде потврђена од стране администратора. У случају да администратор жели да види које поруџбине је потребно потврдити неопходно је на порталу у левом менију одабрати „CERTIFICATES" а потом из падајућег менија одабрати опцију „Requests".



Слика 6

Кликом на број наруџбине (7) са леве стране листе, долази се до детаљног описа захтеваног сертификата где је могуће потврдити или одбити поруџбину.



Слика 7

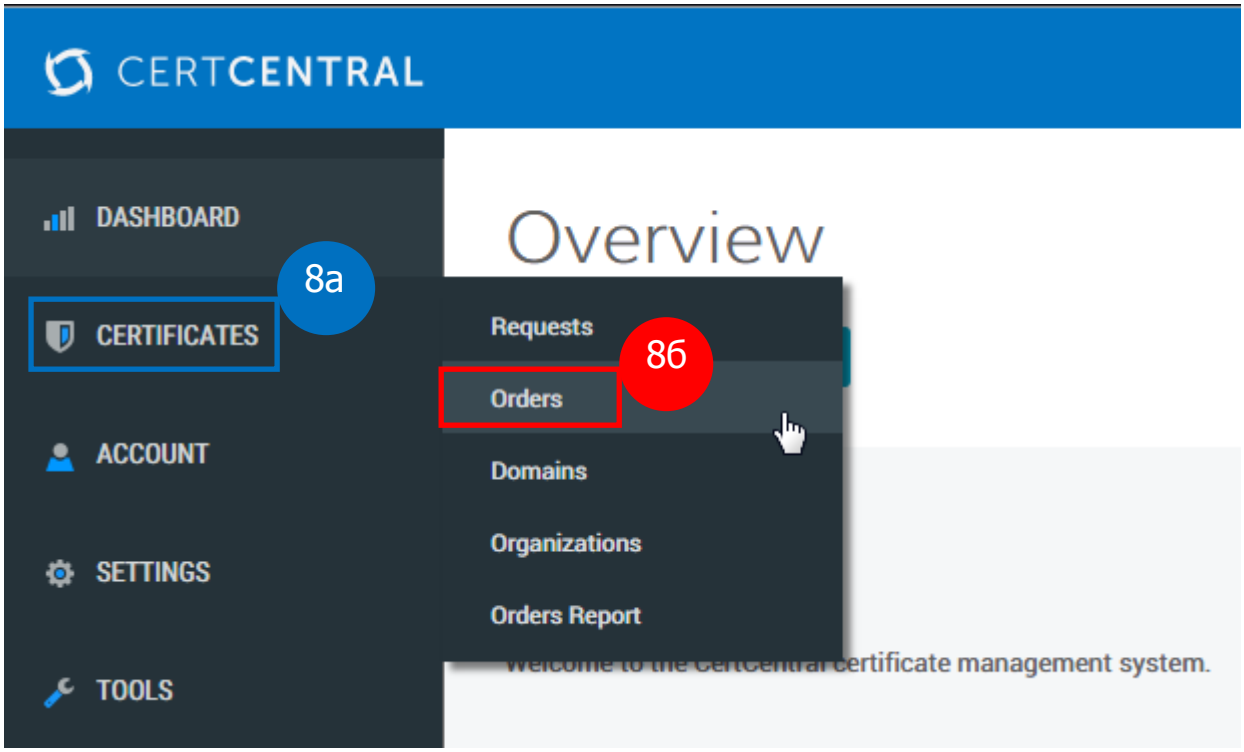
Притиском на дугме „Approve" отвара се нови прозор у коме је потребно уписати коментар који ће бити сачуван. Након уписа произвољног коментара и притиска на дугме „Approve" потврђује се поруџбина сертификата.

KORAK 8

Убрзо након потврђивања наруџбине сертификата, на имејл адресу корисника/администратора који је захтевао сертификат ће пристићи имејл са траженим сертификатом.

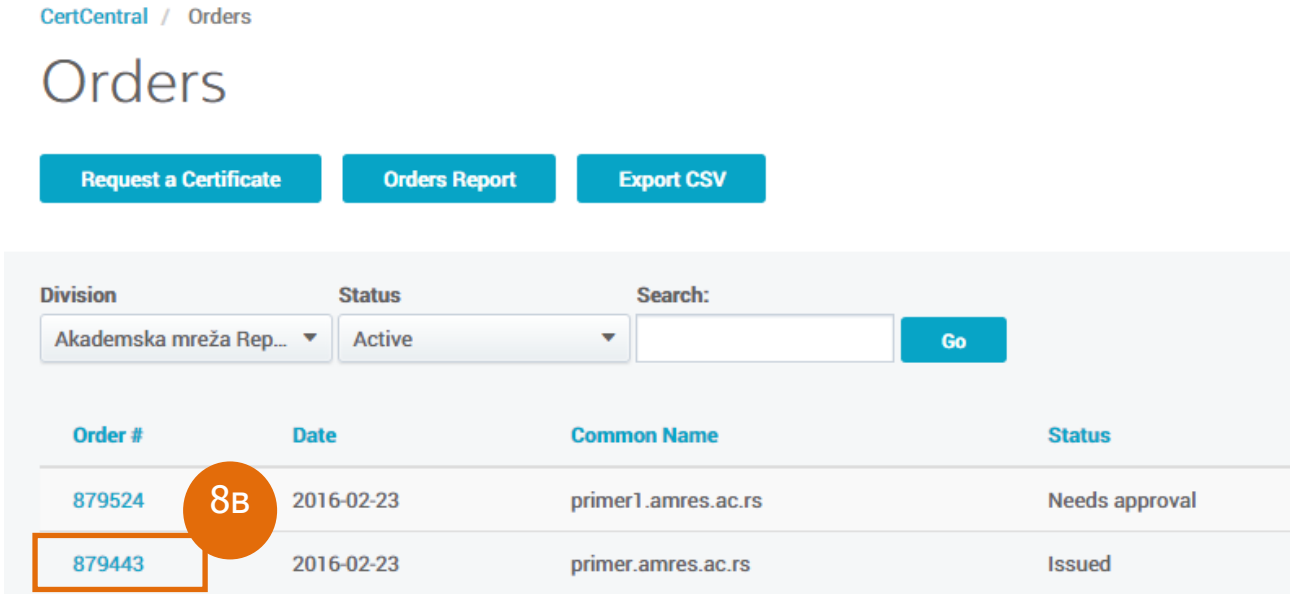
У прилогу имејл поруке, администратор може пронаћи један .zip фајл. У оквиру .zip фајла се налазе тражени сертификат, потом сертификат прелазног сертификационог тела TERENA SSL CA 3 (фајл под именом DigiCertCA.crt) које је потписало тражени сертификат и упутства за инсталацију сертификата на више језика.

Уколико администратор жели да преузме сертификат преко портала, потребно је притиснути опцију „CERTIFICATES" (8а) у левом менију и потом из падајућег менија одабрати опцију „Orders" (8б).



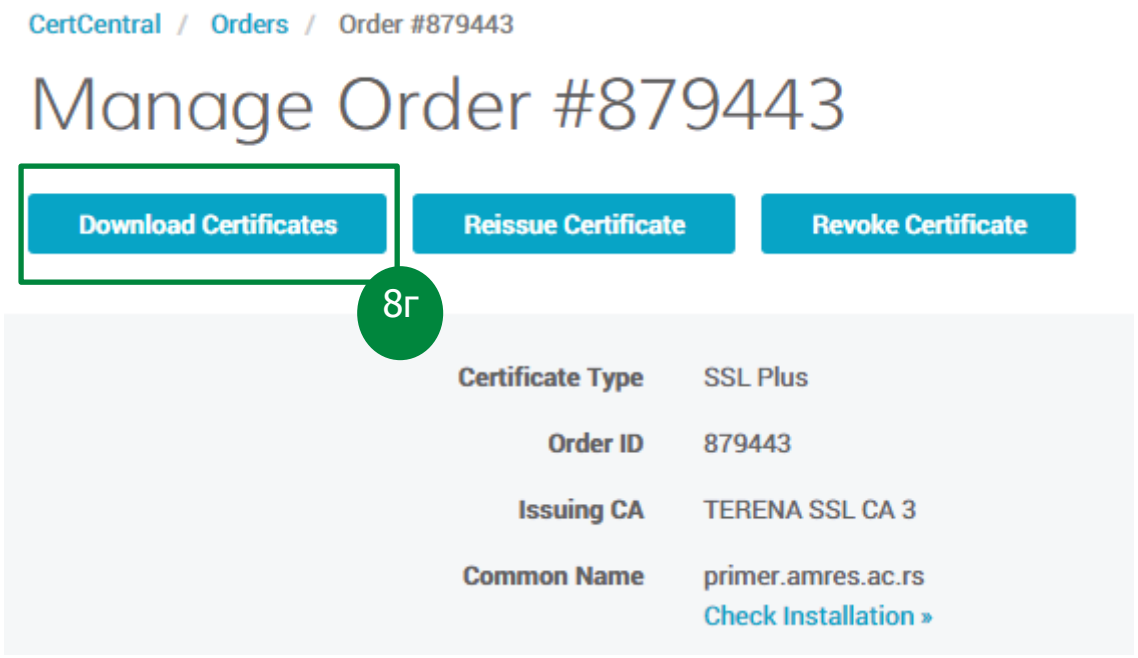
Слика 8

У новоотвореном прозору, администратор може видети списак свих издатих сертификата. Кликом на број поруџбине (8в), портал исписује детаљније податке о сертификату.



Слика 9

У детаљнијем приказу сертификата могуће је преузети сертификат притиском на дугме „Download Certificates" (8г).



Слика 10

НАПОМЕНА: Приликом испоруке сертификата, администратор AMPEC корисника ће примити два сертификата: тражени сертификат и сертификат прелазног сертификационог тела TERENA SSL CA 3. Тражени сертификат је потписан од стране прелазног сертификационог тела TERENA SSL CA 3, а сертификат прелазног сертификационог тела TERENA SSL CA 3 је потписан од стране DigiCert кореног сертификационог тела. Сертификат DigiCert кореног сертификационог тела се не испоручује у TCS сервису будући да је овај сертификат преинсталиран у највећем броју SSL клијената и апликација. У највећем броју случајева сертификациона путања ће бити успостављена коректно, али у ограниченом броју случајева могуће је да ће администраторима затребати и сертификат DigiCert кореног сертификационог тела. У овим ситуацијама, администраторима се препоручује да преузму сертификат „DigiCert Assured ID Root CA" који се може пронаћи на следећој адреси:

- https://www.digicert.com/digicert-root-certificates.htm

Објашњење о креирању сертификационе путање у TCS сервису можете пронаћи и на AMPEC веб страницама.

2.2 Прибављање серверског сертификата за више доменских имена са валидацијом организације

Прибављање серверског сертификата за више доменских имена са валидацијом организације захтева да је AMPEC корисник претходно пријављен за коришћење TCS услуге, има регистрован домен у оквиру „ac.rs" домена и да је извршио валидацију организације и валидацију домена на DigiCert порталу.

Процедура прибављања сертификата захтева следеће акције AMPEC корисника:

- Креирање пара приватног/јавног кључа и захтева за сертификатом
- Подношење захтева за сертификат на DigiCert порталу
- Преузимање сертификата путем имејла или DigiCert портала

У наставку је дат детаљан опис свих потребних корака у процесу прибављања серверских сертификата.

Препоручује се да AMPEC корисници 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 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 Windows оперативне системе препоручује коришћење DigiCert алата.

КОРАК 1

Да би AMPEC 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 AMPEC 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
```

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.

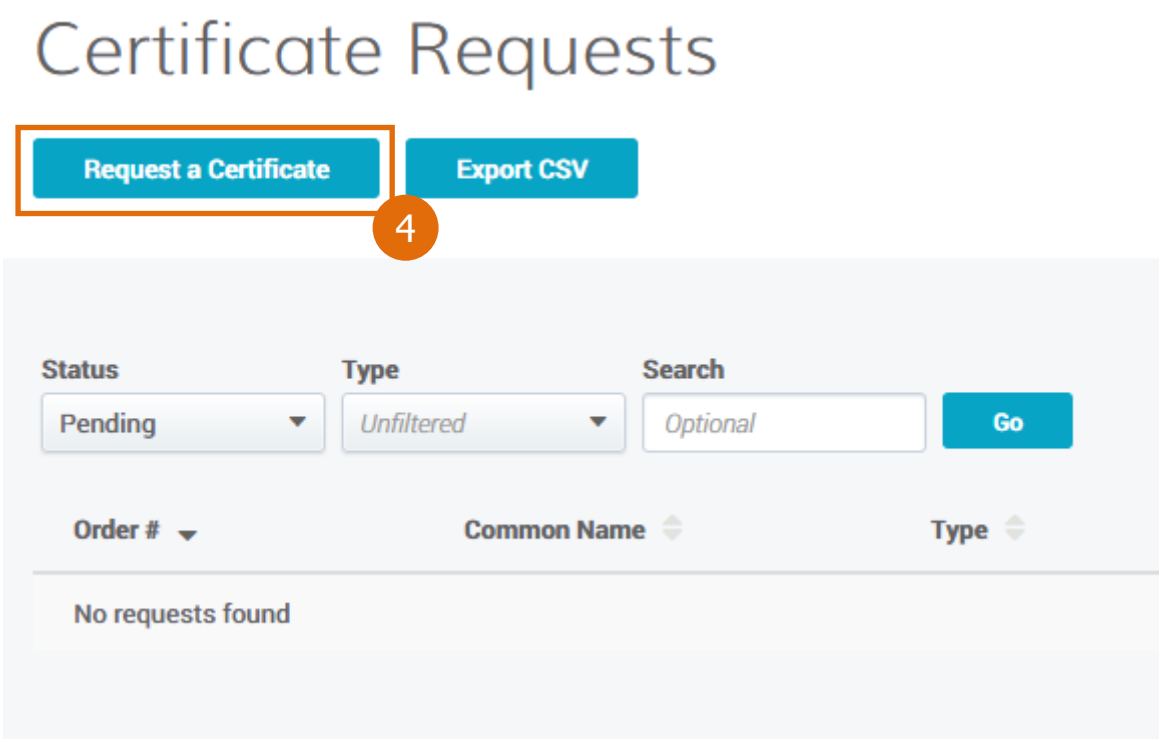
Након попуњавања свих неопходних података, у директоријуму ће бити креирана два нова фајла:

- 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 у наредним корацима прекопирати на DigiCert портал. Садржај .csr фајла се може прочитати било којим текст едитором (vi, nano, joe итд.)

КОРАК 4

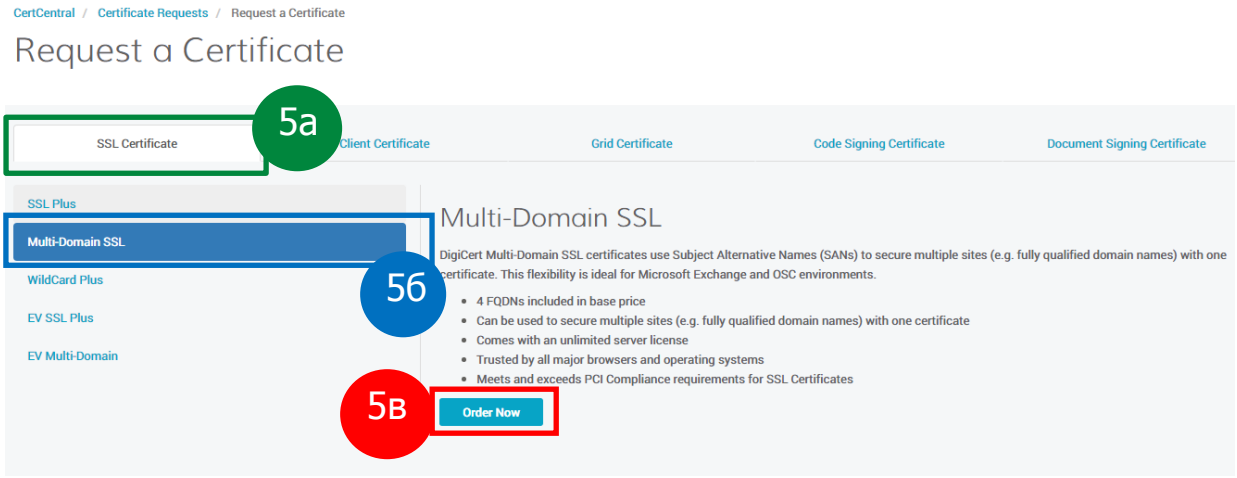
На DigiCert порталу потребно је у менију са леве стране притиснути опцију „CERTIFICATES". У новоотвореном прозору потребно је притиснути дугме „Request a Certificate" (4).



Слика 11

КОРАК 5

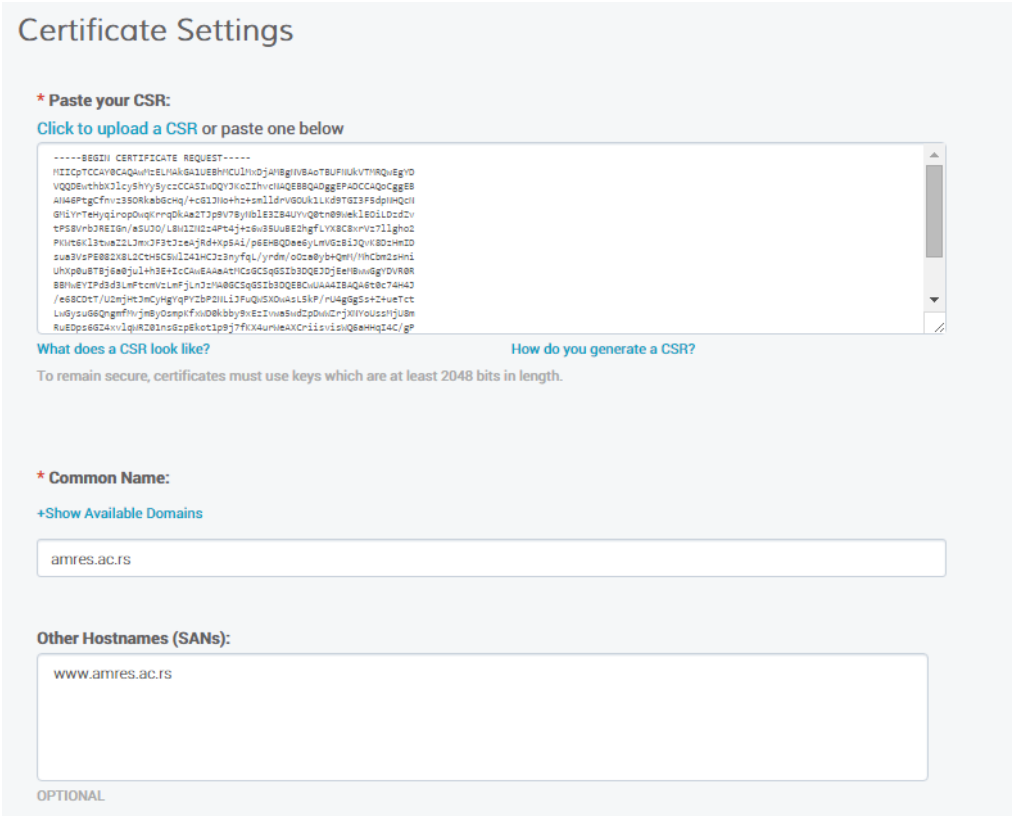
У новоотвореном прозору потребно је одабрати жељени сертификат - таб „SSL Certificate" (5а), опција „Multi-Domain SSL" (5б) са леве стране прозора. У средини прозора приказаће се општи опис одабраног типа сертификата. Потребно је притиснути дугме „Order Now" (5в) како би се захтевао жељени сертификат.



Слика 12

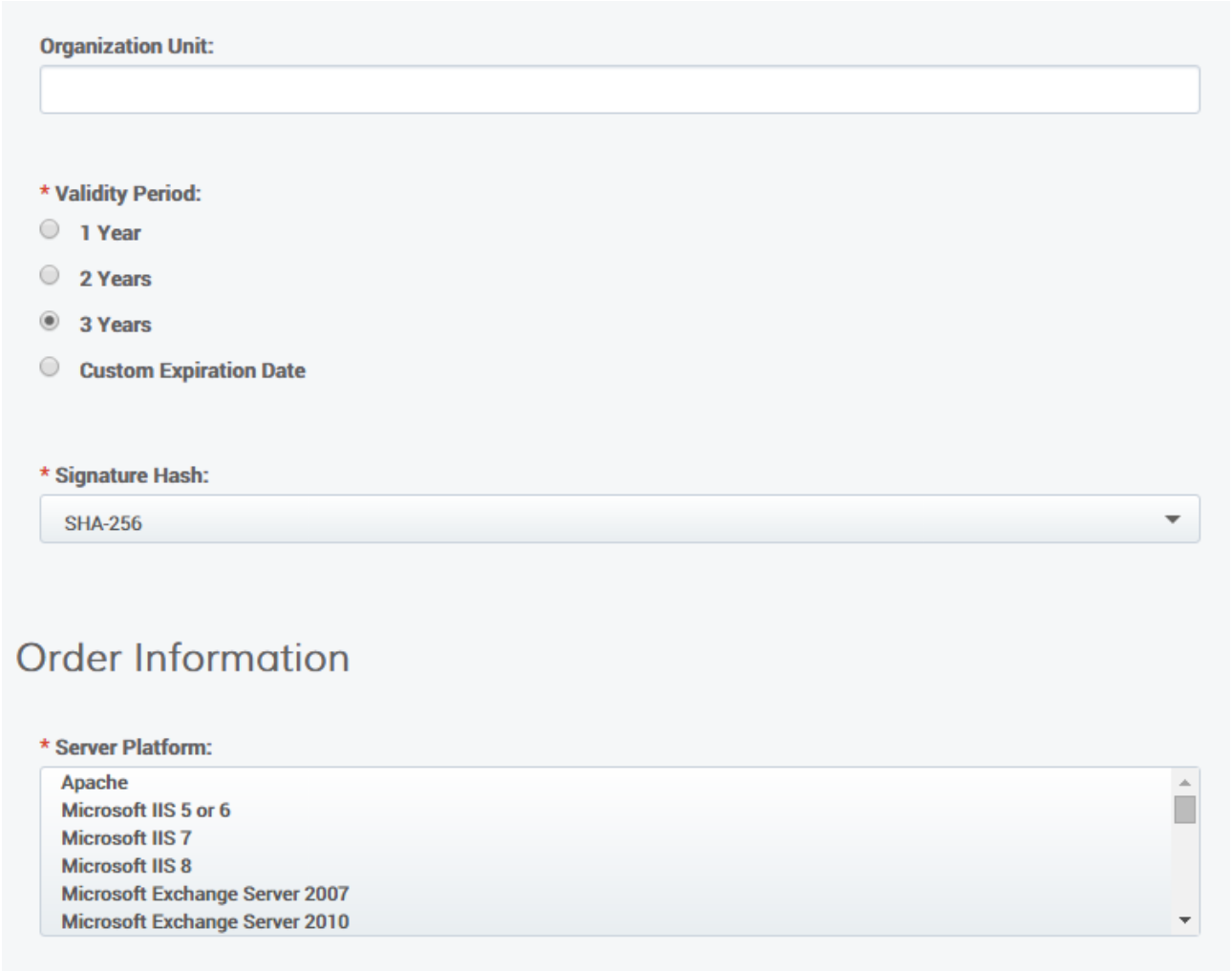
КОРАК 6

Администратору ће се приказати формулар који је потребно попунити како би захтев за сертификат био прослеђен DigiCert провајдеру. У пољу испод „Paste your CSR:" је потребно прекопирати садржај .csr фајла који је добијен у кораку 3. Алтернативно, администратор може притиснути опцију „Click to upload a CSR" која се налази тик изнад поменутог поља како би послао серверу .csr фајл. Након прекопирања садржаја .csr фајла, у пољима „Common Name:" и „Other Hostnames (SANs):" ће се аутоматски исписати FQDN име и алтернативна доменска имена која ће бити заштићена SSL/TLS сертификатом. FQDN и алтернативна доменска имена се читају из .csr фајла и аутоматски уписују у поменута поља.



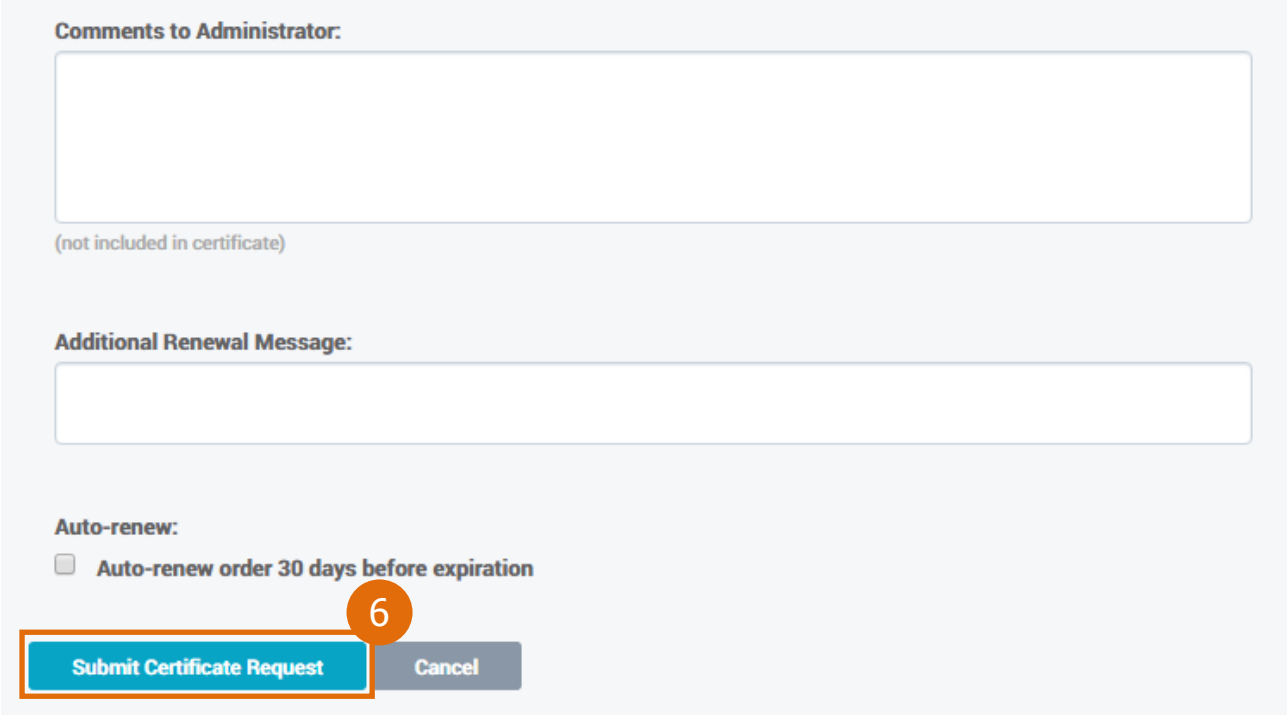
Слика 13

У наставку формулара потребно је одабрати период важења сертификата (1,2 или 3 године), потом изабрати хеш алгоритам који се користи у сертификату (одабрати исти хеш алгоритам који се користио и приликом генерисања захтева у кораку 3 – SHA256) и на крају прецизирати на којој серверској платформи је планирано да се инсталира сертификат након што буде издат. Информација о серверској платформи се прецизира да би DigiCert провајдер заједно са сертификатом испоручио и кратко упутство за инсталацију сертификата на жељеној серверској платформи. Опционо, администратор може прецизирати и организациону јединицу у оквиру институције за коју се захтева сертификат.



Слика 14

На крају формулара је администраторима остављена могућност да оставе поруку осталим администраторима везану за издавање сертификата или да прецизирају поруку коју ће добити приликом будуће нотификације о истеку сертификата и потреби да се исти обнови. Администратори могу обележити опцију „Auto-renew" којом се аутоматски покреће процедура обнове сертификата 30 дана пре истека постојећег сертификата. Све ове опције су опционе и администратори их не морају користити.



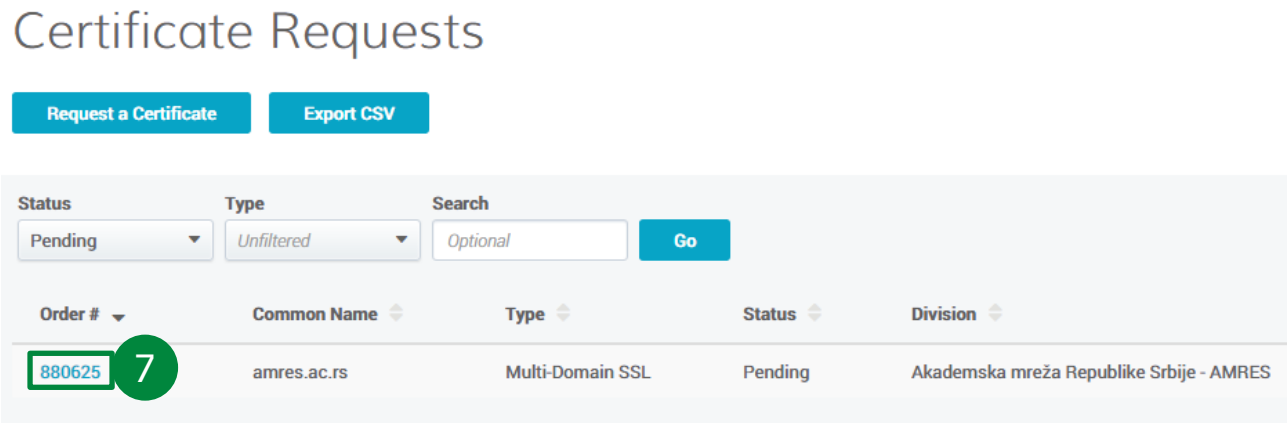
Слика 15

Након попуњавања наведених поља потребно је притиснути дугме „Submit Certificate Request" (6).

КОРАК 7

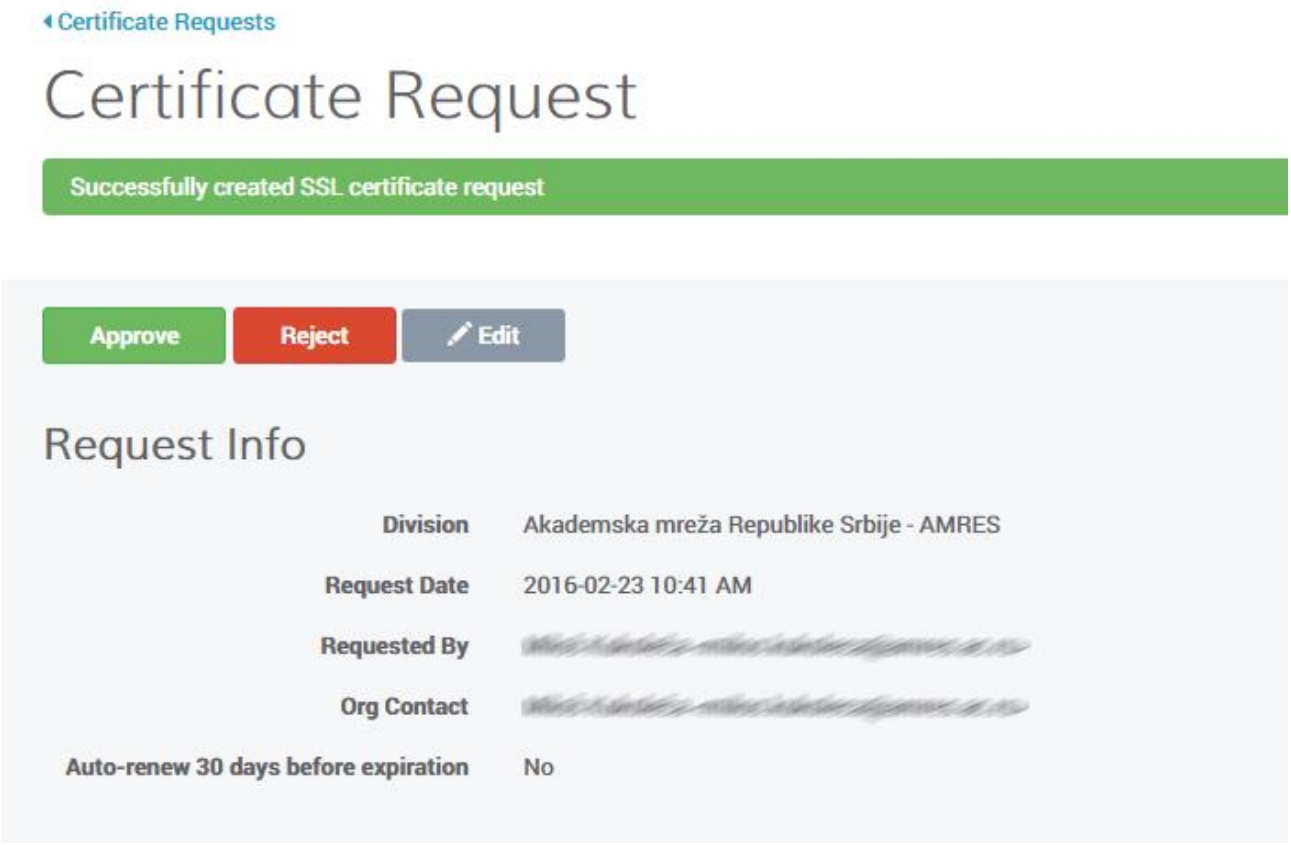
На централном DigiCert порталу је могуће у оквиру једне институције креирати кориснике са привилегијама обичног корисника (User) или администратора (Admin, SAML Admin). Било да је захтев поднео обичан корисник или администратор, захтев мора бити потврђен од стране администратора.

У складу са тим, након слања захтева преко портала, администратору ће се приказати прозор у оквиру кога ће морати да потврди поруџбину сертификата. Администратор може потврдити поруџбину одмах или може то урадити касније. Тражени сертификат неће бити издат док поруџбина не буде потврђена од стране администратора. У случају да администратор жели да види које поруџбине је потребно потврдити неопходно је да на порталу у левом менију одабере „CERTIFICATES" а потом из падајућег менија одабере опцију „Requests".



Слика 16

Кликом на број наруџбине (7) са леве стране листе, долази се до детаљног описа захтеваног сертификата где је могуће потврдити или одбити поруџбину.



Слика 17

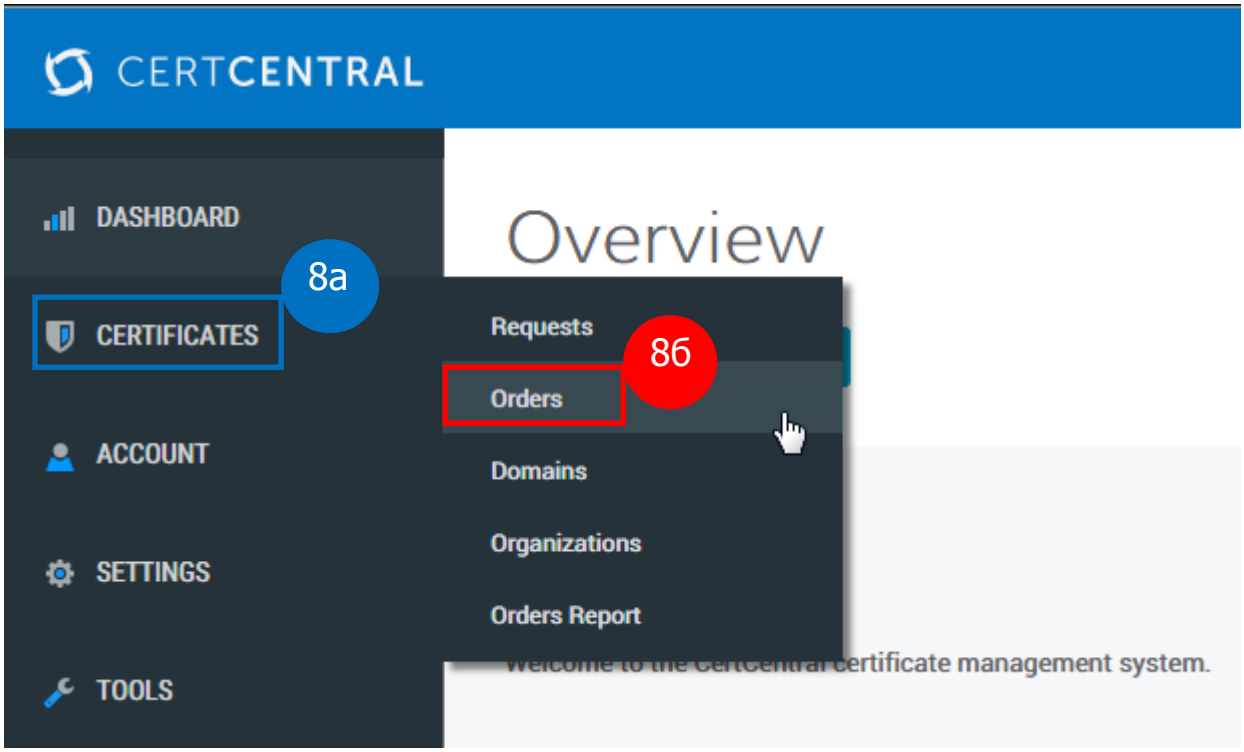
Притиском на дугме „Approve" отвара се нови прозор у коме је потребно уписати коментар који ће бити сачуван. Након уписа произвољног коментара и притиска на дугме „Approve" потврђује се поруџбина сертификата.

KORAK 8

Убрзо након потврђивања наруџбине сертификата, на имејл адресу корисника/администратора који је захтевао сертификат ће пристићи имејл са траженим сертификатом.

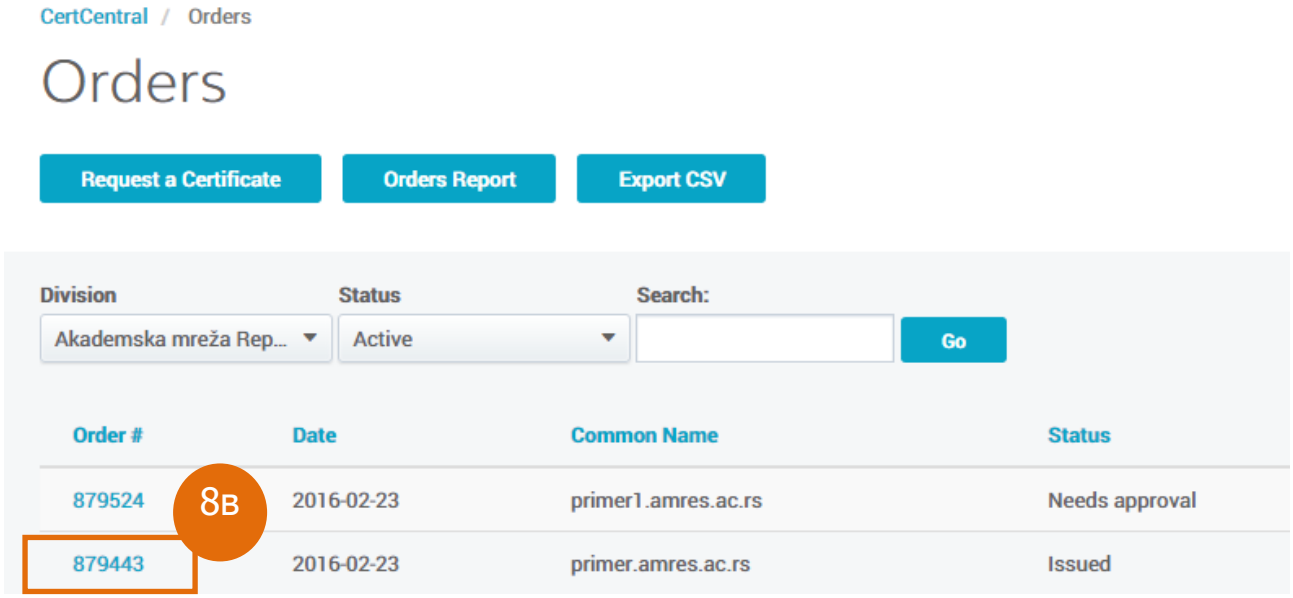
У прилогу имејл поруке, администратор може пронаћи један .zip фајл. У оквиру .zip фајла се налазе тражени сертификат, потом сертификат прелазног сертификационог тела TERENA SSL CA 3 (фајл под именом DigiCertCA.crt) које је потписало тражени сертификат и упутства за инсталацију сертификата на више језика.

Уколико администратор жели да преузме сертификат преко портала, потребно је притиснути опцију „CERTIFICATES" (8а) у левом менију и потом из падајућег менија одабрати опцију „Orders" (8б).



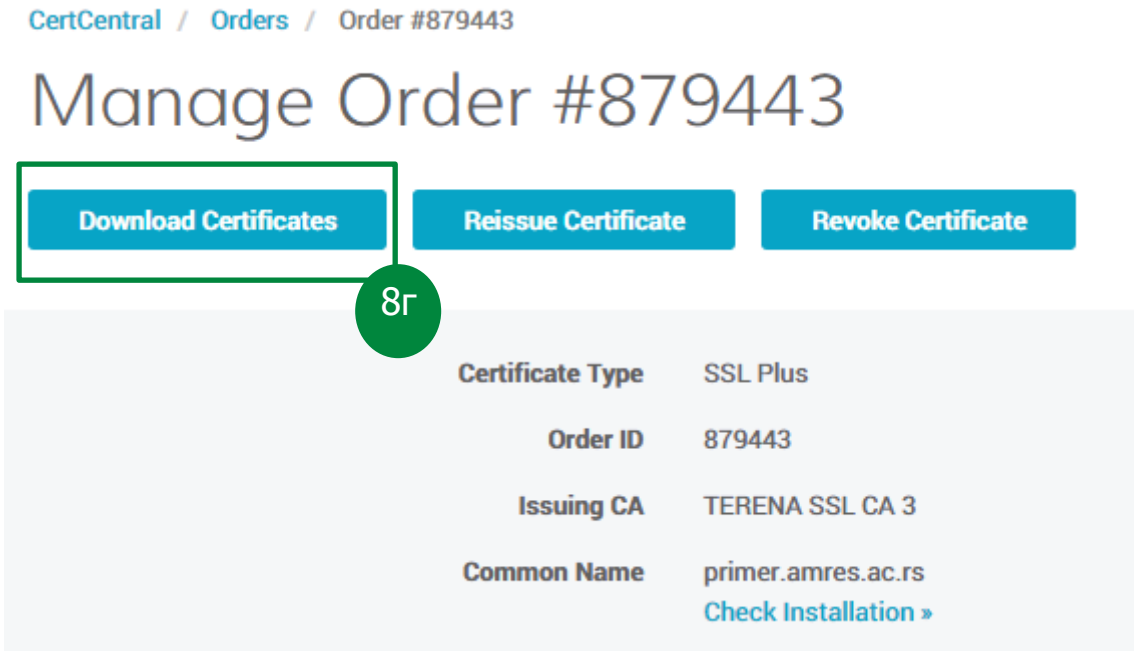
Слика 18

У новоотвореном прозору, администратор може видети списак свих издатих сертификата. Кликом на број поруџбине (8в), портал исписује детаљније податке о сертификату.



Слика 19

У детаљнијем приказу сертификата могуће је преузети сертификат притиском на дугме „Download Certificates" (8г).



Слика 20

НАПОМЕНА: Приликом испоруке сертификата, администратор AMPEC корисника ће примити два сертификата: тражени сертификат и сертификат прелазног сертификационог тела TERENA SSL CA 3. Тражени сертификат је потписан од стране прелазног сертификационог тела TERENA SSL CA 3, а сертификат прелазног сертификационог тела TERENA SSL CA 3 је потписан од стране DigiCert кореног сертификационог тела. Сертификат DigiCert кореног сертификационог тела се не испоручује у TCS сервису будући да је овај сертификат преинсталиран у највећем броју SSL клијената и апликација. У највећем броју случајева сертификациона путања ће бити успостављена коректно, али у ограниченом броју случајева могуће је да ће администраторима затребати и сертификат DigiCert кореног сертификационог тела. У овим ситуацијама, администраторима се препоручује преузму сертификат „DigiCert Assured ID Root CA" који се може пронаћи на следећој адреси:

- https://www.digicert.com/digicert-root-certificates.htm

Објашњење о креирању сертификационе путање у TCS сервису можете пронаћи и на AMPEC веб страницама.

2.3 Прибављање серверског сертификата за сва поддоменска имена једног домена са валидацијом организације (*wildcard*)

Прибављање серверског сертификата за сва поддоменска имена једног домена са валидацијом организације (*wildcard*) захтева да је AMPEC корисник претходно пријављен за коришћење TCS услуге, има регистрован домен у оквиру „ac.rs" домена и да је извршио валидацију организације и валидацију домена на DigiCert порталу.

Процедура прибављања сертификата захтева следеће акције AMPEC корисника:

- Креирање пара приватног/јавног кључа и захтева за сертификатом
- Подношење захтева за сертификат на DigiCert порталу
- Преузимање сертификата путем имејла или DigiCert портала

У наставку је дат детаљан опис свих потребних корака у процесу прибављања серверских сертификата.

Препоручује се да AMPEC корисници 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 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 Windows оперативне системе препоручује коришћење DigiCert алата.

КОРАК 1

Да би AMPEC 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 свим поддоменским именима једног домена потребно је са AMPEC 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 за сертификатом.

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 SCSreq.cnf -utf8 –sha256 -keyout myserver.key –out myserver.csr
```

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. Приликом уписивања FQDN имена потребно је испред домена за који се сертификат захтева навести тзв. *wildcard* каркатер *, на пример *.amres.ac.rs. Домен *.amres.ac.rs представља сва могућа поддоменска имена домена amres.ac.rs.

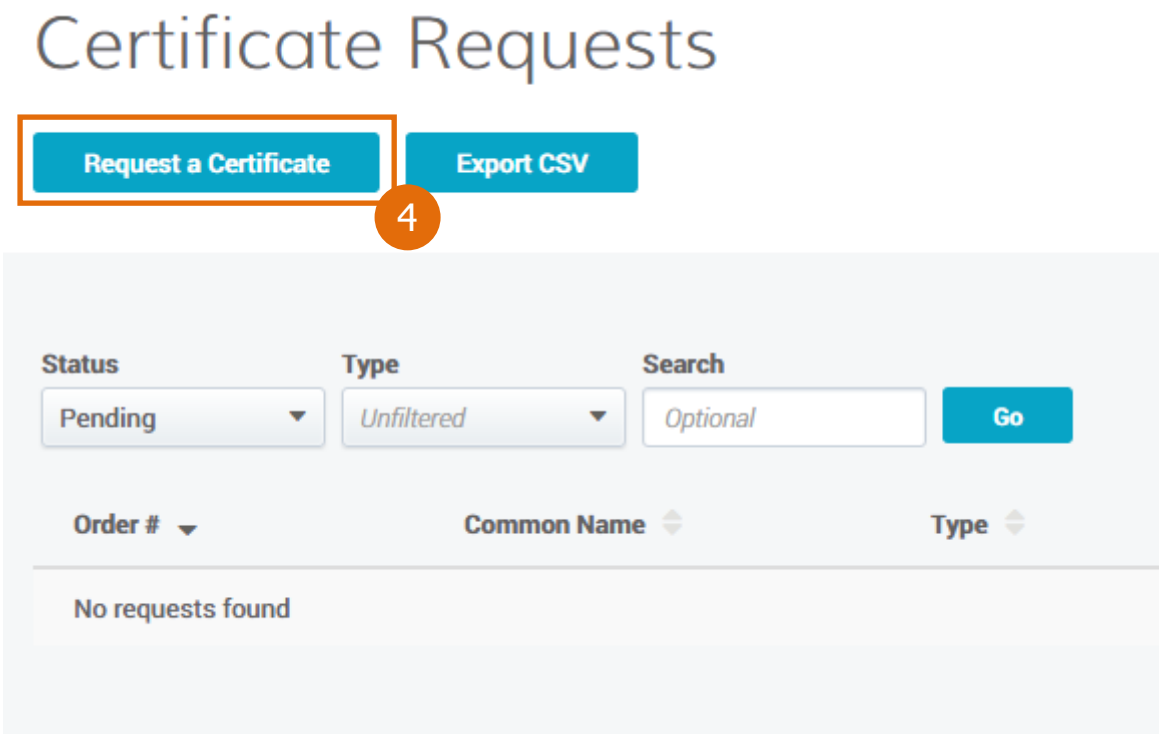
Након попуњавања свих неопходних података, у директоријуму ће бити креирана два нова фајла:

- 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 у наредним корацима прекопирати на DigiCert портал. Садржај .csr фајла се може прочитати било којим текст едитором (vi, nano, joe итд.).

КОРАК 4

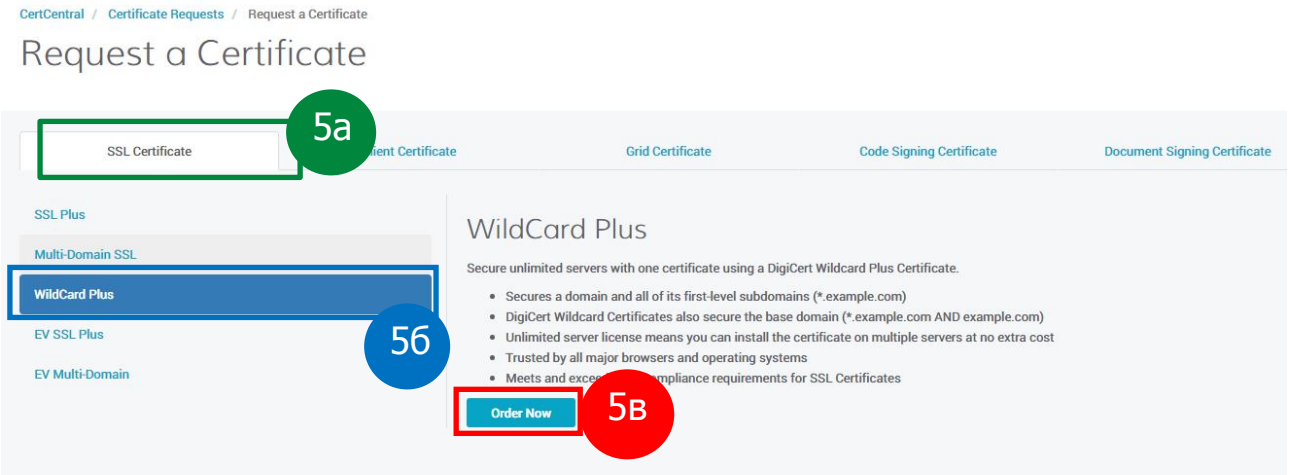
На DigiCert порталу потребно је у менију са леве стране притиснути опцију „CERTIFICATES". У новоотвореном прозору потребно је притиснути дугме „Request a Certificate" (4).



Слика 21

КОРАК 5

У новоотвореном прозору потребно је одабрати жељени сертификат - таб „SSL Certificate" (5а), опција „Wildcard Plus" (5б) са леве стране прозора. У средини прозора приказаће се општи опис одабраног типа сертификата. Потребно је притиснути дугме „Order Now" (5в) како би се захтевао жељени сертификат.

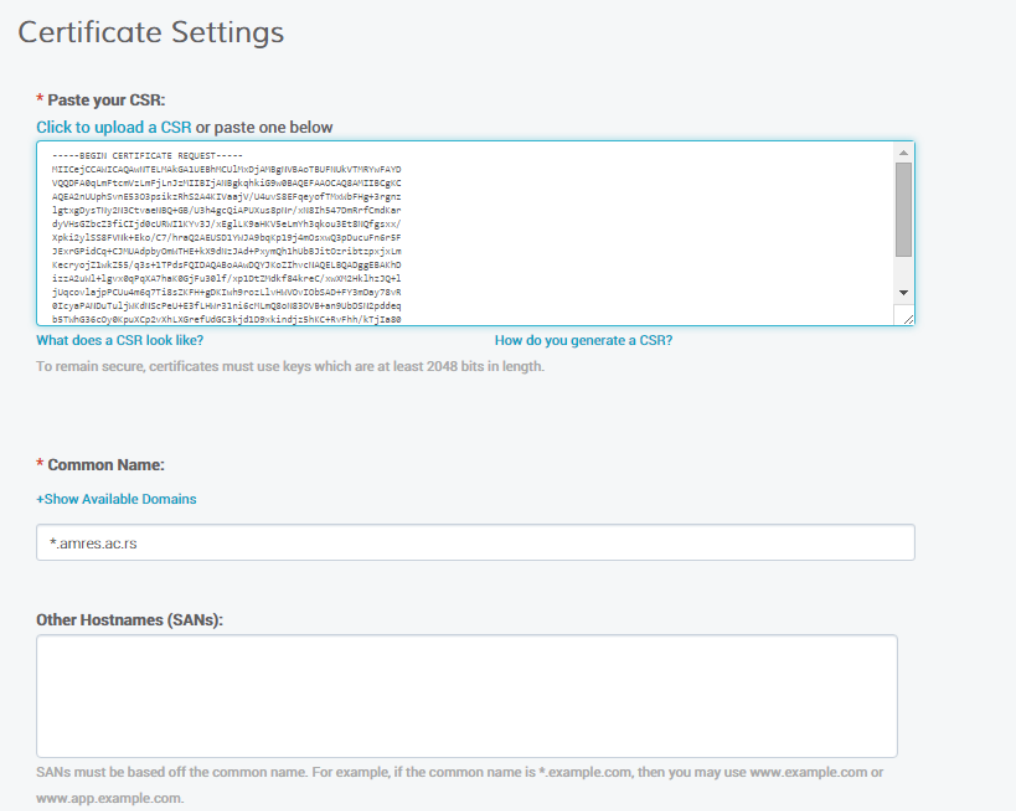


Слика 22

КОРАК 6

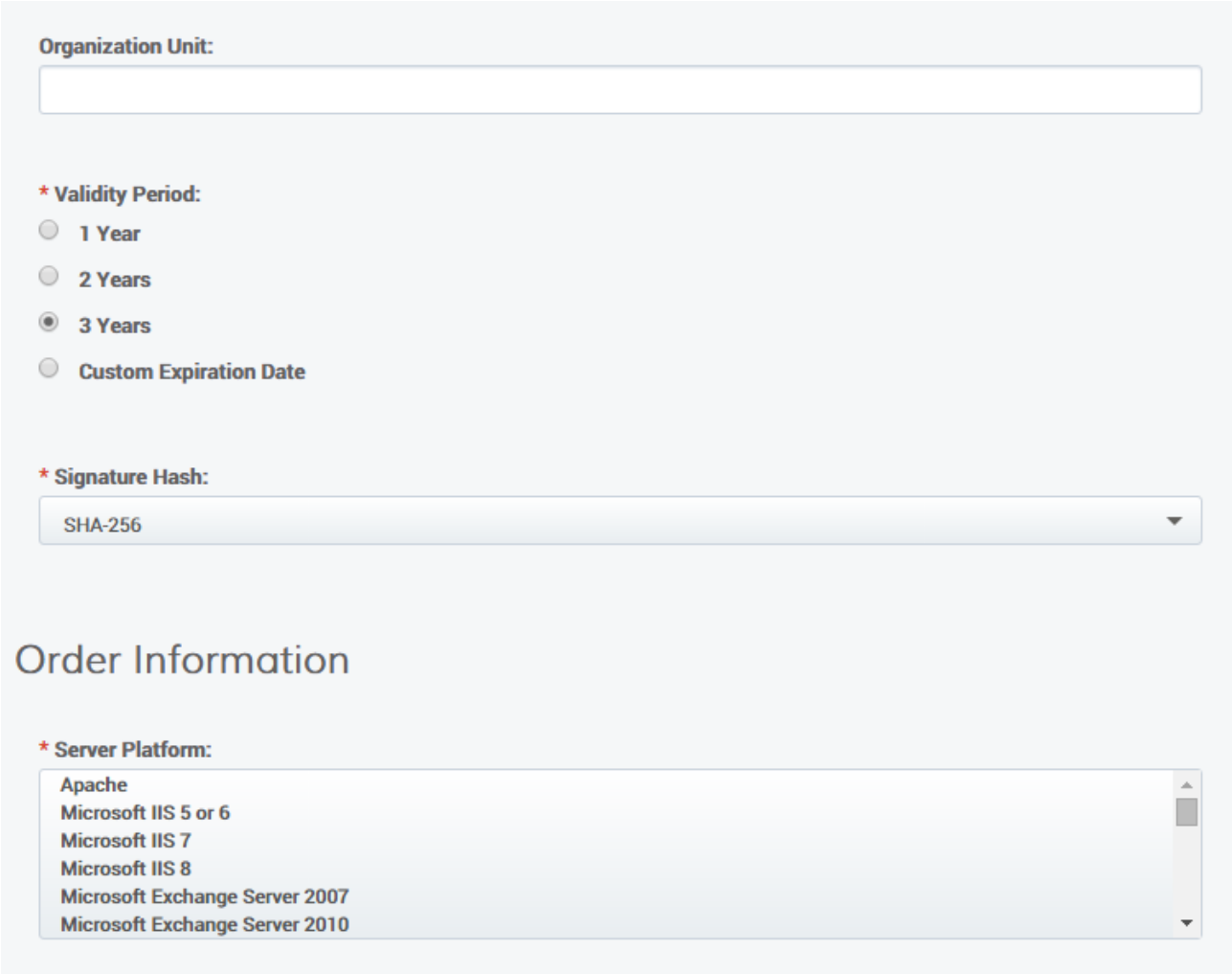
Администратору ће се приказати формулар који је потребно попунити како би захтев за сертификат био прослеђен DigiCert провајдеру. У пољу испод „Paste your CSR:" је потребно прекопирати садржај .csr фајла који је добијен у кораку 3. Алтернативно, администратор може притиснути опцију „Click to upload a CSR" која се налази тик изнад поменутог поља како би послао серверу .csr фајл. Након

прекопирања садржаја .csr фајла, у пољу „Common Name:" ће се аутоматски исписати FQDN име које ће бити заштићено SSL/TLS сертификатом. *Wildcard* FQDN име се чита из .csr фајла и аутоматски уписује у поменуто поље.



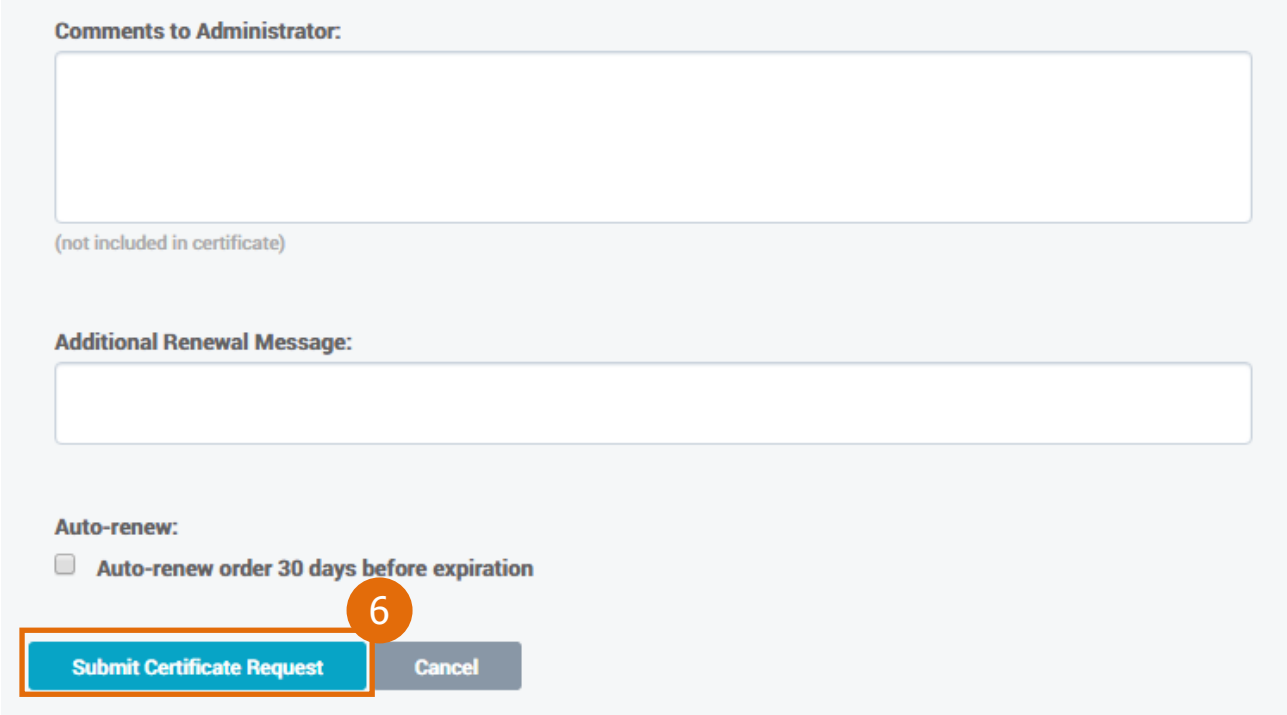
Слика 23

У наставку формулара потребно је одабрати период важења сертификата (1,2 или 3 године), потом изабрати хеш алгоритам који се користи у сертификату (одабрати исти хеш алгоритам који се користио и приликом генерисања захтева у кораку 3 – SHA256) и на крају прецизирати на којој серверској платформи је планирано да се инсталира сертификат након што буде издат. Информација о серверској платформи се прецизира да би DigiCert провајдер заједно са сертификатом испоручио и кратко упутство за инсталацију сертификата на жељеној серверској платформи. Опционо, администратор може прецизирати и организациону јединицу у оквиру AMPEC корисника за коју се захтева сертификат.



Слика 24

На крају формулара је администраторима остављена могућност да оставе поруку осталим администраторима везану за издавање сертификата или да прецизирају поруку коју ће добити приликом будуће нотификације о истеку сертификата и потреби да се исти обнови. Администратори могу обележити опцију „Auto-renew" којом се аутоматски покреће процедура обнове сертификата 30 дана пре истека постојећег сертификата. Све ове опције су опционе и администратори их не морају користити.



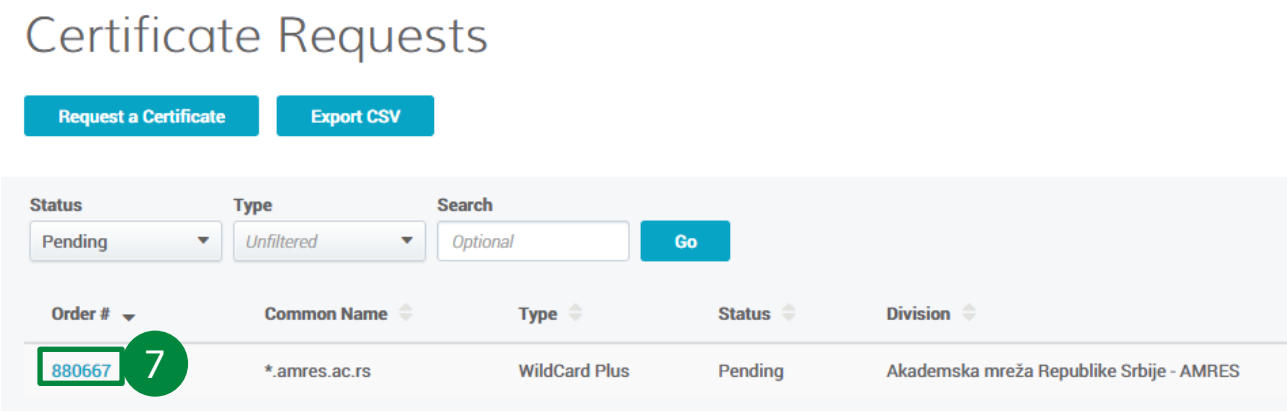
Слика 25

Након попуњавања наведених поља потребно је притиснути дугме „Submit Certificate Request" (6).

КОРАК 7

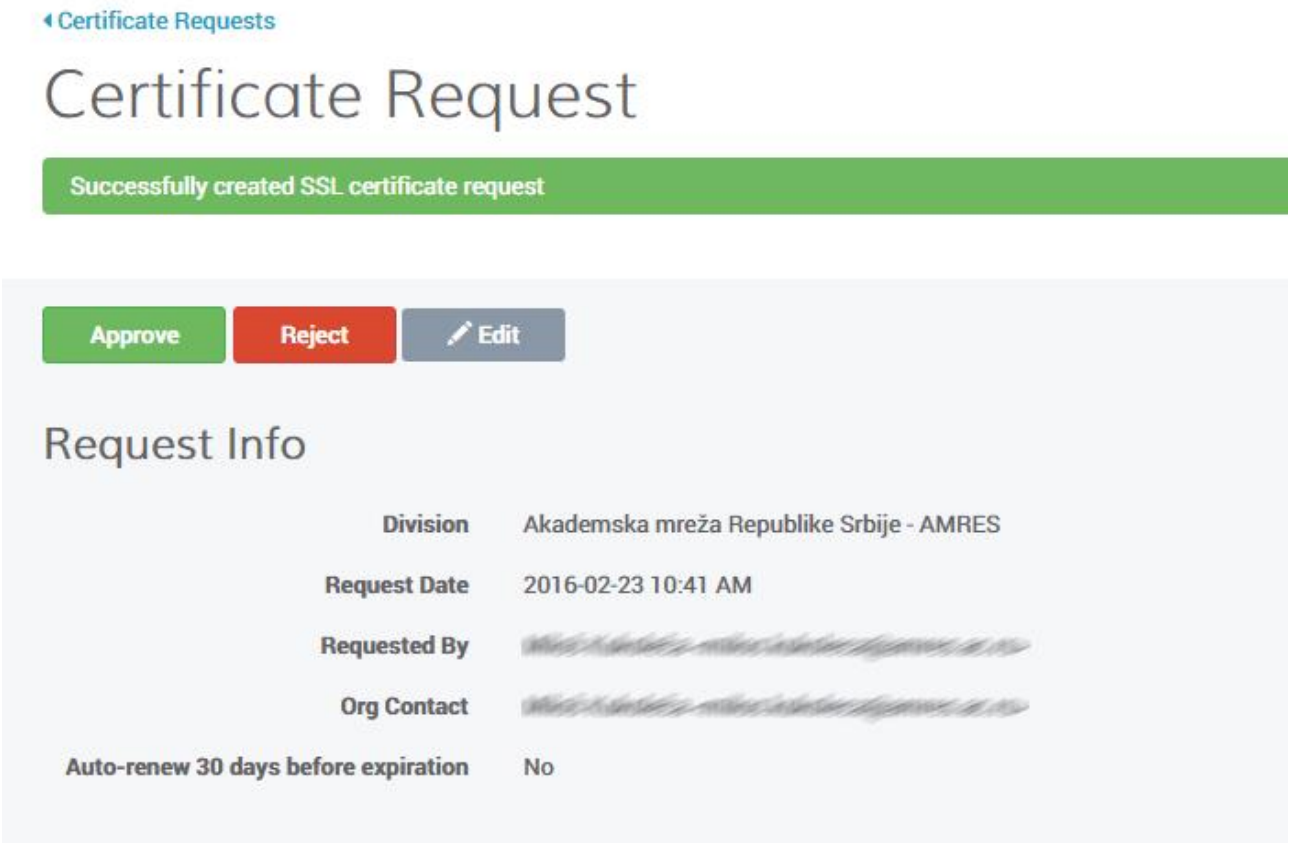
На централном DigiCert TCS порталу је могуће у оквиру једне институције креирати кориснике са привилегијама обичног корисника (User) или администратора (Admin, SAML Admin). Било да је захтев поднео обичан корисник или администратор, захтев мора бити потврђен од стране администратора.

У складу са тим, након слања захтева преко портала, администратору ће се приказати прозор у оквиру кога ће морати да потврди поруџбину сертификата. Администратор може потврдити поруџбину одмах или може то урадити касније. Тражени сертификат неће бити издат док поруџбина не буде потврђена од стране администратора. У случају да администратор жели да види које поруџбине је потребно потврдити неопходно је да на порталу у левом менију одабере „CERTIFICATES" а потом из падајућег менија одабере опцију „Requests".



Слика 26

Кликом на број наруџбине (7) са леве стране листе, долази се до детаљног описа захтеваног сертификата где је могуће потврдити или одбити поруџбину.



Слика 27

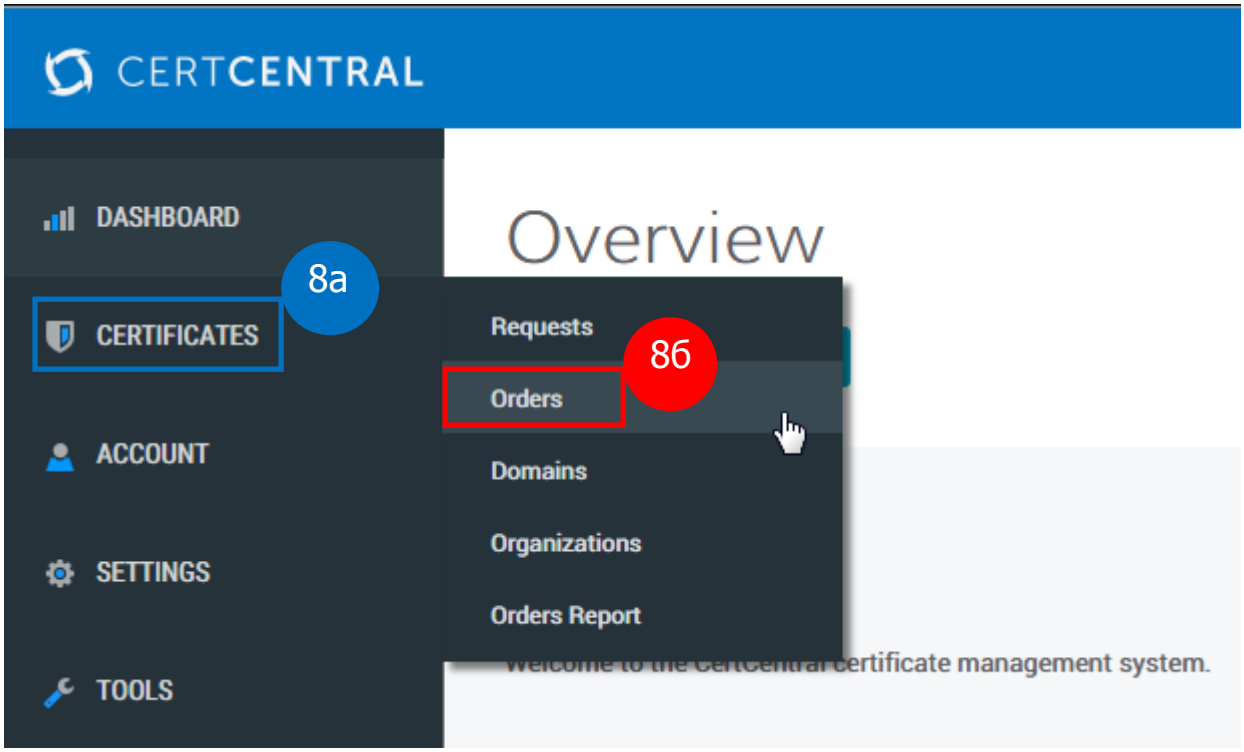
Притиском на дугме „Approve" отвара се нови прозор у коме је потребно уписати коментар који ће бити сачуван. Након уписа произвољног коментара и притиска на дугме „Approve" потврђује се поруџбина сертификата.

KORAK 8

Убрзо након потврђивања наруџбине сертификата, на имејл адресу корисника/администратора који је захтевао сертификат ће пристићи имејл са траженим сертификатом.

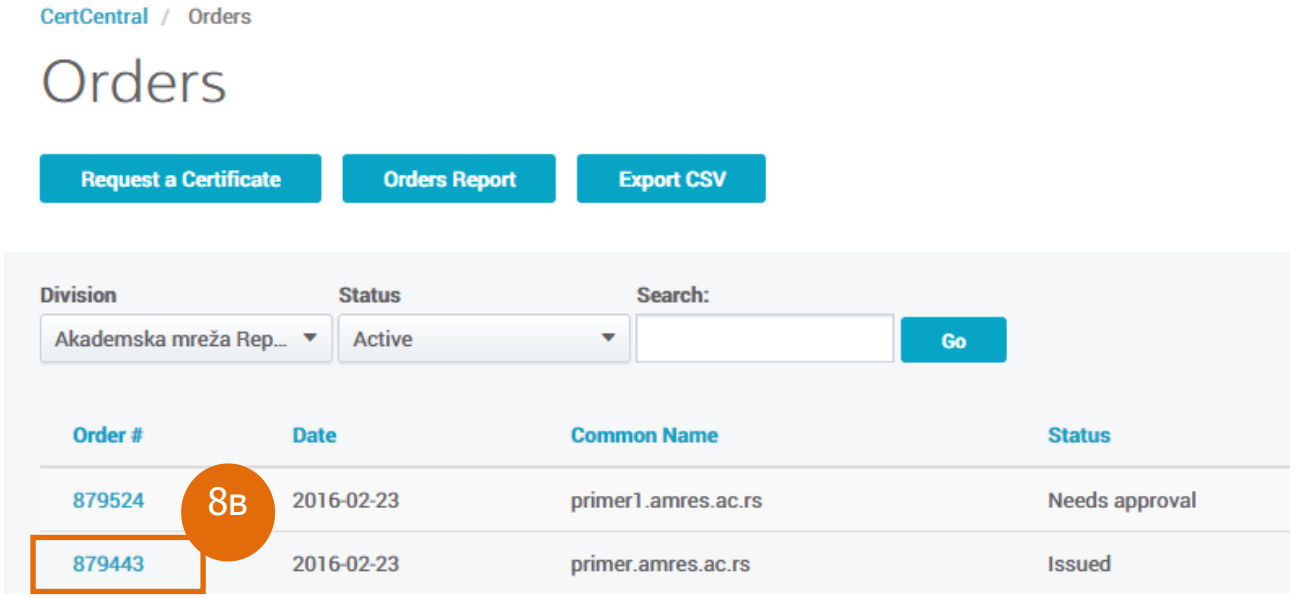
У прилогу имејл поруке, администратор може пронаћи један .zip фајл. У оквиру .zip фајла се налазе тражени сертификат, потом сертификат прелазног сертификационог тела TERENA SSL CA 3 (фајл под именом DigiCertCA.crt) које је потписало тражени сертификат и упутства за инсталацију сертификата на више језика.

Уколико администратор жели да преузме сертификат преко портала, потребно је притиснути опцију „CERTIFICATES" (8а) у левом менију и потом из падајућег менија одабрати опцију „Orders" (8б).



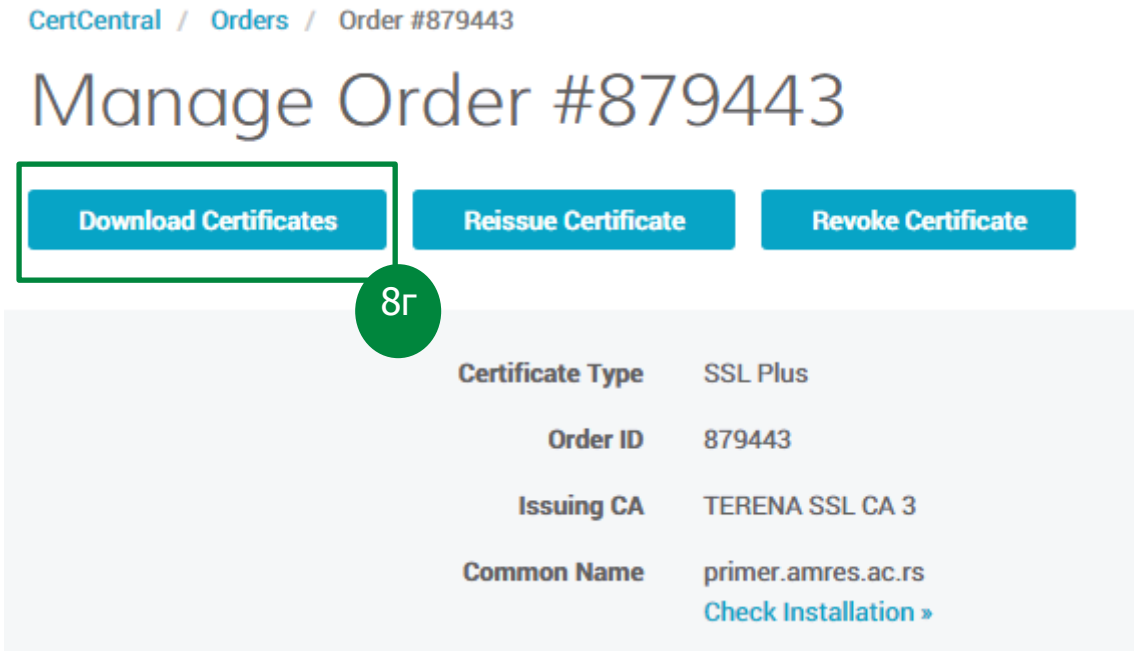
Слика 28

У новоотвореном прозору, администратор може видети списак свих издатих сертификата. Кликом на број поруџбине (8в), портал исписује детаљније податке о сертификату.



Слика 29

У детаљнијем приказу сертификата могуће је преузети сертификат притиском на дугме „Download Certificates" (8г).



Слика 30

НАПОМЕНА: Приликом испоруке сертификата, администратор AMPEC корисника ће примити два сертификата: тражени сертификат и сертификат прелазног сертификационог тела TERENA SSL CA 3. Тражени сертификат је потписан од стране прелазног сертификационог тела TERENA SSL CA 3, а сертификат прелазног сертификационог тела TERENA SSL CA 3 је потписан од стране DigiCert кореног сертификационог тела. Сертификат DigiCert кореног сертификационог тела се не испоручује у TCS сервису будући да је овај сертификат преинсталиран у највећем броју SSL клијената и апликација. У највећем броју случајева сертификациона путања ће бити успостављена коректно, али у ограниченом броју случајева могуће је да ће администраторима затребати и сертификат DigiCert кореног сертификационог тела. У овим ситуацијама, администраторима се препоручује преузму сертификат „DigiCert Assured ID Root CA" који се може пронаћи на следећој адреси:

- https://www.digicert.com/digicert-root-certificates.htm

Објашњење о креирању сертификационе путање у TCS сервису можете пронаћи и на AMPEC веб страницама.

2.4 Прибављање клијентских сертификата

Прибављање клијентских сертификата захтева да је AMPEC корисник (институција) претходно пријављен на AMPEC TCS сервис, има регистрован домен у оквиру „ac.rs" домена и да је извршио валидацију организације и валидацију домена на DigiCert порталу. Након испуњавања свих наведених предуслова, AMPEC корисник може за потребе својих крајњих корисника захтевати клијентске сертификате (раније познате као личне сертификате). У TCS сервису могуће је прибавити следеће клијентске сертификате:

- Клијентски сертификат за потписивање (*Digital Signature Plus*)
- Клијентски сертификат за енкрипцију (*Email Security Plus*)
- Клијентски (S/MIME) имејл сертификат за енкрипцију и потписивање (*Premium*)

AMPEC препоручује свим својим корисницима да прибављају искључиво (*Premium*) клијентске (S/MIME) сертификате будући да ови сертификати имају омогућене све функције типичних личних сертификата.

Клијентски сертификати се могу прибављати помоћу:

- Експлицитног захтева администратора на DigiCert порталу за сваког појединачног корисника
- Федерације идентитета

Када федерација идентитета заживи међу AMPEC корисницима, овај начин прибављања клијентских сертификата ће постати једини могућ. До тада, AMPEC корисницима се оставља могућност прибављања клијентских сертификата помоћу експлицитних захтева администратора AMPEC корисника. На AMPEC веб-страницама се може пронаћи више информација о иAMPEC федерацији идентитета.

Процедура прибављања клијентских сертификата је иста за сваки тип клијентског сертификата и захтева следеће акције:

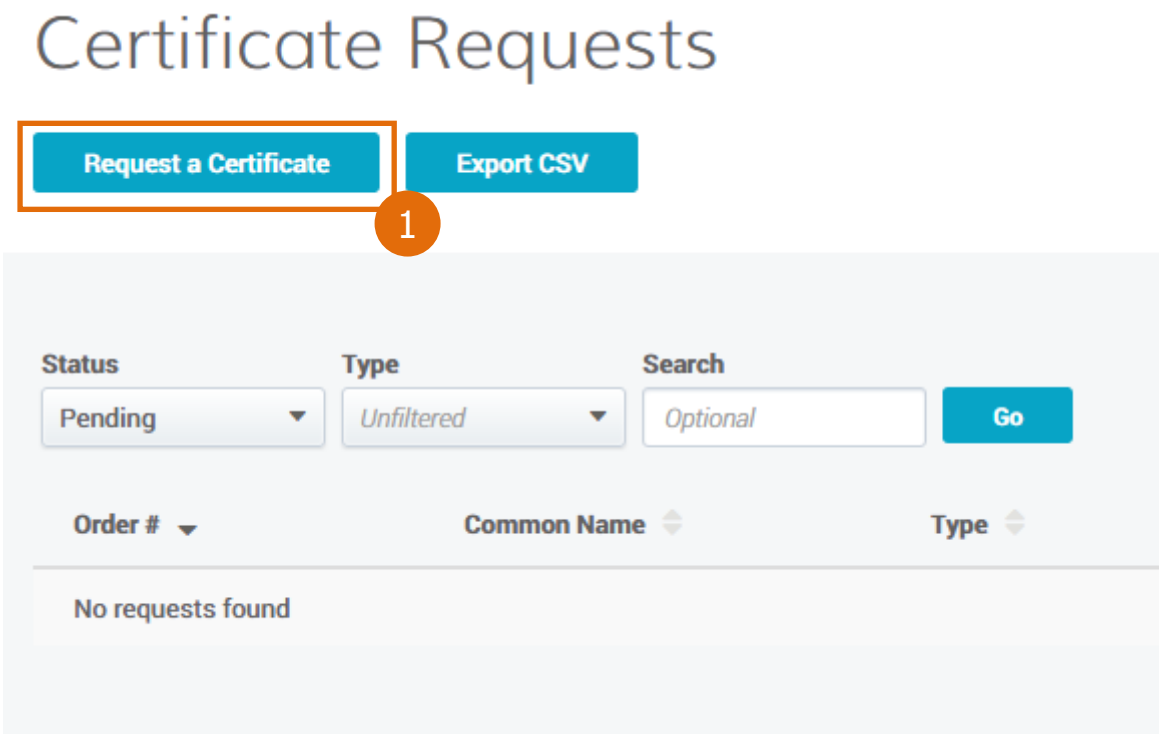
- Подношење захтева за сертификат на DigiCert порталу од стране администратора
- Валидација имејл адресе од стране крајњег корисника
- Генерисање приватног кључа и преузимање сертификата од стране крајњег корисника

У наставку је дат детаљан опис свих потребних корака у процесу прибављања клијентских сертификата.

КОРАК 1

Администратор AMPEC корисника у име крајњег корисника подноси захтев за издавање клијентског сертификата.

На DigiCert порталу потребно је у менију са леве стране притиснути опцију „CERTIFICATES". У новоотвореном прозору потребно је притиснути дугме „Request a Certificate" (1).

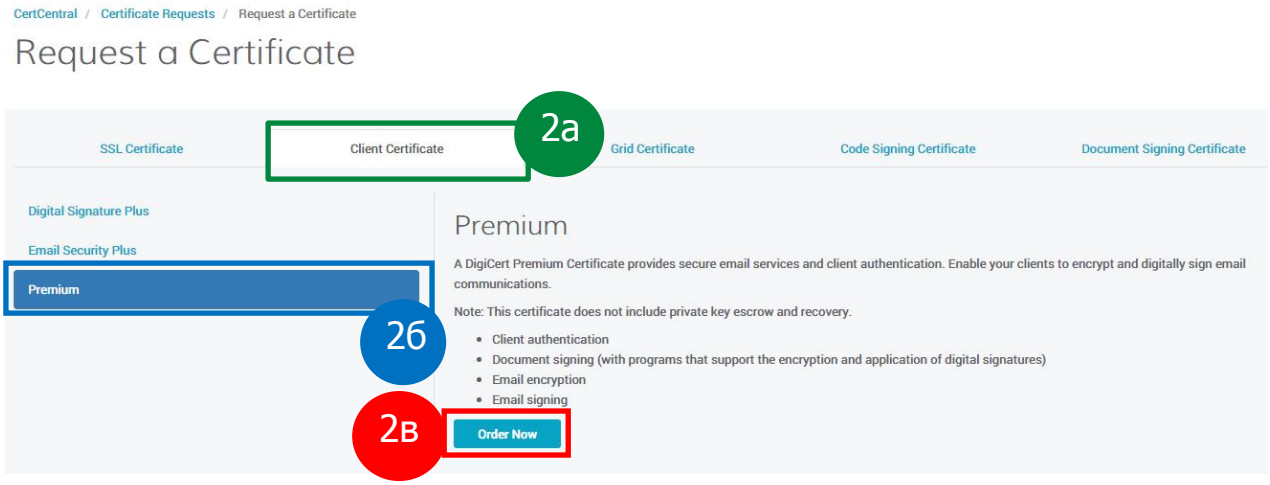


Слика 31

КОРАК 2

У новоотвореном прозору потребно је одабрати жељени сертификат - таб „Client Certificate" (2а), опција „Premium" (2б) са леве стране прозора. У средини прозора приказаће се општи опис одабраног

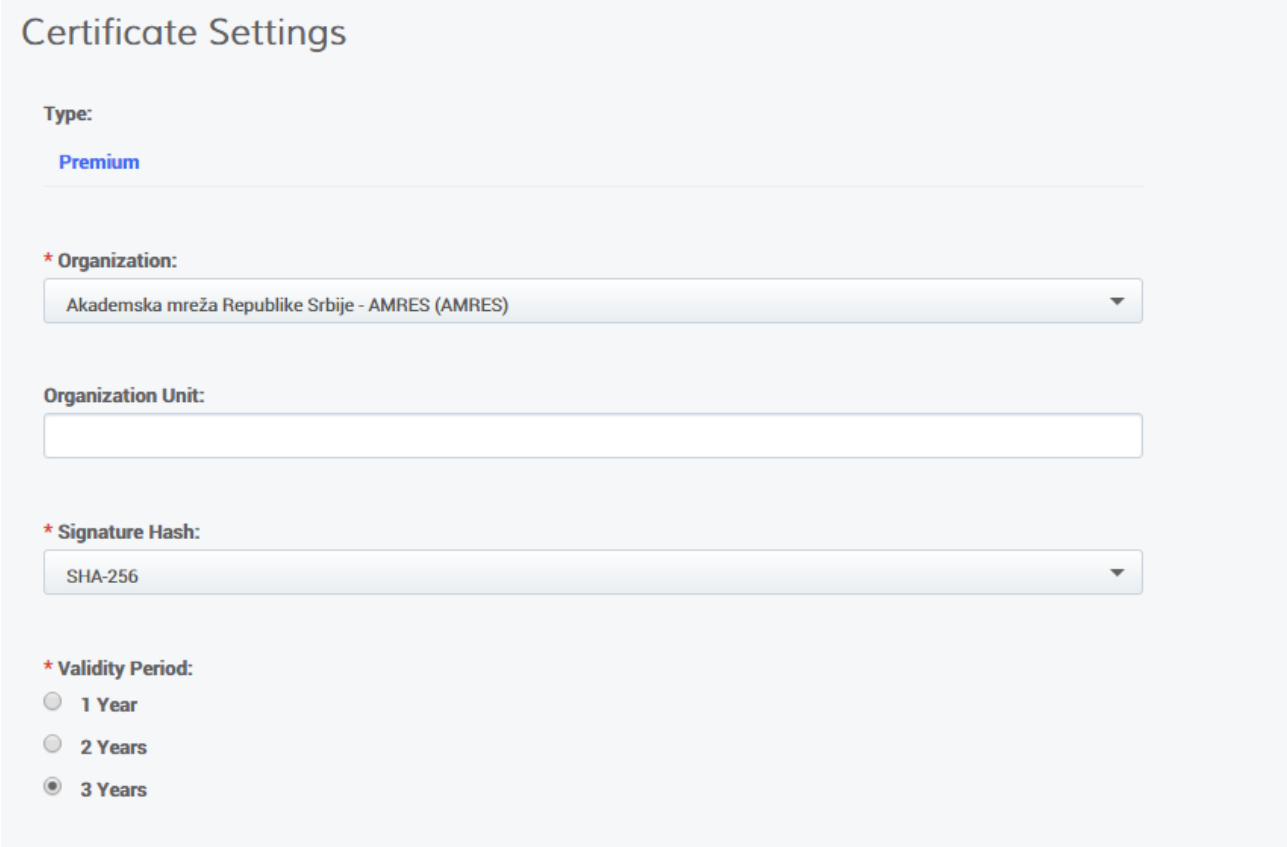
типа сертификата. „Premium" сертификат представља клијентски (S/MIME) имејл сертификат који омогућава аутентификацију корисника, потписивање дигиталних докумената, енкрипцију и потписивање у имејл порукама. Сертификати „Digital Signature Plus" и „Email Security Plus" имају само део ових могућности те се AMPEC корисницима препоручује да својим крајњим корисницима издају само „Premium" сертификате. Након одабира сертификата, потребно је притиснути дугме „Order Now" (2в) како би се захтевао жељени сертификат.



Слика 32

КОРАК 3

У новом прозору на порталу ће се приказати формулар који је потребно попунити како би захтев био прослеђен DigiCert провајдеру. Администратор може опционо уписати име организационе јединице којој припада крајњи корисник уколико жели да та информација такође буде уписана у клијентски сертификат. Такође потребно је одредити одговарајући хешинг алгоритам и период важења сертификата.

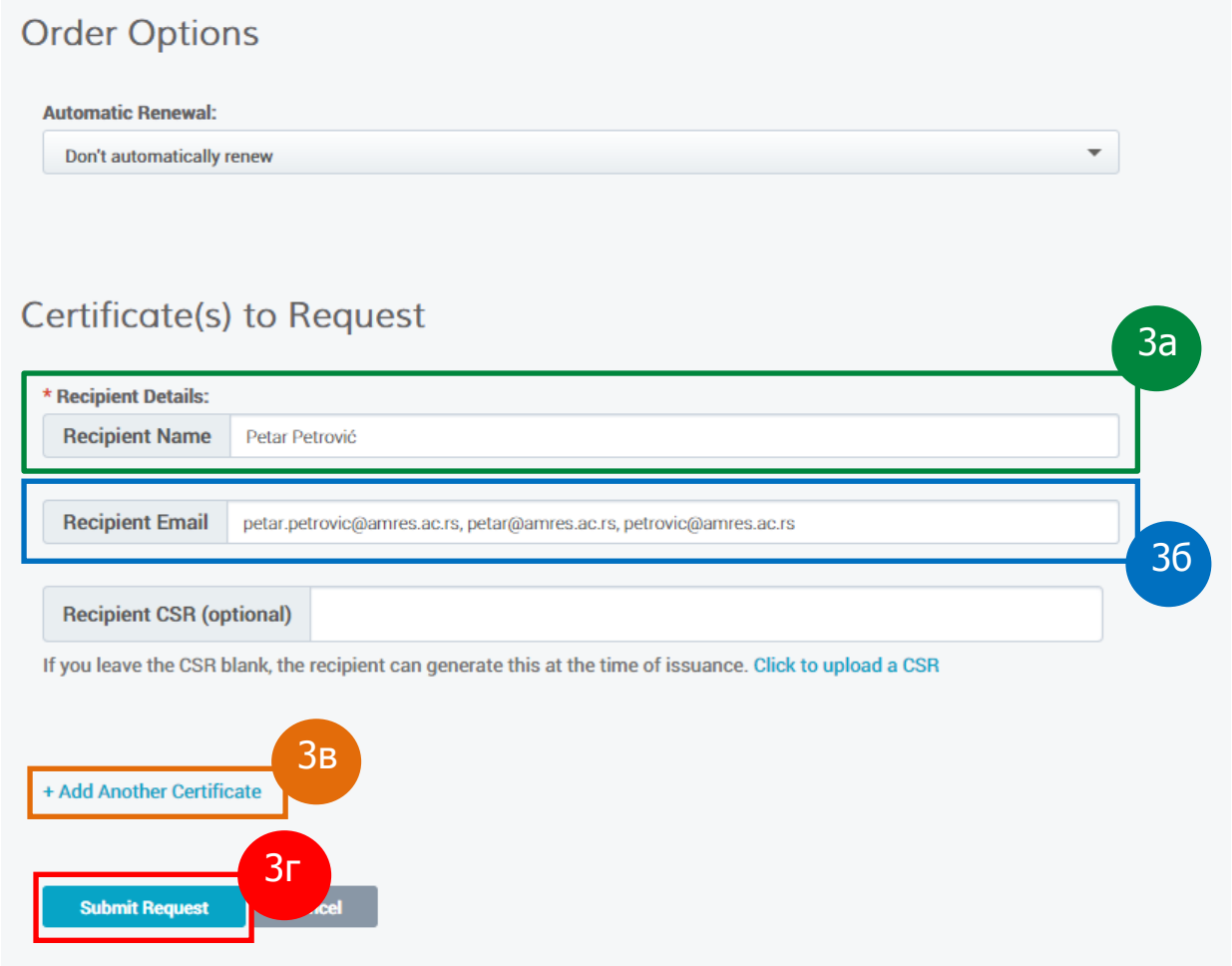


Слика 33

У доњем делу формулара администратор може одабрати да ли ће се за посматрани сертификат вршити аутоматска обнова. У делу „Certificates to Request", администратор у поље „Recipient Name" (3а) треба да упише име и презиме крајњег корисника коме је клијентски сертификат намењен. У пољу „Recipient Email" (3б) потребно је уписати имејл адресе крајњег корисника за које се захтева клијентски сертификат. Уколико се за посматраног корисника региструје више имејл адреса у сертификату, потребно је да у овом пољу те адресе буду одвојене зарезом и знаком размака. Опционо, могуће је да администратор у поље „Recipient CSR (Optional)" упише CSR (захтев за сертификат) који је претходно генерисао корисник. Уколико администратор остави ово поље празно, CSR ће се аутоматски генерисати у Интернет прегледачу крајњег корисника у наредним корацима. Да би се омогућио једноставнији процес прибављања клијентских сертификата AMPEC препоручује да се поље „Recipient CSR (Optional)" остави празно.

На крају формулара налази се опција „+ Add Another Certificate" (3в) која омогућава администратору да креира захтеве за више клијенских сертификата одједном. Притиском на ову опцију, формулар ће се проширити за још једну секцију „Certificates to Request" у којој је могуће уписати податке за другог крајњег корисника и његов сертификат. Ова опција је нарочито корисна у ситуацијама у којима администратор жели да одједном генерише више захтева за различите кориснике.

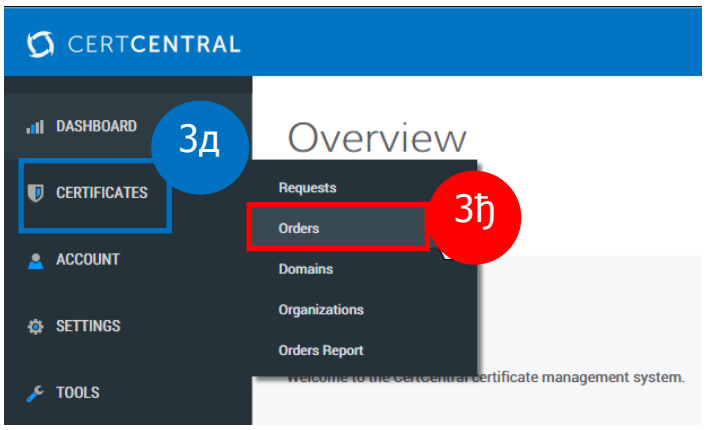
Након свих попуњених података потребно је притиснути дугме „Submit Request" (3г).



Слика 34

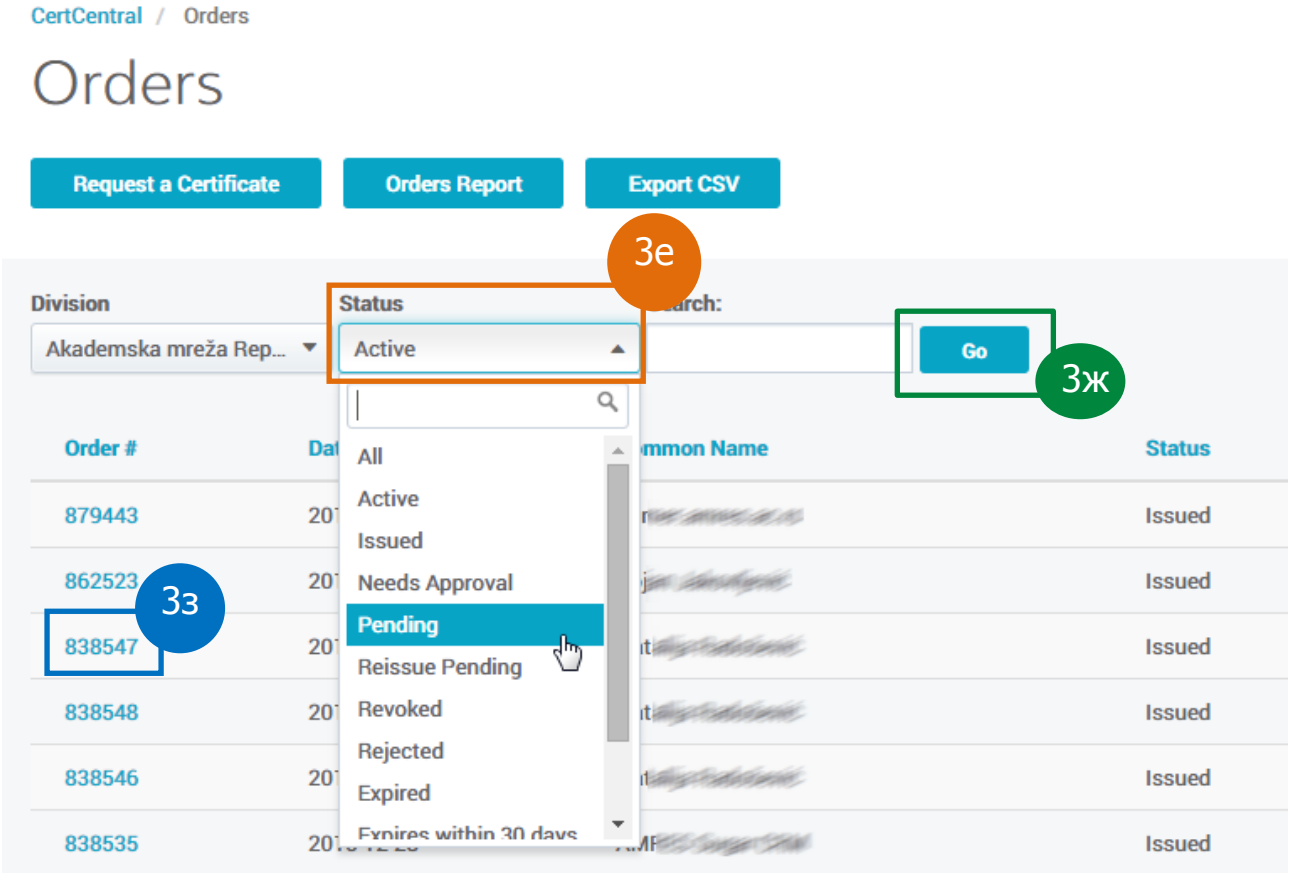
Закључно са овим кораком, администратор је завршио све своје обавезе у погледу издавања клијентског сертификата за крајњег корисника. Све даље кораке вршиће крајњи корисник коме је сертификат намењен.

Администратор може на порталу пратити статус свих захтева за клијентске сертификате. Неопходно је на порталу у левом менију одабрати „CERTIFICATES" (3д) а потом из падајућег менија опцију „Orders" (3ђ).

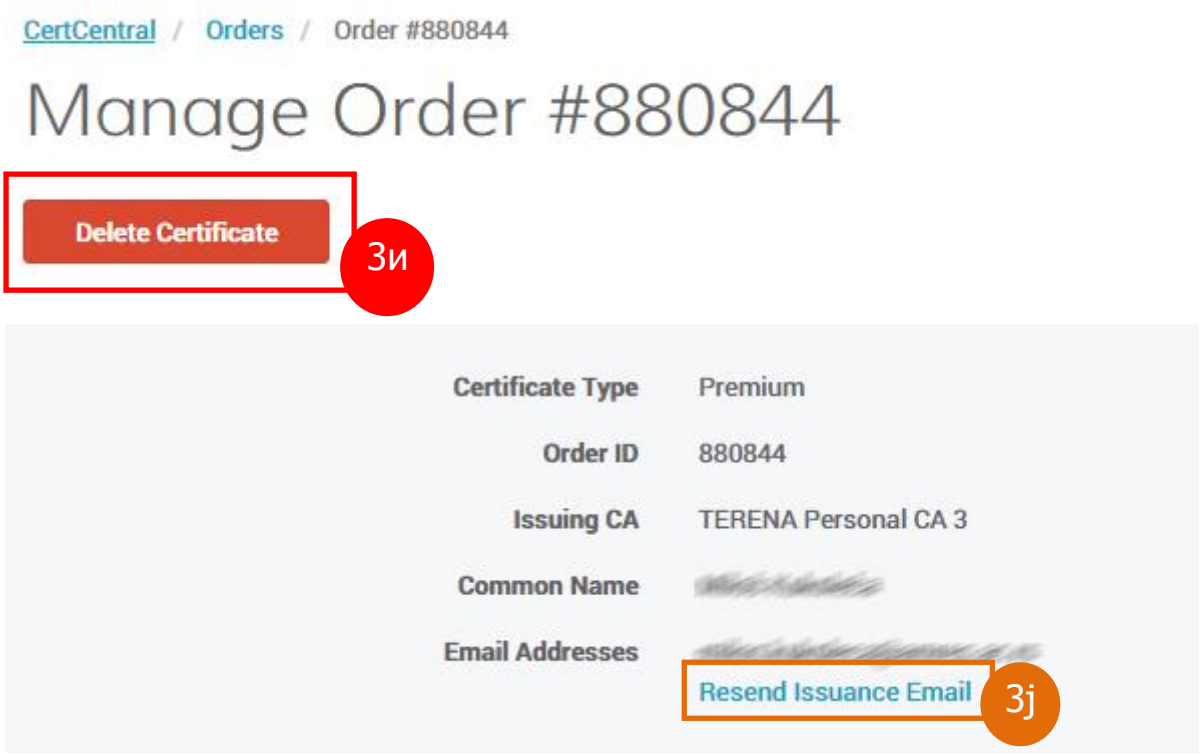


Слика 35

У новоотвореном прозору, потребно је у пољу „Status" (3е) из падајуће листе одабрати опцију „Pending", а потом притиснути дугме „Go" (3ж). Отвориће се нови прозор у коме ће се приказати листа свих поруџбина које чекају на реализацију. Међу тим поруџбинама се налазе и захтеви за клијентске сертификате који још нису комплетирани.



Кликом на број наруџбине (3з) са леве стране листе, долази се до детаљног описа захтеваног сертификата где је могуће обрисати поруџбину кликом на дугме „Delete Certificate" (3и).

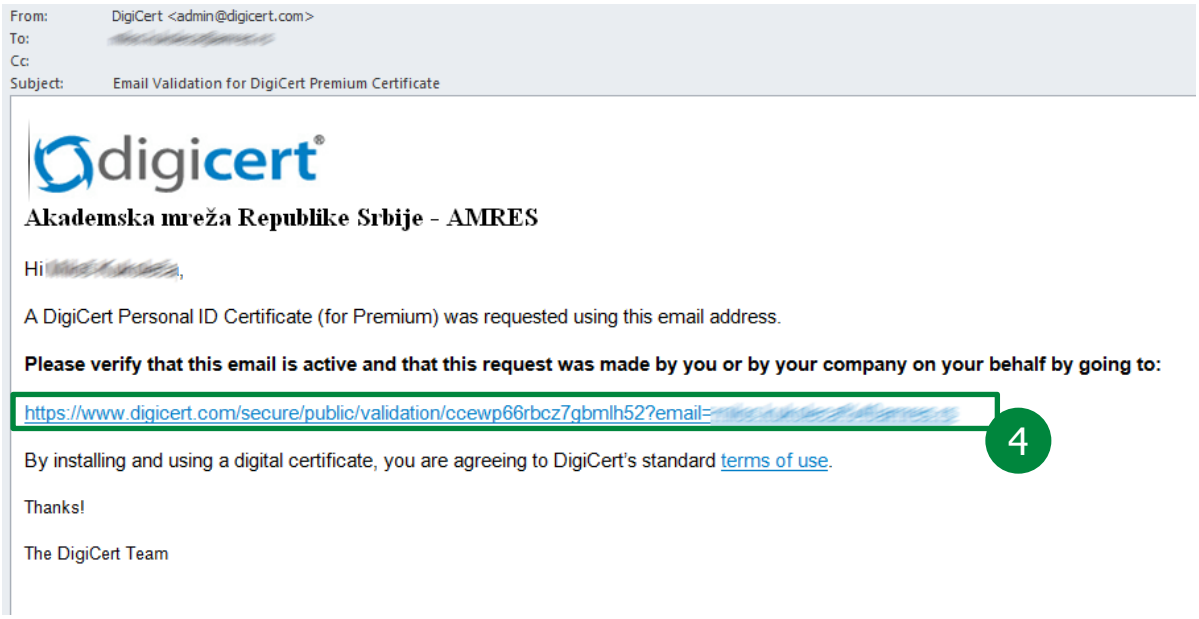


Слика 36

Кликом на дугме „Resend Issuance Email" (3j) кориснику ће поново бити послат имејл у коме се позива да приступи генерисању клијентског сертификата на основу захтева администратора.

КОРАК 4

Након што администратор поднесе захтев за прибављање клијентског сертификата, крајњем кориснику за кога је захтев послат пристићи ће имејл у коме DigiCert врши проверу да ли крајњи корисник заиста има контролу над имејл адресом која је наведена у захтеву за клијентским сертификатом.



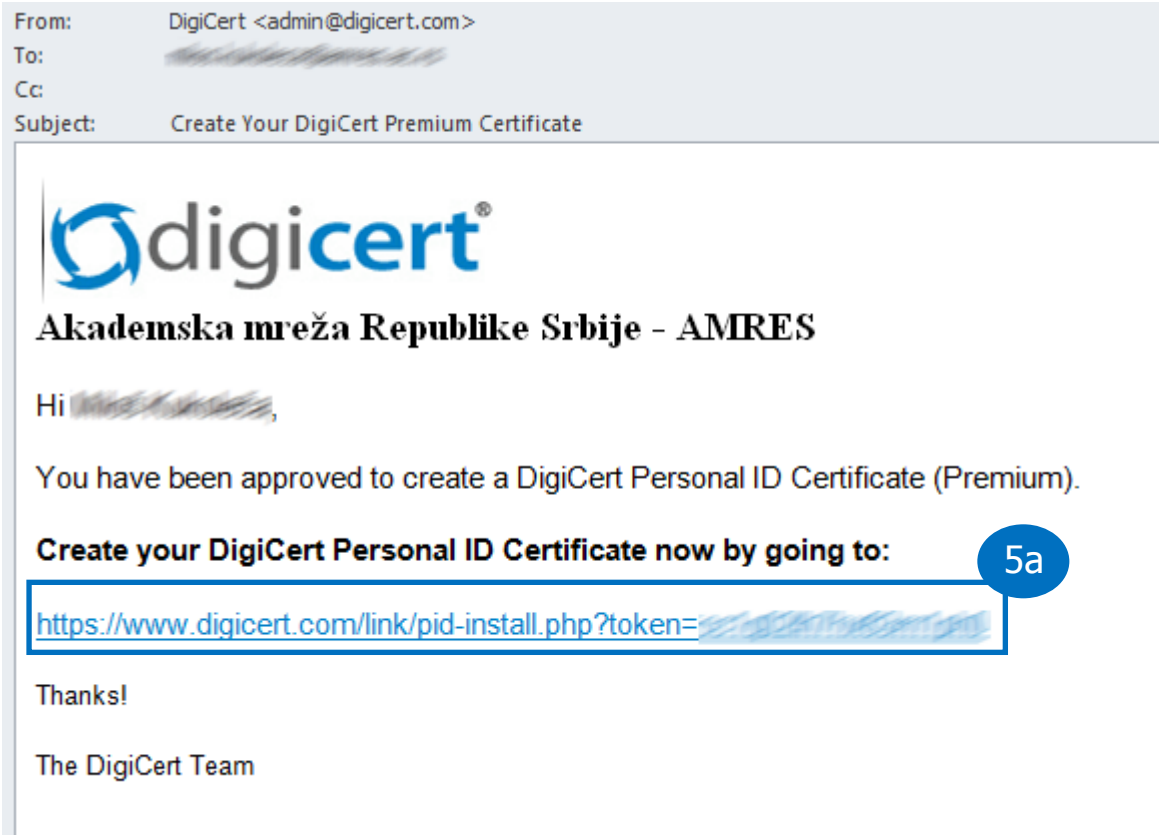
Слика 37

Кликом на приложени линк у имејл поруци (4), крајњи корисник ће бити преусмерен на DigiCert страницу која верификује да крајњи корисник заиста контролише пријављену имејл адресу.

Крајњи корисник ће за сваку имејл адресу наведену у захтеву за клијентски сертификат добити имејл поруку којом се проверава контрола над наведеном имејл адресом. Тек након што корисник потврди контролу над сваком имејл адресом, могуће је приступити следећем кораку.

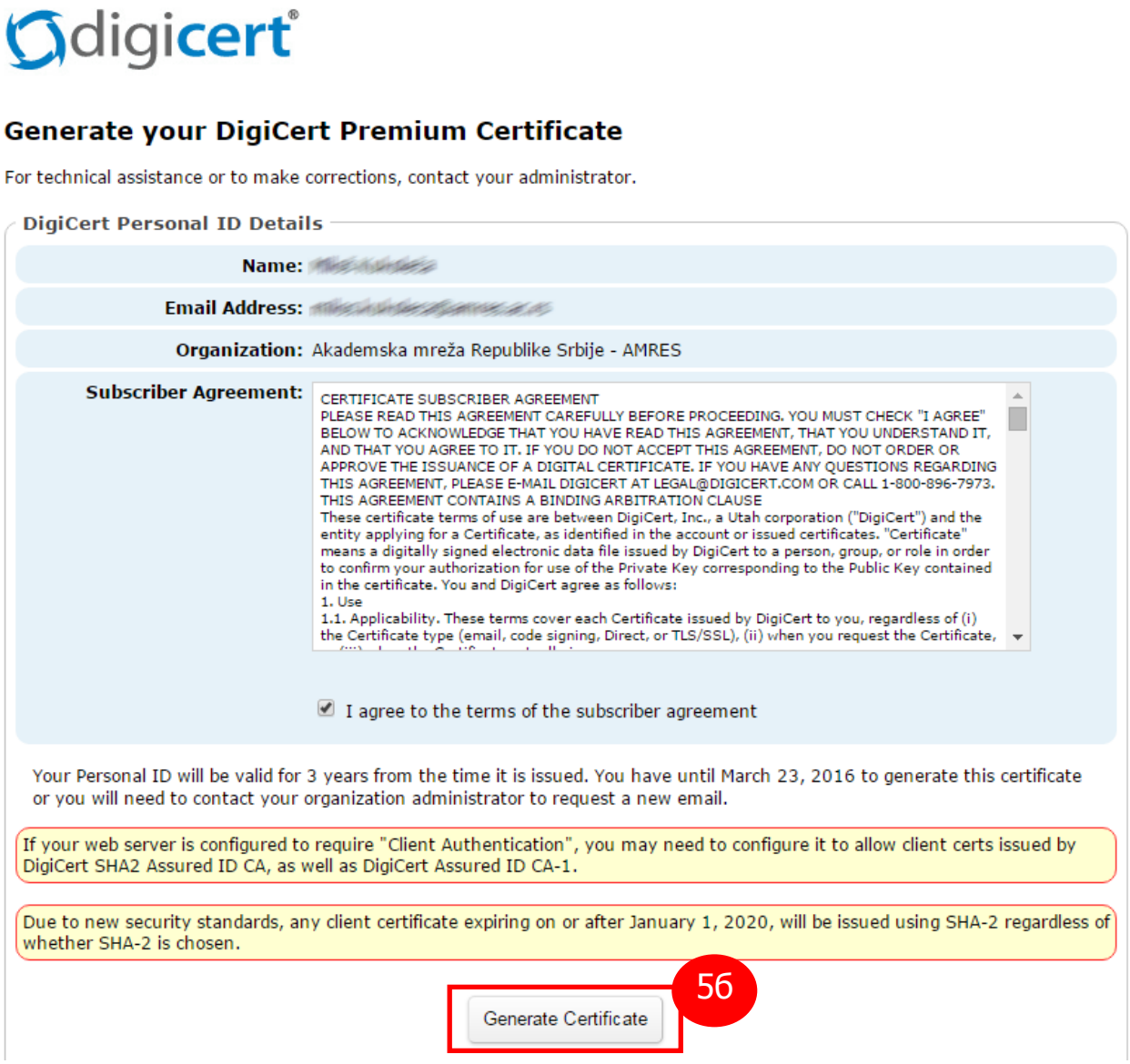
КОРАК 5

Након што крајњи корисник потврди контролу над свим имејл адресама које су наведене у захтеву за клијентски сертификат, на његову имејл адресу пристићи ће још један имејл од DigiCert провајдера у коме се крајњи корисник позива да генерише сертификат на порталу користећи линк (5а) приложен у телу имејл поруке.



Слика 38

Кликом на линк (5а) који је приложен у имејл поруци, крајњи корисник ће бити преусмерен на посебну страницу DigiCert портала. На поменутој страници потребно је да корисник провери све податке, потом потврди да је сагласан са условима под којима се клијентски сертификат издаје и користи и на крају притисне дугме „Generate Certificate" (5б).



Слика 39

Након притиска дугмета „Generate Certificate" у корисниковом Интернет прегледачу биће покренуте следеће акције:

1. Креираће се приватни кључ клијентског сертификата и тај кључ ће бити смештен у локалну базу кључева (*Keystore*). Локална база кључева може бити база оперативног система (нпр. Windows, Linux, OS X) или база Интернета прегледача (нпр. Mozilla Firefox). У коју локалну базу кључева ће приватни кључ бити смештен зависи од Интернет прегледача који крајњи корисник користи приликом приступања страници за генерисање сертификата.
2. Креираће се јавни кључ клијентског сертификата и .CSR фајл који представља захтев за издавање клијентског сертификата. Јавни кључ клијентског сертификата биће укључен у .CSR фајл.
3. .CSR фајл ће аутоматски у позадини бити послат DigiCert порталу.
4. DigiCert портал ће у року од пар секунди обрадити захтев и креирати клијентски сертификат који ће бити послат Интернет прегледачу крајњег корисника.

5. Клијентски сертификат ће бити примљен у Интернет прегледачу и сачуван у локалној бази кључева. Порука о томе ће бити исписана у Интернет прегледачу.

Након што клијентски сертификат буде сачуван односно инсталиран у локалну базу кључева, крајњи корисник може да користи клијентски сертификат у свакодневном раду. За те потребе у локалној бази кључева налазе се приватни кључ клијентског сертификата креиран под тачком 1 и јавни кључ у клијентском сертификату који је примљен у тачки 5.

Више информација о локалној бази кључева, различитим Интернет прегледачима и подешавању клијентског сертификата у имејл клијентима можете пронаћи на AMPEC веб-страници која се бави темом коришћења клијентских сертификата.

3 Закључак

Администратори AMPEC корисника у TCS сервису могу захтевати неограничен број сертификата за потребе своје институције и својих крајњих корисника. Након валидације организације и валидације домена, издавање сертификата преко TCS портала је веома брзо и једноставно.

Приликом издавања клијентских сертификата, администраторима се препоручује да сертификате издају само особама чији је идентитет потврђен и које су у радном односу на институцији или имају статус студента.