Р Е П У Б Л И К А Б Ъ Л Г А Р И Я
ДЪРЖАВНА АГЕНЦИЯ „ЕЛЕКТРОННО УПРАВЛЕНИЕ“

СИСТЕМА ЗА ЕЛЕКТРОНЕН ОБМЕН НА СЪОБЩЕНИЯ (СЕОС)

ПРОЦЕДУРА ЗА ГЕНЕРИРАНЕ И ИЗДАВАНЕ НА ТРАНСПОРТЕН СЕРТИФИКАТ

ВЕРСИЯ 1.1, МАРТ-МАЙ 2017

I. ВЪВЕДЕНИЕ

Настоящият документ описва процедурата по генериране и издаване на транспортен сертификат за целите на електронния обмен на съобщения.

II. ПОПЪЛВАНЕ НА БЛАНКА ЗА РЕГИСТРАЦЯ ЗА ИЗДАВАНЕ НА ТРАНСПОРТЕН СЕРТИФИКАТ

Попълва се Приложение 1. *Бланка за издаване на транспортен сертификат*.

За примерни данни може да се използва Приложение 2. *Примерна бланка за издаване на транспортен сертификат.*

III. ГЕНЕРИРАНЕ НА КЛЮЧОВА ДВОЙКА И ЗАЯВКА ЗА ИЗДАВАНЕ ТРАНСПОРТЕН СЕРТИФИКАТ С ПОМОЩТА НА OpenSSL

1. Инсталиране на OpenSSL

При Linux-базирани операционни системи, това може да стане, като използвате инструментите за управление на пакетите на съответната дистрибуция или от изходен код. Процедурата е тествана с версия 1.0.2g.

При Windows-базирани операционни системи, това може да стане, като изтеглите и инсталирате последния компилиран дистрибутив. Процедурата е тествана с версия 1.1.0 e.

2. Стартиране на OpenSSL

При Linux-базирани операционни системи, след като OpenSSL вече е инсталиран, стартирането става с командата: `openssl`

При Windows-базирани операционни системи, от директорията "*bin*" на разархивирания дистрибутив се стартира "*openssl.exe*". В резултат на това се отваря конзолата за изпълнение на команди на OpenSSL. Подканването в конзолата е с префикса "OpenSSL> ".

3. Генериране на файл, който ще съдържа частния ключ

Генерирането на RSA двойка публичен/частен ключ се извършва с командатата: `genrsa -out file.key 2048`

, където:

- *file.key* – наименование на файла съдържащ частния ключ;
- *2048* - брой битове, от които се състои ключа.

Примерен изход от изпълнението на командата:

```
OpenSSL> genrsa -out file.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................................
+++
.......+++
e is 65537 (0x10001)
```

4. Генериране на заявка за издаване на сертификат

Генерирането на заявка за издаване на сертификат на базата на генерирания частен ключ: `req -new -key file.key -out file.csr`

, където:

- *file.key* – наименование на файла съдържащ частния ключ (генериран от предходната стъпка);
- *file.csr* – наименование на файла съдържащ заявката за издаване на сертификат.

По време на изпълнението на командата, последователно се въвеждат данните от попълнената бланка за регистрация за полетата:

Поле	Описание	Пример
Country Name (2 letter code)	двубуквен код на държавата на латиница	BG
State or Province Name (full name)	ЕИК/БУЛСТАТ на организацията префиксиран с "B:"	B:000695025
Locality Name (eg. city)	населено място на латиница	Sofia
Organization Name (eg. company)	наименование на организацията на латиница	Administratsiya X
Organizational Unit Name (eg. section)	наименование на звено	Administrative Office
Common Name (eg. YOUR name)	наименование на хоста за комуникация[1]	administratsiyaX.obmen.local
Email Address	имейл адрес за контакт	obmen@administratsiyaX.bg

Всички останали полета могат да бъдат оставени празни.

[1] Наименованието на хоста трябва да съответства на частта с наименованието на хоста, на който ще бъде публикувана уеб услугата за комуникация. Например, ако услугата ще бъде публикувана на адрес https://administratsiyaX.obmen.local:8443/, то наименованието на хоста следва да бъде"*administratsiyaX.obmen.local*".

Примерен изход от изпълнението на командата:

```
OpenSSL> req -new -key file.key -out file.csr
You are about to be asked to enter information that will be incorpo
rated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BG
State or Province Name (full name) [Some-State]:B:000695025
Locality Name (eg, city) []:Sofia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Administ
ratsiya X
Organizational Unit Name (eg, section) []:Administrative Office
Common Name (e.g. server FQDN or YOUR name) []:administratsiyaX.obm
en.local
Email Address []:obmen@administratsiyaX.bg

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

5. Изпращане на заявката за издаване на сертификат

Попълнената бланка от предходната глава заедно с генерираната в т.3 заявка за издаване на сертификат (файла "*file.csr*") се изпращат по електронната поща на адрес cert-req@e-gov.bg

6. Издаване на транспортен сертификат

Доставчикът на удостоверителни услуги проверява дали данните от попълнената бланка и генерираната заявка съвпадат.

Ако данните не съвпадат, дотавчикът има право да откаже издаване на транспортен сертификат.

Ако данните съвпадат, доставчикът издава транспортен сертификат и го изпраща по електронна поща обратно на администратора

7. Експортиране на сертификата във формат за инсталиране

Доставчикът на удостоверителни услуги изпраща транспортния сертификат под формата на X.509 сертификат във файл с разширение "*.cer*".

За да може да бъде инсталиран, сертификатът трябва да бъде обединен с частния ключ от т.1 в PKCS#12 хранилище във файл с разширение "*.p12*".

Това може да стане с командата: `pkcs12 -export -in file.cer -out file.p12 -inkey file.key`

, където:

– *file.cer* – наименование на файла съдържащ издадения в т.5 транспортен сертификат, получен от доставчика на удостоверителни услуги;
– *file.p12* – наименование на файла съдържащ транспортния сертификат и неговия частен ключ, готови за инсталиране;
– *file.key* – наименование на файла съдържащ частния ключ генериран в т.2.

По време на изпълнението на командата се въвежда парола за защита на генерирания "*.p12*" файл.

Примерен изход от изпълнението на командата:

```
OpenSSL> pkcs12 -export -in file.cer -out file.p12 -inkey file.key
Enter Export Password:
Verifying - Enter Export Password:
```

IV. КОНТАКТ

За допълнителни въпроси на имейл: cert-req@e-gov.bg

V. ПРИЛОЖЕНИЯ

Приложение 1. *Бланка за издаване на транспортен сертификат*

Наименование	Данни включени в съдържанието на удостоверението
Канонично име на сървър/**Common Name**[2]	
Наименование на организация/**Organization**[3]	
ЕИК/Булстат/**State of Province**[4]	
Име на град/**Locality**	
Име на държавата/**Country**	
Дата	

Вж. приложения файл registration_edoc_blank.xls.

Приложение 2. *Примерна бланка за издаване на транспортен сертификат*

Наименование	Данни включени в съдържанието на удостоверението
Канонично име на сървър/**Common Name**[5]	administratsiyaX.obmen.local
Наименование на организация/**Organization**[6]	Administratsiya X

2 Вписва се точният адрес на системата.
3 Възможно е изписване по два начина: а) Транслитерация според Закона за транслитерацията или б) Английски език
4 Изписва се (9 или 13 цифрен) ЕИК/БУЛСТАТ на съответната организацията.
5 Вписва се точният адрес на системата, който е предварително определен от ДАЕУ.
6 Възможно е изписване по два начина: а) Транслитерация според Закона за транслитерацията или б) Английски език

ЕИК/Булстат/**State of Province**[7]	000695025
Име на град/**Locality**	Sofia
Име на държавата/**Country**	BG
Дата	31.03.2017

Вж. приложения файл registration_edoc_example.xls.

[7] Изписва се (9 или 13 цифрен) ЕИК/БУЛСТАТ на съответната организацията.