

## Инструкция по оформлению запросов на продление сертификатов в электронной форме.

Для удаленного продления действия сертификата ключа проверки электронной подписи воспользуйтесь web-интерфейсом АРМ Пользователя Удостоверяющего Центра (далее – УЦ) по адресу <https://ra.cap.ru/ui/user/user.asp>.

В процессе формирования запроса производится генерация ключевой информации на носитель. Носитель ключевой информации (ключевой носитель) должен быть вставлен в компьютер.

Запрос формируется с использованием АРМ пользователя по ссылке **Новый сертификат**.

- в графе Шаблон сертификата выбрать назначение сертификата, для справки по этому пункту позвоните специалисту;
- галку «Включить усиленную защиту закрытого ключа» ставить необязательно;
- в поле «Информация» заполняется справочная информация для оператора УЦ;
- для сохранения запроса поставьте галку «Сохранить в файл».

После нажатия кнопки **Отправить** система перейдет к процедуре формирования новых ключей:

- выберите необходимый тип ключевого носителя из списка подключенных в СКЗИ КриптоПро CSP;
- проинициализируйте генератор случайных чисел (путем нажатия клавиш на клавиатуре или движением указателя мышки в окне инициализации);
- при необходимости установите пароль (ПИН-код) на создаваемый ключевой контейнер;
- в результате успешного выполнения вышеперечисленных действий сформированный запрос будет отправлен оператору УЦ на рассмотрение, а в таблице запросов на сертификат появится новая строка со статусом запроса **Обработка**;

После этого оператору УЦ необходимо направить по электронной почте подписанные заявление и запрос на изготовление сертификата ключа проверки электронной действующими ключами электронной подписи Пользователя УЦ или уполномоченного представителя юридического лица с использованием приложения КриптоАРМ) или с помощью утилиты csptest.exe - в командной строке выполнить:

```
csptest.exe -sfsign -sign -add -base64 -in test.doc -out test.doc.sig -my test@cap.ru
путь до приложения                путь до вх. Файла    путь для выходного    эл.почта подписи
```

Если установлено несколько сертификатов, утилита предложит выбрать сертификат, на основе которого будет формироваться электронная подпись файла

```
O:\temp>csptest.exe -sfsign -sign -add -base64 -in pp.doc -out pp.doc.sig -my info4@cap.ru
#0:
Subject: CN=info4@cap.ru
Valid : 11.03.2015 03:24:20 - 07.09.2015 03:24:20 (UTC)
Issuer : CN=Communications Server
#1:
Subject: СНИЛС=00911420904, ОГРН=1122130008791, ИНН=002130106185, E=info4@cap.ru, C=RU, S=21
спублики, OU=Сектор сопровождения деятельности удостоверяющего центра, CN=Мининформполитики
Valid : 10.04.2015 15:48:00 - 10.04.2016 15:58:00 (UTC)
Issuer : ОГРН=1122130008791, ИНН=002130106185, STREET=Президентский бульвар д.10, E=certadm
PrivKey: 10.04.2015 15:48:00 - 10.04.2016 15:48:00 (UTC)
#2:
Subject: DC=ru, DC=cap, OU=Мининформполитики Чувашии, CN=Мининформ ЧР Алексей И. Ишалев, E=
Valid : 22.12.2014 12:33:55 - 22.12.2015 12:33:55 (UTC)
Issuer : DC=ru, DC=cap, CN=CAP root CA

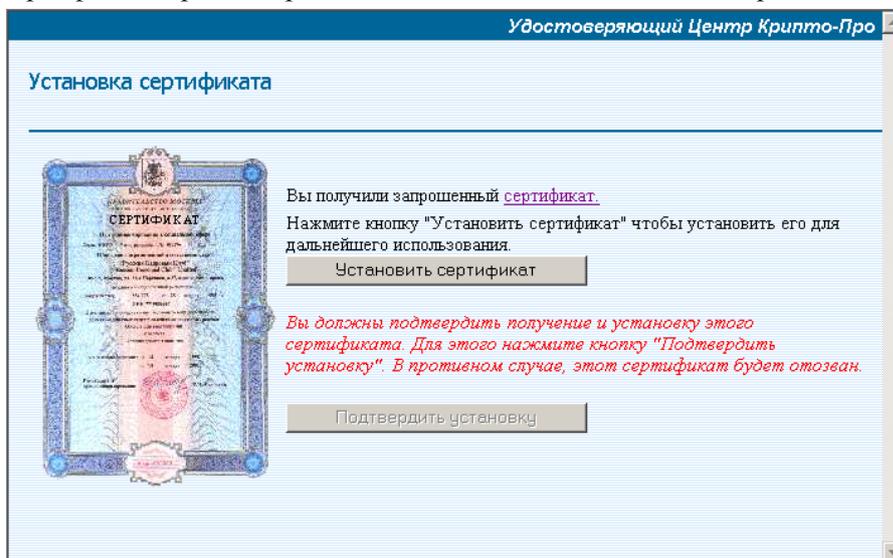
Enter certificate number:
1
A CSP has been acquired.
Source message length: 1
Calculated signature (or signed message) length: 3812
Signature was done. Signature (or signed message) length: 3796
Output file (pp.doc.sig) has been saved
Total: SYS: 0,047 sec USR: 0,000 sec UTC: 65,983 sec
[ErrorCode: 0x00000000]
```

По окончании работы утилиты, в случае отсутствия ошибок, будет сформирован выходной файл с расширением .sig, содержащий электронную подпись.

В срок не позднее 3 (трех) рабочих дней следующих за рабочим днем, в течение которого было получено заявление на изготовление сертификата, запрос будет рассмотрен и после проверки электронной подписи заявления и запроса на изготовление сертификата Пользователя УЦ, Оператор УЦ осуществляет изготовление и предоставление Пользователю УЦ сертификата ключа проверки электронной подписи.

При принятии и подтверждения запроса на сертификат, его статус меняется на состояние **Установить**. Далее для установки сертификата в хранилище сертификатов, выполните следующие действия:

- нажмите ссылку **Установить** в соответствующей строке таблицы запросов на сертификат. При этом рабочая область АРМ пользователя примет следующий вид:



- в появившейся форме убедитесь в соответствии полученного сертификата отправленному запросу. Для этого нажмите на ссылку сертификат данного окна;
- для продолжения установки сертификата нажмите кнопку **Установить сертификат**;
- при успешной установке данного сертификата появится соответствующее сообщение;
- для подтверждения факта установки и сообщения об этом оператору УЦ нажмите кнопку **Подтвердить установку**. В случае не подтверждения установки сертификат будет занесен в список отозванных сертификатов.

До истечения 10 (десяти) календарных дней с момента получения уведомления об изготовлении сертификата Пользователь УЦ должен подписать и предоставить в Удостоверяющий центр копию сертификата ключа проверки электронной подписи.