Оглавление

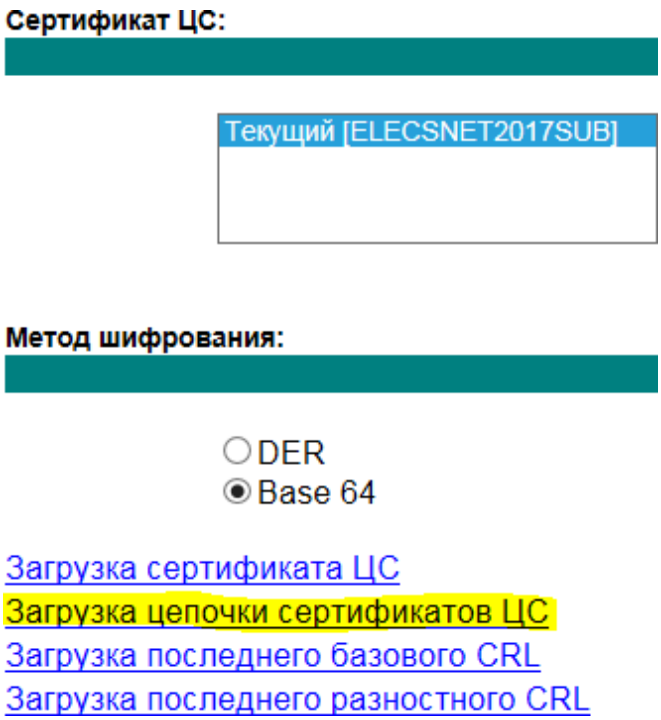
Инструкция по получению и установке сертификатов для доступа к тестовой и боевой среде Элекснет

Для доступа к боевой/тестовой среде надо получить и установить корневой сертификат Центра сертификации Элекснет и клиентский сертификат.
1.Для установки корневого сертификата Центра Сертификации Элекснет
набрать адрес (использовать только Internet Explorer версия не ниже 6 но не выше 9 в случае если Ваша версия выше, для начала необходимо синхронизировать Вашу версию браузера с 9 версией):

https://91.225.194.47/certsrv - для боевых
https://91.225.194.108/certsrv - для тестовых

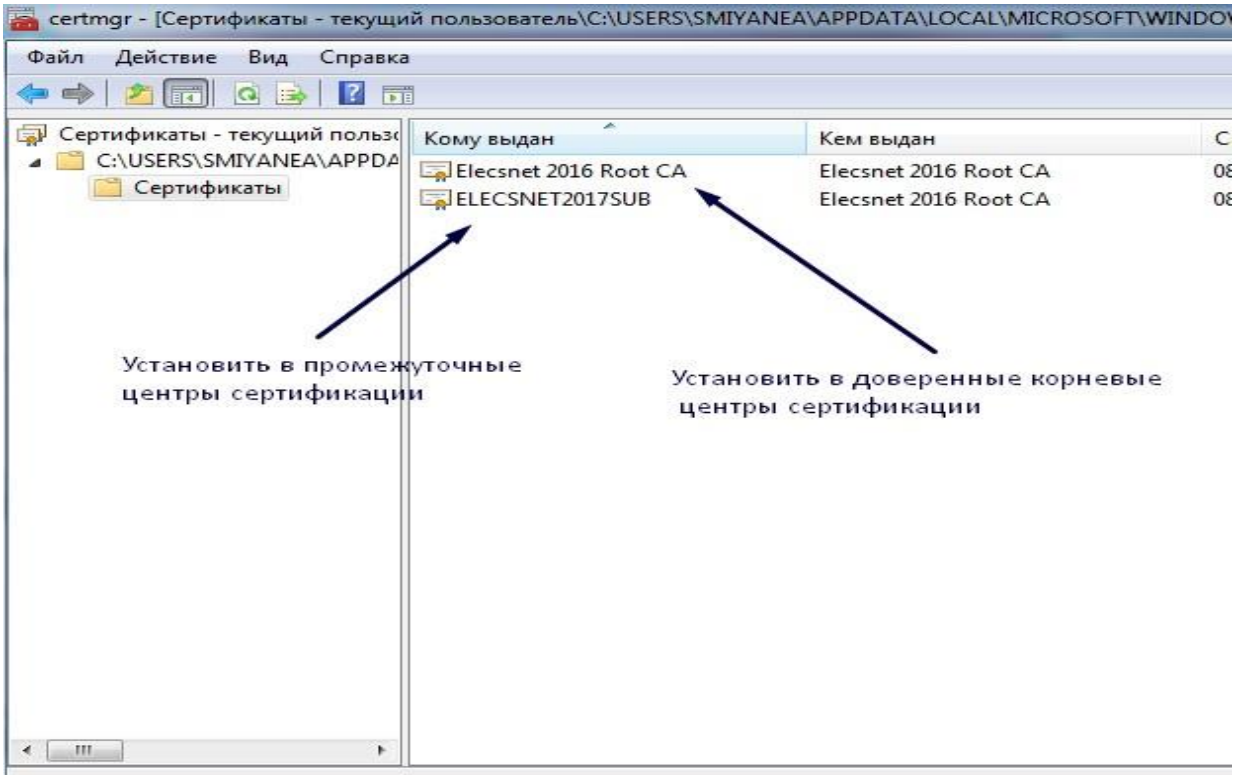
На открывшейся странице приветствия выбрать действие:
Загрузка сертификата ЦС, цепочки сертификатов или CRL

На странице загрузки сертификата ЦС, выбрать метод шифрования **Base 64**
и **Загрузка цепочки сертификатов ЦС**



В окне загрузки файла выберите **Открыть**

Далее, установить сертификат **Elecsnet 2016 Root CA**, поместив его в хранилище **Доверенные корневые центры сертификации. ELECSNET2017SUB** в **Промежуточные центры сертификации.**
(На тестовом будет один сертификат, его установить в Доверенные корневые центры сертификации)



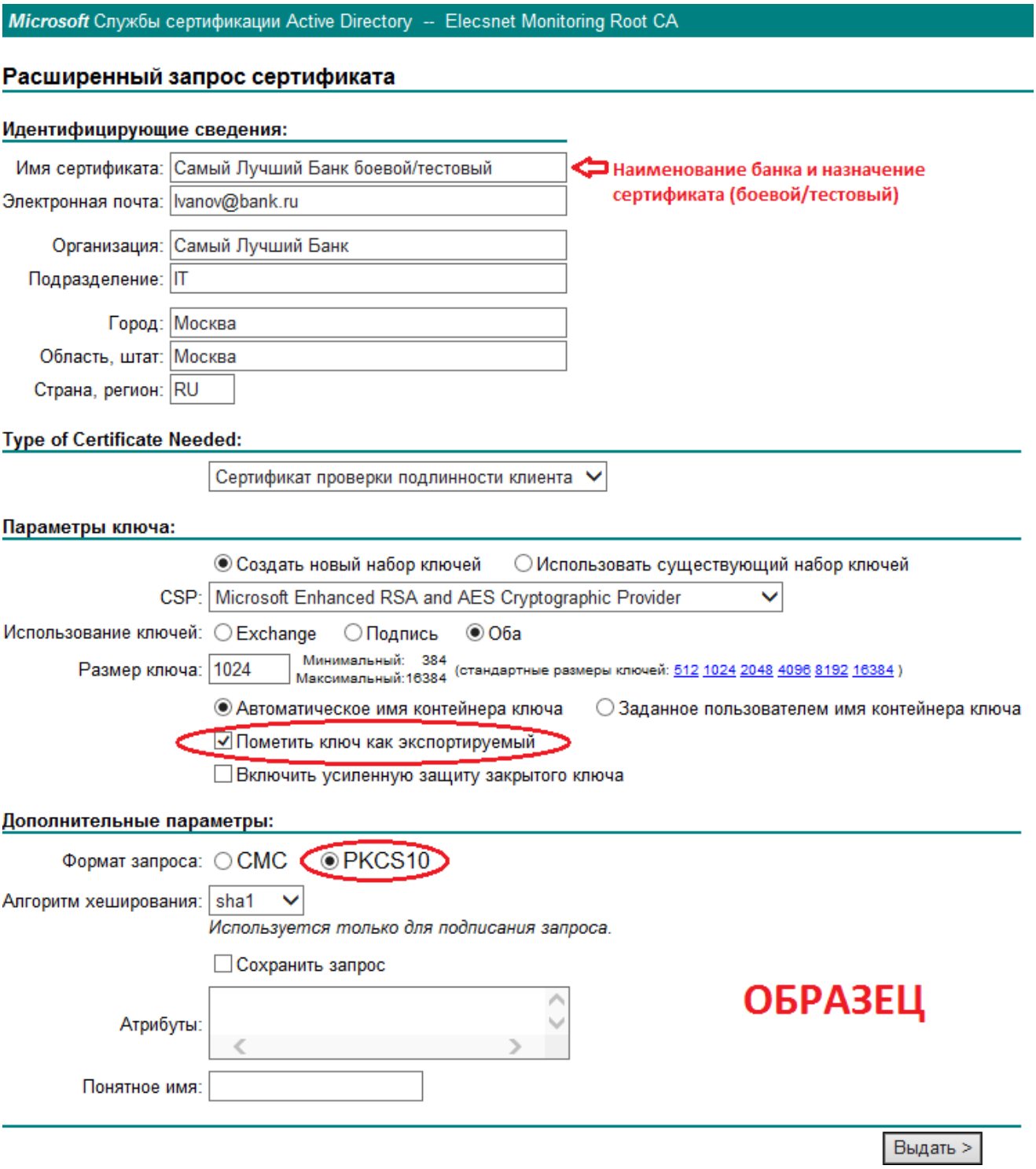
2. Далее, для доступа к боевой/тестовой среде необходимо получить персональный клиентский сертификат.

Сначала сделайте запрос сертификата.

Для этого набрать в Internet Explorer адрес https://91.225.194.47/certsrv (https://91.225.194.108/certsrv для тестовых)

На открывшейся странице приветствия выбрать нужное действие **Запроса сертификата,** на следующей странице выбрать **Расширенный запрос сертификата** и затем **Создать и выдать запрос к этому ЦС.**

Откроется страница **Расширенный запрос сертификата**



Заполните **все** поля в разделе **Идентифицирующие сведения.**

В поле **Имя сертификата** укажите свои **Наименование банка и назначение сертификата (боевой/тестовый)** полностью. (В имени сертификата **не должно быть " - двойных кавычек**)

В поле **Подразделение** можно указать должность, подразделение, либо, для краткости, что-то одно.

В поле **электронная почты** необходимо указать почту сотрудника, которому будут приходить оповещение об окончании срока действия сертификата (при необходимости вы можете указать несколько e-mail адресов через запятую)

Старайтесь избегать слишком длинных наименований. Поля заполняйте кириллицей, за исключением электронной почты и страны (RU).

В разделе **Параметры ключа** по желанию можно поставить галочку **Пометить ключ как экспортируемый.** Это позволит при необходимости экспортировать сертификат с приватным

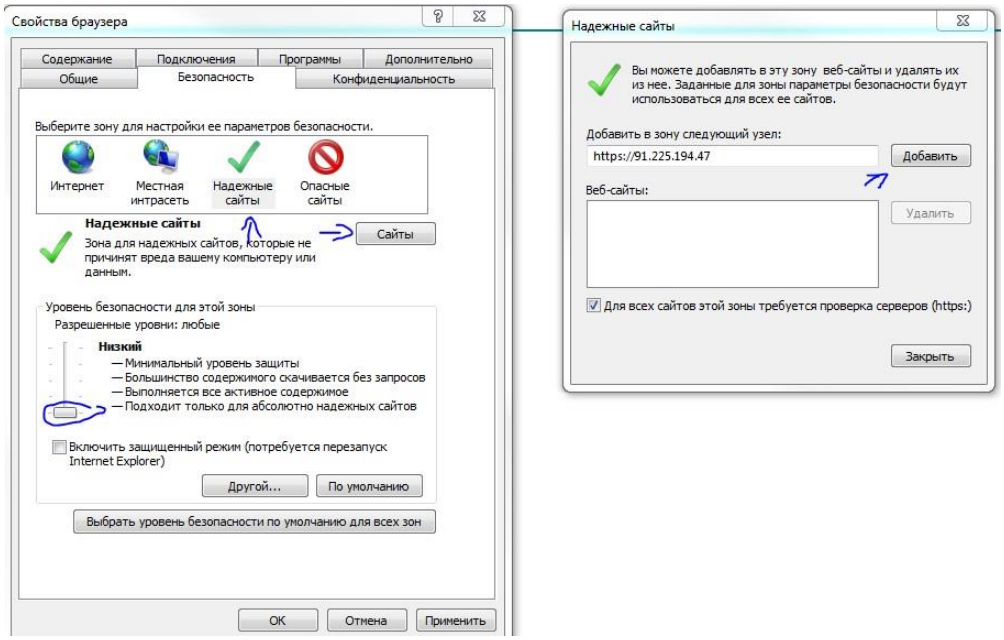
ключом на другой компьютер, однако понизит безопасность хранения сертификата.
В разделе **Дополнительные параметры** выбрать формат запроса **PKCS10.** Остальные параметры оставить без изменений. После заполнения формы нажать кнопку **Выдать.** Далее ответить **Да** на предупредительное сообщение и Ваш запрос на сертификат будет получен центром сертификации.

В случае если при нажатии на «**Расширенный запрос сертификат»** , указанная на образце страница не открывается

Вам необходимо синхронизировать вашу версию Браузера с девятой.
В принципе Ваши админы вполне могут Вам в этом помочь.
В случае если это не так - вот что надо делать.
На открытой странице браузера .На этапе нажатия "Расширенный запрос сертификата" нажимаете "F12"
В нижней части браузера должно всплыть окно с настройками.
Тут есть 2 варианта (в зависимости от версии)
1) В левой части экрана высвечивается вертикальное меню с картинками.
Вам нужно самое нижнее- называется "Emulation" В данной форме Вам нужно в поле "Режим документов" во всплывающем меню выбрать "9" , а в поле "строка агента пользователя" выбрать "Enternet Explorer 9"
2) Формы с меню высвечиваются горизонтальным списком
Тогда Вам так же нужна сама последняя форма "Эмуляция" порядок действий соответствует пункту 1
3)Формы с меню высвечиваются горизонтальным списком.
Вам нужны две последние формы. "Режим браузера", при наведении на неё всплывет список ,выберете "Enternet Explorer 9" и "режим документов"при наведении на неё всплывет список ,выберете "Стандартный Enternet Explorer 9"

После этого нажмете "F12" ещё раз, чтобы убрать отладчик и перейдете на "Расширенный запрос сертификата" . Все должно получится, если после проделывания всех действий- ошибка не исправилась- просьба обратиться к своим админам для проверки прав на Вашем ПК. Вы можете не быть администраторам на своей машине, или какие-либо политики безопасности не позволяют Вам хранить настройки изменений в режиме браузера .

В случае если не грузится поле CSP добавьте адрес в надежные сайты и поставьте низкий уровень безопасности. После запроса сертификата можно будет вернуть обратно.



Затем Вам следует время от времени проверять статус запроса.
Для этого снова зайдите по ссылке https://91.225.194.47/certsrv (https://91.225.194.108/certsrv для тестовых), выберите нужное действие:
Просмотр состояния ожидаемого запроса сертификата.
Если запрос на сертификат ещё находится в ожидании, через некоторое время следует снова вернуться на этот веб-сайт для просмотра состояния. Сертификат будет выдан администратором после получения от менеджера Управления банковских программ заявки на выдачу сертификата и сверки её с запросом. Запрос хранится на сервере сертификации в течение 10 дней.
Если запрошенный Вами сертификат был Вам выдан, установите его. Выпущенный сертификат хранится на сервере 10 дней с момента выдачи его администратором, после чего автоматически удаляется. Если Вы не смогли, не успели установить сертификат в указанный срок,
Вам следует сделать новый запрос.

Ссылка на тестовую среду:
https://91.225.194.107/Payment/gateway.asmx

Ссылка на боевую среду:
https://services.elecsnet.ru/payment/gateway.asmx

Сертификат выдаётся строго на один год. Однако, в течение этого срока он может быть отозван администратором по причине компрометации ключа, компрометации Центра Сертификации, изменения принадлежности, замены сертификата, прекращения работы, либо действие сертификата может быть временно приостановлено.

По техническим вопросам обращайтесь:

Савина Евгения,
Заместитель начальника ОЭПЦ,
e-mail: savinaea@elecsnet.ru,
тел.(495) 662-15-00 доб. 636

Инструкция по получению и установке сертификатов для доступа к web-мониторингу Элекснет

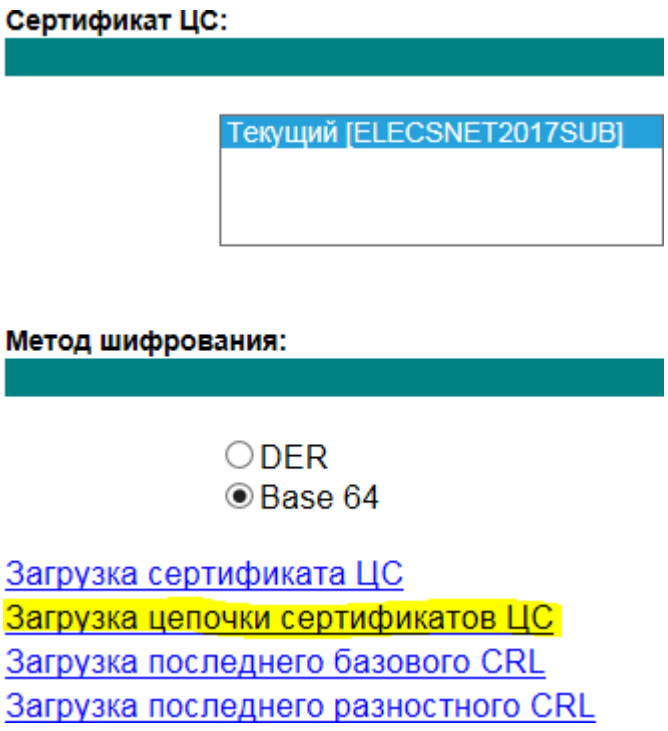
Для доступа к web-мониторингу надо получить и установить корневой сертификат Центра сертификации Элекснет и клиентский сертификат.

1. Для установки корневого сертификата Центра Сертификации Элекснет набрать в браузере адрес (использовать только Internet Explorer):

https://91.225.194.47/certsrv/

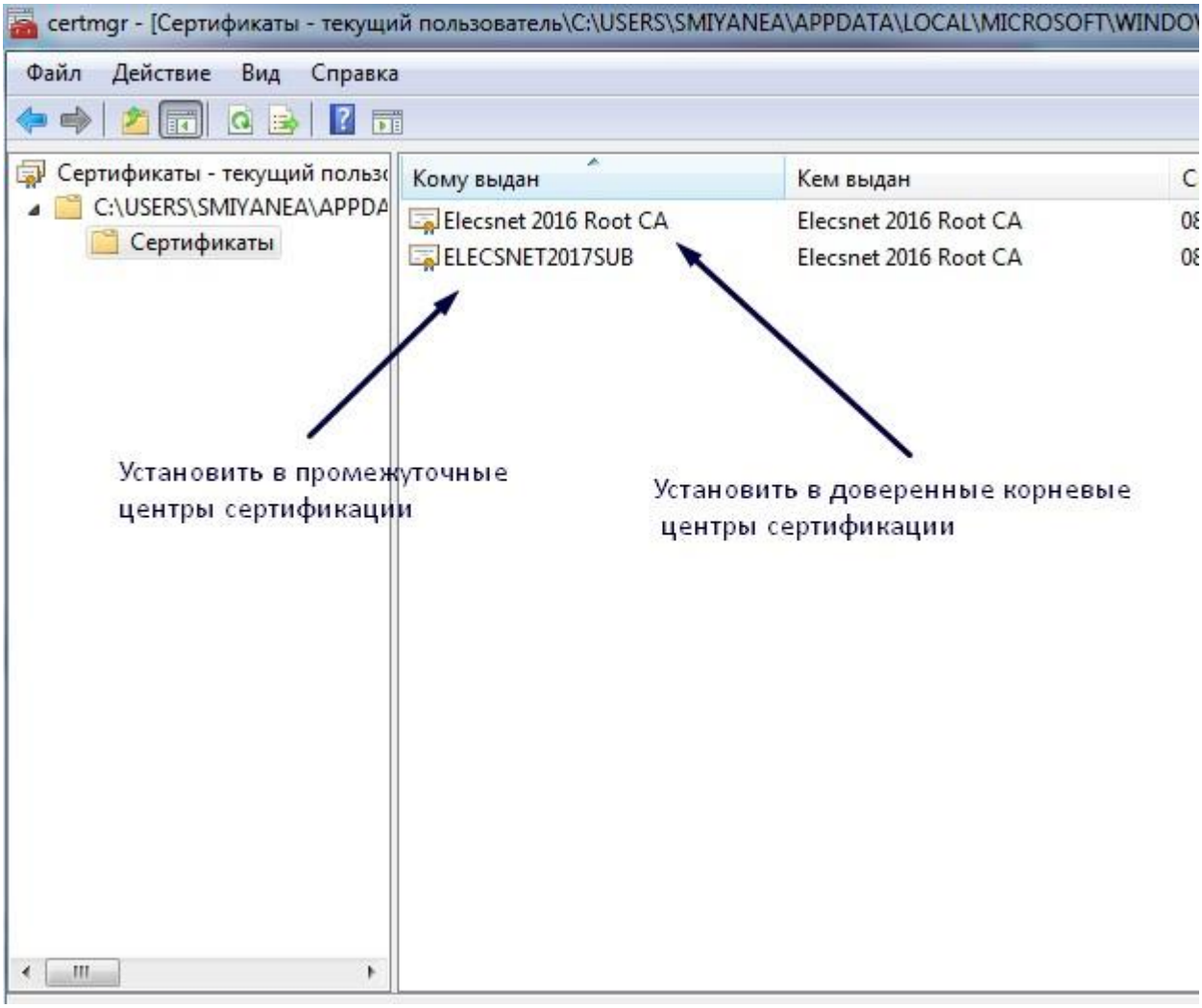
На открывшейся странице приветствия выбрать действие:
Загрузка сертификата ЦС, цепочки сертификатов или CRL

На странице загрузки сертификата ЦС, выбрать метод шифрования **Base 64**
и **Загрузка цепочки сертификатов ЦС**



В окне загрузки файла выберите **Открыть**

Далее, установить сертификат **Elecsnet 2016 Root CA**, поместив его в хранилище **Доверенные корневые центры сертификации. ELECSNET2017SUB** в **Промежуточные центры сертификации.**



2. Далее, для доступа к web-мониторингу необходимо получить персональный клиентский сертификат.

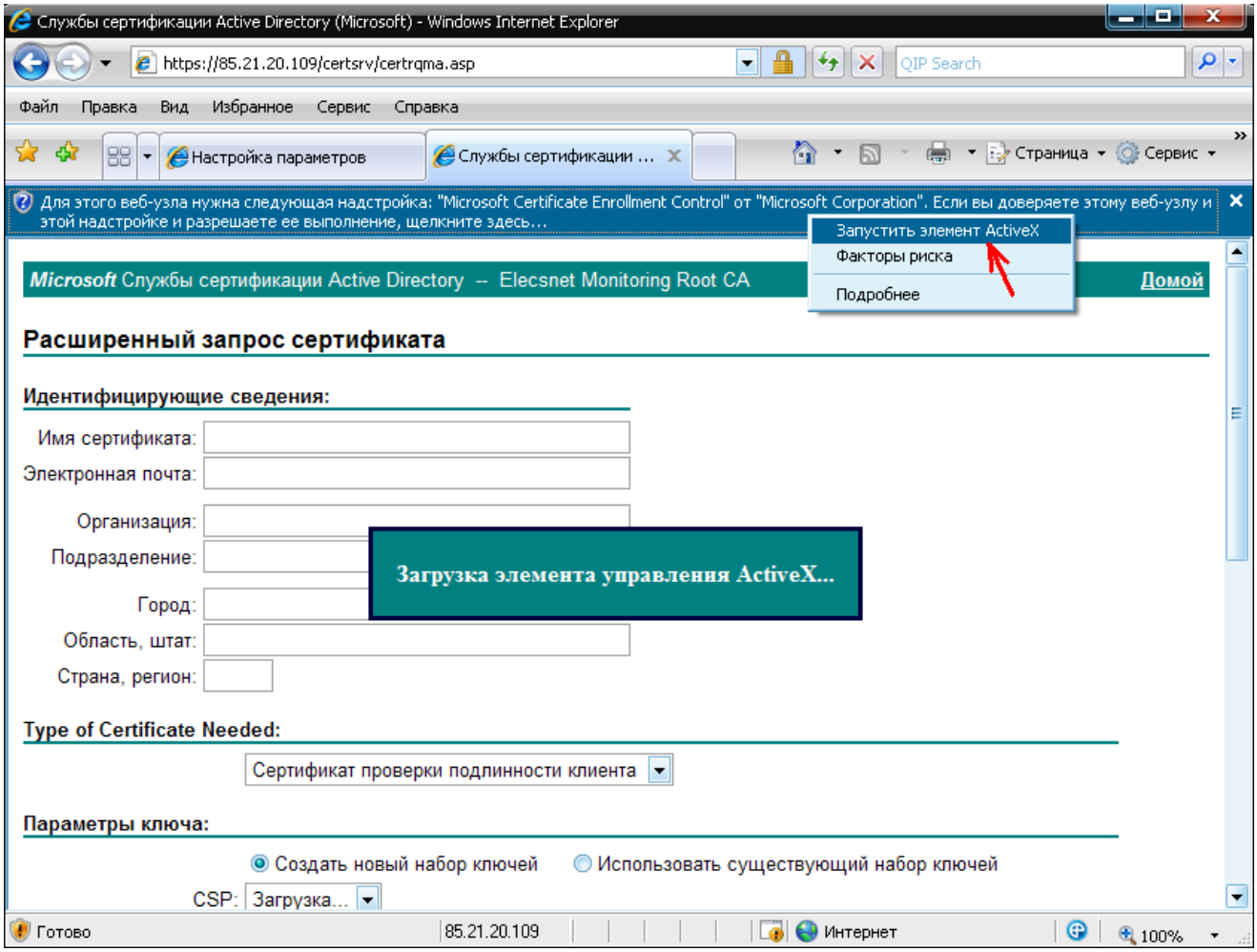
Сначала сделайте запрос сертификата.

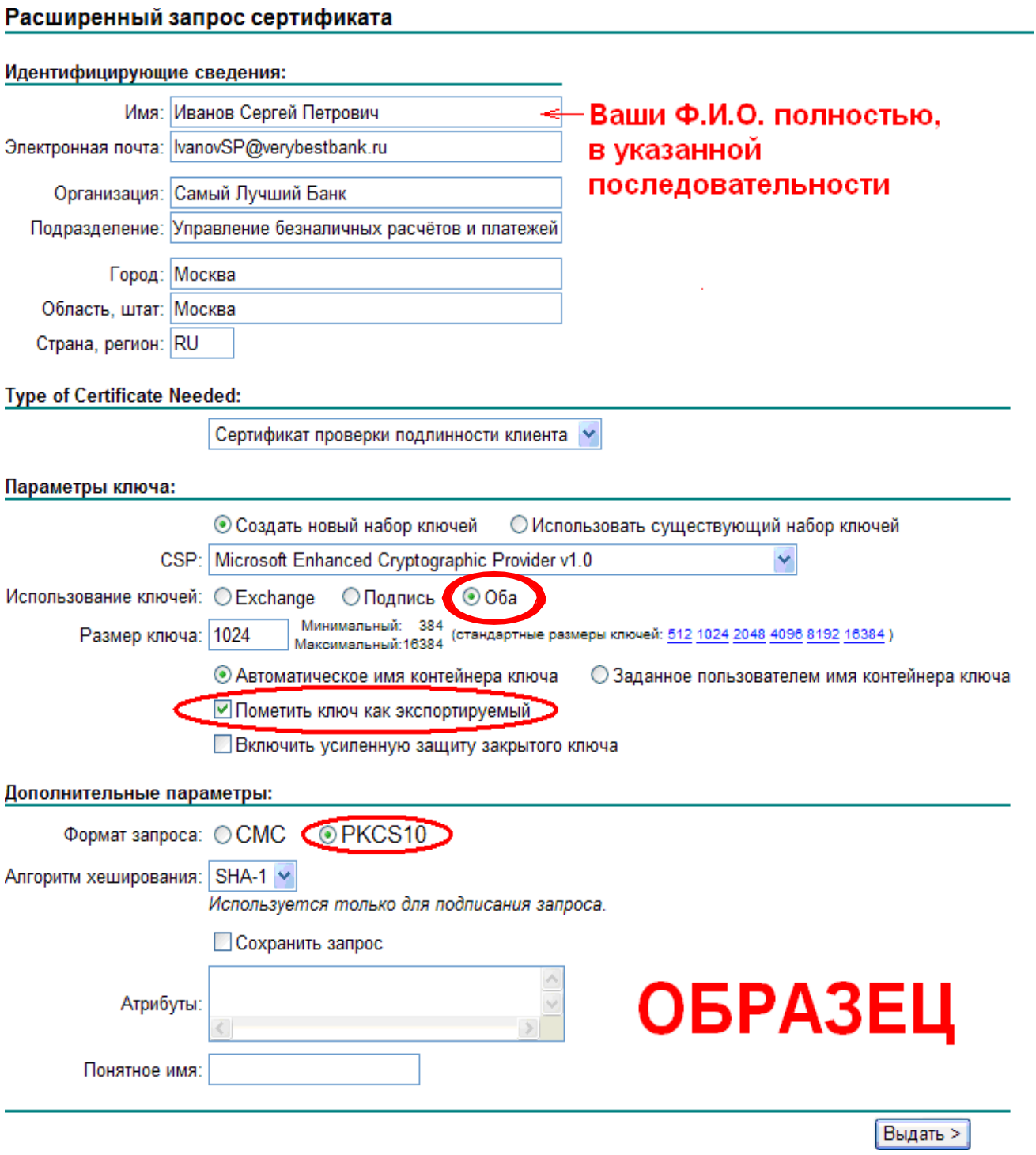
Для этого набрать в Internet Explorer адрес https://91.225.194.47/certsrv/,

На открывшейся странице приветствия выбрать нужное действие **Запрос сертификата,** на следующей странице выбрать **Расширенный запрос сертификата** и затем **Создать и выдать запрос к этому ЦС.**

Откроется страница **Расширенный запрос сертификата.**

Для корректного отображения этой страницы может потребоваться загрузка элемента управления ActiveX. В этом случае наведите курсор мыши на информационную полоску, появившуюся под строкой меню, кликните левую кнопку и запустите элемент ActiveX, как показано ниже на
рисунке.


Службы сертификации Active Directory (Microsoft) - Windows Internet Explorer
https://85.21.20.109/certsrv/certrqma.asp
Файл Правка Вид Избранное Сервис Справка
Настройка параметров
Службы сертификации ...
Страница
Сервис
Для этого веб-узла нужна следующая надстройка: "Microsoft Certificate Enrollment Control" от "Microsoft Corporation". Если вы доверяете этому веб-узлу и этой надстройке и разрешаете ее выполнение, щелкните здесь...
Запустить элемент ActiveX
Факторы риска
Подробнее
Microsoft Службы сертификации Active Directory -- Elecsnet Monitoring Root CA
Домой
Расширенный запрос сертификата
Идентифицирующие сведения:
Имя сертификата:
Электронная почта:
Организация:
Подразделение:
Город:
Область, штат:
Страна, регион:
Загрузка элемента управления ActiveX...
Type of Certificate Needed:
Сертификат проверки подлинности клиента
Параметры ключа:
Создать новый набор ключей
Использовать существующий набор ключей
CSP:
Загрузка...
Готово
85.21.20.109
Интернет
100%



Заполните **все** поля в разделе **Идентифицирующие сведения.**
В поле **Имя сертификата** укажите свои **Фамилию Имя Отчество** полностью.
В поле **Подразделение** можно указать должность, подразделение, либо, для краткости, что-то одно.
В поле **электронная почты** необходимо указать адрес, на который будут приходить оповещение об окончании срока действия сертификата (при необходимости вы можете указать несколько e-mail адресов через запятую)
Старайтесь избегать слишком длинных наименований. Поля заполняйте кириллицей, за исключением электронной почты и страны (RU).

В разделе **Параметры ключа** по желанию можно поставить галочку **Пометить ключ как экспортируемый.** Это позволит при необходимости экспортировать сертификат с приватным ключом на другой компьютер, однако понизит безопасность хранения сертификата.

В разделе **Дополнительные параметры** выбрать формат запроса **PKCS10.** Остальные параметры оставить без изменений. После заполнения формы нажать кнопку **Выдать.**

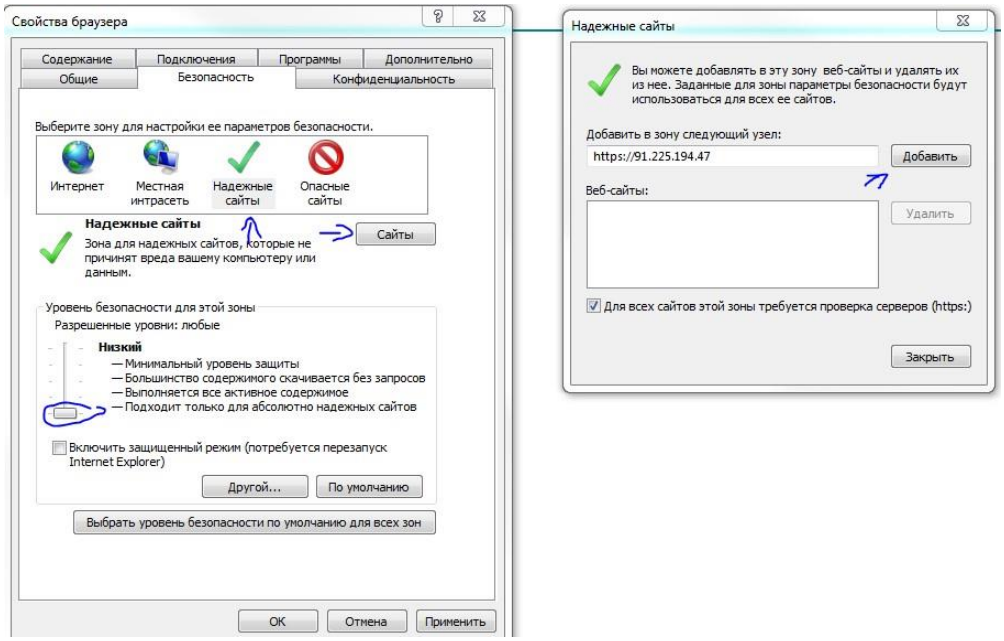
Далее ответить **Да** на предупредительное сообщение и Ваш запрос на сертификат будет получен центром сертификации.

В случае если при нажатии на «**Расширенный запрос сертификат»** , указанная на образце страница не открывается

Вам необходимо Синхронизировать вашу версию Браузера с девятой.
В принципе Ваши админы вполне могут Вам в этом помочь.
В случае если это не так - вот что надо делать.
На открытой странице браузера .На этапе нажатия "Расширенный запрос сертификата" нажимаете "F12"
В нижней части браузера должно всплыть окно с настройками.
Тут есть 2 варианта (в зависимости от версии)
1) В левой части экрана высвечивается вертикальное меню с картинками.
Вам нужно самое нижнее- называется "Emulation" В данной форме Вам нужно в поле "Режим документов" во всплывающем меню выбрать "9" , а в поле "строка агента пользователя" выбрать "Enternet Explorer 9"
2) Формы с меню высвечиваются горизонтальным списком
Тогда Вам так же нужна сама последняя форма "Эмуляция" порядок действий соответствует пункту 1
3)Формы с меню высвечиваются горизонтальным списком.
Вам нужны две последние формы. "Режим браузера", при наведении на неё всплывет список ,выберете "Enternet Explorer 9" и "режим документов"при наведении на неё всплывет список ,выберете "Стандартный Enternet Explorer 9"

После этого нажмете "F12" ещё раз, чтобы убрать отладчик и перейдете на "Расширенный запрос сертификата" . Все должно получится, если после проделывания всех действий- ошибка не исправилась- просьба обратиться к своим админам для проверки прав на Вашем ПК. Вы можете не быть администраторам на своей машине, или какие-либо политики безопасности не позволяют Вам хранить настройки изменений в режиме браузера .

В случае если не грузится поле CSP добавьте адрес в надежные сайты и поставьте низкий уровень безопасности. После запроса сертификата можно будет вернуть обратно.



Затем Вам следует время от времени проверять статус запроса.
Для этого снова зайдите по ссылке https://91.225.194.47/certsrv/
Просмотр состояния ожидаемого запроса сертификата.
Если запрос на сертификат ещё находится в ожидании, через некоторое время следует снова вернуться на этот веб-сайт для просмотра состояния. Сертификат будет выдан администратором после получения от менеджера Управления банковских программ заявки на выдачу сертификата и сверки её с запросом. Запрос хранится на сервере сертификации в течение 10 дней.
Если запрошенный Вами сертификат был Вам выдан, установите его. Выпущенный сертификат хранится на сервере 10 дней с момента выдачи его администратором, после чего автоматически удаляется. Если Вы не смогли, не успели установить сертификат в указанный срок,
Вам следует сделать новый запрос.

После установки сертификата web-мониторинг будет доступен по адресу

https://services.elecsnet.ru/cerber/default.aspx для web-мониторинга платёжных терминалов.

https://services.elecsnet.ru/finmonitor/default.aspx для банков, работающих с Элекснет по банкоматной программе.

Сертификат выдаётся строго на один год. Однако, в течение этого срока он может быть отозван администратором по причине компрометации ключа, компрометации Центра Сертификации, изменения принадлежности, замены сертификата, прекращения работы, либо действие сертификата может быть временно приостановлено.

По техническим вопросам обращайтесь:

Савина Евгения,
Заместитель начальника ОЭПЦ,
e-mail: savinaea@elecsnet.ru,
тел. 8-495-662-15-00 доб. 636