Инструкция по работе с сервисами с использованием электронной подписи

Общие требования для использования ЭП

Для подписания заявления электронной подписью (далее – ЭП) Вам потребуются:

- ключи ЭП и квалифицированный сертификат ключа проверки ЭП;
- сертифицированное ФСБ России шифровальное (криптографические) средство ViPNet CSP или КриптоПро CSP;
- программное обеспечение ViPNet Local Signature Service (далее – ViPNet LSS), предназначенное для создания и проверки электронной подписи (ЭП), а также для шифрования на веб-страницах;
- Microsoft .NET Framework версии 3.5.

Общие требования к компьютеру:

- Операционная система – Windows 7 (32/64-разрядная), Windows 8 (32/64разрядная), Windows 10 (32/64-разрядная);
- Веб-браузер – Microsoft Edge, Спутник, Mozilla Firefox акуальной версии (при использовании Mozilla Firefox Вам необходимо воспользоваться следующей инструкцией).

Ключи ЭП с квалифицированным сертификатом ключа проверки ЭП необходимо получить в аккредитованном удостоверяющем центре (далее – УЦ). Список аккредитованных удостоверяющих центров.

При наличии на Вашем компьютере установленных средств электронной подписи ViPNet CSP версии 4.2 и выше или КриптоПро CSP версии 3.6 и выше Вам необходимо для создания и проверки ЭП, а также для шифрования на веб-страницах сайта ПФР загрузить и установить на Ваш компьютер ViPNet Local Signature Service (далее – ViPNet LSS). Также Вам необходимо будет установить Microsoft .NET Framework версии 3.5.

При отсутствии у Вас средств электронной подписи, программного обеспечения ViPNet LSS, Microsoft .NET Framework версии 3.5 Вы можете воспользоваться Модулем автоматизации процесса установки и регистрации компонентов (МУРК).

Модуль автоматизации процесса установки и регистрации компонентов (МУРК) осуществляет инсталляцию:

1. Средства электронной подписи ViPNet CSP;

2. ViPNet LSS;
3. Microsoft .NET Framework версии 3.5.;
4. Registration Agent.

Также модуль осуществляет автоматизированную регистрацию Средства электронной подписи ViPNet CSP (http://www.infotecs.ru/products/catalog.php?ELEMENT_ID=2096) (в случае, если была проведена его инсталляция).

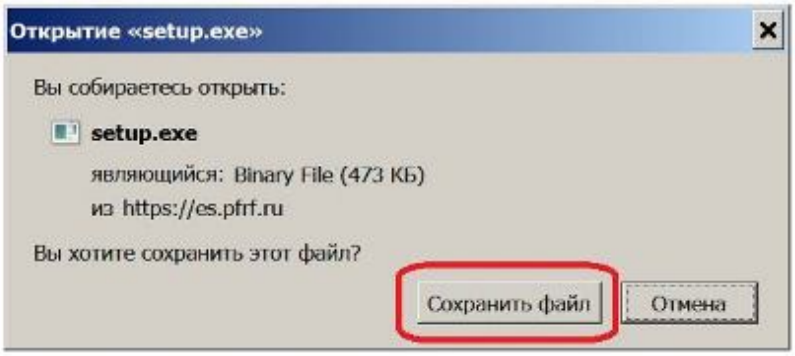
Предварительные условия для установки МУРК

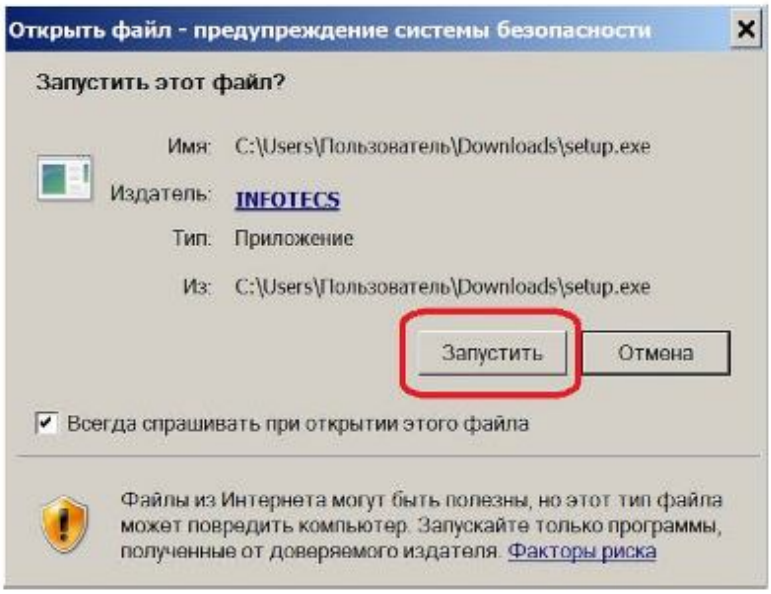
Требования к компьютеру для работы с МУРК:

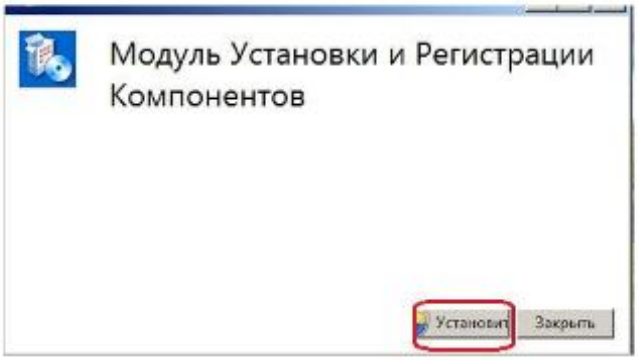
- отсутствие на компьютере иных средств электронной подписи.

Порядок установки МУРК

Загрузите и запустите установочный файл Модуля автоматизации процесса установки и регистрации компонентов (МУРК) (http://es.pfrf.ru/ext/lss/setup.exe) для установки компонентов, необходимых для работы с электронной подписью (далее – ЭП).







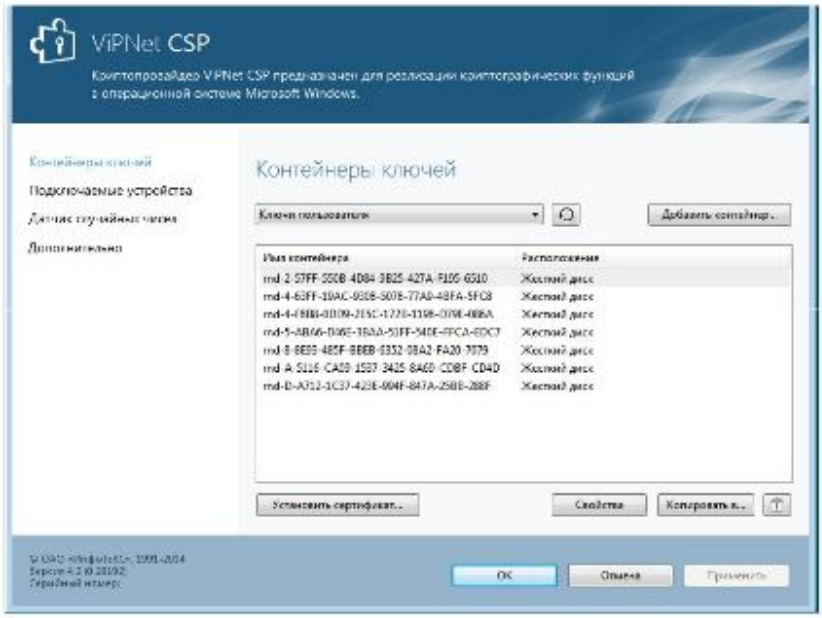
По завершении установки Вам необходимо осуществить перезагрузку компьютера. При загрузке будет автоматически запущена программа ViPNet LSS. Впоследствии эта программа будет автоматически запускаться при каждой загрузке компьютера.

Установка контейнера ключей и сертификатов необходимых для создания ЭП

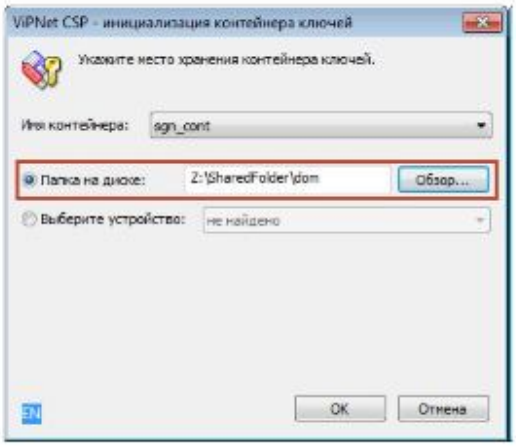
Для создания и проверки ЭП необходимо установить полученный от аккредитованного УЦ сертификат ключа проверки ЭП в системное хранилище.

Для установки выполните следующие действия:

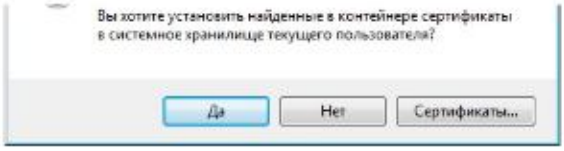
1. В окне ViPNet CSP в разделе Контейнеры ключей нажмите кнопку Добавить контейнер.



2. В окне ViPNet CSP - инициализация контейнера ключей нажмите кнопку Обзор.
   - Если контейнер ключей хранится на жестком диске, в окне Обзор папок укажите путь к папке, содержащей контейнер.
   - Если контейнер ключей хранится на съемном флэш-диске, в окне Обзор папок укажите этот съемный диск. В поле Папка на диске автоматически будет подставлен путь, например E:\Infotecs\Containers.



3. В списке Имя контейнера выберите файл контейнера ключей или оставьте значение по умолчанию «Папка на диске».
4. Нажмите кнопку OK. В окне Контейнер ключей появится сообщение об успешном добавлении контейнера ключей и предложение установить сертификат в системное хранилище.
   Для работы с сертификатами их необходимо установить в хранилище текущего пользователя.
   В окне Контейнер ключей чтобы автоматически установить сертификат в системное хранилище , нажмите кнопку Да.



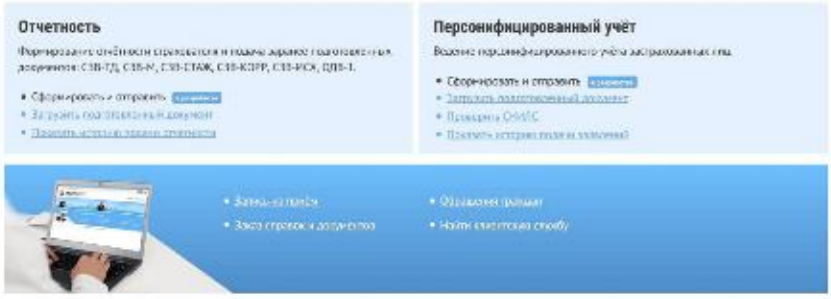
5. После установки (или отмены установки) сертификатов в хранилище в списке доступных контейнеров ключей появится добавленный контейнер ключей.

Использование Электронной подписи

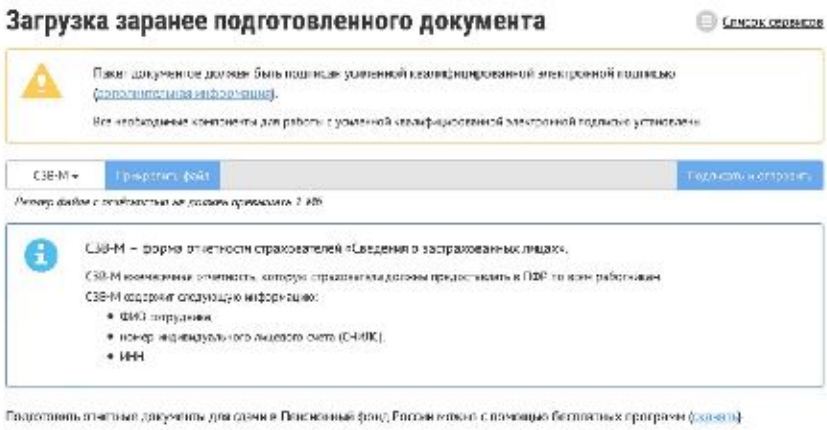
Сервисы, где требуется применение ЭП:

- Заключение соглашения об использовании кабинета страхователя;
- Загрузка заранее подготовленного документа блока "Отчетность";
- Загрузка заранее подготовленного документа блока "Персонифицированный учет" и др.

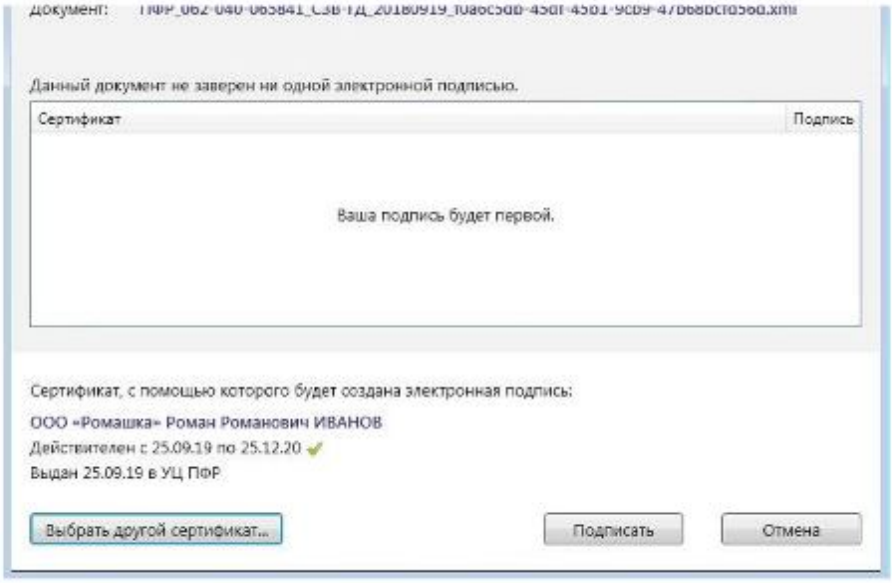
Для загрузки заранее подготовленного документа блока "Отчетность" необходимо перейти по соответствующей ссылке с Главной страницы Кабинета Страхователя.



Выбрать тип загружаемого документа и добавить файл. Далее выбрать «Подписать и отправить».



В окне «Подписание xml-документа» убедитесь, что выбран соответствующий сертификат и нажмите «Подписать». Для подписи необходимо указать пароль доступа к контейнеру ключей. Далее нажмите «ОК»



Документ успешно отправлен.

Краткая инструкция по устранению ошибки возникающей в браузере Mozilla *Firefox*.

В браузере Mozilla *Firefox* возможно возникновение следующей ошибки (см. Рис 1.)

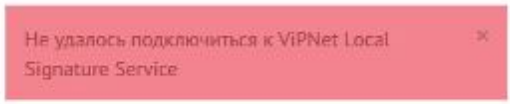
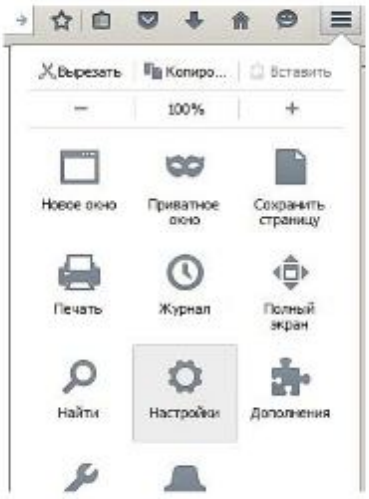
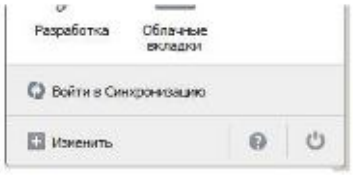


Рисунок 1. Ошибка в браузере Mozilla *Firefox*.

Чтобы устранить эту ошибку, необходимо добавить исключение безопасности в веб-браузере Mozilla *Firefox*.

Для добавления исключения безопасности необходимо зайти в настройки браузера Mozilla *Firefox*





и произвести следующие действия:

1. Перейти на вкладку **«Дополнительные»**.
2. Выбрать **«Сертификаты»**.
3. Нажать кнопку **«Просмотр сертификатов»**.
4. Появится окно **«Управление сертификатами»**. В окне выбрать вкладку **«Серверы»**.
5. Нажать кнопку **«Добавить исключение»**.
6. Появится окно **«Добавить исключение безопасности»**. В окне, в поле **Адрес**, написать – **127.0.0.1:61112** и нажать кнопку **«Получить сертификат»**.
7. Поставить «галочку» **Постоянно хранить это исключение** и нажать кнопку **«Подтвердить исключение безопасности»**.
8. Повторите шаги 5-7 для другого адреса (127.0.0.1:12402).

Последовательность действий отображена на рисунке 2.

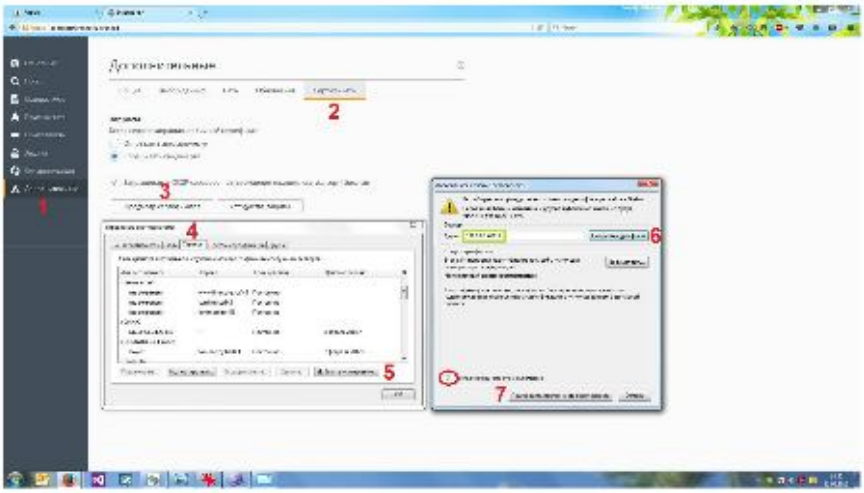


Рисунок 2. Последовательность действий.

В окне управления сертификатами, на вкладке **«Серверы»** должно появиться исключение (см. Рис 3.)

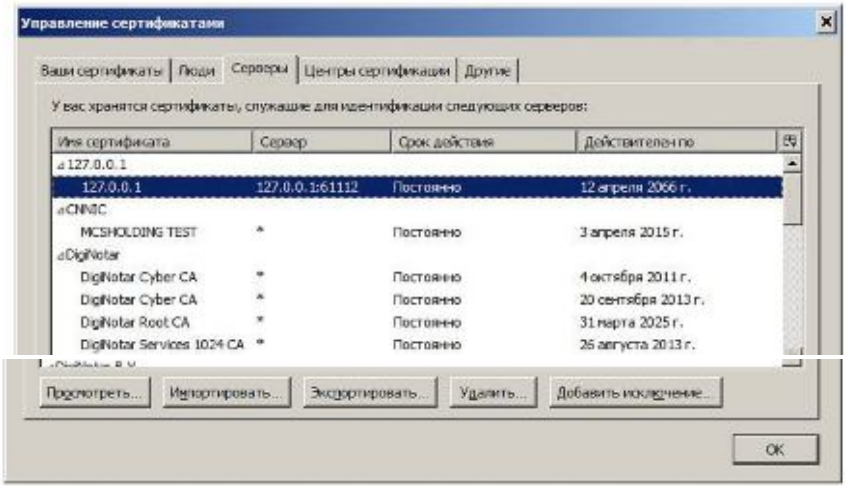


Рисунок 3. Исключение безопасности