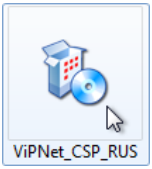
ViPNet CSP 4.2

Быстрый старт

Программа ViPNet CSP — сертифицированный криптопровайдер, обеспечивающий вызов криптографических функций в приложениях Windows. Например, с помощью ViPNet CSP вы можете формировать и проверять электронную подпись в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, шифровать данные в соответствии с алгоритмом ГОСТ 28147-89.
Этот документ поможет вам начать работу с программой ViPNet CSP.

Установка программы



Загрузите установочный файл программы ViPNet CSP на веб-сайте ОАО «ИнфоТеКС» (www.infotecs.ru). При загрузке вам будет предоставлен серийный номер, необходимый для регистрации программы.
Запустите установочный файл программы, примите условия лицензионного соглашения и нажмите кнопку **Установить сейчас**.
По завершении установки перезагрузите компьютер.

Запуск и регистрация программы

Чтобы запустить программу ViPNet CSP, дважды щелкните ярлык программы на рабочем столе либо щелкните соответствующую плитку на начальном экране.

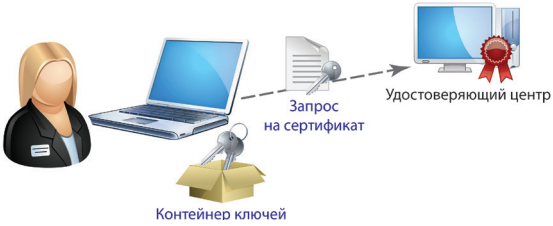
Без регистрации срок действия программы ограничен двумя неделями. Чтобы снять это ограничение, программу необходимо зарегистрировать. Для этого в окне **ViPNet CSP** выберите пункт **Зарегистрировать ViPNet CSP** и нажмите кнопку **Далее**. Следуйте указаниям мастера регистрации.

infotecs

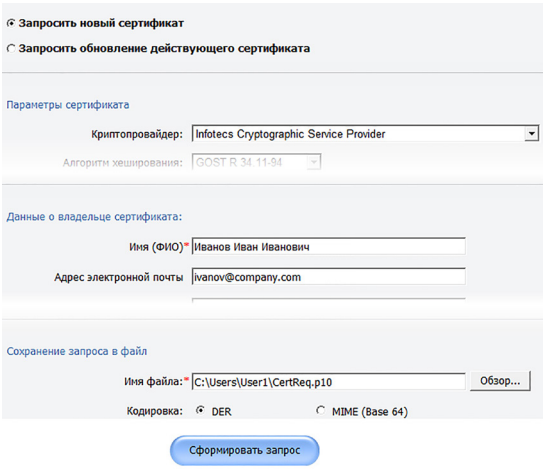
Формирование запроса на сертификат открытого ключа подписи

Если контейнер ключей с установленным сертификатом был выдан вам ранее администратором удостоверяющего центра, перейдите к разделу «Установка контейнера ключей, выданного администратором».

Если контейнера ключей у вас нет, сформируйте запрос на получение сертификата для отправки в удостоверяющий центр:

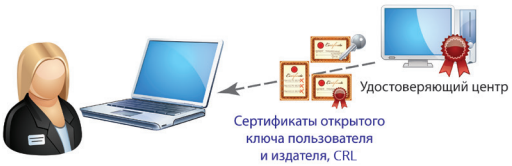


1. В меню **Пуск** выберите **Все программы > ViPNet > ViPNet CSP > Создание запроса на сертификат** либо на начальном экране откройте список приложений и выберите **ViPNet > Создание запроса на сертификат**.
2. В окне **Служба сертификации** выберите действие **Запросить новый сертификат**.
3. Укажите параметры запрашиваемого сертификата, данные о владельце и нажмите кнопку **Сформировать запрос**.
4. В появившемся окне **ViPNet CSP - инициализация контейнера ключей** задайте пароль доступа к создаваемому контейнеру ключей.
5. Для формирования последовательности случайных чисел, необходимой для создания контейнера ключей, поводите указателем в пределах окна **Электронная рулетка**.



В результате будут сформированы и сохранены на компьютере контейнер ключей и файл запроса на сертификат с расширением *.p10. Передайте этот файл администратору вашего удостоверяющего центра.

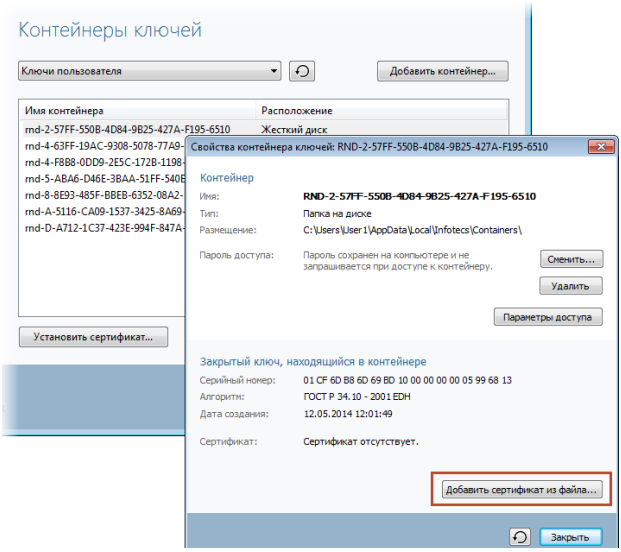
Получите у администратора вашего удостоверяющего центра изданный сертификат открытого ключа. Вместе с этим сертификатом он передаст вам также сертификат издателя и список отозванных сертификатов (CRL).



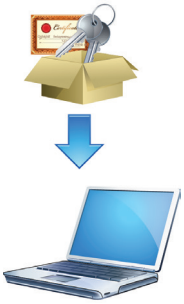
Установка сертификата в контейнер ключей

Сертификат, полученный из удостоверяющего центра, необходимо установить в контейнер ключей, созданный при формировании запроса на сертификат:

1. В главном окне программы ViPNet CSP выберите раздел **Контейнеры ключей**.
2. Дважды щелкните контейнер, который был создан при формировании запроса на сертификат.
3. В окне **Свойства контейнера ключей** нажмите кнопку **Добавить сертификат из файла**.
4. В окне Открыть укажите файл сертификата, полученный от администратора удостоверяющего центра. Если указан верный сертификат, он будет добавлен в контейнер.



Установка контейнера ключей, выданного администратором



Если ранее администратор удостоверяющего центра выдал вам контейнер ключей с установленным сертификатом и сообщил пароль к нему, установите этот контейнер в ViPNet CSP:

1. В окне **ViPNet CSP** в разделе **Контейнеры ключей** нажмите кнопку **Добавить контейнер.**
2. В окне ViPNet CSP - инициализация контейнера ключей укажите расположение контейнера ключей.
3. Нажмите кнопку **OK**. В окне **Контейнер ключей** появится сообщение об успешном добавлении контейнера ключей.

Установка сертификатов пользователя и издателя, а также CRL в системное хранилище

Для выполнения криптографических операций установите ваш сертификат пользователя, а также сертификаты издателей и список отозванных сертификатов (CRL) в системное хранилище. Для этого выполните следующие действия:

- Чтобы установить сертификат пользователя, в окне **Свойства контейнера ключей** (см. раздел «Установка сертификата в контейнер ключей») нажмите кнопку **Открыть**, а затем в окне **Сертификат** нажмите кнопку **Установить сертификат** и следуйте указаниям мастера установки сертификатов.
- Чтобы установить сертификат издателя или CRL, щелкните соответствующий файл правой кнопкой мыши и в контекстном меню выберите пункт **Установить сертификат** или **Установить список отзыва (CRL)**. Следуйте указаниям мастера импорта сертификатов операционной системы Windows.

Сертификат издателя необходимо устанавливать в хранилище **Доверенные корневые центры сертификации.**
CRL необходимо устанавливать в хранилище **Промежуточные центры сертификации.**

Выполнив перечисленные выше действия, вы можете использовать любые приложения, которые в своей работе взаимодействуют с криптопровайдером. Это могут быть программы для работы с электронной подписью, шифрования данных и другие.

ОАО «ИнфоТеКС»
127287, Москва, Старый Петровско-Разумовский проезд, 1/23, стр. 1
Документация для продуктов ViPNet: https://infotecs.ru/downloads/documentacii//
Видеоруководства и презентации: https://www.youtube.com/user/InfotecsDoc
Электронный адрес службы поддержки: hotline@infotecs.ru
Телефон горячей линии (бесплатный звонок с территории России, кроме Москвы): 8–800–250–0–260

ФРКЕ.00106-04 34 04