Код Безопасности

Средство криптографической защиты информации

Континент TLS VPN Клиент
Версия 1.0

Руководство пользователя

RU.88338853.501430.011 91

Почтовый адрес:	**105318, Россия, Москва, а/я 101 ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение

Данный документ предназначен для пользователей изделия "Средство криптографической защиты информации "Континент TLS VPN Клиент" версия 1.0 RU.88338853.501430.011 (далее – Клиент). В нем содержатся сведения, необходимые для установки, настройки и работы с Клиентом.

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8-495-982-30-20 или по электронной почте support@securitycode.ru. Страница службы технической поддержки на сайте компании "Код Безопасности": http://www.securitycode.ru/products/technical-support/.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем Учебного центра можно по электронной почте (edu@itsecurity.ru).

Общие сведения

Назначение и основные функции

Клиент предназначен для реализации защищенного доступа удаленных пользователей к веб-ресурсам корпоративной сети по каналам связи общих сетей передачи данных.

Клиент работает совместно с СКЗИ "Континент TLS VPN Сервер" версия 1.0 (далее – Сервер) и обеспечивает выполнение следующих функций:

- обоюдная аутентификация с Сервером в процессе установки защищенного соединения посредством технологии открытых ключей;
- установление защищенного соединения и обмен зашифрованными данными с Сервером;
- функционирование с открытыми ключами и сертификатами открытых ключей, совместимыми с Удостоверяющим центром "КриптоПро УЦ";
- возможность работы с серверами, поддерживающими протокол TLS v.1.0, TLS v1.2;
- хранение ключевой информации в защищенном контейнере;
- контроль целостности программного обеспечения;
- регистрация событий, связанных с работой Клиента.

Принципы функционирования

Клиент представляет собой устанавливаемое на компьютере удаленного пользователя программное обеспечение и функционирует совместно с СКЗИ "Континент TLS VPN Сервер" версия 1.0.

Для доступа к защищаемым веб-ресурсам удаленный пользователь должен в адресной строке веб-обозревателя ввести IP-адрес или имя Сервера.

По адресу, указанному пользователем, Клиент посылает Серверу запрос на создание защищенного соединения.

На основании принятого запроса сервер запускает процедуру взаимной аутентификации "Клиент – Сервер". Аутентификация проводится на основе сертификатов открытых ключей.

После успешного завершения процедуры взаимной аутентификации выполняется генерация сеансового ключа, и между Клиентом и Сервером устанавливается защищенное соединение по протоколу TLSv1. Далее Сервер направляет запрос Клиента по указанному пользователем адресу веб-ресурса в защищаемую сеть. Полученный от веб-сервера ответ на запрос Сервер возвращает Клиенту в рамках защищенного соединения.

В случае невыполнения по каким-либо причинам требований, предъявляемых к взаимной аутентификации Клиента и Сервера, защищенное соединение не устанавливается и доступ пользователя к веб-ресурсу блокируется.

Сертификаты открытых ключей

Для работы Клиента требуются следующие сертификаты:

- корневой сертификат Удостоверяющего центра;
- сертификат пользователя;
- сертификат Сервера.

Поддерживается работа с сертификатами X.509v3 форматов DER, PEM, а также с контейнерами сертификатов формата PKCS7.

Предусмотрена проверка корневых сертификатов и сертификатов Сервера по CRL. При наличии прямого доступа компьютера к Удостоверяющему центру

загрузка CRL осуществляется автоматически. При отсутствии прямого доступа CRL должны загружаться администратором вручную.

Контроль целостности

Функция контроля целостности предназначена для слежения за неизменностью содержимого установленного программного обеспечения Клиента. Действие функции основано на сравнении текущих значений хэш-кода контролируемых файлов и значений, принятых за эталон.

Список файлов ПО Клиента, подлежащих контролю, и значения хэш-кода для каждого из них хранятся в конфигурационном файле. Конфигурационный файл формируется при сборке инсталляционного пакета. Значения хэш-кодов вычисляются по алгоритму ГОСТ Р 34.11-94.

При установке ПО Клиента значение хэш-кода конфигурационного файла зашифровывается стандартными средствами Windows и в зашифрованном виде записывается в ключ реестра.

Операция контроля целостности выполняется с периодичностью, заданной в конфигурационном файле.

При несовпадении текущих значений хэш-кодов и эталонных значений, хранящихся в реестре, доступ к защищаемым ресурсам блокируется.

События, связанные с работой контроля целостности, регистрируются в журнале приложений Windows.

Регистрация событий

События, связанные с работой Клиента, регистрируются в журнале Windows.

Список регистрируемых событий приведен в Приложении (см. стр.**15**).

Для просмотра зарегистрированных событий пользователь должен входить в группу локальных администраторов компьютера.

Подготовка перед установкой

До начала установки ПО Клиента необходимо получить следующие сертификаты:

- корневой сертификат Удостоверяющего центра (УЦ);
- сертификат пользователя;
- сертификат Сервера.

В качестве ключевых носителей используются USB-ключи eToken PRO (Java) и Rutoken S, а также USB-флеш-накопители.

Корневой сертификат УЦ и сертификат пользователя получают в соответствии с общим порядком, установленным конкретным Удостоверяющим центром.

Сертификат Сервера получают от администратора СКЗИ "Континент TLS VPN Сервер" на отчуждаемом носителе.

Полученные сертификаты передаются пользователю, уполномоченному выполнять функции администратора Клиента.

После получения всех сертификатов администратор Клиента должен выполнить следующее:

- Установить корневой сертификат УЦ в хранилище доверенных центров сертификации в папку "Локальный компьютер". Также необходимо установить в хранилище доверенных центров сертификации в папку "Локальный компьютер"действительный список отозванных сертификатов (CRL).
- Передать пользователю его сертификат и проинструктировать о правилах хранения и использования сертификата при работе с защищаемыми веб-ресурсами. Формат ввода адреса веб-ресурса https://адрес_сервера.
- Подготовить сертификат Сервера для настройки Клиента.

Установка ПО Клиента

Для установки ПО Клиента:

1. Поместите установочный диск в устройство чтения компакт- дисков и запустите на исполнение файл ContinentTLSSetup.exe, находящийся в каталоге с дистрибутивом Клиента, путь к которому указан в документе Release Notes.

   На экране появится окно выбора устанавливаемых компонентов.

Компонент	Описание
Windows Installer 4.5	Устанавливается при необходимости
Rutoken	Драйверы и программы для работы со считывателем Rutoken
eToken	Драйверы и программы для работы со считывателем eToken
Jinn-Admin	Программы для работы с сертификатами и ключевыми контейнерами
"Континент TLS Клиент КС2"	Программное обеспечение Клиента

   Из приведенных выше обязательным устанавливаемым компонентом является "Континент TLS Клиент КС2".

2. Выберите компонент "Континент TLS Клиент КС2".

   На экране появится стартовое окно мастера установки компонента.

3. В окне мастера нажмите кнопку <Далее>.

   На экране появится окно лицензионного соглашения.

4. Прочтите лицензионное соглашение и, если вы принимаете его условия, поставьте отметку в поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее>".

   На экране появится окно ввода лицензионного ключа.

5. Введите лицензионный ключ и нажмите кнопку "Далее".

   На экране появится диалог выбора папки установки. По умолчанию программа установки копирует файлы на системный диск в каталог \Program Files\Security Code\Континент TLS Клиент\.

   Примечание. Для установки программы в другую папку нажмите кнопку "Изменить" и укажите нужную папку в диалоге, появившемся на экране.

6. Нажмите кнопку "Далее>".

   На экране появится диалог "Запуск конфигуратора".

7. Если необходимо выполнить настройку сразу после установки Клиента, установите отметку в поле "Запустить конфигуратор после завершения установки".

   Нажмите кнопку "Далее>".

   На экране появится окно с сообщением о готовности к установке Клиента.

8. Нажмите кнопку "Установить".

   Начнется установка и после ее завершения на экране появится соответствующее сообщение.

9. Нажмите кнопку "Готово" в окне сообщения.

   На экране появится сообщение о необходимости перезагрузить компьютер.

10. Если необходимо установить другой компонент, откажитесь от перезагрузки, выберите компонент в списке и установите его. После установки всех необходимых компонентов, если перезагрузка компьютера не требуется, закройте окно выбора компонентов, используя кнопку <Выход>.

Если установка других компонентов не требуется, выберите "Да" в окне сообщения.

Начнется перезагрузка компьютера.

После установки Клиента и перезагрузки компьютера в меню Windows "Пуск" появится пункт "Настройка Континент TLS Клиент".

Внимание! После установки дополнительных компонентов в меню "Пуск" будут добавлены новые пункты.

Настройка Клиента

Для работы Клиента на компьютере необходимо выполнить следующие настройки:

- настроить прокси;
- настроить веб-обозреватель.

Настройка прокси

Настройку прокси выполняет пользователь, входящий в группу локальных администраторов компьютера.

Для настройки прокси:

1. В меню "Пуск" выберите пункт "Настройка Континент TLS Клиент".

   На экране появится диалог "Настройка сервиса".
2. Введите или измените номер порта. По умолчанию установлено значение 8080.
3. Введите или измените IP-адрес или имя сервера "Континент TLS VPN Сервер".
4. Укажите сертификат сервера. Для этого нажмите кнопку, расположенную справа.
   - Если сертификат хранится на отчуждаемом носителе, поддерживающем файловую систему (USB-флеш-накопитель), вставьте носитель.
   - Если сертификат хранится на внешнем носителе eToken или Rutoken, предварительно выполните импорт сертификата на компьютер.

   На экране появится стандартный диалог выбора файла.
5. Укажите файл сертификата сервера и нажмите кнопку "ОК".

   Указанный сертификат будет внесен в поле "Сертификат".
6. Для работы с TLS-серверами с устаревшими сертификатами ФСБ удалите отметку в поле "Требовать поддержку RFC 5746".

   Внимание! Отметка установлена по умолчанию. Удалять отметку не рекомендуется.
7. Если для выхода во внешнюю сеть используется прокси-сервер, установите отметку в поле "Использовать внешний прокси-сервер" и укажите его адрес и порт.
8. Для завершения настройки нажмите кнопку "ОК".

Настройка веб-обозревателя

Настройка должна быть выполнена для каждого пользователя, которому предоставляется доступ к защищаемым веб-ресурсам.

Для настройки веб-обозревателя:

1. Войдите в систему под учетной записью пользователя.
2. Откройте окно "Свойства обозревателя" и перейдите на вкладку "Подключения".
3. В разделе "Настройка параметров локальной сети" нажмите кнопку "Настройка сети".

   На экране появится окно "Настройка параметров локальной сети".
4. Установите отметку в поле "Использовать прокси-сервер для локальных подключений" и введите значения параметров:

Адрес	127.0.0.1
Порт	8080

Примечание. Номер порта должен соответствовать порту из пункта 2 настройки прокси.

5. Нажмите кнопку "ОК" и закройте окно "Свойства обозревателя".

Работа с защищенными ресурсами

Для доступа к защищенному ресурсу:

1. Запустите веб-обозреватель и в адресной строке введите адрес веб-ресурса с префиксом https://.

   Внимание! Адрес ресурса должен содержать имя сервера TLS, указанное в настройках прокси.

   На экране появится диалог выбора сертификата пользователя.

   В диалоге отображается список внешних носителей с обнаруженными на них сертификатами.
2. Вставьте носитель с сертификатом пользователя и нажмите в диалоге кнопку "Обновить".
3. Выберите носитель и сертификат пользователя и введите пароль доступа к ключевому контейнеру.
4. Если требуется запомнить путь к сертификату и пароль, установите отметку в соответствующем поле.
5. Нажмите кнопку "ОК".

   Диалог выбора сертификата закроется и будет установлено защищенное соединение с указанным веб-ресурсом.

Если пользователь 5 раз подряд предъявил недействительный сертификат, то доступ к серверу заблокируется на 10 минут. Повторная попытка подключения будет возможна только через 10 минут (ограничение реализовано на стороне сервера).

Просмотр событий

Для просмотра зарегистрированных событий пользователь должен входить в группу локальных администраторов компьютера.

Для просмотра событий:

1. Запустите в Windows средство "Просмотр событий".
2. Раскройте папку "Журналы Windows" и выберите журнал "Приложение".

   У событий, связанных с работой Клиента, в качестве источника указано значение "ContinentTLS".

   Для удобства просмотра используйте фильтр.

Удаление ПО Клиента

Для удаления ПО Клиента:

1. Нажмите кнопку "Пуск" и в главном меню Windows найдите и активируйте команду "Панель управления".
2. В окне "Панель управления" активируйте элемент "Установка и удаление программ".
3. Выберите в списке установленных программ элемент "Континент TLS Клиент" и нажмите кнопку "Удалить".

   На экране появится диалог для подтверждения удаления ПО.
4. Нажмите кнопку "Да".

   Начнется удаление и после его завершения на экране появится сообщение о необходимости перезагрузить компьютер.
5. Нажмите кнопку "Да".

   Начнется перезагрузка компьютера.

Приложение

Регистрируемые события

Ниже приведен список событий, связанных с работой Клиента и регистрируемых в журнале Windows.

Событие
Служба ContinentTLS успешно инсталлирована
Служба ContinentTLS деинсталлирована
Служба запущена, версия: xxx
Служба остановлена
Произошла системная ошибка: 'xxxx', код: аааа [бббб]
Блокирована попытка установить соединение неавторизованным пользователем: domain\user
Блокирована попытка инициализации удаленного соединения на защищаемый сервер с адреса: address
Инициализация локального соединения на защищаемый сервер, процесс: pid 'path', учетная запись: domain\user
Инициализация ключевой пары для пользователя с учетной записью domain\user выполнена успешно
Ключевая пара не инициализирована, код ошибки: code
Секретный ключ удален из памяти
Ошибка установки ключевой пары: 'description'
Успешная аутентификация сервера "xxxx"
Защищаемый сервер не прошел аутентификацию. Причина xxxx
Сервер отказал в аутентификации. Код ошибки: xxxx. Описание: уууу
Сервер разорвал соединение на этапе аутентификации: 'xxxx'
Ошибка инициализации конфигурационных параметров
Ошибка №%1 HTTP протокола: '%2'. Описание: %3
Инициализация процедуры проверки целостности файлов выполнена успешно, количество контролируемых файлов: %1
Не задано ни одного файла для контроля целостности
Ошибка инициализации процедуры проверки целостности файлов, требуется переустановка продукта
Проверка целостности файлов выполнена успешно, проверено файлов: %1
Нарушена целостность файла '%1', дальнейшая работа будет приостановлена. %2
Проверка целостности файла '%1' выполнена успешно
Ошибка проверки целостности конфигурационного файла. %1
Настройка "xxxx" изменена. Старое значение «аааа», новое значение "бббб"
Сертификат шифрующего сервера был изменен. Кем выдан: "xxxx", кому выдан: "аааа", серийный номер: "бббб"
Сертификат шифрующего сервера был удален из настроек
Криптографический контейнер успешно прочитан. Серийный номер сертификата контейнера: xxx
Введен неверный пароль криптографического контейнера. Серийный номер сертификата контейнера: xxxx

Превышено количество попыток ввода пароля криптографического контейнера. Серийный номер сертификата контейнера: xxxx. Использование контейнера приостановлено на yyyy
Ошибка чтения криптографического контейнера. Серийный номер сертификата контейнера: xxxx. Причина: yyyy