Средство криптографической защиты информации "Континент TLS-клиент" Версия 2 Комментарии к релизу 2.0.1482.0

Документ содержит описание возможностей изделия "Средство криптографической защиты информации "Континент TLS-клиент". Версия 2" (далее – СКЗИ "Континент TLS-клиент", TLS-клиент или изделие) релиза 2.0.1482.0, а также особенностей и ограничений, которые необходимо учитывать при его эксплуатации.

Оглавление

1. Изменения и новые возможности 2

2. Ограничения на поддержку аппаратных и программных средств 3

3. Особенности работы и ограничения 4

1. Изменения и новые возможности

Ниже приводятся сведения об изменениях и новых возможностях СКЗИ "Континент TLS-клиент" версии 2 (релиз 2.0.1482.0) по сравнению с сертифицированным ФСБ России СКЗИ "Континент TLS VPN Клиент" версии 1.2 (релиз 1.2.1).

1. Модульная архитектура, при которой реализация криптографических алгоритмов выполняется в отдельном стороннем программном модуле – криптопровайдере.

2. Регистрация событий с самодостаточным текстовым описанием в журнале приложений Windows и лог-файлах.

3. TLS-клиент имеет возможность автоматического обновления ПО и автоматической конфигурации списка защищенных ресурсов.

4. Возможность работы с ключевыми носителями JaCarta PKI, JaCarta ГОСТ.

5. Запуск туннелируемых приложений.

6. Регистрация СКЗИ.

7. Неявное проксирование.

8. Обновленный пользовательский интерфейс с настраиваемыми цветовыми схемами.

9. Автоматическое скачивание списка отозванных сертификатов CRL.

10. Автозапуск при старте операционной системы (ОС).

11. Поддержка внешних прокси с Basic-, NTLM-, Kerberos-, Negotiate-аутентификацией.

12. Возможность создавать запрос на сертификат пользователя из TLS-клиента.

2. Ограничения на поддержку аппаратных и программных средств

1	Ключевое устройство	USB-флеш-накопители; USB-ключи — Рутокен, Рутокен Lite, Рутокен S (версия 2.0 и 3.0), Рутокен ЭЦП, JaCarta PKI, JaCarta ГОСТ, JaCarta PKI Flash, JaCarta ГОСТ Flash, eToken PRO (Java), Esmart USB Token, Esmart USB Token ГОСТ; смарт-карты — Рутокен ЭЦП, Рутокен Lite, JaCarta PKI, JaCarta ГОСТ, eToken PRO (Java), eToken PRO, Esmart, Esmart ГОСТ; идентификаторы DS1995, DS1996
2	Операционная система	Windows 10 (включая выпуски Starter и Home Edition); Windows 8.1; Windows 7 SP1; Windows Server 2012 R2 x64; Windows Server 2016 x64; Windows Server 2019 x64
3	Криптопровайдер	КриптоПро CSP версии 4.0; Валидата CSP 5.0; Код Безопасности CSP (не ниже версии 4.0.300.0)
4	Дополнительное ПО	Веб-браузер: Google Chrome 48 или выше (для Windows 7, 8.1, 10, Windows Server 2012, 2016, 2019); Mozilla Firefox 46 или выше (для Windows 7, 8.1, 10, Windows Server 2012, 2016, 2019); Internet Explorer 8, 9, 10 (для Windows 7, Windows Server 2012, 2016, 2019); Internet Explorer 11 (для Windows 7, 8.1, 10, Windows Server 2012, 2016, 2019); Microsoft Edge (для Windows 10, Windows Server 2012, 2016, 2019)Google

3. Особенности работы и ограничения

1. TLS-клиент функционирует совместно с TLS-сервером версий 1.2, 2 по протоколу TLS (версии 1.0, 1.2), криптоалгоритмам ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ 28147-98.

2. При работе с сертификатами по ГОСТ Р 34.10-2001 ("КриптоПро CSP") без установленного криптопровайдера "КриптоПро CSP" в качестве ключевых носителей могут быть использованы только Рутокен и eToken. При этом в качестве ПО для токенов необходимо установить PKI-клиент.

3. Установку стороннего криптопровайдера необходимо выполнять перед инсталляцией TLS-клиента.

4. Перед установкой ПО "TLS-клиент" должны быть установлены последние обновления ОС Windows.

5. Перед установкой ПО "TLS-клиент" необходимо удалить версию 3.7 криптопровайдера "Код Безопасности", если она была установлена. Удаление производится запуском файла csp_uninst.exe из каталога установки C:\Program Files\Security Code\Terminal Station\csp. После удаления криптопровайдера необходимо перезагрузить компьютер.

6. При установке ПО "TLS-клиент" с помощью файла Континент TLS-клиент.exe будут установлены и TLS-клиент, и криптопровайдер "Код Безопасности", если ранее не был установлен сторонний криптопровайдер. В случае необходимости криптопровайдер "Код Безопасности" устанавливается отдельно с помощью файла Код Безопасности CSP.msi.

7. Если при установке ПО TLS-клиента было выбрано использование физического ДСЧ, а платы ПАК "Соболь" не было обнаружено, на экране появится сообщение об ошибке. В этом случае необходимо установить ПО ПАК "Соболь" и после перезагрузки заново запустить процесс установки ПО TLS-клиента.

8. Для использования персональных ключевых носителей Рутокен, JaCarta, eToken и Esmart необходимо скачать и установить их драйверы.

9. Криптопровайдер "КриптоПро CSP" позволяет импортировать сертификаты только собственного выпуска. Криптопровайдер "Код безопасности CSP" позволяет производить импорт сертификатов, выпущенных как посредством ПО "Код безопасности CSP", так и ПО "КриптоПро" (сертификаты, соответствующие ГОСТ Р 34.10-2001).

10. При установленном туннеле в веб-браузере необходимо задавать тот же протокол, который используется на защищенном веб-сервере.

11. После внесения изменений в файл hosts необходим перезапуск ПО TLS-клиента.

12. Имена ресурсов TLS-клиента не могут быть заданы кириллицей.

13. При использовании интернет-браузера Firefox для корректной работы в режиме непрозрачного проксирования необходима его дополнительная настройка.

14. Выполнение функций подсистемой автоматического обновления и автоматической конфигурации защищенных ресурсов при совместной работе с TLS-серверами версий 1.x невозможно.

15. После обновления ПО TLS-клиента необходим перезапуск TLS-клиента.

16. После обновления криптопровайдера необходима перезагрузка компьютера.

17. Нельзя добавлять ресурсы разных типов с одной комбинацией host port.

18. Не допускается присутствие в системе ключевых контейнеров с одинаковыми именами.

19. Если на компьютер установлен криптопровайдер "КриптоПро CSP", то проверка CRL осуществляется средствами TLS-клиента и средствами "КриптоПро CSP". Изменение настройки проверки CRL средствами TLS-клиента не влияет на настройки проверки CRL в криптопровайдере "КриптоПро CSP".

20. По умолчанию автоматическая проверка наличия актуальных обновлений ПО отключена.

21. Поддерживается совместимость с СКЗИ "КриптоПро CSP" версии не ниже 4.0.9944.0.

22. TLS-клиент поддерживает работу только с ключами, созданными с использованием параметров 1.2.643.2.2.35.1, 1.2.643.2.2.35.2, 1.2.643.2.2.35.3, 1.2.643.2.2.36.0, 1.2.643.2.2.36.1. Для проверки валидности сертификата откройте диалог просмотра свойства сертификата. Перейдите на вкладку "Состав" и выберите поле "Параметры открытого ключа". Убедитесь, что восьмой и девятый байты слева имеют значение "02". Если значение не совпадает, создайте запрос на другой сертификат или получите новый сертификат из внешних источников.

23. При необходимости форматирования ключевого контейнера КриптоПРО в формат PKCS#15 используйте утилиту CryptoProToPkcs15, которая поставляется на установочном диске. Описание работы утилиты приводится в файле Readme.txt.

24. В качестве ключевого носителя "Валидата CSP" использует только флеш-часть JaCarta.

25. Если на компьютере используется UEFI с возможностью включения/отключения опции безопасной загрузки Secure Boot, перед установкой TLS-клиента данную опцию необходимо отключить. В противном случае установка TLS-клиента завершится с ошибкой.

26. Если сертификат пользователя, выбранный для подключения по умолчанию, станет недействительным, при попытке подключения появится сообщение о невозможности использования данного сертификата, а само подключение установлено не будет. Имя невалидного сертификата и его статус будет отображаться в разделе "Управление сертификатами" на вкладке "Пользовательские сертификаты". Для установки подключения необходимо выбрать новый сертификат по умолчанию.

27. Указывать в настройках сертификат пользователя, выбранный для подключения по умолчанию, рекомендуется при подключении к ресурсам одного сервера. Если используются ресурсы от разных серверов, то данная настройка будет неактуальна.

28. С помощью TLS-клиента невозможно осуществить туннелирование SMB-трафика, добавив порт 445.

29. Если хотя бы один из ресурсов TLS-клиента является прокси, то корректная работа туннеля через порт 443 невозможна.

30. Добавлять ресурсы прокси для обычного ресурса и портала с одинаковым именем хоста и разными портами нельзя.

31. Если на компьютер установлен "Континент-АП" 4, то TLS-клиент надо устанавливать в папку по умолчанию. В противном случае могут возникнуть проблемы с проверкой контроля целостности (КЦ) для "Континент-АП".

32. Управление TLS-сервером через TLS-клиент может вызывать некоторые трудности при эксплуатации. Рекомендуется использовать "КриптоПро CSP" и Internet Explorer.

33. Если после обновления ПО ОС Windows TLS-клиент не запускается и на экране появляется сообщение об ошибке "В системе отображения конечных точек не осталось доступных конечных точек", проверьте, включена ли служба "Изоляция ключей CNG (KeyIso)". Если она отключена, включите ее с помощью вкладки "Службы и приложения" в "Управлении компьютера" или перезагрузите компьютер. Служба включится автоматически. После этого запустите TLS-клиент заново.

34. Если на компьютере установлены TLS-клиент версии 2.0 и сторонний криптопровайдер, то при установке "Континент-АП" 4.1 криптопровайдер "Код Безопасности CSP" установлен не будет. Наличие отметки о возможности совместной работы со сторонним криптопровайдером в процессе установки будет проигнорировано.

Компания "Код Безопасности"

Почтовый адрес:	115127, Москва, а/я 66
Телефон:	8 495 982-30-20
Факс:	8 495 744-29-31
E-mail:	info@securitycode.ru
Web:	https://www.securitycode.ru