Рутокен Коннект. Описание продукта

Рутокен Коннект — это программа и устройство из семейства Рутокен ЭЦП 2.0 для строгой безопасной двухфакторной аутентификации и шифрования канала с сайтами по ГОСТ алгоритмам, аналогично зарубежному HTTPS. Решение работает в Windows со стандартными браузерами Google Chrome, Mozilla Firefox, Яндекс.Браузером и браузером Спутник.

Рутокен Коннект использует USB-токен или смарт-карту как криптографическое средство строгой двухфакторной аутентификации и шифрования. В устройствах, работающих с Коннектом, российские криптографические алгоритмы реализованы в самом чипе “на борту”. Для взаимодействия с контекстом браузера используются технологии, позволяющие одинаково удобно подключаться к защищенным сайтам вне зависимости от используемой операционной системы или браузера.

Рутокен Коннект реализует следующие механизмы защиты информации:

- двухфакторную аутентификацию на веб-сервисе по аппаратному носителю;
- шифрование канала между компьютером пользователя и веб-сервисом по ГОСТ 28147-89;
- вычисление и проверку электронной подписи по ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (256 и 512 бит);
- вычисление сессионного ключа по VKO ГОСТ Р 34.10-2001 и VKO ГОСТ Р 34.10-2012 (256 и 512 бит);
- разграничение доступа к ресурсам веб-сервиса на основе цифровых сертификатов.

Установка и работа

Установщик Рутокен Коннекта реализован в виде MSI-пакета, не требующего прав администратора и выбора опций. Может быть установлен и настроен в полуавтоматическом режиме с минимальным участием пользователя.

Рутокен Коннект устанавливается и работает на Microsoft Windows 10/8.1/8/7 с правами обычного пользователя и использует только встроенные в браузеры Mozilla Firefox, Google Chrome, Спутник и другие на базе Chromium возможности и API.

Рутокен Коннект не требует установки сторонних средств проксирования, а также дополнительных компонентов, фреймворков и платформ, таких как Java, Microsoft Silverlight и др.

Состав продукта

Рутокен Коннект состоит из нативной части и расширения для браузеров Mozilla Firefox, Google Chrome, Спутник и другие на базе Chromium.

Поддерживаемые устройства

- Рутокен ЭЦП 2.0 и ЭЦП 2.0 Flash;
- Рутокен ЭЦП 2.0 Touch и ЭЦП 2.0 Flash Touch;
- Рутокен ЭПЦ PKI (ограниченная поддержка).

Поддерживаемые стандарты

- Подпись, проверка и вычисление ключа согласования по схеме VKO GOST 34.10-2001 и 34.10-2012 (256 и 512 бит).
- Шифрование по ГОСТ 28147-89.
- Формат цифрового сертификата X.509.
- Поддерживаемые шифронаборы: TLS_GOSTR341001_WITH_28147_CNT_IMIT, TLS_GOSTR341112_256_WITH_28147_CNT_IMIT, TLS_GOSTR341112_256_WITH_NULL_GOSTR3411