|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **УТВЕРЖДАЮ** |  | | | **УТВЕРЖДАЮ** | |
| » |  | | |  | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П.  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024 г. |  | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П.  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024 г. | |
|  |  | | |  | |
| **РАЗРАБОТКА ПРОГРАММНОЙ ДОКУМЕНТАЦИИ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**  Разработка средства удаленного доступа к отечественным ОС с использованием аппаратной криптографии через PKCS#11 | | | | |  |
|  | |  |  | |  |

Москва 2024

**СОДЕРЖАНИЕ**

[1 Общие сведения 3](#_Toc164808137)

[1.1 Обозначение и наименование программы 3](#_Toc164808138)

[1.2 Назначение программы 3](#_Toc164808139)

[1.3 Версия программы 3](#_Toc164808140)

[1.4 Разработчик 3](#_Toc164808141)

[1.5 Целевая аудитория 3](#_Toc164808142)

[2 Функциональность программы 3](#_Toc164808143)

[2.1 Основные и дополнительные функции 3](#_Toc164808144)

[2.2 Требования к аппаратному обеспечению 3](#_Toc164808145)

[2.3 Требования к программному обеспечению 5](#_Toc164808146)

[2.4 Интерфейс пользователя 9](#_Toc164808147)

[3 Архитектура программы 9](#_Toc164808148)

[3.1 Клиентская часть 9](#_Toc164808149)

[3.2 Серверная часть 9](#_Toc164808150)

[3 Документация пользователя 9](#_Toc164808151)

[3.1 Руководство пользователя 9](#_Toc164808152)

[3.2 Руководство администратора 9](#_Toc164808153)

[3.3 Техническое описание 9](#_Toc164808154)

[3.4 Лицензионное соглашение 9](#_Toc164808155)

# **1 Общие сведения**

## **Обозначение и наименование программы**

Средство удаленного доступа к отечественным операционным системам с использованием аппаратной криптографии через PKCS#11

## **1.2 Назначение программы**

Данная программа предназначена для обеспечения безопасного удаленного доступа к отечественным операционным системам с использованием аппаратной криптографии через стандарт PKCS#11.

## **1.3 Версия программы**

Текущая версия: **[Тут указывается версия]**

## **1.4 Разработчик**

Название компании: **[Тут указывается название компании]**

Контактная информация: **[Тут указывается контактная информация (данные)]**

## **1.5 Целевая аудитория**

Программа предназначена для использования системными администраторами и пользователями, которым необходим безопасный удаленный доступ к отечественным операционным системам.

# **2 Функциональность программы**

## **2.1 Основные и дополнительные функции**

Основные функции:

- Удаленное подключение к отечественным операционным системам

- Аутентификация пользователей с использованием аппаратной криптографии

- Шифрование и дешифрование данных с использованием PKCS#11

- Управление сеансами удаленного доступа

Дополнительные функции:

- Логирование событий и действий пользователей

- Управление правами доступа пользователей

- Мониторинг состояния сеансов удаленного доступа

- Восстановление сеансов после разрыва связи

- Шифрование трафика между клиентом и сервером

- Поддержка механизмов безопасности (например, TLS)

- Автоматическое обновление клиентского и серверного ПО

## **2.2 Требования к аппаратному обеспечению**

Таблица - Требования к аппаратному обеспечению (главное)

| **Критерий** | **Astra Linux** | **ОС «Альт»** | **«Ред ОС»** |
| --- | --- | --- | --- |
| **База** | Linux Debian | Linux, собственный репозиторий Sisyphus | Linux |
| **Версии** | ПК  Мобильная  Тонкий клиент  Сервер | | |
| **Архитектуры процессоров** | х86-64  Эльбрус  Байкал | | |
| ARM | х86-32  ARM  RISC-V  AArch64  ppc64le | i686  AArch64  Raspberry Pi  Huawei Kunpeng |
| **Минимальные системные требования** | CPU x86-64  RAM 1 Гб | | CPU 2 ядра 1,6 ГГц  RAM 2 Гб  HDD 20 Гб |
| HDD 4 Гб | HDD 16 Гб |
| **Сертификаты** | Реестр РФ  ФСТЭК России  ФСБ России | | |
| Минобороны РФ | | — |

Таблица - Требования к аппаратному обеспечению (альтернатива)

| **Критерий** | **«РОСА»** | **«ОСнова»** | **«Атлант»** |
| --- | --- | --- | --- |
| **База** | CentOS | Linux Debian | Linux |
| **Версии** | ПК  Сервер | | |
| Тонкий клиент | | — |
| Мобильная | — |
| **Архитектуры процессоров** | х86-64 | | |
| х86-32  ARM  Эльбрус  RISC-V | — | х86-32  ARM |
| **Минимальные системные требования** | CPU 1 ядро  RAM 1 Гб  HDD 10 Гб | CPU x86-64  RAM 1 Гб  HDD 16 Гб | CPU 1 ядро 1 ГГц  RAM 0,5 Гб  HDD 4 Гб |
| **Сертификаты** | Реестр РФ | | |
| ФСТЭК России | | — |

## **2.3 Требования к программному обеспечению**

Для работы с PKCS#11 требуется наличие специализированного программного обеспечения, которое обеспечивает взаимодействие с аппаратными устройствами для криптографии, поддерживающими данный стандарт. Это программное обеспечение позволяет управлять ключами, сертификатами, выполнить шифрование и дешифрование данных, аутентифицировать пользователей и другие операции, используя функционал PKCS#11.

Для удовлетворения этого требования необходимо установить специализированное ПО, которое поддерживает работу с PKCS#11. Обычно это включает в себя библиотеки или драйверы, предоставляемые производителями аппаратного обеспечения для криптографии. Также может потребоваться установка дополнительных компонентов или конфигурация операционной системы для корректной работы с PKCS#11.

Таблица – Поддерживаемые ОС

| **PKCS#11** | **Поддерживаемые ОС** |
| --- | --- |
| **Рутокен S** | * Microsoft Windows 11\*/2022\*/10\*/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее   \*Только при отключении функции Целостность памяти - [Изоляция ядра](https://dev.rutoken.ru/display/KB/DM1008) (Memory Integrity - Core Isolation) |
| **Рутокен Lite** | * Microsoft Windows 11/2022/10/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее * Android 5+   iOS\iPadOS 16.2 и новее |
| **Рутокен ЭЦП 2.0 (2000)** | * Microsoft Windows 11/2022/10/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее * Android 5+   iOS\iPadOS 16.2 и новее |
| **Рутокен ЭЦП 2.0 2100** | * Microsoft Windows 11/2022/10/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее * Android 5+   iOS\iPadOS 16.2 и новее |
| **Рутокен ЭЦП PKI** | * Microsoft Windows 11/2022/10/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее   iOS\iPadOS 16.2 и новее |
| **Рутокен ЭЦП 2.0 Flash** | * Microsoft Windows 11/2022/10/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее * Android 5+   iOS\iPadOS 16.2 и новее |
| **Рутокен ЭЦП 2.0 3000** | * Microsoft Windows 11/2022/10/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее * Android 5+   iOS\iPadOS 16.2 и новее |
| **Рутокен ЭЦП 3.0 3100** | * Microsoft Windows 11/2022/10/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее * Android 5+ * iOS\iPadOS 16.2 и новее   Аврора 4+ |
| **Рутокен ЭЦП 3.0 3220 (SD)** | * Microsoft Windows 11/2022/10/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее * Android 5+ * iOS\iPadOS 16.2 и новее   Аврора 4+ |
| **Рутокен ЭЦП 3.0 NFC 3100** | * Microsoft Windows 11/2022/10/2019/2016/8.1/8/2012R2/7/2008R2, * GNU/Linux, в том числе отечественные, * Apple macOS 10.9 и новее * Android 5+ * iOS\iPadOS 16.2 и новее - при контактном подключении * iOS 13 и новее (iPhone XR, XS, XS Max и новее) - при подключении по NFC   Аврора 4+ |

Таблица – Криптопровайдер

| **PKCS#11** | **Криптопровайдер** |
| --- | --- |
| **Рутокен S** | собственный Crypto Service Provider |
| **Рутокен Lite** | собственный Crypto Service Provider |
| **Рутокен ЭЦП 2.0 (2000)** | * собственный Crypto Service Provider * Microsoft Base Smart Card Crypto Provider * Microsoft Smart Card Key Storage Provider |
| **Рутокен ЭЦП 2.0 2100** | * собственный Crypto Service Provider * Microsoft Base Smart Card Crypto Provider * Microsoft Smart Card Key Storage Provider |
| **Рутокен ЭЦП PKI** | * собственный Crypto Service Provider * Microsoft Base Smart Card Crypto Provider * Microsoft Smart Card Key Storage Provider |
| **Рутокен ЭЦП 2.0 Flash** | * собственный Crypto Service Provider * Microsoft Base Smart Card Crypto Provider * Microsoft Smart Card Key Storage Provider |
| **Рутокен ЭЦП 2.0 3000** | * собственный Crypto Service Provider * Microsoft Base Smart Card Crypto Provider * Microsoft Smart Card Key Storage Provider |
| **Рутокен ЭЦП 3.0 3100** | * собственный Crypto Service Provider * Microsoft Base Smart Card Crypto Provider * Microsoft Smart Card Key Storage Provider |
| **Рутокен ЭЦП 3.0 3220 (SD)** | * собственный Crypto Service Provider * Microsoft Base Smart Card Crypto Provider * Microsoft Smart Card Key Storage Provider |
| **Рутокен ЭЦП 3.0 NFC 3100** | * собственный Crypto Service Provider * Microsoft Base Smart Card Crypto Provider * Microsoft Smart Card Key Storage Provider |

Криптографические возможности:

- Поддержка алгоритма ГОСТ 28147-89

- Поддержка алгоритмов ГОСТ Р 34.12-2015/ГОСТ Р 34.12-2018 - Магма и Кузнечик

- Поддержка алгоритма ГОСТ Р 34.10-2012

- Поддержка алгоритма ГОСТ Р 34.10-2001

- Поддержка алгоритма ГОСТ 34.11-2012 (256 и 512 бит)

- Поддержка алгоритма ГОСТ 34.11-94

- Выработка сессионных ключей (ключей парной связи)

- Расшифрование по схеме EC EI-Gamal

- Поддержка алгоритма RSA

- Поддержка алгоритма ECDSA

- Формирование электронной подписи

- Генерация ключевых пар

- Импорт ключевых пар

- Неизвлекаемость ключевых пар

- Размер ключей

- Поддержка алгоритмов DES (3DES), AES, RC2, RC4, MD4, MD5, SHA-1, SHA-256, SHA-384, SHA-512

- Работа с СКЗИ "КриптоПро 5.0" по протоколу защиты канала SESPAKE (ФКН2)

## **2.4 Интерфейс пользователя**

Программа предоставляет графический интерфейс пользователя для управления удаленным доступом и настройкой параметров безопасности.

# **3 Архитектура программы**

## **3.1 Клиентская часть**

- Интерфейс для взаимодействия с пользователем

- Реализация аутентификации через аппаратную криптографию

- Шифрование и дешифрование данных с использованием PKCS#11

- Управление сеансами удаленного доступа

## **3.2 Серверная часть**

- Прием и обработка запросов на удаленное подключение

- Аутентификация пользователей с использованием аппаратной криптографии

- Управление сеансами удаленного доступа

- Шифрование и дешифрование данных с использованием PKCS#11

# **3 Документация пользователя**

## **3.1 Руководство пользователя**

Документация пользователя содержит инструкции по установке программы, настройке параметров безопасности, аутентификации пользователей и использованию функций удаленного доступа.

## **3.2 Руководство администратора**

Документация администратора содержит инструкции по установке программы, настройке параметров безопасности, аутентификации пользователей и использованию функций удаленного доступа.

## **3.3 Техническое описание**

Документация содержит техническое описание программы, принципы работы с аппаратной криптографией через PKCS#11, требования к окружающей среде и рекомендации по безопасности.

## **3.4 Лицензионное соглашение**

Документация включает лицензионное соглашение, определяющее условия использования программы.