

Системные требования

ИТ-инфраструктура компании должна соответствовать минимальным требованиям:

- [к серверным компонентам](#);
- [к клиентским компонентам](#);
- [к сетевому взаимодействию](#).

Рутокен KeyBox поддерживает определенный [список устройств аутентификации](#).

Требования к серверным компонентам

Аппаратные требования

- Не менее 8 ГБ оперативной памяти
- Не менее 50 ГБ свободного дискового пространства
- Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО

Программные требования

Операционная система:

- Windows Server 2008 SP2 x64 (с обновлением KB980368)
- Windows Server 2008 R2 SP1
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Языком программ, не поддерживающих Юникод должен быть русский, независимо от основного языка операционной системы.

- Debian 9 - 11
- Astra Linux Special Edition 1.6 - 1.7
- Ubuntu 18.04 LTS - 20.04 LTS
- Red Hat Enterprise Linux 7 - 9
- CentOS 7
- CentOS Stream 8 - 9
- РЕД ОС 7.2 - 7.3

Веб-сервер:

- Internet Information Services 7.0 и выше для следующих ОС.

Для быстрой установки Internet Information Services с требуемыми модулями используйте скрипт PowerShell из дистрибутива системы (скрипт располагается в каталоге \\IIS.Setup.Scripts).

Для развертывания сервера RutokenKeyBox необходимо выполнить установку Microsoft .NET Framework 4.5 и Microsoft .NET Core 3.1 после установки и настройки компонентов Internet Information Services (IIS).

- Nginx 1.22.1 и выше в качестве обратного прокси-сервера (Reverse Proxy) для ОС Linux.
- Apache 2.4.25 и выше в качестве обратного прокси-сервера (Reverse Proxy) ОС Linux.

Дополнительные компоненты Microsoft:

- Microsoft .NET Core 3.1
- Microsoft .NET Framework 4.5 и выше

Компоненты КриптоПро:

- КриптоПро CSP 4.0R4 и выше (в случае использования с Microsoft Enterprise CA, настроенного на выпуск сертификатов по алгоритмам ГОСТ Р34.10-2001/2012, КриптоПро УЦ 2.0, Валидата УЦ)
- КриптоПро CSP 5.0 и выше (в случае использования с КриптоПро DSS 2.0)

В случае использования TLS-соединения между сервером Рутокен KeyBox и Центрами Регистрации КриптоПро, и Валидата УЦ, защищенного в соответствии с Государственными Стандартами РФ, необходимо наличие серверной лицензии КриптоПро CSP.

Требования к окружению

Каталог пользователей:

- Active Directory
- Центр Регистрации КриптоПро УЦ 2.0

Центр сертификации:

- Центр сертификации предприятия Microsoft (Microsoft Enterprise CA), в том числе настроенного на выпуск сертификатов с использованием КриптоПро CSP:
 - на базе Windows Server 2003 и 2008 начиная с редакции Enterprise
 - на базе Windows Server 2012/2012 R2 всех редакций
 - на базе Windows Server 2016 всех редакций
 - на базе Windows Server 2019 всех редакций
- КриптоПро УЦ 2.0
- Валидата УЦ версии 3.1, 4.0

Хранилище данных:

- СУБД Microsoft SQL Server 2012 SP2 и выше всех редакций
- СУБД PostgreSQL версии 10 и выше
- СУБД Postgres Pro Standard, Postgres Pro Enterprise версии 11 и выше

Поддерживаемые поставщики службы криптографии (CSP):

RSA

- CSP производителя устройства (Рутокен, eToken и т.д.)
- Microsoft Base Smart Card Cryptographic Service Provider (если CSP не предоставляется производителем устройства)

Поддерживается в том числе и в связке с УЦ КриптоПро 2.0.

ГОСТ Р34.10-2001/2012

- КриптоПро CSP 4.0R4 и выше
- Аппаратная криптография Рутокен ECP 2.0, Рутокен ECP 3.0 NFC, Рутокен 2151, JaCarta ГОСТ, JaCarta-2 ГОСТ, ESMART Token ГОСТ, MS_KEY К-"Ангара"

Поддерживается в том числе и в связке с Microsoft Enterprise CA.

Требования к клиентским компонентам

Аппаратные требования

- Не менее 300 МБ свободного дискового пространства
- Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО

Программные требования

Операционная система:

- Windows Vista SP2 x86/x64
- Windows 7 SP1 x86/x64
- Windows 8/8.1 x86/x64
- Windows 10 x86/x64
- Windows 11 x86/x64
- Windows Server 2008 SP2 x86/x64 (с обновлением KB980368)
- Windows Server 2008 R2 SP1
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Debian 9 - 11
- Astra Linux Special Edition 1.6 - 1.7
- Astra Linux Common Edition 2.12
- Ubuntu 18.04 LTS и выше
- Red Hat Enterprise Linux 8 - 9
- CentOS 7

- CentOS Stream 8 - 9
- РЕД ОС 7.3
- Альт Рабочая станция 9 - 10

Требования к окружению:

- Установленные драйверы (PKI-менеджеры) используемых устройств (смарт-карт, USB-токенов)
- Microsoft Internet Explorer 11
- Microsoft Edge 41.16299 и выше
- Mozilla Firefox 60.0.2 и выше
- Google Chrome или Chromium 88.0 и выше
- Яндекс.Браузер 21.3.0 и выше
- КриптоПро CSP 4.0R4 и выше (в случае выпуска сертификатов с Microsoft Enterprise CA по алгоритмам ГОСТ Р34.10-2001/2012, КриптоПро УЦ 2.0, Валидата УЦ)
- КриптоПро CSP 5.0 и выше (в случае использования с КриптоПро DSS 2.0)

Требования к сетевому взаимодействию

Порты, используемые сервером RutokenKeyBox

Веб-приложения, HTTP, HTTPS

- 80 (TCP), входящие и исходящие подключения.
- 443 (TCP), входящие и исходящие подключения.
- 3001/3002 (TCP), входящие и исходящие подключения для компонента Rutoken KeyBox AirCard Enterprise.
- 3003 (TCP), входящие и исходящие подключения для компонента Rutoken KeyBox Агент.

Почтовые уведомления, SMTP сервер

- 25 (TCP), исходящие подключения.
- 465 (TCP), исходящие подключения.
- 587 (TCP), исходящие подключения.

Active Directory, входящие и исходящие подключения

- 53 (TCP/UDP), исходящие подключения — DNS.
- 135 (TCP) — NetBIOS.
- 389 (TCP/UDP) — LDAP.
- 636 (TCP) — LDAPS.
- 3268 (TCP/UDP) — Microsoft Global Catalog.
- 3269 (TCP) – LDAP Global Catalog SSL.
- 88 (TCP/UDP) — Kerberos.
- 464 (TCP/UDP) — Kerberos.

SQL Server, входящие и исходящие

- 135 (TCP) — Transact-SQL debugger.
- 1433 (TCP) — SQL Server default instance.
- 1434 (UDP) — SQL Server Browser service.
- 4022 (TCP) — Service Broker.

PostgreSQL Server, входящие и исходящие

- 5432 (TCP/UDP) — PostgreSQL default port.

Microsoft Enterprise CA, входящие и исходящие

- 135 (TCP) — NetBIOS.
- 389 (TCP) — LDAP.
- 636 (TCP) — LDAPS.
- Случайный DCOM/RPC (TCP) порт верхнего диапазона:
 - 1024 - 5000 для MS CA на базе Windows 2003 и более ранних версий;
 - 49152 - 65535 для MS CA на базе Windows 2008 и более новых версий.

Microsoft CA реализован с помощью технологии DCOM. По умолчанию приложения DCOM используют случайные номера TCP портов верхнего диапазона. Также существует возможность настроить удостоверяющий центр на использование жестко заданного TCP порта.

КриптоПро УЦ 2.0, входящие и исходящие

- 443 (TCP) — Центр Регистрации КриптоПро УЦ 2.0.

КриптоПро DSS 2.0, входящие и исходящие

- 443 (TCP) — Центр идентификации КриптоПро DSS.

Валидата УЦ, входящие и исходящие

- 13434 (TCP) — Порт по умолчанию для RPC сервера Центра Регистрации Валидата УЦ (в случае онлайн-режима работы).

Indeed Access Manager

- 80 (TCP), входящие и исходящие подключения.
- 443 (TCP), входящие и исходящие подключения.

Secret Net Studio, входящие и исходящие

- 135 (TCP) — RPC.
- 443 (TCP) — Сервер безопасности.
- 389 (TCP/UDP) — LDAP.
- 636 (TCP) — LDAPS.
- 5355 (TCP/UDP) — Link-Local Multicast Name Resolution (LLMNR)
- 50000/50001 (TCP) — Secret Net LDS.
- 50002/50003 (TCP) — Secret Net-GC LDS.

Порты, используемые рабочими станциями пользователей и операторов Рутокен KeyBox

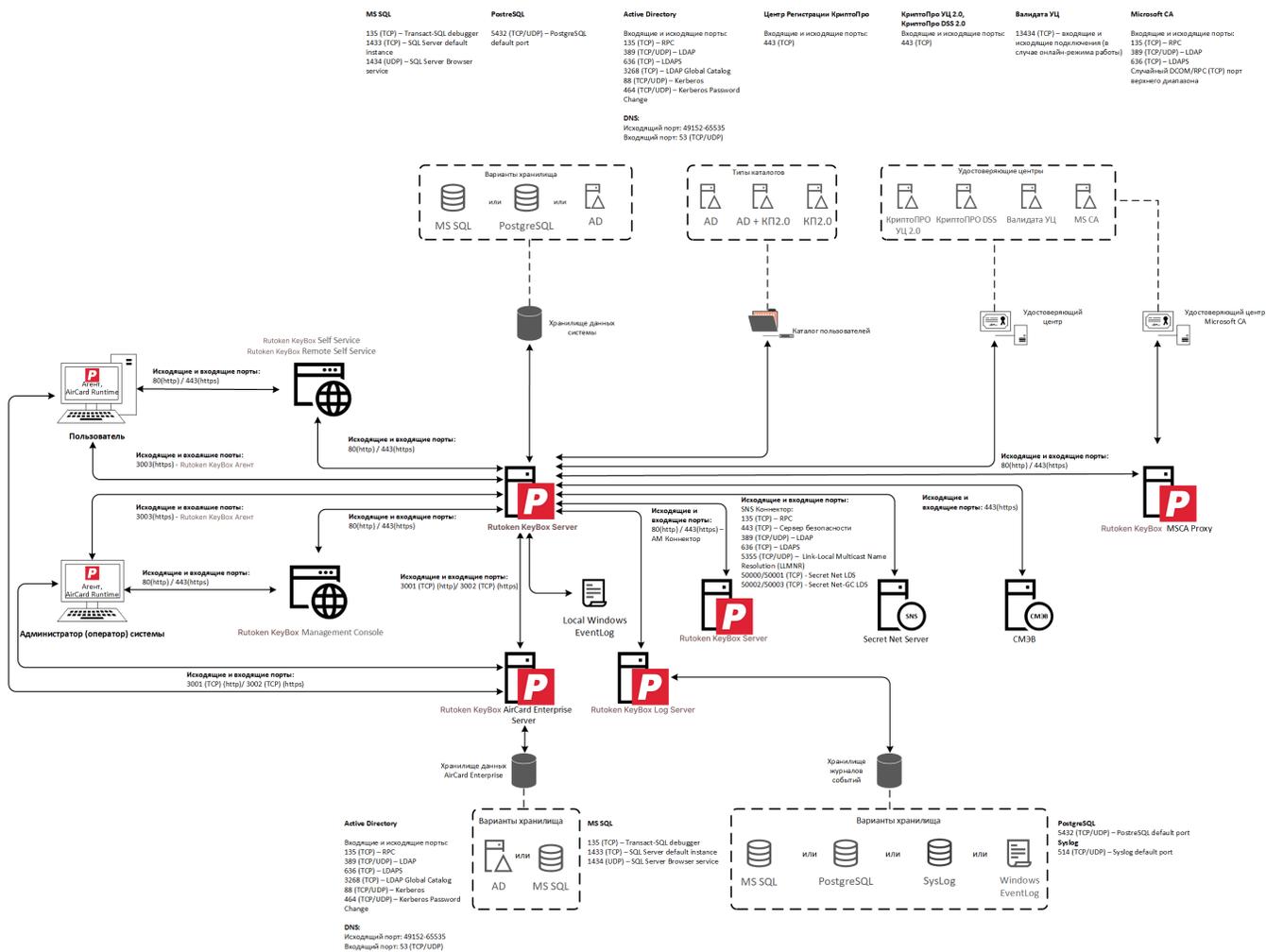
DNS

- 53 (TCP/UDP), исходящие подключения.

Веб-приложения, HTTP, HTTPS

- 80 (TCP), входящие и исходящие подключения.
- 443 (TCP), входящие и исходящие подключения.
- 3001/3002 (TCP), входящие и исходящие подключения для Rutoken KeyBox AirCard Enterprise
- 3003 (TCP), входящие и исходящие подключения для компонента Rutoken KeyBox Агент.

Схема сетевого взаимодействия



Список поддерживаемых устройств аутентификации

ОС Linux	
Производитель	Модель
Аладдин Р.Д.	JaCarta PKI
	JaCarta PKI/Flash
	JaCarta PKI/BIO
	JaCarta PKI/ГОСТ
	JaCarta PKI/ГОСТ/Flash
	JaCarta-2 PKI/ГОСТ
	JaCarta-2 PKI/ГОСТ/Flash
	JaCarta-2 SE

Компания «Актив»	<p>Рутокен Lite и смарт-карта Рутокен Lite</p> <p>Рутокен ЭЦП PKI и смарт-карта Рутокен ЭЦП PKI</p> <p>Рутокен ЭЦП 2.0 и смарт-карта Рутокен ЭЦП 2.0</p> <p>Рутокен 2151 и смарт-карта Рутокен 2151</p> <p>Рутокен ЭЦП 3.0 NFC и смарт-карта Рутокен ЭЦП 3.0 NFC</p>
ОС Windows	
Производитель	Модель
Аладдин Р.Д.	<p>JaCarta PKI</p> <p>JaCarta PKI/Flash</p> <p>JaCarta PKI/BIO</p> <p>JaCarta PKI/ГОСТ</p> <p>JaCarta PKI/ГОСТ/Flash</p> <p>JaCarta-2 PKI/ГОСТ</p> <p>JaCarta-2 PKI/ГОСТ/Flash</p> <p>JaCarta-2 SE</p>
Компания «Актив»	<p>Рутокен S</p> <p>Рутокен Lite и смарт-карта Рутокен Lite</p> <p>Рутокен ЭЦП PKI и смарт-карта Рутокен ЭЦП PKI</p> <p>Рутокен ЭЦП 2.0 и смарт-карта Рутокен ЭЦП 2.0</p> <p>Рутокен 2151 и смарт-карта Рутокен 2151</p> <p>Рутокен ЭЦП 3.0 NFC и смарт-карта Рутокен ЭЦП 3.0 NFC</p>
Компания Индид	Сетевая смарт-карта AirCard
ACS	ACOS5-64
Avest	Avest Key 256A
Bit4id	ID-One Cosmo
CRYPTAS	TicTok V2/V3
Cryptovision	ePasslet Suite v3.0, JCOP V3.0
Feltian	<p>ePass2003 (A1+, A2)</p> <p>BioPass2003</p>
HID	<p>Crescendo C1150 Series</p> <p>Crescendo C1300 Series</p> <p>Crescendo C2300 Series</p>
ISBC	<p>ESMART Token 64K и ESMART Token SC 64K</p> <p>ESMART Token ГОСТ и ESMART Token SC ГОСТ</p> <p>MS_KEY К-"Ангара"</p>
Kaztoken	Kaztoken, Kaztoken SC

Microsoft	<p>Реестр Локального компьютера</p> <p>Реестр Пользователя</p> <p>TPM Virtual Smart Card (Microsoft VSC) - виртуальная смарт-карта на базе Trusted Platform Module v.2.0</p> <p>Windows Hello for Business (WHfB)</p>
RSA	RSA SecurID 800
Thales Group (Ex SafeNet and Gemalto)	<p>SafeNet eToken PRO 32k</p> <p>SafeNet eToken PRO 64k</p> <p>eToken PRO Java 72K OS755</p> <p>SafeNet eToken 5105</p> <p>SafeNet eToken 5110</p> <p>IDCore30B eToken 1.7.7</p> <p>IDPrime MD 830</p> <p>IDPrime MD 840</p> <p>IDPrime MD 3810</p> <p>IDPrime MD 3811</p>
Yubico	YubiKey 5 Series