

iMobile

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«RDP-FIDO-GATE»

Версия 1.25.1

**Сведения о соответствии требованиям законодательства
Российской Федерации**

IM.RDP-FIDO.RU.06

Листов 11

АННОТАЦИЯ

Настоящий документ дополняет комплект документации программы «RDP-FIDO-GATE» версии 1.25.1 сведениями, существенными при поставке и применении программы в Российской Федерации: о составе документации, о статусе программы в едином реестре российских программ, об обработке персональных данных и о средствах защиты информации.

Документ содержит сведения поставщика о программе. Он не является сертификатом соответствия, заключением экспертизы или юридической консультацией и не заменяет оценку, которую проводит сам заказчик.

СОДЕРЖАНИЕ

1. Общие сведения	4
1.1. Персональные данные, которые может обрабатывать программа	4
1.2. Место хранения данных	4
1.3. Сведения, передаваемые поставщику	5
2. Состав и оформление документации	5
3. Единый реестр российских программ	6
4. Обработка персональных данных	6
4.1. Роли	6
4.2. Размещение баз данных на территории Российской Федерации	6
4.3. Трансграничная передача	7
4.4. Что предоставляет программа	7
4.5. Что остаётся за оператором	8
5. Защита информации	8
5.1. Криптография	8
6. Использование искусственного интеллекта	9
7. Что обычно требует договор и где это находится	9
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	11

1. ОБЩИЕ СВЕДЕНИЯ

Сведение	Значение
Наименование и версия	RDP-FIDO-GATE 1.25.1
Способ развёртывания	Клиентская и серверная части, устанавливаются на оборудовании заказчика
Обработка содержимого заказчика на серверах поставщика	Нет
Языки интерфейса	Клиент и установщики для Windows: русский, английский, немецкий, французский, испанский, китайский. Клиент для Linux: русский, английский. Клиент для Android: английский, русский. Командная строка и журнал шлюза: английский. Веб-кабинет хаба: русский, английский.

1.1. Персональные данные, которые может обрабатывать программа

- В клиенте: адреса и названия компьютеров, имена пользователей и домены, сохранённые пароли сессий (в зашифрованном виде), снимки экрана удалённых рабочих столов для плиток, заметки
- В клиенте для Windows: адрес электронной почты учётной записи и токен активации
- В консоли SSH: сохранённые пароли и команды, заметки для помощника, история разговоров с помощником (может содержать текст терминала)
- На шлюзе: названия и открытые ключи зарегистрированных ключей FIDO2, секреты одноразовых кодов, счётчики и время использования, IP-адреса клиентов в журнале
- На хабе: идентификаторы и имена компьютеров привязанных шлюзов, IP-адреса клиентов, учётные записи кабинета (логин, имя, хеш пароля), журнал событий
- Учётному серверу поставщика клиент для Windows передаёт: адрес электронной почты, идентификатор установки, версию и язык клиента, события показа и нажатия рекламной плитки; сервер хранит учётную запись и её редакцию

1.2. Место хранения данных

Данные хранятся локально на оборудовании заказчика. Клиент для Windows — каталог %LOCALAPPDATA%\RdpFidoClient (sessions.json, thumbs, account.json, console.json, console-chats.json, applock.dat, client.log). Шлюз для Windows — %ProgramData%\RdpFidoGate (gate.json, enrollment.json, gate.log), доступ только у SYSTEM и администраторов. Клиент для Linux — ~/.config/rdpfido (права 0600), пароли — в связке ключей рабочего стола. Шлюз для Linux — /var/lib/rdpfido-gate (доступ только root). Клиент для Android — закрытый каталог приложения. Хаб — /var/lib/rdpfido-cloud. У поставщика хранятся только сведения учётной записи, перечисленные в разделе об активации.

1.3. Сведения, передаваемые поставщику

- Клиент для Windows → учётный сервер, запрос кода активации: адрес электронной почты, идентификатор продукта, язык интерфейса
- Клиент для Windows → учётный сервер, активация: адрес электронной почты, код из письма, идентификатор продукта
- Клиент для Windows → учётный сервер, условия редакции (раз в час, а пока показывается рекламная плитка — раз в 10 минут): токен учётной записи, идентификатор продукта, версия клиента, язык интерфейса, идентификатор установки
- Клиент для Windows → учётный сервер, статистика рекламной плитки (только редакция Free): токен учётной записи, идентификатор продукта, тип события (показ или нажатие), идентификатор объявления; загрузка картинок объявлений
- Клиент для Windows → учётный сервер, проверка обновлений: идентификатор продукта и версия клиента; загрузка файлов обновления
- При каждом обращении учётный сервер видит IP-адрес клиента
- Шлюз, клиенты для Linux и Android, хаб и реле поставщику ничего не передают

2. СОСТАВ И ОФОРМЛЕНИЕ ДОКУМЕНТАЦИИ

Документация поставляется на русском языке. Состав документов определён с учётом стандартов Единой системы программной документации (ГОСТ 19) и требований к документам, представляемым для включения сведений о программе в единый реестр российских программ (постановление Правительства Российской Федерации от 16.11.2015 № 1236).

Документ комплекта	Чему соответствует
Описание функциональных характеристик	ГОСТ 19.502-78 «Описание применения»; описание функциональных характеристик по правилам реестра
Руководство по установке и администрированию	ГОСТ 19.503-79 «Руководство системного программиста»; сведения, необходимые для установки и эксплуатации, по правилам реестра
Руководство пользователя	ГОСТ 19.505-79 «Руководство оператора»
Описание процессов, обеспечивающих поддержание жизненного цикла программы	Описание процессов жизненного цикла, устранения неисправностей и совершенствования, сведения о персонале по правилам реестра
Спецификация поставки и сведения о сторонних компонентах	ГОСТ 19.202-78 «Спецификация»

Документы оформлены с учётом ГОСТ 19.105-78 и ГОСТ 19.106-78: титульный лист, аннотация, содержание, лист регистрации изменений. Программа и методика испытаний (ГОСТ 19.301-79) в комплект не входит и составляется по требованиям конкретного договора.

3. ЕДИНЫЙ РЕЕСТР РОССИЙСКИХ ПРОГРАММ

На дату выпуска настоящего документа сведения о программе в единый реестр российских программ для электронных вычислительных машин и баз данных не внесены.

Из этого следует:

- при закупках по федеральным законам № 44-ФЗ и № 223-ФЗ действует запрет на допуск программного обеспечения, происходящего из иностранных государств (постановление Правительства Российской Федерации от 23.12.2024 № 1875); российское происхождение программы подтверждается номером реестровой записи, поэтому до внесения программы в реестр поставка лицензий по таким закупкам возможна только там, где запрет не применяется;
- государственным органам и заказчикам, закупаящим по Федеральному закону № 223-ФЗ, запрещено использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры (Указ Президента Российской Федерации от 30.03.2022 № 166).

Документы комплекта подготовлены в составе, который требуется для подачи заявления о включении сведений о программе в реестр.

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

К обработке персональных данных с помощью программы применяется Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

4.1. Роли

При установке на оборудовании заказчика оператором персональных данных, обрабатываемых в программе, является заказчик. Поставщик доступа к этим данным не имеет и их обработку не осуществляет.

Сведения, перечисленные в подразделе «Сведения, передаваемые поставщику», поставщик обрабатывает как оператор в целях исполнения лицензионного договора.

4.2. Размещение баз данных на территории Российской Федерации

При сборе персональных данных граждан Российской Федерации оператор обеспечивает их запись, систематизацию, накопление, хранение, уточнение и извлечение с использованием баз данных, находящихся на территории Российской Федерации (часть 5 статьи 18).

Программа хранит данные там, где она установлена. Размещение баз данных на территории Российской Федерации обеспечивается выбором места установки и относится к обязанностям заказчика.

4.3. Трансграничная передача

Если серверы, на которые передаются сведения, расположены за пределами Российской Федерации, передача персональных данных на них является трансграничной (статья 12 Федерального закона № 152-ФЗ); оператор уведомляет о ней Роскомнадзор до начала передачи. Место размещения серверов поставщика: указывается в договоре.

4.4. Что предоставляет программа

- **Разграничение доступа.** Доступ к защищаемому порту открывается после проверки на шлюзе: ключом FIDO2 (подпись вызова, идентификатор проверяющей стороны, счётчик подписей, признак присутствия пользователя и, если включено, проверки PIN или биометрии) либо, если шлюз настроен на коды, одноразовым кодом TOTP. Способ один на шлюз. Ключ регистрируется по одноразовому коду регистрации, который администратор получает на шлюзе (действует 15 минут). Доступ выдаётся только адресу, прошедшему проверку, на заданное окно (по умолчанию 90 секунд, не более 600). Неудачные попытки ограничиваются: 8 за 5 минут с адреса — блокировка адреса на 5 минут. Можно ограничить страны по локальной таблице адресов. Ролей пользователей на шлюзе нет, кроме роли ключа в общем сеансе FIDO Stream («управлять» или «только смотреть»). Командами шлюза управляет администратор операционной системы. После открытия порта вход на компьютер проверяет сама операционная система (учётная запись и пароль). Клиент можно закрыть мастер-паролем или ключом FIDO2. Кабинет хаба имеет учётные записи с ролями владельца, администратора, аудитора и пользователя.
- **Журналирование.** Шлюз ведёт текстовый журнал `gate.log` (в Linux дополнительно журнал `systemd`): регистрация ключей с адресом, каждое открытие и закрытие доступа с адресом и названием ключа, отклонённые попытки и причины, срабатывания ограничений, изменения состояния защиты, обновления. Журнал ограничен 4 МБ, хранится один предыдущий файл. Клиент ведёт `client.log` (обращения к шлюзам и ошибки). Хаб ведёт журнал службы и журнал событий кабинета по дням (хранится 90 дней). Записи в журнал событий Windows, отправки в syslog или SIEM и защиты журналов от изменения нет.
- **Выгрузка и удаление данных.** Данные хранятся в файлах JSON и текстовых журналах в перечисленных каталогах и копируются средствами операционной системы; отдельной функции выгрузки нет. Удаление: сессия удаляется в клиенте вместе с сохранённым паролем и снимком; ключ на шлюзе — командой `remove-key`; все данные — удалением каталога данных после удаления программы (каталоги данных при удалении программы сохраняются; каталог шлюза для Linux удаляет `purge` пакета `deb`). Функции удаления учётной записи на учётном сервере в клиенте нет: такой запрос направляется поставщику.

4.5. Что остаётся за оператором

- определение целей и правовых оснований обработки (статья 6), уведомление Роскомнадзора об обработке (статья 22);
- определение уровня защищённости персональных данных (постановление Правительства Российской Федерации от 01.11.2012 № 1119) и выбор мер защиты по требованиям ФСТЭК России к защите персональных данных в информационных системах;
- рассмотрение обращений субъектов персональных данных с использованием средств выгрузки и удаления, названных выше;
- уведомление Роскомнадзора об инцидентах с персональными данными в сроки, установленные частью 3.1 статьи 21.

5. ЗАЩИТА ИНФОРМАЦИИ

Программа не является сертифицированным средством защиты информации: сертификаты ФСТЭК России и ФСБ России на неё не оформлялись. В государственных информационных системах, на значимых объектах критической информационной инфраструктуры и в иных случаях, когда нормативные акты требуют средств защиты, прошедших оценку соответствия, программа применяется совместно с такими средствами.

5.1. Криптография

В программе применяется следующая криптография:

- Подтверждение входа: FIDO2 / WebAuthn; шлюз проверяет подписи ECDSA (P-256, P-384, P-521, с SHA-256/384/512) и RSA (PKCS#1 v1.5 с SHA-256/384/512, PSS с SHA-256); ключи EdDSA не принимаются. Подтверждение (attestation) модели ключа не проверяется
- Одноразовые коды: TOTP по RFC 6238 — HMAC-SHA1, шаг 30 секунд, 6 цифр, секрет 160 бит
- Канал клиент — шлюз: HTTPS с самоподписанным сертификатом шлюза, который клиент закрепляет по отпечатку SHA-256; клиенты для Windows и Linux допускают только TLS 1.2 и 1.3. Шлюз для Windows: сертификат RSA 2048 бит (SHA-256), TLS средствами Windows (http.sys, Schannel). Шлюз для Linux: сертификат ECDSA P-256, OpenSSL 3, TLS не ниже 1.2, в TLS 1.2 только наборы ECDHE с AES-GCM или ChaCha20-Poly1305
- FIDO Stream: согласование ключей ECDH P-256, вывод ключей HKDF-SHA256 с привязкой к билету шлюза, шифрование каждой датаграммы AES-256-GCM, защита от повторов
- Хаб: рукопожатие с HMAC-SHA256 общего секрета и эфемерным ECDH P-256, записи AES-256-GCM; TLS клиента и шлюза хаб не расширяет
- Сохранённые пароли: Windows — DPAPI учётной записи пользователя; Linux — связка ключей рабочего стола; Android — AES-GCM с ключом в хранилище ключей Android

- Мастер-пароль (защита входа): случайный ключ 256 бит, которым пароли шифруются AES-256-GCM; ключ хранится обёрнутым производным от пароля ключом PBKDF2-HMAC-SHA256, 600 000 итераций
- Обновления и условия редакции: подпись ECDSA P-256 учётного сервера, контрольные суммы SHA-256
- Хеширование: коды регистрации хранятся как SHA-256 с солью; пароли учётных записей кабинета хаба — PBKDF2-HMAC-SHA256, 200 000 итераций
- Реализации: Windows CNG и DPAPI; OpenSSL 3 в Linux; javax.crypto и хранилище ключей Android. Алгоритмы ГОСТ не применяются. Криптография служит аутентификации и защите собственных каналов и данных программы

Программа не является средством криптографической защиты информации, сертифицированным ФСБ России. Там, где законодательство требует применения сертифицированных средств криптографической защиты, программа используется совместно с ними.

6. ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Программа использует большие языковые модели следующим образом. Помощник в консоли SSH (клиенты для Windows и Linux) предлагает команды в ответ на вопрос пользователя. Он обращается к сервису, который указал сам пользователь: Claude API или сервер, совместимый с OpenAI, в том числе локальный. Модель в состав программы не входит, серверы поставщика в этом обмене не участвуют. Текст терминала (последние 200 строк экрана с каждым вопросом) передаётся модели только при включённом флажке «Видит консоль».

- Если поставщик моделей расположен за пределами Российской Федерации, а передаваемое содержимое включает персональные данные, такая передача является трансграничной (статья 12 Федерального закона № 152-ФЗ).
- Результат работы модели проверяется человеком до его использования.

7. ЧТО ОБЫЧНО ТРЕБУЕТ ДОГОВОР И ГДЕ ЭТО НАХОДИТСЯ

Что обычно требуется	Где находится
Описание функциональных характеристик	Одноимённый документ комплекта
Инструкция по установке и эксплуатации	Руководство по установке и администрированию
Руководство пользователя на русском языке	Руководство пользователя
Сведения о технической поддержке и обновлениях	Описание процессов, обеспечивающих поддержание жизненного цикла программы; сроки — в договоре
Комплектность, системные требования, сторонние компоненты	Спецификация поставки и сведения о сторонних компонентах
Номер записи в реестре российского программного обеспечения	Отсутствует: сведения о программе в реестр не внесены
Сертификаты ФСТЭК России, ФСБ России	Отсутствуют

Что обычно требуется	Где находится
Программа и методика испытаний	В комплект не входит, составляется по требованиям договора
Лицензионный договор, гарантии, цена, реквизиты правообладателя	Договор

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Версия документа	Дата	Версия программы	Содержание изменения
1.0	2026-10-06	1.25.1	Первая редакция документа