

iMobile

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«RDP-FIDO-GATE»

Версия 1.25.1

Описание функциональных характеристик

IM.RDP-FIDO.RU.01

Листов 11

АННОТАЦИЯ

Настоящий документ описывает функциональные характеристики программы RDP-FIDO-GATE: назначение, состав, функции, интерфейсы, применяемую криптографию, редакции и известные ограничения. Документ предназначен для специалистов заказчика, оценивающих программу перед закупкой и вводом в эксплуатацию, в том числе для специалистов по защите информации.

Описаны выпущенные версии: шлюз и клиент для Windows 1.25.0, пакеты для Linux 1.25.1, клиент для Android 0.9.1 (предварительная бета-версия), хаб 1.22.0.

СОДЕРЖАНИЕ

1. Общие сведения	4
1.1. Наименование и версии	4
1.2. Назначение	4
1.3. Область применения	4
1.4. Класс программы	4
2. Функциональные возможности	5
2.1. Заккрытие порта и допуск по второму фактору	5
2.2. Проверки при подтверждении входа	5
2.3. Регистрация ключей и вход по одноразовому коду	5
2.4. Клиент	6
2.5. FIDO Stream	6
2.6. Консоль SSH	7
2.7. Работа через хаб	7
3. Архитектура и состав	7
4. Интерфейсы и обмен данными	8
4.1. Сетевые протоколы	8
4.2. Программные интерфейсы и форматы	8
4.3. Обмен с серверами поставщика	8
4.4. Применяемая криптография	8
5. Редакции и ограничения	9
5.1. Редакции	9
5.2. Известные ограничения	9
6. Требования к среде	10
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	11

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование и версии

Наименование программы — RDP-FIDO-GATE. В интерфейсе и в именах файлов используются названия RDP FIDO (клиент), RDP FIDO Gate (шлюз) и rdpfido (программы для Linux).

Составная часть	Платформа	Версия	Дата выпуска
Шлюз RDP FIDO Gate и клиент RDP FIDO Client	Windows	1.25.0	05.10.2026
Шлюз rdpfido-gate и клиент rdpfido	Linux	1.25.1	06.10.2026
Клиент RDP FIDO (предварительная бета-версия)	Android	0.9.1	06.10.2026
Хаб rdpfido-cloud и реле rdpfido-relay	Linux	1.22.0	28.09.2026

Выпуск 1.25.1 содержит только пакеты для Linux; сборки для Windows с этим номером нет.

1.2. Назначение

Программа предназначена для защиты удалённого доступа к компьютерам. Шлюз держит порт удалённого рабочего стола (RDP) закрытым в сетевом экране самого компьютера и открывает его на короткое время только тому сетевому адресу, с которого предъявлен зарегистрированный на этом шлюзе ключ безопасности FIDO2 или, если шлюз так настроен, одноразовый код из приложения-аутентификатора. Шлюз для Linux тем же способом защищает SSH и другие заданные TCP-порты.

1.3. Область применения

Удалённое администрирование серверов и рабочих станций, удалённая работа сотрудников, доступ подрядчиков к отдельным компьютерам — там, где порт RDP или SSH доступен из сети общего пользования или из сети с пониженным доверием. Все части программы устанавливаются на оборудовании заказчика. Проверка ключа и подключение выполняются без участия серверов поставщика; клиенту для Windows серверы поставщика нужны для активации и получения обновлений.

1.4. Класс программы

Программа управления удалённым доступом с многофакторной аутентификацией: сетевой шлюз доступа и клиентские программы подключения. Сертификатов соответствия требованиям безопасности информации (ФСТЭК России, ФСБ России, FIDO Alliance и иных) программа не имеет.

2. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

2.1. Заккрытие порта и допуск по второму фактору

- Шлюз для Windows отключает разрешающие правила брандмауэра Windows для порта RDP, после чего входящие соединения блокируются профилем по умолчанию. Шлюз для Linux создаёт собственную таблицу nftables (если nftables в системе нет — цепочки iptables и ip6tables) с запретом порта для IPv4 и IPv6.
- После успешной проверки шлюз создаёт разрешающее правило для одного адреса на окно доступа: по умолчанию 90 секунд, не более 600. Окно ограничивает начало соединения. Установленный сеанс не разрывается: правило сохраняется, пока сеанс активен (но не дольше суток), и снимается после его завершения.
- Каждые 30 секунд шлюз проверяет свои правила и восстанавливает их; шлюз для Windows включает брандмауэр, если его выключили. В Linux правила ставятся при загрузке до запуска сети и сервера xrdp; если поставить их не удалось, xrdp не запускается.
- Порт закрывается не при установке шлюза, а в момент регистрации первого ключа. Защиту можно аварийно снять командой `unlock` и вернуть командой `arm`.

2.2. Проверки при подтверждении входа

Перед открытием доступа шлюз проверяет:

- принадлежность адреса разрешённой стране, если задан список стран;
- подпись ключа по открытому ключу, сохранённому при регистрации;
- что запрос подтверждения (challenge) выдан этим шлюзом этому адресу, не использован и не старше 120 секунд;
- идентификатор проверяющей стороны, назначение и тип операции в данных клиента;
- что счётчик подписей ключа вырос (защита от копии ключа);
- признак присутствия пользователя, а при включённой настройке — проверку пользователя ключом (PIN или биометрия);
- число неудач: 8 неудачных попыток за 5 минут блокируют адрес на 5 минут.

Пароль учётной записи операционной системы шлюзу не передаётся.

2.3. Регистрация ключей и вход по одноразовому коду

- Ключ регистрируется из клиента по одноразовому коду регистрации. Код выдаёт установщик или команда `code`, выполненная администратором на защищаемом компьютере; код действует 15 минут и хранится в виде хеша.
- Подходят аппаратные ключи FIDO2 (USB, NFC) и Windows Hello; в клиенте для Android ключом может служить сам телефон (ключ в защищённом хранилище телефона). На шлюзе хранится только открытый ключ.
- Команды `keys`, `remove-key`, `key-role` показывают ключи, удаляют их (удаление действует сразу) и задают роль ключа.

- Вместо ключей шлюз можно настроить на вход по 6-значному коду из приложения-аутентификатора (TOTP). Способ входа один на шлюз. Код открывает только RDP; FIDO Stream и обновление шлюза из клиента в этом режиме отключены. Один код принимается один раз; 30 неверных кодов за 10 минут приостанавливают вход по коду на 10 минут. Секреты кодов хранятся в файле настроек шлюза, доступном только администраторам.
- Команда `code --keep` выдаёт многоразовый код регистрации для демонстрационных стендов; на рабочих компьютерах его применять не следует.

2.4. Клиент

- Клиент хранит сохранённые сессии (адрес, имя пользователя, пароль, параметры экрана и локальных ресурсов), запрашивает подтверждение ключом и запускает подключение: `mstsc` в Windows, FreeRDP в Linux, стороннее приложение RDP в Android.
- Сертификат шлюза закрепляется по отпечатку; при несовпадении клиент прерывает соединение до отправки данных.
- Клиент для Windows раз в минуту проверяет, что порт RDP защищаемых компьютеров не отвечает без ключа, и выделяет плитку сессии при нарушении.
- Защита входа: клиент можно закрыть мастер-паролем, которым дополнительно шифруются сохранённые пароли, либо ключом FIDO2 (ключ охраняет только вход и пароли не шифрует).
- В клиенте для Windows сессию можно сохранить и без шлюза — как обычное подключение RDP.

2.5. FIDO Stream

Второй режим подключения — собственный протокол передачи экрана, звука и ввода по UDP с малой задержкой. Поток открывается тем же подтверждением ключом; порт UDP открывается только адресу клиента на время сеанса.

- Видео: H.264, HEVC или AV1, на хосте Windows — аппаратное кодирование (NVIDIA NVENC, кодеры Intel и AMD через Media Foundation) или программный H.264; коррекция потерь кодом Рида–Соломона; частота кадров до 240 Гц; 10 бит, 4:4:4 и HDR при поддержке обеими сторонами.
- Звук в обе стороны (Opus), клавиатура, мышь, до четырёх геймпадов (на хосте Windows — виртуальный контроллер через драйвер ViGEmBus).
- Передача файлов в обе стороны в папку «RDP FIDO» каталога загрузок; на хосте её можно запретить.
- Совместный доступ: до 8 участников одного сеанса, управляет один; гостя можно пригласить кодом с ролью «управлять» или «только смотреть» и ограниченным сроком действия ключа.
- Если прямое соединение невозможно, поток идёт через реле; реле пересылает зашифрованные датаграммы и ключей не имеет.

Поток показывает действующий графический сеанс хоста (в Windows — консольный) в его текущем состоянии: если сеанс не заблокирован, пароль операционной системы не запрашивается. FIDO Stream отключается настройкой `streamEnabled` шлюза.

2.6. Консоль SSH

Окно с терминалом и боковой панелью в клиенте для Windows и Linux. Программа запускает системный `ssh`, вводит сохранённые пароли по щелчку или в ответ на запрос, хранит часто используемые команды. Помощник на основе модели искусственного интеллекта предлагает команды; он обращается к сервису, который указал 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 передаётся модели только при включённом флажке «Видит консоль» (последние 200 строк экрана с каждым вопросом).

2.7. Работа через хаб

Шлюз без публичного адреса можно привязать к хабу `rdpfido-cloud`, который заказчик размещает на своём сервере. Шлюз держит исходящее соединение с хабом; клиент обращается по имени шлюза на порт 443. Хаб пересылает обращения клиента к шлюзу, не расшифровывая их, а RDP проходит через хаб в зашифрованном туннеле по билету шлюза. Хаб видит адреса, объёмы и время соединений и имя шлюза. Непривязанный шлюз исходящих соединений не устанавливает. Хаб, которым управляет поставщик, — закрытый сервис: шлюз к нему подключает iMobile по договорённости, в поставку он не входит.

3. АРХИТЕКТУРА И СОСТАВ

Часть	Где работает	Функции
Шлюз (<code>RdpFidoGate.exe</code> , <code>rdpfido-gate</code>)	Защищаемый компьютер, системная служба	Правила сетевого экрана, проверка ключей и кодов, выдача доступа, агент FIDO Stream, журнал
Клиент (<code>RdpFidoClient.exe</code> ; <code>rdpfido</code> , <code>rdpfido-gui</code>)	Рабочее место пользователя	Сессии, подтверждение ключом, запуск RDP, окно FIDO Stream, консоль SSH
Клиент для Android	Устройство Android	Сессии, ключ в телефоне или ключ по NFC и USB, FIDO Stream, передача подключения приложению RDP
Хаб <code>rdpfido-cloud</code> (необязательный)	Сервер заказчика с публичным адресом	Связь клиентов со шлюзами без публичного адреса, веб-кабинет администратора
Реле <code>rdpfido-relay</code> (необязательное)	Сервер заказчика с публичным адресом	Пересылка датаграмм FIDO Stream
Учётный сервер поставщика	Серверы iMobile	Активация клиента для Windows, условия редакции, раздача обновлений

4. ИНТЕРФЕЙСЫ И ОБМЕН ДАННЫМИ

4.1. Сетевые протоколы

Канал	Протокол и порт	Защита
Клиент — шлюз	HTTPS, TCP 7440 (настраивается)	TLS, сертификат шлюза закреплён по отпечатку
Удалённый рабочий стол	RDP, TCP 3389	Средствами RDP; порт открыт только по правилу шлюза
FIDO Stream	UDP 7441 и следующие порты	AES-256-GCM, ключи из ECDH P-256
Клиент и шлюз — хаб	TCP 443	TLS до шлюза насквозь; туннель AES-256-GCM
Клиент для Windows — учётный сервер	HTTPS, TCP 443	TLS с проверкой сертификата, подпись ответов

4.2. Программные интерфейсы и форматы

Шлюз принимает запросы клиента по HTTPS в формате JSON (/v1/hello, /v1/enroll/begin, /v1/enroll/finish, /v1/auth/begin, /v1/auth/finish, /v1/revoke, /v1/stream/open, /v1/stream/invite, /v1/update/push). Управление шлюзом выполняется из командной строки. Хаб имеет интерфейс командной строки и интерфейс JSON веб-кабинета. Настройки и данные хранятся в файлах JSON. Интерфейсов для интеграции со службами каталогов, системами управления событиями безопасности и единого входа нет.

4.3. Обмен с серверами поставщика

К учётному серверу поставщика обращается только клиент для Windows: при активации (адрес электронной почты, код из письма), при запросе условий редакции (токен учётной записи, версия, язык, идентификатор установки), при учёте показов рекламной плитки в редакции Free и при проверке обновлений (идентификатор продукта и версия). Адреса защищаемых компьютеров, учётные данные и содержимое сеансов поставщику не передаются. Шлюз, клиенты для Linux и Android, хаб и реле к серверам поставщика не обращаются.

4.4. Применяемая криптография

Назначение	Алгоритмы	Реализация
Подтверждение ключом FIDO2	ECDSA P-256, P-384, P-521; RSA PKCS#1 v1.5 и PSS; SHA-256, SHA-384, SHA-512	Windows CNG; OpenSSL 3
Одноразовые коды	TOTP (RFC 6238): HMAC-SHA1, 30 секунд, 6 цифр	Собственная

Назначение	Алгоритмы	Реализация
Канал клиент — шлюз	TLS 1.2 и 1.3; сертификат RSA 2048 (Windows) или ECDSA P-256 (Linux)	Windows Schannel; OpenSSL 3
FIDO Stream и туннель хаба	ECDH P-256, HKDF-SHA256, AES-256-GCM, HMAC-SHA256	Windows CNG; OpenSSL 3
Сохранённые пароли	DPAPI (Windows), связка ключей (Linux), AES-GCM с ключом в хранилище Android	Средства ОС
Мастер-пароль	AES-256-GCM, PBKDF2-HMAC-SHA256, 600 000 итераций	Windows CNG; OpenSSL 3; Android
Обновления и условия редакции	Подпись ECDSA P-256, контрольные суммы SHA-256	Windows CNG

Клиенты для Windows и Linux допускают только TLS 1.2 и 1.3. Алгоритмы ГОСТ не применяются. Подтверждение модели ключа (attestation) шлюз не проверяет. Криптография используется для аутентификации и для защиты собственных каналов и данных программы.

5. РЕДАКЦИИ И ОГРАНИЧЕНИЯ

5.1. Редакции

Характеристика	Free	Pro
Сохранённые сессии в клиенте для Windows	Не более 10	Без ограничения
Рекламная плитка в клиенте для Windows	Есть	Нет
Шлюз, проверка ключа, FIDO Stream, консоль SSH, защита входа	Есть	Есть

Редакция привязана к учётной записи (адресу электронной почты) и действует в клиенте для Windows. Клиент для Windows требует активации: без неё он подключается 14 дней с первого запуска. Шлюз, клиенты для Linux и Android редакцию не проверяют.

5.2. Известные ограничения

- Программа ограничивает сетевой доступ к порту и не заменяет аутентификацию операционной системы: после открытия порта вход проверяется паролем учётной записи (в Windows — с NLA). Если у нескольких узлов общий внешний адрес (NAT), окно доступа открыто для всех узлов за этим адресом.
- Каждая версия работает один год с даты выпуска: затем клиент не подключается, а шлюз не открывает доступ, пока не установлено обновление. Регистрация ключей и команда unlock продолжают работать.
- Исполняемые файлы и пакеты для Windows не имеют цифровой подписи кода.
- Обновление шлюза для Windows может запустить из клиента любой пользователь, вошедший по зарегистрированному ключу FIDO2. Отдельной настройки для отключения этой возможности нет; она отключена только в режиме одноразовых кодов.

- Шлюз для Windows защищает только порт RDP; SSH и другие порты защищает только шлюз для Linux.
- Через хаб проходят только RDP и обращения к шлюзу. Правила доступа, которые ведёт веб-кабинет хаба, шлюзы выпущенных версий не применяют: доступ определяют ключи, зарегистрированные на самом шлюзе.
- FIDO Stream на хосте Linux работает только с сеансами X11 (Wayland не поддерживается) и кодирует программно в H.264.
- Сертификат шлюза самоподписанный; доверие устанавливается по отпечатку при первом обращении, если отпечаток не сверен вручную.
- Клиент для Android — предварительная бета-версия: проверен на одном телефоне, защита входа версии 0.9.1 проверена только в эмуляторе; одноразовые коды, туннель RDP через хаб, совместный доступ и передача файлов в нём не реализованы.
- С физическим ключом безопасности не проверены работа клиента для Linux (проверялась виртуальным ключом) и вход в клиент по ключу FIDO2 (проверялся программным ключом).
- Журналы — локальные текстовые файлы ограниченного размера; централизованного управления ключами нескольких шлюзов нет.

6. ТРЕБОВАНИЯ К СРЕДЕ

- Шлюз для Windows: Windows 10 версии 1903 и новее, Windows 11 или Windows Server, x64; включённый брандмауэр Windows.
- Клиент для Windows: Windows 10 версии 1903 и новее или Windows 11, x64; ключ FIDO2 или Windows Hello.
- Linux, x86_64: Ubuntu 22.04 и 24.04, Astra Linux, РЕД ОС 7.3, ALT Linux p10; systemd; nftables или iptables; для RDP — xrdp (шлюз) и FreeRDP (клиент).
- Клиент для Android: Android 9 и новее.
- Хаб и реле: сервер Linux x86_64 с публичным адресом.

Подробные требования, порты и порядок установки приведены в руководстве по установке и администрированию.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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