

RDP-FIDO-GATE

Product Description and Functional Specification

Document ID	IM.RDP-FIDO.INT.01
Document version	1.0
Date of issue	2026-10-06
Applies to	RDP-FIDO-GATE 1.25.1
Language	English
Publisher	iMobile

Contents

- 1. General information 3
 - 1.1. Name and versions 3
 - 1.2. Purpose 3
 - 1.3. Scope of use 3
 - 1.4. Product class 3
- 2. Functions 3
 - 2.1. Closing the port and admitting by a second factor 3
 - 2.2. Checks made before access opens 4
 - 2.3. Key enrollment and one-time codes 4
 - 2.4. Client 4
 - 2.5. FIDO Stream 5
 - 2.6. SSH console 5
 - 2.7. Working through a hub 5
- 3. Architecture and components 5
- 4. Interfaces and data exchange 6
 - 4.1. Network protocols 6
 - 4.2. Programming interfaces and formats 6
 - 4.3. Exchange with the vendor's servers 6
 - 4.4. Cryptography used 6
- 5. Editions and limitations 7
 - 5.1. Editions 7
 - 5.2. Known limitations 7
- 6. Environment requirements 8

About this document

This document describes what RDP-FIDO-GATE does: its purpose, components, functions, interfaces, the cryptography it uses, its editions and its known limitations. It is written for the customer's specialists who assess the product before purchase and deployment, including information security reviewers.

It covers the released versions: the gate and client for Windows 1.25.0, the Linux packages 1.25.1, the Android client 0.9.1 (pre-beta) and the hub 1.22.0.

1. General information

1.1. Name and versions

The product name is RDP-FIDO-GATE. The user interface and file names use RDP FIDO (the client), RDP FIDO Gate (the gate) and `rdpfido` (the Linux programs).

Component	Platform	Version	Release date
Gate (RDP FIDO Gate) and client (RDP FIDO Client)	Windows	1.25.0	5 October 2026
Gate <code>rdpfido-gate</code> and client <code>rdpfido</code>	Linux	1.25.1	6 October 2026
Client RDP FIDO (pre-beta)	Android	0.9.1	6 October 2026
Hub <code>rdpfido-cloud</code> and relay <code>rdpfido-relay</code>	Linux	1.22.0	28 September 2026

Release 1.25.1 consists of the Linux packages only; there is no Windows build with that number.

1.2. Purpose

The product protects remote access to computers. The gate keeps the Remote Desktop (RDP) port closed in the computer's own firewall and opens it for a short time only to the network address that presented a FIDO2 security key enrolled on that gate or, if the gate is configured that way, a one-time code from an authenticator app. The Linux gate protects SSH and other chosen TCP ports in the same way.

1.3. Scope of use

Remote administration of servers and workstations, remote work, and contractor access to individual computers, wherever an RDP or SSH port is reachable from the internet or from a less trusted network. Every component is installed on the customer's equipment. Key verification and the connection itself involve no vendor server; the Windows client needs the vendor's servers for activation and for updates.

1.4. Product class

Remote access control software with multi-factor authentication: a network access gate and client applications. The product holds no security certifications (such as FIDO Alliance certification, Common Criteria or FIPS 140 validation).

2. Functions

2.1. Closing the port and admitting by a second factor

- The Windows gate disables the allow rules of Windows Firewall for the RDP port, so inbound connections fall under the default block. The Linux gate creates its own `nftables` table (or `iptables` and `ip6tables` chains when `nftables` is absent) that drops the port for IPv4 and IPv6.

- After a successful check the gate adds an allow rule for one address for the access window: 90 seconds by default, 600 at most. The window limits when a connection may start. An established session is not cut: the rule stays while the session is active (but no longer than a day) and is removed when it ends.
- Every 30 seconds the gate checks and restores its rules; the Windows gate switches the firewall back on if it was turned off. On Linux the rules are applied at boot before the network and the xrdp server start; if they cannot be applied, xrdp does not start.
- The port is closed not at installation but when the first key is enrolled. Protection can be lifted in an emergency with the `unlock` command and restored with `arm`.

2.2. Checks made before access opens

- the address belongs to an allowed country, if a country list is set;
- the key's signature verifies against the public key stored at enrollment;
- the challenge was issued by this gate to this address, has not been used and is not older than 120 seconds;
- the relying-party identifier, the origin and the operation type in the client data are the expected ones;
- the key's signature counter has increased (protection against a cloned key);
- the user-presence flag is set and, when the setting is on, the key verified the user (PIN or biometrics);
- failures are limited: 8 failed attempts within 5 minutes block the address for 5 minutes.

The operating system account password is never sent to the gate.

2.3. Key enrollment and one-time codes

- A key is enrolled from the client with a one-time enrollment code. The installer shows the code, or an administrator obtains it on the protected computer with the `code` command; it is valid for 15 minutes and is stored as a hash.
- FIDO2 hardware keys (USB, NFC) and Windows Hello are supported; in the Android client the phone itself can be the key (a key held in the phone's secure hardware). The gate stores only the public key.
- The `keys`, `remove-key` and `key-role` commands list keys, remove them (with immediate effect) and set a key's role.
- Instead of keys, a gate can be set to sign users in with a 6-digit code from an authenticator app (TOTP). A gate uses one method. A code opens RDP only; FIDO Stream and gate updates from the client are switched off in this mode. A code is accepted once; 30 wrong codes within 10 minutes pause code sign-in for 10 minutes. The code secrets are kept in the gate's settings file, which only administrators can read.
- The `code --keep` command issues a reusable enrollment code intended for demonstration machines; it should not be used on production computers.

2.4. Client

- The client keeps saved sessions (address, user name, password, display and local resource settings), asks for the key confirmation and starts the connection: `mstsc` on Windows, FreeRDP on Linux, a third-party RDP app on Android.
- The gate certificate is pinned by its thumbprint; on a mismatch the client aborts the connection before sending any data.
- Once a minute the Windows client checks that the RDP port of each protected computer does not answer without a key, and marks the session tile if it does.

- Entry lock: the client itself can be locked with a master password, which additionally encrypts the saved passwords, or with a FIDO2 key (the key guards the entry only and encrypts nothing).
- In the Windows client a session can also be saved without a gate, as an ordinary RDP connection.

2.5. FIDO Stream

A second connection mode: the product's own low-latency protocol that carries the screen, audio and input over UDP. A stream is opened by the same key confirmation; the UDP port opens only to the client's address for the duration of the session.

- Video: H.264, HEVC or AV1; on a Windows host hardware encoding (NVIDIA NVENC, Intel and AMD encoders through Media Foundation) or software H.264; Reed–Solomon loss recovery; frame rates up to 240 Hz; 10-bit, 4:4:4 and HDR when both ends support them.
- Audio in both directions (Opus), keyboard, mouse and up to four gamepads (on a Windows host a virtual controller through the ViGEmBus driver).
- File transfer in both directions into the "RDP FIDO" folder of the downloads directory; it can be disabled on the host.
- Shared sessions: up to 8 participants in one session, one of whom controls it; a guest can be invited with a code, with a lead or watch-only role and a limited key lifetime.
- When a direct connection is impossible, the stream goes through a relay; the relay forwards encrypted datagrams and holds no keys.

A stream shows the host's current desktop session (the console session on Windows) as it is: if that session is not locked, no operating system password is asked for. FIDO Stream is switched off with the gate's `streamEnabled` setting.

2.6. SSH console

A window with a terminal and a side panel in the Windows and Linux clients. It starts the system `ssh`, types saved passwords on a click or in answer to a prompt, and keeps frequently used commands. An assistant based on an artificial intelligence model suggests commands; it calls the service the user configured (the Claude API or an OpenAI-compatible server, including a local one). No model is part of the product and the vendor's servers take no part in this exchange. Terminal text is sent to the model only when the "sees the console" option is ticked (the last 200 screen lines with each question).

2.7. Working through a hub

A gate without a public address can be linked to the hub `rdpfido-cloud`, which the customer hosts on its own server. The gate keeps an outgoing connection to the hub; the client connects to the gate's name on port 443. The hub forwards the client's calls to the gate without decrypting them, and RDP passes through the hub in an encrypted tunnel authorised by a ticket from the gate. The hub sees addresses, volumes and times of connections and the gate's name. A gate that is not linked makes no outgoing connections. The hub operated by the vendor is a private service: iMobile links a gate to it by arrangement, and it is not part of the delivery.

3. Architecture and components

Component	Where it runs	What it does
Gate (<code>RdpFidoGate.exe</code> , <code>rdpfido-gate</code>)	The protected computer, as a system service	Firewall rules, key and code verification, access grants, the FIDO Stream agent, the log

Component	Where it runs	What it does
Client (<code>RdpFidoClient.exe</code> ; <code>rdpfido</code> , <code>rdpfido-gui</code>)	The user's workstation	Sessions, key confirmation, starting RDP, the FIDO Stream window, the SSH console
Android client	An Android device	Sessions, the phone as a key or a key over NFC and USB, FIDO Stream, hand-over to an RDP app
Hub <code>rdpfido-cloud</code> (optional)	A customer server with a public address	Connects clients to gates without a public address; administrator's web cabinet
Relay <code>rdpfido-relay</code> (optional)	A customer server with a public address	Forwards FIDO Stream datagrams
Vendor's account server	iMobile servers	Activation of the Windows client, edition terms, update distribution

4. Interfaces and data exchange

4.1. Network protocols

Channel	Protocol and port	Protection
Client to gate	HTTPS, TCP 7440 (configurable)	TLS, gate certificate pinned by thumbprint
Remote desktop	RDP, TCP 3389	By RDP itself; the port is open only under the gate's rule
FIDO Stream	UDP 7441 and the following ports	AES-256-GCM, keys from ECDH P-256
Client and gate to hub	TCP 443	TLS end to end to the gate; AES-256-GCM tunnel
Windows client to account server	HTTPS, TCP 443	TLS with certificate validation, signed replies

4.2. Programming interfaces and formats

The gate accepts client requests over HTTPS in 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`). The gate is managed from the command line. The hub has a command-line interface and the JSON interface of its web cabinet. Settings and data are kept in JSON files. There are no interfaces for integration with directory services, security event management systems or single sign-on.

4.3. Exchange with the vendor's servers

Only the Windows client contacts the vendor's account server: for activation (e-mail address, the code from the message), to read the edition terms (account token, version, language, installation identifier), to count impressions of the advertising tile in the Free edition, and to check for updates (product identifier and version). Addresses of protected computers, credentials and session content are not sent to the vendor. The gate, the Linux and Android clients, the hub and the relay do not contact the vendor's servers.

4.4. Cryptography used

Purpose	Algorithms	Implementation
FIDO2 key confirmation	ECDSA P-256, P-384, P-521; RSA PKCS#1 v1.5 and PSS; SHA-256, SHA-384, SHA-512	Windows CNG; OpenSSL 3
One-time codes	TOTP (RFC 6238): HMAC-SHA1, 30 seconds, 6 digits	Own code
Client-to-gate channel	TLS 1.2 and 1.3; RSA 2048 certificate (Windows) or ECDSA P-256 (Linux)	Windows Schannel; OpenSSL 3
FIDO Stream and the hub tunnel	ECDH P-256, HKDF-SHA256, AES-256-GCM, HMAC-SHA256	Windows CNG; OpenSSL 3
Saved passwords	DPAPI (Windows), desktop keyring (Linux), AES-GCM with an Android Keystore key	Operating system facilities
Master password	AES-256-GCM, PBKDF2-HMAC-SHA256 with 600,000 iterations	Windows CNG; OpenSSL 3; Android
Updates and edition terms	ECDSA P-256 signature, SHA-256 checksums	Windows CNG

The Windows and Linux clients allow only TLS 1.2 and 1.3. The gate does not verify the attestation of the key model. Cryptography is used for authentication and to protect the product's own channels and data.

5. Editions and limitations

5.1. Editions

Feature	Free	Pro
Saved sessions in the Windows client	At most 10	Unlimited
Advertising tile in the Windows client	Yes	No
Gate, key verification, FIDO Stream, SSH console, entry lock	Yes	Yes

The edition is bound to an account (e-mail address) and applies in the Windows client. The Windows client requires activation: without it, it connects for 14 days from first run. The gate and the Linux and Android clients do not check the edition.

5.2. Known limitations

- The product restricts network access to a port and does not replace operating system authentication: once the port is open, sign-in is checked by the account password (with NLA on Windows). When several hosts share one external address (NAT), the access window is open to every host behind that address.
- Every version works for one year from its release date: after that the client does not connect and the gate opens no access until an update is installed. Key enrollment and the `unlock` command keep working.
- The Windows executables and packages carry no code-signing signature.
- An update of the Windows gate can be started from the client by any user who signed in with an enrolled FIDO2 key. There is no separate setting to switch this off; it is off only in one-time-code mode.
- The Windows gate protects the RDP port only; SSH and other ports are protected only by the Linux gate.
- Only RDP and calls to the gate pass through the hub. The access rules kept in the hub's web cabinet are not applied by the gates of the released versions: access is determined by the keys enrolled on the gate itself.
- FIDO Stream on a Linux host works with X11 sessions only (no Wayland) and encodes in software to H.264.

- The gate certificate is self-signed; trust is established by its thumbprint on first contact unless the thumbprint is checked manually.
- The Android client is a pre-beta: it has been verified on a single phone, and the entry lock of version 0.9.1 only in an emulator; one-time codes, the RDP tunnel through a hub, shared sessions and file transfer are not implemented in it.
- Not verified with a physical security key: the Linux client (tested with a virtual key) and unlocking the client with a FIDO2 key (tested with a software key).
- Logs are local text files of limited size; there is no central management of keys across gates.

6. Environment requirements

- Gate for Windows: Windows 10 version 1903 or later, Windows 11 or Windows Server, x64; Windows Firewall switched on.
- Client for Windows: Windows 10 version 1903 or later or Windows 11, x64; a FIDO2 key or Windows Hello.
- Linux, x86_64: Ubuntu 22.04 and 24.04, Astra Linux, RED OS 7.3, ALT Linux p10; systemd; nftables or iptables; xrdp (gate) and FreeRDP (client) for RDP.
- Client for Android: Android 9 or later.
- Hub and relay: a Linux x86_64 server with a public address.

Detailed requirements, ports and installation steps are given in the Installation and Administration Guide.

Document history

Document version	Date	Product version	Change
1.0	2026-10-06	1.25.1	First issue