

RDP-FIDO-GATE

Security and Data Protection Statement

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

Contents

- 1. Deployment model 3
- 2. Data processed 3
 - 2.1. Personal data 3
 - 2.2. Where data is stored 3
 - 2.3. Data sent to the vendor 4
- 3. Artificial intelligence functions 4
- 4. Access control 4
- 5. Cryptography 4
- 6. Logging and audit 5
- 7. Data export and deletion 5
- 8. Updates and vulnerability handling 5
- 9. Certifications and assessments 6
- 10. Accessibility 6
- 11. Known limitations 6

About this document

This statement describes how RDP-FIDO-GATE version 1.25.1 handles data and which security mechanisms it implements. It describes the product as shipped. It is not a certification and does not replace the customer's own risk assessment.

1. Deployment model

Client and server components, all installed on the customer's equipment.

Every part is installed on the customer's equipment. The gate is a service on each protected computer (Windows or Linux). The client is an application on users' workstations (Windows, Linux) and an app on Android devices. The optional hub `rdpfido-cloud` and relay `rdpfido-relay` go on a customer server with a public address when the gates cannot be reached directly. The vendor's servers run only the account server (activation of the Windows client, edition terms) and the update distribution; session data never passes through them. The hub operated by the vendor is a private service and is not part of the delivery.

When installed on the customer's equipment, the product runs on infrastructure the customer controls, and the vendor has no access to the content processed there. Connections the product makes to third-party services that the customer configures are described in the Product Description and under "Artificial intelligence functions" below.

Independently of the deployment option, the vendor receives the data listed under "Data sent to the vendor".

2. Data processed

2.1. Personal data

- In the client: computer addresses and labels, user names and domains, saved session passwords (encrypted), screenshots of remote desktops for the tiles, notes
- In the Windows client: the account e-mail address and the activation token
- In the SSH console: saved passwords and commands, notes for the assistant, the history of conversations with the assistant (may contain terminal text)
- On the gate: labels and public keys of enrolled FIDO2 keys, one-time-code secrets, use counters and times, client IP addresses in the log
- On the hub: identifiers and machine names of linked gates, client IP addresses, cabinet accounts (login, name, password hash), the event log
- Sent by the Windows client to the vendor's account server: the e-mail address, the installation identifier, the client version and language, impressions and clicks of the advertising tile; the server keeps the account and its edition

2.2. Where data is stored

Data is stored locally on the customer's equipment. Windows client: the directory

`%LOCALAPPDATA%\RdpFidoClient` (sessions.json, thumbs, account.json, console.json, console-chats.json, applock.dat, client.log). Windows gate: `%ProgramData%\RdpFidoGate` (gate.json, enrollment.json, gate.log), accessible to SYSTEM and administrators only. Linux client: `~/.config/rdpfido` (mode 0600), passwords in the desktop keyring. Linux gate: `/var/lib/rdpfido-gate` (root only). Android client: the app's private directory. Hub: `/var/lib/rdpfido-cloud`. The vendor holds only the account details listed under activation.

2.3. Data sent to the vendor

- Windows client → account server, activation code request: e-mail address, product identifier, interface language
- Windows client → account server, activation: e-mail address, the code from the message, product identifier
- Windows client → account server, edition terms (hourly, or every 10 minutes while the advertising tile is shown): account token, product identifier, client version, interface language, installation identifier
- Windows client → account server, advertising tile statistics (Free edition only): account token, product identifier, event type (impression or click), advertisement identifier; download of the advertisement pictures
- Windows client → account server, update check: product identifier and client version; download of the update files
- With every request the account server sees the client's IP address
- The gate, the Linux and Android clients, the hub and the relay send nothing to the vendor

3. Artificial intelligence functions

The assistant in the SSH console (Windows and Linux clients) suggests commands in answer to the user's question. It calls the service the user has 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 (the last 200 screen lines with each question) is sent to the model only when the "sees the console" option is ticked.

4. Access control

Access to a protected port opens after a check on the gate: with a FIDO2 key (signature over the challenge, relying-party identifier, signature counter, user-presence flag and, when enabled, PIN or biometric verification) or, if the gate is set to codes, with a TOTP one-time code. A gate uses one method. A key is enrolled with a one-time enrollment code that the administrator obtains on the gate (valid for 15 minutes). Access is granted only to the address that passed the check, for a set window (90 seconds by default, at most 600). Failed attempts are limited: 8 within 5 minutes from an address block that address for 5 minutes. Countries can be restricted using a local address table. The gate has no user roles other than a key's role in a shared FIDO Stream session (lead or watch only). Gate commands are run by the operating system administrator. Once the port is open, sign-in to the computer is checked by the operating system itself (account and password). The client can be locked with a master password or a FIDO2 key. The hub cabinet has accounts with owner, administrator, auditor and user roles.

5. Cryptography

- Sign-in confirmation: FIDO2 / WebAuthn; the gate verifies ECDSA signatures (P-256, P-384, P-521 with SHA-256/384/512) and RSA signatures (PKCS#1 v1.5 with SHA-256/384/512, PSS with SHA-256); EdDSA keys are not accepted. The attestation of the key model is not verified
- One-time codes: TOTP per RFC 6238 — HMAC-SHA1, 30-second step, 6 digits, 160-bit secret
- Client-to-gate channel: HTTPS with the gate's self-signed certificate, pinned by the client by its SHA-256 thumbprint; the Windows and Linux clients allow only TLS 1.2 and 1.3. Windows gate: RSA 2048-bit certificate (SHA-256), TLS by Windows (http.sys, Schannel). Linux gate: ECDSA P-256 certificate, OpenSSL 3, TLS 1.2 or later, in TLS 1.2 only ECDHE suites with AES-GCM or ChaCha20-Poly1305

- FIDO Stream: ECDH P-256 key agreement, HKDF-SHA256 key derivation bound to the gate's ticket, AES-256-GCM on every datagram, replay protection
- Hub: a handshake with HMAC-SHA256 over a shared secret and ephemeral ECDH P-256, AES-256-GCM records; the hub does not decrypt the TLS between client and gate
- Saved passwords: Windows — DPAPI of the user account; Linux — the desktop keyring; Android — AES-GCM with a key in the Android Keystore
- Master password (entry lock): a random 256-bit key that encrypts the passwords with AES-256-GCM; the key is stored wrapped by a key derived from the password with PBKDF2-HMAC-SHA256, 600,000 iterations
- Updates and edition terms: the account server's ECDSA P-256 signature, SHA-256 checksums
- Hashing: enrollment codes are stored as salted SHA-256; hub cabinet account passwords as PBKDF2-HMAC-SHA256, 200,000 iterations
- Implementations: Windows CNG and DPAPI; OpenSSL 3 on Linux; javax.crypto and the Android Keystore. Cryptography is used for authentication and to protect the product's own channels and data

6. Logging and audit

The gate keeps a text log `gate.log` (on Linux also the systemd journal): key enrollments with the address, every opening and closing of access with the address and the key label, rejected attempts and their reasons, rate-limit triggers, changes of the protection state, updates. The log is limited to 4 MB with one previous file kept. The client keeps `client.log` (gate calls and errors). The hub keeps a service log and a daily cabinet event log (kept for 90 days). There is no writing to the Windows event log, no syslog or SIEM forwarding and no tamper protection of the logs.

7. Data export and deletion

Data is kept in JSON files and text logs in the directories listed above and is copied with operating system tools; there is no separate export function. Deletion: a session is deleted in the client together with its saved password and screenshot; a key on the gate with the `remove-key` command; everything by deleting the data directory after uninstalling (the data directories survive an uninstall; the Linux gate's directory is removed by a `purge` of the deb package). The client has no function for deleting the account on the account server: such a request is addressed to the vendor.

8. Updates and vulnerability handling

The Windows client asks the account server for an update manifest at start (when the setting is on) and on the user's command, sending the product identifier and its own version. The manifest is signed with the server's key (ECDSA P-256, the public key is built into the client); the client downloads the file, checks its SHA-256 against the manifest and replaces itself with the user's consent. The Windows gate is updated by installing a new MSI package or from the client: after a successful FIDO key check the client sends the gate a new executable, the gate checks its SHA-256, replaces itself keeping a backup and rolls back if the service does not start. The Linux packages, the Android app and the hub are updated by installing the new version over the old one. One year after a version's release date an update is mandatory.

Suspected vulnerabilities can be reported through:

- contact form: <https://new-imobile.com/contact>
- e-mail: admin@new-imobile.com

Reports are handled as described in the document "Software Lifecycle, Maintenance and Support".

9. Certifications and assessments

No third-party security certification or audit (for example Common Criteria, FIPS 140-3, ISO/IEC 27001 or SOC 2) is claimed for the product or for the vendor in this document.

10. Accessibility

No accessibility assessment (WCAG or similar) has been carried out. The Windows client can be operated from the keyboard (the shortcuts are listed in the User Guide) and follows the Windows display language and scaling; the Linux client and the gate have a complete command line. Operation with screen readers has not been tested; the session tiles in the Windows client are drawn by the program itself.

11. 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
- The Windows client requires activation through the vendor's account server within 14 days; there is no offline activation
- 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. The Linux gate is not updated from the client
- In one-time-code mode only RDP opens; FIDO Stream and gate updates from the client are unavailable; the Android client does not support this mode
- Only RDP and calls to the gate pass through the hub; extra ports and the SSH console need the gate's direct address. The access rules kept by the hub cabinet are not applied by the gates of the released versions
- FIDO Stream on a Linux host: X11 sessions only (no Wayland), software H.264 encoding without HEVC, AV1 or HDR; the Linux stream window decodes in software
- 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: verified on a single phone, the entry lock of version 0.9.1 only in an emulator; RDP opens in a third-party app; shared sessions and file transfer are not implemented
- Not verified with a physical security key: the Linux client (tested with a virtual key, PIN entry not tested) and unlocking the client with a FIDO2 key (tested with a software key)
- There is no central management of keys across gates; logs are local files of limited size
- The product holds no security certifications

Document history

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