

RDP-FIDO-GATE

Country Annex — United States

Vendor statement of facts relevant to local requirements

Document ID	IM.RDP-FIDO.US.A1
Document version	1.0
Date of issue	2026-10-06
Applies to	RDP-FIDO-GATE 1.25.1
Language	English
Publisher	iMobile

Contents

- 1. Purpose and status 3
- 2. Product facts 3
 - 2.1. Personal data the product can process 3
 - 2.2. Where data is stored 4
 - 2.3. Data sent to the vendor 4
- 3. Privacy 4
 - 3.1. Roles 4
 - 3.2. What the product provides 5
 - 3.3. What remains with the customer 5
- 4. Accessibility 5
- 5. Software supply chain 6
- 6. Cryptography and export controls 6
- 7. Authentication and remote access 7
- 8. Use of artificial intelligence 7
- 9. Government contracts 7
- 10. Language 7
- 11. Documents usually requested and where to find them 8

About this document

This annex supplements the documentation of RDP-FIDO-GATE version 1.25.1 for customers in the United States. It sets out the facts about the product that matter under the local rules named below and shows which obligations stay with the customer.

The annex is a statement by the vendor about its product. It is not legal advice, not a certificate of conformity and not a substitute for the customer's own assessment.

1. Purpose and status

No certification, authorisation or registration by United States federal or state authorities is claimed for the product or for the vendor in this document.

2. Product facts

Item	Fact
Product and version	RDP-FIDO-GATE 1.25.1
Deployment	Client and server components, all installed on the customer's equipment
Customer content on vendor servers	No
Interface languages	Windows client and installers: Russian, English, German, French, Spanish, Chinese. Linux client: Russian, English. Android client: English, Russian. Gate command line and log: English. Hub web cabinet: Russian, English.

2.1. Personal data the product can process

- 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. Privacy

The United States has no single federal privacy statute for the private sector. Contracts most often refer to the state consumer-privacy laws, above all the California Consumer Privacy Act as amended by the CPRA (Cal. Civ. Code § 1798.100 et seq.), and to sector laws.

3.1. Roles

For personal data processed in the product on the customer's own equipment, the customer is the business (the CCPA term; "controller" in other state laws). The vendor has no access to that data and is not a service provider for it.

For the data listed under "Data sent to the vendor", which the vendor receives in order to perform the licence agreement, the vendor is itself a business (the CCPA term; "controller" in other state laws).

3.2. What the product provides

- **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.
- **Logging.** 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.
- **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.
- **Encryption.** See the section on cryptography below.

3.3. What remains with the customer

- the notice at collection and the privacy policy;
- answering consumer requests to know, delete and correct, using the export and deletion functions above;
- deciding whether regulated categories of data may be placed in the product. No assessment of the product against HIPAA, GLBA, FERPA, COPPA or PCI DSS is claimed in this document.

4. Accessibility

Federal agencies, and many state bodies and universities, buy information technology against Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), whose standards incorporate WCAG 2.0 Level AA, and ask the vendor for an Accessibility Conformance Report on the VPAT template.

Status of the product: 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.

No Accessibility Conformance Report (VPAT) is provided for this version.

5. Software supply chain

Federal agencies set their own software-assurance requirements (OMB Memorandum M-26-05). An agency may ask a software producer for a statement on secure development practices aligned with the NIST Secure Software Development Framework (NIST SP 800-218) and for a software bill of materials (SBOM).

- Development and release practices are described in "Software Lifecycle, Maintenance and Support".
- Third-party components and their licences are listed in "Delivery Specification and Third-Party Components". The list is human-readable; no SBOM in SPDX or CycloneDX format is provided for this version.
- No secure-development attestation is provided for this version.

6. Cryptography and export controls

The product uses cryptography as follows:

- 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
- The product has not been validated under FIPS 140-3. Where the list above names cryptographic services of the operating system, their validation status is that of the operating system.
- The product is developed and published outside the United States. No U.S. export classification (ECCN) is claimed for it. A customer that exports or re-exports the product from the United States determines its own obligations under the Export Administration Regulations (15 C.F.R. Parts 730–774).

7. Authentication and remote access

Contracts frequently refer to NIST SP 800-63B (authenticator assurance levels and phishing-resistant authentication) and, in the payment-card sector, to PCI DSS requirement 8 on multi-factor authentication. The product's mechanisms are described in the Product Description; in brief: 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.

No assessment of conformity with these documents and no FIDO Alliance certification of the product is claimed.

8. Use of artificial intelligence

The product uses large language models as follows. 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.

There is no federal statute on artificial intelligence in commercial software. State laws are developing and mainly address automated decisions with significant effects on individuals; whether the customer's use of these functions falls under them depends on that use. The output of these functions is to be reviewed by a person before it is relied on.

9. Government contracts

- **Rights in software.** The software and its documentation are "commercial computer software" and "commercial computer software documentation" within the meaning of Part 12 of the Federal Acquisition Regulation and DFARS 227.7202. U.S. Government end users acquire them with only the rights set out in the vendor's licence agreement.
- **Country of origin.** A statement for the purposes of the Trade Agreements Act (19 U.S.C. § 2501 et seq.; FAR 52.225-5) depends on the contracting entity and is given in the contract; none is made here.

10. Language

This package is supplied in English. This annex is laid out for US Letter paper; the other documents of the package are laid out for A4.

Interface languages of the product: Windows client and installers: Russian, English, German, French, Spanish, Chinese. Linux client: Russian, English. Android client: English, Russian. Gate command line and log: English. Hub web cabinet: Russian, English.

11. Documents usually requested and where to find them

Usually requested	Where it is
Product description, functional specification	Product Description and Functional Specification
Installation and operating instructions	Installation and Administration Guide
User manual	User Guide
Maintenance and support description	Software Lifecycle, Maintenance and Support. Service levels: contract
List of third-party and open-source components	Delivery Specification and Third-Party Components
Security and data-protection description	Security and Data Protection Statement
Accessibility Conformance Report (VPAT)	Not provided for this version
SBOM (SPDX or CycloneDX), secure-development attestation	Not provided for this version; component list as above
Service-provider terms (CCPA), business associate agreement (HIPAA)	Contract, where applicable
Licence agreement, warranties, prices	Contract

Document history

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