

RDP-FIDO-GATE

Country Annex — European Union

Vendor statement of facts relevant to local requirements

Document ID	IM.RDP-FIDO.EU.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. Data protection — GDPR 4
 - 3.1. Roles 4
 - 3.2. What the product provides (Articles 25 and 32) 5
 - 3.3. What remains with the customer 5
- 4. Product cybersecurity — Cyber Resilience Act 5
- 5. Supply-chain security — NIS2 6
- 6. Accessibility 6
- 7. Artificial intelligence — AI Act 6
- 8. Language 6
- 9. Documents usually requested and where to find them 7

About this document

This annex supplements the documentation of RDP-FIDO-GATE version 1.25.1 for customers in the European Union and the European Economic Area. 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 CE marking, EU declaration of conformity or certificate under a European cybersecurity certification scheme is claimed for the product 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. Data protection — GDPR

Regulation (EU) 2016/679 (GDPR) applies to the personal data the customer processes with the product.

3.1. Roles

For personal data processed in the product on the customer's own equipment, the customer is the controller. The vendor has no access to that data and is not a processor 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 controller.

Details of the vendor's establishment and, where Article 27 applies, of its representative in the Union are stated in the contract.

3.2. What the product provides (Articles 25 and 32)

- **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 lawful basis for processing (Article 6) and information to data subjects (Articles 13 and 14);
- the record of processing activities (Article 30) and, where required, a data protection impact assessment (Article 35);
- answering data-subject requests (Articles 15 to 22) with the export and deletion functions above;
- notifying a personal-data breach to the supervisory authority within 72 hours (Article 33);
- for installations on the customer's equipment, the choice of where that equipment is located.

4. Product cybersecurity — Cyber Resilience Act

Regulation (EU) 2024/2847 sets cybersecurity requirements for products with digital elements placed on the Union market. Its main obligations (conformity assessment, EU declaration of conformity, CE marking) apply from 11 December 2027; the manufacturer's duty to report actively exploited vulnerabilities and severe incidents applies from 11 September 2026.

- No EU declaration of conformity under the Regulation has been issued for this version.
- Vulnerability reports are accepted through the channels named in the Security and Data Protection Statement.
- The period during which security updates are provided is set in the contract.
- The components the product contains are listed in "Delivery Specification and Third-Party Components".

5. Supply-chain security — NIS2

Customers that are essential or important entities under Directive (EU) 2022/2555 must address the security of their supply chain (Article 21(2)(d)). The Security and Data Protection Statement and the Delivery Specification contain the facts usually collected in a supplier assessment. The product's multi-factor authentication can be used by the customer when implementing Article 21(2)(j).

6. Accessibility

Public-sector buyers apply the standard EN 301 549, which Directive (EU) 2016/2102 uses for public-sector websites and mobile applications. Directive (EU) 2019/882 (European Accessibility Act) has applied since 28 June 2025 to the consumer products and services it lists.

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 EN 301 549 conformance report is provided for this version.

7. Artificial intelligence — AI Act

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.

Regulation (EU) 2024/1689 applies to AI systems placed on the Union market. The models involved are general-purpose AI models supplied by third parties or chosen by the customer.

- Article 50 of the Regulation sets transparency obligations, which apply from 2 August 2026. Article 50(2) requires providers of systems that generate synthetic content to mark the output in a machine-readable format; for systems placed on the market before 2 August 2026 it applies from 2 December 2026. No machine-readable marking of output as AI-generated is claimed for this version.
- No use listed in Annex III of the Regulation (high-risk systems) is among the purposes described in the product documentation.
- Where an AI function evaluates data about natural persons, the customer assesses it under Article 22 GDPR (automated individual decision-making, including profiling).
- Content sent to a model provider outside the European Economic Area that contains personal data is a transfer under Chapter V GDPR.

The output of these functions is to be reviewed by a person before it is relied on.

8. Language

This package is supplied in English. Member states may require the national language for documentation supplied to consumers or to public bodies (for example France, Law No. 94-665 of 4 August 1994). National-language documentation is not part of this package.

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.

9. 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
Technical and organisational measures (Article 32 GDPR)	Security and Data Protection Statement
Data processing agreement (Article 28 GDPR), standard contractual clauses	Contract; needed only where the vendor processes customer data
EN 301 549 accessibility report	Not provided for this version
EU declaration of conformity (Cyber Resilience Act)	Not issued; not yet required
Public-sector standard terms (for example EVB-IT in Germany, CCAG-TIC in France)	Contract; the documents of this package serve as the product description those terms refer to
Licence agreement, warranties, prices	Contract

Document history

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