RFT Secure File Transfer Service. Client FAQ & Executive Summary

October 28, 2025

Executive Summary: Why Choose RFT?

RFT (Raw File Transfer) is a highly secure, cloud-native file transfer platform engineered to meet or exceed NIST SP 800-53, FedRAMP Moderate/High, and ISO/IEC 27001 security standards. Designed for regulated industries and security-conscious organizations, RFT delivers:

- End-to-end data protection with FIPS-compliant encryption in transit and at rest
- Complete data segregation - each client’s files are isolated in dedicated S3 prefixes
- Zero infrastructure exposure - no VM, container, or filesystem access for clients
- Dual-protocol support: Secure file transfer via SFTP (SSH) *or* HTTPS (REST API) - no firewall changes required
- Stateless, horizontally scalable architecture supporting hundreds of clients with consistent performance
- Strong, modern cryptographic support, including NIST-recommended and post-quantum–ready algorithms
- Centralized, auditable key and access management via secure database (no authorized_keys files)
- Compliance-ready with immutable logging, least-privilege design, and regular third-party assessments

RFT ensures your data remains private, tamper-proof, and fully under your control - while simplifying integration and reducing operational risk.

Frequently Asked Questions

What does “RFT” stand for?

RFT = Raw File Transfer - a purpose-built, zero-trust file exchange platform focused on security, simplicity, and scalability.

Which protocols does RFT support?

RFT supports both:

- SFTP (SSH File Transfer Protocol) – for traditional SFTP clients
- HTTPS (REST API) – for programmatic or web-based integrations

Both operate over standard ports (22 for SFTP, 443 for HTTPS), so no firewall modifications are needed.

What SSH key types are supported for SFTP authentication?

RFT supports the following industry-standard, cryptographically strong public key algorithms:

- ssh-ed25519 *(recommended for performance and security)*
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- ssh-rsa *(2048-bit minimum; note: RSA is supported for compatibility but Ed25519 or ECDSA is preferred per NIST guidance)*

All keys are validated and stored securely in our access-controlled PostgreSQL database.

How do I authenticate?

- SFTP: Using one of the supported SSH public key types listed above
- HTTPS: API keys or OAuth 2.0 tokens (configurable per client)

Credentials are never stored in flat files - only in our hardened, encrypted database with strict access controls.

Is my data isolated from other clients?

Yes. Every client receives a unique, dedicated prefix in our encrypted S3 storage (e.g., s3://rft-bucket/client-xyz/). No cross-client access is possible - by design.

Where is my data stored during and after transfer?

- During transfer: Files are held only in RAM - never written to local disk or persistent storage.
- After transfer: Immediately encrypted and uploaded to your isolated S3 location using AES-256 or AWS KMS encryption.

Can I access the server, OS, or file system?

No. RFT provides zero access to underlying infrastructure - no shell, no terminal, no volumes, and no container or VM access. You interact solely through secure, protocol-limited channels (SFTP/HTTPS).

How does RFT ensure compliance?

RFT is architected to meet or exceed:

- NIST SP 800-53
- FedRAMP Moderate and High
- ISO/IEC 27001

Key compliance enablers:

- FIPS 140-2 validated cryptographic modules
- Immutable audit logs for all authentication and transfer events
- Role-based access control (RBAC)
- Automated patching and vulnerability management
- Support for NIST-recommended algorithms (e.g., Ed25519, ECDSA P-384)

Can the service scale with my needs?

Yes. Built on stateless microservices (rft-gateway for management, sftp-backend for transfers), RFT scales horizontally to support hundreds of concurrent clients without performance degradation.

Can session or throughput limits be applied?

Yes. We can enforce:

- Maximum concurrent SFTP sessions per client (SSH_SERVER_MAX_SESSIONS)
- IP allowlists, rate limits, and transfer quotas - configured to align with your security policy.

Who manages the platform?

Our team handles all infrastructure, monitoring, encryption, patching, and scaling. You only manage your authentication credentials and initiate transfers.

RFT: Secure by design. Simple by default.
Trusted by federal agencies, financial services, healthcare providers, and global enterprises for mission-critical, compliant file exchange.