ZERO TRUST DRIVE

Built for Security. Made for Teams.

TECHNICAL WHITE PAPER

Zero-Knowledge Encrypted File Sharing Platform

Security Architecture & Data Protection Overview

This document provides a public overview of ZeroTrustDrive's security architecture: zero-knowledge principles, encryption design, access control, and infrastructure. Intended for prospective customers, technical evaluators, and anyone evaluating the platform's approach to data security.

Version 1.0 (Public Edition) | 2026

Table of Contents

1 Executive Summary

ZeroTrustDrive is a zero-knowledge, end-to-end encrypted file sharing and storage platform built for organizations that demand uncompromising data privacy. The platform is designed around a fundamental principle: no server — not even ZeroTrustDrive's own infrastructure — can ever access the plaintext content of a user's files.

> *All cryptographic operations are performed exclusively on the client side, in the user's browser. Encryption keys are never transmitted to or stored on our servers in decrypted form.*

The platform employs a hybrid encryption model, combining strong symmetric encryption for file content with public-key cryptography for secure key distribution. Each file is protected with its own unique, randomly generated key, and group sharing is achieved through a key-wrapping mechanism that preserves zero-knowledge guarantees even in multi-user environments.

ZeroTrustDrive is offered as a SaaS platform with white-label and reseller capabilities, deployed on GDPR-compliant European cloud infrastructure, and is designed to support enterprise teams, managed service providers, and security-critical industries.

2 The Problem With Traditional Cloud Storage

Traditional cloud storage services — even those that advertise encryption — typically encrypt data at rest using keys managed by the provider. The provider holds the keys and can, in principle, access any user's data. This model exposes organizations to real risk:

- Provider-side key management creates a single point of compromise
- Legal requests can compel providers to disclose plaintext data
- Insider threats at the provider cannot be fully mitigated
- A data breach at the provider can expose easily decryptable content
- Data sovereignty and strict compliance requirements become difficult to meet

ZeroTrustDrive eliminates these risks by implementing true end-to-end, zero-knowledge encryption. Data is always encrypted on the client before it leaves the device and can only be decrypted by the intended recipient, using keys that never leave the client environment unencrypted.

The platform is especially suited for legal firms, healthcare organizations, financial institutions, government contractors, technology companies, and any team handling confidential intellectual property or personal data.

3 Architecture Overview

3.1 The Zero-Knowledge Principle

Zero-knowledge means our servers store only ciphertext. They have no access to encryption keys, no way to decrypt files, and no knowledge of file contents. Even in the event of a server compromise, an attacker would obtain only meaningless ciphertext. All key derivation, encryption, and decryption operations run in the user's browser.

3.2 Hybrid Encryption Model

ZeroTrustDrive uses a two-layer hybrid encryption scheme, combining industry-standard symmetric and asymmetric cryptography:

Layer	Purpose	Strength
Symmetric encryption	File content encryption	256-bit (AES-GCM)
Asymmetric encryption	Secure key distribution	4096-bit (RSA-OAEP)
Key derivation	Deriving keys from a user passphrase	SHA-256 based, 100,000+ iterations
Transport	Channel security	TLS 1.3

This model combines the performance of symmetric encryption for large files with the secure, multi-party key distribution of asymmetric cryptography — without any key ever being shared in plaintext.

At a high level, the platform is built from a browser-based client application that performs all cryptographic operations, a backend service that manages metadata and encrypted keys, encrypted object storage for file content, and a management layer for subscriptions, white-label, and reseller accounts. The backend and storage layers never have access to unencrypted keys or file content.

4 How Encryption Keys Are Generated & Protected

During registration, the user chooses a Master Key — a passphrase known only to the user and never transmitted to our servers. From this single passphrase, the user's entire cryptographic identity is derived, entirely within the browser.

- A unique random salt is generated for the account
- A strong key-derivation function is applied to the Master Key, producing a personal encryption key
- That personal key is used, on the client, to protect the user's private key material
- A one-time recovery phrase is generated and shown to the user

> *The Master Key itself is never stored anywhere — not in the browser, not on our servers. Only someone who knows the Master Key can unlock access to their data.*

Each user also receives a unique public/private key pair. The public key is used by others to share content with that user; the private key is protected with the user's personal key and can only be recovered by someone who knows the Master Key.

For organizational (team) accounts, a similar mechanism protects a shared team key, allowing approved members to access team content without ever exposing the underlying key material to our infrastructure.

5 Authentication & Session Security

Authentication in ZeroTrustDrive is a two-factor process by design: standard account credentials, plus the user's Master Key. Even if an attacker were to obtain login credentials alone, they could not access any encrypted content without the Master Key.

- Credentials and the Master Key are verified through independent mechanisms
- Session-specific key material lives only in the browser for the duration of the active session
- All keys are cleared from the browser when the user logs out or closes the session
- Session tokens are server-issued, short-lived, and bound to the authenticated session

> *Key material used during a session is ephemeral by design. It exists only for the duration of an active session and is never persisted beyond it.*

The platform also enforces rate limiting on both read and write operations, IP-based abuse protection, mandatory authentication checks on every API request, and email verification before any protected resource can be accessed.

6 File Upload & Encryption

Every file uploaded to ZeroTrustDrive is encrypted before any data leaves the user's device. The process is fully automated and transparent to the end user.

- Each upload generates a fresh, random, single-use encryption key and initialization vector
- That key is used to encrypt the file content using authenticated encryption, protecting both confidentiality and integrity
- The file's encryption key is itself encrypted ("wrapped") separately for the file owner and, where relevant, for the team, so each authorized party can independently decrypt it

> *This dual-key wrapping enables zero-knowledge group sharing: the uploader can decrypt via their personal key, and any approved team member can decrypt via the team key — without our servers ever seeing the plaintext key.*

Large files are split into chunks on the client before encryption and upload, enabling resumable uploads, a reduced memory footprint through streaming encryption, and consistent performance for large datasets. All data in transit is protected with TLS 1.3.

7 File Download & Decryption

Decryption is performed entirely on the client. Our servers stream encrypted content to the browser, which decrypts it locally using keys reconstructed from the authenticated session. At no point does plaintext file data pass through our infrastructure.

- The browser reconstructs the user's private key locally, using session-scoped key material
- That private key is used to unwrap the file's encryption key — via the user's own key if they own the file, or via the team key if it was shared with a group
- The file's encryption key then decrypts the content locally, and decrypted data is streamed directly to the user's download

> *At no point does plaintext file data pass through our servers. Our infrastructure only orchestrates the transfer of ciphertext and encrypted metadata.*

8 Team & Group Sharing

8.1 Roles & Permissions

ZeroTrustDrive supports secure file sharing within organizational teams without compromising the zero-knowledge guarantee. Each team has its own protected key, and every approved member receives access to that key wrapped specifically for them — new members can be added without needing to re-encrypt existing files.

The platform implements a multi-tier permission system:

Role	Capabilities
Super Admin	Full platform administration
Manager	Manages team members and team content
Team Member	Upload, download, and share files within the team
Guest	Limited access to specific files shared explicitly
Reseller	Manages sub-accounts and white-label configuration

Folder- and file-level permissions are enforced consistently across the platform, and security-relevant events are logged for audit purposes.

8.2 Guest Access

- Guests can be granted access to specific files or folders without becoming full team members
- Access can be revoked by a manager at any time
- Guests cannot access team content that was not explicitly shared with them

9 Master Key Changes & Account Recovery

Changing the Master Key is a cryptographically sensitive operation that must preserve access to all existing encrypted data. ZeroTrustDrive handles this entirely on the client, without ever transmitting the Master Key to our servers.

- The user confirms their current Master Key, which is verified locally
- A new Master Key is chosen and confirmed
- The user's private key material is re-protected under the new Master Key

> *The user's underlying key pair does not change during a Master Key update — only its protection is refreshed. All previously encrypted files remain fully accessible, with no need to re-encrypt any files.*

A one-time recovery phrase is generated on the client during registration and shown once to the user. It is never transmitted to our servers, and users are strongly advised to store it securely offline — it is the only way to restore access if the Master Key is forgotten.

10 Application Security

Beyond encryption, ZeroTrustDrive is built with defense-in-depth application security practices, since a compromised application layer could undermine even strong cryptography.

Input Handling

- All user input is validated and sanitized on both client and server
- Dynamic content is safely encoded before being rendered
- Database access uses parameterized queries to prevent injection attacks

Transport & Browser Security

- Content Security Policy headers restrict script execution to trusted origins
- Strict Transport Security enforces encrypted-only connections
- Standard protections are in place against clickjacking and content-type sniffing

Additional Protections

- Cross-site request forgery protection on all state-changing requests
- Safeguards against race conditions on concurrent operations
- Comprehensive logging of authentication events and unauthorized access attempts

11 Infrastructure & Compliance

ZeroTrustDrive is deployed on GDPR-compliant European cloud infrastructure, ensuring data sovereignty within the EU. The platform is built for high availability, with redundancy and automatic failover, and separate production and testing environments with full version control.

GDPR & Data Sovereignty

- All data is stored exclusively within the European Union
- No plaintext personal file data is accessible to ZeroTrustDrive staff
- Data minimization: only the metadata necessary for service delivery is stored
- Right to erasure: user data and encrypted files can be permanently deleted on request
- Privacy by design: encryption is an architectural requirement, not an add-on feature

Security Logging & Auditing

The platform maintains comprehensive security event logging, covering unauthorized access attempts, sensitive account and permission changes, authentication events, and infrastructure-level health and availability monitoring.

12 Independent Security Testing

Prior to production launch, and at regular intervals thereafter, ZeroTrustDrive undergoes independent third-party security testing, covering the web application, API, cryptographic implementation, and underlying infrastructure.

- Penetration testing of the web application and API endpoints
- Independent review of the cryptographic implementation
- Infrastructure hardening assessment
- Load and resilience testing

> *Enterprise customers and regulated-industry clients may request a summary of our penetration test results and security certification under NDA. Contact: security@zerotrustdrive.com*

13 Product Features Summary

Feature	Description
End-to-End Encryption	Client-side AES-256 encryption, per file
Zero-Knowledge Architecture	Our servers never hold plaintext keys or data
Team Secure Sharing	File sharing via protected team keys
Master Key Protection	Strong key derivation from your passphrase
File Self-Destruction Timer	Programmable file expiry and auto-deletion
Multi-Device Support	Consistent secure access across all your devices
Role & Permission Management	Admin, manager, member, guest, reseller roles
Two-Factor Authentication	SMS or authenticator app (TOTP)
Contact Management	Organized contact lists for sharing
File Tagging System	Tags for fast file search and organization
White-Label Module	Full re-branding capability for resellers
Reseller / Sub-Accounts	Multi-tier account management for MSPs
Cloud Storage Management UI	Visual encrypted file browser
GDPR-Compliant Infrastructure	EU data residency
Independent Security Testing	Regular third-party penetration testing

14 Conclusion

ZeroTrustDrive represents a fundamentally different approach to cloud file storage: one where security is not a feature layer added on top, but the architectural foundation upon which everything else is built. By combining zero-knowledge encryption, hybrid RSA/AES cryptography, rigorous access control, and GDPR-compliant European infrastructure, ZeroTrustDrive delivers a platform where organizations can store and share their most sensitive data with confidence.

The platform has been designed for real-world usability as much as maximum security: team sharing works seamlessly without manual key exchanges, file access management is intuitive, and the SaaS model — with white-label and reseller support — makes it commercially viable for managed service providers and enterprise resellers across multiple industries.

> *For technical inquiries, enterprise evaluations, or to request our security documentation, please contact ZeroTrustDrive at info@zerotrustdrive.com — zerotrustdrive.com*