Privacy by Design: How ZTmail Protects User Privacy

September 20, 2026

Privacy protection is not a feature that should be added after a product has been designed. For ZTmail, it is part of the reason the platform exists. From the beginning, the company brand name – ZoTrus came from zero trust, it has represented a commitment to treating privacy as a fundamental security boundary rather than as a statement made only in a policy document.

Email is essential to everyday life, education, and business, but it also carries identity information, contracts, financial records, confidential discussions, and details about personal and professional relationships. Protecting privacy therefore requires more than securing the message while it is in transit. It requires architecture that limits unnecessary data collection, keeps cryptographic authority with the appropriate party, and provides automation without turning convenience into centralized custody.

This article does not restate ZTmail's formal privacy terms. Instead, it explains the architectural and operational decisions through which ZTmail seeks to protect user privacy in practice.

1. Making Encryption Automatic at the User Endpoint

Much of the information exchanged through email is traditionally stored as readable content on mail servers. Transport encryption such as TLS can protect a connection while a message is moving between systems, but it does not by itself ensure that the message remains encrypted after it reaches a mail server, a backup system, or another storage environment. If the message is stored in plaintext, anyone who gains inappropriate access to the relevant mailbox or server may be able to read it.

Privacy concerns do not end with message content. For many email services, reading users' email and displaying targeted advertising has become a major revenue model, while the growing use of email data and user interactions for AI training introduces another important question: how much of a user's private information should a service provider be able to access, retain, or reuse?

ZTmail was created to address this gap by making S/MIME encryption practical and automated at the user endpoint. The objective is not to ask users to remember a manual encryption procedure for every sensitive message. It is to make signing, encryption, decryption, certificate handling, and verification part of the normal email workflow.

© 2026 **ZoTrus Technology Limited**



The user's email is protected with the appropriate public keys, and the resulting encrypted message remains within the user's own email server. ZTmail does not need to retain a readable copy of the user's mail in its cloud merely to provide automated encryption, the encryption is done by ZTmail App in user's device, not in the cloud.

Automation matters because privacy protection that depends entirely on manual discipline will be applied inconsistently. By making S/MIME operations part of the normal email experience, ZTmail reduces avoidable mistakes while preserving user control over the underlying cryptographic material. And the emails are stored in encrypted form on the user's mail server, effectively preventing anyone other than the user from reading the private information in emails.

2. Deliberately Not Providing a Public-Key Exchange Service

At an early stage, ZTmail considered public-key exchange to be one of the main barriers to wider email encryption. In a conventional S/MIME workflow, the sender needs the recipient's public certificate before an encrypted message can be prepared. This appears to create a need for a certificate directory that can locate a recipient's certificate before a message is sent.

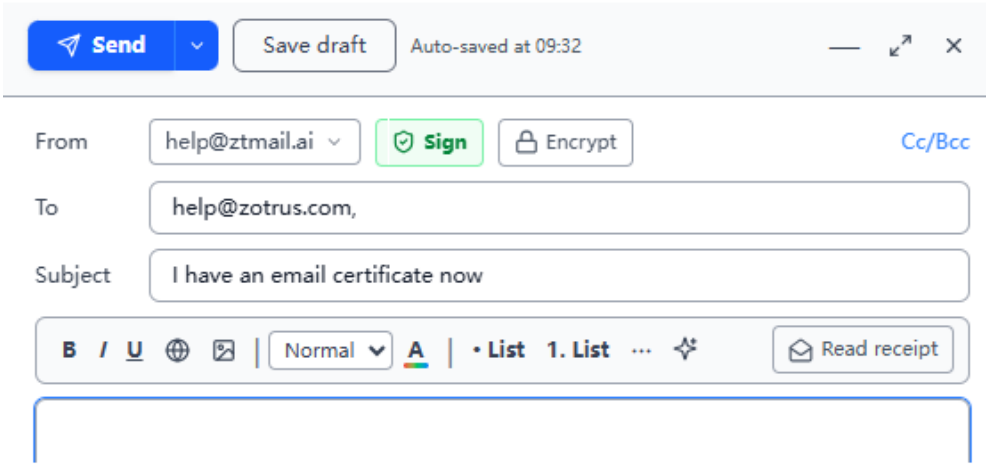
Further evaluation, however, showed that a centralized public-key lookup service could expose sensitive metadata about communication relationships. A service that records which sender is searching for which recipient's certificate could potentially reveal who is preparing to communicate with whom, which organizations are connected, or which recipients a user is contacting on a particular day. Even without message content, this relationship data can itself be private.

For that reason, ZTmail deliberately decided not to provide a centralized public-key exchange service. This is a privacy-oriented architectural decision: it avoids creating a new central observation point for users' communication patterns when the technical problem can be addressed through ordinary email interaction.

The practical obstacle is also less absolute than it first appears. When a user sends a digitally signed S/MIME email, the sender's public certificate can be included with the message. After the recipient receives the signed message, the email client can extract the public certificate and store it locally. When

© 2026 **ZoTrus Technology Limited**

the recipient later replies with an encrypted message, the locally available certificate can be used without a prior lookup through a third-party directory.



The parties already have a reason to communicate by email. A signed message can carry the public certificate needed for subsequent encrypted communication, allowing certificate exchange to occur as part of normal correspondence without requiring ZTmail to operate a service that observes certificate-search activity.

3. No Key Escrow, But Automated Key Management

A user's cryptographic keys are among the most sensitive assets associated with encrypted email. A private key enables the user to decrypt protected correspondence and preserve access to historical encrypted messages. Whoever controls that key may possess the practical ability to access information that encryption was intended to protect.

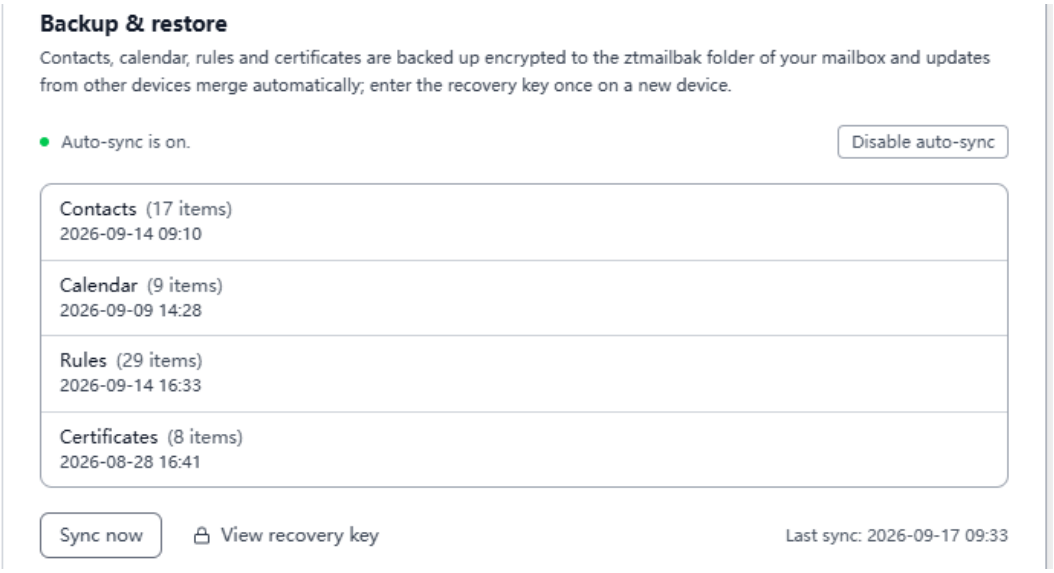
ZTmail therefore does not position itself as a key-escrow provider that takes custody of readable user keys for the S/MIME automation service. ZTmail's cloud services can provide certificate automation and trusted CA connectivity without requiring ZTmail to maintain a readable copy of a user's private key or to become the holder of the user's decryption authority.

At the same time, simply telling users to manage every backup, export, migration, and recovery task on their own would not be responsible. Manual key management is error-prone, especially when users change devices, reinstall operating systems, migrate email clients, or need to open messages encrypted years earlier.

ZTmail's solution is to provide automated key-management functions without turning them into key custody. Relevant certificate and private-key material are packaged into an encrypted backup archive

© 2026 **ZoTrus Technology Limited**

and automatically stored in the user's own mailbox rather than uploaded as readable key material to a ZTmail-controlled repository. The mailbox provides storage and synchronization, while the backup remains encrypted.



The user remains responsible for protecting the Recovery Key needed to unlock the archive. ZTmail automates the work of creating, updating, storing, and retrieving the backup, but it does not assume ownership of the secret that grants access to the protected material.

4. No Centralized Address-Book Backup, But User-Controlled Automatic Synchronization

Address books are more than convenience data. They can reveal customers, suppliers, colleagues, family members, partners, professional relationships, and organizational structure. Calendars can reveal meetings, travel plans, project schedules, and sensitive business activity. Mail-sorting rules may also expose how a user classifies and prioritizes communications.

Many services automatically synchronize this information to the provider's cloud because centralized storage makes multi-device access easier. The convenience is real, but the model can create a persistent collection of personal relationship data outside the user's direct control.

ZTmail does not provide a centralized address-book backup service in which users' contacts are routinely copied into a ZTmail-controlled cloud. At the same time, refusing to provide any synchronization mechanism would be impractical. Users who carefully organize contacts, calendars, and mail-sorting rules on one device should not have to recreate that work on every other device.

ZTmail therefore applies the same privacy-oriented backup model used for certificate and private-key material. Contacts, calendars, and mail-sorting rules can be included in an automated backup package

© 2026 **ZoTrus Technology Limited**

and stored in the user's own mailbox rather than in ZTmail's cloud. The user's mailbox becomes the user-controlled backup data's synchronization channel.

This approach balances privacy and usability. The service provider does not automatically accumulate a separate cloud copy of the user's address book and relationship graph, while the user can still move to another device and recover the working environment. Automation reduces repetitive work without silently expanding the amount of personal information held by the platform.

5. Outsourcing Identity Validation to Specialized Providers

Some ZTmail paid services, including the Trusted Identity Edition and the Global Ecosystem Edition, depend on identity validation. These services may require validated information about an individual, an organization, or the relationship between them so that an S/MIME certificate can express an appropriate level of identity assurance.

Identity validation is a specialized activity with operational, regulatory, security, and data-protection requirements. Rather than building a broad identity-validation operation inside ZTmail and collecting large amounts of identity evidence directly, ZTmail follows a data-minimization principle and uses specialized professional providers for the validation process.

Under this model, a professional identity validation provider performs the relevant identity checks, such as individual validation for an IV certificate. The specific provider or providers may vary by market and service arrangement. ZTmail has evaluated the appropriate specialized multi-providers for worldwide customers.

ZTmail should not retain unnecessary identity-proofing materials or raw personal identity data, such as identity-document numbers, simply because a user has completed validation. Instead, it needs only the identity information required for the resulting certificate and service operation, such as the validated individual name and organization name that must appear in the identity certificate.

This separation reduces the amount of sensitive identity evidence ZTmail itself needs to collect and retain. Specialized providers perform identity validation, while ZTmail uses the resulting validated identity attributes for the cryptographic certificate and trusted-identity experience.

6. Protecting Document Privacy Through Local and Cloud Signing

Privacy by design should extend beyond email messages to the documents people sign. Contracts,

© 2026 **ZoTrus Technology Limited**

financial records, personal documents, business proposals and internal company files may contain information that users do not want to transfer to another signing service simply to obtain a digital signature.

Many online document-signing workflows require the original document to be uploaded to the signing platform. The platform then manages the document as part of the signing transaction. Although this model can be convenient, it introduces another environment in which the original document must be handled and protected.

ZTmail Sign takes a different architectural approach. It divides the signing process between ZTmail App on the user's device and a cloud signing service, without requiring the original document to leave the device.

ZTmail App calculates the document's cryptographic hash locally using SHA-2 and sends only the hash to the cloud signing service. The cloud service signs the hash using its trusted platform-identity signing certificate and returns the signed data. ZTmail App completes the document-signing process locally.

This design allows the cloud to provide the required signing capability without receiving the original document. It helps protect personal information and commercial secrets by reducing the need to transfer sensitive documents into an external platform's document-management environment.

ZTmail Sign also supports digital signing with the user's own identity certificate. In this mode, the signature presents the user's validated identity rather than the platform signing identity used by the cloud signing service. Both models are integrated into the same document workflow, while preserving the distinction between platform-based cloud signing and signing with the user's own certificate.

The principle is consistent with ZTmail's broader privacy architecture: automates the cryptographic work without collecting or taking custody of information that does not need to leave the user's control. For email, ZTmail makes encryption practical at the user endpoint. For document signing, it separates the original document from the cloud signing operation. In both cases, the goal is the same: make cryptographic capabilities easier to use without making unnecessary data transfer a condition of convenience.

7. Privacy Protection Is an Architectural Commitment

The privacy model described here is not based on a single feature. It is the combined result of several

© 2026 **ZoTrus Technology Limited**

decisions: make S/MIME encryption automatic at the user endpoint; avoid operating a centralized public-key exchange service that could reveal communication relationships; do not take custody of readable private keys; automate encrypted backup while leaving recovery authority with the user; avoid creating a centralized cloud copy of address books and related personal data; and use specialized providers for identity validation while applying data minimization to retained information; and separate document signing between the user's device and the cloud so that the original document does not need to be uploaded to the signing service.

These choices reflect a consistent distinction between automation and ownership. ZTmail seeks to automate the work required to make cryptographic email and e-document practical, but automation should not require the platform to collect everything, observe everything, or control every secret. A system can provide synchronization without becoming the owner of a user’s contact graph. It can provide certificate services without holding readable private keys. It can support validated identity without retaining every piece of identity evidence used during validation; It can provide document signing services without having to upload the original document to be signed.

For ZTmail, privacy protection is therefore not limited to preventing unauthorized access to message content or the document has been tampered with or accessed illegally. It also means reducing unnecessary data collection, avoiding avoidable metadata exposure, preserving user control over cryptographic authority, and designing cloud services so that convenience does not automatically become centralized custody.

The next generation of email security and document security will combine cryptography, automation, and user experience so that trust is no longer assumed, but verified throughout email, chat and document lifecycle. This is the direction ZTmail is committed to advancing: making privacy personal or organizational and protected.

Richard Wang

September 20, 2026
In Shenzhen, China

© 2026 **ZoTrus Technology Limited**

Follow ZTmail at X (Twitter) for more info.
The author has published 132 articles in English (more than 184K words) and 290 articles in Chinese (more than 861K characters in total).



© 2026 **ZoTrus Technology Limited**