

Hybrid Trust: ZTmail's Innovative Trust Model

October 22, 2026

Digital trust should not force users to choose between global interoperability, rich identity display, and affordable certificate costs. Nor should the transition to post-quantum cryptography require organizations to abandon existing cryptographic infrastructure overnight.

ZTmail addresses these challenges through an innovative approach called **Hybrid Trust**. By combining two trust domains and applying multiple digital signatures, ZTmail enables standard email clients and document readers to validate globally trusted signatures while ZTmail App presents additional trusted identity information. The same architectural approach also provides a foundation for a future transition to post-quantum cryptography.

To understand Hybrid Trust, we first need to understand ZTmail's two trust domains.

1. Two Trust Domains: ZTmail Trust and Global Trust

ZTmail operates two complementary trust domains: **ZTmail Trust** and **Global Trust**. Each serves a different purpose within the cryptographic application ecosystem.

● **ZTmail Trust**

ZTmail Trust is the trust domain established within the ZTmail ecosystem. It supports trusted identity services and cryptographic applications for email and documents, including identity levels such as:

- **T2 — Individual Validation (IV):** Presents the validated individual's name.
- **T3 — Organization Validation (OV):** Presents the validated organization's name.
- **T4 — Sponsor Validation (SV):** Presents the validated organization's name and the employee's name.

These identity certificates enable ZTmail App to display the corresponding trusted identity information after validating the relevant digital signature and certificate information. ZTmail Trust is designed to support trusted identity and cryptographic application services within the ZTmail ecosystem.

● **Global Trust**

Global Trust connects ZTmail's cryptographic applications with the wider global ecosystem. It relies on certificates issued by publicly trusted Certificate Authorities (CAs), supporting interoperable

S/MIME email signatures and document signatures that can be validated by compatible applications outside the ZTmail ecosystem like Outlook for emails and Adobe Reader for PDF documents.

Global Trust covers both S/MIME certificates and document signing certificates. Its role is to provide a globally recognized cryptographic trust path, allowing standard clients and document readers to validate signatures without depending on ZTmail App.

● **Two Domains, Complementary Roles**

The distinction is straightforward:

- **ZTmail Trust** provides trusted identity services and identity presentations within the ZTmail ecosystem.
- **Global Trust** provides public-CA-based trust and interoperability across the wider ecosystem.

These two trust domains are complementary rather than competing, because for large-scale organizational applications, most signing and encryption stuff is still done within the organization. ZTmail innovatively brings them together to deliver a practical combination of interoperability, trusted identity display, and cost efficiency, this is called “Hybrid Trust”.

2. What Is Hybrid Trust?

Hybrid Trust is a ZTmail trust model that combines a globally trusted digital signature with a second digital signature based on ZTmail Trust.

Instead of requiring every identity certificate to be issued by an international public CA, Hybrid Trust separates two functions: establishing global interoperability and presenting a more detailed validated identity within ZTmail App. The model applies to both email signing and document signing.

● **Hybrid Trust for Email Signing**

In the optimized email certificate strategy, the sender uses:

- A globally trusted MV (Mailbox Validation) S/MIME certificate issued by a public CA.
- A ZTmail Trust IV, OV, or SV identity certificate issued by ZTmail CA.

The globally trusted MV certificate provides the standard S/MIME trust path. The additional identity signature enables ZTmail App to present the sender’s validated identity at the appropriate level.

For recipients using compatible standard email clients, such as Microsoft Outlook, the globally trusted S/MIME signature can be validated through the public CA trust chain. ZTmail App can additionally validate the second signature and display the corresponding **T2**, **T3**, or **T4** trusted identity information.

As shown in the table below, no matter what type of S/MIME certificate a user uses to sign an email, Microsoft Outlook only shows a valid signature icon. This means that the Microsoft Outlook UI and ZTmail App UI display for Hybrid Trust looks the same as Global Trust.

	Global Trust	Hybrid Trust
Outlook UI	Signed By help@zotrus.com 	Signed By help@zotrus.com 
ZTmail App UI	T2 [CN] [Richard Wang]   T3 [CN] [Email @ ZoTrus Technology Limited]   T4 [CN] [Richard Wang @ ZoTrus Technology Limited]  	T2 [CN] [Richard Wang]   T3 [CN] [Email @ ZoTrus Technology Limited]   T4 [CN] [Richard Wang @ ZoTrus Technology Limited]  

● Hybrid Trust for Document Signing

The same principle can be applied to document signing.

The first signature uses a cloud-signing service and a platform signing certificate trusted by compatible document readers. The second signature uses the signer's ZTmail Trust IV, OV, or SV document signing certificate.

A compatible document reader, such as Adobe Reader, can validate the platform signature through its applicable trust configuration. ZTmail App can validate the additional identity signature and display the corresponding **T2**, **T3**, or **T4** trusted identity information.

As shown in the table below, no matter what type of document signing certificate users use to digitally sign a PDF document, Adobe Reader always shows the signatures are valid, which makes the Adobe Reader UI and ZTmail App UI display for Hybrid Trust looks the same as Global Trust.

	Global Trust	Hybrid Trust
Adobe Reader UI (Standard)	 Signed and all signatures are valid.	 Signed and all signatures are valid.
ZTmail App UI	  T2 [CN] Richard Wang   T3 [CN] ZoTrus Technology Limited	  T2 [CN] Richard Wang   T3 [CN] ZoTrus Technology Limited

	  T4 [CN] Richard Wang @ ZoTrus Technology Limited	  T4 [CN] Richard Wang @ ZoTrus Technology Limited
--	--	--

The two signatures serve complementary purposes: one establishes the applicable external trust path, while the other provides additional identity evidence within the ZTmail ecosystem.

● Why Does Hybrid Trust Matter?

Besides having the same UI display in the app, you can also get a real sense of the actual value of Hybrid Trust by comparing the product prices of the two. The table below shows a price comparison of the two types of trust plans for ZTmail.

Identity level	Global Trust	Hybrid Trust
T2 — IV	US\$29 / year	US\$17 / year
T3 — OV	US\$36 / year	US\$20 / year
T4 — SV	US\$39 / year	US\$21 / year

The Hybrid Trust option combines a public-CA-issued MV certificate with a ZTmail-issued IV, OV, or SV identity certificate. This reduces certificate costs while preserving global S/MIME interoperability and the corresponding identity display in ZTmail App. The pricing advantage is significant, especially for organizations that need trusted identity presentation for many employees.

The key is to understand what is, and is not, being replaced. Hybrid Trust does not turn a ZTmail Trust identity certificate into a globally trusted public-CA certificate. Instead, it uses a globally trusted signature for interoperability and a second identity signature for the richer identity experience within ZTmail App.

The result is a more cost-effective way to combine global interoperability with trusted identity presentation.

3. How Does Hybrid Trust Work?

Hybrid Trust uses two digital signatures; each associated with its own certificate and trust domain. The implementation differs slightly between email and documents.

● Email: Global S/MIME Signature Plus ZTmail Identity Signature

If user chooses services related to hybrid trust, or the user imports a globally trusted S/MIME MV certificate, ZTmail App will automatically sign the email using Hybrid Trust, it creates an S/MIME digital signature with the globally trusted MV certificate first, then adds a second signature associated with the ZTmail Trust IV, OV, or SV identity certificate, using a CMS (Cryptographic Message Syntax) signature structure.

This arrangement provides two distinct validation paths.

For email clients like Outlook:

- (1) The client receives the digitally signed email.
- (2) It validates the global S/MIME signature against the public CA certificate chain and its configured trust policies.
- (3) It can display the signature as valid and the signing certificate as trusted when those checks succeed.

For ZTmail App:

- (1) The app validates the global S/MIME signature.
- (2) It validates the additional identity signature.
- (3) It reads the identity certificate information and displays the appropriate **T2**, **T3**, or **T4** icon and corresponding trusted identity details.

The result is an email that can benefit from global S/MIME interoperability while also displaying richer validated identity information in ZTmail App.

The two signatures are independently verifiable according to their respective certificate chains, signature formats, and trust policies. Each verification result can be evaluated on its own merits.

● **Documents: Cloud Platform Signature Plus ZTmail Identity Signature**

For document signing, if user chooses services related to hybrid trust, ZTmail App will combine a platform-based cloud signature with an additional identity signature.

The first signature is produced through ZTmail cloud-signing service using the platform signing certificate. This provides an economical way to establish a signature that compatible document readers can validate through the applicable trust configuration. The second signature uses the signer's ZTmail Trust IV, OV, or SV document signing certificate. ZTmail App validates this signature and presents the corresponding **T2**, **T3**, or **T4** icon and identity information.

Consequently, the document can offer two complementary experiences:

- **In Adobe Reader:** The platform signature can establish the applicable signature-validity and trust status.
- **In ZTmail App:** The additional signature supports the display of the signer's T2, T3, or T4 trusted identity information.

This model combines external signature validation with identity presentation in the ZTmail ecosystem without requiring every user to purchase a globally trusted identity certificate.

The exact verification result depends on the signature structure, certificate chain, application support, and trust configuration.

4. Hybrid Trust as a Foundation for Post-Quantum Cryptography Migration

Hybrid Trust is not limited to combining two trust domains. It underlies a principle: using multiple signatures with different cryptographic properties can also support the transition to post-quantum cryptography (PQC).

Quantum computing poses a long-term challenge to widely deployed public-key cryptographic algorithms. As organizations prepare for post-quantum safe, they need migration strategies that preserve existing interoperability while introducing new algorithms in a controlled manner.

A sudden switch to PQC could create compatibility challenges for existing email clients, document readers, certificate infrastructures, and business systems. A hybrid approach offers a potential path forward.

● Combining Traditional and Post-Quantum Signatures

ZTmail plans to support S/MIME signing and encryption using PQC-capable certificates and algorithms. For digital signatures, the proposed Hybrid Trust approach can combine a traditional signature with a second signature using a PQC algorithm.

The signing process would work conceptually as follows:

- (1) ZTmail App creates the traditional S/MIME digital signature using a conventional algorithm.
- (2) Following a CMS-compatible design, it adds a second digital signature using a supported PQC algorithm.
- (3) The resulting signed email or document carries signatures based on two different cryptographic algorithms.
- (4) Compatible traditional clients validate the conventional signature, while PQC-capable

applications validate the PQC signature.

This allows different applications to verify the signature they support, provide the email format, algorithm identifiers, certificate profiles, and verification implementations are compatible. The same architectural principle can be applied to documents, allowing traditional and PQC signature verification to coexist during a migration period.

● **A Gradual Transition, not a Forced Replacement**

The purpose of this approach is to make migration more manageable. Organizations can retain a conventional signature path for existing systems while introducing PQC signatures for applications that support them.

Over time, as PQC-capable clients and document readers become more widely available, organizations can expand their use of post-quantum algorithms without making an immediate, ecosystem-wide replacement a prerequisite.

However, successful migration requires more than adding a second signature. Certificate profiles, algorithm support, signature encoding, trust policies, and interoperability must all be addressed. PQC encryption also requires suitable hybrid key-establishment and encryption design; a dual-signature mechanism alone does not provide post-quantum confidentiality.

Hybrid Trust therefore provides an architectural direction for migration, while actual PQC deployment depends on supported standards and interoperable implementations.

5. One Architecture, Multiple Trust Challenges

ZTmail's Hybrid Trust model addresses two distinct challenges through a shared architectural idea.

For trust and identity:

- Global Trust provides public-CA-based interoperability.
- ZTmail Trust provides additional validated identity information within the ZTmail ecosystem.
- The combined model reduces certificate costs while preserving the intended user experience.

For post-quantum migration:

- Traditional signatures support compatibility with existing applications.
- PQC signatures provide a path toward adopting quantum-resistant signature algorithms.
- A carefully designed hybrid implementation can support coexistence during migration.

These applications share the principle of combining complementary cryptographic capabilities rather than relying on a single trust path or algorithm for every requirement.

6. Hybrid Trust, a ZTmail Innovation

Digital trust is not a single certificate or a single verification result. It involves interoperability, certificate trust, validated identity, application support, and the ability to evolve as cryptographic requirements change.

ZTmail's Hybrid Trust model brings together two complementary trust domains: ZTmail Trust and Global Trust. For email and document signing, it combines a globally trusted signature with an additional ZTmail Trust identity signature, enabling compatible external applications to validate the global signature while ZTmail App presents richer trusted identity information.

This architecture creates a practical commercial advantage: users can obtain global interoperability and the intended trusted identity display in ZTmail App at a lower certificate cost than purchasing globally trusted IV, OV, or SV certificates. The savings on this certificate are crucial for large-scale deployments in medium and large organizations.

Beyond today's trust and pricing challenges, the same multi-signature design principle offers a potential foundation for introducing post-quantum signatures alongside traditional algorithms.

Hybrid Trust is more than a certificate strategy. It is a flexible trust architecture designed to connect global interoperability, trusted identity, cost efficiency, and the evolution of cryptography.

Richard Wang

October 22, 2026
In Shenzhen, China

Follow ZTmail at X (Twitter) for more info.

The author has published 141 articles in English (more than 204K words) and 300 articles in Chinese (more than 909K characters in total).

