

KNOWLEDGE BASE · PUBLIC DOCUMENT

TLS or end-to-end encryption in e-mail: what each one protects, and when you need it

Comparisons and alternatives

CODE

RLX-MZ-KB-2079

VERSION

v2026.10.20

COUNTRY · LANGUAGE

Mozambique · English

MozOut Mozambique

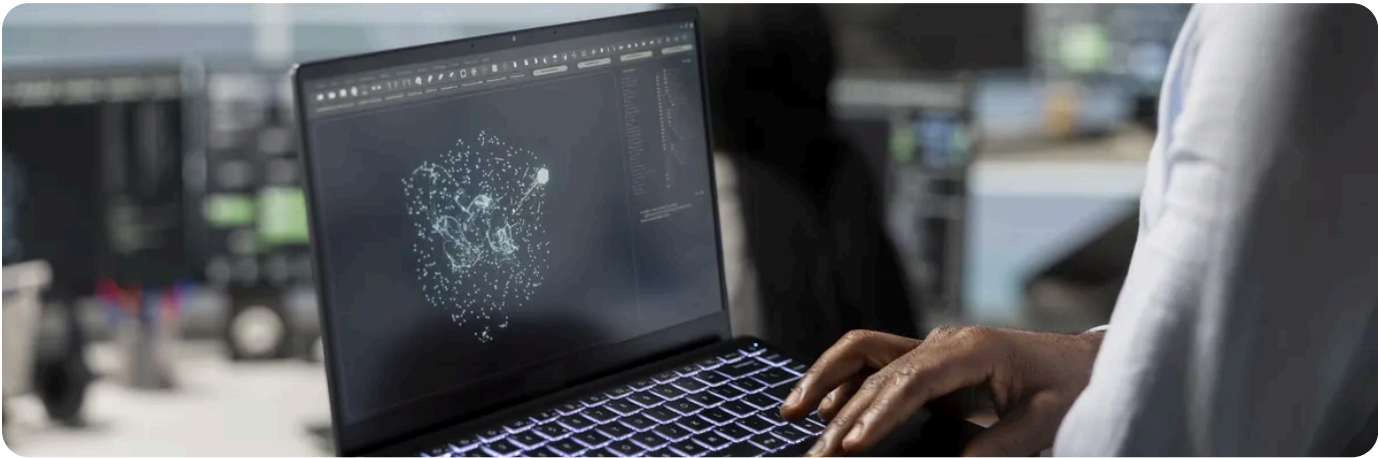
RLX Holdings, S.A. · Group RLX Holdings

Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

<https://www.meu.mozout.co.mz/knowledgebase/2079>

TLS or end-to-end encryption in e-mail: what each one protects, and when you need it

 Comparisons and alternatives  Created on **October 16, 2026**  Updated on **October 20, 2026**  4 min read



The short answer: **TLS** encrypts the message **on the way**: between your device and our server, and between servers when both sides accept it. Once delivered, the message sits readable in the sender’s and the recipient’s mailboxes. **End-to-end encryption** (S/MIME or OpenPGP) encrypts the **content**, so only the recipient can open it, but both sides have to set it up. For everyday mail TLS is enough; for sensitive documents, consider end-to-end or a simpler alternative.

What each one protects

Kind	What it protects	What it does not protect
TLS between your device and our server	Your password and messages in transit, for example on public Wi-Fi. It is on when the app uses SSL/TLS or STARTTLS.	The message stored on the server and on the device.
TLS between our server and the recipient’s	The hand-over from one server to the other, when both accept an encrypted connection.	It does not depend only on us or on you: it also depends on the recipient’s server. And the copy kept there is readable.
S/MIME	The content and attachments, with a certificate per person. It can also sign, to prove who sent it.	The subject, sender, recipients and dates usually stay visible. Both sides need a certificate.
OpenPGP	The content and attachments, with a key pair per person.	The same as S/MIME, and every recipient needs their public key exchanged beforehand.
Password-protected file	The attached document, if the password travels by another channel.	The e-mail text, and the subject.

➔ What to do in practice

1 Make sure every app uses an encrypted connection: IMAP on 993 with SSL/TLS, SMTP on 465 with SSL/TLS or on 587 with STARTTLS. Never choose “None” for security. See **SMTP ports 465, 587 and 25**.

2 Open webmail only at its https address, with the padlock in the browser: **how to access your webmail**.

3 For sensitive documents, weigh up end-to-end. Both sides need certificates or keys, and programs that use them: Outlook, Apple Mail and Thunderbird support S/MIME, and Thunderbird includes OpenPGP. In webmail and on phones, support varies.

4 The simple alternative: send the document as a password-protected file and give the password by another channel, by phone or by message.

5 If you use end-to-end, keep the private key or certificate somewhere safe. Without it, old encrypted messages no longer open, not even for you.

! The padlock does not make a message secret forever.
Once delivered, it sits readable in the recipient’s mailbox and on every device that syncs it. Do not send passwords, card data or identity documents by e-mail just because the connection is encrypted. And be wary of messages asking for them: **how to recognise phishing**.

💡 A protected file plus the password by another channel
covers most cases without either side installing certificates.

🗣️ NEED A HAND?

Not sure your app is using an encrypted connection? Tell us which one you use and send a screenshot of the account settings, without the password.

 **Open a support ticket** ➔

📁 Where to see it in your account

✓ The right settings: in cPanel, **Email Accounts**, the **Connect Devices** button next to each account shows the secure settings: the incoming and outgoing server, IMAP on 993, POP3 on 995 and SMTP on 465, all with SSL/TLS, and the username, which is the full address.

- ✓ **In your program:** check the connection security of each server (SSL/TLS, or STARTTLS on 587) and that the outgoing server asks for authentication. In Thunderbird it is in **Account Settings**, under **Server Settings** and **Outgoing Server (SMTP)**.
- ✓ **S/MIME and OpenPGP live in the program, not on the server:** in Outlook under **Trust Center > Email Security**; in Thunderbird under **Account Settings > End-To-End Encryption**. The private key stays on your device.
- ✓ **In webmail**, an encrypted message usually shows up as an attachment called smime.p7m or as a block of scrambled text: open it in the program that holds the key. Signed messages read normally.

SEE ALSO

SMTP ports 465, 587 and 25: SSL, STARTTLS and which one to use



How to access your webmail



How to recognise a phishing e-mail or message, and what to do if you clicked



Your e-mail account has been hacked: what to do in the first hour



Keeping your own copy of your e-mail: how to back up a mailbox



The Gmail app or the Outlook app for your domain mailbox: phone and computer compared



MozOut Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT) 401 191 607

LEGAL ENTITY NO. (NUEL) 105 045 974

ECONOMIC ACTIVITY
CODE (CAE) 62022

REGISTERED OFFICE Bairro 7 de Setembro
Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique

CONTACT info@mozout.co.mz · +258 84 635 1111 · +258 86 635 1111 ·
www.mozout.co.mz

OPENING HOURS Monday to Friday - 08 AM to 04 PM
Saturday & Sunday - Closed



Online version of this
document

RLX-MZ-KB-2079 · v2026.10.20 · Generated on 21/10/2026 17:45