

CryptSecure for Outlook & Word

Installation and User Guide

Version 3.0.5

Encrypt email and documents in one click,
right inside Outlook and Word.

Installed in minutes · Nothing new to learn · Post-quantum · Keys locked to you

Applies to CryptSecure for Outlook & Word 3.0.x (current release 3.0.5). Requires the CryptSecure app 3.0.5 or newer for Windows on the same computer.

Opey's IT · November 2026

Why CryptSecure for Outlook & Word

Encrypt the email. Keep the workflow.

CryptSecure for Outlook & Word puts a **CryptSecure** button in Microsoft Outlook and Microsoft Word. Click it, write, and your email, its attachments or part of your document are encrypted and signed before they leave your computer. Your recipient clicks the same button to open it. No new program to learn, no new mailbox, no change to the way you work.

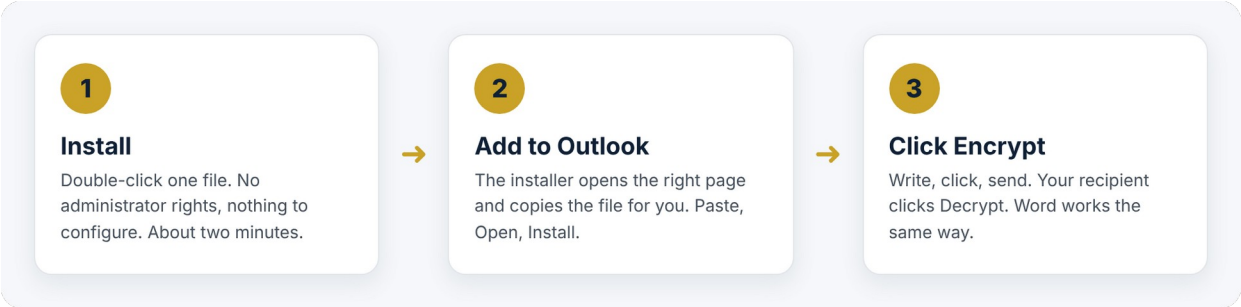


Figure 1. From download to your first encrypted email in three steps.

Easy to install

- **One file, one double-click.** About ten minutes from download to your first encrypted email. No administrator rights and nothing to configure.
- **The installer does the technical part.** It sets up the secure connection, prepares Word, adds Start menu shortcuts and starts itself every time you sign in.
- **Just as easy to remove.** One entry in Settings › Apps takes everything away again; your keys are never touched (section 12).

Easy to integrate

- **Works where you already work.** Classic Outlook, the new Outlook for Windows, Outlook on the web and Microsoft Word. Add it to your mailbox once and it appears in every Outlook you use.
- **Same keys, same contacts, same broker.** It uses the keys, contacts and CryptSecure broker you already have in the CryptSecure desktop app. No new account, no new server, no change to your email system.
- **Ready for whole teams.** Each person installs it in minutes, or your IT department can roll it out to everyone.

Easy to use

- **One button. Encrypt** in a new email, **Decrypt** in a received one. Recipients are filled in from **To** and **Cc** automatically.
- **Opens by itself.** The panel finds the encrypted message and opens it. Pin it, and every email you click opens automatically.
- **Find anyone by email address.** Connected to your organization's CryptSecure broker, the panel fetches a colleague's key the moment you address them. No key files to swap.
- **Reply in one click. Encrypt a reply to the sender** writes an encrypted reply for you. Files go along, encrypted with the message.

© 2026 Opey's IT

- **Groups and older keys handled for you.** Address several people and each opens the same email with their own key. If someone also has an older key, CryptSecure always uses their strongest one.
- **Clear answers.** A coloured banner tells you, in plain words, who sent the message and that nothing was changed.

Security you can prove

- **Post-quantum by default.** Every message is sealed with ML-KEM-1024 + ECDH P-384 (the CNSA 2.0 suite) and AES-256-GCM, and signed with ML-DSA-87: NIST-standardized algorithms (FIPS 203 and FIPS 204).
- **New in 3.0.5: your keys are locked to you.** Your private keys are stored encrypted and open only with this computer's TPM, a security key or your passphrase. A stolen laptop or a copied key folder gives nobody your keys, and CryptSecure shows you every time Outlook or Word uses them.
- **Your keys never leave your computer.** All cryptography runs in the CryptSecure app on your PC. The add-in talks only to your own computer.
- **Proof it arrived intact.** Sender and recipient see the same SHA-256 fingerprint. If one character changes on the way, the message will not open (section 8 shows it from start to finish).

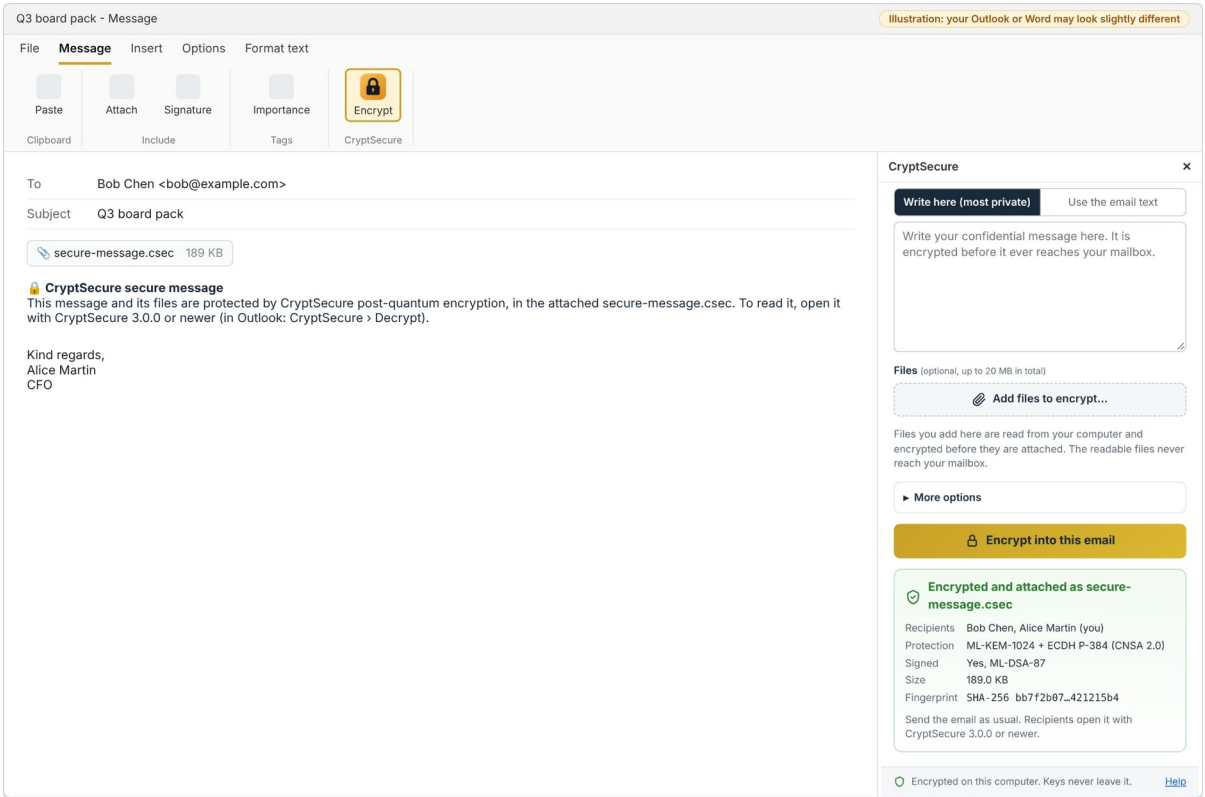


Figure 2. One click: the email now carries only the encrypted attachment, and the panel confirms who can open it (illustration around a real panel screenshot).

© 2026 Opey's IT

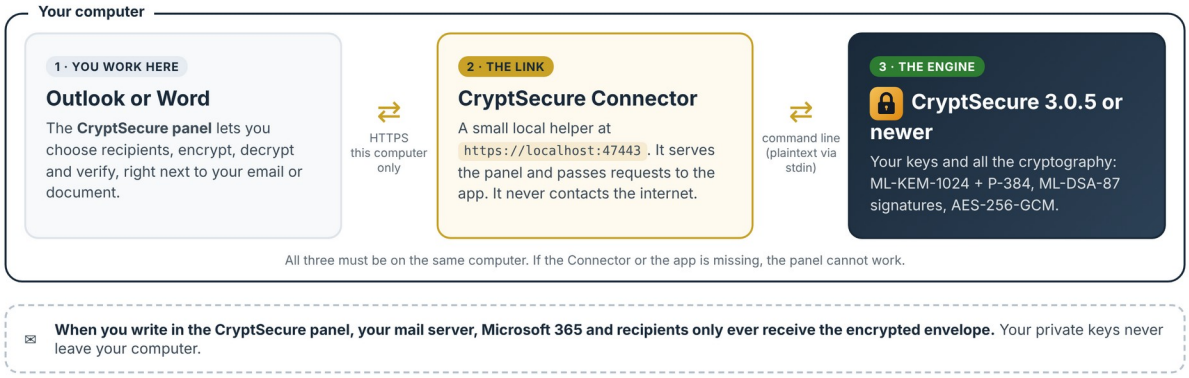


Figure 3. How the three parts work together on your computer.

© 2026 Opey's IT

Contents

Why CryptSecure for Outlook & Word 2

1 Before you start 7
1.1 What you need 7
1.2 Which Outlook works 8
1.3 How to read this guide 9

2 Install 10
2.1 Check CryptSecure (3.0.5 or newer) and your key 10
2.2 Run the installer 10
2.3 Check that it is running 15
2.4 Add CryptSecure to Outlook 15
2.5 Open CryptSecure in Word 18
2.6 Send yourself a test email 18

3 Connect to your broker 20
3.1 Connect once, in the CryptSecure app 20
3.2 If the panel says something else 21

4 Send an encrypted email 23
4.1 The panel at a glance 23
4.2 Encrypt an email 24
4.3 Write to someone new: find them on your broker 27
4.4 What your recipient receives, and more options 28

5 Open an encrypted email 30
5.1 Open it and check who sent it 30
5.2 When something is wrong 31
5.3 When CryptSecure asks you to unlock your keys 32

6 Reply securely 34

7 Contacts and trust 35
7.1 Share your public key and add contacts 35
7.2 Verify a contact with safety numbers 36
7.3 Your older keys and one address with several keys 37

8 Example from start to finish 38

9 Use CryptSecure in Word 42
9.1 Encrypt text 42
9.2 Open encrypted text 44

10 Quick reference: how do I 45

11 Help and troubleshooting 46
11.1 The status light and panel messages 46
11.2 Check that everything is working 47
11.3 Common problems and fixes 49
11.4 Get support 50

12 Update or remove 52
12.1 Update or repair 52

© 2026 Opey's IT

12.2 Remove CryptSecure (uninstall) ... 52
12.3 Remove it from Outlook ... 53
12.4 Uninstall the Connector ... 53
12.5 Check that everything is gone ... 56
12.6 Reinstall later ... 56
12.7 If something goes wrong ... 56

13 Your privacy and security ... 58
13.1 What stays on your computer ... 58
13.2 How the Connector is protected ... 58
13.3 What it cannot protect ... 58
13.4 Good practice ... 58

Glossary ... 59

Legal notices ... 60

© 2026 Opey's IT

1 Before you start

CryptSecure for Outlook & Word is three parts working together on **one** computer (Figure 3). The Office add-in is the panel you see. It does not encrypt anything itself: it hands every request to the **CryptSecure Connector**, which passes it to the **CryptSecure** app (3.0.5 or newer), where your keys live and all the cryptography happens.

> **CRITICAL: The three must-haves**
>
> 1. **CryptSecure 3.0.5 or newer** installed on this computer (3.1 and later also work), with **your own key** created in it.
> 2. The **CryptSecure Connector** installed and **running** whenever you use the panel.
> 3. The **CryptSecure add-in** added to Outlook (and, if you want it, Word).
>
> If any of these is missing, the panel shows a red status light and tells you which one. If the Connector is not running at all, Outlook cannot open the panel and shows a blank or error page instead.

1.1 What you need

Requirement	Needed for	Details and how to check
Windows 10 or 11, 64-bit	Everything	Settings › System › About shows "64-bit operating system".
CryptSecure desktop app, 3.0.5 or newer	All encryption, decryption, signing and keys	From the Microsoft Store or your organization. Checked in step 2.1.
Your own CryptSecure 3 key	Signing what you send and opening what is sent to you	Created in the desktop app: **Keys & contacts › New key...**
CryptSecure Connector 3.0.5	Linking Outlook and Word to the app	Installed by **CryptSecure-for-Outlook-and-Word-Setup-3.0.5**, the file you download (step 2.2). It includes everything it needs; nothing else to download. Starts automatically at sign-in.
Microsoft Outlook	Encrypting and opening email	Outlook for Microsoft 365, Outlook 2021 or 2024, the new Outlook for Windows, or Outlook on the web, with a Microsoft 365, Outlook.com or Exchange account.
Outlook that supports the Mailbox 1.8 API	Encrypted attachments, opening .csec attachments, attaching your public key	Microsoft 365, Outlook 2021 and later. Older Outlook can still encrypt and open message text.
Microsoft Word (optional)	Encrypting text in documents	Word for Microsoft 365, or Word 2016 or later, on Windows.

© 2026 Opey's IT

Requirement	Needed for	Details and how to check
Internet connection	Outlook and Word load Microsoft's add-in framework	The encryption itself happens on your computer, offline.
Permission to add custom add-ins	Adding the Outlook add-in	Personal accounts allow it. Work accounts may block it; your IT department can then add it for you.
Your contacts' public keys	Encrypting to someone	Exchange .cspub files, or find them on your CryptSecure broker.

1.2 Which Outlook works

Outlook add-ins are attached to your mailbox, so once you add CryptSecure (step 2.4) it appears in every supported Outlook you use with that account. Each one still needs the Connector running on the computer you are using.

Outlook	Supported?	Notes
Classic Outlook for Windows: Microsoft 365, Outlook 2021, Outlook 2024	✔️ Yes	Full support, including attachments and the pinned panel.
Classic Outlook 2016 or 2019, retail (bought from a shop or Microsoft)	✔️ Yes	Full support. If the Microsoft Edge WebView2 Runtime is not installed, Outlook uses the older Edge component: install WebView2 (recommended), or ask your IT department for the one-line loopback setting.
Classic Outlook 2016 or 2019, volume-licensed (from an organization)	✖️ No	These show add-ins with Internet Explorer 11, which cannot run modern secure add-ins. The panel says so and explains what to do. Use the new Outlook or Outlook on the web instead. Microsoft ended all support for Office 2016 and 2019 on October 14, 2025.
New Outlook for Windows	✔️ Yes	Full support. The button is under **Apps** on the ribbon.
Outlook on the web (Microsoft 365 and Outlook.com) in Edge or Chrome	✔️ Yes	On the computer where the Connector runs.
"Light version" of Outlook on the web	✖️ No	It does not run add-ins, and Microsoft has retired it. If you see it, update your browser and sign in again.
Outlook Lite (Android)	✖️ No	Microsoft retired the app on May 25, 2026. It did not run add-ins.

© 2026 Opey's IT

Outlook	Supported?	Notes
Outlook for Mac, iPhone, iPad and Android	✖ Not in 3.0.x	CryptSecure and the Connector run on Windows.

CRITICAL: Recipients need CryptSecure 3 too

Only someone with CryptSecure 3.0.0 or newer (the desktop app, or this add-in) and the right private key can open what you send. Make sure your recipients have it, and that you have their public key, before you send something important.

NOTE: No administrator rights needed

Everything installs for your own Windows account. The Connector uses the keys of the Windows user who runs it, so each person on a shared PC sets it up under their own sign-in.

1.3 How to read this guide

This guide takes you from nothing installed to sending your first encrypted email, then explains every part of the panel. It assumes no technical knowledge: every click, every command and every result you should see is spelled out.

You see	It means
Bold	Something on screen to click, choose or look for, such as **Encrypt** or **My add-ins**.
`Monospace`	Text to type exactly, a command, a file name or a folder.
Sample output	What you should see. Dates, thumbprints, user names and fingerprints will differ on your computer.
CRITICAL, NOTE, TIP, CHECK, WHY	Coloured boxes. CRITICAL means the add-in will not work, or your security depends on it.

NOTE: Versions

This guide covers CryptSecure for Outlook & Word 3.0.5 and also applies to the earlier 3.0.x releases. All CryptSecure products carry the same version number. **Add-in 3.0.5 works with the CryptSecure app 3.0.5 or newer** (3.1 and later too). With an older app (3.0.0 to 3.0.5, or the Microsoft Store package 3.0.1, which reports 3.0.0) the panel shows **Update needed** and does nothing until CryptSecure is updated. Messages are compatible both ways: anyone with CryptSecure 3.0.0 or newer can open what you send. For everything else about the desktop app, see the CryptSecure Encryption Client 3.0.5 User Guide.

© 2026 Opey's IT

2 Install

Allow about 10 minutes. Do the steps in order: each one shows the screens you will see, and gold outlines mark what to click.

Step	What you do	Time
2.1	Check that CryptSecure 3.0.5 or newer is installed and that you have a key	2 min
2.2	Double-click the downloaded installer	2 min
2.3	Make sure the Connector is running	1 min
2.4	Add the add-in to your Outlook mailbox	3 min
2.5	Find the CryptSecure button in Word	1 min
2.6	Test it with an email to yourself	2 min

2.1 Check CryptSecure (3.0.5 or newer) and your key

1. Open the **CryptSecure** app from the Start menu (from the Microsoft Store it is listed as **CryptSecurev3.0**). Choose **Settings › About**: it must show version **3.0.5** or a higher number. If CryptSecure is not installed, or is older, install or update it first (Microsoft Store › Library › Get updates).
1. Open the **CryptSecure** app from the Start menu and choose **Keys & contacts**. Under **My keys** you should see your name. If the list is empty, choose **New key…**, enter your name and email address, leave **Type** on **CryptSecure 3 … (recommended)**, and choose **OK**.
2. Close the Command Prompt.

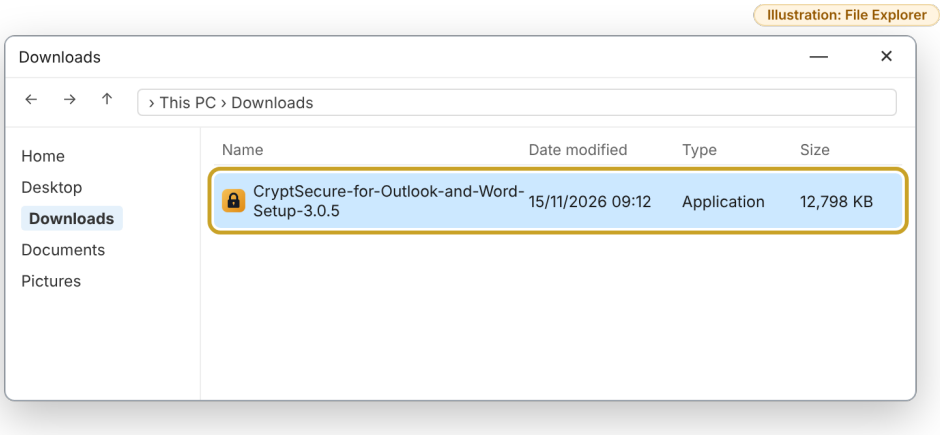
2.2 Run the installer

Every screen you will see is shown below, in order. Gold outlines mark what to click.

1 Close Outlook and Word.

© 2026 Opey's IT

2 Download **CryptSecure for Outlook & Word** from the Opey's IT website (or get it from your IT department). Open your **Downloads** folder and double-click **CryptSecure-for-Outlook-and-Word-Setup-3.0.5**: the file with the gold padlock icon, Type **Application**. (If your File Explorer shows file extensions, its name ends in `.exe`.)



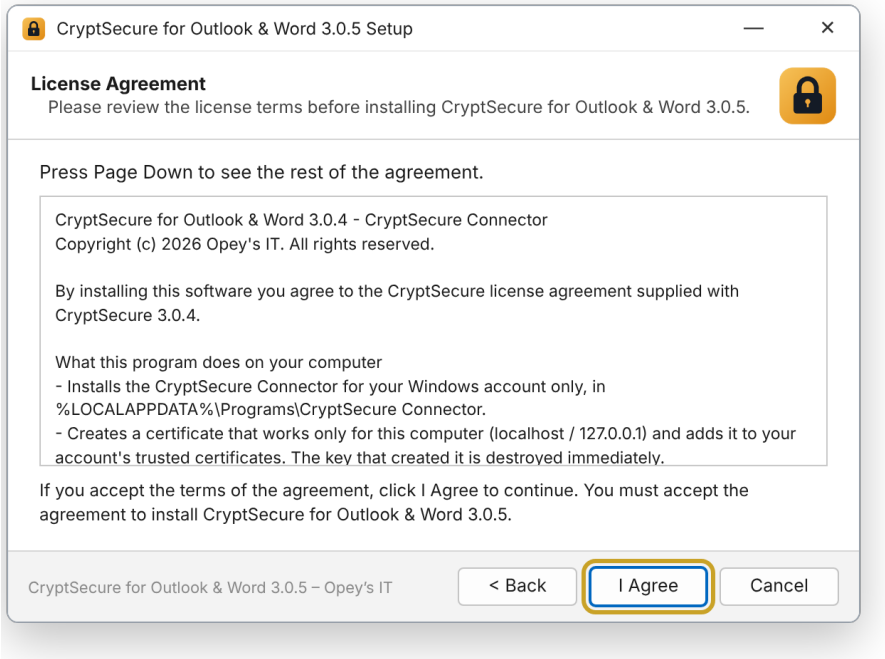
3 If a blue **Windows protected your PC** message appears, the installer is simply new to Windows. Choose **More info**, then **Run anyway**, but only if the file came from Opey's IT or your IT department.

4 The **Welcome** page says **Install CryptSecure for Outlook & Word 3.0.5**. Choose **Next**.



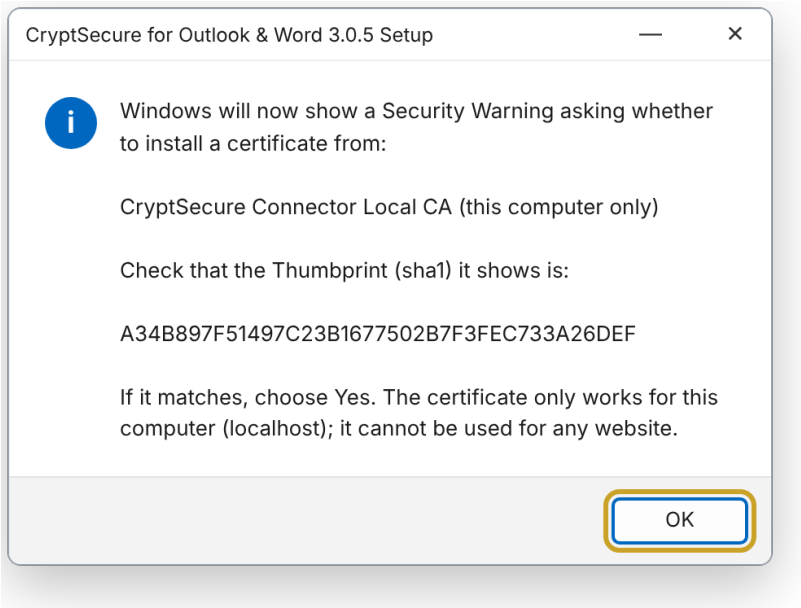
© 2026 Opey's IT

5 The **License Agreement** page explains exactly what the Connector does on your computer. Choose **I Agree**.

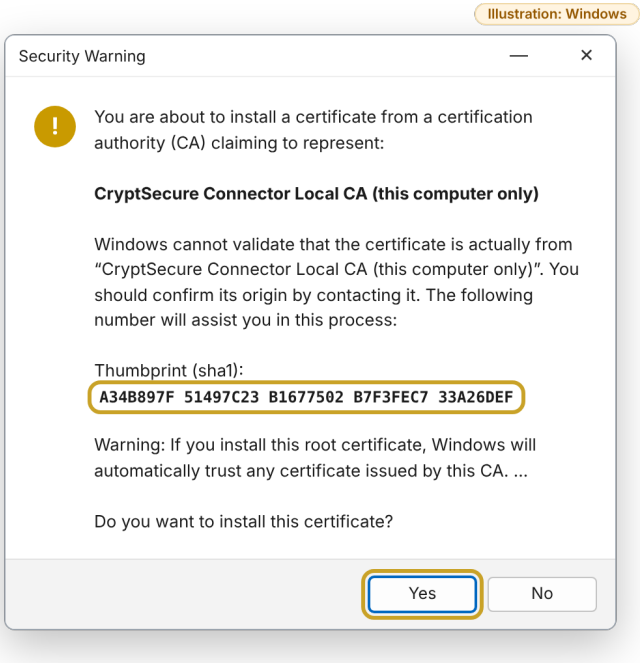


6 The installer copies its files and checks for CryptSecure 3.0.5 or newer. If the app is missing or older, a message says so: choose **Cancel**, do step 2.1, and run the installer again.

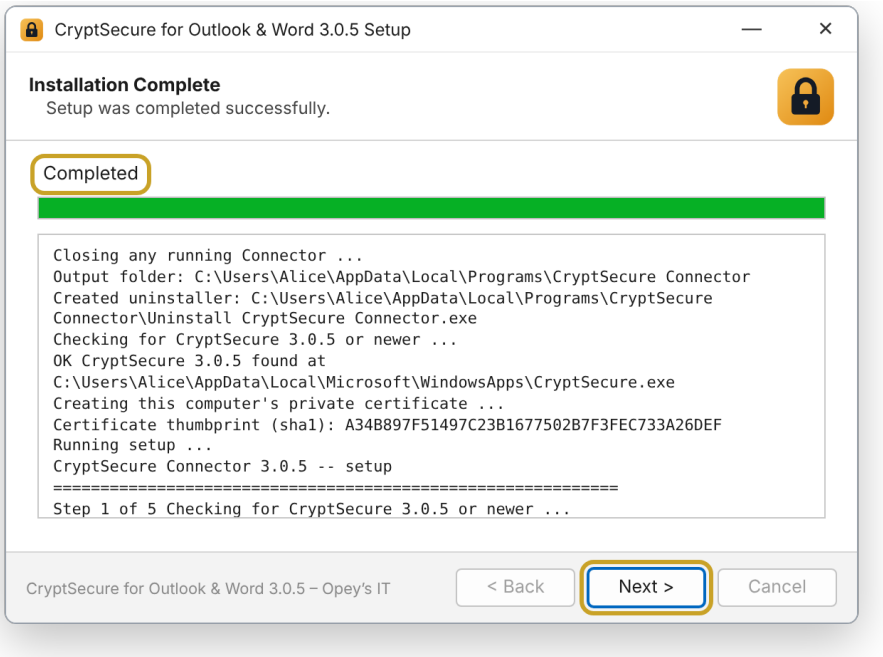
7 A message shows the certificate **thumbprint**, a 40-character code such as `A34B897F51497C23B1677502B7F3FEC733A26DEF` (yours is different). Keep it on screen and choose **OK**.



8 Windows shows a **Security Warning** about **CryptSecure Connector Local CA (this computer only)**. Check that its **Thumbprint (sha1)** is the code from the previous step. If it matches, choose **Yes**.



9 The installer finishes the setup and starts the Connector (a minimized **CryptSecure Connector** window appears on the taskbar: leave it there). When the page says **Completed**, choose **Next**.



© 2026 Opey's IT

10 The last page says **CryptSecure is installed and running**. Leave **Add CryptSecure to Outlook now** ticked and choose **Finish**. Continue with step 2.3.



WHY: Why Windows asks about a certificate, and why it is safe

Outlook only loads add-ins over a secure (HTTPS) connection. The certificate lets Outlook talk securely to the Connector on your own computer.

It is technically limited to **localhost** and **127.0.0.1** (your own computer), so it cannot be used to impersonate any website. The key that created it was destroyed immediately after use, so nothing else can ever be signed with it. It is installed for your Windows account only.

CRITICAL: If the installer says "Setup did not finish completely"

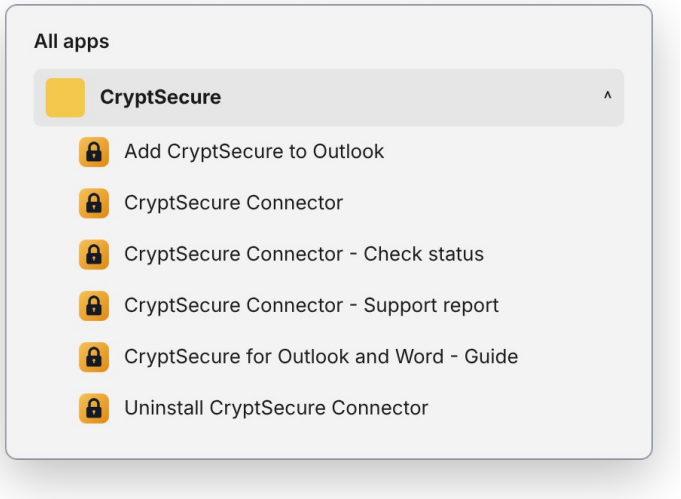
The details list shows the reason on the line that starts with X. If you chose **No** in the Security Warning, choose **Retry** and then **Yes**. If CryptSecure (3.0.5 or newer) is missing, choose **Cancel**, do step 2.1 and run the installer again. Section 11.3 lists every cause.

© 2026 Opey's IT

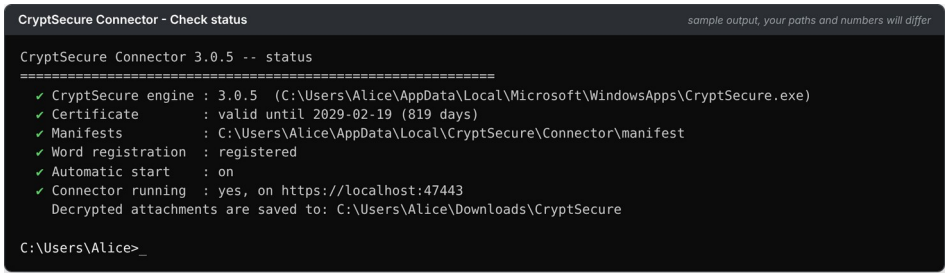
2.3 Check that it is running

1 Your Start menu now has a **CryptSecure** folder with everything you need, now and later. Choose **Start › CryptSecure › CryptSecure Connector - Check status**.

Illustration: Windows Start menu



2 A window opens and every line shows ✔. Close it. That is all: the Connector is running and starts by itself every time you sign in.



NOTE: The small CryptSecure Connector window on the taskbar

Leave it there: Outlook and Word use it whenever you open the CryptSecure panel. If you close it by mistake, choose **Start › CryptSecure › CryptSecure Connector**.

CRITICAL: Classic Outlook 2016 or 2019 only: check for WebView2

Open **Settings › Apps › Installed apps** and look for **Microsoft Edge WebView2 Runtime**. If it is not there, install it from Microsoft (the free **Evergreen Bootstrapper**), then restart Outlook. Microsoft 365, Outlook 2021, Outlook 2024 and the new Outlook do not need this step.

2.4 Add CryptSecure to Outlook

Outlook add-ins are added to your **mailbox**, so after this step CryptSecure is available in every Outlook you use with this account: classic Outlook, the new Outlook and Outlook on the web.

© 2026 Opey's IT

When you chose **Finish** in step 2.2, three things opened: a Command Prompt with these instructions (Figure 4), a File Explorer window showing the file `CryptSecure-Outlook.xml`, and Edge at the Outlook add-ins page. The file's full path is already copied, ready to paste. (To do this again later: **Start › CryptSecure › Add CryptSecure to Outlook**.)

Add CryptSecure to Outlook *sample output, your paths and numbers will differ*

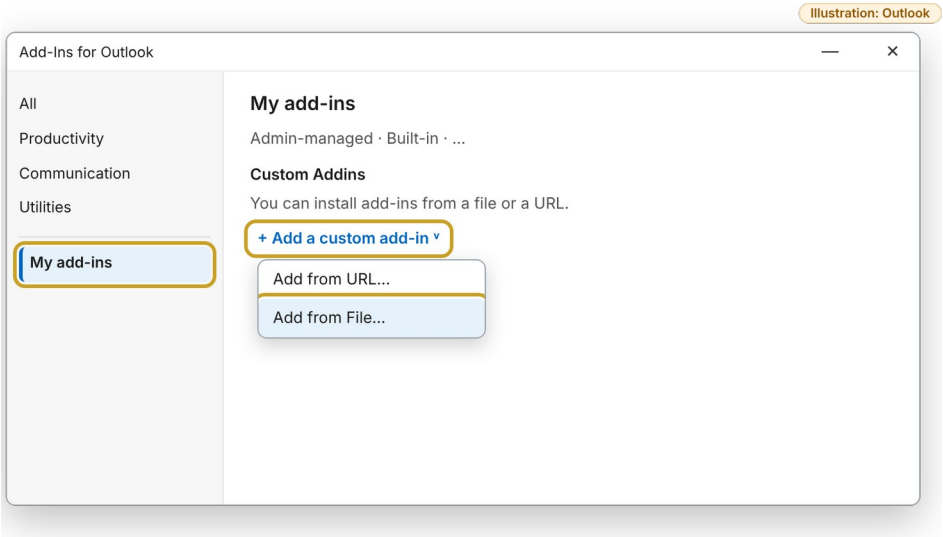
```
Add CryptSecure to Outlook
============================================================
1. In the page that opens, choose  My add-ins  (sign in if asked).
2. Under  Custom Addins  choose  Add a custom add-in > Add from File...
3. In the file window, paste (Ctrl+V) this path into the File name box and choose Open:
     C:\Users\Alice\AppData\Local\CryptSecure\Connector\manifest\CryptSecure-Outlook.xml
4. Choose Install, then close the window and restart Outlook.

C:\Users\Alice>_
```

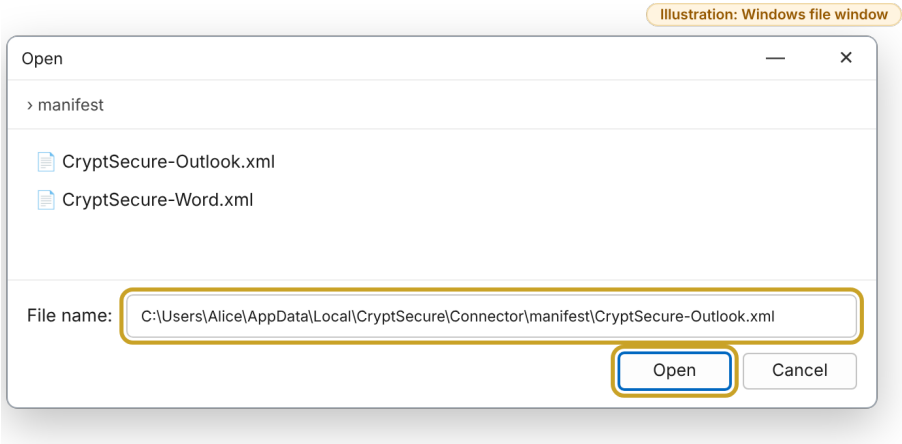
Figure 4. The instructions window opened by the installer.

1 In Edge, sign in with the account you use in Outlook if asked. Outlook on the web opens and, after a few seconds, the **Add-Ins for Outlook** window appears. (If it does not, go to `https://aka.ms/olksideload`. In classic Outlook you can also choose **Get Add-ins** on the **Home** tab or **File › Info › Manage Add-ins**; in the new Outlook, **Apps › Add apps**. They open the same window.)

2 On the left, choose **My add-ins**. Scroll down to **Custom Addins**, choose **Add a custom add-in**, then **Add from File...**.

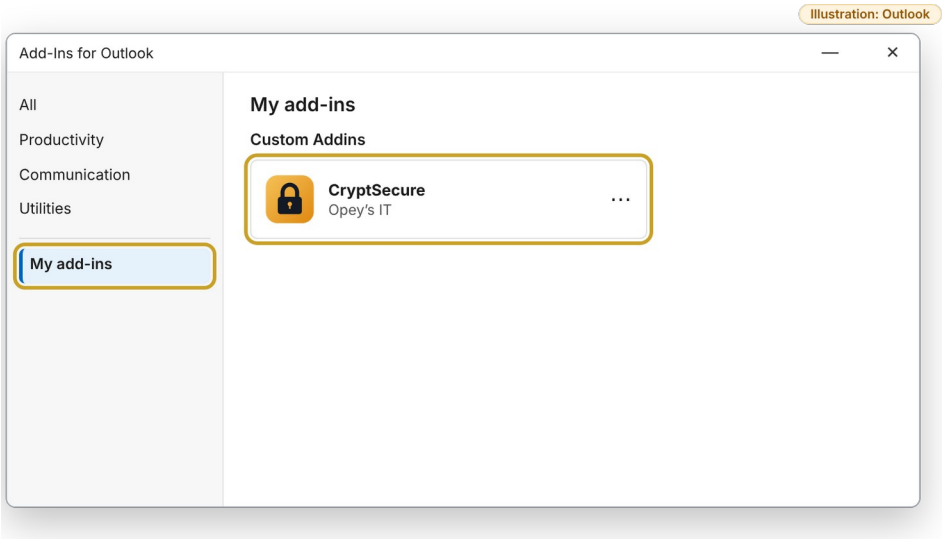


3 In the file window, click in the **File name** box, press **Ctrl + V** to paste the path, and choose **Open**.



4 A warning explains that the add-in has not been verified by Microsoft. This is normal for add-ins supplied directly by a vendor or your organization. Choose **Install**.

5 CryptSecure now appears under **Custom Addins**. Close the window, the Command Prompt and the File Explorer window.



6 Close and reopen Outlook.

> **NOTE: If Ctrl + V pastes nothing**
> Type the path instead: in the file window's address bar type `%LOCALAPPDATA%\CryptSecure\Connector\manifest`, press **Enter**, select `CryptSecure-Outlook.xml` and choose **Open**.

© 2026 Opey's IT

CHECK: You should now see

In a **new email**, an **Encrypt** button. In a **received email**, a **Decrypt** button. Where they are depends on your Outlook:

Outlook	Where the CryptSecure buttons are
Classic Outlook, classic ribbon	**CryptSecure** group at the right of the **Home** tab (reading an email) or the **Message** tab (writing one).
Classic Outlook, simplified ribbon	Choose **...** (More commands) at the right of the ribbon, then **CryptSecure**. If your ribbon shows **Apps**, it is there too.
New Outlook for Windows	Choose **Apps** on the ribbon, then **CryptSecure**. If **Apps** is not visible, choose **...** at the right of the ribbon or in the email's header.
Outlook on the web	Same as the new Outlook: **Apps**, then **CryptSecure**.

TIP: Keep the panel open while you read

When reading email in classic or new Outlook, choose the **pin** icon at the top of the CryptSecure panel. The panel then stays open and opens each email you select automatically.

NOTE: Classic Outlook can take a while

Microsoft notes that classic Outlook on Windows can take up to 24 hours to show a newly added custom add-in, because of caching. Outlook on the web and the new Outlook usually show it immediately, so you can start there.

CRITICAL: If there is no "Add a custom add-in" option

Your organization does not allow users to add custom add-ins. Ask your IT department to deploy CryptSecure for you. The Connector still needs to be installed on each computer.

2.5 Open CryptSecure in Word

The installer already registered CryptSecure with Word.

1. Open Word and open any document.
2. On the **Home** tab, look for the **CryptSecure** group at the right and choose **CryptSecure**. The panel opens on the right.
3. If the button is not there: choose **Home › Add-ins** (in some versions **Insert › My Add-ins**), look under **Developer Add-ins**, select **CryptSecure**, and choose **Add**.

2.6 Send yourself a test email

1 In Outlook, create a **new email** addressed to **yourself**.

© 2026 Opey's IT

2. Choose **CryptSecure › Encrypt**. The panel opens with a green **CryptSecure 3.0.5** light (or your newer version number), and you appear under **To** marked **you**.

3. Under **Message**, keep **Write here (most private)** and type `My first CryptSecure message`.

4. Choose **Encrypt into this email**. A green **Encrypted and inserted into your email** card appears. (Section 4.2 shows each of these screens.)

5. Type a subject and choose **Send**.

6. When it arrives, open it and choose **CryptSecure › Decrypt**. The panel opens it and shows **Signed by you**.

CHECK: Installation complete

If you saw your message in step 6, everything is working: the add-in, the Connector, the app and your key.

TIP: Next: reach the people you write to

If your organization has a CryptSecure broker, connect it now (section 3): colleagues are then found automatically by email address. Otherwise, send your public key to your regular contacts (section 7.1) and ask for theirs. Once you have compared safety numbers, every message between you is encrypted and signed with one click.

© 2026 Opey's IT

3 Connect to your broker

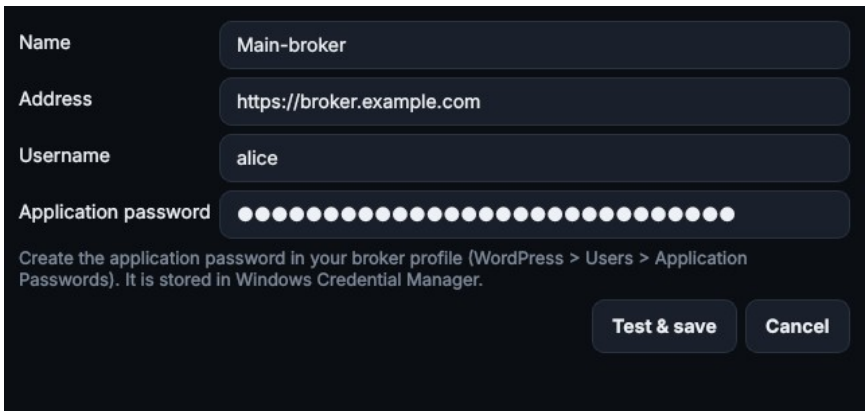
A **CryptSecure broker** is your organization's secure key directory and delivery service. Once you are connected, you never swap key files again: address an email as usual and CryptSecure fetches the right key for you. A broker is optional. Without one, exchange public keys by email instead (section 7.1).

> **NOTE: What you need from your broker operator or IT department**
> The broker's address (it starts with `https://`) and your username. You create the application password yourself in step 1.

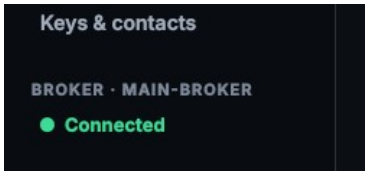
3.1 Connect once, in the CryptSecure app

1. In your broker's web portal, create an **application password**: in WordPress, go to **Users › Profile › Application Passwords**. It is a separate password just for CryptSecure, and you can revoke it at any time without changing your main password.

2. Open the **CryptSecure** app and choose **+ Add a broker** in the sidebar (or **Settings › Brokers › Add broker…**). Enter a name you will recognize, the broker address, your username and the application password, then choose **Test & save**.

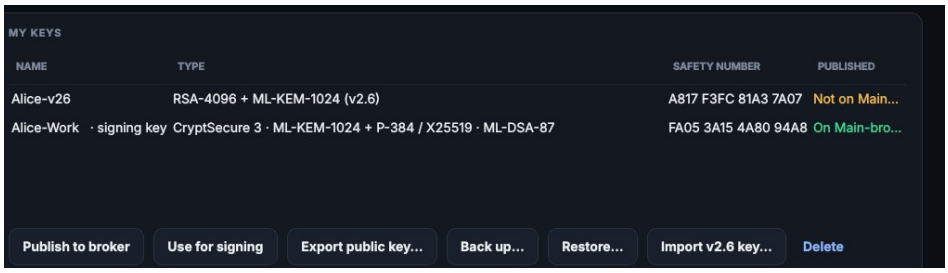


3. CryptSecure checks the connection and your login. The sidebar now shows your broker with a green **Connected** light.

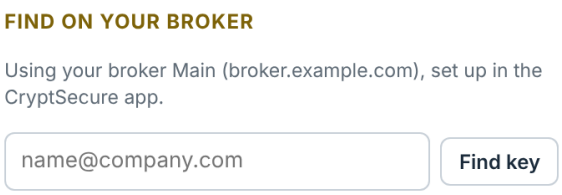


© 2026 Opey's IT

4 Let colleagues find you: choose **Keys & contacts**, select your key under **My keys** and choose **Publish to broker**. The **Published** column then shows **On** and the broker's name.



5 In Outlook, open the CryptSecure panel and choose the **Keys** tab. Under **Find on your broker** it now says **Using your broker**, with your broker's name. Nothing else to set up: the add-in always uses the broker that is active in the CryptSecure app.



3.2 If the panel says something else

The panel says	What it means	What to do
No broker connected	No broker is set up in the CryptSecure app.	Do the steps in 3.1. Or exchange public keys by email (7.1).
No key published for this address yet	The person has not published a key on your broker.	Ask them to publish it (**Publish to broker**), or to email you their public key (.cspub).
Key changed	The key on the broker is different from the one you have for this person.	Phone them and compare safety numbers before accepting the new key in the CryptSecure app. The add-in will not use it until you do.
A red broker light in the CryptSecure app	The broker cannot be reached, or your application password was revoked.	Check your connection. If the light says **Sign-in failed**, create a new application password and update it in **Settings › Brokers**.

© 2026 Opey's IT

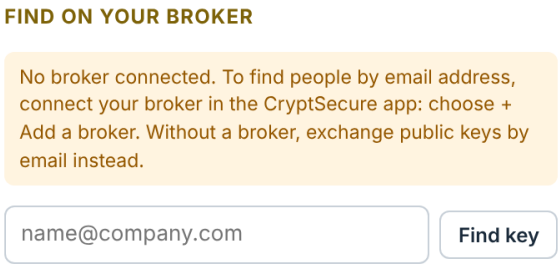
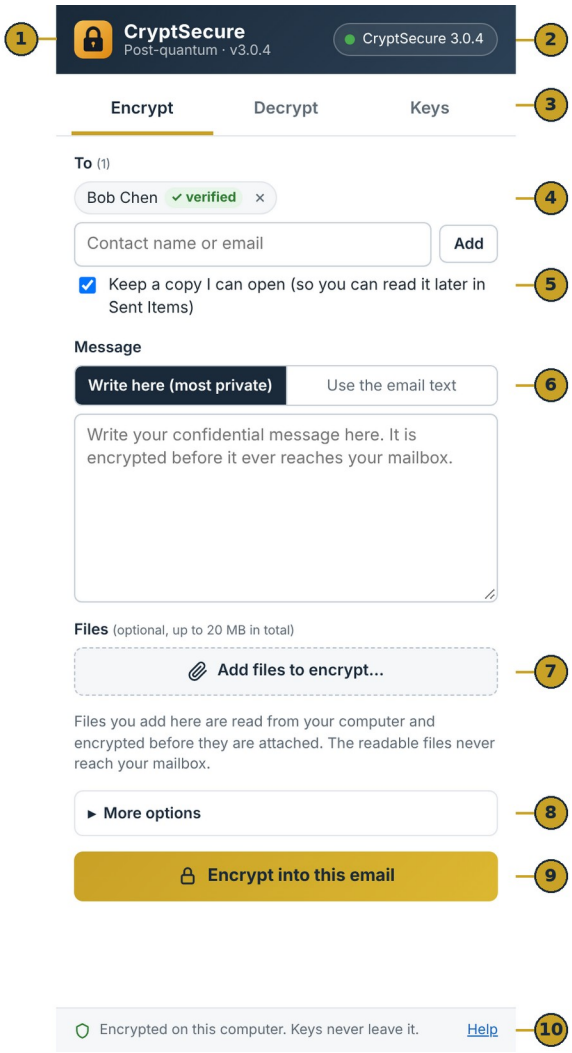


Figure 5. What the Keys tab shows when no broker is connected yet.

© 2026 Opey's IT

4 Send an encrypted email

4.1 The panel at a glance



The Encrypt tab in a new email

#	Part	What it does
1	Title	CryptSecure and the version.
2	Status light	Green: connected to CryptSecure (3.0.5 or newer) and ready. Red: something is missing; the panel says what. Click it to check again.
3	Tabs	**Encrypt**, **Decrypt** and **Keys**. A gold dot on a tab means it has something for you.
4	To	Recipients. Filled in automatically from the email's To, Cc and Bcc when CryptSecure has their key.

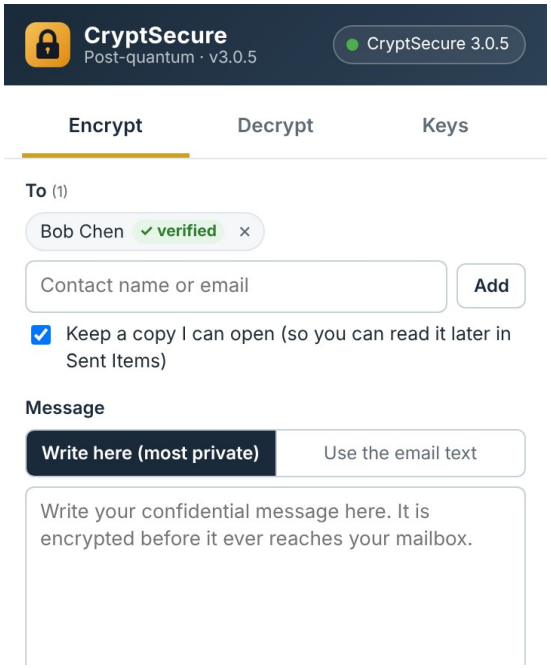
© 2026 Opey's IT

#	Part	What it does
5	Keep a copy I can open	Also encrypts to your own key, so you can read the message later in Sent Items. On by default. Your copy joins the CryptSecure 3 part; if every recipient has only an older 2.6 key there is no such part, so the email goes without your copy and the result card says so.
6	Message source	**Write here** (most private) or **Use the email text**. See 4.2.
7	Files	Files to encrypt with the message, read straight from your computer.
8	More options	Optional passphrase, protection type, and which of your keys signs.
9	Encrypt button	Encrypts, signs and inserts the result into your email.
10	Footer	Reminder that encryption happens on this computer, and a link to help.

4.2 Encrypt an email

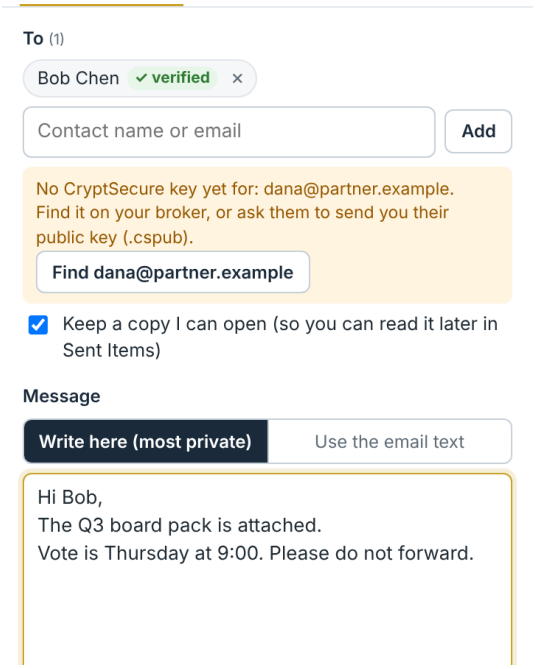
1 Create a new email, or reply, and add your recipients in **To** or **Cc** as usual.

2 Choose **CryptSecure › Encrypt**. Recipients that CryptSecure has keys for appear under **To** with a badge: ✓ **verified** (you compared safety numbers), **unverified** (key known, not yet compared) or **you**.

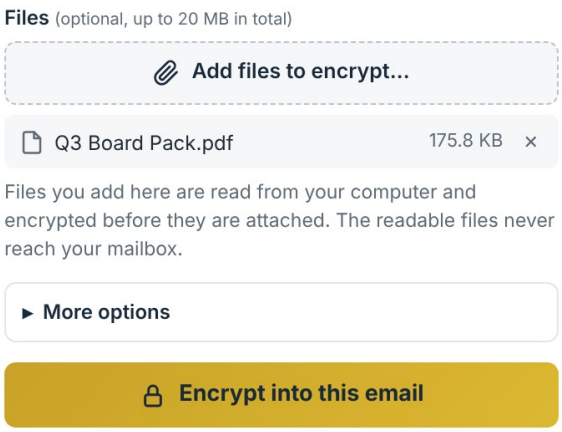


© 2026 Opey's IT

3 Write your message in the panel's box (recommended), or choose **Use the email text** to encrypt what you already typed. If an address has no key yet, an orange note says so, with a **Find** button (for example **Find carol@example.com**) that looks it up on your CryptSecure broker. Without a broker, ask that person for their public key (7.1).

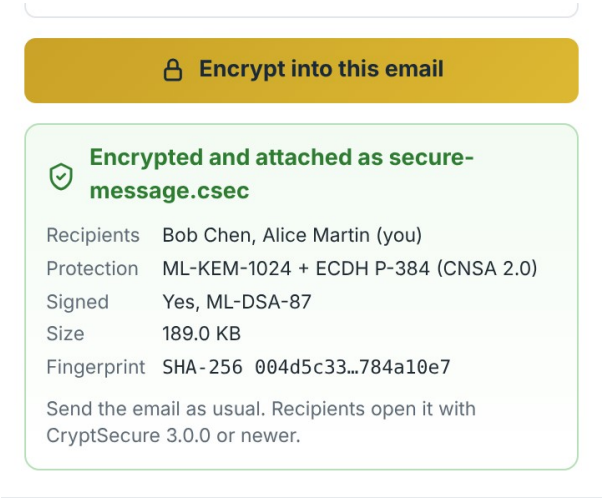


4 Optional: choose **Add files to encrypt...** and pick files from your computer (up to 20 MB in total).



© 2026 Opey's IT

5 Choose **Encrypt into this email**. The green card confirms who can open it. Send the email as usual.



TIP: Sending to several people

Add everyone in **To** and **Cc** as usual, or add them in the panel's **To** box one after another (type a name or address and press Enter): each one is added after the others and nothing is removed; **×** on a chip removes just that person. Everyone with a CryptSecure 3 key shares one encrypted message, and each person opens the email with their own key; nobody else can. You are added automatically (**Keep a copy I can open**), so the email in Sent Items opens for you too.

NOTE: When someone has more than one key

A colleague may have a new CryptSecure 3 key and an older 2.6 key on the same address. CryptSecure always encrypts to the strongest one: CryptSecure 3 first, verified before unverified, then the newest. To use one particular key, type its name in the panel's **To** box: the key you name is used. If the address is also in the email's To, both are used.

NOTE: Recipients with an older CryptSecure 2.6 key

A 2.6 key can only receive a message of its own, so when one is among your recipients the panel says so under **To** ("2 separate encryptions…") and puts one part per 2.6 key into the email, after the part for everyone with CryptSecure 3. Each part is headed "===== CryptSecure: for <name> =====". CryptSecure 3 users (in Outlook, Word or the app) open the email as usual: the right part is picked for them. A CryptSecure 2.6 user copies only the lines under their name. With files, each part is its own attachment (secure-message-for-<name>.csec). The result card lists every part.

© 2026 Opey's IT

Who is in To	What goes into the email or document
Only people with CryptSecure 3 keys (any number, plus you)	One encrypted message (one attachment with files), signed, post-quantum.
CryptSecure 3 people + one or more CryptSecure 2.6 keys	One part for all CryptSecure 3 people (and your copy), plus one part per 2.6 key. Your copy is kept.
Only CryptSecure 2.6 keys	One part per 2.6 key, without your copy (a 2.6 part holds one recipient). Not signed: 2.6 has no signatures.
A 2.6 RSA-only key in any of the above	Same, and that part is not post-quantum (RSA). Every other part still is.

CRITICAL: Write in the panel for the most privacy

Outlook saves drafts to your mailbox automatically while you type. If you type confidential text in the email itself and then use **Use the email text**, a readable draft may already have been saved on the mail server. CryptSecure replaces the text in the email, but it cannot recall a draft Outlook already saved.

When you write in the panel, the text is encrypted before it reaches Outlook at all.

CRITICAL: The subject line is never encrypted

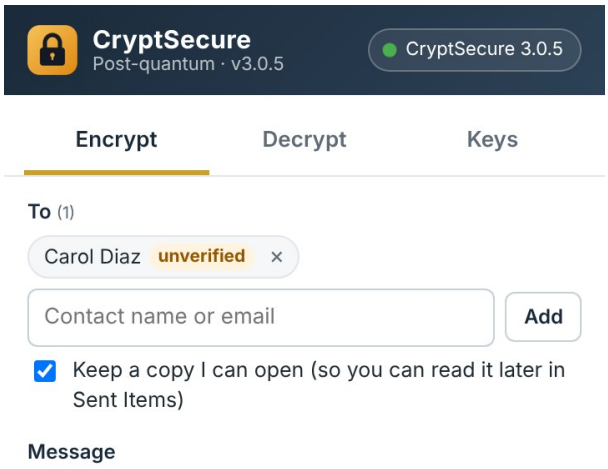
Email subjects, sender, recipients and dates travel unencrypted, as they do for all encrypted email. Keep confidential details out of the subject.

4.3 Write to someone new: find them on your broker

1 Write a new email and address it as usual, then choose **CryptSecure › Encrypt**. If CryptSecure does not have that person's key yet, an orange note offers a **Find** button with their address.



2 Choose the **Find** button. CryptSecure fetches the key from your broker and adds the person under **To**, marked **unverified**. Write your message and choose **Encrypt into this email** as usual.



3 The first time, compare safety numbers with them by phone (section 7.2). It takes a minute and from then on they show ✓ **verified**.

You can also look someone up before writing: on the **Keys** tab, type their address under **Find on your broker** and choose **Find key**. Then choose **Use as recipient** or **Verify…**.

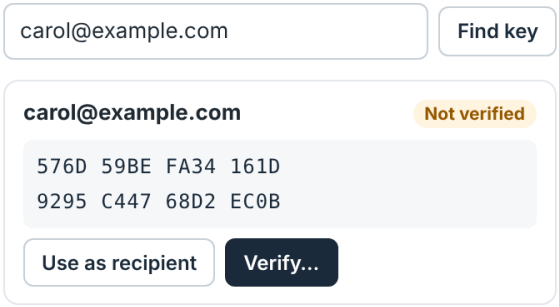


Figure 6. A colleague found on the broker, ready to use and to verify.

4.4 What your recipient receives, and more options

What gets inserted

You encrypted	What the recipient receives
Text only	A short line explaining the message is protected by CryptSecure, followed by the encrypted block, which starts `-----BEGIN CRYPTSECURE ENVELOPE-----`. Your email signature is kept below it.
Text and files	The same explanation line, and one attachment, `secure-message.csec`, containing the message and all the files, encrypted and signed together.

© 2026 Opey's IT

More options

Option	Use it when
Passphrase	You want a second, separate secret. Agree it with the recipient by phone or in person, never in the same email. They will need it to open the message.
Protection: Automatic (recommended)	Always, unless told otherwise. CryptSecure picks the strongest protection every recipient supports.
ML-KEM-1024 + ECDH P-384 (CNSA 2.0)	Your policy requires the CNSA 2.0 suite.
X-Wing: ML-KEM-768 + X25519	Compatibility with systems that standardize on X-Wing.
ML-KEM-1024 only	Your policy requires pure post-quantum protection.
Sign as	You have more than one key. The default signing key is pre-selected.

The result card

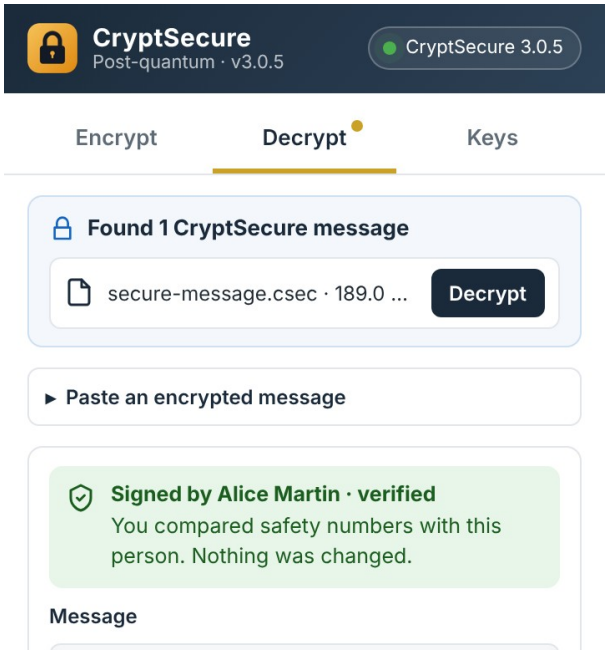
After encrypting, the green card lists the **recipients**, the **protection** used, whether it was **signed** (ML-DSA-87), the **size**, and the envelope's **SHA-256 fingerprint**, a unique identifier for exactly what you sent.

© 2026 Opey's IT

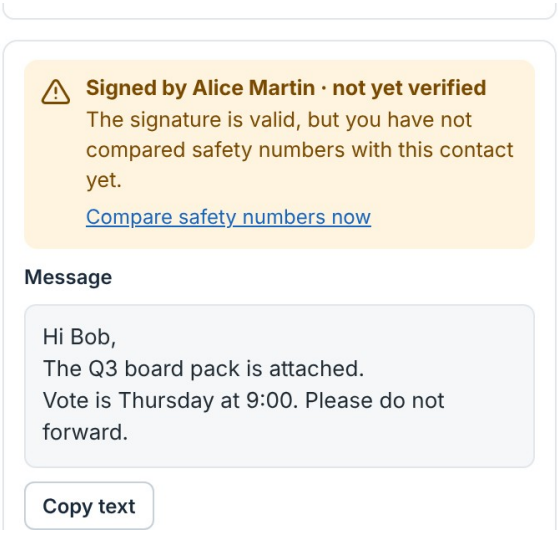
5 Open an encrypted email

5.1 Open it and check who sent it

1 Open the email and choose **CryptSecure › Decrypt**. The panel finds the encrypted message and opens it by itself. (If an email holds several, choose **Decrypt** next to the one you want.)

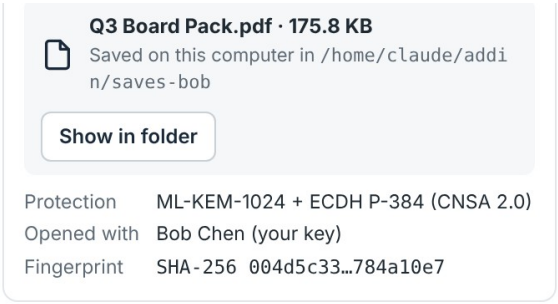


2 Read the coloured banner: it tells you who signed the message and whether you have verified them (see the table below).



© 2026 Opey's IT

3 Attached files are saved on your computer, in `Downloads\CryptSecure`. Choose **Show in folder** to open that folder. Opening the same email again does not create duplicate copies.

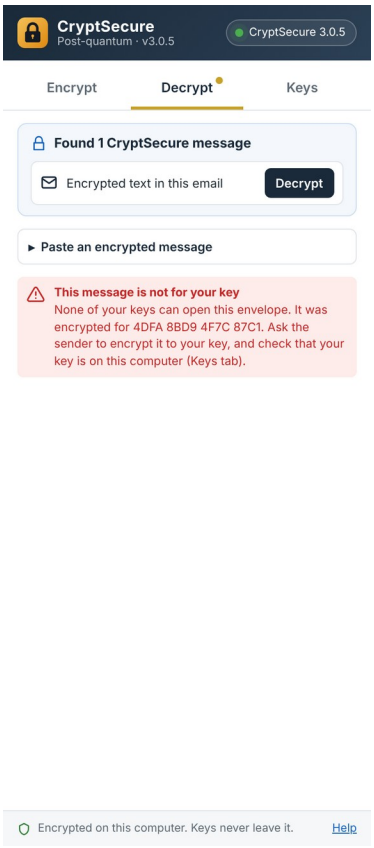


Banner	Meaning	What to do
Green: Signed by … · verified	Signed by a contact whose safety number you compared. Nothing was changed.	Nothing. This is the best result.
Green: Signed by you	You sent it (your own copy).	Nothing.
Amber: Signed by … · not yet verified	The signature is valid, but you have not compared safety numbers with this contact yet.	Choose **Compare safety numbers now** (7.2) before acting on anything important.
Amber: Signed by an unknown sender	Valid signature from someone not in your contacts.	Be careful. Add and verify them if you know them.
Red: Signature does not match	The message may have been changed or forged.	Do not trust it. Contact the sender another way.
Grey: Not signed	The sender cannot be confirmed.	Treat requests in it with care.

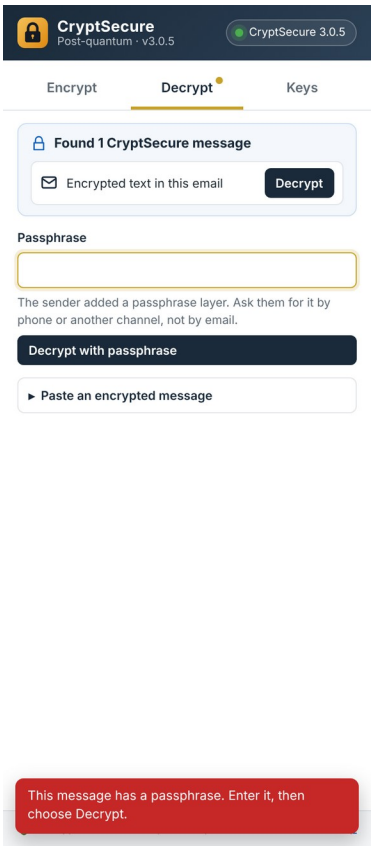
5.2 When something is wrong

Problems appear in a red card that stays on screen until you try again:

© 2026 Opey's IT



Not encrypted to your key



A passphrase is needed

Card or prompt	Meaning	What to do
This message is not for your key	It was encrypted for other people, or your key is not on this computer.	Ask the sender to encrypt it to your key. Check the **Keys** tab shows your key.
This message failed its integrity check	It was changed after it was sent, or the passphrase is wrong.	Ask the sender to send it again.
This is not a complete CryptSecure message	Part of the encrypted block is missing.	Make sure everything from BEGIN to END is included (use **Paste an encrypted message**).
Passphrase box	The sender added a passphrase.	Ask them for it by phone, type it, choose **Decrypt with passphrase**.

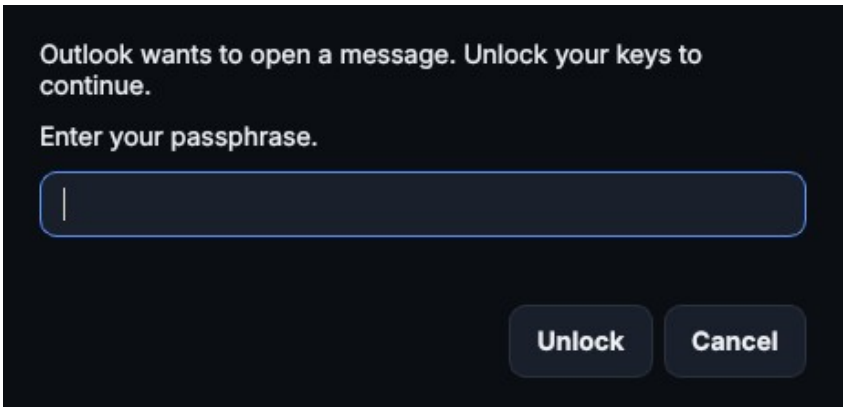
If a message was copied somewhere else, open **Paste an encrypted message** on the **Decrypt** tab, paste everything from `-----BEGIN CRYPTSECURE ENVELOPE-----` to `-----END CRYPTSECURE ENVELOPE-----`, and choose **Decrypt pasted text**. Quoting marks (`>`) added by replies are removed automatically.

5.3 When CryptSecure asks you to unlock your keys

Your private key stays protected in the CryptSecure app. When the panel needs it, to open a message or to sign one you send, the **CryptSecure** window appears in front of Outlook or Word

© 2026 Opey's IT

and says which program is asking. The panel waits and shows **If CryptSecure asks, unlock your keys in its window.**



CryptSecure's own window when Outlook needs your key. Outlook, Word and the panel never see your passphrase or your key.

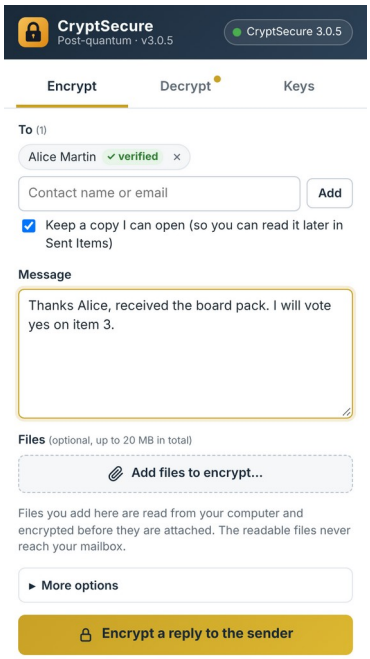
- Unlock in that window as you do in the app: touch your **security key**, enter your **PIN** in the Windows window, or type your **passphrase**. The window asks each time the panel needs your key: the 15-minute unlock applies to the CryptSecure window itself.
- Choose **Cancel** if you did not just ask for something. Nothing is opened or sent, and the panel says **Your keys are locked**.
- If your keys are protected by the computer's TPM without a PIN, or by your Windows account, no window appears.
- How your keys are protected, backed up and restored is explained in **Chapter 12** of the CryptSecure Encryption Client User Guide.

© 2026 Opey's IT

6 Reply securely

1 While reading the message, open the **Encrypt** tab in the panel. The sender is already selected.

2 Write your reply in the panel and choose **Encrypt a reply to the sender**.



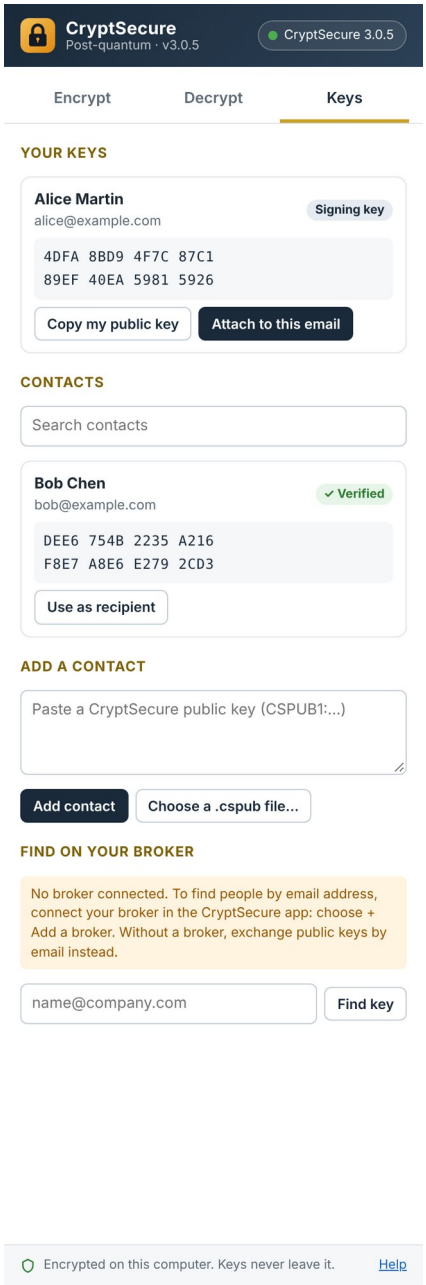
3 Outlook opens a reply that already contains your encrypted message. Check it and choose **Send**.

© 2026 Opey's IT

7 Contacts and trust

7.1 Share your public key and add contacts

Everything about keys is on the **Keys** tab.



The Keys tab

To	Do this
Send someone your public key	In a new email to them, choose **Attach to this email** under your key. It attaches `<Your name> - CryptSecure public key.cspub`. Public keys are safe to share. (Or choose **Copy my public key** and paste it.)

© 2026 Opey's IT

To	Do this
Add a key someone emailed you	Open their email and the panel. If it contains a key, the **Keys** tab shows **This email contains a CryptSecure public key** with an **Add** button (it shows the contact's name).
Add a key you received another way	Paste it into **Add a contact** and choose **Add contact**, or choose **Choose a .cspub file...**.
Find someone on your broker	Type their email under **Find on your broker** and choose **Find key**. Connect your broker first (section 3).
Encrypt to a contact	Choose **Use as recipient** on their card.

> **TIP: After adding a contact, verify them**
> CryptSecure offers the safety-number check as soon as you add someone. It takes a minute on the phone and protects every message you exchange afterwards.

7.2 Verify a contact with safety numbers

Encryption guarantees that only the holder of a key can read a message. It cannot tell you **who** holds the key. A safety number closes that gap: if it matches on both computers, you are using the right person's key.

1. Call the person on a number you already know, or meet in person. Do not use contact details that came with the key.
2. Choose **Verify...** on their card in the **Keys** tab (or **Compare safety numbers now** on a message banner).
3. Ask them to read the safety number shown for **their own key** in CryptSecure, all eight groups.
4. If every group matches the panel, choose **All 8 groups match**. If anything differs, choose **Cancel** and do not send to that key.

© 2026 Opey's IT

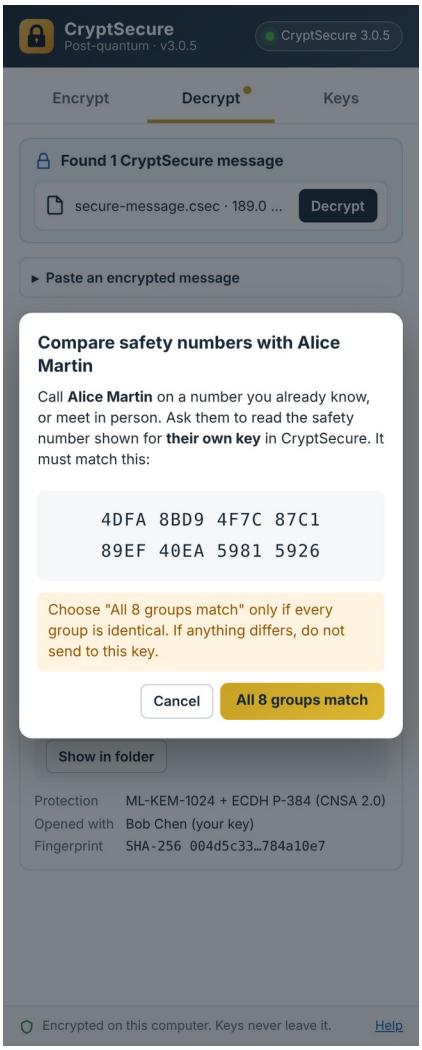


Figure 7. Comparing safety numbers.

7.3 Your older keys and one address with several keys

If you used CryptSecure 2.6, bring your older keys into the CryptSecure app once: **Keys & contacts › Import older key…**, with your email address. You can keep your new CryptSecure 3 key and any number of older keys on the same address. In Outlook and Word nothing changes:

- **Old messages still open. Decrypt** tries every key you have, so email sent to an older key opens as usual.
- **New messages use your strongest key.** People who write to you, and the copy you keep for yourself, use your CryptSecure 3 key.
- **Change an address any time.** In the CryptSecure app, select a key or contact and choose **Set email…**.

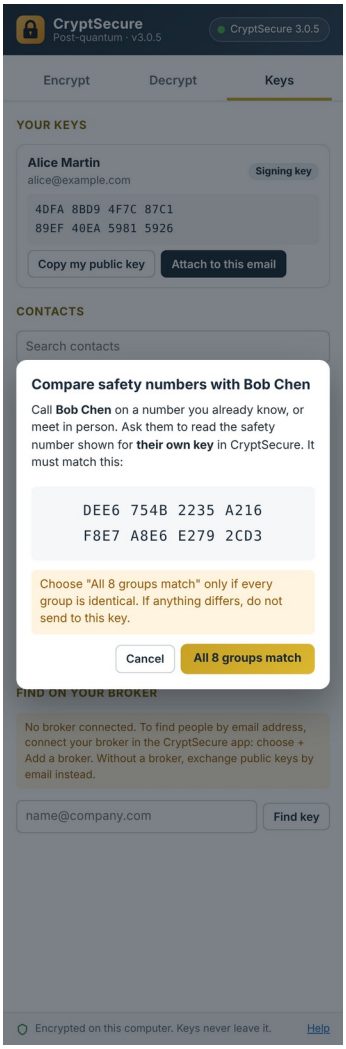
© 2026 Opey's IT

8 Example from start to finish

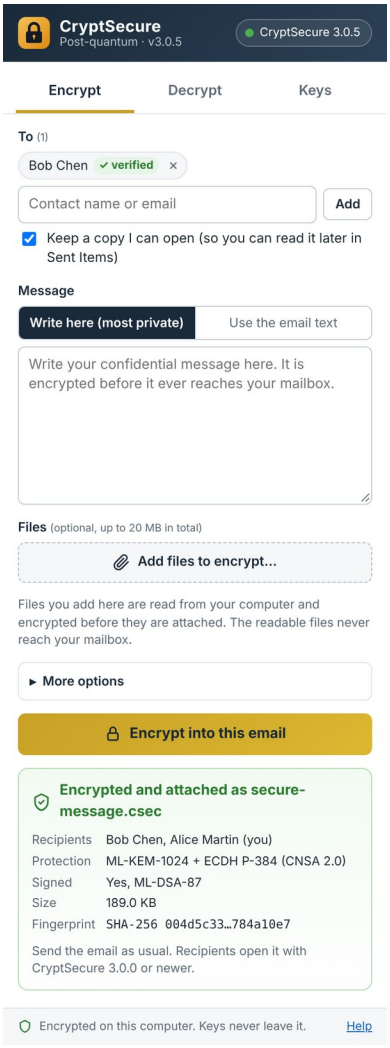
This walkthrough follows one real message from start to finish, and shows every point where you can check that it worked. Alice Martin (CFO) sends Bob Chen the Q3 board pack. Bob opens it, checks it, and replies, also encrypted. The screenshots are the real CryptSecure panel.

Step 1 Alice confirms she has Bob's real key (once per contact)

1. Alice opens a new email to Bob and chooses **CryptSecure › Encrypt**. Bob appears under **To** as **unverified**.
2. She opens the **Keys** tab and chooses **Verify…** on Bob's card.
3. She phones Bob on the number she already has. Bob reads the safety number shown for his own key in CryptSecure. All eight groups match, so Alice chooses **All 8 groups match**. From now on Bob shows ✔ **verified**.



Comparing safety numbers with Bob by phone



Encrypted: the card shows the fingerprint

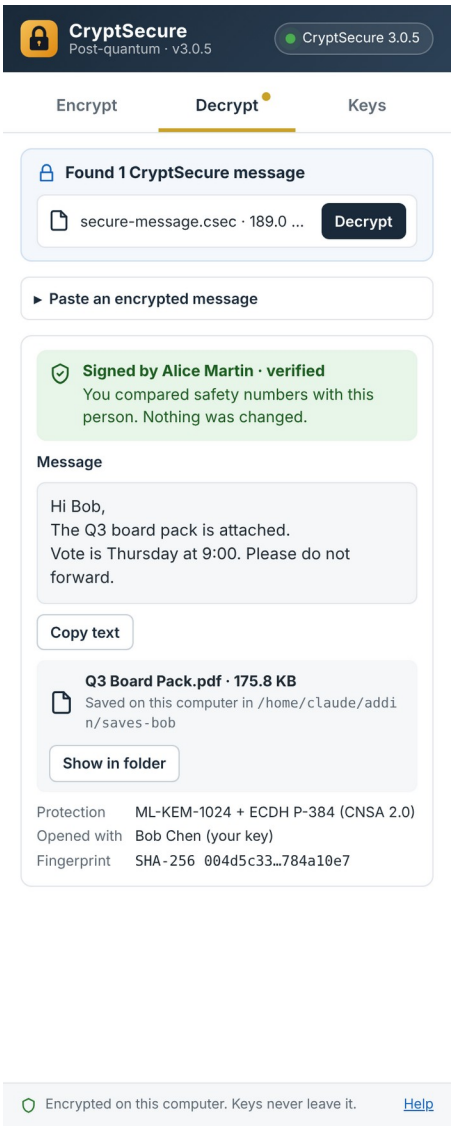
Step 2 Alice encrypts and sends

1. Back on **Encrypt**, she writes the message in the panel, chooses **Add files to encrypt…** and picks the board pack PDF.
2. She chooses **Encrypt into this email**. The green card confirms: **Recipients** Bob Chen and Alice Martin (you), **Protection** ML-KEM-1024 + ECDH P-384 (CNSA 2.0), **Signed** Yes, ML-DSA-87, and a **Fingerprint**, here `SHA-256 016442f7…d1abf039`.
3. She notes the fingerprint (the first and last eight characters are enough), types a subject and chooses **Send**. The email carries only `secure-message.csec` and a short explanation line.

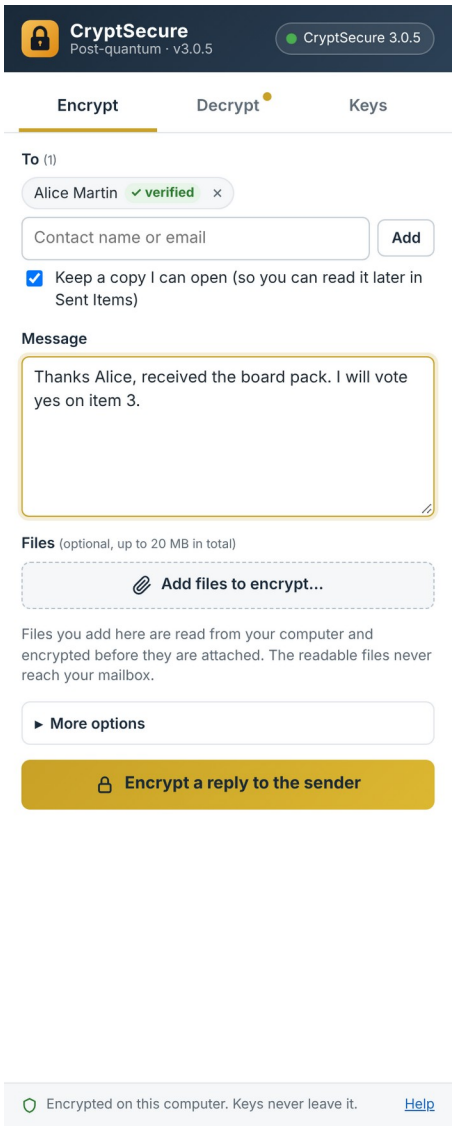
Step 3 Bob opens it and checks it

1. Bob opens the email and chooses **CryptSecure › Decrypt**. The panel finds the message and opens it.
2. The green banner says **Signed by Alice Martin · verified**: Bob compared safety numbers with Alice earlier, and nothing was changed.
3. The **Fingerprint** row shows `SHA-256 016442f7…d1abf039`, the same as on Alice’s card. Bob has exactly the envelope Alice sent.
4. The PDF is saved in `Downloads\CryptSecure`. **Show in folder** opens it.

© 2026 Opey’s IT



Bob: signed by Alice, verified; same fingerprint



Bob writes an encrypted reply

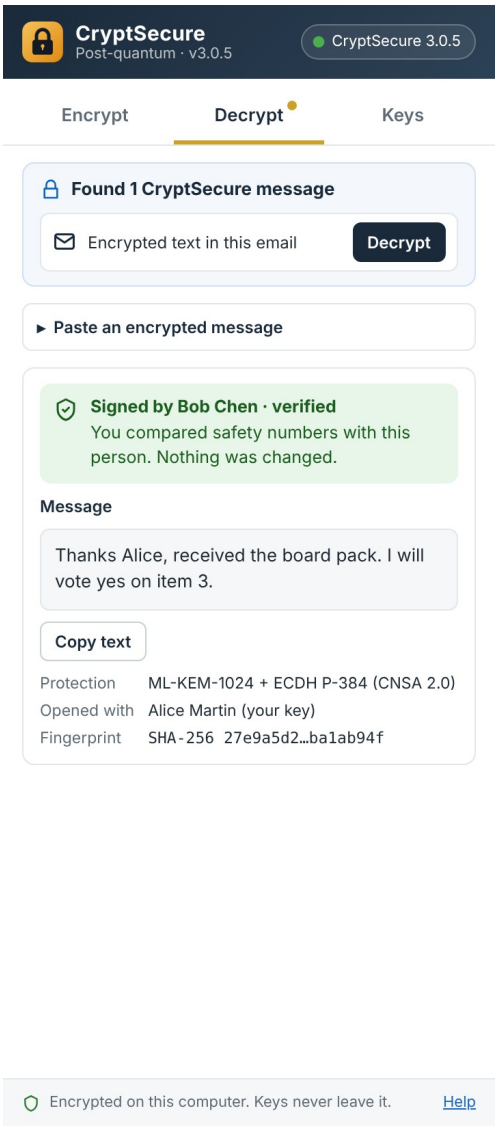
Step 4 Bob replies, encrypted

1. Still in Alice's email, Bob opens the **Encrypt** tab. Alice is already selected, marked ✓ **verified**.
2. He types his reply in the panel and chooses **Encrypt a reply to the sender**. Outlook opens a reply that already contains the encrypted message. He chooses **Send**.

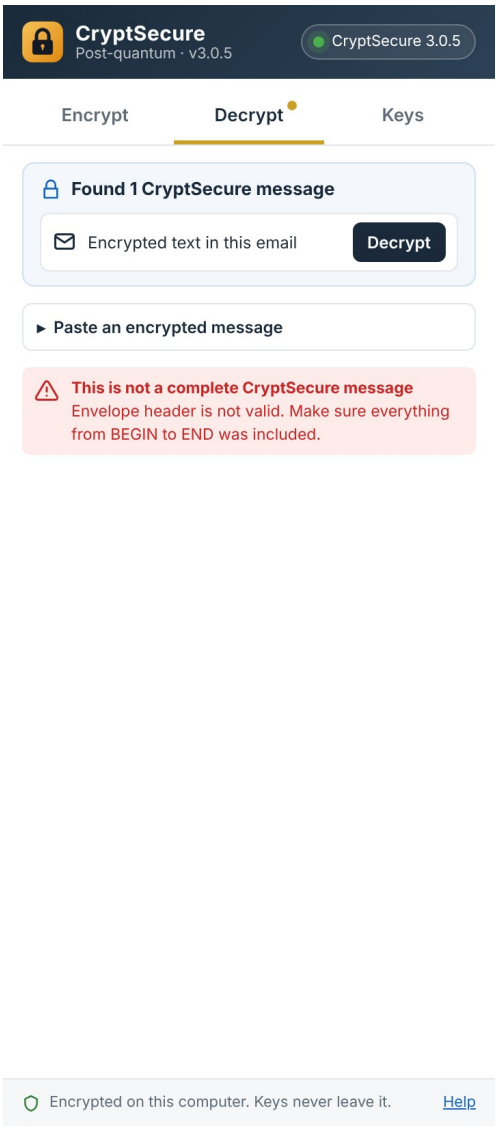
Step 5 Alice reads the reply

1. Alice opens Bob's reply and chooses **CryptSecure › Decrypt**. The banner says **Signed by Bob Chen · verified**. His reply appears under **Message**. The round trip is complete: both messages were encrypted on the sender's computer, signed, and checked on arrival.

© 2026 Opey's IT



Alice: the reply, signed by Bob, verified



A message changed on the way is refused

What each check proves

Check	Where you see it	What it proves
Safety numbers match (once per contact)	**Keys › Verify…**, then **✓ verified** on the contact	You are encrypting to the right person's key, not an impostor's.
Green **Signed by … · verified** banner	Top of the opened message	Who sent it, and that nothing in it was changed.
Same **Fingerprint** on both sides	Sender's green card and recipient's message details	The recipient has exactly the envelope that was sent, byte for byte.
Red **This message failed its integrity check** card	Instead of the message	The message was altered after it was sent. Nothing from it is shown. Ask the sender to send it again.

© 2026 Opey's IT

9 Use CryptSecure in Word

In Word, CryptSecure encrypts text in your document, for example one confidential paragraph in a document you circulate, or a whole document.

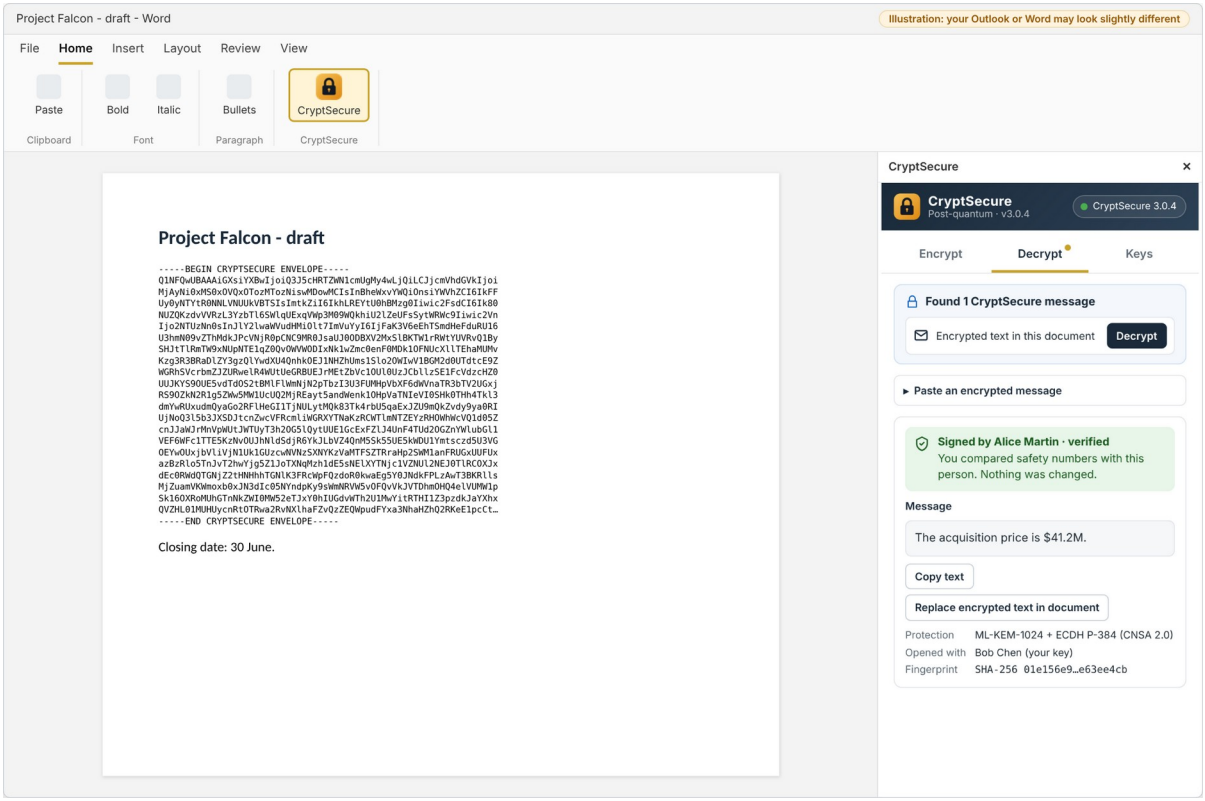
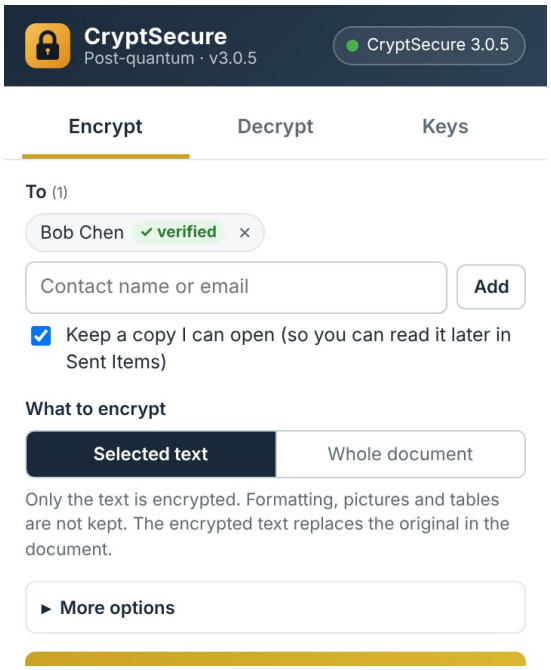


Figure 8. A decrypted paragraph in Word, with the option to put it back (illustration around a real panel screenshot).

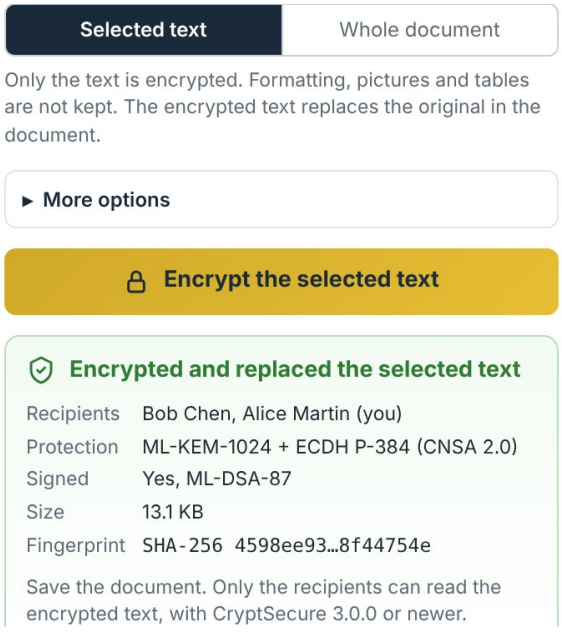
9.1 Encrypt text

1 Choose **Home › CryptSecure**.

2 Add recipients under **To** (type a contact's name or email and choose **Add**). Select the text to encrypt and keep **Selected text**, or choose **Whole document**.



3 Choose **Encrypt the selected text** (or **Encrypt the whole document**). The text is replaced by an encrypted block, and the green card confirms who can open it.



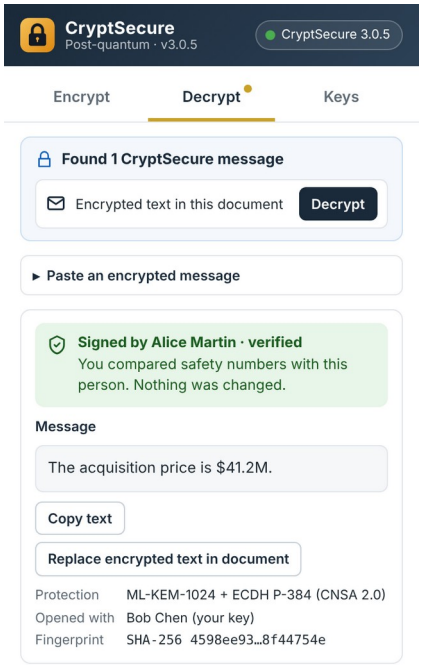
4 Save the document.

© 2026 Opey's IT

> **NOTE: Text only**
> Only the text is encrypted. Formatting, pictures and tables in the selection are not kept. To protect a whole file exactly as it is, attach it to an email with **Add files to encrypt...**, or use the CryptSecure desktop app.

9.2 Open encrypted text

1 Open the document and choose **Home › CryptSecure**. The panel finds the encrypted block and opens it automatically.



2 Read it in the panel, or choose **Replace encrypted text in document** to put the readable text back. CryptSecure asks you to confirm, because anyone who opens the saved document can then read it.

> **NOTE: Word 2016**
> On Word 2016, select the whole encrypted block (from BEGIN to END) before choosing Replace.

> **CHECK: Check it worked**
> The recipient's panel shows a green **Signed by ... · verified** banner and the original text. After **Replace encrypted text in document**, the paragraph reads exactly as the sender wrote it.

© 2026 Opey's IT

10 Quick reference: how do I...

How do I...	Do this	Section
Install it	Double-click **CryptSecure-for-Outlook-and-Word-Setup-3.0.5** › **Next** › **I Agree** › **OK** › **Yes** › **Next** › **Finish**	2.2
Add it to Outlook	**My add-ins** › **Add a custom add-in** › **Add from File...** › **Ctrl + V** › **Open** › **Install**	2.4
Connect my broker	CryptSecure app › **+ Add a broker** › **Test & save** › **Publish to broker**	3.1
Encrypt an email	New email › **CryptSecure › Encrypt** › write in the panel › **Encrypt into this email** › **Send**	4.2
Encrypt files	In the panel, **Add files to encrypt...** before choosing **Encrypt into this email**	4.2
Write to someone new	Address the email › **CryptSecure › Encrypt** › **Find** (needs your broker connected)	4.3
Open an encrypted email	Open it › **CryptSecure › Decrypt**	5.1
Open a message pasted somewhere else	**Decrypt** tab › **Paste an encrypted message** › **Decrypt pasted text**	5.2
Reply encrypted	In the received email: **Encrypt** tab › **Encrypt a reply to the sender**	6
Send my public key	**Keys** tab › **Attach to this email**	7.1
Bring in my older keys	CryptSecure app › **Keys & contacts › Import older key...**	7.3
Add someone's key	Open their email › **Keys** tab › **Add**	7.1
Check who I am writing to	**Keys** tab › **Verify...** › compare by phone › **All 8 groups match**	7.2
Prove a message arrived intact	Compare the **Fingerprint** on the sender's card with the recipient's	8
Encrypt part of a Word document	Select it › **Home › CryptSecure** › **Encrypt the selected text**	9.1
Check everything is working	**Start › CryptSecure › CryptSecure Connector - Check status**	11.2
Get help	**Start › CryptSecure › CryptSecure Connector - Support report**	11.4
Update or repair	Run the installer again	12.1
Uninstall	Outlook: **My add-ins** › CryptSecure › **Remove**; then **Settings › Apps › Installed apps** › **Uninstall**	12.2

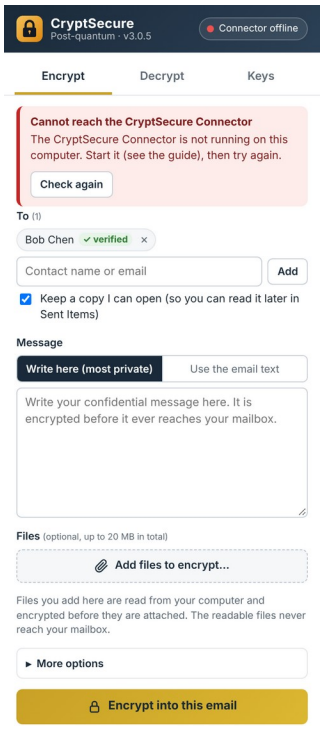
© 2026 Opey's IT

11 Help and troubleshooting

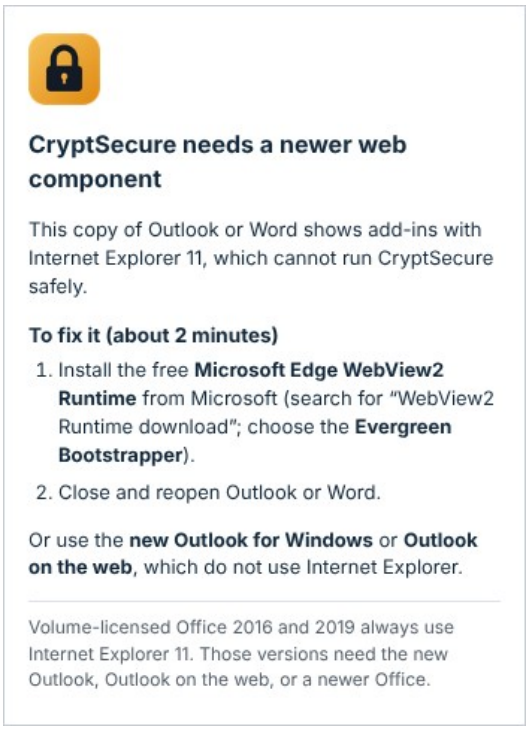
11.1 The status light and panel messages

You see	Meaning	What to do
● green CryptSecure 3.0.5	Connected and ready (a newer app shows its own number).	Nothing.
● amber blinking Checking...	The panel is checking the connection.	Wait a moment.
● red Connector offline	The panel cannot reach the Connector.	Choose **Start › CryptSecure › CryptSecure Connector**, then click the light.
● red App not found	The Connector cannot find the CryptSecure app.	Install CryptSecure 3.0.5 or newer. The light turns green within a minute (click it to check again).
● red Update needed	An older CryptSecure is installed (3.0.0 to 3.0.4, or Microsoft Store package 3.0.1). Nothing is encrypted or decrypted until it is updated.	Update CryptSecure to 3.0.5 or newer (Microsoft Store › Library › Get updates), then click the light.
Blank panel, or "add-in could not be started"	The Connector is not running, so Outlook cannot load the panel.	Start the Connector, then close and reopen the panel.
"You need your own CryptSecure 3 key first"	No key of your own.	Create one in the desktop app (step 2.1).
"Files are over the 20 MB limit"	Email attachments are limited.	Send large files with the CryptSecure desktop app.
"This version of Outlook cannot add attachments"	Older Outlook without the Mailbox 1.8 API.	Encrypt text only, or use Microsoft 365 / Outlook 2021 or later.

© 2026 Opey's IT



The Connector is not running



Outlook uses Internet Explorer 11

11.2 Check that everything is working

Start with the Connector's own check: choose **Start › CryptSecure › CryptSecure Connector - Check status**. Every line should show ✔.

CryptSecure Connector - Check status *sample output, your paths and numbers will differ*

```
CryptSecure Connector 3.0.5 -- status
============================================================
  ✔ CryptSecure engine : 3.0.5  (C:\Users\Alice\AppData\Local\Microsoft\WindowsApps\CryptSecure.exe)
  ✔ Certificate        : valid until 2029-02-19 (819 days)
  ✔ Manifests          : C:\Users\Alice\AppData\Local\CryptSecure\Connector\manifest
  ✔ Word registration  : registered
  ✔ Automatic start    : on
  ✔ Connector running  : yes, on https://localhost:47443
    Decrypted attachments are saved to: C:\Users\Alice\Downloads\CryptSecure

C:\Users\Alice>_
```

Figure 9. Sample output: a healthy installation.

Two more checks, if the panel still does not open:

1. Open **Microsoft Edge** and go to `https://localhost:47443/health`. You should see the text in Figure 10, with **no certificate warning**: `"status": "running"` and `"engine_ok": true`.
2. Go to `https://localhost:47443/taskpane.html`. The CryptSecure panel opens in the browser with a green **CryptSecure 3.0.5** light (Figure 11). Close the tab.

© 2026 Opey's IT

Pretty-print ☐

{"service": "CryptSecure Connector", "version": "3.0.4", "status": "running", "engine_found": true, "engine_version": "3.0.4", "engine_ok": true}

Figure 10. The health check in the browser.

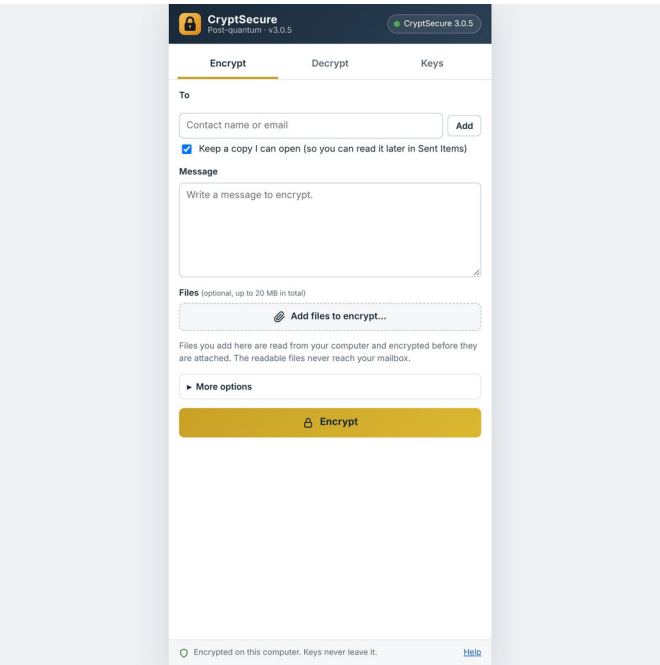


Figure 11. The panel test page.

> **NOTE: The Connector window**
>
> A line appears in the Connector window (Figure 12) each time the panel asks it to do something. Message contents are never shown or logged.

CryptSecure Connector *sample output, your paths and numbers will differ*

```
CryptSecure Connector 3.0.5
============================================================
  Engine  : ✔ CryptSecure 3.0.5  (C:\Users\Alice\AppData\Local\Microsoft\WindowsApps\CryptSecure.exe)
  Address : https://localhost:47443   (this computer only)
  Saves   : decrypted attachments go to C:\Users\Alice\Downloads\CryptSecure
============================================================
Keep this window open while you use CryptSecure in Outlook or Word.
Press Ctrl+C to stop.
[01:54:47] POST /api/status 200 ok (0 ms)
[01:54:50] POST /api/keys 200 ok (2830 ms)
[01:54:51] POST /api/encrypt 200 ok (1207 ms)
[01:54:54] POST /api/decrypt 200 ok (2655 ms)
```

Figure 12. The Connector window.

© 2026 Opey's IT

11.3 Common problems and fixes

Problem	Likely cause	Fix
The panel says **Your keys are locked**	You cancelled the CryptSecure window, typed a wrong passphrase, or your security key was not plugged in.	Try again and unlock in the CryptSecure window that appears.
The panel says **made by a newer CryptSecure**	Someone with a newer version sent it in a format this app does not know yet.	Update CryptSecure on this computer.
The panel is blank, or Outlook says the add-in could not start	The Connector is not running.	Choose **Start › CryptSecure › CryptSecure Connector**. Check `https://localhost:47443/health` in Edge.
Edge shows "Your connection isn't private" for localhost	The certificate is not trusted (**No** was chosen).	Run the installer, **CryptSecure-for-Outlook-and-Word-Setup-3.0.5**, again and choose **Yes** in the Security Warning.
The installer says CryptSecure 3.0.5 or newer was not found	The app is missing or older than 3.0.5, or its command alias is off.	Install or update CryptSecure, do step 2.1, then run the installer again.
The panel or Check status says "needs CryptSecure 3.0.5 or newer"	An older CryptSecure is installed (3.0.0 to 3.0.4, or Microsoft Store package 3.0.1).	Update CryptSecure (Microsoft Store › Library › Get updates). Nothing in Outlook or Word needs to change.
"Port 47443 is in use by another program"	Another program uses the same port.	Close that program and restart the Connector, or ask your IT department.
No "Add a custom add-in" in Outlook	Your organization blocks custom add-ins.	Ask your IT department to deploy the add-in for you.
CryptSecure does not appear in classic Outlook	Outlook caching (up to 24 hours).	Use Outlook on the web meanwhile, or restart Outlook later.
No CryptSecure button in Word	Word was open during installation, or the registration was removed.	Close all Word windows and reopen. Or step 2.5, step 3. Or run the installer again.
"2 separate encryptions, because a CryptSecure 2.6 key can only receive a message of its own"	One recipient has only an older CryptSecure 2.6 key.	Nothing to do: the email gets one part per 2.6 key, each headed with who it is for. Ask that person to create a CryptSecure 3 key so future emails are a single post-quantum message.

© 2026 Opey's IT

Problem	Likely cause	Fix
The Connector window closed	It was closed by mistake.	Choose **Start › CryptSecure › CryptSecure Connector**. It also starts by itself at your next sign-in.
"CryptSecure Connector could not start: some of its program files are missing"	Files in the installation folder were deleted or quarantined.	Run the installer, **CryptSecure-for-Outlook-and-Word-Setup-3.0.5**, again. If your antivirus removed files, ask IT to allow the installation folder.
Each action takes a second or two	Each action starts CryptSecure for that request.	Normal. Large files take longer.
The panel says "CryptSecure needs a newer web component"	Your Outlook shows add-ins with Internet Explorer 11.	Install the Microsoft Edge WebView2 Runtime and restart Outlook. Volume-licensed Office 2016/2019: use the new Outlook or Outlook on the web.
The pinned panel still shows the previous email	Very old Outlook builds do not tell add-ins about a new selection.	Close the panel and open it again on the new email.
No **Apps** button in the new Outlook	The ribbon is collapsed or the window is narrow.	Widen the window, or choose **...** at the right of the ribbon.
Older Office: the panel cannot connect to localhost	Office builds that use the older Edge (EdgeHTML) panel need a loopback exemption.	Install the Microsoft Edge WebView2 Runtime, or ask your IT department.
A decrypted file seems missing	It is saved in `Downloads\CryptSecure`.	Choose **Show in folder** in the panel.
The panel says an attached file "could not be saved here"	The sender (on a Mac or Linux) named the file with a name Windows reserves, such as CON or NUL.	Open the message with the CryptSecure desktop app, or ask the sender to rename the file. Files sent from this add-in are always named safely.

11.4 Get support

1. Choose **Start › CryptSecure › CryptSecure Connector - Support report**. A Command Prompt shows the report and saves it on your Desktop as `CryptSecure-support-report.txt` (Figure 13).
2. Send that file to Opey's IT support with a short description of what you were doing.

© 2026 Opey's IT

CryptSecure Connector - Support report *sample output, your paths and numbers will differ*

```
CryptSecure Connector 3.0.5 -- support report
Created  : 2026-11-22 01:54:58 -0000
Windows  : Windows-10-10.0.19043-SP0  (AMD64)
Program  : C:\Users\Alice\AppData\Local\Programs\CryptSecure Connector\CryptSecureConnector.exe
Data     : C:\Users\Alice\AppData\Local\CryptSecure\Connector
Saves    : C:\Users\Alice\Downloads\CryptSecure
Address  : https://localhost:47443

Engine   : OK  version=3.0.5  path=C:\Users\Alice\AppData\Local\Microsoft\WindowsApps\CryptSecure.exe

Cert     : present  expires=2029-02-19  days_left=819  ca_thumbprint=A34B897F51497C23B1677502B7F3FEC733A26DEF
Manifest : CryptSecure-Outlook.xml  present
Manifest : CryptSecure-Word.xml  present
Word reg : registered
Autostart: on  (C:\Users\Alice\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\CryptSecure
Connector.cmd)
Running  : yes
Panel    : present  (C:\Users\Alice\AppData\Local\Programs\CryptSecure Connector\app\web)

Last 60 log lines (requests and errors only):
  2026-11-22 01:54:47 POST /api/status 200 ok (0 ms)
  2026-11-22 01:54:50 POST /api/keys 200 ok (2830 ms)
  2026-11-22 01:54:51 POST /api/encrypt 200 ok (1207 ms)
  2026-11-22 01:54:54 POST /api/decrypt 200 ok (2655 ms)

✔ Saved to C:\Users\Alice\Desktop\CryptSecure-support-report.txt
  Send this file to Opey's IT support. It contains no keys, messages or passphrases.

C:\Users\Alice>_
```

Figure 13. Sample support report. It contains versions, settings and recent request lines only.

> **NOTE: What the support report contains**
>
> Versions, folders, certificate expiry, whether the Connector, the manifests and the Word registration are in place, and the last 60 lines of the Connector log (`%LOCALAPPDATA%\CryptSecure\Connector\connector.log`). It never contains keys, messages, file contents or passphrases.

© 2026 Opey's IT

12 Update or remove

12.1 Update or repair

Updating is the same as installing: run the installer again. You never need to uninstall first, and nothing you have set up is lost.

1. Close Outlook and Word.

2. Double-click the new installer (or the same **CryptSecure-for-Outlook-and-Word-Setup-3.0.5**, to repair an installation) and follow step 2.2: **Next**, **I Agree**, **Next**, **Finish**.

3. The installer stops the running Connector, replaces its files and starts it again. Your certificate, settings, keys and contacts are kept, and Windows does not ask about the certificate again.

4. Only if the release notes say the add-in changed: remove CryptSecure from Outlook (step 12.3) and add it again (step 2.4).

> **NOTE: Certificate renewal**
> The certificate lasts about two years. When fewer than 30 days remain, the Connector warns you in its window. Run the installer again to renew it; Windows then asks once to trust the new certificate.

12.2 Remove CryptSecure (uninstall)

Removing CryptSecure for Outlook & Word takes about three minutes and leaves your computer exactly as it was before. Your CryptSecure app, your keys and your contacts are never touched, so you can reinstall at any time and carry on where you left off.

Step	What you do	Time
12.3	Remove CryptSecure from Outlook	1 min
12.4	Remove the Connector from Windows (this also removes it from Word)	1 min
12.5	Confirm nothing is left behind	1 min

> **TIP: Remove it from Outlook first**
> Do step 12.3 before step 12.4. If you do it the other way round, the CryptSecure button stays in Outlook until you remove it, but opens an empty panel.

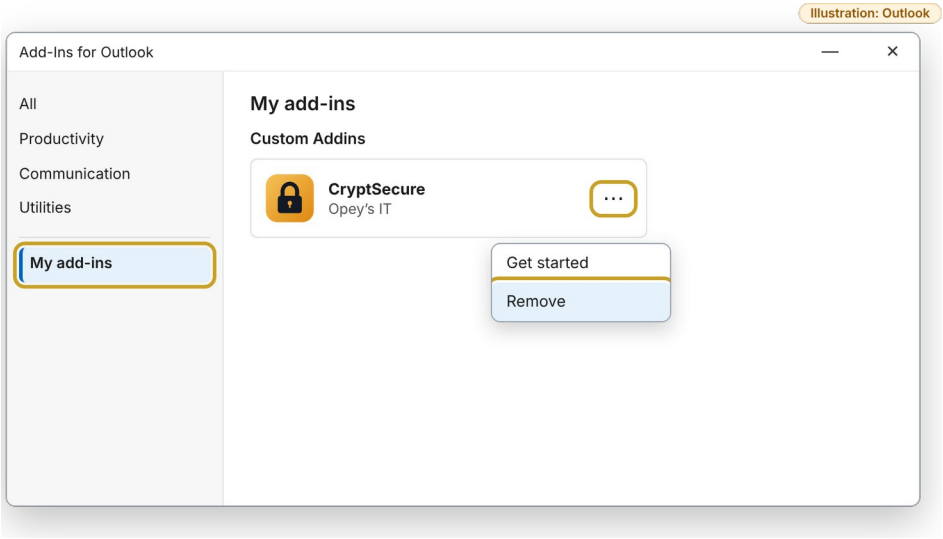
© 2026 Opey's IT

12.3 Remove it from Outlook

Outlook add-ins belong to your mailbox, so removing it once removes it from classic Outlook, the new Outlook and Outlook on the web.

1. Open **Microsoft Edge** and go to `https://aka.ms/olksideload`. Sign in with your Outlook account if asked. (In classic Outlook you can also choose **Get Add-ins** on the **Home** tab; in the new Outlook, **Apps › Add apps**.)

2. In the **Add-Ins for Outlook** window, choose **My add-ins**. Under **Custom Addins**, find **CryptSecure**, choose **…** and then **Remove**. Confirm if asked.



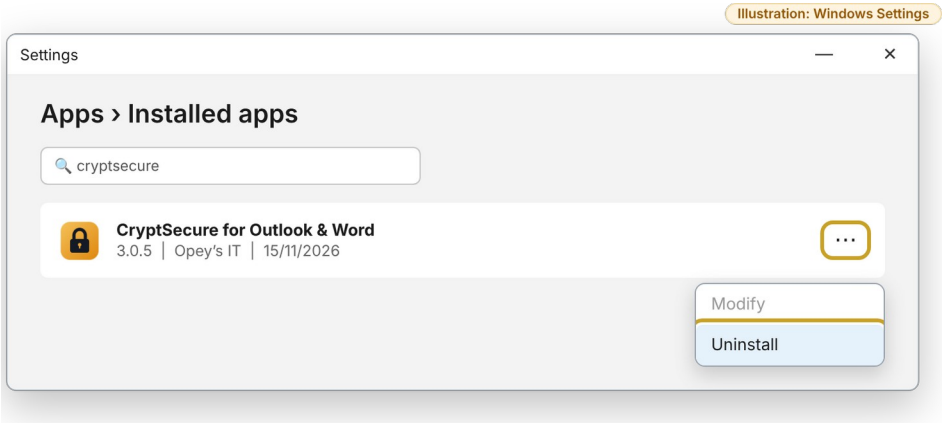
3. Close the window, then close Outlook.

12.4 Uninstall the Connector

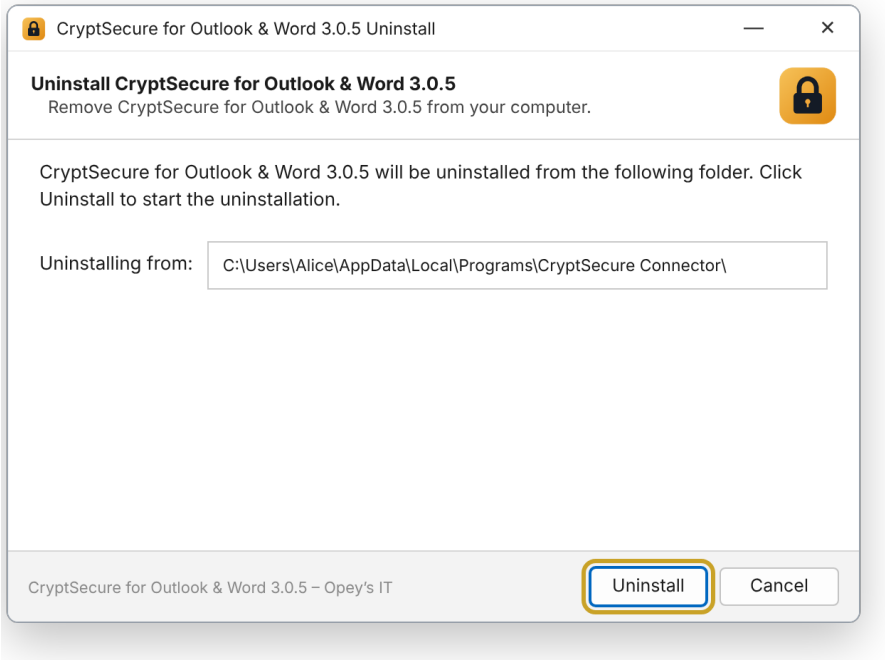
1. Close Word.

© 2026 Opey's IT

2 Open **Settings › Apps › Installed apps** and type `cryptsecure` in the search box. Next to **CryptSecure for Outlook & Word**, choose **…** and then **Uninstall**, and confirm. (Or use **Start › CryptSecure › Uninstall CryptSecure Connector**.)

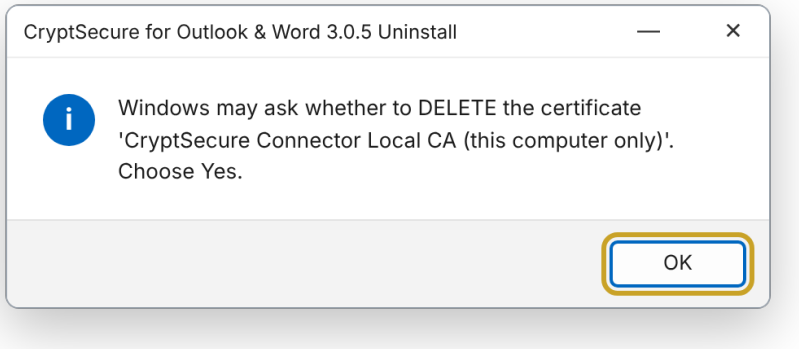


3 The uninstaller opens. Choose **Uninstall**.



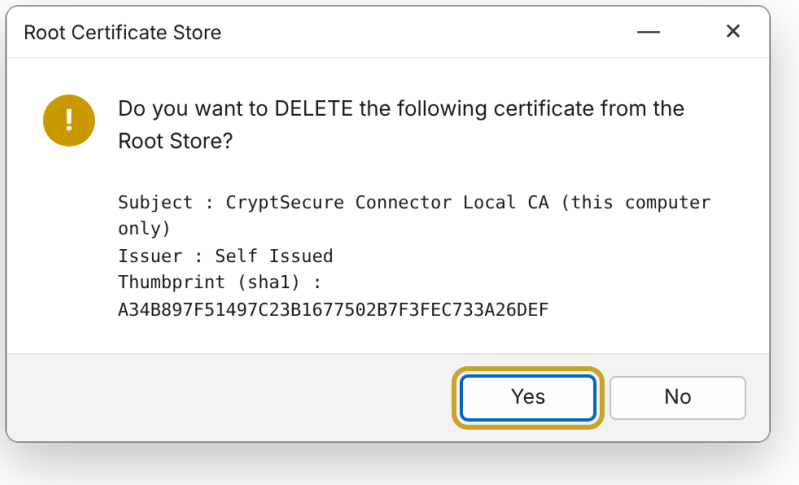
© 2026 Opey's IT

4 A message says Windows may ask to **delete** the CryptSecure certificate. Choose **OK**.

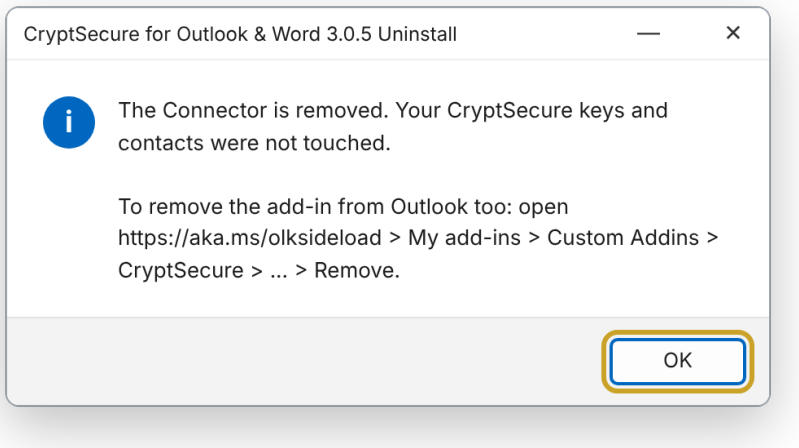


5 Windows asks: **Do you want to DELETE the following certificate from the Root Store?** It names **CryptSecure Connector Local CA (this computer only)**. Choose **Yes**.

Illustration: Windows



6 A message confirms that the Connector is removed and that your keys and contacts were not touched. Choose **OK**, then **Close**.



© 2026 Opey's IT

> **CHECK: Word is done too**
> The uninstaller removes CryptSecure from Word automatically. There is nothing to do in Word.

12.5 Check that everything is gone

Check	You should see
Settings › Apps › Installed apps, search `cryptsecure`	No **CryptSecure for Outlook & Word** entry. (Your **CryptSecure** desktop app is still listed: that is correct.)
Start menu	No **CryptSecure** folder with the Connector shortcuts. (The CryptSecure desktop app stays.)
Edge, `https://localhost:47443/health`	**Can't reach this page**: the Connector is no longer running.
Outlook, after restarting	No CryptSecure button. Classic Outlook can take a while to refresh its add-in list; restart it again later if the button is still there.
Word, after closing every Word window and reopening	No CryptSecure button on the **Home** tab.

Removed	Kept
The Connector and its folder, its log, its certificate and the Windows trust for it, the add-in files, the Word set-up, automatic start, the Start menu folder and the Settings entry.	Your CryptSecure app, your keys and contacts, and files you decrypted into `Downloads\CryptSecure` (delete that folder yourself if you no longer need them).

12.6 Reinstall later

Run **CryptSecure-for-Outlook-and-Word-Setup-3.0.5** again (step 2.2), then add CryptSecure to Outlook again (step 2.4). Your keys and contacts are still there, so you can encrypt straight away.

12.7 If something goes wrong

Problem	What to do
There is no **CryptSecure for Outlook & Word** entry in Settings	It is already uninstalled. If the Start menu folder is still there, run the installer once, then uninstall again.
I chose **No** when Windows asked to delete the certificate	Nothing is at risk: the certificate only works for this computer. To remove it, run the installer, choose **Yes** at the Security Warning, then uninstall again and choose **Yes** this time.
The CryptSecure button is still in Outlook	Do step 12.3. In classic Outlook, restart it; it can take a while to refresh.

© 2026 Opey's IT

Problem	What to do
The CryptSecure button is still in Word	Close every Word window (check the taskbar) and open Word again.

© 2026 Opey's IT

13 Your privacy and security

13.1 What stays on your computer

- **Your private keys.** They stay in the CryptSecure app, locked by your unlock method, and never leave the computer. The add-in and the Connector never see your keys, your passphrase or your recovery code.
- **Readable text and files you put in the panel.** They are encrypted on your computer before they reach Outlook or Word.
- **The panel itself.** It is served by the Connector from your computer, not downloaded from a website. Only Microsoft's Office framework is loaded from Microsoft.

13.2 How the Connector is protected

- It listens only on **127.0.0.1**, your own computer. Other computers on the network cannot reach it.
- It refuses requests from any website other than the CryptSecure panel itself, and never allows cross-site access.
- Its certificate works only for localhost, and the key that issued it was destroyed after use.
- It hands readable text to CryptSecure in a private temporary folder that only your account can read, never on a command line other programs can see, and passphrases through a private setting of that one request.
- Temporary files are overwritten and deleted after every operation. Decrypted attachments are saved only in `Downloads\CryptSecure`.
- The panel runs under a strict content security policy: it cannot run code injected into a message, and message text is always shown as plain text.
- It sends no telemetry or usage data anywhere.

13.3 What it cannot protect

- **Subject lines, sender, recipients and dates** are not encrypted (true of all encrypted email).
- **Drafts Outlook already saved**, if you typed confidential text in the email before encrypting (see 4.2).
- **A compromised computer.** If malware controls your PC or your recipient's, it can read what is shown on screen, and while your keys are unlocked it could use them.
- **What recipients do** with a message after they open it.

13.4 Good practice

- Write confidential text in the panel, not in the email body.
- Verify each contact's safety number once, by phone or in person.
- Make a recovery package in the CryptSecure app (Back up my keys…), write the recovery code on paper and keep the two apart.
- Keep Windows, Office and CryptSecure up to date.
- Keep the subject line free of confidential details.

© 2026 Opey's IT

Glossary

Term	Meaning
Add-in	An extension that adds buttons and a panel to Outlook or Word.
Broker	An optional CryptSecure server that publishes public keys and delivers envelopes with receipts. Set up in the desktop app.
CNSA 2.0	The U.S. NSA Commercial National Security Algorithm Suite 2.0, which includes ML-KEM-1024.
Connector	The small local program that links Outlook and Word to the CryptSecure app.
.csec	A CryptSecure encrypted envelope file.
.cspub	A CryptSecure public key file. Safe to share.
Envelope	An encrypted, signed CryptSecure message, as a block of text or a .csec file.
localhost	Your own computer, as seen by programs on it (address 127.0.0.1).
Manifest	The small XML file that tells Outlook or Word about an add-in.
ML-KEM / ML-DSA	NIST post-quantum standards for key encapsulation (FIPS 203) and digital signatures (FIPS 204).
Public key / private key	Your public key lets others encrypt to you and check your signature. Your private key, which never leaves your computer, opens messages to you and signs what you send.
Safety number	A 32-character fingerprint of a public key. If it matches on both computers, you have the right key.

© 2026 Opey's IT

Legal notices

Copyright © 2026 Opey’s IT. All rights reserved. CryptSecure is a product of Opey’s IT.

Microsoft, Outlook, Word, Windows, Microsoft Edge and Microsoft 365 are trademarks of the Microsoft group of companies. CryptSecure for Outlook & Word is an independent product and is not affiliated with, sponsored or endorsed by Microsoft.

Algorithm names refer to published standards (NIST FIPS 203, FIPS 204, FIPS 197; NSA CNSA 2.0). Their use does not imply certification or endorsement by NIST or NSA.

Window illustrations in this guide are simplified drawings built around real screenshots of the CryptSecure panel; your Outlook or Word may look different. Sample outputs show typical results; your values will differ.

This guide is provided for information. Encryption reduces risk but cannot remove it; follow the good practice in section 13. The software is provided under the terms of its license agreement.