

Krywerk – user guide

This guide is for everyone who works with Krywerk – teachers, administrative staff, and anyone who stores confidential files in OneDrive or another storage service. No technical knowledge is required. If you manage team folders for others, chapter 5 has additional information for you.

The guide describes Krywerk on Windows. On macOS and Linux everything works the same way, except that the system tray is called the menu bar on macOS, and drives appear in Finder or your file manager under `~/Krywerk` instead of with their own drive letter in Explorer. The context menu is called “Quick Actions” on macOS; on Linux it appears under “Actions” in Dolphin and under “Scripts” in Nautilus.

For printing: user guide as PDF.

Contents

1. [What is Krywerk?](#)
2. [Installation and setup](#)
3. [Personal vault](#)
4. [Using team folders](#)
5. [Managing team folders \(for managers\)](#)
6. [Switching from Boxcryptor](#)
7. [Common questions and problems](#)
8. [Glossary](#)

The essentials at a glance

- Krywerk shows encrypted folders as a **drive**. Whatever you put there is encrypted automatically before it ends up in OneDrive and similar services.
- There are three kinds of drives: **personal vaults** (your own password), **team folders** (access through your organization account, without a shared password), and **Boxcryptor (legacy)** for switching over.
- Depending on what you use, there are three things you must keep safe: your **vault password**, your **unlock code**, and – if you manage team folders – their **recovery keys**. Krywerk cannot recover any of them.

1. What is Krywerk?

Krywerk encrypts folders and shows them decrypted as a drive – on Windows with its own letter in File Explorer, for example **Z:**. You work in it like in any other folder: open, save, copy, and rename files. In the background, Krywerk stores everything encrypted in an ordinary folder.

This folder can be anywhere folders are synced or shared: in **OneDrive**, Google Drive, Dropbox, Nextcloud, or iCloud Drive, on a **network drive** (SMB, NFS), or on a **USB stick**. The storage provider only sees encrypted data.

What stays visible and what doesn't?

	Visible to the storage provider?
File contents	No
File and folder names	No (with Boxcryptor (legacy) only if filename encryption is turned on)
How many files there are and roughly how large they are	Yes
When files were changed	Yes

Three kinds of drives

	Personal vault	Team folder	Boxcryptor (legacy)
What for?	Your own confidential files	Collaboration (subject group, committee, administration)	Keep using existing Boxcryptor data
How is it unlocked?	With the vault password	With your organization account (e.g. Microsoft 365), without a shared password	With the Boxcryptor key file and password
Who has access?	Anyone who knows the password	Only people and groups who have been granted access	Anyone who has the key file and password
On your phone?	Yes, with the Cryptomator app	Not yet	No
Label in Krywerk	"Personal (password)"	"Team"	"Boxcryptor (legacy)"

Personal vaults use the open Cryptomator format. That is why you can also open them with the Cryptomator apps for Android, iOS, and Linux.

Team folders need a key server run by your organization – **Krywerk Server** or a Cryptomator Hub. The server manages who may open a team folder; it cannot read the files themselves. Your

IT administration will give you its address.

Boxcryptor (legacy) is only meant for the transition. The method is older and does not protect against targeted tampering with the encrypted files. So switch such folders over step by step (chapter 6).

What Krywerk looks like

- **Overview:** At the top are status indicators, for example “Organization account: Your Name”. Below them are notices when something needs your attention, and the list “**My drives**” with all your drives and team folders.
- **Settings:** via “**⚙ Settings**” at the top right, or by right-clicking the Krywerk icon in the system tray. There you find the sections *General*, *Organization account*, *Boxcryptor (legacy)* (only if you use Boxcryptor folders), and *About Krywerk*.
- **System tray:** Krywerk keeps running in the background when you close the window. You find the icon at the bottom right of the taskbar, possibly hidden behind the arrow “^”.
Quit by right-clicking the icon – this unmounts all drives.

2. Installation and setup

Requirements

Krywerk is available for Windows, macOS and Linux. If your IT department distributes Krywerk, most of this is already done – ask them first. Packages to download are at <https://krywerk.eu/en/download/>.

Windows 10 or 11:

1. Install **Krywerk**: run `Krywerk_..._x64-setup.exe` and confirm the administrator prompt. The installer sets up everything needed – including **WinFsp**, the component Krywerk uses to provide drives, and on Windows 10 *WebView2* for the window if needed.
2. If Windows says “Windows protected your PC”, that is because the pre-release is not signed yet: choose **“More info”** › **“Run anyway”**.

macOS:

1. Install **FUSE-T** (<https://www.fuse-t.org>), e.g. with `brew install macos-fuse-t/homebrew-cask/fuse-t`.
2. Drag **Krywerk.app** from the downloaded ZIP into the Applications folder.
3. On first launch macOS says the app cannot be verified (the pre-release is not notarized yet): **right-click Krywerk.app** › **“Open”** › **“Open”**. On newer macOS versions use *System Settings* › *Privacy & Security* › *“Open Anyway”*.

Linux:

1. **Debian, Ubuntu, Linux Mint**: install `Krywerk_..._amd64.deb`, e.g. by double-clicking it or with `sudo apt install ./Krywerk_..._amd64.deb`. Required components (FUSE, WebKitGTK) are installed automatically.
2. **Other distributions**: make `Krywerk_..._amd64.AppImage` executable and run it. Your distribution's `fuse3` package must be installed.
3. **“Remember password”** needs a keyring in your session (KDE: KWallet, GNOME: Keyring – usually present). On GNOME the Krywerk icon only appears in the top bar with the *AppIndicator and KStatusNotifierItem Support* extension.

Drives appear with their own drive letter on Windows, and on macOS and Linux in the `Krywerk` folder in your home folder (e.g. `~/Krywerk/Confidential`) and in the sidebar of Finder or your file manager.

First start

After you start it, the Krywerk window appears, along with the Krywerk icon in the system tray (at the bottom right of the taskbar, possibly hidden behind the arrow “^”). The list “My drives” is

empty at first.

What comes next depends on what you want to use:

- your own confidential files → [Chapter 3: Personal vault](#)
- your organization's team folders → [Chapter 4: Using team folders](#)
- existing Boxcryptor data → [Chapter 6: Switching from Boxcryptor](#)

Starting automatically

Under **Settings > General** you can turn on **“Start automatically when I sign in to the computer”**. Krywerk then starts without a window, with just the icon in the system tray. Drives with “Mount automatically” turned on and a remembered password are available right away. You open team folders after signing in to your organization account.

Closing the window and quitting Krywerk

- **Closing or minimizing the window:** Krywerk keeps running in the system tray, and your drives remain available. Clicking the icon brings the window back.
- **Quitting:** Right-click the icon > **Quit**. This unmounts all drives. Save any open files first.

Cache (only change it if there are problems)

Under **Settings > General > Advanced**, **“Use cache (recommended)”** is turned on. It makes drives faster. Only turn it off if changes that OneDrive or another storage service fetches from other devices don't appear in the drive, or appear only after a delay. The change takes effect the next time you mount.

3. Personal vault

A personal vault is an encrypted folder with **its own password**. It is suitable for your own confidential files – for example grade lists, assessments, or personnel records.

Creating a vault

1. On the overview, under “My drives”, click “**+ Add**”. If an organization account is connected, a choice appears – select “**Personal vault or existing folder ...**” there.
2. Leave the format set to “**Modern (recommended)**”.
3. Under “**Folder for the vault**”, click “**Browse ...**” and choose an **empty folder**, for example a new folder `Confidential` in your OneDrive. Krywerk creates the vault in it.
4. Enter a **vault password** with at least 8 characters and repeat it.
5. Optionally check “**Remember password**”. The password is then stored on this computer, protected by your Windows user account, and you don't have to enter it when mounting.
6. Optionally choose a **name** (shown in File Explorer) and a **drive letter**. “Automatic” takes the next free letter, starting at `Z:`.
7. Click “**Save**”.

Important: Without the vault password the data cannot be recovered – not even by IT or by Krywerk. Keep it in a safe place, for example in a password manager.

Adding an existing vault

If you already have a vault – for example one created with the Cryptomator app or with Krywerk on another computer – follow the same steps, but in step 3 choose the vault's folder (the folder containing the file `vault.cryptomator`) and enter its password.

Mounting and working

- **Mount:** In the vault's row, enter the password (if it isn't remembered) and click “**Mount**”. Afterwards the row shows “Mounted as Z:”.
- **Open:** Clicking “**Open**” shows the drive in File Explorer. You can also open it directly in File Explorer under “This PC”.
- **Unmount:** Click “**Unmount**” when you are done. When you quit Krywerk, all drives are unmounted automatically.

With “**Mount automatically**” (under “**Edit**”), Krywerk mounts the vault by itself at startup, provided the password is remembered.

Editing or removing a vault

Under **“Edit”** (only while the vault is unmounted) you can change the name, drive letter, “Mount automatically”, and “Read-only”. You'll also find:

- **“Delete remembered vault password”** – Krywerk asks for the password again the next time you mount.
- **“Remove”** – takes the vault off Krywerk's list and forgets the remembered password. **The encrypted files are kept**; you can add the vault again at any time.

Opening it on your phone

Personal vaults use the Cryptomator format. To open them on the go:

1. Install the **Cryptomator app** for Android or iOS (from the respective app store).
2. In the app, **add an existing vault** and connect OneDrive (or your storage service).
3. Choose the vault's folder (it contains `vault.cryptomator`) and enter the vault password.

Changes made on your phone appear on the computer as soon as OneDrive has synced them – and vice versa.

4. Using team folders

A team folder is an encrypted folder for several people – for example for a subject group, a committee, or the administration. There is **no shared password**: anyone with access opens the team folder with their own organization account (for example the school's Microsoft 365 account). Your organization's key server manages the key; the server itself cannot read the files.

One time: connect your organization account

1. Open **Settings > Organization account**.
2. Under **"Key server address"**, enter the address you received from your IT department, for example `https://schluessel.schule.example`.
3. Click **"Connect organization account"**.
4. Krywerk asks once: **"Confirm key server"**. Confirm with **"Trust and continue"** if the address is the one your organization gave you. The second address shown belongs to the identity provider (for example Microsoft).
5. Krywerk opens **a new tab in your default browser** with the sign-in page. Sign in there with your organization account. The browser then shows "Sign-in successful"; you can close the tab.
6. At the top of the Krywerk window you now see, in green, **"Organization account: Your Name"**.

The first time: set up your account and keep your unlock code safe

If you use team folders for the first time, Krywerk shows **"Set up account ..."**. Click it. Krywerk then shows **your unlock code – only this one time**.

- Keep the unlock code in a safe place: **"Copy"** it into a password manager, or **"Save as file ..."** in a safe location (not in the team folder itself).
- Check **"I have stored the unlock code safely."** and click **"Done"**.

Krywerk has already unlocked this computer in the process. You need the unlock code for **every additional computer** – without it you cannot open team folders there.

Unlocking another computer

On another computer, connect your organization account as described above. Krywerk then shows **"Unlock device ..."** (or asks for it the first time you open a team folder). Enter your unlock code – spaces, hyphens, and upper or lower case don't matter.

Signing in after a restart

Krywerk remembers your sign-in until you quit Krywerk. After a restart, the top of the window shows, in yellow, **"Organization account: not signed in – Sign in"**. Clicking it (or **"Sign in now"**)

opens the sign-in in your browser again.

Opening a shared team folder

To open a team folder, you need **two kinds of access**:

1. **The files:** The folder has to reach your computer – usually the person responsible shares it with you in **OneDrive** (in OneDrive: “Shared” > folder > “Add shortcut to My files” so that it is synced).
2. **The key:** The person responsible adds you in Krywerk and grants you access.

As soon as both are in place, the team folder appears in “My drives” with the label “Team”. Krywerk looks for the folder in OneDrive and other cloud folders by itself.

- **“Open”** mounts the team folder as a drive. **“Show in Explorer”** opens it, **“Close”** unmounts it.
- If it says **“Folder not found on this device”**, the folder is not synced (yet). Check the OneDrive share – or select the folder yourself with **“Find folder ...”**.
- If Krywerk reports when opening that access has not been granted yet, ask the person responsible to click **“Manage” > “Grant access”** for this team folder in Krywerk.

Creating and sharing a team folder yourself

1. On the overview, choose **“+ Add” > “Create and share team folder ...”**.
2. **Where?** Choose an empty folder – or a folder in which Krywerk creates a new subfolder (field “New subfolder”). A folder in OneDrive is a good choice for collaboration.
3. **Team folder name** – this is how others see it in Krywerk. Empty = the folder's name.
4. **Who?** Search for people or groups (name, email, or group) and add them:
 - **“Add”** – as a **member**: can open the team folder and read and edit files.
 - **“Add as manager”** – can additionally add and remove people, grant access, show the recovery key, set up emergency access, archive, and renew the key.

With Krywerk Server, people only show up in the search after they have signed in once with Krywerk (or Cryptomator) – so ask new colleagues to connect their organization account first.

5. Click **“Create team folder”**.
6. Krywerk shows the **recovery key** – see [chapter 5](#). Print or save it, check “I have stored the recovery key safely.”, and click “Done”.
7. **Also share the folder in OneDrive** with the same people (right-click > Share). Krywerk only controls who can decrypt the files – OneDrive still distributes them.

Recommendation: Add a second person as a manager and set up emergency access. Otherwise, if you are unavailable, nobody can add people or grant access anymore.

Granting access

Someone newly added to a team folder only receives the key once a manager **grants** access. This can only be done from the manager's computer, because Krywerk encrypts the key for the new person in the process.

Krywerk points this out to you:

- on the overview: "1 person is waiting for access ...", and on the team folder "1 waiting for access",
- in the system tray: in the icon's tooltip and in the entry "Pending access: ..." in the right-click menu.

On the team folder, click "**Manage**", check the people under "Waiting for access", and click "**Grant access**". For people whose identity has not been confirmed yet ("**not verified** Verify identity ..." – see [chapter 5](#).

Your fingerprint

Before someone grants you access, they can check whether the key server really gives them **your** key. You find your fingerprint under  **Settings** > **Organization account** > "**Show fingerprint**" (eight blocks of digits and the letters A–F). The first time on a computer, Krywerk asks once for your unlock code. Read your fingerprint out to the person asking **on the phone or in person** – not by email or chat, because those could run through the same channels as the key server.

5. Managing team folders (for managers)

This chapter is for people who **manage** a team folder – the list then shows “managed by you”, and there is a **“Manage”** button.

People and groups

Under **“Manage”** you see all members with their role.

- **Add:** Under “Add”, search for a name, email, or group, then click **“Add”** (member) or **“Add as manager”**. Afterwards, check the people under “Pending access” and click **“Grant access”** – preferably only after you have verified their identity (see below).
- **Change role:** **“Make manager”** or **“Make member”**.
- **Remove:** **“Remove”** next to the person. This applies to future opening. Anyone who has already opened the team folder may have kept files they downloaded and a copy of the key. So for confidential content, **renew the key** afterwards (see below).

Groups come from your organization account (for example Microsoft 365 groups). New group members get access as soon as you have granted it.

Verifying identity

When granting access, Krywerk encrypts the team folder's key to the key that the key server provides for that person. A manipulated key server could slip in someone else's key. With **“Verify identity ...”** you make sure the key really belongs to the person.

Under “Waiting for access” and in the member list, each person is marked:

- **“verified ✓”** – you have verified the identity (or someone whose identity you verified has verified it). The person is preselected for granting access.
- **“not verified Δ”** – not verified yet, or the person has received new keys (for example after an account reset). The person is **not** preselected.

How to verify an identity:

1. Call the person or talk to them in person – **not by email or chat**.
2. Ask them to open **⚙ Settings › Organization account › “Show fingerprint”** in Krywerk and read their fingerprint out to you.
3. Click **“Verify identity ...”** next to the person and type in the first characters (the dialog says how many; at least 8). Spaces and upper or lower case don't matter.
4. The very first time you verify on a computer, Krywerk also asks for **your** unlock code. After that, it works without it on this computer.
5. **“Confirm identity”**. If the characters don't match, Krywerk confirms nothing – have the fingerprint read out to you once more. If they still don't match, do not grant access and

inform your IT administration.

You can still check a person who is not verified. Krywerk then shows a warning and asks again before granting access. This only makes sense if you trust the key server.

For **emergency access**, too, Krywerk indicates when the identity of council members or of the requesting person has not been verified. Krywerk doesn't block anything there. Verify the identity and, if in doubt, set up emergency access again.

Recovery key

Every team folder has a **recovery key** (28 groups of four letters and digits). With it, the team folder can be opened **even without the key server** – for example if the server fails or is shut down. Whoever has it can read all the team folder's files.

- Krywerk shows it once when the folder is created. To see it again later: **“Manage” > “Show recovery key ...”**.
- To keep it safe: **“Print ...”** it and deposit it sealed with the school management, or **“Save as file ...”** in a secure password manager. Not in the team folder itself, and not unencrypted in OneDrive.
- **Opening without a server:** In the team folder's row, choose **“Open without server ...”** and enter the key. Krywerk does not remember the key.

Emergency access (four-eyes principle)

If all managers become unavailable, nobody can add people or grant access anymore. That is what emergency access is for: an **emergency council** (for example the principal and the deputy) can jointly give a person the manager role – but only if enough people approve.

Setting it up (manager): **“Manage” > Emergency access > “Set up ...”**

1. Choose people for the council (only people with a set-up organization account, no groups).
2. Specify **how many must approve** – at least 2. A single person never gets access alone.
3. **“Set up emergency access”**.

In an emergency (council member):

1. Open  **Settings > Organization account > Emergency access**.
2. On the team folder, choose **“Request emergency access ...”** and give a reason. Your own vote does not count.
3. The other council members see the notice “An emergency request is waiting for you” on their overview with **“Review”**, and approve with **“Approve ...”**. **Only approve once you have checked the request** – for example in person or by phone.
4. Once there are enough approvals, the requesting person clicks **“Complete”** and then manages the team folder. An open request can be withdrawn with **“Cancel ...”**.

Renewing the key (after someone leaves)

When someone leaves the group, the team folder should get a **new key**. Anyone who was excluded then cannot read the new content, even with an old copy of the key.

Beforehand: Ask all members to **close** the team folder. Changes made during the process are lost. On your own computer, Krywerk closes the folder itself.

1. **"Manage" > "Renew key ..."**.
2. Under **"Don't carry over"**, check the people who have left.
3. Optionally **"Keep old encrypted data"** – it then stays next to the folder, readable with the old key.
4. Click **"Renew key"**. Krywerk creates a new team folder with a new key, carries over the members, re-encrypts the content, and swaps it **in the same folder**. The OneDrive share stays in place. The old team folder is archived.
5. Krywerk shows a **new recovery key**. The old one only opens the archived state.

Afterwards, OneDrive syncs the entire content again. Older copies (recycle bin, OneDrive version history, copies held by people who have left) remain readable with the old key. If the process is interrupted, **"Resume key renewal ..."** continues it later.

Archiving

"Manage" > "Archive ..." locks the team folder: nobody can open it anymore, but the files are kept. **"Reactivate"** undoes this.

6. Switching from Boxcryptor

Boxcryptor is no longer being developed. Krywerk keeps opening existing Boxcryptor folders and migrates them **step by step** to the modern format – into a personal vault or a team folder. You can keep working normally in the meantime.

Beforehand: back up your key file

For Boxcryptor folders you need your **Boxcryptor key file** (extension `.bckey`, exported from Boxcryptor) and your **Boxcryptor password**. Without both, the data cannot be read.

- Keep a **backup of the key file** in a separate place, for example on a USB stick – until all folders have been migrated. In Krywerk you do this under ⚙ **Settings > Boxcryptor (legacy) > “Back up key file ...”** (while the account is unlocked).
- Practice the migration first with a **copy of a small folder**.

Adding a Boxcryptor folder

1. Choose **“+ Add”** (if applicable > “Personal vault or existing folder ...”).
2. Choose the format **“Classic (transition)”**.
3. Select the **encrypted Boxcryptor folder**, set a name and drive letter, and click **“Save”**.
4. The card **“Unlock Boxcryptor account”** appears on the overview. If the key file is still missing, first click **“Choose key file ...”**.
5. Enter the password, optionally check **“Remember password”**, then click **“Unlock”**. The top of the window now shows, in green, “Boxcryptor account unlocked”.
6. In the drive's row, click **“Mount”**. It carries the label “Boxcryptor (legacy)”.

Under ⚙ **Settings > Boxcryptor (legacy)** you'll also find “Change password ...”, “Delete saved password”, “Lock”, and two settings for classic drives: encrypt the filenames of new files (recommended), and the right-click menu in File Explorer.

Migrating

1. With the Boxcryptor drive mounted, click **“Switch to modern ...”**.
2. Choose the **target**:
 - **Password vault** – for your personal data, with its own vault password.
 - **Team folder (key server)** – for data that several people use. For this you must be signed in to your organization account; otherwise it shows **“Sign in now”**.
3. Specify the **folder for the new vault**. Krywerk suggests a **new** folder next to the Boxcryptor folder (name ending in “(Krywerk)"); you can also choose another empty folder, for example in OneDrive. The folder must not be inside the Boxcryptor folder.
4. For a password vault, set a vault password; for a team folder, optionally a name.

5. **“Start migration”**. For a team folder, Krywerk shows the recovery key – keep it safe (chapter 5).

From now on, the drive shows **both together**: everything new and every file you change automatically ends up in the modern format. The row shows how many files are still in the old format.

Migrating the rest – in one of two ways:

- **All at once: “Migrate all”**.
- **Folder by folder**: In File Explorer, right-click a folder in the drive › **“Switch to modern format with Krywerk”**. On Windows 11 the entry may only appear under “Show more options”.

Finishing

Once nothing is left in the old format, **“Finish migration”** becomes clickable. Afterwards the drive only shows the new vault or team folder. A team folder then appears with the label “Team”; you add people and groups under **“Manage”** (chapters 4 and 5).

The old Boxcryptor folder is no longer needed. **Check the result** – open a few files – and only then delete the old folder. Once all Boxcryptor folders have been migrated, Krywerk hides everything related to Boxcryptor.

7. Common questions and problems

The top of the window says “Organization account: not signed in”

Krywerk only remembers your sign-in until you quit Krywerk. Click the yellow notice or **“Sign in now”** and sign in in your browser. As long as you are not signed in, team folders without a folder on this computer are missing, as is “Manage”; personal vaults work regardless.

The browser signed me in automatically – with the wrong account

If someone is already signed in to the identity provider in the browser, the browser reuses that sign-in without asking. Sign out in the browser (at your organization's identity provider, e.g. Microsoft) and sign in again in Krywerk. The account that is signed in is shown at the top of the Krywerk window.

The sign-in tab in the browser is closed and Krywerk no longer responds

Krywerk waits up to 5 minutes for the sign-in. Restore the tab (in the browser, **Ctrl+Shift+T**) and sign in – or wait until Krywerk cancels the sign-in with a message, and try again.

A team folder shows “Folder not found on this device”

The folder is not on your computer yet. Check whether it has been shared with you in OneDrive and added as a shortcut to “My files”, and whether OneDrive has finished syncing. Or select it yourself with **“Find folder ...”**.

When opening a team folder, it says access has not been granted yet

You have been added, but the person responsible has not granted access yet. Ask them to click **“Manage”** › **“Grant access”** in Krywerk.

Changes made by colleagues don't arrive

First check whether OneDrive is syncing (OneDrive icon in the system tray). If the changes still don't appear in the drive, or only appear late, turn off the **cache** under ⚙ **Settings** › **General** › **Advanced** and mount the drive again.

The drive doesn't appear

- Is it mounted? The list must show “Mounted as ...” or “Opened at ...”.
- On Windows, **WinFsp** must be installed (chapter 2).
- If the chosen drive letter is already taken (e.g. by a network drive), choose a different one or “Automatic” under “Edit”.

I forgot my vault password

A personal vault cannot be opened without its password – not even by IT. If the password is remembered in Krywerk, you can keep opening the vault on this computer; in that case, create a new vault and copy the files over.

I lost my unlock code

You can keep working on computers that are already unlocked. For a new computer you need the unlock code. Contact your IT administration.

My computer was lost or stolen

Report it to your IT administration. Anyone who manages team folders the computer had access to should **renew the key** after a loss (chapter 5). Personal vaults with a remembered password are protected by your Windows user account – which is why a strong Windows password is important.

The key server cannot be reached

Team folders that are already open stay open. To open one without the server you need the **recovery key** ("**Open without server ...**", chapter 5) – the person responsible has it.

Can I open team folders on my phone?

Not yet. You open personal vaults with the Cryptomator app (chapter 3).

8. Glossary

Boxcryptor (legacy) – label for Boxcryptor folders in Krywerk. An older method, only for the transition.

Boxcryptor key file (`.bckey`) – file exported from Boxcryptor containing your Boxcryptor keys, protected by your Boxcryptor password.

Cache – makes drives faster; only turn it off if there are problems with changes from other devices.

Emergency council / emergency request – people who can jointly (four-eyes principle) give a person management rights to a team folder if all managers become unavailable.

Fingerprint – 64 characters (eight blocks) calculated from a person's public keys. If the person reads it out and it matches what you see, the key really belongs to them.

Grant access – the step in which a manager makes a team folder's key available to new members.

Identity provider – the service where you sign in with your organization account, for example Microsoft 365. Krywerk opens it in your browser.

Identity verified / not verified – whether you (or a person you trust) have compared a person's fingerprint with them. Recommended before granting access.

Key server – manages who may open which team folder (Krywerk Server or Cryptomator Hub). It cannot read the files themselves.

Krywerk Server – key server for team folders that your organization runs itself. Compatible with Cryptomator Hub, without license limits.

Member / manager – roles in a team folder. Members open and edit files; managers can additionally add people, grant access, and take care of emergency access and recovery keys.

Mount / unmount – make a drive available or remove it again. The files are kept either way.

Organization account – your account at your school or organization (e.g. Microsoft 365), which you use to open team folders.

Personal vault – encrypted folder with its own password, in the Cryptomator format.

Recovery key – 28 groups of four characters that can open a team folder without the key server. Should be kept safely by the people responsible.

Renew key – give a team folder a new key, for example after a person has left.

Team folder – encrypted folder for several people, opened through the organization account.

Unlock code (also *Account Key*) – your personal code for team folders. Krywerk shows it once when you set up your account. You need it to unlock additional computers. Only you have it.

Unlock device – allow a computer for your organization account so that it can open team folders.

Vault password – the password of a personal vault. Cannot be recovered.