Mozout

Generated on 15/11/2026 00:39

KNOWLEDGE BASE · PUBLIC DOCUMENT

Getting an API key for an AI model, and keeping it safe

Agents & AI on a VPS

CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-2940	v2026.10.10	International · English

MozOut International
RLX Holdings (Pty) Ltd. · Group RLX Holdings
Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/2940

Getting an API key for an AI model, and keeping it safe

Agents & AI on a VPS Created on **October 10, 2026** 3 min read



An **API key** is a long password that identifies your account with an AI model provider. Whoever holds it uses your account and **spends your money**. You get one from a developer account at the provider, and you keep it **on the server, outside the code and outside any published folder**. That last part is the one people get wrong.

How to get one

1. **Choose the provider.** The best known are OpenAI, Anthropic and Google, and there are others. Each has its own developer platform, separate from the chat app you use on your phone.

2. **Create the developer account** and attach a payment method if the provider requires one. APIs charge by use, apart from any subscription to the chat app.

3. **Set the spending limit** or usage alerts before you create the key. Most providers offer this in the console.

4. **Create the key** in the API keys section, name it for what it is for, and if there are permissions, choose the minimum.

5. **Copy it straight away.** Many providers show it only once. If you lose it you cannot get it back: create another and revoke the old one.

Where each option sits changes from provider to provider and over time. Follow the provider’s documentation, not a screen you saw in a video. The price is always on their pricing page.

Where to keep it, and where never

Place	Fine?	Why
An environment variable on the server	Yes	It stays out of the code. See **environment variables and secrets**.
A configuration file outside the public folder, readable only by you	Yes	It is not served to anyone and does not go into the repository.
A password vault	Yes, as a copy	If you lose the server you do not lose the key.
Inside the website's code, or in JavaScript the visitor downloads	Never	Any visitor can see it, and starts spending on your account.
In a public repository (GitHub, etc.)	Never	Programs sweep repositories looking for keys, and they are quick about it.
In a chat, e-mail or message	Never	It stays in places you do not control.

If the key has leaked
(it showed up in a repository, a shared screen, an e-mail), revoke it **now**, in the provider's console, and create another. Then check usage to see whether anyone has used it. Deleting the message is not enough: the key may already have been copied.

1. **One key per project or agent.** You can revoke one without stopping the others.
2. **Rotate them now and then** and whenever someone who knew them leaves the project.
3. **Keep the limit as low as the project allows,** and raise it only when you need to.

On a WordPress site, if a plugin asks for the key, it is stored in the site's database. That is acceptable, but only if the site is kept updated and protected. See **WordPress with AI help**.

NEED A HAND?

Need help working out where to keep a key on your VPS? Tell us how it is set up.

Open a support ticket →

SEE ALSO

- Tokens explained: how AI model APIs are counted
- Environment variables and secrets for your application
- What OpenClaw costs: the API keys, not the server

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-INT-KB-2940 · v2026.10.10 · Generated on 15/11/2026 00:39