Mozout

Generated on 29/11/2026 04:04

KNOWLEDGE BASE · PUBLIC DOCUMENT

Keeping your AI key safe: only on your server, never in the browser or a mobile app

Using the AI API

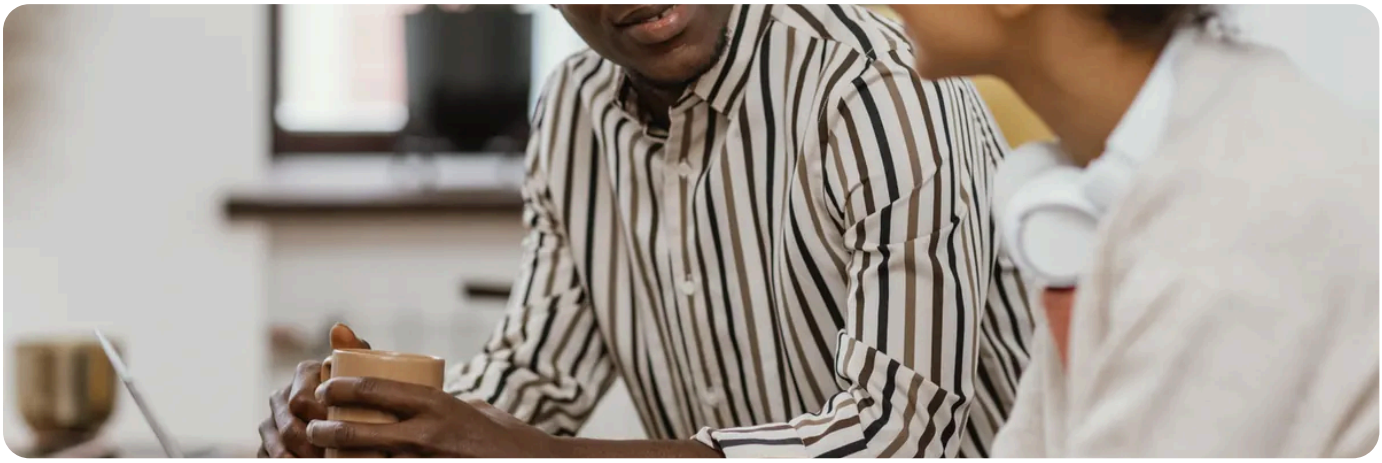
CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-9132	v2026.11.28	International · English

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/9132

Keeping your AI key safe: only on your server, never in the browser or a mobile app

Using the AI API Created on **November 28, 2026** 2 min read



In short: whoever has your key spends your AI credits. So the key stays only on your server, in an environment variable. Never put it in code that runs in the browser or in a mobile app: anyone can open that code and copy it.

Why not in the browser or in the app

The code of a web page reaches the browser of whoever visits it in full. A mobile app can also be opened and read. Hiding the key in the middle of the code is not enough. And browsers can only call our API from the documentation: the pages of your website cannot use the key directly.

The right way

1. The browser or the app sends the question to **your** server, with your website's login and rules.
2. Your server adds the key, read from the environment variable, and makes the request to our API.
3. Your server gets the answer and passes it to the browser. With streaming, it passes the pieces as they arrive: see **showing the reply as it is written**.

This way the key never leaves the server, and your server decides who can ask and how much.

The key in an environment variable

The code reads the key from the variable and never has it written down. In Python, Node.js and PHP:

```
client = OpenAI(base_url="https://api.mozout.com/v1", api_key=os.environ["MOZOUT_API_KEY"])
```

```
const client = new OpenAI({ baseURL: "https://api.mozout.com/v1", apiKey: process.env.MOZOUT_API_KEY });
```

```
$key = getenv("MOZOUT_API_KEY");
```

Never keep the key in a repository. If you use a `.env` file, it must not be in a public folder of the website: see **the files that must never be public**.

A key just for AI

When you create the key	What to choose
Permissions	Only `ai:read` and `ai:write`. One key per program.
Mode	`sandbox_` while you develop, `prod_` on the real server. A `sandbox_` key also reads real account data: keep it just as carefully.
Validity	30, 90 or 365 days, or no expiry. The default is 90 days. Prefer a short validity.
IP list	If your server has a fixed IP, add it. From any other IP, the key gives `403 ip_not_allowed`.

If the key gets out

Revoke it straight away in the **API Center** and create another. Then look at the **History** tab of All in One AI: each request shows the model, the key and the credits spent, with filters and CSV export. The step by step is in **a key has leaked**.

RECOMMENDED

Want to see which keys used AI and how much they spent? Open the History in All in One AI.

See All in One AI →

SEE ALSO

- **An API key or token has leaked: what to do, in the right order** →
- **Looking after your API keys: one per program, expiry, revoking and replacing a key** →
- **Creating an API key: name, mode, permissions, validity, IP list and spending limit** →
- **Environment variables and secrets for your application** →
- **All in One AI** →

Mozout

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-9132 · v2026.11.28 · Generated on 29/11/2026 04:04