



LACSPACE

Developer Documentation

Security Kit — the seven layers, as code

@lacspace/otp

TOTP / HOTP 2FA

v1.1.1 · zero dependencies · isomorphic · generated 2026-09-01

Overview

Google Authenticator-compatible two-factor auth over Web Crypto — runs on Node, edge and browser. Generate secrets, verify codes with drift tolerance and replay protection, build otpauth:// URIs, and issue single-use hashed backup/recovery codes. A tiny speakeasy alternative, verified against the RFC test vectors.

NOTE

When to use — Adding TOTP/HOTP two-factor authentication (Google Authenticator-style) to an app.

Package: @lacspace/otp · v1.1.1

Kit: Security Kit — the seven layers, as code

Runtime: zero dependencies · isomorphic

Install

```
npm i @lacspace/otp
```

Quick example

```
await verifyTotp(code, secret)
```

Returns: **0 (valid) | null**

Tips & warnings

TIP

``keyuri()`` produces the ``otpauth://`` URL for a QR code; show it once during enrollment.

TIP

``verifyTotp()`` accepts a small time window to tolerate clock drift.

TIP

Zero-dependency and isomorphic — safe to import on the server, in the browser, on the edge and in React Native. It tree-shakes, so you only ship what you import.

WARNING

Store the shared secret encrypted (see @lacspace/crypto) and offer backup codes for recovery.

Links & full reference

- npm: <https://www.npmjs.com/package/@lacspace/otp>
- Source & full README: <https://github.com/lacspace/npm-packages/tree/main/otp>
- Docs: lacspace.com/docs/otp

The npm page and GitHub README carry the complete API reference and more examples.