LACSPACE

Developer Documentation

Security Kit — the seven layers, as code

@lacspace/crypto

AES-256-GCM encryption

v1.1.1 · zero dependencies · isomorphic · generated 2026-08-25

Overview

Authenticated AES-256-GCM encrypt/decrypt (with AAD), PBKDF2 & HKDF key derivation, SHA-2, HMAC, secure random and constant-time compare — a thin, correct layer over Web Crypto. Plus a versioned Keyring for envelope encryption & key rotation. Encrypt Mongo fields, S3 payloads and cookies.

> **NOTE**
> When to use — Encrypting a field before it lands in your database or object storage, using authenticated AES-256-GCM.

Package: @lacspace/crypto · v1.1.1

Kit: Security Kit — the seven layers, as code

Runtime: zero dependencies · isomorphic

Install

```
npm i @lacspace/crypto
```

Quick example

```
await decrypt(await encrypt(data, key), key)
```

Returns: **data**

Tips & warnings

> **TIP**
> Built on Web Crypto — the same code works in Node, browsers and the edge.

> **TIP**
> Store the key outside your code (env/secret manager); rotate by versioning ciphertext.

> **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**
> Never hand-roll crypto or reuse a nonce — the package manages nonces per message; don't override that.

> **WARNING**
> Losing the key means losing the data — back it up securely.

Links & full reference

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

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