

ENGINEERING & OPERATIONS GUIDE

Re-Mem Pro

User Guide & Security Manual

Comprehensive guide to installing, operating, and securing credentials with Re-Mem Pro — the 100% offline, zero-knowledge password manager and hardware passkey vault for Windows 10 & 11.

ARCHITECTURE

100% Offline

CRYPTOGRAPHY

Argon2id + AES-256

DEPLOYMENT

Store & Portable USB

Table of Contents

This manual covers end-to-end operation, cryptographic guarantees, and emergency recovery workflows for both the Installed Desktop Edition and the Standalone Portable USB Edition.

01 Core Philosophy & Security Architecture Zero-knowledge, Argon2id, AES-256-GCM, and envelope encryption.	02 Editions: Desktop vs. Portable USB Choosing between Microsoft Store / MSIX and zero-install USB mode.
03 Setup, Vault Creation & Windows Hello Master password hygiene, Argon2id salts, and biometric unlock.	04 Printable Emergency Kit & QR Rescue Generating paper kits, smartphone scanning, and master password resets.
05 Hardware Passkeys & Live TOTP 2FA FIDO2 / WebAuthn NIST P-256 keys and integrated 30s live rings.	06 Browser Extension & Multi-Profile Support Local loopback IPC autofill and profile isolation (Work vs Personal).
07 Developer Secrets & .env Exporter Masked API keys, 1-click .env generation, and rollback audit logs.	08 Tamper Shield & 10-Attempt Auto-Destruct Anti-brute force defenses and physical security protocols.
09 Hardware Device ID Binding & Licensing Finding your Device ID, activating perpetual licenses, and GST invoices.	10 Disaster Recovery & Operational FAQ Moving vaults across PCs, air-gapped backups, and support channels.

1. Core Philosophy & Security Architecture

Most commercial password managers synchronize customer vaults across centralized cloud servers. While convenient, this architecture presents a persistent target for cloud breaches, credential stuffing, and unauthorized third-party access. **Re-Mem is architected on a zero-knowledge, strictly offline model:**



0% Cloud Exposure
No remote databases, telemetric trackers, or network sockets communicating externally.



Argon2id KDF
64 MB RAM allocation, 4 iterations, rendering GPU brute-force attacks computationally unfeasible.



AES-256-GCM
Military-grade authenticated encryption guaranteeing confidentiality and tampering detection.

Envelope Encryption Architecture

Re-Mem separates the key used to encrypt your credentials from your master password using cryptographic envelope encryption:

- Data Encryption Key (DEK):** A high-entropy 256-bit symmetric key that directly encrypts and decrypts your vault records.
- Key Encryption Key (KEK):** Derived dynamically from your Master Password using `Argon2id` and a cryptographically random 16-byte salt. The KEK wraps (encrypts) the DEK.
- Recovery KEK:** A secondary wrapping layer derived from your unique 32-character Emergency Recovery Key, enabling master recovery without cloud dependencies.

2. Editions: Desktop vs. Portable USB

Re-Mem Pro is available in two distinct distribution editions tailored to different operational requirements:

FEATURE	INSTALLED DESKTOP EDITION	PORTABLE USB EDITION
Distribution	Microsoft Store / MSIX Package	Standalone ZIP Archive (<code>Re-Mem-Portable.zip</code>)
Administrator Rights	Standard user or Store install	Zero privileges required (Runs anywhere)
Storage Location	<code>%LOCALAPPDATA%\Novvitech\Re-Mem\</code>	Self-contained in adjacent <code>data/</code> folder
Ideal Use Case	Primary workstation, auto-updates via Store	USB flash drives, corporate locked PCs, air-gapped systems

 **Portable USB Operation:** To run Re-Mem on a USB drive, extract `Re-Mem-Portable.zip` directly onto your flash drive (e.g., `E:\Re-Mem-Portable\`). All vaults, settings, and encryption states will remain strictly on the USB stick. When unplugged, zero credential traces remain on the host machine.

3. Setup, Vault Creation & Windows Hello

Step 1: First-Time Initialization

1. Launch **Re-Mem** (or `Re-Mem-Portable.exe`).
2. The Setup Wizard will guide you through creating your master vault.
3. Choose a strong, memorable Master Password. Minimum requirement: 8 characters. We recommend a 4-word diceware passphrase (e.g., `correct-horse-battery-staple`).
4. Re-Mem computes the `Argon2id` salt and produces your initial encrypted vault file (`vault.remem`).

Step 2: Windows Hello Biometrics & Quick Unlock

If your machine supports Windows Hello (Fingerprint reader, Infrared Facial Recognition camera, or TPM-backed Windows PIN), Re-Mem offers **Quick Unlock**:

- Upon successful first login, Re-Mem prompts to activate Windows Hello.
- When enabled, Re-Mem securely wraps your session DEK using Windows Data Protection API (DPAPI) and Windows Biometric Credential Manager.
- On subsequent launches, tap "  **Quick Unlock with Windows Hello** " to decrypt your vault in under 1 second without typing your master password.

 **Biometric Security Note:** Windows Hello acts as a local convenience unlock. Your Master Password is still strictly required after PC reboots, or when modifying core security settings. Never forget your master password.

4. Printable Emergency Recovery Kit & QR Rescue

Because Re-Mem is 100% offline with zero cloud access, **NovviTech engineers cannot reset your password** if you forget it. To eliminate lockout risk, Re-Mem generates an official Printable Emergency Kit.

Generating Your Emergency Kit

1. In Re-Mem, open **Settings** → Scroll to **Emergency Kit** → Click "**Generate Emergency Kit**".
2. Select a destination folder. Re-Mem creates a formatted HTML document and opens it in your default browser.
3. Click "  **Print / Save PDF**". Store the physical printed page in a fireproof safe, bank locker, or with your trusted executor.

How to Restore Access When Locked Out

If you ever forget your master password:

1. At the Re-Mem Unlock Screen, click "**Forgot Password? (Recover)**".
2. **Retrieve your printed Emergency Kit:**
 - **Smartphone QR Scan (Recommended):** Point your smartphone camera (Google Lens or iOS Camera) at the printed QR code. Tap "Copy text" to instantly grab the 32-character key without typos.
 - **USB Barcode Scanner:** Scan the QR code directly into the PC prompt.
 - **Manual Entry:** Type the 32-character key printed in 4-character blocks (e.g., `ABCD-1234-EF56-...`). Hyphens and case are automatically normalized.
3. Click **OK**. Re-Mem unwraps your vault using the secondary Recovery KEK.
4. Re-Mem prompts: "**Enter your NEW master password**". Enter and confirm your new password. Your vault is re-encrypted with the new key and unlocked immediately!

5. Hardware Passkeys & Live TOTP 2FA

FIDO2 / WebAuthn Hardware Passkeys (NIST P-256)

Re-Mem features a built-in cryptographic passkey manager that completely replaces passwords on modern services (Google, GitHub, Microsoft, AWS, Cloudflare):

- Generates asymmetric cryptographic keypairs using the **ES256 (NIST P-256)** curve.
- Private keys remain encrypted inside your local vault and never leave your machine.
- Protects you against 100% of phishing, spoofing, and SIM-swap attacks.

Integrated Live TOTP 2FA Authenticator

Eliminate dependency on mobile authenticator apps (Google Authenticator, Authy):

- Scan or paste any standard `otpauth://` URI or base32 secret key.
- Displays a real-time 30-second animated circular ring indicator with active 6-digit codes.
- 1-click copy or automatic autofill into login prompts via global hotkey (`Ctrl+Alt+L`).

6. Browser Companion Extension & Multi-Profiles

Re-Mem includes a lightweight companion extension for **Google Chrome, Microsoft Edge, Brave, and Firefox** that autofills login credentials without exposing secrets to the web.

Local Loopback Architecture (Zero Web Exposure)

Unlike cloud password extensions that send tokens to remote servers, the Re-Mem extension communicates strictly via a **local loopback IPC bridge (127.0.0.1)** with the desktop app. It operates only when the desktop app is unlocked.

Browser Multi-Profile Isolation (Work vs. Personal)

If you use distinct browser profiles (e.g., *Work* vs *Personal*, or client-specific workspaces), Re-Mem prevents credential contamination:

- Assign specific entries or categories to designated profiles.
- When browsing under a Work profile, personal credentials remain completely hidden from autofill lists.
- Profiles can be created, switched, or renamed directly inside the extension popup.

7. Developer Secrets & .env Manager

Re-Mem Pro is engineered with native developer workflows, providing first-class management of environment variables and infrastructure tokens.

 **Why Local .env Management Matters:** Many teams commit sensitive `.env` files to git or store production secrets in plaintext on disk. Re-Mem encrypts all environment keys inside your Argon2id vault and generates sanitized exports on demand.

Core Developer Features:

- **Masked Key-Value Storage:** Store Stripe secret keys, AWS access tokens, database connection strings, and SSH passphrases behind click-to-reveal masks.
- **1-Click `.env` Exporter:** Export selected developer credentials into a standard UNIX/Windows `.env` file formatted for Next.js, Django, Node, or Docker.
- **Environment Variable Importer:** Ingest existing `.env.local` files into your vault with automatic duplicate detection.
- **Password Revision History & Rollback:** Every update to an entry creates an immutable timestamped audit record. Accidental overwrites or changed API keys can be rolled back in 1 click.

8. Tamper Shield & 10-Attempt Auto-Destruct

To defend against physical laptop theft and offline hardware brute-forcing rigs, Re-Mem implements an active tamper mitigation shield:

- **10-Attempt Auto-Destruct:** If an unauthorized party attempts 10 consecutive incorrect master passwords, Re-Mem immediately executes an anti-forensic shredding routine on the active database.
- **Safety Isolation:** A temporary emergency backup is moved to an isolated recovery state, requiring the 32-character Emergency Recovery Key to resurrect.
- **Clipboard Auto-Purge:** Any credential copied to the Windows clipboard is automatically purged after 30 seconds to prevent malware scrapers from intercepting keys.

9. Hardware Device ID Binding & Licensing

How Device Binding Works

Every Re-Mem Pro license key is cryptographically bound to your machine's unique **Hardware Device ID** (derived from CPU, Motherboard BIOS, and Storage identifiers). This prevents unauthorized key sharing while granting you unlimited lifetime usage on your PC.

How to Find Your Device ID & Activate

1. Open Re-Mem on your computer.
2. Click **Settings** (gear icon in sidebar).
3. Scroll to **License & Device Details**.
4. Click **"Copy Device ID"** (e.g., `A1B2-C3D4-E5F6-7890`).
5. Paste this Device ID into the checkout form on novvitech.com/products/re-mem. Your permanent license key is generated instantly.
6. Click **"Enter License Key"** in Re-Mem and paste your key. PRO features unlock perpetually.

GST Invoicing & International LUT Declarations

All purchases include statutory commercial invoicing: Indian businesses receive GST invoices under SAC Code **998313** eligible for Input Tax Credit (ITC). International orders are processed under statutory LUT export endorsements (ARN: `AD0809260136601`).

10. Disaster Recovery & Operational FAQ

Q: How do I back up my vault?

Simply copy your `vault.remem` file (or your entire `data/` folder if using Portable Edition) to a secondary backup drive. Because the file is encrypted with AES-256-GCM, it is completely secure even in cold storage.

Q: Can I run Re-Mem completely air-gapped without internet access?

Yes, 100%. Re-Mem has zero cloud dependencies, requires no online activation checks, and contains no telemetric phone-home code. It is certified for fully air-gapped and military/isolated environments.