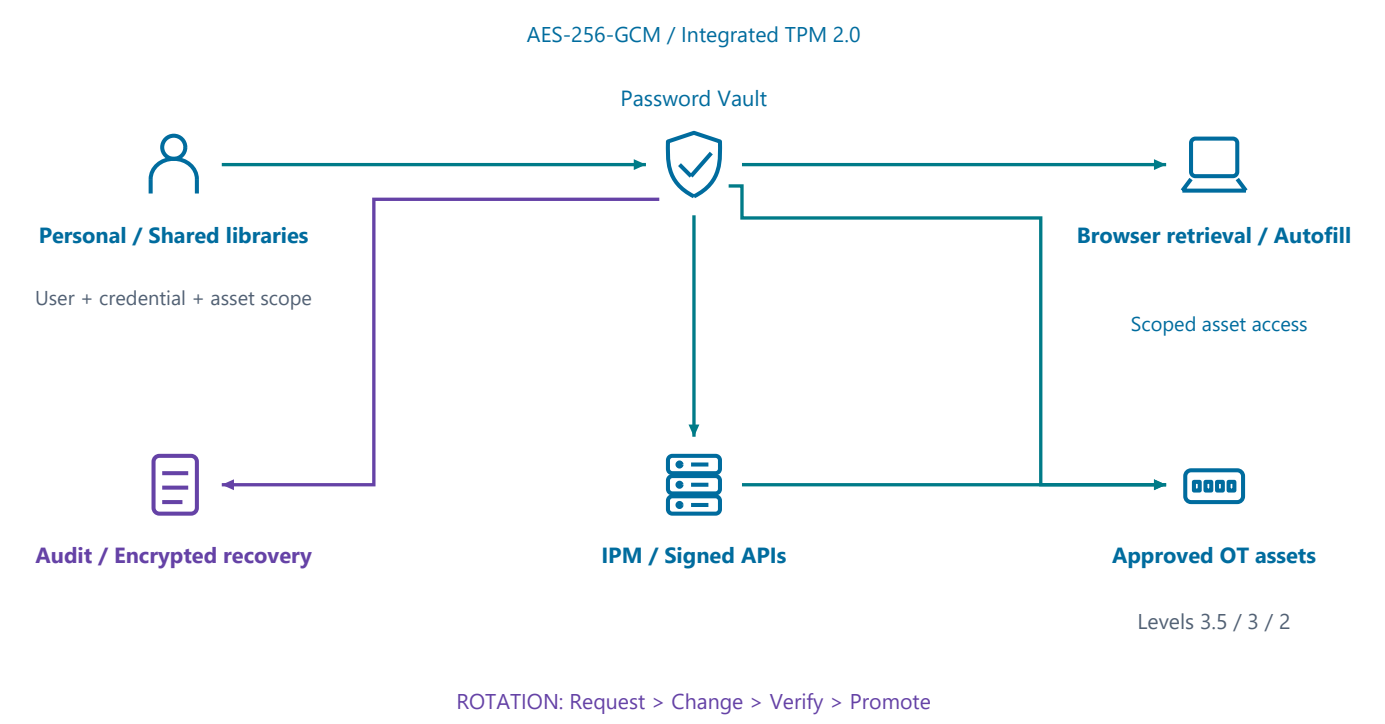


Protect secrets. Govern their use.

Unify personal credential retrieval, approved shared libraries, browser autofill and controlled rotation with user- and asset-scoped access.



Illustrative workflow. Connections and permissions follow the approved deployment.

PRODUCT WORKFLOWS / KEY CAPABILITIES

- 01

Personal and shared access

Retrieve personal credentials and approved shared libraries.
- 02

Browser-assisted sign-in

Retrieve and autofill in supported Chrome, Edge and Firefox workflows.
- 03

Scoped IPM integration

Bind retrieval and rotation to authorized users and target assets.
- 04

Controlled rotation

Verify target changes before promotion and retain audit evidence.

The capabilities behind the workflow.

REPLIL Password Vault - detailed product features



Personal retrieval and shared password libraries

Give authorized users access to personal credentials and approved shared password libraries. Keep shared access governed by the assigned retrieval scope.



Browser retrieval and autofill

Retrieve approved credentials and autofill supported browser sign-in workflows in Chrome, Edge and Firefox, within the configured permissions.



Private ownership and scoped access

Authorize credential access by user, credential, and asset context. Separate metadata viewing, secret retrieval, and rotation permissions; ordinary platform administration does not automatically reveal user secrets.



AES-256-GCM envelope encryption

Encrypt secret values, sensitive metadata, MFA seeds, and recoverable API signing keys using per-value data keys. Protect them with separately supplied key-encryption material and authenticated owner, record, version, and purpose context.



TPM 2.0-backed key protection

Support Linux TPM 2.0-backed protection of bootstrap key material through systemd encrypted credentials. Required TPM mode fails closed when the required protection or key material is unavailable.



Independent encrypted recovery

Maintain an independently encrypted recovery wrapping of vault key material for approved restoration onto replacement infrastructure. Recovery custody is separate from ordinary account sign-in.



Per-user signed API access

Use independently revocable, expiring access keys with credential scopes. RFC 9421 signed requests bind request context and body integrity, with timestamp and nonce replay checks.



Controlled target password rotation

Run supported manual and scheduled rotation workflows with encrypted pending values, account coordination, verification before promotion, and reconciliation after uncertain outcomes. Connector acceptance depends on the target platform.



Deep IPM workflow integration

Use IPM user and asset context for scoped credential retrieval and rotation through signed APIs and stable credential references. Integration availability depends on the deployed IPM and vault versions.



Strong vault sign-in and auditing

Protect vault login passwords with PBKDF2-HMAC-SHA512 hashing, require TOTP MFA, and retain access and rotation audit records without logging secret values.

Make the workflow fit the facility.



- **Operator credential retrieval**
 Give authorized users access to their personal credentials and approved shared libraries.
- **Browser-assisted sign-in**
 Retrieve and autofill approved credentials in supported browser workflows.
- **IPM-context rotation**
 Scope retrieval and rotation by user and asset, with verification and audit evidence.

MINIMUM DEPLOYMENT RESOURCES

CPU	RAM	STORAGE
2 vCPU	16 GB minimum	40 GB SSD

Minimum 16 GB RAM. TPM 2.0-backed deployment requires a compatible TPM/Secure Boot profile; encrypted recovery and approved backups are sized separately.

Ubuntu Server 24.04 LTS x64 / configured TPM or key-protection profile

BUILT FOR CRITICAL INFRASTRUCTURE








Oil & gas
 Energy & utilities
 Manufacturing
 Water
 Smart cities
 Transport