Vault App

General description and Software Requirement Specification

Version 0.1 – 2025-12-22

Robert Zondervan
Conduction

Vault App

General design and Software Requirement Specification

Table of Contents

General description

Functionality

The vault app is a Nextcloud application for storing and sharing secrets with other users or applications. This means that the vault is usable as a key store for applications, but also as password manager[1].

The application stores encrypted secrets in the database (for the way this works, see the chapter Encryption.

Creating secrets

In creating a secret the secret must have a name (which is stored unencrypted) a key (password, api key, etc., stored encrypted) and may have a login field (username, client id) and additional fields (all stored encrypted, additional fields will be stored as an encrypted json blob).

The backend provides a generator for secrets which can be configured with the call from frontend to backend to fit the requirements of the user. (See Key Generator for the requirements for the key generator).

Sharing secrets with other users

Secrets can be shared with other users, by doing this the secret will be copied, and its fields will be encrypted for the user the secret is shared with. When either user changes the secret, this will be written also to the secrets that are shared from the original secret.

Sharing secrets with applications

Secrets can also be shared with either internal and external applications (this functionality does not differ for internal and external).

When sharing the secret the user must have been granted access to share secrets with that application. The user can then either share a secret in their own vault to the application, or write a new secret for the application. When using this last functionality, note that the user can never read the secret after storing it, although they can override it by saving the secret anew.

Sharing secrets with link

The third way to share secrets is with a secret link. This will generate a link for external parties to fetch the secret, and a password that has to be entered by the user to decrypt the encrypted secret. The user can set the amount of times the password can be used, after that the shared secret is removed.

Registering an (external) application

Registering an application can be done by any user, and even anonymous. However, if the user is not the administrator of the Nextcloud instance or an app administrator of the vault, the application will be placed in a queue to be activated by the app administrator. Until that moment no secrets can be attributed to the created application.

---

[1] At this moment in time, a browser plugin for autofill is not in scope of the project, but a desirable stretch goal