Password Vault File Structure

The password vault has the following file structure on disk. To keep things simple, all integers will be unsigned and stored in native byte order (little endian).

|  |  |  |
| --- | --- | --- |
| Size (bytes) | Name | Description |
| 8 | ppSalt | Salt for the user's master passphrase |
| 12 | keyEncNonce | Nonce for the database key encryption |
| 16 | keyEncAuthTag | Authentication Tag for the encrypted database key |
| 16 | keyEncData | Encrypted database key |
| 2 | dbVersion | DB version number |
| 4 | dbSize | Size of the encrypted password database (in bytes) |
| 12 | dbEncNonce | Nonce for the encrypted password database |
| 16 | dbEncAuthTag | Authentication tag for the encrypted password database |
| dbsize | dbEncData | The encrypted password database |

The decrypted password database structure is as follows:

|  |  |  |
| --- | --- | --- |
| **Size (bytes)** | **Name** | **Description** |
| **4** | entryCount | Number of accounts/entries in the password database |
| **dbSize** | dbEntries | The account data |

 Each account record has the following structure. Note that strings are *not* NULL-terminated.

|  |  |  |
| --- | --- | --- |
| **Size (bytes)** | **Name** | **Description** |
| **4** | recordSize | Size of the account record (in bytes), including this field |
| **2** | pwSize | Size of the encrypted password |
| **12** | pwEncNonce | Nonce for the encrypted password |
| **16** | pwEncAuthTag | Authentication tag for the encrypted password |
| **pwSize** | pwEncData | Encrypted password |
| **2** | acctNameLen | Length of the account name |
| **acctNameLen** | acctName | Account name |
| **2** | acctLoginLen | Length of the account login name |
| **acctLoginLen** | acctLogin | Account login name (username) |
| **2** | acctUrlLen | Length of the account URL |
| **acctUrlLen** | acctUrl | URL to the account |

# Sample Vault

A sample vault file is provided with the source distribution. The passphrase for this vault is:

An enticing aroma of fruit flavors accented by licorice.

The passwords for the three accounts defined in this vault are:

addition pack solar ring

GLV2TE@#P+FvMC?B9wYBz5rj

O1d-Tongue 0pportunity-ball

The master key is:

ca ab 23 30 eb a7 db 71 eb ed 10 91 7f 78 88 c2

The database/vault key is:

9b 34 4f fb bb d5 4d 52 23 b6 03 f0 aa da 9b 7a