Das Handbuch zu KWallet

George Staikos
Lauri Watts
Entwickler: George Staikos
Deutsche Übersetzung: Gregor Zumstein

Das Handbuch zu KWallet

Inhaltsverzeichnis

Zusammenfassung

Das Passwortspeicher-Subsystem erlaubt die bequeme und gleichzeitig sichere Aufbewahrung Ihrer Passwörter.

Kapitel 1

Einleitung

Computernutzer müssen eine riesige Datenmenge verwalten, ein Teil davon ist sicherheitsrelevant. Insbesondere müssen sie viele Zugangsdaten und Passwörter verwalten. Sich diese alle zu merken ist schwierig, sie auf Papier oder in einer Textdatei aufzuschreiben ist unsicher.

KWallet bietet eine sichere Möglichkeit, Passwörter und andere persönliche Informationen zu speichern. Damit muss sich der Benutzer nur noch ein einzelnes Passwort anstatt zahlloser verschiedener Passwörter und Anmeldedaten merken.

1.1 Einen Passwortspeicher erstellen

KWallet ist ein Speicher für Passwörter. Es ist normalerweise ausreichend, nur einen Passwortspeicher zu benutzen, der durch ein Hauptpasswort gesichert ist. Sie können eine große Anzahl von Passwörtern in Speichern mit KWallet Manager organisieren.

Als Voreinstellung wird ein Passwortspeicher mit dem Namen **kdewallet** zur Speicherung Ihrer Passwörter verwendet. Dieser Passwortspeicher wird durch Ihr Passwort zur Anmeldung abgesichert und wird automatisch bei der Anmeldung geöffnet, wenn „kwallet_pam“ installiert und richtig eingerichtet ist. Bei bestimmten Distributionen wie z. B. Archlinux ist „kwallet_pam“ nicht in der Voreinstellung installiert.

Andere Passwortspeicher müssen manuell geöffnet werden.

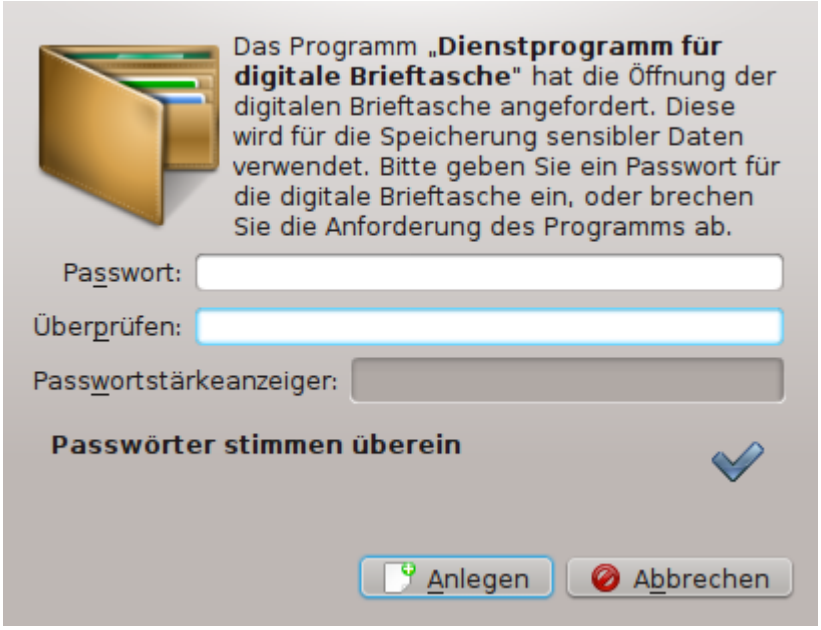
Es gibt zwei Möglichkeiten, einen neuen Passwortspeicher zu erstellen:

- Verwenden Sie den Menüeintrag **Datei** → **Neuen Passwortspeicher** im KWallet Manager
- Verwenden Sie den Knopf **Neu** im Systemeinstellungen-Modul **Passwortverwaltung**

Falls Sie bisher noch keinen Passwortspeicher erstellt haben, lesen Sie den Abschnitt KWallet benutzen.
KWallet bietet zwei unterschiedliche Methoden, Ihre Daten zu speichern:

Blowfish-Verschlüsselung

KWallet speichert genau diese sicherheitsrelevanten Daten in einer mit starker Kryptografie verschlüsselten Datei, auf die alle Anwendungen zugreifen können. Die Daten werden durch ein von Ihnen festgelegtes Hauptpasswort geschützt.



Die Daten werden mit dem symmetrischen Blockverschlüsselungsalgorithmus Blowfish verschlüsselt. Der Schlüsselalgorithmus wird aus dem SHA-1-Hash-Wert des Passworts berechnet, mit einer Schlüssellänge von 156 Bit (20 Byte). Aus den Daten in der Passwortspeicher-Datei werden zusätzlich Hash-Werte mit SHA-1 berechnet und vor der Entschlüsselung und dem Zugriff von Programmen überprüft

GPG-Verschlüsselung

GnuPG verwendet einige sehr starke Verschlüsselungsalgorithmen und verwendet lange Schlüssel, die mit einer Passphrase geschützt sind.

Das obere Bildschirmfoto zeigt die Situation, wenn kein GPG-Schlüssel gefunden im System wurde. Benutzen Sie in diesem Fall Anwendungen wie KGpg oder Kleopatra zur Erzeugung eines Schlüssels und versuchen Sie es erneut.

Wurde ein GPG-Schlüssel gefunden, dann können Sie im nächsten Dialog einen Schlüssel für Ihren neuen Passwortspeicher auswählen.

KWallet verwendet dann GPG beim Speichern und Öffnen eines Passwortspeichers. Der Passphrasen-Dialog erscheint nur einmal. Sogar wenn der Passwortspeicher nach dem anfänglichen Öffnen geschlossen wird, erfolgt das nachfolgende Öffnen ohne erneute Abfrage der Passphrase während derselben Sitzung.

In einer Sitzung können beide Dateiformate gleichzeitig benutzt werden. KWallet erkennt automatisch des Dateiformat und lädt das zugehörige Backend zur Verarbeitung.

Um Ihre sensiblen Daten aus einem klassischen Passwortspeicher mit dem neuen Backend zu benutzen, folgen Sie diesen Anweisungen:

- Erstellen Sie einen neuen Passwortspeicher mit GPG-Verschlüsselung
- Starten Sie KWallet Manager mit KRunner (**Alt-F2**) oder dem Anwendungsstarter bzw Anwendungsmenü, öffnen Sie Ihren alten Passwortspeicher und wählen dann **Datei** →

Verschlüsselt exportieren, um eine Archiv-Datei mit dem Inhalt des Passwortspeichers zu erzeugen.

- Öffnen Sie den neuen Passwortspeicher und wählen Sie dann mit **Datei** → **Verschlüsselt importieren** die vorher gespeicherte Datei.
- Gehen Sie in den Systemeinstellungen zur Seite **Benutzerkontodetails** → **Passwortverwaltung** und wählen Sie den neu erstellte GPG-basierten Passwortspeicher im Kombinationsfeld **Standardpasswortspeicher**.

Alternativ können Sie **Passwortspeicher importieren** benutzen, aber dann müssen sie die `.kwl`-Datei zu Ihrem alten Passwortspeicher auswählen, die sich im Ordner `kwalletd` in **`qtpaths --paths GenericDataLocation`** befindet.

> TIP
> Für sehr sicherheitsrelevante Aktionen sollten Sie einen Passwortspeicher für Passwörter im lokalen System und einen für Netzwerk-/Internet-Passwörter sowie Formulardaten benutzen. Standardmäßig werden allerdings alle Passwörter in einer einzigen Datei gehalten. Die Einstellungen hierzu können Sie im Systemeinstellungen-Modul von KWallet vornehmen. Als Voreinstellung wird alles in einem Passwortspeicher namens **kdewallet** gespeichert.

Ein Passwortspeicher ist per Voreinstellung geschlossen, das heißt, sie müssen ein Passwort angeben, um ihn zu öffnen. Sobald der Passwortspeicher geöffnet ist, kann jeder Benutzer den Inhalt lesen, dies kann ein Sicherheitsrisiko sein.

1.2 KWallet benutzen

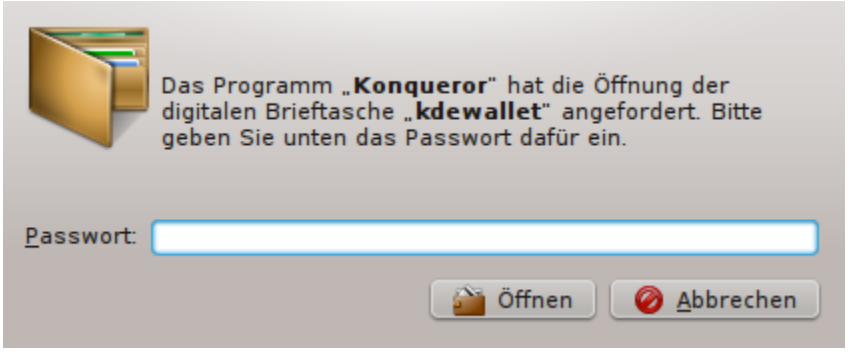
Wenn Sie z. B. zur Webseite des KDE-Fehlerverfolgungssystems gehen und das erste Mal die Anmeldedaten eingegeben haben, wird ein Dialog angezeigt, in dem die Speicherung des Passwortes in einem Passwortspeicher angeboten wird:

Möchten Sie diese Informationen speichern, dann drücken Sie den Knopf **Speichern**. Haben Sie bis dahin noch keinen Passwortspeicher erstellt, wird im nächsten Dialog nach der Verschlüsselungs-Methode gefragt und dann ein Passwortspeicher namens kdewallet erstellt.

Wenn Sie dieselbe Webseite das nächste Mal besuchen, fordert das Programm die Anmeldedaten vom Passwortspeicher an und füllt das Formular damit aus.

Ausgefüllte Anmeldedaten

Ist der Passwortspeicher geschlossen, fordert das Programm das Öffnen des Passwortspeichers an. Geben Sie das Passwort für den Passwortspeicher ein und drücken Sie den Knopf **Öffnen**.



Damit erhält das Programm Zugriff auf den Passwortspeicher, kann die Anmeldedaten darin lesen und sie in die Anmeldungsfelder dieser Webseite eintragen. Hat ein Programm erst einmal Zugriff auf den Passwortspeicher, kann es automatisch alle Anmeldeinformationen darin bei den zugehörigen Webseiten für Sie eintragen.

Kapitel 2

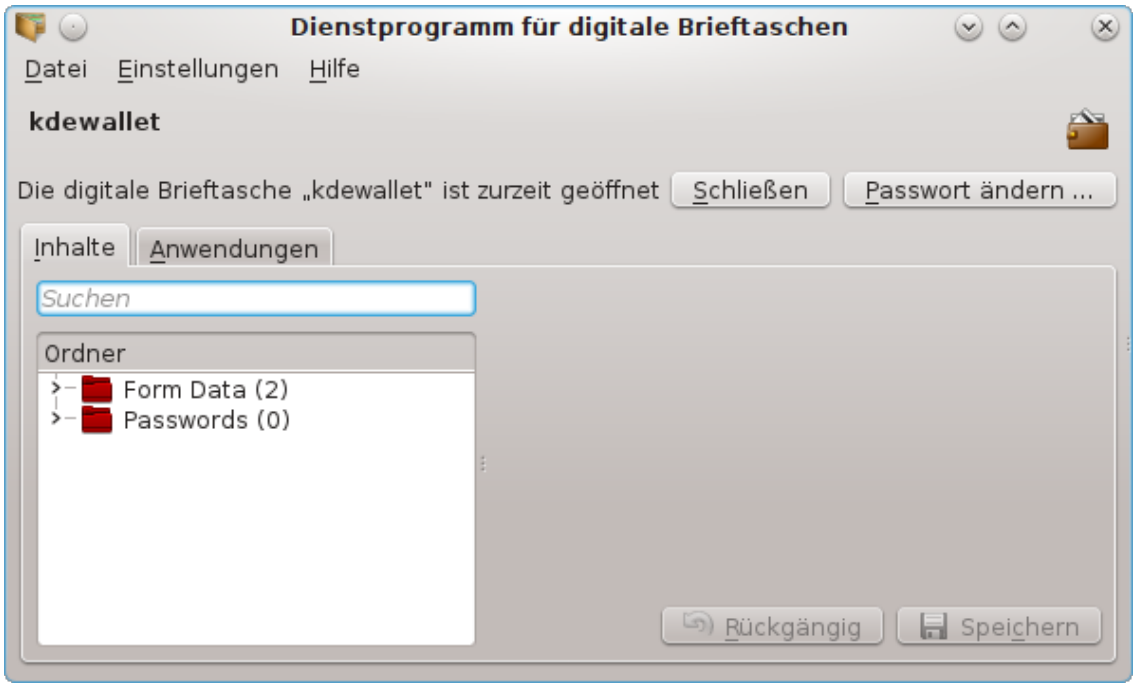
KWallet Manager

KWallet Manager erfüllt eine Reihe von Aufgaben. Zuerst erlaubt Ihnen KWallet Manager zu sehen, ob und welche Passwortspeicher offen sind und welche Anwendungen darauf zugreifen. Sie können den Zugriff einer Anwendung auf einen Passwortspeicher im KWallet Manager unterbinden.

Auch lassen sich hier die installierten Passwortspeicher verwalten und deren Inhalt ändern. Ebenso lassen sich neue Passwortspeicher hinzufügen oder bestehende Passwortspeicher löschen sowie deren Inhalt (Schlüssel ändern) bearbeiten.

Das Programm KWallet Manager wird mit **Programme** → **System** → **KWallet Manager (Passwortverwaltung)** aus dem Anwendungs-Starter aufgerufen. Alternativ starten Sie KRunner mit dem Kurzbefehl **Alt**+**F2** und geben dann den Befehl **kwalletmanager5** ein.

Klicken Sie auf das Brieftaschensymbol im Systemabschnitt der Kontrollleiste, um das KWallet Manager-Fenster zu öffnen.

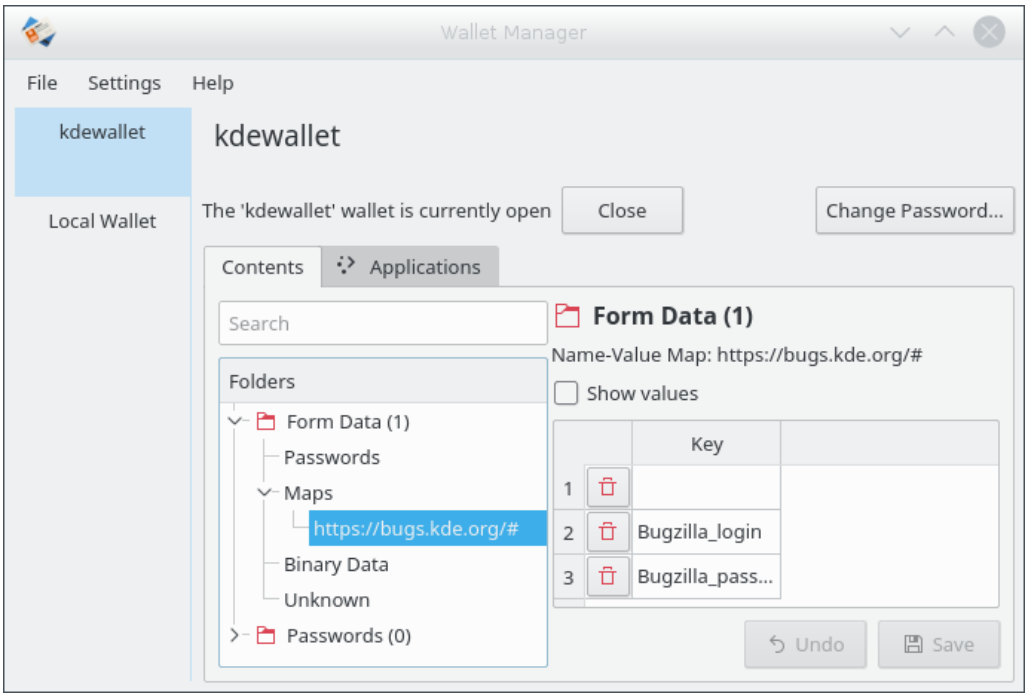


Hauptfenster mit einem Passwortspeicher

2.1 Das Fenster zum Passwortspeicher

Wenn Sie mehr als einen Passwortspeicher haben, werden alle verfügbaren Passwortspeicher links angezeigt.

Ein Klick auf einen Passwortspeicher im Fenster von KWallet Manager zeigt den Status und den Inhalt eines geöffneten Passwortspeicher. Ein Passwortspeicher kann beliebig viele Ordner enthalten, in denen Passwortdaten abgelegt werden können. Jeder Passwortspeicher enthält bereits die Ordner „Form Data” und „Passwords”.



Hauptfenster mit zwei Passwortspeichern

Benutzen Sie den Knöpf **Öffnen**, um den Inhalt eines geschlossenen Passwortspeichers anzuzeigen. Dazu müssen Sie das Hauptpasswort für den Passwortspeicher eingeben.

2.1.1 Karteikarte Inhalte

Auf der Karteikarte **Inhalte** gibt es drei Abschnitte:

- Eine Suchleiste zur Filterung der Einträge im Passwortspeicher
- Die im Passwortspeicher enthaltenen Ordner als Baumansicht. Klicken Sie auf die Symbole **>** / **v**, um die Baumansicht ein- oder auszuklappen.
- Den Inhalt des ausgewählten Ordnereintrags auf der rechten Seite. Als Standard sind Passwort und Wert ausgeblendet. Um sie anzuzeigen und zu bearbeiten, aktivieren Sie **Werte anzeigen** oder klicken Sie auf **Inhalt anzeigen**.

Ordner können mit dem Kontextmenü hinzugefügt oder gelöscht werden. Wird ein Ordner ausgewählt, so werden die Ordnereinträge und die Übersicht aktualisiert. Wird ein Ordnereintrag ausgewählt, so wird der Inhaltsbereich aktualisiert und die Einträge können geändert werden.

Einträge können auch über das Kontextmenü für die Ordnereinträge hinzugefügt, umbenannt oder gelöscht werden.

Alle Ordner und Einträge können auf andere Passwortspeicher respektive Ordner gezogen werden. Dies erlaubt es, einfach einen neuen Passwortspeicher anzulegen, die in einer anderen Umgebung verwendet werden kann. So kann zum Beispiel ein neuer Passwortspeicher angelegt und auf einen Wechselspeicher kopiert werden. So können wichtige Passwörter dorthin verschoben werden, sodass Sie sie überall zur Verfügung haben.

2.1.1.1 Importieren und Exportieren

Wenn Sie Ihre Passwörter auf ein anderes Gerät oder einen anderen Rechner übertragen möchten, benutzen Sie die Aktionen im Menü **Datei**. Mit **Verschlüsselt exportieren** können Passwortspeicher in eine verschlüsselte Archiv-Datei exportiert werden. Beim Importieren dieser Archiv-Datei mit **Verschlüsselt importieren** müssen Sie das Hauptpasswort des Passwortspeichers eingeben.

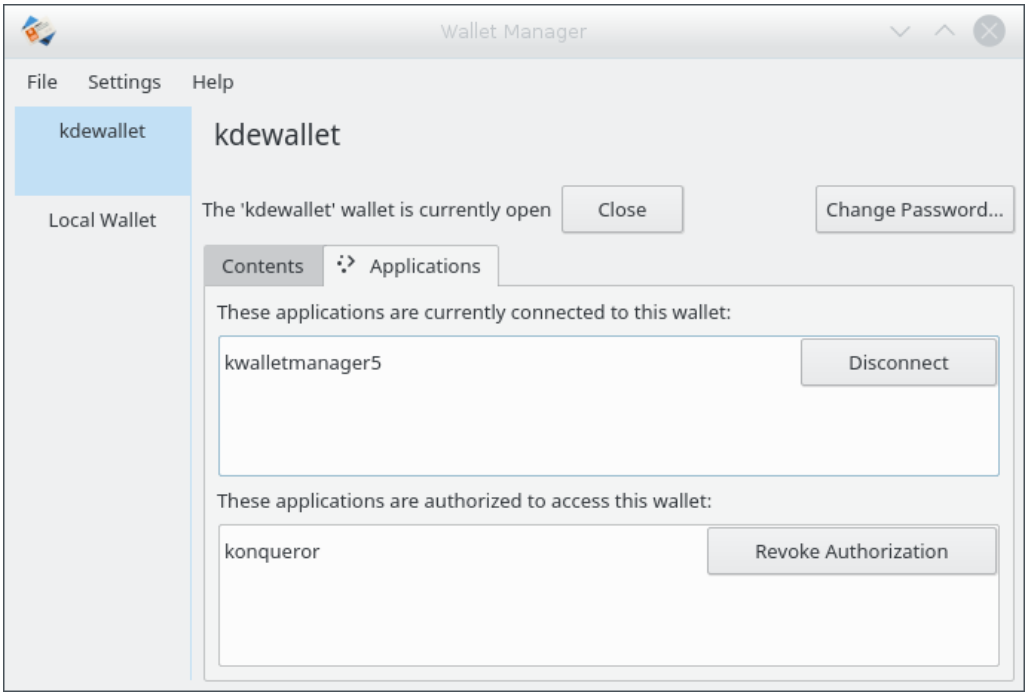
Als Alternative können Sie das Format `.xml` zum Übertragen des Inhalts eines Passwortspeicher verwenden. Bedenken Sie, dass alle Passwörter als lesbarer Text in diesem Format gespeichert werden.

2.1.1.2 Einträge manuell hinzufügen

Öffnen Sie das Kontextmenü mit der rechte Maustaste auf **Paare** in der **Ordner**-Baumansicht. Wählen Sie **Neu** und geben dann einen Namen für den neuen Eintrag ein.

Auf der Karteikarte Inhalte wählen Sie **Neuer Ordner** aus dem Kontextmenü der Einträge „Form Data” oder „Passwords”. Für Passwörter klicken Sie dann auf **Inhalte anzeigen** und geben das Passwort ein. Für Paare müssen Sie einen **Schlüssel** und einen **Wert** angeben. Klicken Sie auf den Knopf **Speichern**, um die neuen Einträge verschlüsselt in den Passwortspeicher einzufügen.

2.1.2 Karteikarte Anwendungen



Karteikarte Anwendungen

Die erste Liste zeigt alle Anwendungen, die gerade mit dem ausgewählten Passwortspeicher verbunden sind. Benutzen Sie den Knopf rechts neben jedem Eintrag, um die Verbindung der Anwendung zu trennen.

In der zweiten Liste werden alle Anwendungen angezeigt, deren Zugriff auf den Passwortspeicher autorisiert ist. Benutzen Sie den Knopf rechts neben jedem Eintrag in der Liste, um die Autorisierung zurückzuziehen.

Kapitel 3

KWallet einrichten

3.1 Einstellungen für den Passwortspeicher

KWallet besitzt einen Dialog mit diversen Einstellungen, der Ihnen die Anpassung von KWallet an Ihre Bedürfnisse erlaubt. Die Standardeinstellungen sollten allerdings für die meisten Benutzer genügen.

Markieren Sie das Ankreuzfeld, um das Passwortspeicher-Subsystem von KDE zu aktivieren. Ist dieses Feld nicht markiert, ist KWallet komplett deaktiviert und die anderen Einstellungen sind wirkungslos. KWallet speichert dann auch keine Informationen und bietet keine Hilfe beim Ausfüllen von Formularen an.

PASSWORTSPEICHER SCHLIESSEN

Bei Nichtgebrauch schließen nach:

Schließt den Passwortspeicher nach einem Zeitraum ohne Aktivitäten. Ist diese Einstellung markiert, können Sie den gewünschten Zeitraum im Drehfeld einstellen; Die Voreinstellung ist 10 Minuten. Wird ein Passwortspeicher geschlossen, benötigen Sie für einen erneuten Zugriff das Passwort.

Schließen, wenn der Bildschirmschoner aktiv wird

Schließt den Passwortspeicher, sobald der Bildschirmschoner aktiv wird. Wird ein Passwortspeicher geschlossen, benötigen Sie für einen erneuten Zugriff das Passwort.

Schließen, sobald keine Anwendung mehr darauf zugreift

Schließt den Passwortspeicher, sobald keine Anwendung mehr darauf zugreift. Beachten Sie, dass der Passwortspeicher erst dann geschlossen wird, wenn alle Anwendungen, die darauf zugreifen die Verbindung gelöst haben. Wird ein Passwortspeicher geschlossen, benötigen Sie für einen erneuten Zugriff das Passwort.

AUTOMATISCHE WAHL DES PASSWORTSPEICHERS

Standardpasswortspeicher:

Wählen Sie aus, welchen Passwortspeicher Sie als Voreinstellung verwenden möchten. Beachten Sie , dass nur der Passwortspeicher mit dem Namen **kdewallet** automatisch bei der Anmeldung geöffnet wird, wenn das Passwort für den Passwortspeicher und die Anmeldung identisch sind.

Anderen Passwortspeicher für lokale Passwörter:

Ist diese Einstellung markiert, wird für lokale Passwörter ein anderer Passwortspeicher verwendet.

PASSWORTVERWALTUNG

Passwortverwaltung im Systembereich anzeigen

Aktiviert die Anzeige eines Symbols für die Passwortverwaltung im Systemabschnitt der Kontrollleiste.

Kontrollleistensymbol ausblenden, wenn der letzte Passwortspeicher geschlossen ist

Ist kein Passwortspeicher mehr in Benutzung, wird das Symbol aus dem Systemabschnitt entfernt.

Zuletzt gibt es auch noch den Knopf **Passwortverwaltung starten**, um diesen Dienst zu aktivieren.

Dieser Knopf wird nur dann angezeigt, wenn KWallet Manager nicht ausgeführt wird.

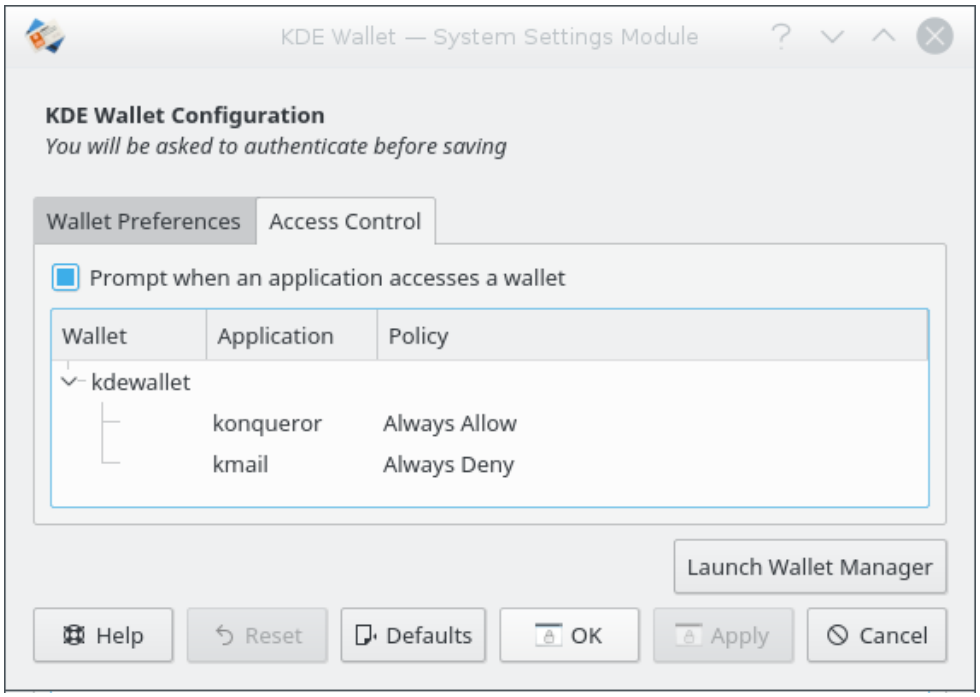
3.2 Zugriffsüberwachung

Auf dieser Seite gibt es nur eine Einstellung:

Nachfragen, wenn eine Anwendung auf einen Passwortspeicher zugreifen will.

Nachfragen, wenn eine Anwendung auf einen geöffneten Passwortspeicher zugreifen will..

Darunter befindet sich eine Baumansicht mit den Zugriffsdaten und Regeln für den Passwortspeicher.

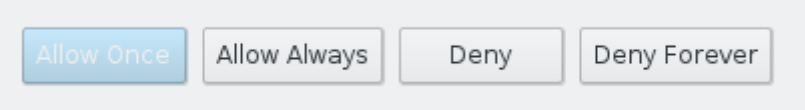


Klicken Sie mit der linken Maustaste auf das kleine >-Symbol neben den Namen eines Passwortspeichers, um den Baum zu öffnen. Sie sehen dann den Namen jeder Anwendung, die Zugriff auf den Passwortspeicher hat und die Richtlinien, die sie dafür festgelegt haben. Sie können keine Richtlinien ändern oder hinzufügen, einzig löschen können Sie einen Eintrag, wenn Sie mit der rechten Maustaste das Kontextmenü öffnen und darin **Löschen** wählen oder die Taste **Entf** drücken.

Ein Programm, das den Passwortspeicher öffnen darf, kann auch alle darin enthaltenen Passwörter lesen.

Wenn Sie versehentlich eine Anwendung so eingerichtet haben,KWallet nicht zu benutzen, löschen Sie die Regelung für diese Anwendung hier.

Beim nächsten Start dieser Anwendung können Sie dann eine neue Regelung für den Zugriff auf den Passwortspeicher festlegen.



Anforderung einer Anwendung zum Zugriff auf einen Passwortspeicher.

Kapitel 4

Weitergehende Funktionen

Ein Passwortspeicher kann aus dem KWallet Manager-Fenster auf ein Dateiverwaltungs-Fenster gezogen werden, um dort eine Kopie oder eine Verknüpfung anzulegen oder sie dorthin zu verschieben.

Verwenden Sie diese Möglichkeit, wenn Sie einen Passwortspeicher auf ein Wechselmedium wie einen USB-Stick kopieren wollen. So haben Sie Ihre Passwörter immer dabei, zu Hause, bei der Arbeit oder in den Ferien.

Kapitel 5

Danksagungen und Lizenz

Übersetzung Gregor Zumstein gz@orchester-bremgarten.ch