

Anleitung zur Einrichtung der Zwei-Faktor Authentifizierung für Linux Desktop-Betriebssysteme

I. Technisches Verständnis

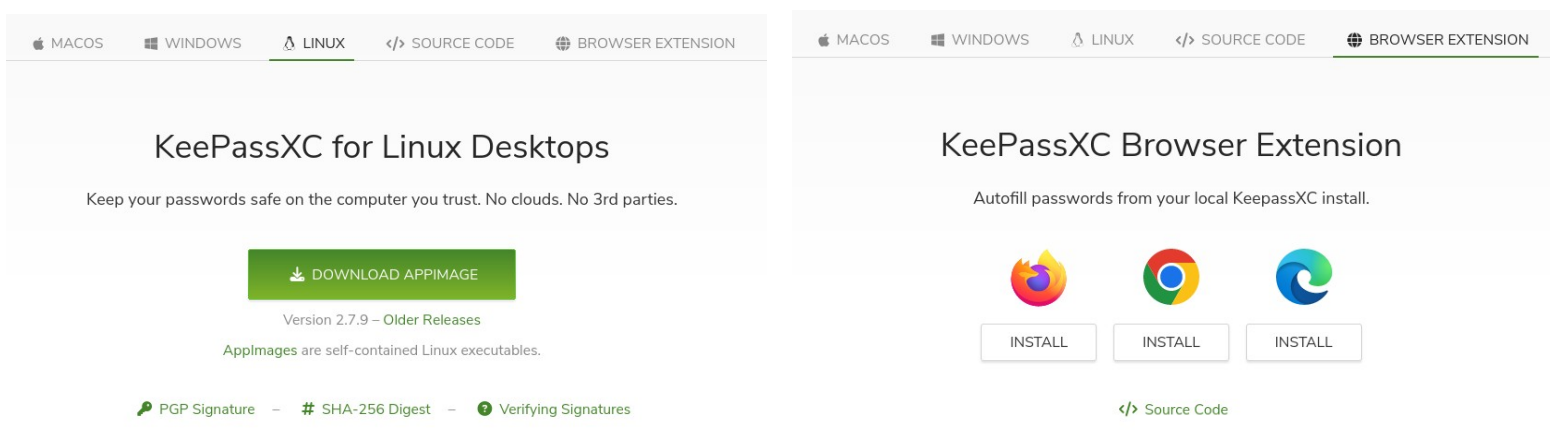
Bei einer [2-Faktor-Authentifizierung](#) tritt ein weiterer Sicherheitsfaktor neben das Benutzerpasswort. Dies kann eine Transaktionsnummer (TAN) sein, wie z.B. die Ihnen von der Universität Hamburg per E-Mail zugesandte Liste von 2FA-Codes, oder ein von einer Authenticator-App wie „*Google Authenticator*“ erstelltes „[Time-based One-Time Passwords](#)“ (TOTP), wie es z.B. die Datenbank [beck-online.beck.de](#) erfordert.

Die Universität Hamburg verwendet als zweiten Faktor ein Verfahren, das auf dem von der [FIDO-Allianz](#) entwickelten [FIDO2-Standard](#) basiert. Bei dem von der Universität Hamburg zur Authentifizierung verwendeten Verfahrens mittels eines „*Passkeys*“ handelt es sich nicht um ein „echtes“ hardwarebasiertes Sicherheitstoken, sondern um einen duplizierbaren Geheimschlüssel, der lokal auf dem Smartphone oder Computer der Nutzerinnen und Nutzer gespeichert wird.

Passkeys sind grundsätzlich geeignet, [Passwörter vollständig zu ersetzen](#). Die Universität Hamburg setzt diese derzeit jedoch nur als zweiten Faktor ein, ergänzend zum Benutzerpasswort, um die Sicherheit der Authentifizierung zu erhöhen.

Die Verwendung von Passkeys unter Linux erfolgt mittels eines [Passwort-Managers](#), der eine sichere Speicherung und Nutzung dieser Schlüssel ermöglicht.

Im Folgenden wird die Einrichtung am Beispiel des kostenlosen Open-Source-Passwort-Managers „[KeePassXC](#)“ und der Linux-Distribution Linux Debian 12 erklärt.



The image shows two side-by-side screenshots of the KeePassXC website. The left screenshot is titled "KeePassXC for Linux Desktops" and features a green "DOWNLOAD APPIMAGE" button. Below the button, it states "Version 2.7.9 - Older Releases" and "AppImages are self-contained Linux executables." At the bottom, there are links for "PGP Signature", "SHA-256 Digest", and "Verifying Signatures". The right screenshot is titled "KeePassXC Browser Extension" and features three "INSTALL" buttons for Firefox, Chrome, and Edge. Below these buttons is a "Source Code" link.

*Hinweis: Manche Linux-Distributionen bieten über ihre Paketmanager noch nicht die neueste Version von KeePassXC an. Sie müssen **mindestens KeePassXC Version 2.7.7** verwenden, [da erst ab dieser Version Passkeys unterstützt werden](#). Mit dem AppImage können Sie die neuste Version von KeePassXC auf den meisten Linux Desktop-Distributionen nutzen.*

II. Einrichtung unter Linux

Schritt 1: Laden Sie das Programm KeePassXC als [AppImage](#) herunter ([LINK](#)).

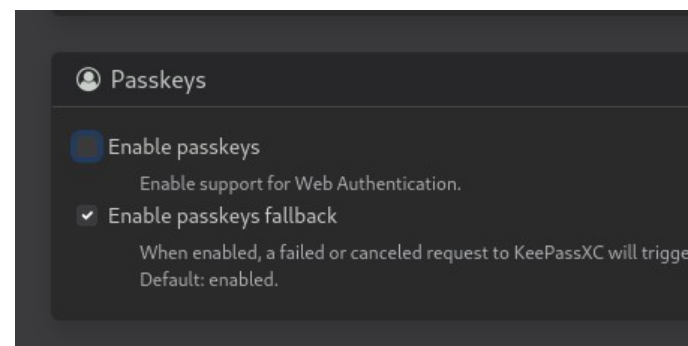
Schritt 2: Verschieben Sie das AppImage an [einen beliebigen Ort](#) auf Ihrem Computer. Machen Sie es ausführbar (z.B. mittels Rechtsklicks auf das AppImage, indem Sie unter „*Eigenschaften*“ den Haken bei „*Ausführbar als Programm*“ setzen).

Schritt 3: Legen Sie eine verschlüsselte Passwortdatenbank an. Folgen Sie dazu der [offiziellen KeePassXC-Dokumentation](#).

Schritt 4: Installieren Sie anschließend die Browser-Erweiterung von KeePassXC ([LINK](#)).

Schritt 5: Verknüpfen Sie die Browser-Erweiterung und KeePassXC entsprechend der [offiziellen KeePassXC-Dokumentation](#).

Schritt 6: Setzen Sie in den Einstellungen der KeePassXC-Browser-Erweiterungen unter „Passkeys“ einen Haken bei „Enable Passkeys“.



Sie haben nun Ihren Passwortmanager eingerichtet und können beginnen ihn zu nutzen.

III. Hinzufügen des Passkeys der Universität Hamburg

Um einen Passkey hinzuzufügen, folgen Sie erneut der [offiziellen KeePassXC-Dokumentation](#).

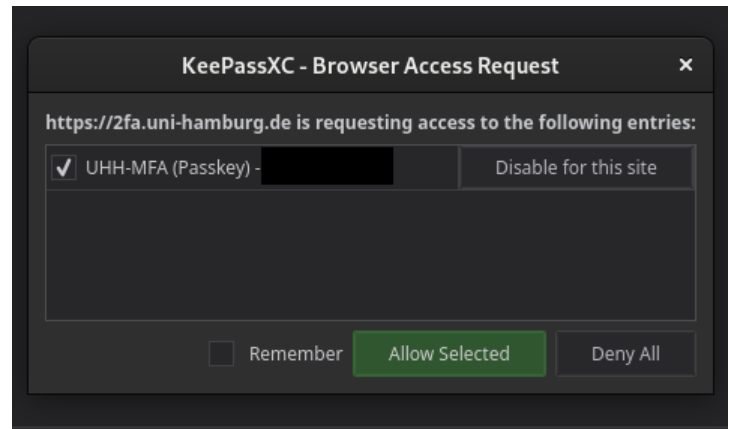
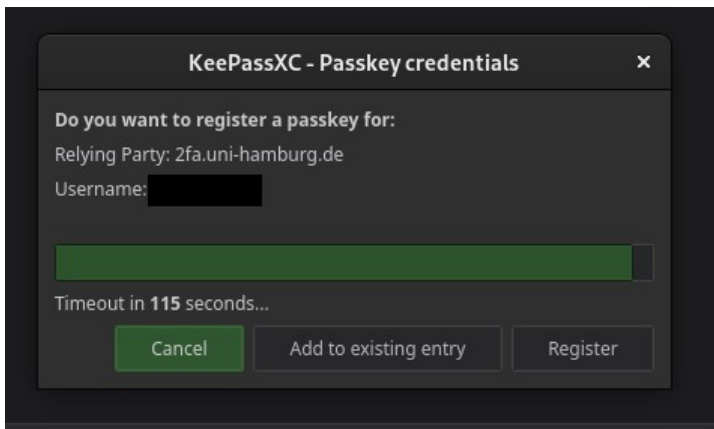
Schritt 1: Entsperren Sie Ihre KeePassXC-Passwort-Datenbank und lassen Sie diese im Hintergrund geöffnet.

Schritt 2: Rufen Sie die [URL der Universität zur Einrichtung der 2FA](#) auf.

Schritt 3: Melden Sie sich mit Ihrer Benutzerkennung und Ihrem Passwort an und authentifizieren Sie sich mittels einer beliebigen Methode, etwa mittels der Ihnen per E-Mail zugesandten 2FA-Codes.

Schritt 4: Klicken Sie anschließend auf „*Gerät Einrichten*“. Auf die Frage: „*Welches Gerät möchten Sie registrieren?*“ wählen Sie „*Dieses Gerät*“. Klicken Sie auf „*Mit Registrierung fortfahren*“. Anschließend klicken Sie auf „*Ich habe mein Gerät vorbereitet*“.

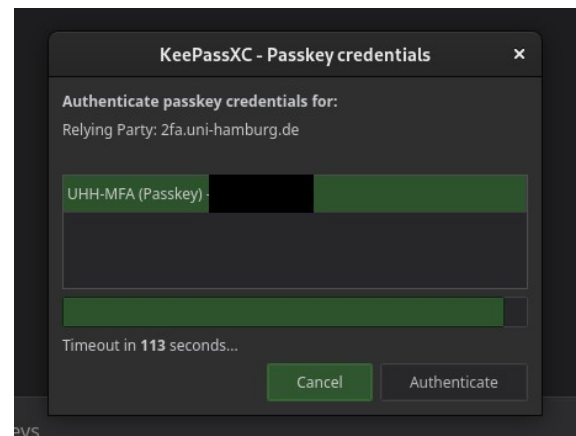
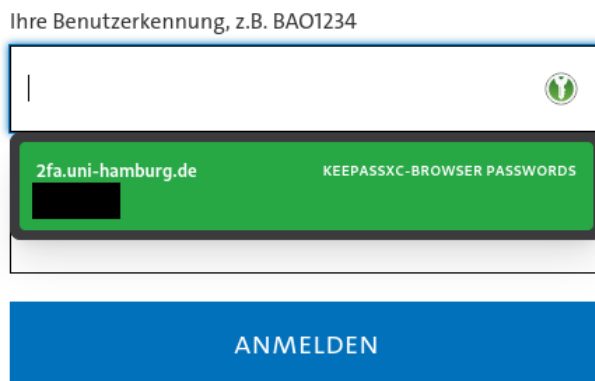
Schritt 5: Vergeben Sie einen Namen für das Gerät, z.B. „*MeinLinuxPC*“. Anschließend öffnet sich KeePassXC automatisch und Sie können dort den Passkey zu Ihrer Passwort-Datenbank hinzufügen.



Wenn Sie Ihren Passkey erfolgreich hinzugefügt haben, sehen Sie einen entsprechenden Eintrag in Ihrer Passwortdatenbank.

IV. Anmeldung mittels Passkeys

Um den Passkey zur Anmeldung zu verwenden, entsperren Sie Ihre zunächst Ihre Passwort-Datenbank. Melden Sie sich dann wie gewohnt auf der Internetseite der Universität mit Benutzerkennung und Passwort an (optional können Sie diese Anmeldedaten ebenfalls in Ihrer Passwort-Datenbank hinterlegen). Klicken Sie anschließend in dem sich automatisch öffnenden Fenster auf „Authenticate“:



Nach der Bestätigung wird Ihr Passkey zur Authentifizierung verwendet.

Sie können auch unter macOS und Windows KeePassXC einrichten und anstelle von „iCloud Keychain“ und „Windows Hello“ nutzen.

Viel Erfolg!