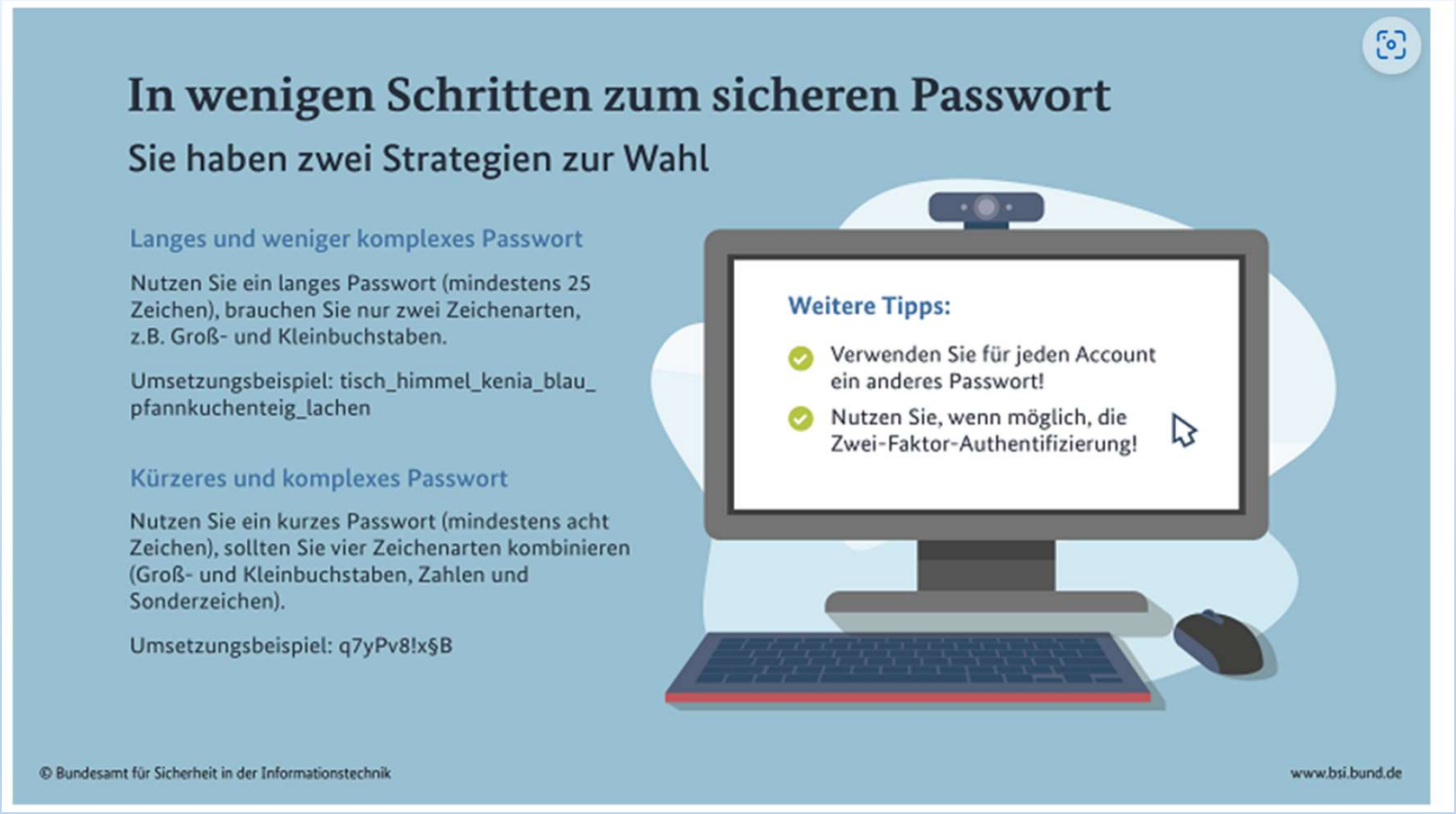
Passwort-Manager, Passkey, .pdf

Bilder vom BSI und von Wikipedia

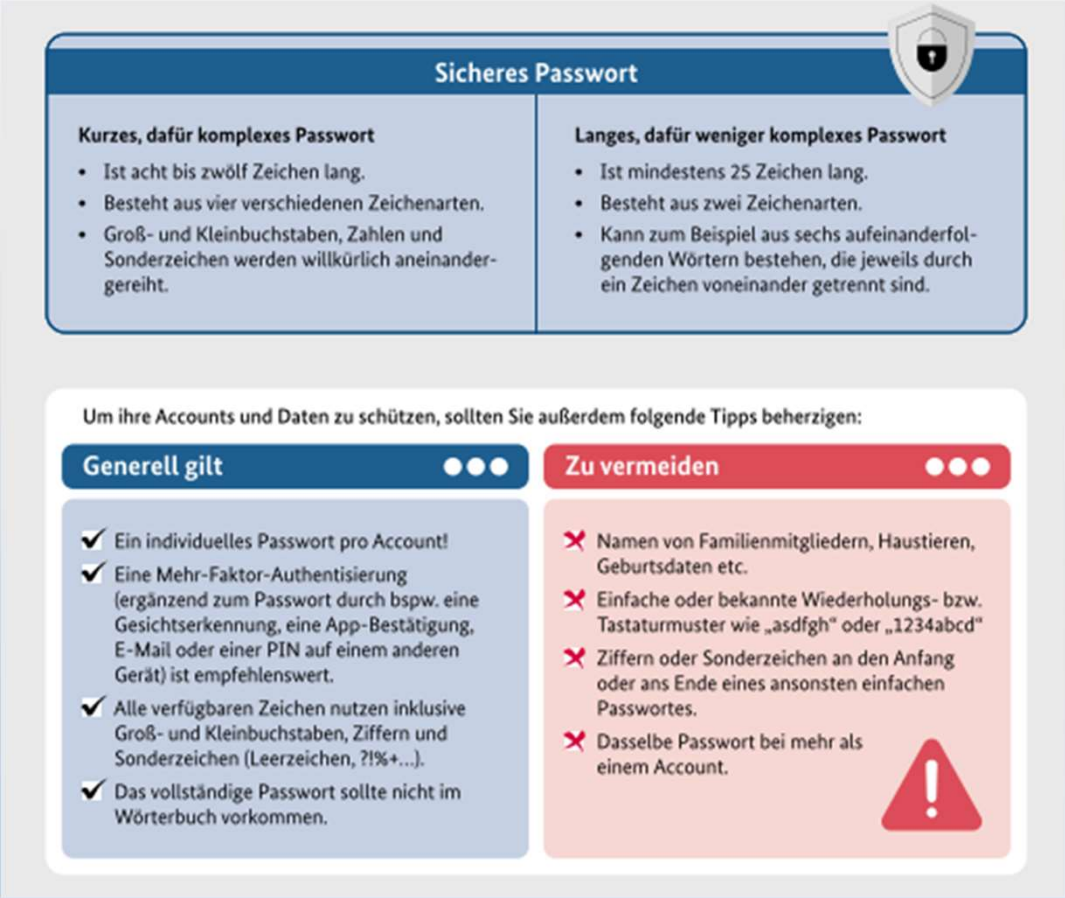
Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf



Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf



Sicheres Passwort

Kurzes, dafür komplexes Passwort

- Ist acht bis zwölf Zeichen lang.
- Besteht aus vier verschiedenen Zeichenarten.
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen werden willkürlich aneinandergereiht.

Langes, dafür weniger komplexes Passwort

- Ist mindestens 25 Zeichen lang.
- Besteht aus zwei Zeichenarten.
- Kann zum Beispiel aus sechs aufeinanderfolgenden Wörtern bestehen, die jeweils durch ein Zeichen voneinander getrennt sind.

Um ihre Accounts und Daten zu schützen, sollten Sie außerdem folgende Tipps beherzigen:

Generell gilt

- ✓ Ein individuelles Passwort pro Account!
- ✓ Eine Mehr-Faktor-Authentisierung (ergänzend zum Passwort durch bspw. eine Gesichtserkennung, eine App-Bestätigung, E-Mail oder einer PIN auf einem anderen Gerät) ist empfehlenswert.
- ✓ Alle verfügbaren Zeichen nutzen inklusive Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...).
- ✓ Das vollständige Passwort sollte nicht im Wörterbuch vorkommen.

Zu vermeiden

- ✗ Namen von Familienmitgliedern, Haustieren, Geburtsdaten etc.
- ✗ Einfache oder bekannte Wiederholungs- bzw. Tastaturmuster wie „asdfgh“ oder „1234abcd“
- ✗ Ziffern oder Sonderzeichen an den Anfang oder ans Ende eines ansonsten einfachen Passwortes.
- ✗ Dasselbe Passwort bei mehr als einem Account.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=4#download=1

Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf

Passwortsafes sind ein Hilfsmittel um sich komplexe Passwörter zu merken.

Eine Liste auf einem Blatt Papier, von dem man weiß wo es ist und aufpasst, dass sie nicht von unerwünschten Lesern gefunden werden kann, ist auch ein Passwortsafe.

Das sollte nicht unverschlüsselt als Datei auf einem Speichermedium aufbewahrt werden. Es sei denn, man wendet dieselben Sicherheitsmaßnahmen wie bei dem Blatt Papier an.

Das sichere Passwort-Merkblatt

****

Alle Accounts im Blick

Diese Methode erleichtert Ihnen die Passwortverwaltung im Alltag! Anstelle von vielen verschiedenen Passwörtern müssen Sie sich nur noch ein Passwort merken. Denn: Bei diesem Ansatz besteht jedes Passwort aus zwei Teilen. Der erste Teil ist für jedes Passwort identisch. Diesen Teil müssen Sie sich merken. Der zweite Teil des jeweiligen Passworts ist für jeden Ihrer Accounts unterschiedlich. Diesen tragen Sie in die Liste ein. Gelangen Dritte an das Passwort-Merkblatt, kennen sie nur den zweiten Teil des Passworts, nicht aber den ersten. Damit ist das Merkblatt für jede Person außer Sie selbst unbrauchbar und Ihre Accounts sind sicher. Für beide Teile gilt: **Beachten Sie die Regeln zu Erstellung eines sicheren Passworts**!

1. Teil des Passworts merken

- Für jeden Account gleich
- Ohne persönlichen Bezug
- Mindestens acht Zeichen lang
- Besteht bspw. aus zwei ausgedachten, aneinander gereihten Wörtern (tisch-himmel)

2. Teil des Passworts in Liste eintragen

- Für jeden Account anders
- Entweder kurz und komplex oder besonders lang
- Besteht bspw. aus willkürlich aneinander gereihten Zeichen oder aus vier Wörtern, die durch Sonderzeichen getrennt sind (Berg_spät_hüpfen_Kühlschrank)

Sichere Passwörter für jeden Account

(tisch-himmelBerg_spät_hüpfen_Kühlschrank)

Account	Nutzername/ E-Mail-Adresse	2. Teil des Passworts
1. Musteraccount	maxine@musterfrau.de	Berg_spät_hüpfen_Kühlschrank
2. Musteraccount	maxine@musterfrau.de	q74Pv8!x§B2

Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf

Passwort Manager sind ein technisches Hilfsmittel um Passörter zu speichern, können aber noch mehr.

Checkliste für die Auswahl eines Passwort-Managers:

- Von E-Mail bis Social Media: Für welche Konten brauchen Sie einen Passwort-Manager?
- Browser-basiert oder eigenständig: Welches Programm passt am besten zu Ihren Online-Gewohnheiten?
- › Cloud oder Festplatte: Wo werden Ihre Daten gesichert?
- Sensible Daten: Benötigen Sie einen › zweiten Faktor zur Authentisierung?
- Komplexe Kombinationen: Haben Sie ein sicheres Masterpasswort?

Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf

Vorteile eines Passwort-Managers

- **Verwahren von Passwörtern** und Benutzernamen mittels Verschlüsselung
- **Unterstützung bei der Passwortvergabe,** z. B. durch die Generierung starker Kombinationen und Kennzeichnung schon verwendeter oder schwacher Begriffe.
- **Warnung vor gefährdeten Websites und möglichen Phishing-Attacken**, z. B. wenn sich die URL der aufgerufenen Webseite von der gespeicherten unterscheidet.
- **Synchronisieren möglich:** Wer Online-Dienste auf mehreren Geräten wie Computer und Smartphone mit unterschiedlichen Betriebssystemen nutzen möchte, kann ein Programm verwenden, das diese synchronisiert.

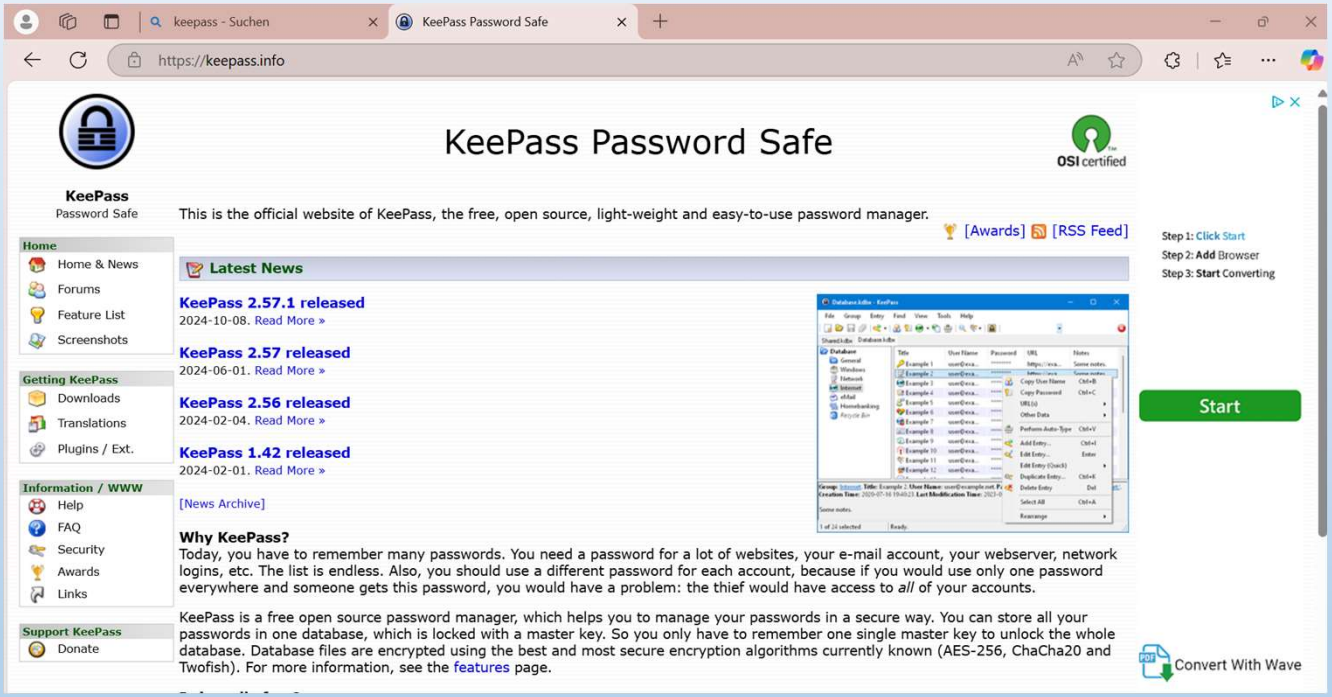
Passwort-Manager, Passkey, .pdf

Nachteile des Passwort-Managers

- Beim Vergessen des Masterpassworts sind im schlechtesten Fall alle Daten verloren. Das bedeutet oftmals viel Arbeit, da die einzelnen Zugänge zu den Konten individuell wiederhergestellt werden müssen.
- Alle Passwörter können auf einmal gestohlen werden, sollte ein Cyber-Angriff auf einen Passwort-Manager erfolgreich sein.
- Bei cloudbasierten Diensten vertrauen Sie den Zugang zu all Ihren sensiblen Daten in der Regel einem Unternehmen an. Hier lohnt sich ein Blick in die AGB und Datenschutzerklärungen des jeweiligen Herstellers. Die Informationen über den Standort des Cloud-Dienste-Anbieters und der Server geben Auskunft darüber, welchem Datenschutzrecht die Daten unterliegen.

Passwort-Manager, Passkey, .pdf

Ich verwende KeePass



Die Homepage
https://www.keepass.info
Sieht nicht so schick aus, ist aber funktionell.

Sie ist nicht werbefrei, also Vorsicht wohin man klickt.

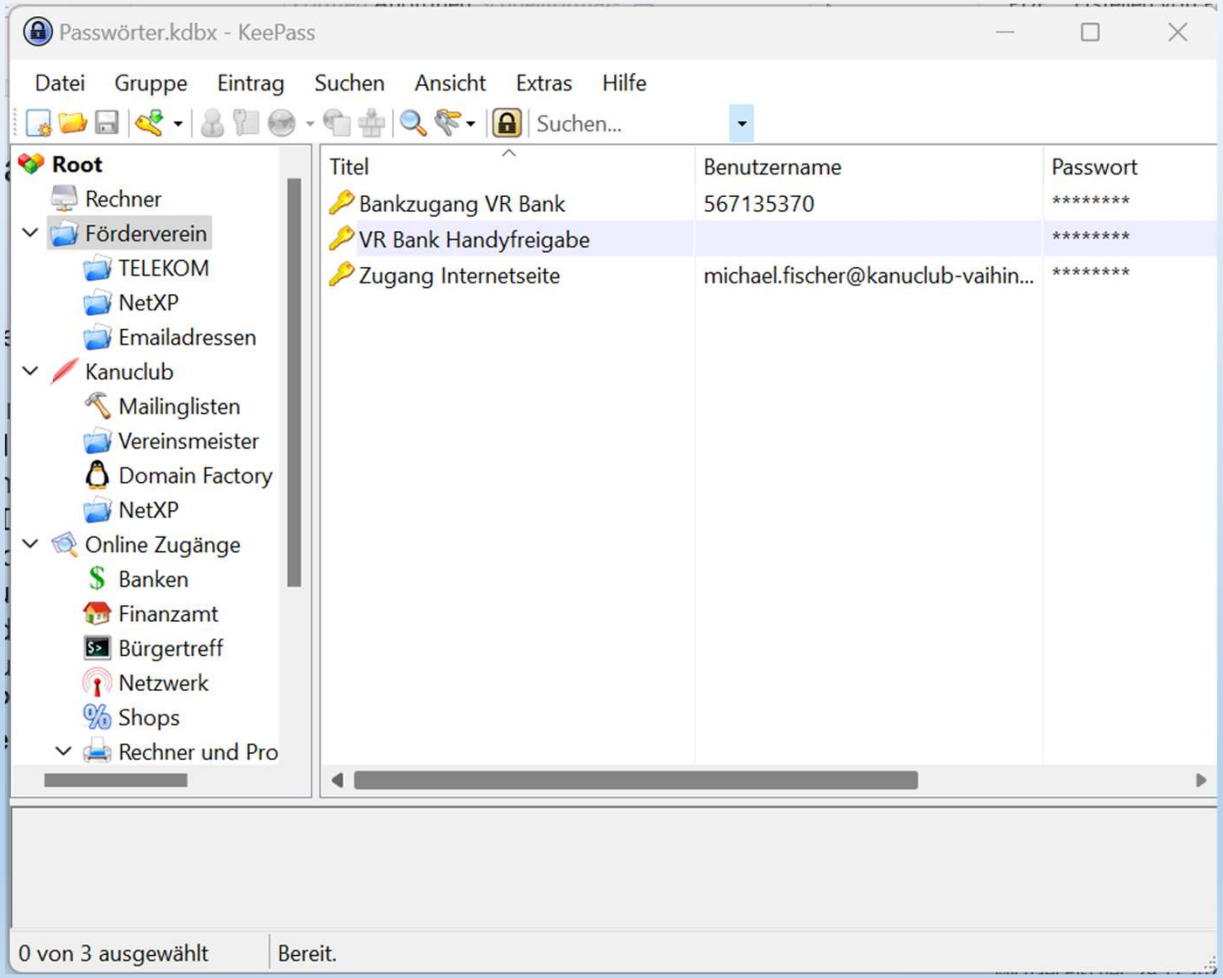
Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf

Meine Entscheidungskriterien für KeePass:

- Das Programm wird auf dem Rechner installiert, ich habe es in der Hand, auf welchen Rechnern ich es installieren möchte.
- Die Datenbank kann ich installieren wo ich möchte, Heimnetz, Rechner, Internet.
- Ich habe die Datenbank bei mir im Heimnetz und kann sie daher mit mehreren Rechnern nutzen.
- Es stehen Browserintegrationen für die gängigen Browser zur Verfügung.
- Die Passwörter werden automatisch nach einigen Sekunden aus der Zwischenablage des Rechners gelöscht, leider nicht bei der Handyversion.
- KeePass ist unter GNU Lizenz, d.h. für Privatanwendungen kostenlos, die Software ist open source also der Programmcode frei im Internet zugänglich.
- Es gibt ein positives Code Review vom BSI für KeePass.

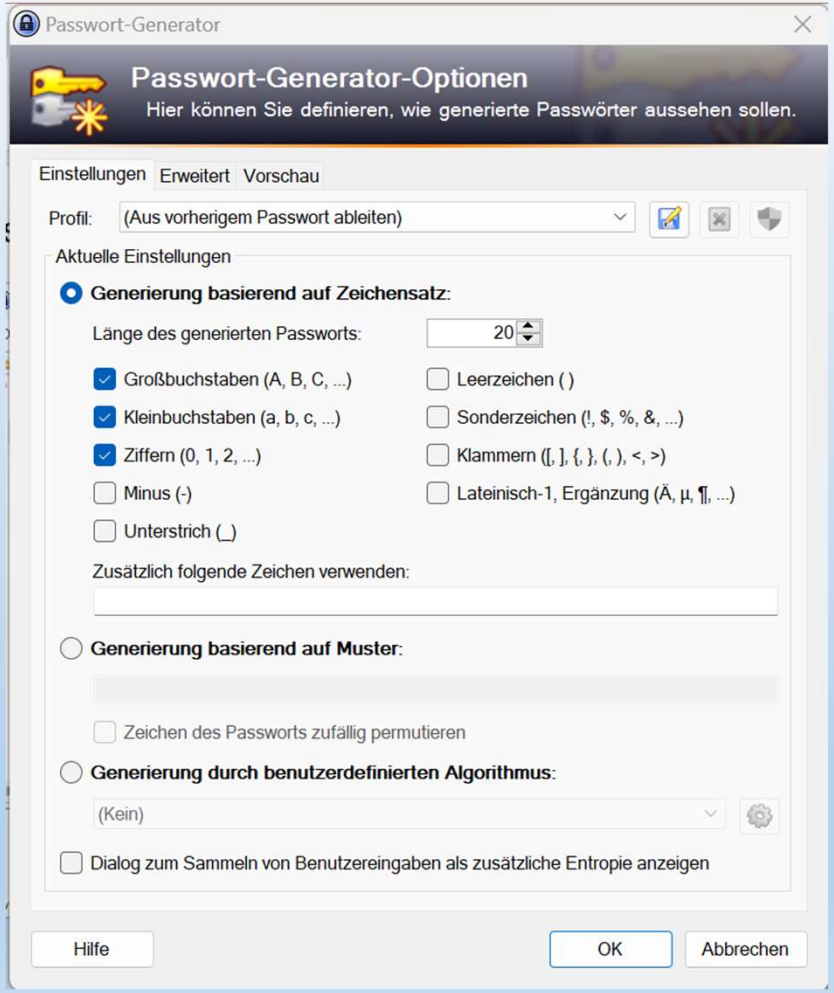
Passwort-Manager, Passkey, .pdf



So sieht die Oberfläche nach der Integration der deutschen Sprachdatei aus.

Man kann seine Passwörter gruppieren, und mit einer eingebauten Suche wiederfinden.

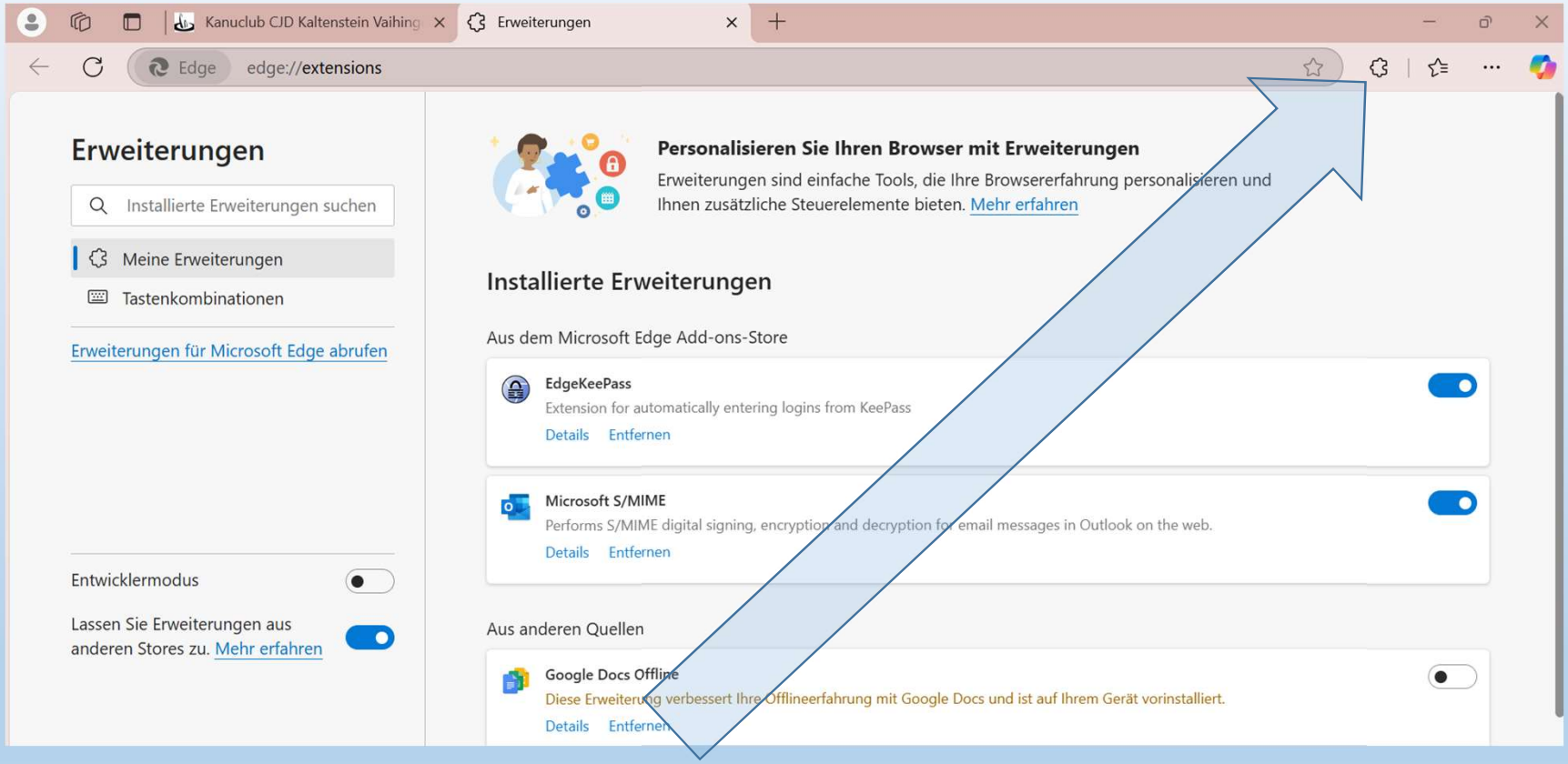
Passwort-Manager, Passkey, .pdf



Das ist der eingebaute Passwortgenerator.
Der lässt sich sehr flexibel parametrieren.

Michael Fischer, 29.11.2024

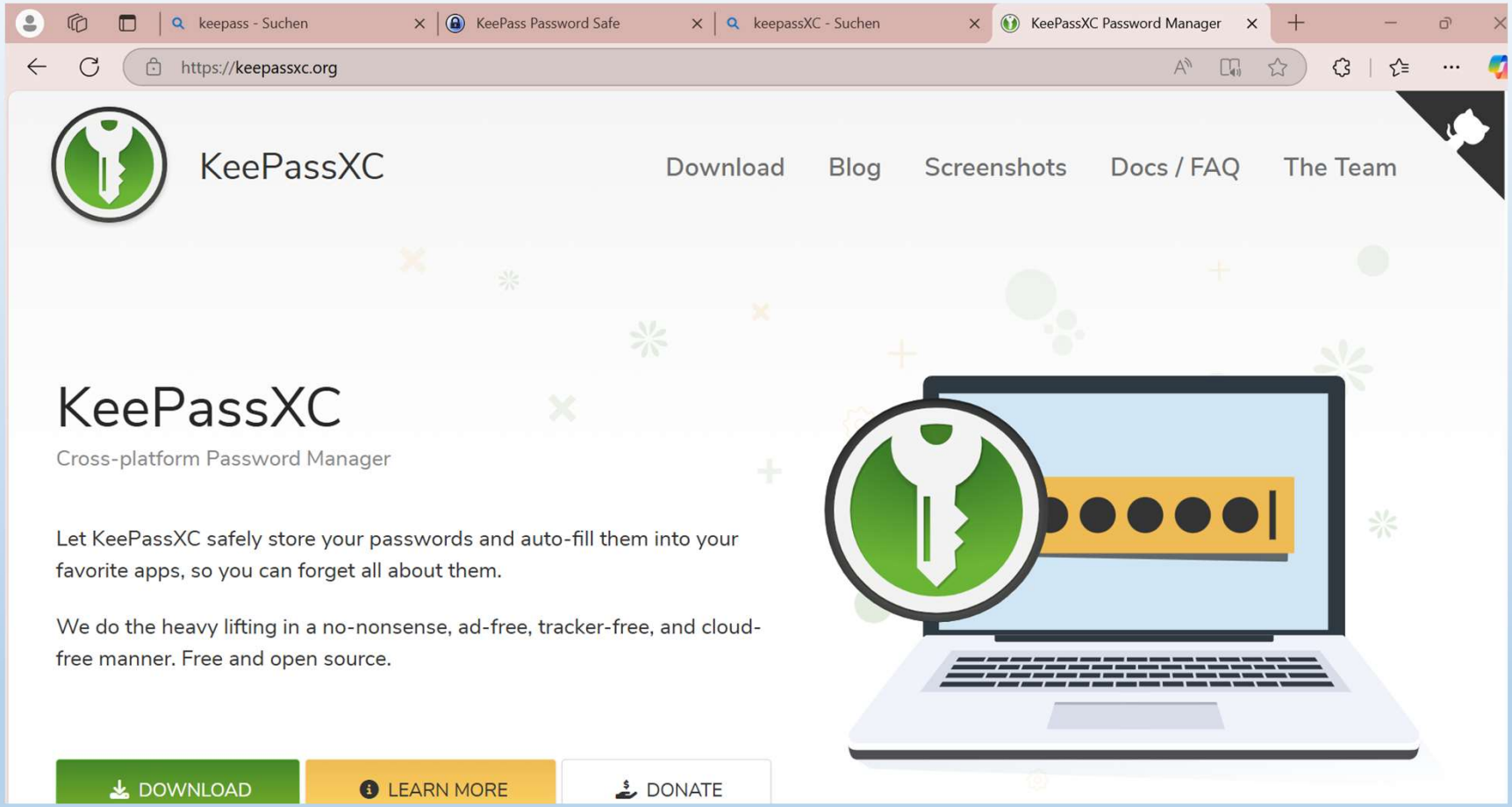
Passwort-Manager, Passkey, .pdf



Für die gängigen Browser stehen Erweiterungen zur Verfügung
um Passwörter aus KeePass direkt zu übertragen.
Bequemlichkeit und Sicherheit sind unterschiedliche Ziele.

Michael Fischer, 29.11.2024

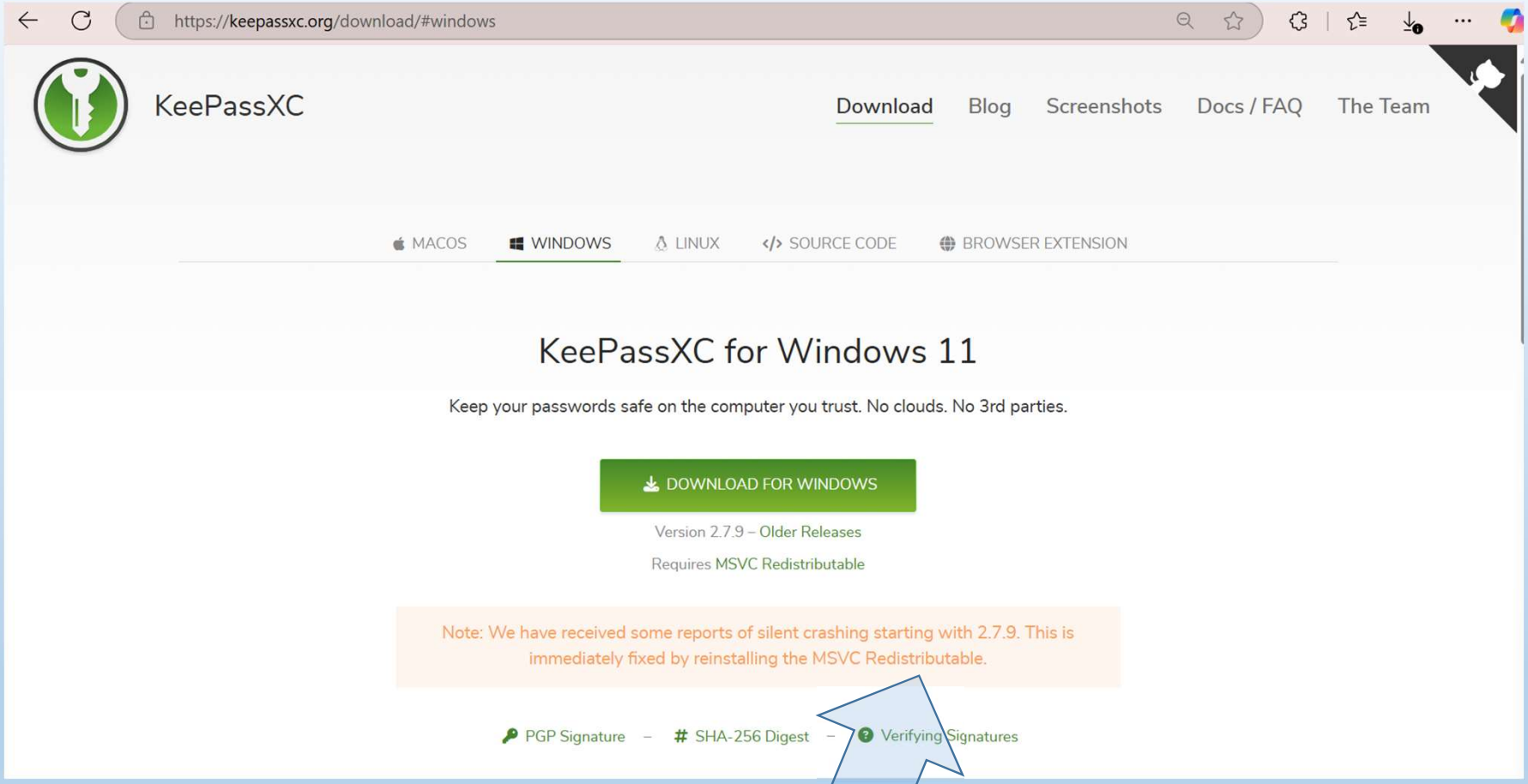
Passwort-Manager, Passkey, .pdf



Es gibt auch eine schicke deutsche Version von KeePass die heißt KeePassXC

Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf



Sie verwendet die neuesten C und C++ Bibliotheken, die müssen vor der Installation bei den meisten Systemen installiert oder upgedatet werden.

Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf

Passkey der neue Stern am Einloghimmel:

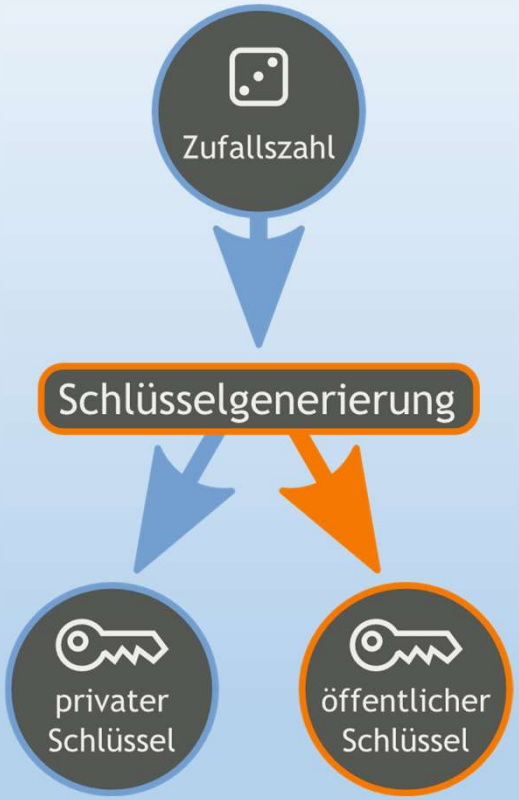
Passkey ist eine Erweiterung des FIDO2 Protokolls.

FIDO steht für **F**ast **ID**entity **O**nline

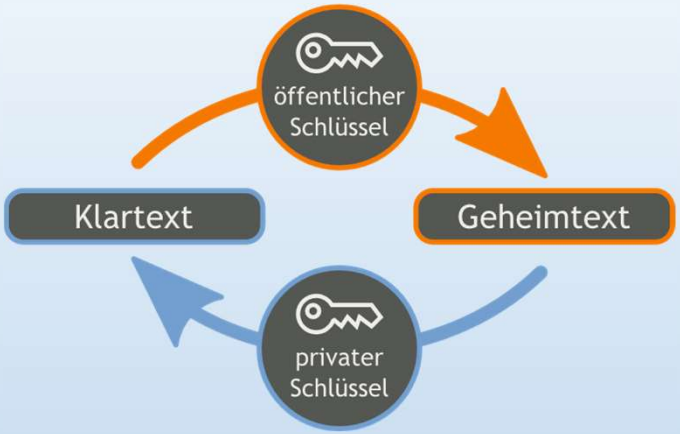
FIDO ist eine kryptographische Methode zur Identifizierung eines Benutzers im Internet

Passkey ist eine reine Software Realisierung des FIDO Projekts und kommt daher ohne spezielle Hardwarekomponenten wie USB Sticks oder eingebaute Sicherheits-Chips aus.

Passwort-Manager, Passkey, .pdf

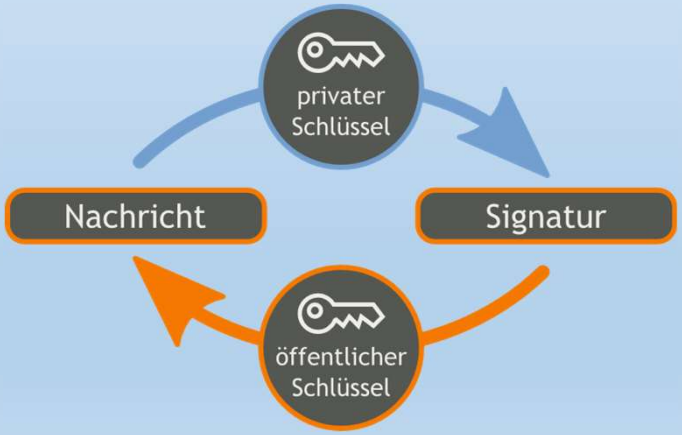


Erzeugung eines Schlüsselpaars:
Blaue Bildelemente sind geheim,
orange sind öffentlich



Verschlüsselung mit öffentlichem Schlüssel und Entschlüsselung mit privatem Schlüssel

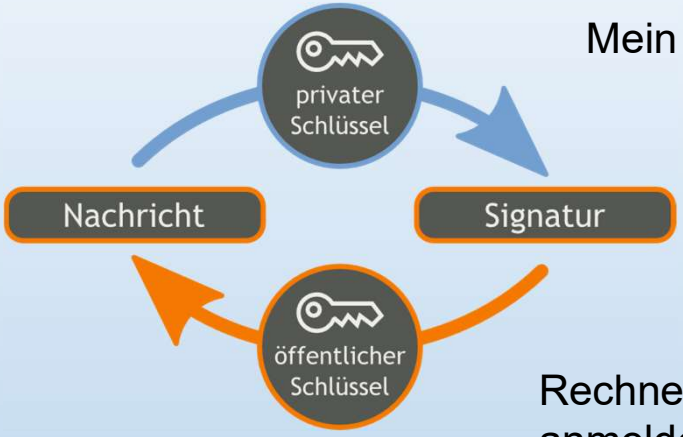
Signieren mit privatem Schlüssel und Verifikation mit öffentlichem Schlüssel



Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf

Signieren mit privatem Schlüssel und
Verifikation mit öffentlichem Schlüssel



Mein Rechner

Rechner bei dem ich mich anmelden will

Vereinfachte Darstellung:
Der Rechner bei dem ich mich anmelden will schickt mir eine Nachricht. Die kann jeder lesen.

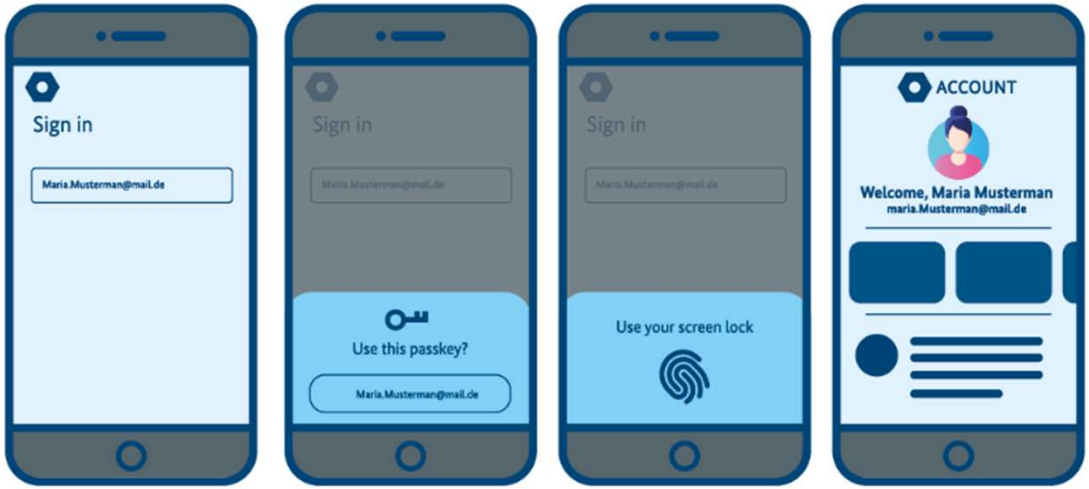
Mein Rechner verschlüsselt die Nachricht mit dem geheimen Schlüssel und schickt die Nachricht zurück.

Der Rechner bei dem ich mich anmelden will entschlüsselt die Nachricht mit dem öffentlichen Schlüssel. Wenn die empfangene und gesendete Nachricht gleich ist, weiß der Rechner das die Nachricht von mir verschlüsselt wurde denn nur ich kenne den geheimen Schlüssel

Passwort-Manager, Passkey, .pdf

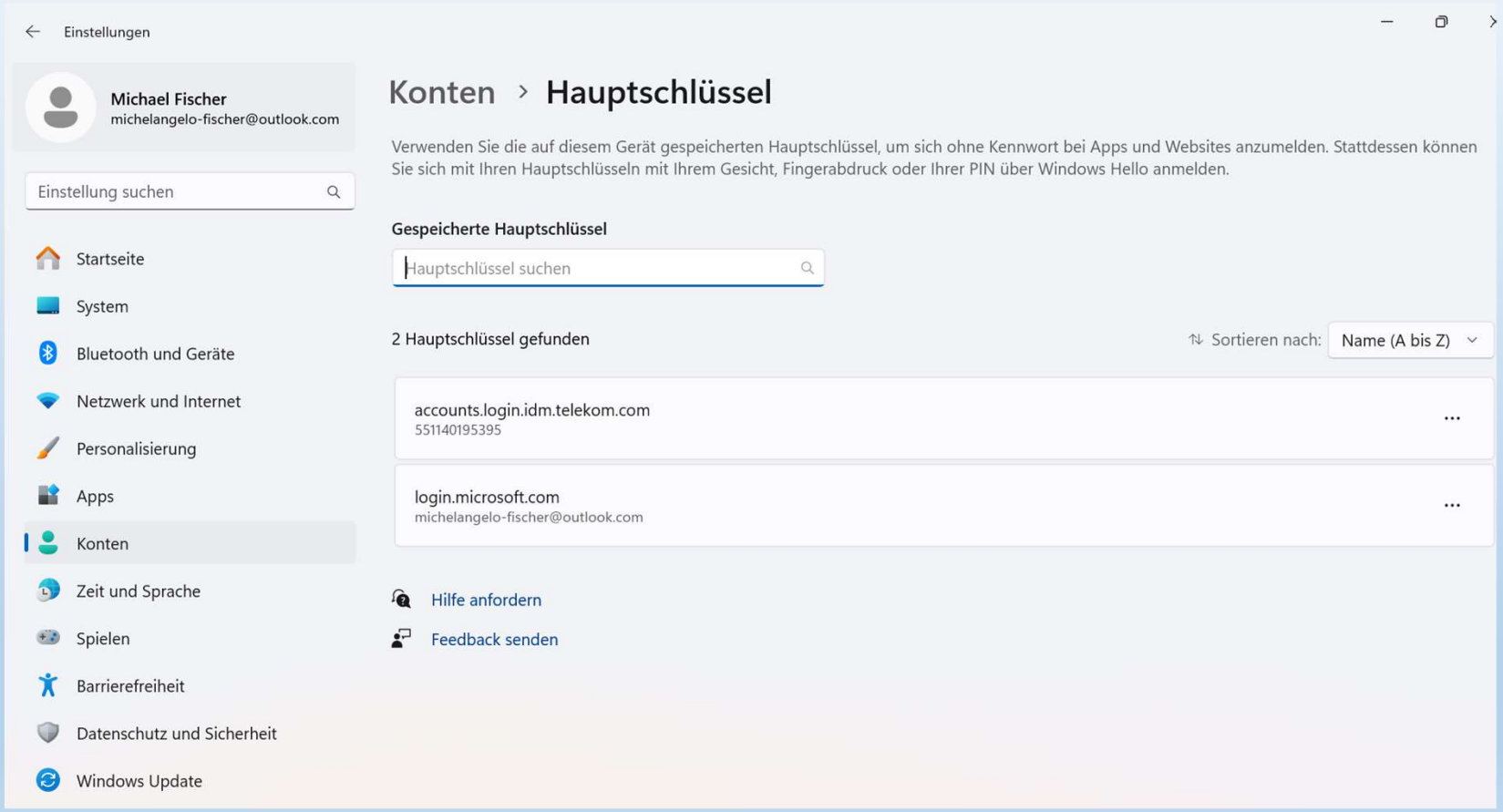
Wie funktioniert Passkey?

Wenn ein Diensteanbieter den Login mittels Passkey ermöglicht, müssen Sie zunächst einmal die Anmeldung per Passkey im entsprechenden Account einrichten. Das geht über die Sicherheitseinstellungen auf der Webseite oder in der App des Anbieters. Ist die Funktion eingerichtet, hinterlegt Ihr Gerät einen sogenannten geheimen Schlüssel im internen Speicher. Gleichzeitig wird ein passender öffentlicher Schlüssel erstellt, der bei Ihrem Onlinedienst, z. B. einem Onlineshop oder einem Streamingdienst, gespeichert wird. Diese Schlüssel sind die Grundlage für ein komplexes, kryptografisches Verfahren, das ab der Registrierung bei jeder Anmeldung von Ihnen unbemerkt abläuft.



Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf



Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf

Die geheimen Schlüssel sind nicht kopierbar oder über das Ethernet aus zu lesen.

Um die Verwendung von Passkeys auf mehreren Geräten zu ermöglichen ist ein Austausch der geheimen Schlüssel über Low Energy Bluetooth implementiert.

Low Energy wegen der geringen Reichweite und Bluetooth um einen separaten, hardwareunabhängigen Kanal zu benutzen.

Dieser Austausch kann zwischen Windows Geräten, aber auch mit Android oder iOS Geräten erfolgen.

Passwort-Manager, Passkey, .pdf

.pdf Portable Document Format

Das Dateiformat wurde 1992 von der Fa. Adobe erfunden.

Ziel war, ein Dateiformat für elektronische Schriftstücke zu schaffen, sodass diese unabhängig vom ursprünglichen Anwendungsprogramm, vom Betriebssystem oder von der Hardwareplattform originalgetreu wiedergegeben werden können.

Das Ziel wurde erreicht und findet seinen Niederschlag in der ISO-Normenserie 32000 (ISO 15930 für PDF/X).

Ein Leser einer PDF-Datei soll das Schriftstück immer in der Form betrachten und ausdrucken können, die der Autor festgelegt hat. Die typischen Konvertierungsprobleme (wie veränderter Zeilen- und Seitenumbruch oder falsche Schriftarten) beim Austausch eines Schriftstückes zwischen verschiedenen Programmen entfallen dadurch.

Michael Fischer, 29.11.2024

Passwort-Manager, Passkey, .pdf

Weitverbreitetes Gerücht, pdf-Dokumente lassen sich nicht ändern und eigen sich daher per se für Archivierung, oder geben immer das wieder, was der Autor hineingeschrieben hat.

Das ist nicht wahr, pdf-Dokumente lassen sich, inzwischen, in alle gängigen Textverarbeitungsprogramme importieren, ändern und wieder als pdf ausgeben.

pdf-Dateien lassen sich schützen, dazu sind aber spezielle Programme notwendig.

Es gibt ein pdf-Archivierungsformat pdf/A. In dessen Definition wird sichergestellt, dass Dokumente auch in etlichen Jahrzehnten noch lesbar sind, da nur die Grundmechanismen der pdf-Definition zur Erzeugung benutzt werden. Auch diese Dokumente sind nachträglich änderbar.

Michael Fischer, 29.11.2024