



| | | |
|---------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mi 15.01.2025 | AKIS-71 & FLUG | Cybersicherheit Cecilia und Jona Sander - Agile-Penguin |
| Mi 05.02.2025 | AKIS-72 | SmartHome Absicherung mit FIIPS Hermann Sauer - GF Comidio GmbH |
| Mi 19.03.2025 | AKIS-73 | PASSKEY-Vorbereitung Dieter Carbon |
| Mi 30.04.2025 | AKIS-74 | Einführung in PASSKEYS Christian Mueller - Sr. Channel Sales Manager DACH, Yubico |
| Mi 21.05.2025 | AKIS-75 & FLUG | System Software Development: Versionskontrolle Grundlagen Uwe Kleine-König - FOSS |
| Mi 04.06.2025 | AKIS-76 | Cybersicherheit und digitale Kompetenzen ein muss für Jedermann um nicht Opfer und/oder unbewusst zum Täter zu werden Markus Wortmann M.A. - Kriminologe & Polizeiwissenschaftler, Dipl.- Verwaltungswirt (FH), Business-Coach, zertifizierter Fachberater für Opferhilfe & Social Media Manager (IHK) |
| Mi 16.07.2025 | AKIS-77 & FLUG | Grundlagen des Hardenings von Servern in kleinen Netzwerken Frank Ewert - Sicherheitsberater, White Hat & Ethical Hacker |
| Mi 06.08.2025 | AKIS-78 & FLUG | Heimautomation mit Home Assistent Benno Vock - "pragmatischer, undogmatischer, hardwareaffiner EDV-Autodidakt" |
| Mi 17.09.2025 | AKIS-79 & FLUG | Passkeys mit KeePassXC Clemens Schweigler, Linuxianer mit Herzblut |
| Mi 01.10.2025 | AKIS-80 | Einsatz von KI und Herausforderungen Stephan Auge - Prokurist und Lead-Auditor, migosens management GmbH |
| Mi 19.11.2025 | AKIS-81 & FLUG | Persönliches Dateimanagement Karl Voit - Vordenker, IT life hacking, PIM-Optimierer |
| Mi 03.12.2025 | AKIS-82 | Technisch-organisatorische Absicherung des Datenschutzes in Zeiten von KI Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz |



Online-Workshops: Programmieren mit dem Raspberry Pi Pico

Was erwartet Sie?

- ☺ Grundlegende Programmier-Erfahrung
- ☺ Funktionsweisen von Sensoren
- ☺ Sensibilisierung für Messgenauigkeiten und Kalibrierung
- ☺ Realisieren nützlicher Klein-Projekte
- ☺ Eigene Ideen ausprobieren
- ☺ Tipps zum Umsetzen größerer Projekte
- ☺ Erste Schritte für ein eigenes Smart Home
- ☺ Nicht richtig oder falsch, sondern ANDERS machen dürfen

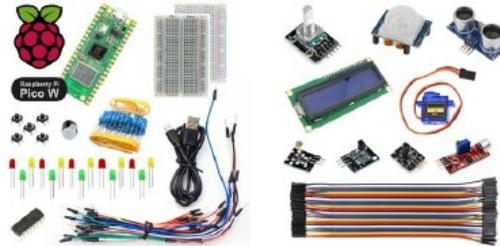
Lust auf mehr?

- Abstandsmessung
- Alarmanlage
- Ampelsteuerung
- Dämmerungsschalter
- Eieruhr
- Klatschschalter
- LED-Lauflicht
- Lichtschranke
- Meeting-Kosten
- Morsegenerator
- Reaktionsspiel
- Smart Home
 - Taster
 - Sensoren
 - Displays
 - Relais
 - Fernabfrage
- Temperatur-Logger
- Vortrags-Timer
- Zutrittskontrolle
- ...



Pico macht süchtig!
aber nicht abhängig

Elektronik-Sets



Informationen zu den Workshops für Unternehmen und Bildungseinrichtungen



Dipl.-Ing. Dieter Carbon

Mitgründer Comidio GmbH
Mitglied bei Störfallexperten
Leiter AK „Internet-Sicherheit“ VDI Rheingau-BV
dieter.carbon@comidio.de
0176 10209513

<https://www.elektronik-kompodium.de/service/events/picobello/>

**Elektronik
Kompodium**

PicoBello

Workshops für
Einsteiger

MINT

WLAN



IoT

Smart Home

Hardware-nahes
Programmieren mit
Raspberry Pi Pico und
MicroPython



Online-Workshops: Programmieren mit dem Raspberry Pi Pico

| Pico Bello | Inhalte (je Workshop: 60 Min. + Pause + 60 Min., online oder vor Ort) |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Für Einsteiger ohne Vorkenntnisse: Einführung 1: in den Pico, die Programmierumgebung Thonny und die Programmiersprache MicroPython anhand von einfachen Programm-Beispielen; abschließend erste externe Steuerung einer LED. Zu Hause kann (muss aber nicht) weiterge"arbeitet" werden. |
| 2 | Für Einsteiger mit Vorkenntnissen: Einführung 2: wir verwenden den internen Temperatursensor des Picos, bauen eine Ampel und einen Morsecodegenerator. |
| 3 | Sensor A: wir schließen ein zweizeiliges Display an den Raspberry Pi Pico an und verwenden es als Anzeige und zur Datenausgabe. Außerdem bauen wir ein digitales Thermometer und einen Bewegungsmelder. |
| 4 | Sensor B: besondere Highlights sind das Messen von Abstand, Licht und Lautstärke und natürlich das Kalibrieren der Sensoren. Nach diesem Online-Workshop haben wir einen Abstandsmesser, Dämmerungsschalter und Klatschschalter gebaut. |
| 5 | Pico W als Client: wir stellen mit dem Pico W eine WLAN-Verbindung her und nutzen ihn als Web-Client. Dabei wird der Pico u.a. Onboard-Temperatursensor Werte per E-Mail senden und Wetterdaten vom Deutschen Wetterdienst abrufen. |
| 6 | Pico W als Server: nun dient der Pico W mit WLAN-Verbindung als Web-Server. Vom Pico können per Browser Inhalte abgerufen werden z.B. Sensordaten, aber auch Aktivitäten ausgelöst werden, wie z.B. Onboard-LED schalten. |
| 7 | Smart Home Basis: jetzt steigen wir in die Smart Home Welt ein mittels MQTT-Protokoll: ein Raspberry Pi als MQTT-Broker und je zwei Pico W als MQTT-Publisher und MQTT-Subscriber, gesteuert über Node-RED; und als besonderes Extra: weltweiter Zugriff per VPN. |
| 8 | Node-RED Vertiefung: wir lernen die 20 wichtigsten Node-RED-Knoten kennen, und wie sie für Raspi-Anwendungen im Smart Home Bereich genutzt werden können; zu jedem Knoten gibt es Muster-Beispiele zur eigenen Anpassung und Verwendung. |
| 9 | Ein- und Ausgabesteuerung: wir lernen verschiedene Möglichkeiten kennen, wie die Umwelt mit dem Pico (Eingabe) und der Pico mit seiner Umgebung (Ausgabe) kommuniziert; Eingabe: u.a. Taster, Joystick, Rotary Decoder per Interrupt, LDR, Hall-Dekoder, Sensoren, ADC; Ausgabe: u.a. LEDs, LCD-Anzeigen, Relais, Summer, Servo, MP3-Player, Neopixel. |
| 10 | Fern-Einsatz mit LoRa: LoRaWAN und The Things Network (TTN); Einsatz und Test mit einem LoRa-Modul und dem Datenaustausch mit dem TTN-LoRaWAN. |

Für wen?

- ☺ Für die eigenen Mitarbeiter
- ☺ Für die Kinder der eigenen Mitarbeiter
- ☺ Für Ihre Kunden
- ☺ Für die Kinder Ihrer Kunden
- ☺ Als Sponsoring einer Jugend-Organisation

Für was?

- ☺ Demo mit Prämierung
- ☺ Programmier-Challenge mit Ergebnis-Präsentation
- ☺ Aktivität bei einem Tag der offenen Tür
- ☺ Kunden-Aktivität

Voraussetzungen

- ✓ Interesse haben
- ✓ ab 10 Jahre
- ✓ PC vorhanden
- ✓ Internetverbindung (bei Online-Workshop)



Bitte glauben Sie nicht mir ...

Siddhartha Gautama aus dem Adelsgeschlecht der Shakya wurde ca. 560 v. Chr. in Lumbini, Indien geboren. Nach seiner Erleuchtung unter dem Bodhi-Baum lehrte er während 45 Jahren als Buddha im Nordosten Indiens bevor er im Alter von ca. 80 Jahren starb.

Glaube nichts, weil ein Weiser es gesagt hat.

Glaube nichts, weil alle es glauben.

Glaube nichts, weil es geschrieben steht.

Glaube nichts, weil es als heilig gilt.

Glaube nichts, weil ein anderer es glaubt.

Glaube nur das, was Du selbst als wahr erkannt hast.



c't magazin für computer technik 8
5.4.2024
Europas größtes IT- und Tech-Magazin

Notebook
mit faltbarem 16-Zoll-OLED

Sicher und bequem: Passkey statt Passwort

So funktioniert der Passwort-Nachfolger • So sicher ist die Kryptografie • So legen Sie jetzt los

TEST
22 SSDs mit PCIe 4.0 und 5.0
MacBook Air mit M3-Prozessor
Mini-PC mit USB-C-Stromversorgung
Gut schlafen: Smarte Matratzenauflage
S/W-Laser-Multifunktionsdrucker

Leiser 17-Watt-PC fürs Büro
c't-Bauvorschlag mit Core i-14000

FOKUS
Zeitenwende: Bundeswehr entwickelt agil
c't-Notfall-Windows 2024 erweitern
Weg von Google: App-Stores für Autos
Funktionsupdate für Windows 11 im Detail
Streit um den digitalen Euro

Geheim-schlüssel

Passkeys: Der Passwort-Nachfolger startet durch

Passkeys: Der Passwort-Nachfolger startet durch Seite 14
Passkeys richtig verwalten Seite 18
Statt Passwort: Accounts mit Passkeys schützen Seite 24
Funktionsweise von Passkeys im Detail erklärt Seite 28

c't magazin für computer technik 12
17.5.2024
Europas größtes IT- und Tech-Magazin

Xiaomi: Mehr Kamera als Handy

Frisches Linux statt olles Windows

So gelingt der Umzug • Neues Leben für Windows-10-PCs
Umsteigerfreundliches Mint oder modernes Fedora

TEST
Sparsamer Büro-PC mit KI-Einheit
Kompakter Scanner fürs papierlose Büro
Plattformen für Ahnenforscher-Communities
Teleskop findet Sterne per App

Gaming-Notebooks
16-Zöller mit GeForce RTX 4070 bis 2000 Euro

EU-Digital
Kassensturz v

FOKUS
Was Sie be
Raspi als Streamer für Netflix, Disney+ & Co.
Notstrom aus dem E-Auto
Secure Boot: Sperre für alle Windows-Bootloader

Smarte Growboxen für Cannabis
Hanf legal pflanzen und ernten • Einsteigerfreundlich dank Hightech

Token 2

ct magazin für computer technik 8
5.4.2024
Europas größtes IT- und Tech-Magazin

Notebook
mit faltbarem 16-Zoll-OLED

Sicher und bequem: Passkey statt Passwort

So funktioniert der Passwort-Nachfolger • So sicher ist die Kryptografie • So legen Sie jetzt los

TEST
22 SSDs mit PCIe 4.0 und 5.0
MacBook Air mit M3-Prozessor
Mini-PC mit USB-C-Stromversorgung
Gut schlafen: Smarte Matratzenauflage
S/W-Laser-Multifunktionsdrucker

Leiser 17-Watt-PC fürs Büro
c't-Bauvorschlag mit Core i-14000

FOKUS
Zeitenwende: Bundeswehr entwickelt agil
c't-Notfall-Windows 2024 erweitern
Weg von Google: App-Stores für Autos
Funktionsupdate für Windows 11 im Detail
Streit um den digitalen Euro

MS Office: Copi
Was der KI-Assistent kann und was n

Geheim- schlüssel

Passkeys: Der Passwort-Nachfolger startet durch

ct 2024, Heft 8

Passkeys: Der Passwort-Nachfolger startet durch Seite 14
 Passkeys richtig verwalten Seite 18
 Statt Passwort: Accounts mit Passkeys schützen Seite 24
 Funktionsweise von Passkeys im Detail erklärt Seite 28

Europas g
Fris
 sta
 So geline
 Umsteig
TEST
 Sparsame
 Kompakte
 Plattform
 Teleskop
Gamin
 16-Zöller mi
EU-Dig
 Kassensturz
FOK
 Was Sie b
 Raspi als
 Notstrom
 Secure B
Sma
 Hanf lega

Viel Passkey für wenig Geld

FIDO2-Sticks mit Platz für 300 Passkeys

Die neuen FIDO2-Sticks des Genfer Herstellers Token2 können gleich 300 Passkeys speichern. Zudem bieten die Sticks komfortable Verwaltungstools und einen günstigen Preis. Wir haben einen ersten Blick darauf geworfen.

Von Ronald Eikenberg und Dirk Nopp

Die neue FIDO2-Sticks des Genfer Herstellers Token2 speichern bis zu 300 Passkeys und toppen damit die bisherigen Spitzenreiter, die Titan-Sicherheitsschlüssel von Google (250 Passkeys). Bei anderen Sticks wie den YubiKeys ist schon nach 25 das Ende der Fahnenstange erreicht. Interessanter ist aber, dass man die ganzen Passkeys anschließend auch verwalten und einzeln wieder löschen kann, etwa nachdem sie ungültig geworden sind. Die Google-Sticks sind hingegen eine Einbahnstraße: Ist der Speicher voll, kann man ihn nur komplett löschen.

Die Token2-Sticks mit dem etwas sperrigen Namen „T2F2-PIN+ Release2“ gibt es in drei Ausführungen: mit USB-A-Anschluss für 25 Euro, mit USB-C für 24 Euro und mit beiden Anschlüssen für 26 Euro. NFC für

die kontaktlose Nutzung ist immer an Bord. Hinzu kommen noch 9 Euro Versand.
 Zur Freigabe der Passkeys dient ein kapazitiver Knopf, den man nur leicht berühren muss, um ihn zu aktivieren. Dort leuchtet eine weiße Betriebs-LED, die bei Authentifizierungsanfragen blinkt. Eine firmwaregeschützte PIN-Abfrage sichert die Passkeys vor unbefugten Nutzern.

Aktueller FIDO2.1-Standard
 Die Sticks unterstützen den aktuellen FIDO2.1-Standard. Zur Verwaltung und Diagnose bietet der Hersteller diverse eigene Tools wie den „FIDO2.1 Manager“ für Windows (siehe ct.de/yk3x) an. Damit kann man die gesammelten Passkeys auflisten und löschen. Unter Linux und macOS klappt das direkt im Browser, sofern es sich um einen Chromium-Browser wie Google Chrome handelt.

Darüber hinaus gibt's das Windows-Kommandozeilentool fido2-manage.exe. Damit kann man die Sticks nicht nur verwalten, es listet auch die Eigenschaften des Sticks auf, etwa die unterstützten Kryptoverfahren (ECDSA, SHA256, AES, HMAC und ECDH) sowie den aktuellen Füllstand.

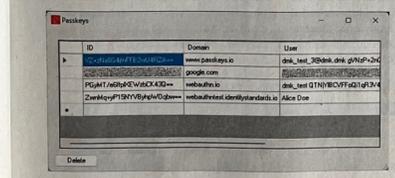
Neben Passkeys (FIDO2) bieten die Token2-Sticks weitere Funktionen zur sicheren Authentifizierung. Per App kann man sie für die Zwei-Faktor-Verfahren TOTP und HOTP konfigurieren, ähnlich

der teureren YubiKeys. Wie die meisten FIDO2-Sticks sind die „T2F2-PIN+ Release2“ abwärtskompatibel zu FIDO1 (U2F). Darüber hinaus kann man sie für die OpenSSH-Authentifizierung verwenden. Der Hersteller bietet konkrete Konfigurationsanfragen für viele Szenarien in englischer Sprache auf seiner Website an (siehe ct.de/yk3x).

Klein und wasserdicht
 Die Sticks sind sehr klein, die USB-C-Version etwa misst lediglich 42 x 17 x 6 Millimeter bei 5 Gramm Gewicht. Token2 verspricht eine „erweiterte Wasserdichtigkeit“, die die Sticks durch eine spezielle Beschichtung der Platine vor eindringendem Wasser schützt. Eine IPX-Zertifizierung liegt jedoch nicht vor.

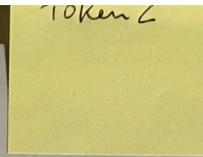
In einem ersten Test hat die USB-C-Variante einen guten Eindruck hinterlassen: Die Passkey-Authentifizierung funktionierte problemlos und auch die Verwaltung per Manager-App klappte auf Anhieb. Der einzige Wermutstropfen ist, dass die Sticks nicht Open Source sind, man muss dem Hersteller also vertrauen. Sie wurden jedoch unabhängig nach Authenticator Certification Level 1 (L1) zertifiziert.

Fazit
 FIDO2-Sticks sind derzeit die sicherste Option zum Speichern von Passkeys. Wer sich dafür entscheidet, dem liefert Token2 mit den „T2F2-PIN+ Release2“ ein rundes Gesamtpaket: Speicher für viele Passkeys, umfangreiche Verwaltungs-Apps und eine ausführliche Doku. Einzige die Produktbezeichnung ist etwas verwirrend. Falls Sie zugreifen möchten, sollten Sie auf die Formulierung „Release2“ achten, um sicherzustellen, dass es sich um die aktuelle Variante mit dem großen Passkey-Speicher handelt. (rei@ct.de) ct



Die App „FIDO2.1 Manager“ verwaltet die auf den Sticks gespeicherten Passkeys.

Herstellungshot, Tools & Doku: ct.de/yk3x



Passkeys | Aktuell





Based on FIDO standards, passkeys are a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices.

Unlike passwords, passkeys are always strong and phishing-resistant.

Passkeys simplify account registration for apps and websites, are easy to use, work across most of a user's devices, and even work on other devices within physical proximity.

Basierend auf FIDO-Standards sind Passkeys ein Ersatz für Passwörter, der schnellere, einfachere und sicherere Anmeldungen bei Websites und Apps über die Geräte eines Nutzers hinweg ermöglicht. Im Gegensatz zu Passwörtern sind Passkeys immer stark und phishing-sicher. Passkeys vereinfachen die Kontoerstellung für Apps und Websites, sind einfach zu verwenden, funktionieren auf den meisten Geräten eines Nutzers und sogar auf anderen Geräten in physischer Nähe.



stelle Seiten-inhalte zusammen für eine powerpoint präsentation zu folgendem Passkeys-Thema:

- 1 Was sind Passkeys?
- 2 wer kann sie gebrauchen?
- 3 wie werden sie eingesetzt?
- 4 welche websites erlauben sie?
- 5 welche Authenticator-Ausprägungen gibt es?
- 6 vergleich Authenticator-Ausprägungen Vorteile, Nachteile
- 7 wie sieht ein erster Einsatz bei einem Privat-Anwender aus?
- 8 welche Fido2-Stick-Anbieter gibt es?
- 9 warum setzen so wenige Anwender Passkeys ein?
- 10 was muss ich tun, wenn ich meinen Fido2-Stick verloren habe?



ChatGPT ▾

stelle Seiten-inhalte zusammen für eine powerpoint präsentation zu folgendem Passkeys-Thema:

- 1 Was sind Passkeys?
- 2 wer kann sie gebrauchen?
- 3 wie werden sie eingesetzt?
- 4 welche websites erlauben sie?
- 5 welche Authenticator-Ausprägungen gibt es?
- 6 vergleich Authenticator-Ausprägungen Vorteile, Nachteile
- 7 wie sieht ein erster Einsatz bei einem Privat-Anwender aus?
- 8 welche Fido2-Stick-Anbieter gibt es?
- 9 warum setzen so wenige Anwender Passkeys ein?
- 10 was muss ich tun, wenn ich meinen Fido2-Stick verloren habe?



Hier ist eine Gliederung für eine PowerPoint-Präsentation zum Thema Passkeys:

Folie 1: Titel

- **Titel:** Passkeys: Eine Einführung
- **Untertitel:** Was, Wer, Wie, Wo und Warum
- **Präsentator:** [Dein Name]
- **Datum:** [Datum]

Folie 2: Was sind Passkeys?

- **Definition:** Passkeys sind eine sichere Authentifizierungsmethode, die Passwörter ersetzt.





Folie 2: Was sind Passkeys?

- **Definition:** Passkeys sind eine sichere Authentifizierungsmethode, die Passwörter ersetzt.
- **Technologie:** Basieren auf kryptographischen Schlüsseln, die lokal auf dem Gerät gespeichert werden.
- **Sicherheit:** Bieten Schutz gegen Phishing und Credential Stuffing.

Folie 3: Wer kann sie gebrauchen?

- **Zielgruppen:**
 - Einzelpersonen
 - Unternehmen
 - Entwickler
- **Einsatzbereiche:**
 - Online-Dienste
 - Geschäftsanwendungen
 - Mobile Apps

Folie 4: Wie werden sie eingesetzt?

- **Registrierung:** Nutzer registrieren ihr Gerät bei einem Dienst.
- **Anmeldung:** Authentifizierung erfolgt über biometrische Daten oder eine PIN.
- **Schritte:**
 1. Registrierung des Geräts
 2. Authentifizierung mittels Biometrie oder PIN
 3. Zugriff auf den Dienst

Folie 5: Welche Websites erlauben sie?

- **Beispiele:**
 - Google
 - Microsoft
 - Facebook
 - Dropbox
 - Twitter



Folie 6: Welche Authenticator-Ausprägungen gibt es?

- Typen:
 - Hardware-Token (z.B. FIDO2-Sticks)
 - Software-Authenticator (z.B. Authenticator-Apps)
 - Plattform-gebundene (z.B. Windows Hello, Apple Face ID)

Folie 7: Vergleich Authenticator-Ausprägungen: Vorteile, Nachteile

- **Hardware-Token:**
 - Vorteile: Hohe Sicherheit, unabhängig vom Gerät
 - Nachteile: Verlust möglich, zusätzliche Hardware notwendig
- **Software-Authenticator:**
 - Vorteile: Flexibel, einfach zu bedienen
 - Nachteile: Abhängig vom Gerät, Sicherheitsrisiken bei Malware
- **Plattform-gebundene:**
 - Vorteile: Bequem, integriert in das Betriebssystem
 - Nachteile: Abhängig von der Plattform, eventuell weniger universell



Folie 8: Wie sieht ein erster Einsatz bei einem Privat-Anwender aus?

- Schritte:
 1. Kauf und Einrichtung eines FIDO2-Sticks oder Installation einer Authenticator-App
 2. Registrierung des Geräts bei einem unterstützten Dienst
 3. Nutzung der Passkey-Funktion zur Anmeldung

Folie 9: Welche Fido2-Stick-Anbieter gibt es?

- **Bekannte Anbieter:**
 - Yubico (YubiKey)
 - Feitian Technologies
 - Thetis
 - Kensington
 - Google (Titan Security Key)



Folie 10: Warum setzen so wenige Anwender Passkeys ein?

- **Gründe:**
 - Unbekanntheit der Technologie
 - Bequemlichkeit von Passwörtern
 - Kosten für Hardware-Token
 - Kompatibilitätsprobleme

Folie 11: Was muss ich tun, wenn ich meinen Fido2-Stick verloren habe?

- **Maßnahmen:**
 - Sofortige Sperrung des Zugangs über den Anbieter
 - Registrierung eines neuen FIDO2-Sticks
 - Nutzung von Backup-Authentifizierungsmethoden
 - Aktualisierung der Sicherheitsinformationen bei den Diensten

Folie 12: Zusammenfassung und Fragen

- **Zusammenfassung:**
 - Passkeys bieten eine sichere und benutzerfreundliche Alternative zu Passwörtern.
 - Verschiedene Authentifikationsmethoden haben unterschiedliche Vor- und Nachteile.
 - Der Einsatz von Passkeys nimmt zu, aber es gibt noch Hürden.
- **Fragen:**
 - Offene Diskussionsrunde

Diese Struktur bietet eine umfassende Übersicht über das Thema Passkeys und ermöglicht eine klare und informative Präsentation.





| Account | | Kunden-Name (z.B. Mail-Adresse) | Passwort | 2FA | Passkey |
|-------------------------|-------------------------------------------------------------------------------|------------------------------------|----------|-----|---------|
| Amazon | | | | | |
| Apple | | | | | |
| AZ Delivery | | | | | |
| Berrybase | https://www.berrybase.de/ | | | | |
| Die Bahn | | | | | |
| eBay | | | | | |
| FritzBox | | | | | |
| Github | https://github.com/dietercarbon | | | | |
| Google | | | | | |
| LinkedIn | | | | | |
| Medimops | | | | | |
| Microsoft | | | | | |
| Miles & More Mastercard | | | | | |
| Mein Spiel | | | | | |
| NAS | | | | | |
| Paypal | | | | | |
| Pearl | | | | | |
| RMV | | | | | |
| TP-Link | | | | | |
| VDI | | | | | |
| Volksbank | | | | | |
| Völkner | | | | | |
| Woocommerce | | | | | |
| | | | | | |

support@az-delivery.com
datenschutzbeauftragter@sertronic.de
p.d-datenschutz@deutschebahn.com



Yubico Authenticator

Home

USB
No YubiKey present

Home

Insert your YubiKey

Yubico Authenticator

Application

Settings
Change application preferences

YubiKey 5 NFC
S/N: 28082487 F/W: 5.4.3

Passkeys

Administrator privileges required

WebAuthn management requires elevated privileges. Alternatively, you can use Windows Settings to manage FIDO configuration.

Request access | Open Windows settings

Home

Accounts

Passkeys

Certificates

Slots

Yubico Authenticator

FIDO2

Passkeys

Enter the FIDO2 PIN for your YubiKey

PIN

Change PIN
8 attempt(s) remaining

Unlock

Yubico Authenticator

YubiKey 5 NFC
S/N: 28082487 F/W: 5.4.3

Passkeys

Manage

Change PIN
8 attempt(s) remaining

Search passkeys

- login.microsoft.com
dieter.carbon@comidio.de
- google.com
dieter.carbon@comidio.de
- amazon.de
dieter.carbon@comidio.de
- apple.com
- demo.yubico.com
dietercarbon

5 of 25 passkeys used. Non-passkey credentials may exist, but can not be listed.



Yubico Authenticator

YubiKey 5 NFC
S/N: 28082487 F/W: 5.4.3

Passkeys

FIDO2

Manage

Change PIN
8 attempt(s) remaining

Search passkeys

- login.microsoft.com
dieter.carbon@comidio.de
- google.com
dieter.carbon@comidio.de
- amazon.de
dieter.carbon@comidio.de
- apple.com
- demo.yubico.com
dietercarbon

5 of 25 passkeys used. Non-passkey credentials may exist, but can not be listed.

Home

Accounts

Passkeys

Certificates

Slots



- Der ultimative Schutz Ihrer Accounts: Verwalten von bis zu 60 TOTP-Konten
- Sichere Zwei-Faktor-Authentisierung (2FA) mit TOTP: Wirkungsvoller Schutz vor Identitäts-Diebstahl
- Für Smartphone, Tablet, Notebook oder Desktop
- Bei allen führenden Online-Plattformen sofort nutzbar
- Sicherheit aus Deutschland

Time-based One-time Password Algorithmus

Der Time-based One-time Password Algorithmus (TOTP) ist ein Verfahren zur Erzeugung von zeitlich limitierten Einmalkennwörtern basierend auf dem Keyed-Hash Message Authentication Code, welcher im Rahmen der Authentifizierung Anwendung findet.

Das Verfahren basiert im Kern auf einer kryptografischen Hash-Funktion HMAC, mit deren Hilfe aus dem zwischen Sender und Empfänger vereinbarten und geheimen Schlüssel K und der absoluten Uhrzeit ein kryptografischer Hash-Wert berechnet wird. ... Das Einmalkennwort ist innerhalb dieser Dauer von 30 Sekunden gültig. ... Wesentlich bei diesem Verfahren ist, dass die beiden Systeme, Sender und Empfänger, über hinreichend genaue Uhren oder über einen Zugang wie dem Network Time Protocol (NTP) zu einer genauen Uhrzeitinformation verfügen müssen, da andernfalls die Authentifizierung fehlschlägt.



<https://github.com/dietercarbon>

The screenshot shows the GitHub settings page for user Dieter Carbon. The left sidebar contains navigation options such as Public profile, Account, Appearance, Accessibility, Notifications, Access, Billing and plans, Emails, Password and authentication (selected), Sessions, SSH and GPG keys, Organizations, Enterprises, Moderation, Code, planning, and automation, Repositories, Codespaces, Packages, Copilot, Pages, Saved replies, Security, Code security, Integrations, Applications, and Scheduled reminders. The main content area is titled 'Password and authentication' and includes sections for Password, Passkeys, and Two-factor authentication. The Passkeys section lists three passkeys: AT2, A_Yubikey, and BT2, each with a 'Seen from this browser' label and edit/delete icons. The Two-factor authentication section is currently disabled, with a message stating 'Two-factor authentication is not enabled yet.' and a button to 'Enable two-factor authentication'.



← → ↻ <https://docs.github.com/de/authentication/authenticating-with-a-passkey/about-passkeys#about-passkeys> ☆ 🔍 Suchen

GitHub-Dokumentation | Version: Free, Pro, & Team ▾ GitHu

← Startseite

Authentication

- Kontosicherheit ▾
- Schützen deines Kontos mit 2FA ▾
- Authentifizieren mit einem Hauptschlüssel ▲
- Grundlegendes zu Hauptschlüsseln**
- Verwalten deiner Hauptschlüssel
- Anmelden mit einem Hauptschlüssel
- Verbinden mit SSH ▾
- Fehlerbehebung bei der SSH ▾
- Überprüfen von Commitsignaturen ▾
- Problembehandlung bei der Überprüfung ▾

Authentifizierung / Authentifizieren mit einem Hauptschlüssel /

Grundlegendes zu Hauptschlüsseln

Mit einem Hauptschlüssel kannst du dich ohne Kennwort und Zwei-Faktor-Authentifizierung sicher und einfach anmelden.

Wer kann dieses Feature verwenden?

👤 Personal account owners who manage their own credentials

In diesem Artikel

- Grundlegendes zu Hauptschlüsseln
- Über Authentifikatoren
- Feedback
- Weiterführende Themen

Grundlegendes zu Hauptschlüsseln [↗](#)

Mit einem Passkey können Sie sich sicher bei GitHub in Ihrem Browser anmelden, ohne Ihr Kennwort eingeben zu müssen.

Wenn du die Zwei-Faktor-Authentifizierung (2FA) verwendest, werden mit einem Hauptschlüssel sowohl die Kennwort- als auch die 2FA-Anforderungen erfüllt, sodass du deine Anmeldung in nur einem Schritt abschließen kannst. Wenn Sie keine 2FA verwenden, entfällt bei Verwendung eines Hauptschlüssels die Anforderung, ein neues Gerät per E-Mail zu verifizieren. Du kannst Hauptschlüssel außerdem für den sudo-Modus und zum Zurücksetzen deines Kennworts verwenden.

Hauptschlüssel sind Paare kryptografischer Schlüssel (öffentlicher Schlüssel und privater Schlüssel), die von einem von Ihnen gesteuerten Authentifikator gespeichert werden. Der Authentifikator kann nachweisen, dass ein Benutzer anwesend ist und berechtigt ist, den Hauptschlüssel zu verwenden.



Join FIDO & Thales on April 2

(https://event.on24.com/wcc/r/4896810/3D192F559B851EFDA267FBD9ED7A2A5F?utm_campaign=website&utm_medium=email&utm_source=sendgrid.com)

Webinar: The Essential Role of Passkeys in Modern Passwordless for End-Customers, Partners & Workforce

April 2, 2025 | 9:00am CT

Join us for a webinar (https://event.on24.com/wcc/r/4896810/3D192F559B851EFDA267FBD9ED7A2A5F?utm_campaign=website&utm_medium=email&utm_source=sendgrid.com) as Thales explores a unique approach to creating a seamless and secure authentication experience for consumers, employees, and partners. As organizations strive to enhance security while improving overall user experiences, breaking free from passwords has become a crucial step in the evolution of authentication.

In this session, we'll explore the compelling advantages of a passwordless framework, supported by robust FIDO mechanisms. Our discussion will cover essential topics such as key lifecycle management, the role of passkeys, and identity assurance in a secure digital environment. Attendees will gain actionable insights into how passkeys strengthen security, streamline authentication, and reduce the risks associated with traditional passwords.

Learn from our expert speakers how organizations across various industries are leveraging passwordless authentication to enhance user experience, reduce friction, and strengthen security.

*  Key Takeaways:*

- * Taking a strategic, phased approach, to eliminating passwords
- * Role of FIDO in passwordless authentication and passkeys
- * Overview of FIDO key lifecycle management processes
- * Best practices for implementing FIDO-powered passwordless strategies
- * Q&A session for addressing your specific concerns

Don't miss this opportunity to transform your authentication processes and embrace a future without passwords.

 Can't attend? Register to watch on demand

Register Now (https://event.on24.com/wcc/r/4896810/3D192F559B851EFDA267FBD9ED7A2A5F?utm_campaign=website&utm_medium=email&utm_source=sendgrid.com)

Sponsored by:

FIDO Events

3855 SW 153rd Drive, Suite 600 , Beaverton , OR 97003

<https://docs.github.com/de/authentication/authenticating-with-a-passkey/about-passkeys#about-passkeys>



- About the Alliance
- Alliance Membership
- Passkeys
- Specifications
- Certification
- Device Onboarding
- Resources
- News & Events**
- FIDO News Center
- Events Center
- FIDO in the News
- Press Center
- Newsletter Sign-Up

FIDO in the News

Articles written about FIDO Alliance in publications around the world, highlighting the push for a new era of ubiquitous, phishing-resistant, strong authentication to protect internet users worldwide.

797 results found in 1ms

March 17, 2025

IT News: Over 200,000 myGov users disable passwords in passkey shift

New figures reveal that over 200,000 users of myGov ...

[VIEW DETAILS](#) FIDO in the News

March 17, 2025

Mobile ID World: VicRoads Implements Passkeys Authentication System for Enhanced Digital Security

VicRoads, Victoria's road transport authority, has implemented a passkeys ...

[VIEW DETAILS](#) FIDO in the News

March 17, 2025

The Payers: Fime secures FIDO IDV certification for identity verification

Fime's testing laboratories in both EMEA and Taiwan have ...

[VIEW DETAILS](#) FIDO in the News

March 17, 2025

Help Net Security: Goodbye passwords? Enterprises ramping up passkey adoption

87% of companies have, or are in the midst of ...

[VIEW DETAILS](#) FIDO in the News



Join FIDO & Thales on April 2

(https://event.on24.com/wcc/r/4896810/3D192F559B851EFDA267FBD9ED7A2A5F?utm_campaign=website&utm_medium=email&utm_source=sendgrid.com)

Webinar: The Essential Role of Passkeys in Modern Passwordless for End-Customers, Partners & Workforce

April 2, 2025 | 9:00am CT

Join us for a webinar (https://event.on24.com/wcc/r/4896810/3D192F559B851EFDA267FBD9ED7A2A5F?utm_campaign=website&utm_medium=email&utm_source=sendgrid.com) as Thales explores a unique approach to creating a seamless and secure authentication experience for consumers, employees, and partners. As organizations strive to enhance security while improving overall user experiences, breaking free from passwords has become a crucial step in the evolution of authentication.

In this session, we'll explore the compelling advantages of a passwordless framework, supported by robust FIDO mechanisms. Our discussion will cover essential topics such as key lifecycle management, the role of passkeys, and identity assurance in a secure digital environment. Attendees will gain actionable insights into how passkeys strengthen security, streamline authentication, and reduce the risks associated with traditional passwords.

Learn from our expert speakers how organizations across various industries are leveraging passwordless authentication to enhance user experience, reduce friction, and strengthen security.

*  Key Takeaways:*

- * Taking a strategic, phased approach, to eliminating passwords
- * Role of FIDO in passwordless authentication and passkeys
- * Overview of FIDO key lifecycle management processes
- * Best practices for implementing FIDO-powered passwordless strategies
- * Q&A session for addressing your specific concerns

Don't miss this opportunity to transform your authentication processes and embrace a future without passwords.

 Can't attend? Register to watch on demand

Register Now (https://event.on24.com/wcc/r/4896810/3D192F559B851EFDA267FBD9ED7A2A5F?utm_campaign=website&utm_medium=email&utm_source=sendgrid.com)

Sponsored by:

FIDO Events



****Webinar: Die essenzielle Rolle von Passkeys in der modernen passwortlosen Authentifizierung für Endkunden, Partner und Mitarbeiter****

 ****2. April 2025 | 9:00 Uhr CT****

16.00 Uhr unserer Zeit

Nehmen Sie an unserem Webinar teil ([Hier registrieren](https://event.on24.com/wcc/r/4896810/3D192F559B851EFDA267FBD9ED7A2A5F?utm_campaign=website&utm_medium=email&utm_source=sendgrid.com)), in dem ****Thales**** einen einzigartigen Ansatz für eine nahtlose und sichere Authentifizierung für Verbraucher, Mitarbeiter und Partner vorstellt. Da Unternehmen sowohl die Sicherheit erhöhen als auch das Benutzererlebnis verbessern möchten, ist der Verzicht auf Passwörter ein entscheidender Schritt in der Weiterentwicklung der Authentifizierung.

****Was erwartet Sie?***

In dieser Sitzung beleuchten wir die überzeugenden Vorteile eines passwortlosen Frameworks, das auf ****starken FIDO-Mechanismen**** basiert. Zu den Themen gehören:

- Verwaltung des Schlüssel-Lebenszyklus
- Die Rolle von Passkeys
- Identitätsprüfung in einer sicheren digitalen Umgebung

Teilnehmer erhalten praxisnahe Einblicke, wie Passkeys die Sicherheit erhöhen, die Authentifizierung vereinfachen und die Risiken traditioneller Passwörter minimieren.

****  Wichtige Erkenntnisse:***

- ◆ Strategische, schrittweise Einführung einer passwortlosen Zukunft
- ◆ Die Rolle von FIDO bei der Authentifizierung mit Passkeys
- ◆ Überblick über das FIDO-Schlüssel-Lebenszyklusmanagement
- ◆ Best Practices für die Implementierung von FIDO-basierten, passwortlosen Strategien
- ◆ ****Q&A-Session**** zur Klärung individueller Fragen

 ****Nicht verfügbar?*** Registrieren Sie sich trotzdem, um die Aufzeichnung später auf Abruf anzusehen!

 ****Jetzt registrieren:*** [Hier klicken](https://event.on24.com/wcc/r/4896810/3D192F559B851EFDA267FBD9ED7A2A5F?utm_campaign=website&utm_medium=email&utm_source=sendgrid.com)

- ◆ ****Gesponsert von:*** FIDO Events



<https://yopad.eu/p/Passkeys>



| | | |
|---------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mi 15.01.2025 | AKIS-71 & FLUG | Cybersicherheit Cecilia und Jona Sander - Agile-Penguin |
| Mi 05.02.2025 | AKIS-72 | SmartHome Absicherung mit FIIPS Hermann Sauer - GF Comidio GmbH |
| Mi 19.03.2025 | AKIS-73 | PASSKEY-Vorbereitung Dieter Carbon |
| Mi 30.04.2025 | AKIS-74 | Einführung in PASSKEYS Christian Mueller - Sr. Channel Sales Manager DACH, Yubico |
| Mi 21.05.2025 | AKIS-75 & FLUG | System Software Development: Versionskontrolle Grundlagen Uwe Kleine-König - FOSS |
| Mi 04.06.2025 | AKIS-76 | Cybersicherheit und digitale Kompetenzen ein muss für Jedermann um nicht Opfer und/oder unbewusst zum Täter zu werden Markus Wortmann M.A. - Kriminologe & Polizeiwissenschaftler, Dipl.- Verwaltungswirt (FH), Business-Coach, zertifizierter Fachberater für Opferhilfe & Social Media Manager (IHK) |
| Mi 16.07.2025 | AKIS-77 & FLUG | Grundlagen des Hardenings von Servern in kleinen Netzwerken Frank Ewert - Sicherheitsberater, White Hat & Ethical Hacker |
| Mi 06.08.2025 | AKIS-78 & FLUG | Heimautomation mit Home Assistent Benno Vock - "pragmatischer, undogmatischer, hardwareaffiner EDV-Autodidakt" |
| Mi 17.09.2025 | AKIS-79 & FLUG | Passkeys mit KeePassXC Clemens Schweigler, Linuxianer mit Herzblut |
| Mi 01.10.2025 | AKIS-80 | Einsatz von KI und Herausforderungen Stephan Auge - Prokurist und Lead-Auditor, migosens management GmbH |
| Mi 19.11.2025 | AKIS-81 & FLUG | Persönliches Dateimanagement Karl Voit - Vordenker, IT life hacking, PIM-Optimierer |
| Mi 03.12.2025 | AKIS-82 | Technisch-organisatorische Absicherung des Datenschutzes in Zeiten von KI Prof. Dr. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz |



Danke für Ihr Interesse!

Gibt es Fragen ... ?



Vielen Dank für Ihre Teilnahme,
bis zum nächsten Mal 😊,
bleiben Sie gesund zu Hause
und haben Sie eine sichere Zeit!

Dieter Carbon