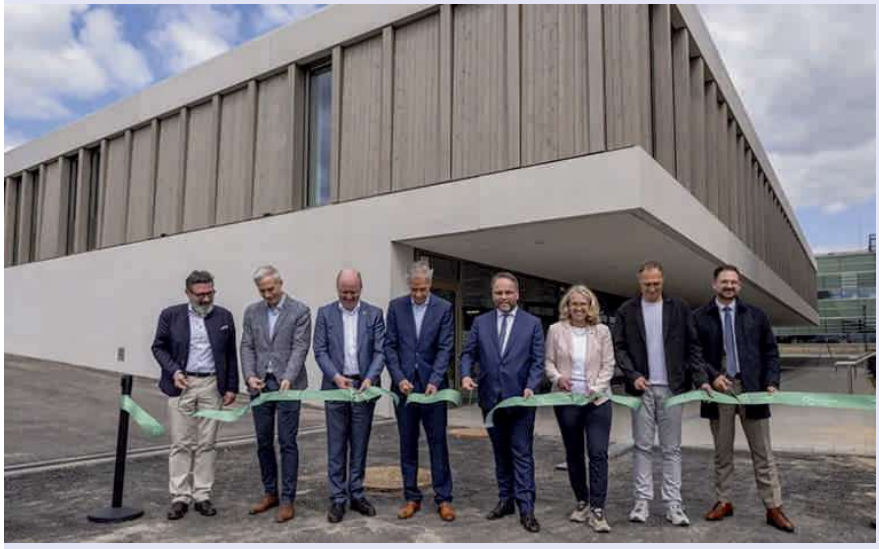
# Rheingau-Bezirksverein

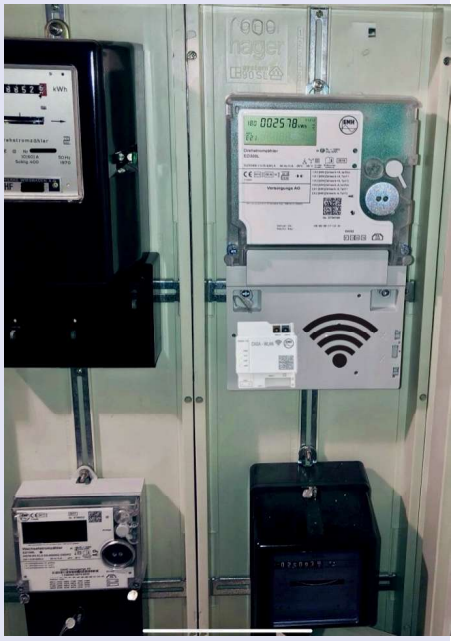
# Regional-Magazin 3/2025

## Hochschule Geisenheim

***Eröffnung GTZ***



## Smart Meter

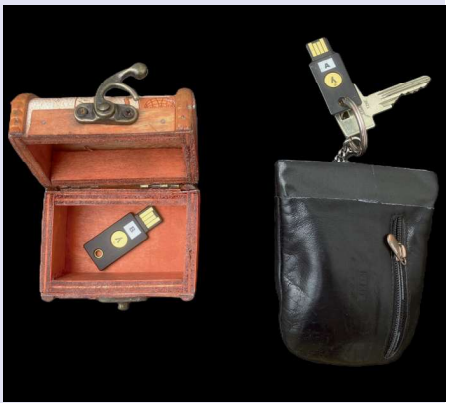


## IMS Tec GmbH

***Firmenportrait***

## PassKey

***ein neuer Schlüssel im Bund***



# Internet - Sicherheit

## Sicher, einfach, passwortfrei: Die neue Rubrik „PassKeys“

## Wie Sie mit modernen Sicherheitsschlüsseln Ihre Online-Konten schützen – ganz ohne Passwörter

PassKeys gelten als der sicherste Weg, sich künftig bei Online-Diensten anzumelden – ohne klassische Passwörter. Unterstützt durch einen Hardware-Stick (z. B. YubiKey, Nitrokey, Token2), machen PassKeys Phishing und Datenlecks weitgehend wirkungslos. Unsere neue Rubrik beleuchtet technische Hintergründe, stellt Anbieter vor und zeigt Schritt für Schritt, wie Sie PassKeys einrichten.

### Was ist ein PassKey?

- Login ohne Passwort
- Lokale Hardware (FIDO-2 Stick prüft Identität)
- Kein „Passwort merken“ mehr nötig
- Sehr hoher Schutz gegen Phishing

### Wer bietet PassKeys schon an?

| Anbieter | Anzahl möglicher Passkeys | „Passwort vergessen“ - Fallback |
|---|---|---|
| Amazon | 5 | nein |
| Apple | mehrere Geräte & Schlüssel | ja (z. B. Apple-ID-Wiederherstellung, Gerätecode) |
| Dropbox | mehrere | ja (Notfallcode erforderlich) |
| eBay | mehrere | ja (per Mail oder Telefonnummer) |
| facebook * | ? | ? |
| GitHub | mehrere | ja |
| Hyatt * | ? | ? |
| IKEA * | ? | ? |
| Google | mehrere pro Account | ja (via Recovery-Mail/SMS) |
| Linked in * | ? | ? |
| Microsoft | mehrere | ja (z. B. via Telefonnummer) |
| NETFLIX * | ? | ? |
| PayPal * | ? | ? |
| SAMSUNG * | ? | ? |
| T-Mobile * | ? | ? |
| TikTok * | ? | ? |
| Toyota * | ? | ? |
| Uber * | ? | ? |
| yahoo! * | ? | ? |
| YouTube * | ? | ? |
| 1Password | mehrere | ja (Master-PW + Recovery-Key) |

* laut Passkey Directory (siehe unten); wird noch geprüft.

***Datenstand: 25.06.2025 – ohne Gewähr.*** Weitere Updates und PassKey-Anbieter folgen.

### Stimmen zu PassKeys

**BSI:** „Schafft die Passwörter ab?! Anmelden ohne Passwort mit Passkey“

*https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Passkeys/passkeys-anmelden-ohne-passwort_node.html*

**Verbraucherzentrale NRW:** „Passkeys als Alternative zu Passwörtern“

*https://www.verbraucherzentrale.nrw/wissen/digitale-welt/datenschutz/passkeys-als-alternative-zu-passwoertern-94842*

**fido Alliance:** „Introduction to Passkeys“ (Einführung in PassKeys)
*https://www.passkeycentral.org/introduction-to-passkeys/*

**Passkey Directory** (Liste der PassKey-anbietenden Online-Services)
https://fidoalliance.org/passkeys-directory/

## Selber ausprobieren?

Google “Einfacher und sicherer in Ihren Konten anmelden – ganz ohne Passwort”
*https://safety.google/authentication/passkey/*

Apple “Informationen zur Sicherheit von Passkeys”
*https://support.apple.com/de-de/102195*

YubiKey “Keine Kontoübernahmen mehr” (also kein Identitäts-Diebstahl möglich)
https://www.yubico.com/?lang=de

GitHub „Signing in with a passkey“
*https://docs.github.com/en/authentication/authenticating-with-a-passkey/signing-in-with-a-passkey*

## Erste VDI PassKey-Party voraussichtlich noch dieses Jahr

- ***wo:*** Mainz

- ***wie:*** jeder ist eingeladen, sich zu informieren; für Brezeln und Getränke wird gesorgt; wer Laptop und PassKey-Stick mitbringt kann vor Ort seine PassKeys bei Amazon, Apple, Google und anderen selbst einrichten

- ***Details folgen***

In jeder Ausgabe ab sofort: „PassKeys“ – die Rubrik für sichere Anmeldung ohne Passwort

*Dieter Carbon*

Die digitale Kommunikation ersetzt zunehmend den persönlichen Kontakt; für die Generation, die in dieses Zeitalter hineinwächst ist das vollkommen normal; für die Generationen davor eher befremdlich. Nichtsdestotrotz, der VDI entwickelt sich mit und ist in bester Gesellschaft. Soziale Medien sind keine Hürde. Speziell hervorzuheben sind weiterhin Quellen wie die **VDI Homepage** vdi.de „Mein VDI“, **VDI Technik aufs Ohr Podcasts, VDI Net** und die **VDI Nachrichten** in Papier- oder Digitalformat. Der BV Rheingau bemüht sich zudem, Sie auch mit regionalen Nachrichten und Ankündigungen von Veranstaltungen zu versorgen; per Email und mit unserem Regionalmagazin.

Damit Sie alle Informationen zuverlässig erhalten, ist es erforderlich, dass Sie Ihre persönlichen Kontaktdetails, speziell Ihre E-Mail Adresse auf neuesten Stand halten. Überprüfen Sie dazu auf der Homepage des VDI unter "Mein VDI" Ihre persönlichen Daten

***https://www.vdi.de/mein-vdi/intern/profil***

Falls Sie Probleme haben, kontaktieren Sie gerne unser Vereinsbüro (bv-rheingau@vdi.de) in Flörsheim.

## AKIS-73: PASSKEY-Vorbereitung

**Referent:** Dieter Carbon

73. Veranstaltung vom 19.03.2025

Mit der Präsentation „AKIS-73“ bereitet der VDI-Arbeitskreis Internet-Sicherheit engagiert und praxisnah den Weg in eine neue Ära der digitalen Authentifizierung: **Passkeys.** Diese Technologie auf Basis des FIDO2-Standards ersetzt nicht nur unsichere Passwörter, sondern macht das digitale Leben für Privatpersonen wie auch Unternehmen sicherer, komfortabler und zukunftsfähiger.

### Was sind Passkeys?

Passkeys ermöglichen passwortlose Logins, die phishing-resistent, plattformübergreifend nutzbar und benutzerfreundlich sind. Anders als klassische Passwörter oder Einmalcodes werden Passkeys niemals übers Netz übertragen – sie bleiben sicher auf dem Gerät oder einem dedizierten Sicherheitsschlüssel gespeichert. Das bedeutet: Schutz vor Datenklau, Phishing und Missbrauch – bei gleichzeitig deutlich verbesserter Benutzererfahrung.

### Für wen sind Passkeys geeignet?

Im Grunde für alle: vom Technikaffinen bis zum Einsteiger, vom Privatanwender bis zum Großunternehmen. In der Präsentation wird deutlich, dass Passkeys nicht länger Zukunftsmusik sind, sondern heute schon nutzbar – auf Plattformen wie Google, Apple, Microsoft, GitHub, PayPal, LinkedIn, eBay u. v. m. Der Einstieg ist leicht: Wer über ein Smartphone mit biometrischer Sperre verfügt oder einen FIDO2-Stick nutzt, kann direkt loslegen.

### Warum setzen bisher so wenige Menschen Passkeys ein?

Oft fehlt schlicht das Wissen – genau hier setzt der AKIS-Workshop an. Viele wissen nicht, dass sie Passkeys schon heute aktivieren können. Auch der Umstieg von bestehenden Logins scheint komplex – dabei zeigen Beispiele aus der Präsentation, wie einfach ein erster Einsatz gelingen kann. Tools wie KeePassXC oder der Yubico Authenticator bieten bereits Schnittstellen zur passwortlosen Anmeldung.

### Welcher Authenticator passt zu wem?

Die Präsentation erläutert praxisnah die Unterschiede zwischen App-basierten Lösungen (z. B. mit TOTP) und hardwaregebundenen Varianten, etwa FIDO2-Sticks von Anbietern wie Yubico, Nitrokey, SoloKeys oder Reiner SCT. Der Vorteil: Diese Geräte sind robust, offline-fähig, unabhängig vom Betriebssystem – und ideal für sicherheitskritische Umgebungen.

### Was passiert, wenn ein FIDO2-Stick verloren geht?

Auch hier bietet der Vortrag praxisnahe Hinweise: Viele Dienste ermöglichen ein Hinterlegen mehrerer Geräte. Für Notfälle kann eine sichere Backup-Strategie eingerichtet werden – mit Passwortmanager, Zweitstick oder fallbackfähiger App. Wichtig ist: Der Verlust eines Sticks bedeutet keinen Kontrollverlust, wenn man vorbereitet ist

### Digitale Selbstermächtigung als Ziel

Diese Präsentation zeigt klar: Passkeys sind keine Spezialtechnik für IT-Profis, sondern ein wirksamer Schutzmechanismus für jeden, der sich online bewegt. Der AKIS-Vortrag stellt nicht nur die Technik vor, sondern betont auch die gesellschaftliche Bedeutung: Wer starke Authentifizierung nutzt, schützt nicht nur sich selbst, sondern auch die Gemeinschaft – z. B. durch die Vermeidung von Botnetzen, Identitätsdiebstahl oder Betrugswellen.

### Fazit:

Der AKIS-Arbeitskreis zeigt mit dieser Präsentation auf motivierende Weise, dass der Einstieg in die passwortlose Zukunft möglich, sinnvoll und sofort umsetzbar ist. Mit fundierten Informationen, konkreten Anwendungstipps und einem klaren Sicherheitsgewinn wird der Übergang zu Passkeys greifbar gemacht – nicht als technische Hürde, sondern als Chance, digitale Identität souverän zu schützen.

Jetzt ist der richtige Zeitpunkt: Schluss mit Passwörtern – willkommen in der Ära der Passkeys!

Wir freuen uns, in AKIS-74 hierzu Gedanken mit dem Miterfinder von FIDO – und damit von Passkeys - austauschen zu können.

*B. Betz, C. Schweigler, D. Carbon*

## AKIS-74: Einführung in PASSKEYS

**Referent:** Christian Müller - Sr. Channel Sales Manager DACH, Yubico

74. Veranstaltung vom 30.04.2025

In AKIS-73 haben wir uns intensiver mit Passkeys beschäftigt und Erfahrungen und Fragen gesammelt, um diese „heute“ vom weltweiten Marktführer beantwortet bzw. validiert zu bekommen.
Die digitale Welt steht an einem Wendepunkt: Passwörter, die über Jahrzehnte zentrale Zugangskontrolle waren, haben ausgedient. Die Yubico-Präsentation zur Passkey-Einführung zeigt eindrucksvoll, wie Unternehmen durch passwortlose, phishing-resistente Authentifizierung eine neue Ära der IT-Sicherheit einläuten. Dabei steht ein Ziel im Vordergrund: Benutzer schützen – nicht nur Logins.

Mit mehr als 22 Millionen verkauften YubiKeys und Kunden wie Google, Microsoft oder Salesforce ist Yubico weltweit führend im Bereich starker Authentifizierung. Der YubiKey als physischer Sicherheitsschlüssel basiert auf dem FIDO2-Standard und ermöglicht **Login-Prozesse ganz ohne Passwörter.** Die Vorteile sind vielfältig: Keine Passwort-Resets, keine Kontoübernahmen, keine unnötige Supportlast – dafür aber maximale Sicherheit bei minimaler Komplexität.

Besonders hervorgehoben wird der Wandel vom „phishing-resistenten Login“ hin zum „phishing-resistenten Benutzer“. Während klassische Zwei-Faktor-Verfahren wie SMS oder OTPs weiterhin von Phishing-Angriffen ausgehebelt werden können, bieten hardwaregebundene Passkeys ein völlig neues Sicherheitsniveau. Diese bleiben lokal auf dem Gerät oder auf dem YubiKey gespeichert, kommunizieren nicht über das Netzwerk und sind nicht kopierbar – ein Meilenstein in Sachen Datenschutz und Sicherheit.

Yubico differenziert zwischen verschiedenen Implementierungsmustern: Synchronisierte Passkeys, App-verwaltete Passkeys und hardwaregebundene Passkeys. Nur Letztere bieten höchsten Schutz und erfüllen regulatorische Anforderungen wie NIST AAL3. Sie eignen sich besonders für Unternehmen mit hohen Sicherheitsanforderungen – sei es im Finanzwesen, in Behörden oder im Gesundheitssektor.

Die Präsentation zeigt auch praxisnahe Szenarien: Vom sicheren VPN-Zugang über Remote Work und Shared Workstations bis hin zu kritischen Administratorkonten. Unternehmen wie T-Mobile (200.000 Nutzer) oder die Stadt München (32.000 Mitarbeitende) belegen, dass der großflächige Einsatz von YubiKeys nicht nur praktikabel, sondern auch effektiv ist: keine Passwörter, keine OTPs, keine Phishing-Vorfälle – dafür deutlich gesteigerte Produktivität und Benutzerfreundlichkeit.

Ein weiterer Fokus liegt auf der Umsetzung: Mit Tools wie YubiEnroll oder dem Premium-Service FIDO Pre-reg wird die Einführung von Passkeys auch bei großen Nutzerzahlen unkompliziert – inklusive werkseitiger Vorkonfiguration. Selbst sensible Umgebungen ohne Internetzugang oder mobile Geräte („mobile restricted“) können problemlos abgesichert werden.
Nicht zuletzt überzeugt Yubico durch Qualität und Langlebigkeit: Die Schlüssel sind robust, wasserdicht, benötigen weder Batterie noch Internetverbindung, werden in Schweden und den USA produziert und erfüllen höchste Compliance-Standards wie DSGVO, FIPS oder PSD2. Sie sind nicht nur ein Werkzeug, sondern ein langfristiger Sicherheitsanker in einer unsicheren Welt.

**Fazit:** Yubico liefert nicht nur eine Technologie, sondern ein überzeugendes Gesamtpaket für die sichere Zukunft digitaler Identitäten. Wer den Wandel hin zur phishing-resistenten Authentifizierung jetzt gestaltet, spart nicht nur Kosten und Supportaufwand, sondern gewinnt vor allem eins: Vertrauen – intern wie extern.
Nach ausführlicher Präsentation kommentiert und antwortet Herr Müller, über eine Stunde lang, was das große Interesse der über 30 Teilnehmenden zeigt.

**Mit Passkeys wird Sicherheit endlich einfach, skalierbar und nachhaltig.**

AKIS wird weiter über Passkey-Anwendung und -Verbreitung berichten und erwägt, im Rahmen von „Passkey-Parties“ den Umstieg von Passwortnutzung auf Passkeys live (und analog) zu zeigen und zu unterstützen.

*B. Betz, C. Schweigler, D. Carbon*