



Passkeys, FIDO, Smart Card & Co

Dirk Gluch

Principal Security Engineer
gluch@avantec.ch

Passwordless mit Passkeys, FIDO & Smartcard

- **Gestohlene Zugangsdaten?
Nicht mit Passkeys, FIDO & Smartcard, ... - Wieso?**
- **Was ist passwordless?**
- **Warum Passkey - FIDO - Smart Cards - WHfB - ...?**
- **Alle Fragen bitte in den Chat!**



Secure Authentication 2026 - Agenda

- Was ist eine sichere Authentisierung 2026 und danach
 - An welchen Geräten?
 - An welchen Diensten
 - Mit welchen Mitteln – passwordless
 - FIDO, Passkey
 - Smart Card
 - WHfB
 - ...
- EDR für Credentials
- Privileged user



```
30 82 01 0a 02 82 01 01 00 ea 4a a9 fa 88 51 d5 ae e7 dc 53 26 3f 05 56
45 1c 50 97 05 52 8c 2c c1 7d 29 63 9f ca f0 78 fa 14 8a 2c dc 50 2b f1
6f 11 f3 c5 b9 c4 7f 8b af 9b 92 71 2a 3b bc 3e e9 d1 ca be 3f 36 6d 21
cf 5c f5 9d 5e 76 41 ee 6a 35 9a 8f 55 38 9f e3 52 ba 96 6f 31 38 cc dd
9f 31 12 f3 3a ee 32 97 6f 00 17 c3 9b 34 10 0d d4 f7 87 77 5b ff 14 35
ef cc df 64 51 e4 d7 00 e1 a7 c5 1f be c8 8c bd c5 5d 3e 76 d0 74 04 8d
e7 b2 bb 10 07 f7 6f ea 49 3f 73 5c ea 40 da e7 54 70 1b a4 22 e7 24 07
7c cc dc 01 c7 5f 3d 74 c5 55 d8 07 eb c2 7d d9 55 2f 08 ca 03 84 24 4a
b2 86 a6 8e 18 85 95 5f b5 71 db 5f 9d 84 cf 0f a0 73 b1 ab 9c b2 72 64
26 70 21 f6 2c 45 3a 3c 6f 60 ec 06 0f 53 47 3d 84 db d0 c3 27 90 c0 b1
e9 8f ca 57 c6 a7 6f 33 44 f3 f1 81 be dd cc 62 25 58 d4 6a e0 3b 38 be
43 02 03 01 00 01
```

Collection of public articles

INNOVATION > CYBERSECURITY

Gmail Passwords Confirmed Within 183 Million Account Infostealer Leak

By [Davey Winder](#), Senior Contributor. © Davey Winder is a veteran cybersecur... ▼

[Follow Author](#)

Published Oct 28, 2025, 10:04am EDT

[Share](#) [Save](#) [Comment](#)



Collection of public articles

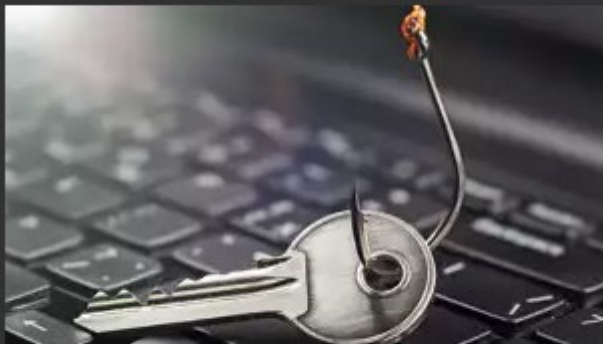
INNOVATION > CYBERSECURITY

Gmail Passwords Confirmed Within 187 Million Accounts

By Davey Winder

Published Oct 28

< Share



ALERT

Infostealer für Windows, macOS und Linux in zehn Paketen auf npm gefunden

Die npm-Pakete waren seit Juli verfügbar, haben die Schadroutinen aufwendig verschleiert und setzen auf ein Fake-CAPTCHA, um authentisch zu erscheinen.

30.10.2025 09:36 Uhr  14  heise Developer

Collection of public articles

Stop Using Public Wi-Fi, Google Warns—Change Your Phone Settings

By [Zak Doffman](#), Contributor. © Zak Doffman writes about security, surveillanc... ▾

[Follow Author](#)

Published Nov 05, 2025, 04:23am EST, Updated Nov 06, 2025, 03:02am EST

[Share](#) [Save](#)



Is this real? Google's surprising new advice.

GETTY IMAGES

Google has just told smartphone users to “avoid using public Wi-Fi whenever possible.”

S und Linux in zehn

ar, haben die Schadroutinen
in Fake-CAPTCHA, um

per

Collection of public articles

Stop Using Public Wi-Fi, Google Warns—Change Your Phone Settings

By [Zak Doffman](#), Contributor. © Zak Doffman writes about security, surveillanc... ▼

Follow Author

Published Nov 05, 2025, 04:23am EST, Updated Nov 06, 2025, 03:02am EST

"The malware operators made an effort to carefully mimic all the key interface details to avoid raising any suspicions," the Check Point Research report said.

Once FluHorse wiggles its way into a victim's device, it can steal their credentials and two-factor authentication (2FA) codes. How? Firstly, once the imposter app is installed, it asks victims to allow it to send and view SMS messages.

Next, quarries are prompted to input their credentials (e.g., password and credit card details). At some point, a command-and-control server intercepts any incoming SMS traffic to snatch 2FA codes.



Is this real? Google's surprising new advice.

GETTY IMAGES

S und Linux in zehn

ar, haben die Schadroutinen
in Fake-CAPTCHA, um

per

Collection of public articles

Stop Using Public Wi-Fi, Google Warns—Change Your Phone Settings

By [Zak Doffman](#), Contributor. © Zak Doffman writes about security, surveillanc... ▼

[Follow Author](#)

Published Nov 05, 2025, 04:23am EST, Updated Nov 06, 2025, 03:02am EST

S und Linux in zehn

"The n any su Google Responds To Android Pixnapping Attack Threat

Once l authel send a A Google spokesperson, while stating that there have been no instances of Pixnapping evidenced as being exploited in the wild, confirmed that a September Android security patch for CVE-2025-48561 partially mitigates the impact of such an attack. "We are Next, i point, issuing an additional patch for this vulnerability in the December Android security bulletin," the Google spokesperson added.



Is this real? Google's surprising new advice.
GETTY IMAGES

lie Schadroutinen
APTCHA, um

Google has just told smartphone users to "avoid using public Wi-Fi whenever possible."

Collection of 1.3 Billion Unique Passwords' Exposed In 'Extensive' Data Leak

Stop Using Public Wi-Fi, Your Phone Security

By [Zak Doffman](#), Contributor. © Zak Doffman writes about security, surveillanc...

Follow Author

By [Zak Doffman](#), Contributor. © Zak Doffman Published Nov 06, 2025, 04:46am EST, Updated Nov 06, 2025, 04:48am EST

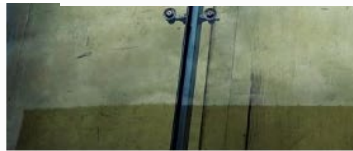
Published Nov 05, 2025, 04:23am EST, Updated Nov 05, 2025, 04:23am EST

[Share](#) [Save](#)

"The n any su **Google Resp**

Once l A Google spokes auther A Google spok send a evidenced as bein

Next, i patch for CVE-20 point, issuing an additic bulletin," the Goc



Is this real? Google's surprising new advice. GETTY IMAGES

Google has just told smartpho...



Coll
Stop
Your

Android 2FA Code Theft — Google Pixel And Samsung Galaxy Users Warned

By [Davey Winder](#), Senior Contributor. © Davey Winder is a veteran cybersecur...

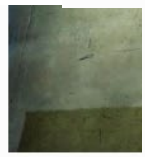
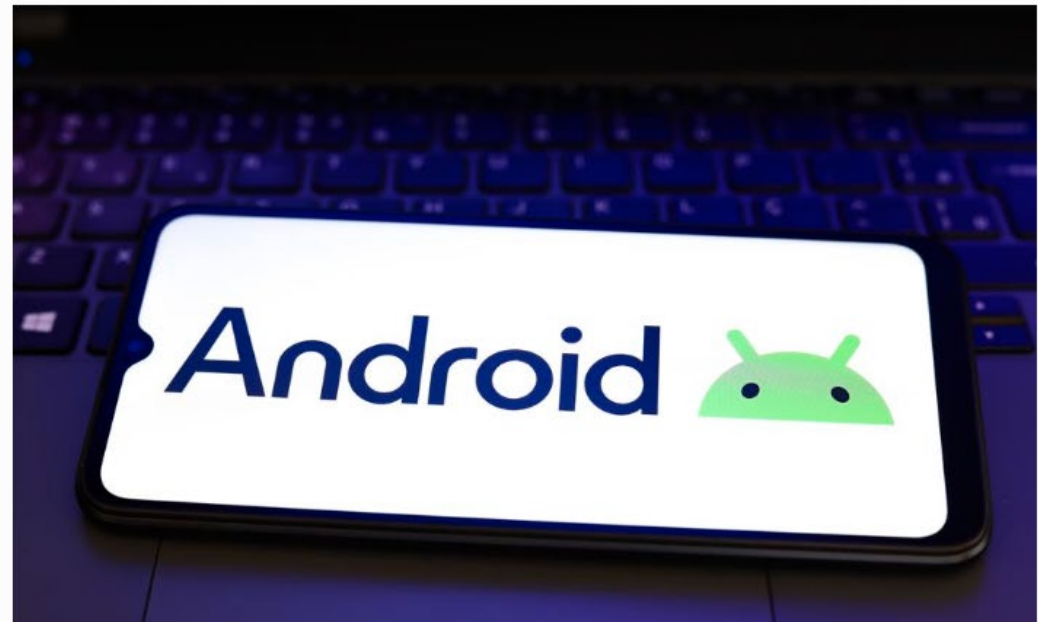
Follow Author

By [Zak Doffman](#)
Published Nov 05, 2025

Published Oct 15, 2025, 06:21am EDT, Updated Oct 15, 2025, 09:58am EDT

Share Save

"The n
any su
Go
Once I
auther
send a
evid
Next, I
point,
issu
bull



Is this real? Google
GETTY IMAGES

Google has in

Coll
Stop
Your

By Zak Doffman
Published Nov 05,:

"The n
any su

Once l
authel
send a

Next, i
point,
issu
bull



Is this real? Google
GETTY IMAGES

Google has in

Android 2FA Samsung Gala

By Davey Winder, Senior Contributor. © D
Published Oct 15, 2025, 06:21am EDT, Updated O

Share Save



Password-Manager: Datenklau durch Browser-Erweiterungen

Ein IT-Forscher hat eine Lücke in Browser-Erweiterungen von Passwort-Managern entdeckt, die das Stehlen von Zugangsdaten erlaubt.

🇬🇧 🔊 🖨️ 💬 206



Coll

Stop Your

By Zak Doffman

Published Nov 05

"The n
any su

Go

Once I
auther
send a

evic

Next, I
point,

pat

issu

bul



Is this real? Google
GETTY IMAGES

Google has in

BSI: Checkliste für Vorgehen bei geknackten Konten

Das BSI hat eine Checkliste für Privatanwender veröffentlicht, die Hilfestellung zu Maßnahmen bei geknackten Zugängen liefert.



206



Arch Browser-

von Passwort-Managern



Hauptanforderung

- Einen Menschen zu einer digital Identity verbinden
 - Wie stellen wir sicher, dass dieser eine Mensch, dass ihm zugewiesen Benutzerobjekt verwendet?
- **Strong secure Authentication against** **Credential Theft & Phishing resistant**
- Hardware ist besser als Software
- Two factor – multiple factors → **HABEN – WISSEN – SEIN**
 - Risk based authentication
 - Context based authentication als Ergänzung
- **Non-repudiation** (asymmetric)
- Expiration
- Synergien (physical access, money, signing, encryption)

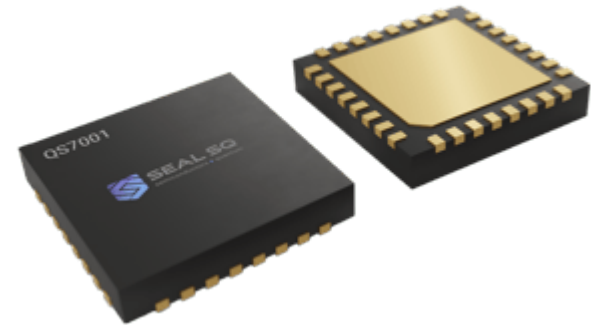
Strong Authentication User

- Asymmetrische Algorithmen
- Highest protection of private keys
- Credentials could not be stolen
- Non-reputation
- Phishing resistant

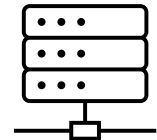
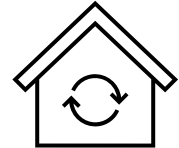


Geräte

- Desktop / Laptop
 - Win
 - MacOS
 - LNX
- Mobile devices (iOS v android)
 - Smartphone
 - Tablet
- Virtual devices
- Other OT devices
- API credentials

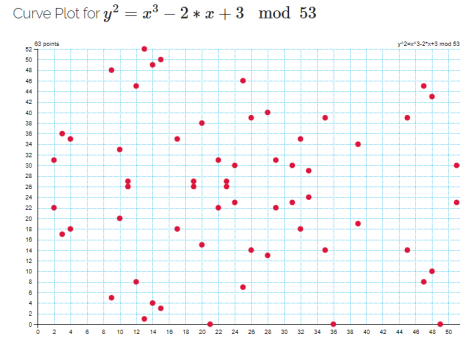


- On premise ressources
 - Active Directory
 - Server
 - Appliances
- Cloud Services
 - IdPs (MS EntraID, Okta, Ping, ... STA, AWS, GCP)
- Applications
- Appliances



Authentication Technology and Authenticator

- Cryptography
 - OTP AES or SHA
 - FIDO just ECC
 - SC RSA or ECC
- Protection key material
 - Software / Hardware / second factor / Biometrie
- Operation
 - Expiration, reset, lock account
- Enrollment
- Recovery
 - Backup der secrets in der Cloud?



FIDO

- FIDO2 v FIDO2.1
- Just public private key based on ECC
- Certified device
- Consumer product
- Enrolment user oriented
- Recovery – not existing – re-enrollment
- Revoke token
- Unlock token

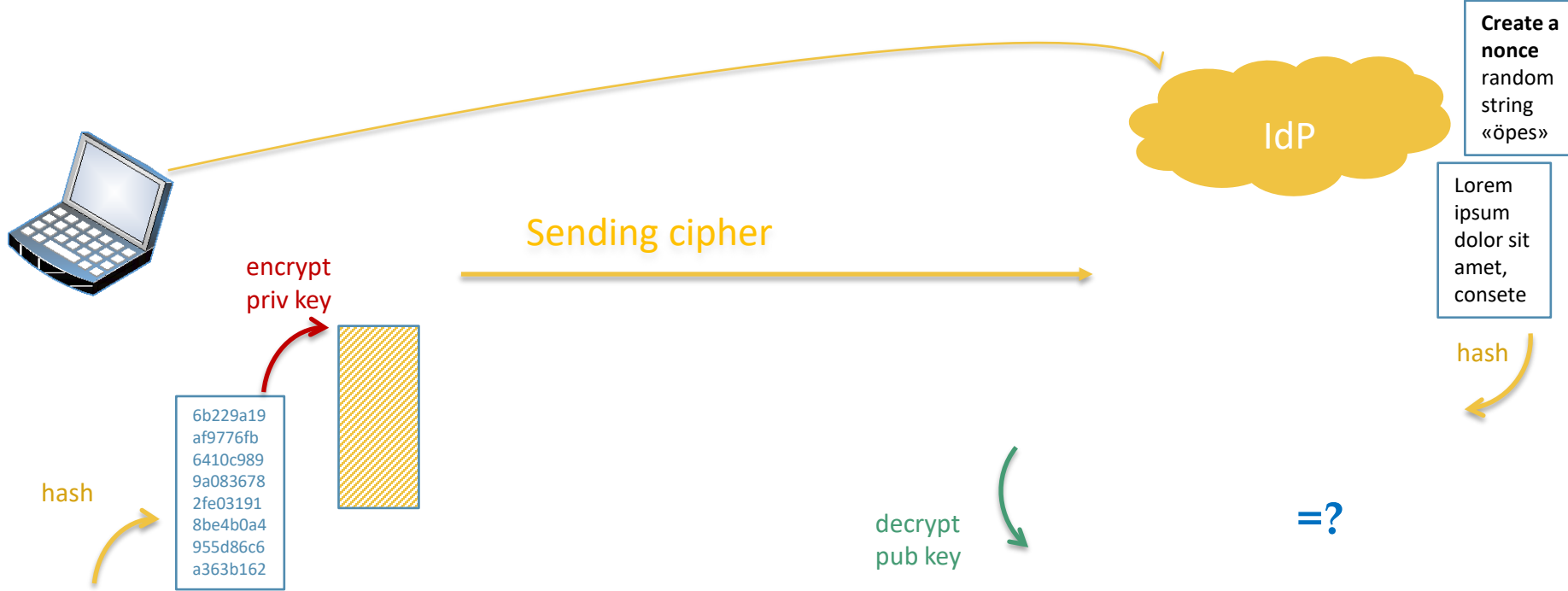


FIDO2.1 Enterprise

- Tec-bite video
<https://www.tec-bite.ch/fido-im-unternehmen/>
- [WebAuthn](#) (Browser)
- [CTAP \(Apps\)](#) - [Client to Authenticator Protocol](#)
- „Ursprünglich war geplant, dass Daten wie die eindeutige und geheime Primärschlüsselkennung eines Authentifikators (Security-Token) in Klartext nicht auslesbar sind und immer und ausschließlich am Authentifikator verbleiben.^[3] Dieses Grundprinzip wurde allerdings zugunsten des Komforts in bestimmten Implementierungen wie bei den auf [FIDO2](#) basierenden und ohne physische Authentifikatoren auskommenden [Passkeys](#) verworfen.“



Passwordless - asymmetric Authentication



Non-repudiation

- User is owner of the private key!
- Nonce was not manipulated!



Passkey – FIDO without Token

- Ala FIDO – public key cryptography
- Private key synch through cloud and distributed between devices
- STA MobilePASS+ auch mit Thales STA oder SAS on premise
- Passkey im Browser MS Edge
- MS Authenticator App
- Secure element
 - https://de.wikipedia.org/wiki/Secure_Element
 - Google Titan
 - Samsung Knox - SE
 - “Apple Passkeys are automatically backed up through iCloud Keychain, which securely stores your passkeys and syncs them across all your Apple devices. iCloud Keychain is configured for end-to-end encryption, so only your trusted device has access to the keychain-stored passkeys.”

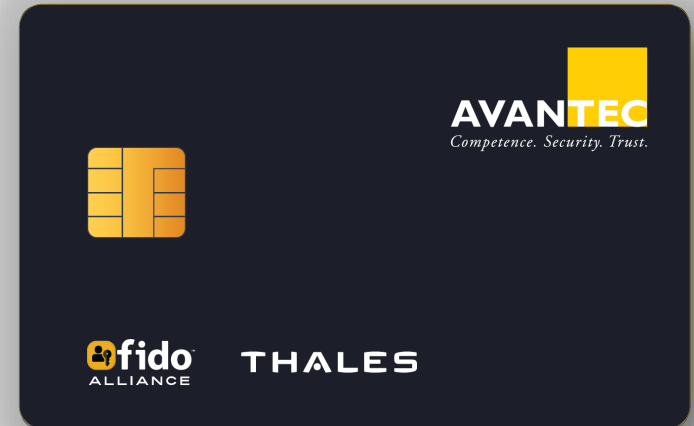


Smart Card

- Since 1950s
- ID-1 oder SIM-Kartenformate
- Hybrid Smart Cards
 - cba, FIDO, RFID (legic/MiFare), Layout

Zertifikatsbasierte Authentisierung

- Private keys always protected!
- Unlock, Recovery, Enrolment – enterprise like
- **RFID**
 - Physical access
 - Payment
 - Secure printing
 - Time recording
 - ...



Comparing cba and FIDO2

Certificate based auth with SC

- Private key not exportable
- Zentrales richtlinienbasiertes Ausstellen
- cba
 - Trust
 - Validity
 - Revocation
 - Subject / san
 - Key usage / EKU
 - RSA or ECC – key length
- PIN Policy
- Unblock card / PIN reset
- recovery

FIDO / passkey

- Key attestation
- Passkey - Privater Schlüssel wird in die Cloud und auf die Geräte synchronisiert
- Just private key authN – like ssh priv key auth
- Key renewing
- Benutzerseitiges registrieren der Token
 - Unblock Token / PIN Reset only Thales EF
- Recovery if lost / damaged → re-enrolment

Security Chips

- Smart Card – tec-bite.ch – today *IDPrime 930 (FIPS) / 940 (CC)* – *eToken Fusion*
 - first SC with PQC Thales Public ID-Card / Infineon SLC27
- HSM – tec-bite.ch - most vendors PQC ready
- TPM - [Trusted Platform Module](#) - Trusted Platform Module Infineon Optiga SLB 9672
- TEE - [trusted execution environment](#)
- Samsung [SE - Secure Element](#) - S3K250AF starting 2020 - S3SSE2A – 2025 (PQC)
- Google [Titan-M](#)
- Apple [Secure Enclave](#) in the SoC



Karten und Token



SafeNet IDPrime
FIDO



SafeNet eToken
FIDO



SafeNet eToken
FIDO



QC resistant ID-Cards

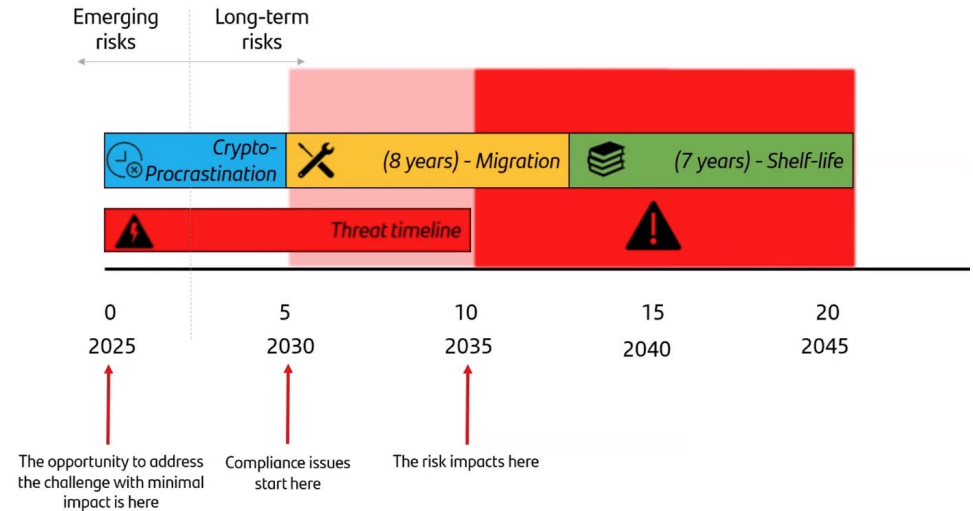
Quantum-resistant
smartcard



PQC Migration

- HNDL, digital Signing, Authentication
- Inventarisierung
- Replacing hardware
- Replacing or Update Software
- New Algorithms ML-DSA, SLH, FN

Augmented Mosca's theorem



→ 2030 deprecated → 2035 disallowed

Windows Hello for Business – WHfB and others

- Key-based
- cba – certificate based authentication

- On TPM

- Enrollment, Recovery ?

- Hypr
- Specific Apps on mobile devices
 - MS Authenticator,

- Reduce the number of managed accounts

- Identity Manager
 - HR controls Roles, Memberships, password sync

- Kerberos (Smart Card Logon Windows)
 - Central AuthN
 - Asymmetric protection kerberos tickets

- SAML, OIDC

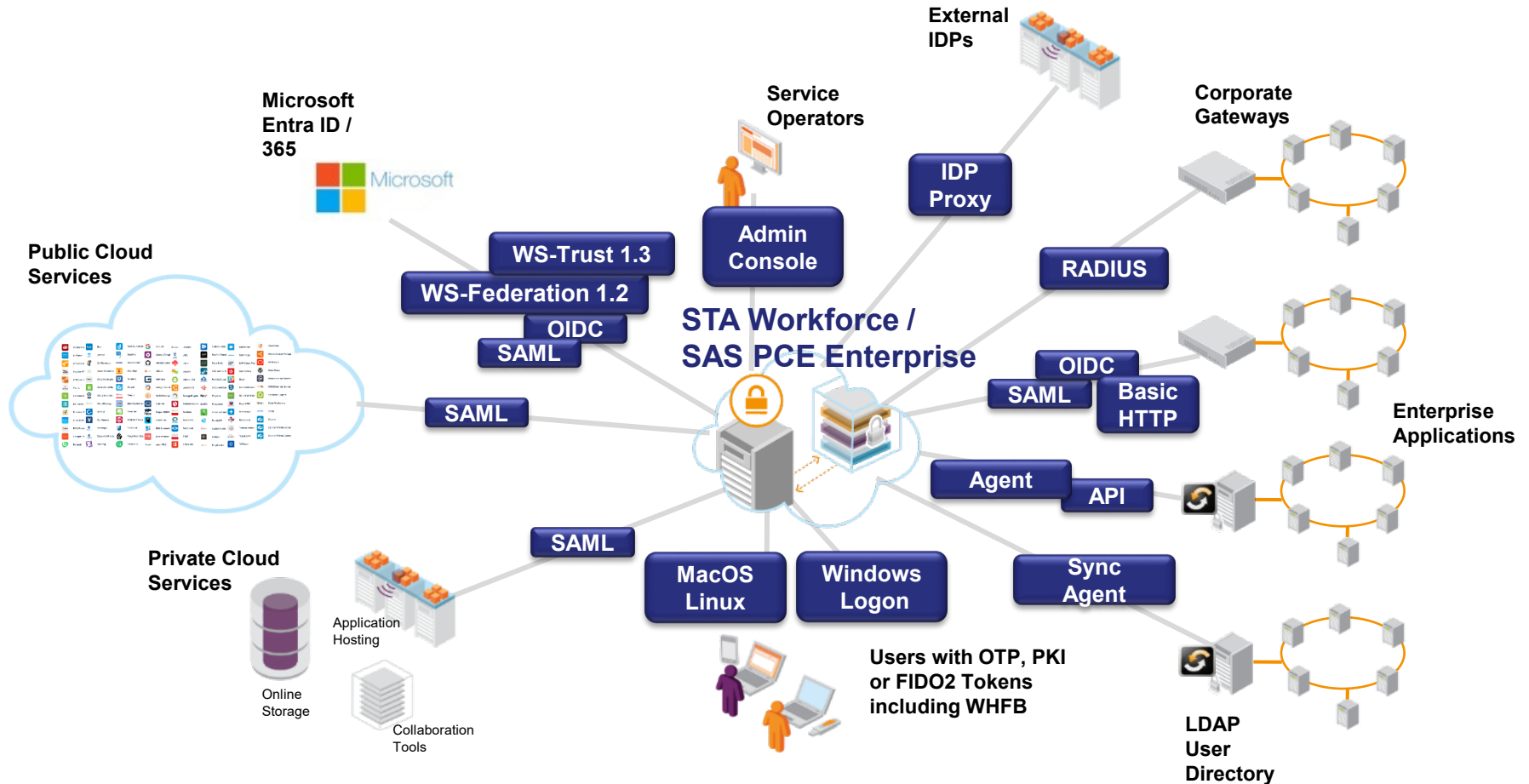
- IdPs
 - Trennung Authentication and accessing resources (SP)

SafeNet Trusted Access & SafeNet Authentication Services

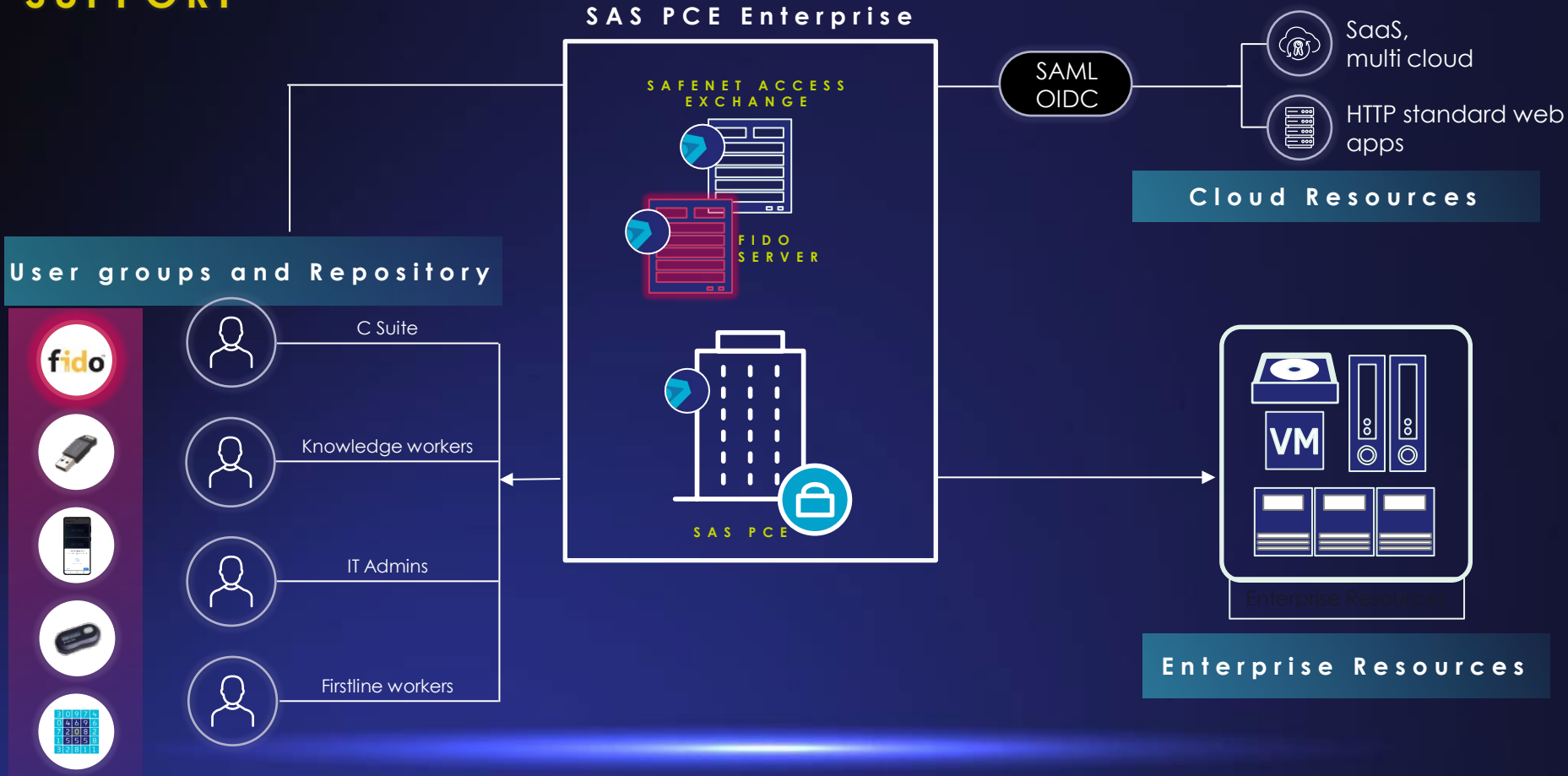
- STA – Cloud Services
 - AVANTEC Product since more then 13 years
 - Authentication – Identity Provider
 - Conditional Access Portal for Application & Services
- SAS – on premise IdP
 - Authentication und umfangreiche Integration in Enterprise Applikationen und Dienste
- Beide vielfältige Authentisierungsmöglichkeiten von OTP → passwordless



SafeNet Trusted Access (STA) Workforce or SAS PCE Enterprise



SAS PCE Enterprise with FIDO Support



Andere Themen bezüglich der Credentials

- Wo und wie werden **Credentials** genutzt und wie sind verknüpft?
 - Auditing
 - EDR für credentials
- Ausführung privilegierter Aufgaben / Prozesse ohne Eingabe von admins Creds
- Nutzung von **priviligierten / administrative Accounts**
 - Not on daily used Client - **PAW**
 - On Server, Appliances - Cloud
- Permission on demand
 - Entfernen von Rollen oder Gruppenmitgliedschaften, wenn sie nicht gebraucht werden

EDR

PAM

Auditing - Follow the credential usage

- Different Credentials – one Identity
 - Collecting data from different IdPs, DBs, Services
 - Check quality of credentials
 - Check against breach lists
- Analysing usage log
- [Identity Security Insights](#)

ISI

- AWS
- GCP
- AD, EntraID
- Github
- Okta
- PingOne
- Salesforce
- ServiceNow
- DataBricks

Elevation

- Administrative rights without input credentials
- No elevated user rights
 - Administrative rights per task / application
- Detecting usage of admin credentials on Clients

EPM

Privilege administrative accounts - PAW

- Client Access to Gateway's
- Strong Authentication
- Advantages
 - Trennung Client User and administrative Credentials
 - Store administrative credentials, cookies not on daily used Wkst
 - Hiding credentials, not readable for Client, just using
 - Credential rotation
 - Easy using asymmetric Auth or OTP
- **Target systems**
 - Windows Server
 - Application
 - DBMS
 - Web-UI
 - Linux
 - Appliances
 - Cloud instances too
 - OT systems
 - IoT

PRA

“Jede Identität muss heute als privilegiert gelten”

Control credentials and Roles / permissions

- Remove permissions, group membership, Roles (RBAC)
 - Directly on server, AD, groups and Roles in MS EntraID

- JIT access to resources
 - Approval
 - Change group or role membership
 - Auditing
 - Integrated in our access concept

Entitle

Control credentials and Roles / permissions

- Remove permissions, group membership, Roles (RBAC)
 - Directly on server, AD, groups and Roles in MS EntraID

Entitle

- JIT access to resources
 - Approval
 - Change group or role
 - Auditing
 - Integrated in our access



Active Directory



Google Workspace



JumpCloud



LDAP



Microsoft 365 Admin Center



Microsoft Entra ID (Azure AD)



Okta



OneLogin