



# Security Changes Everything.

Roger Mahler – PreSales Consultant Thales

Dirk Gluch (Principal Security Engineer) . [gluch@avantec.ch](mailto:gluch@avantec.ch)

# AVANTech-Day 2026



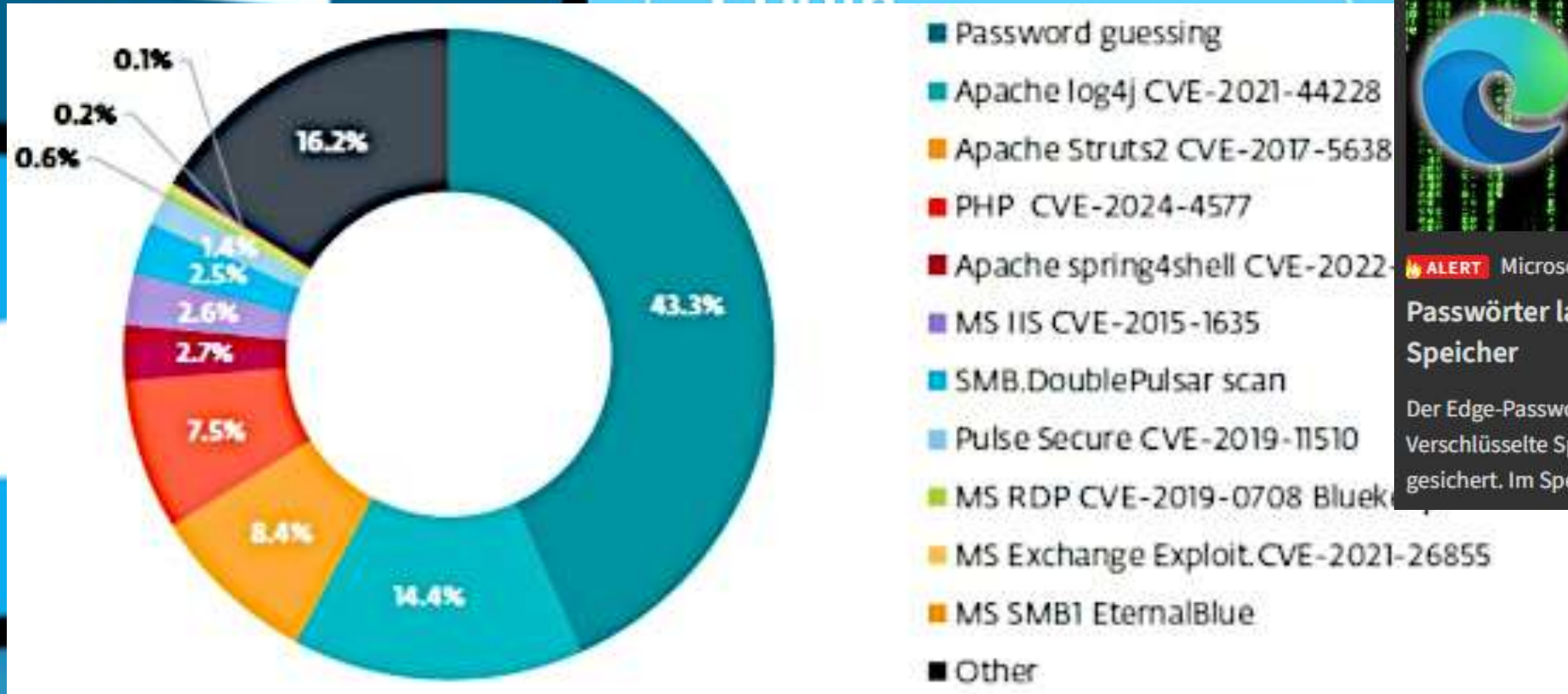
**Authentication –  
passwordless, strong,  
secure**

**Dirk Gluch**

Principal Security Engineer,  
AVANTEC



# WORLD PASSWORD DAY



**ALERT** Microsoft Edge  
**Passwörter landen als Klartext im Speicher**  
Der Edge-Passwort-Manager wirkt sicher: Verschlüsselte Speicherung, von Windows Hello gesichert. Im Speicher liegt aber Klartext.

**When ever possible – do NOT use passwords**

# Agenda

- Welcome / Introduction
- AVANTEC SC usage
  - Smart Card Logon Windows Desktop, pwd, wiki, projects, LanCrypt
  - FIDO Logon PRA
  - FIDO & SC on mobile device
  - Authentication IDPrime + NFC + FIDO
- Background / Explanation – theory
  - AuthN, Signing, Encryption
- Challenges
  - What is passwordless (asymmetric authN)
  - FIDO versus Passkey
  - Advantages SC versus FIDO2.1 EF (certificates versus just public private keys)
- Enrolment SC versus FIDO Token
  - Registering card / token for unblocking & recovery
- What's happen next QCRC or PQC

# Zero Trust starts with secure AuthN

## Aktuelle Lage

Ransomware ist nach wie vor eine der grössten Bedrohungen für viele Unternehmen. So ist z.B. die Gruppe Akira wieder besonders aktiv. Laut NCSC-Meldung vom Oktober 2025 wurden bereits 200 Schweizer Unternehmen erfolgreich durch die Gruppe attackiert, und dies allein in den letzten Monaten. Die Angreifer entwenden zuerst sensitive Unternehmensdaten, bevor sie Systeme in den meisten Fällen auch verschlüsseln. Wird kein Lösegeld gezahlt, droht zusätzlich noch die Veröffentlichung der Daten auf einer Dark-Web-Plattform. Besonders oft gelingt der Zugriff über veraltete Software oder über Fernzugänge wie VPN- oder Remote-Desktop-Verbindungen, die nicht durch Mehrfaktor-Authentifizierung abgesichert sind. [1]

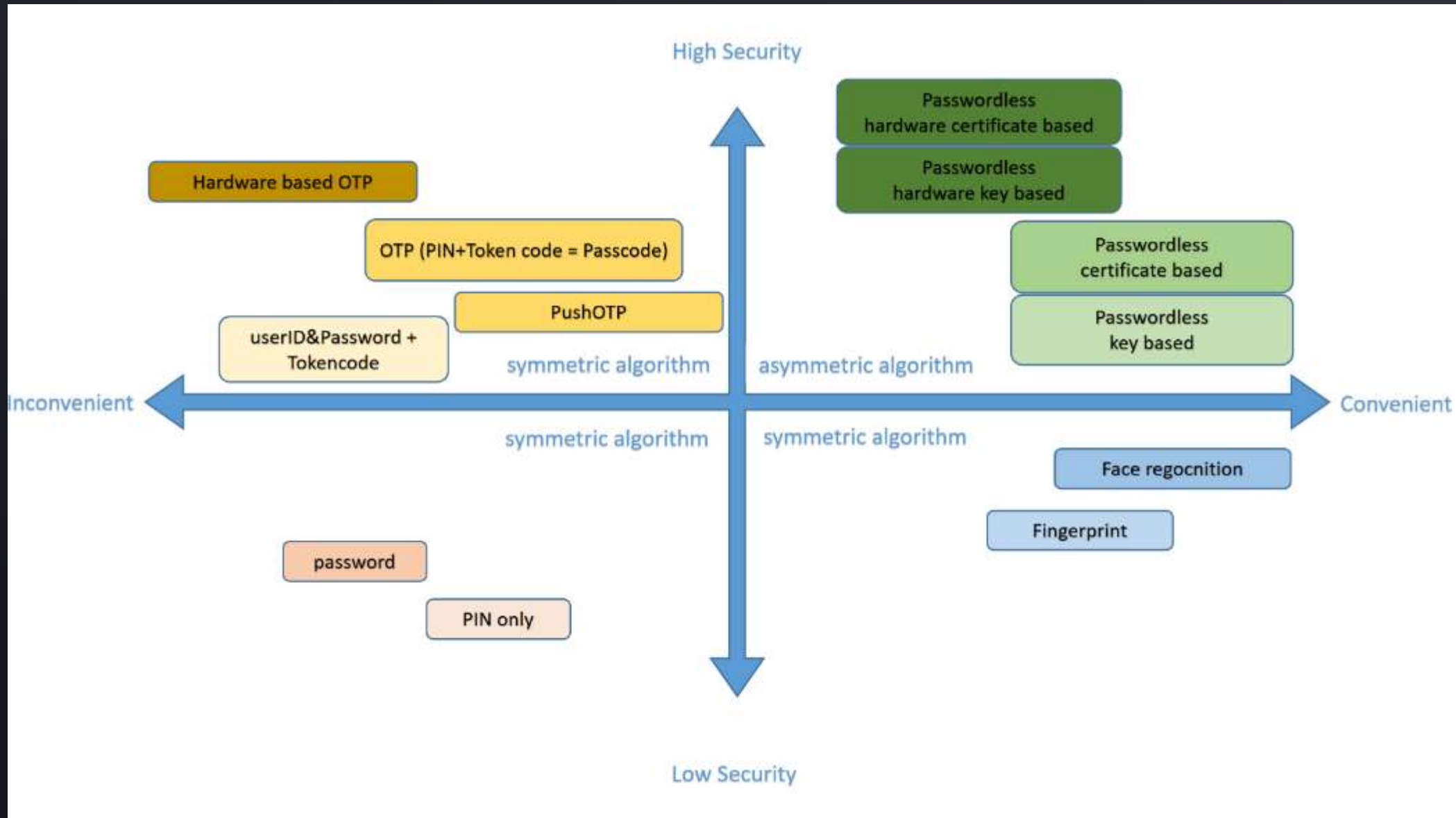
Das Thema identitätsbasierter Angriffe ist an sich nicht neu und wurde im Jahr 2024 schon vermehrt ausgenutzt. Im Jahr 2025 hat sich die Situation aber nochmal wesentlich verschärft, so sah Microsoft bereits im ersten Halbjahr einen Anstieg von 32%. [2] Die Angreifer nutzen dabei die generativen KIs, um ihre Phishing-Kampagnen, Social-Engineering-Aktivitäten und auch die Automatisierung der Angriffe auf das nächste Level zu heben.

Demgegenüber steht die Herausforderung von immer grösser werdenden Angriffsflächen, u.a. durch Cloud-Dienste und komplexe Lieferketten.

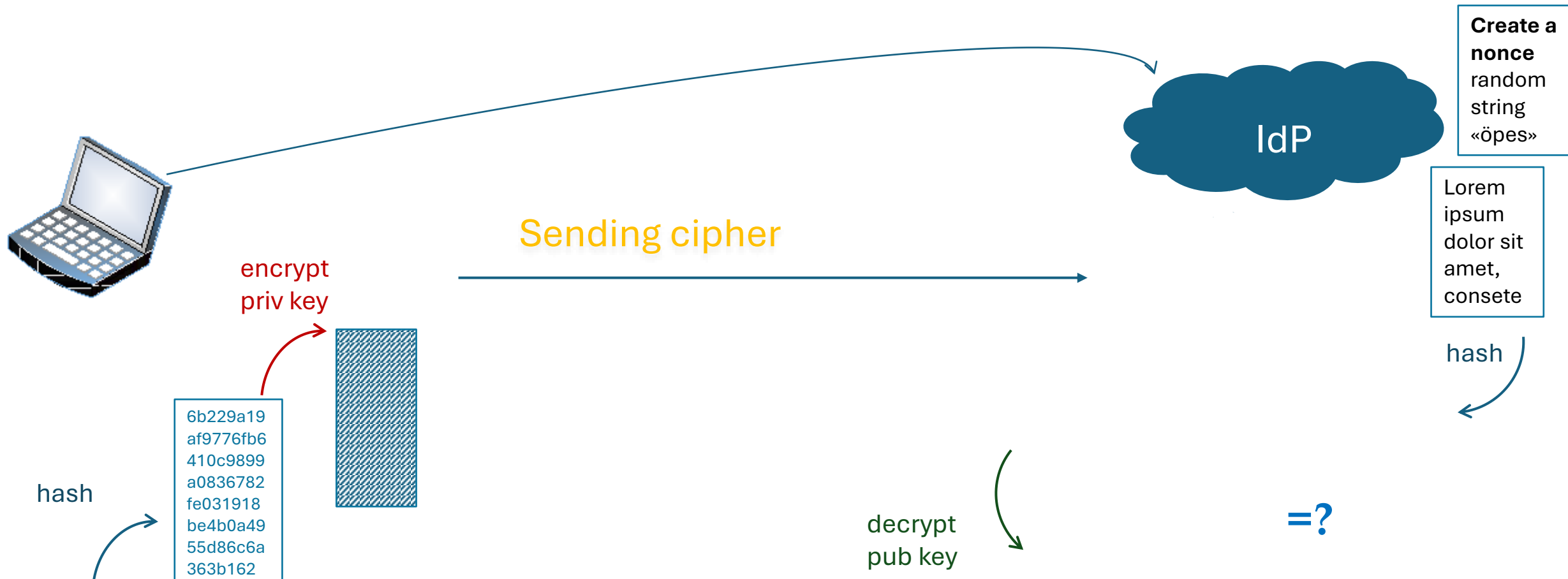
# Main aspect - security

- passwordless
  - No symmetric keys or secrets that could be stolen
  - asymmetric / public key cryptography
  - Not transfer of symmetric credentials (include hashes) or storing creds or seeds
- hardware based
  - anti-tampering protection
  - cryptographic operation on secure device / independent of Client-OS
  - Real 2FA
- Protection against
  - Key logger
  - Info stealer
  - Phishing resistant
  - Man-in-the-Middle attacks

# What is passwordless



# Passwordless - asymmetric Authentication



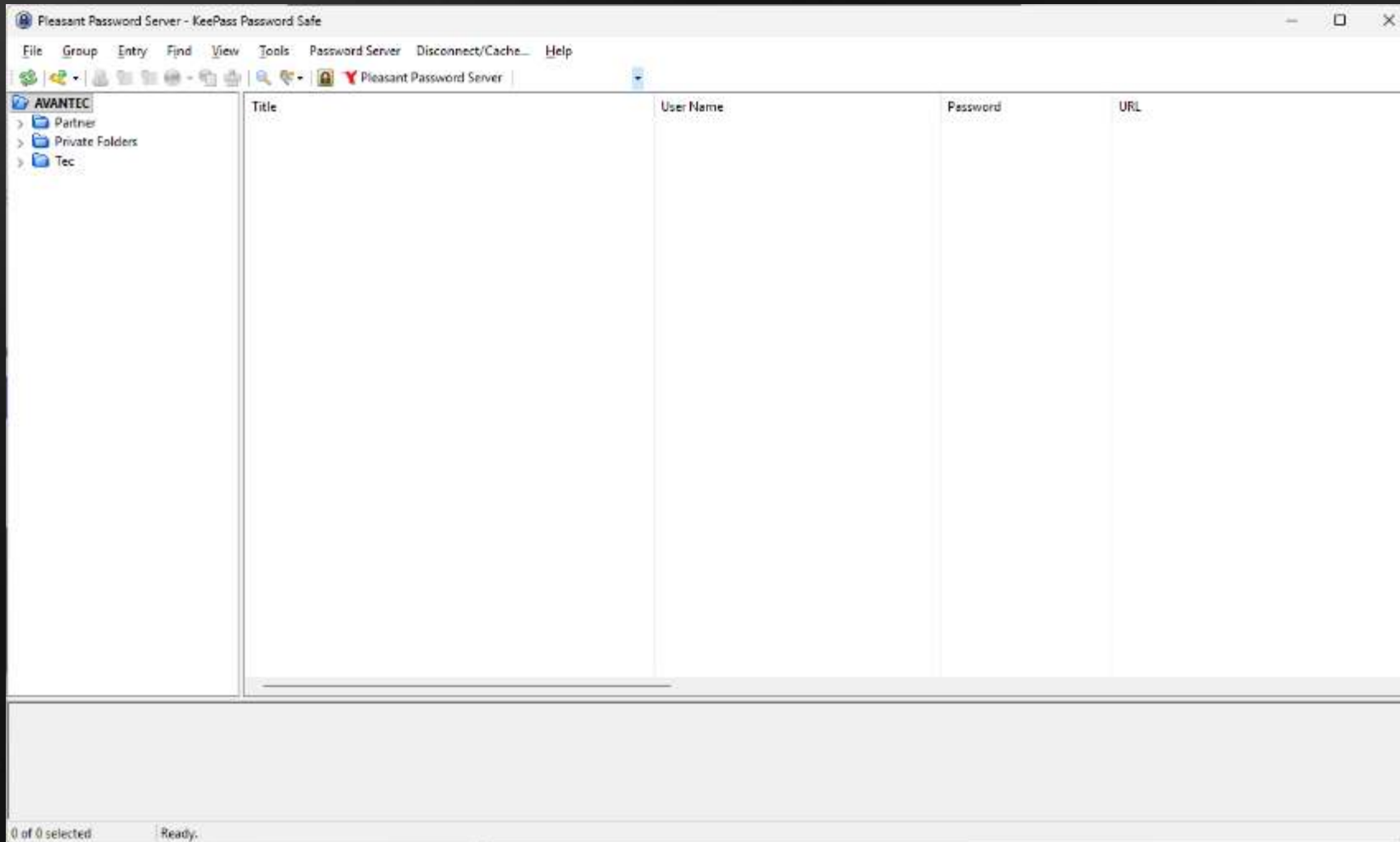
## Non-repudiation

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



# AVANTEC use cases

- Smart Card Logon
  - Desktop Logon - IDPrime + NFC + FIDO + RFID (legic)
  - [Zscaler, M365, Outlook / Teams] based on SAML
  - Logon to different resources
    - Internal Websites via SAML (ADFS) – Wiki, Passwordsafe, ...
    - Pathfinder -
    - LanCrypt
    - SC removable behaviour
- FIDO Logon
  - PRA
  - Websites
- Other AuthN – Mobile devices
  - MS AuthN, MobilePASS+ (STA Portal)
  - Asymmetric & passkey
- Challenges
  - Enrolment, unblocking, recovery token, keys



# Logon PRA with FIDO-Token - ac

Privileged Remote Access Console - pra - Dirk Gluch

File Help

Home

Jump Items Vault Accounts Queues Group Chat

Jump Create Copy... Remove Properties... Export

Add Filter Search Jump Items...

My Jump Groups	Name	Hostname / IP	Jump Method	Comments	Group	Tag	Status	Last Accessed
Recently Used	Blue DC-02	10.240.0.112	RDP Remote RDP		Personal		Available	
Jump On Startup (0/10)	BLUE-ADFS01	BLUE-ADFS01.b	RDP Remote RDP		external-system		Available	10/30/2025 01:04:52 pm
Personal	dc - avanatec.lab	10.240.0.11	Remote Jump		Personal		Unavailable	11/08/2024 10:43:55 am
external-system	DC-01	10.240.0.101	RDP Remote RDP		Personal		Available	
Gateways	DC-BLUE	10.240.0.111	RDP Remote RDP		Personal		Available	
	EnergieThun	10.20.102.158	RDP Remote RDP		Personal		Available	08/06/2025 03:22:46 pm
	Fortigate SSH	10.111.1.1	Shell Jump		Gateways	Fortigate	Available	04/24/2023 12:13:33 pm
	Fortigate Web	10.111.1.1	Web Jump		Gateways	Fortigate	Available	08/19/2025 04:40:25 pm
	ICS	104.101.40.42	Web Jump		Gateways	ICS	Available	07/24/2024 09:33:01 am
	Issuing-AVALAB	10.240.0.103	RDP Remote RDP		Personal		Available	
	Issuing2 - w2k25	10.240.0.125	RDP Remote RDP		Personal		Available	
	Luki	10.241.0.132	RDP Remote RDP		Personal		Available	
Michael	Luki - win11-Demo	win11-c.	RDP Remote RDP		Personal		Available	03/05/2025 01:42:55 pm
	Techie	10.21.0.20	RDP Remote RDP		Personal		Available	01/05/2026 03:08:46 pm
	Win-C - PMC	10.241.0.132	Remote Jump		Personal		Available	
	Win11-B-rdp	10.241.0.112	RDP Remote RDP		Personal		Available	06/29/2023 03:59:34 pm
	Win11-B-rj	10.241.0.112	Remote Jump	real 2FA	Personal	2FA	Available	03/22/2023 01:40:58 pm
	with Approval	10.240.0.103	RDP Remote RDP		Personal		Unavailable	

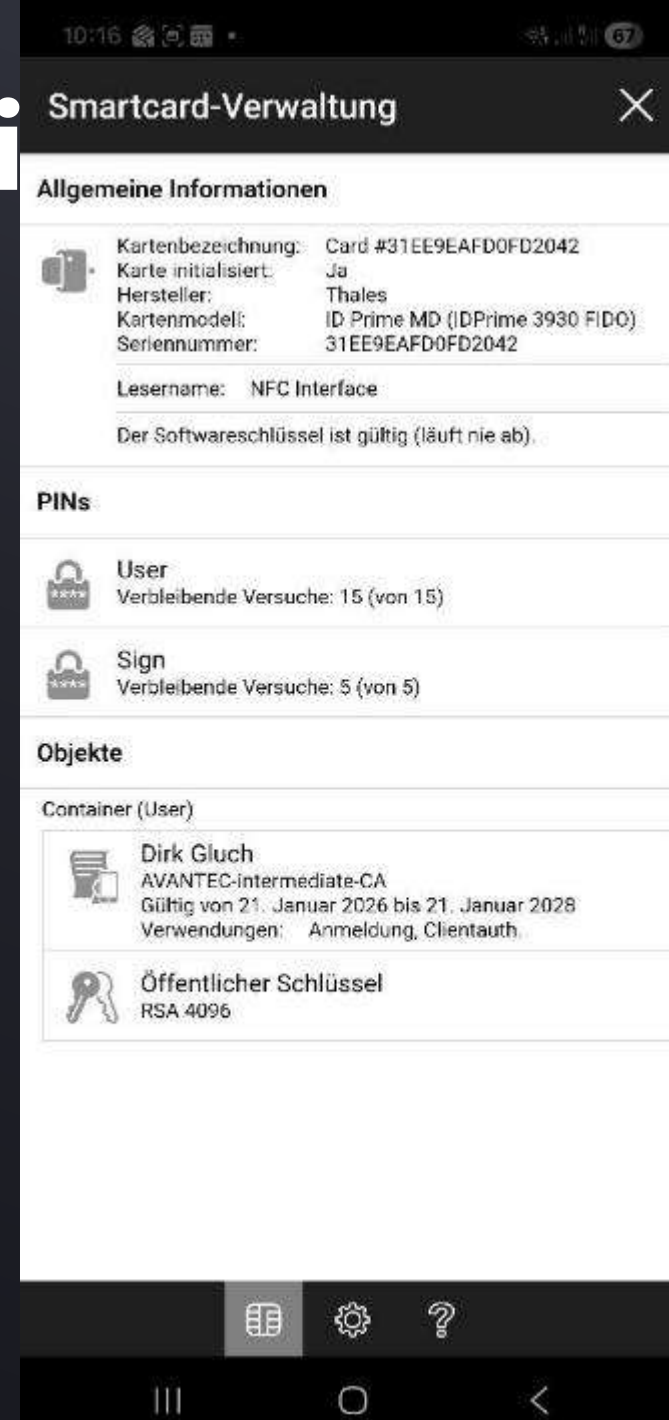
# Logon PRA with FIDO-Token - web

The screenshot displays a web interface for managing jump groups. On the left, there is a sidebar with 'Jump Groups' and a search bar. The main area shows 'My Jump Groups' with a search bar and a '+ Create Jump Shortcut' button. Below this is a table with 18 items. The table columns are Name, Hostname / IP, Jump Method, Group, Status, and Last Accessed. The status column shows 'Available' or 'Unavailable'.

Name	Hostname / IP	Jump Method	Group	Status	Last Accessed
BLUE-ADFS01	BLUE-ADFS01	Remote RDP	external-system	Available	10/30/2025 01:04:52 PM
Blue DC-02	10.240.0.112	Remote RDP	Personal	Available	
DC-01	10.240.0.101	Remote RDP	Personal	Available	
dc -	10.240.0.11	Remote Jump	Personal	Unavailable	11/08/2024 10:43:55 AM
DC-BLUE	10.240.0.111	Remote RDP	Personal	Available	
EnergieThun	10.20.102.158	Remote RDP	Personal	Available	08/08/2025 03:22:46 PM
Fortigate SSH	10.111.1.1	Shell Jump	Gateways	Available	04/24/2023 12:13:33 PM
Fortigate Web	10.111.1.1	Web Jump	Gateways	Available	08/19/2025 04:40:25 PM
iCS	194.191.80.42	Web Jump	Gateways	Available	07/24/2024 09:33:01 AM
Issuing2 - w2k25	10.240.0.125	Remote RDP	Personal	Available	
Issuing-AVALAB	10.240.0.103	Remote RDP	Personal	Available	
LUKI	10.241.0.132	Remote RDP	Personal	Available	

# Demo with mobile device

- Logon to Teams with SC
- Using FIDO for
  - Website
  - RS?



# Advantages of separate hardware

- Keys on a hardware device – anti-tampering protection
  - Physical (Legic, MiFare, Desfire, ...)
  - Logical (cba / PKI)
  - NOT just software protection
- Communication between computer and key holder device secured
  - Authentication and encrypted
  - Relevant signing operation on key holder device
  - PIN / passphrase transferred locally
- Strong authentication if PIN is enforced = 2FA
- Phishing resistant
- Protected against key logger or Info stealer
- Protected against attacks on service provider
- No symmetric keys / secrets - passwordless



# Thales Smart Cards – ID-1 format

- IDPrime 930 (FIPS) versus 940 (CC) (contact based cba)
- IDPrime 931 930+ RFID (MIFARE, DESFire, HID, ...)
- IDPrime 941 940 + RFID
- IDPrime 3930 versus 3940 (contact based and NFC cba)
- IDPrime 930C
- IDPrime Bio (FIDO)
- Combination
  - IDPrime 39x0 + FIDO
  - IDPrime 39x0 + FIDO + Legic v DesFire
- eToken Fusion
  - Based on IDPrime (cba and FIDO)
  - NFC
  - BIO



# Thales IDPrime (PKI - cba)

- X.509 Certificate based usage (not just authentication) – PKI cards
- IDPrime 930 / 3930
- IDPrime 930C (upcomming)
  - FIPS 140-3 (listed in the [validation program](#))
  - RSA 4096
  - ECDSA, ECDH up-to P-521
  - Mit FIDO2.1
- IDPrime 940 / 3940
  - Common Criteria EAL6+
- Europe's first PQC ready card (ID card)
  - <https://www.thalesgroup.com/en/news-centre/press-releases/thales-launches-europes-first-certified-smartcard-ready-quantum-age>



# Thales ID card with QCRC (PQC)



# Thales IDCore & PIV

- IDCore 230 / 3230 under NIST Validation

[https://cpl.thalesgroup.com/sites/default/files/content/product\\_briefs/f024-02/safenet-idcore-230-3230-pb.pdf](https://cpl.thalesgroup.com/sites/default/files/content/product_briefs/f024-02/safenet-idcore-230-3230-pb.pdf)

- IDPrime PIV 4.0 FIDO under NIST -  
<https://cpl.thalesgroup.com/de/acc>

- IDPrime 930C

- <https://csrc.nist.gov/Projects/cryptographic-modules-in-process/modules-in-process-list>



# Custom Cards by Thales DIS BPS



- Design and production of smartcards w/wo contact in LF-, HF- and UHF-frequency ranges certified ISO 9001:2015
- Own Dual-Interface- DIS (soldering technology) and hybrid cards, also embedding service
- Dual-Interface-Coil-on-Module
- Twin- cards with any combinations of chip available like MF, Desfire, Hitag, IDPrime with FIDO...
- In-house development of applets, emulation and testing
- Technical consulting services incl. Legic-Partnership



## Our features for you:

- Layout in any colour, wide spread of materials
- Printing in Thermotransfer, Inkjet, special lack
- Laser engraving as standard option (both sides)
- Special features like self printing foils, magnetic stripes, holographics

Contact us on: [www.thales-dis-bps.de](http://www.thales-dis-bps.de)



# Credentials Management with vSEC:CMD from Versasec

# Smart Card enrollment

- [Setting up vSEC:CMS E](#)
- [Managing Hardware C](#)

vSEC:CMS - Lifecycle

File Go Help

**versasec** Lifecycle Actions v Repository v Templates v Options v

Home > Lifecycle

### 1. Select a Credential

Use the credential inserted in

Gemalto USB SmartCard Reader 0

User ID:  
Lukas AVANTEC Search

### 2. Select Process

```
graph TD; Unregistered --> Registered; Registered --> Unregistered; Registered --> Issued; Registered --> Active; Registered --> Inactive; Registered --> Locked; Issued --> Active; Active --> Inactive; Inactive --> Locked; Inactive --> Unregistered; Locked --> Unregistered; Locked --> Retired; Locked --> Revoked; Locked --> Deleted; Retired --> Unregistered; Revoked --> Unregistered; Deleted --> Unregistered;
```

Performing process...

### 3. Execute Process

Selected process(es): Register, Issue

Execute Batch

### Selected Credential

Card serial number:	F42F 2A79 6240 00B2 F42F 2A79
Card template:	User vSEC SmartCard - AD User (Minidriver)
Card status:	Assigned, Cert enrolled, Issued, Initiated
User ID:	Lukas AVANTEC
Certificate(s):	CN=Lukas AVANTEC, OU=...

### Smart card successfully issued

- ✓ Smart card successfully registered
- ✓ Smart card administrator key successfully set
- ✓ Card assigned to [Lukas AVANTEC](#)
- ✓ PIN policy for [Primary credential PIN](#) successfully updated
- ✓ [VSECCMSUserSmartcardLogon](#) certificate successfully enrolled
- ✓ [Primary credential PIN](#) successfully initialized
- ✓ Card successfully initiated
- ✓ Data successfully exported to [data export](#)
- ✓ CMS Authentication keys successfully updated ([1 keys added](#))

ID: VEZK-7497

OK

vSEC:CMS - Lifecycle

File Go Help

versasec Lifecycle Actions v Repository v Templates v Options v

Home > Lifecycle

### 1. Select a Credential

Use the credential inserted in

Gemalto USB SmartCard Reader 0

User ID:

F42F 2A79 6240 00B2 F42F 2A79

### 2. Select Process

```

graph TD
    Unregistered --> Registered
    Registered --> Issued
    Registered --> Active
    Registered --> Inactive
    Registered --> Locked
    Issued --> Active
    Active --> Inactive
    Inactive --> Active
    Inactive --> Locked
    Locked --> Inactive
    Locked --> Deleted
    Active --> Deleted
    Inactive --> Deleted
    Locked --> Deleted
    Retired --> Issued
    Revoked --> Issued
    Revoked --> Deleted
    Deleted --> Retired
    Deleted --> Revoked
    Deleted --> Unregistered
  
```

### 3. Execute Process

Selected process(es):

### Selected Credential

Card serial number: F42F 2A79 6240 00B2 F42F 2A79  
 Card template:  
 Card status:  
 User ID:

### Selected Credential Template Description

smtp4dev

smtp4dev  
rob@rnwood.co.uk

Messages Sessions

Received	Subject	To

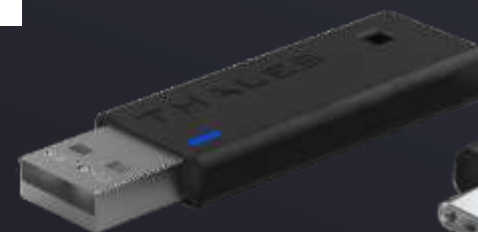
# Thales IDPrime BIO (FIDO)

- Mit FIDO2, geräteinterner Biometrie und NFC
- Nach FIDO 2.1 Level 1 und Chip CC EAL6+ zertifiziert
- Benutzerverifizierung mit PIN und Biometrie (Fingerabdruck)
- Kontakt- und kontaktlose Modi
- Unterstützt von Windows, Mac, Linux, Android und iOS
- Kompatibel mit allen Diensten, die WebAuthn und U2F unterstützen



# Thales eToken

- USB devices = Smart Cards + SC Reader
- eToken 5110+
  - Cba based on IDPrime 930
- eToken Fusion
  - IDPrime + FIDO 2.1 Enterprise Features
  - NFC
  - BIO
  - PIV or FIPS 140-3
  - USB-A, USB-C and NFC
- Made in Europe (France)



# Advantages FIDO

- Asymmetric cryptography
  - No symmetric secrets or data on cloud over the net
- Phishing resistant
- Protecting against man-in-the- middle attacks
- Short PIN or passphrase locally
- No need to change password regularly
- No long complex passwords
- No certificates and PKI needed





## Comply with market regulations

- FIDO2
- Common Criteria
- eIDAS
- French ANSSI
- FIPS 140-2
- FIPS 140-3
- FIPS 201

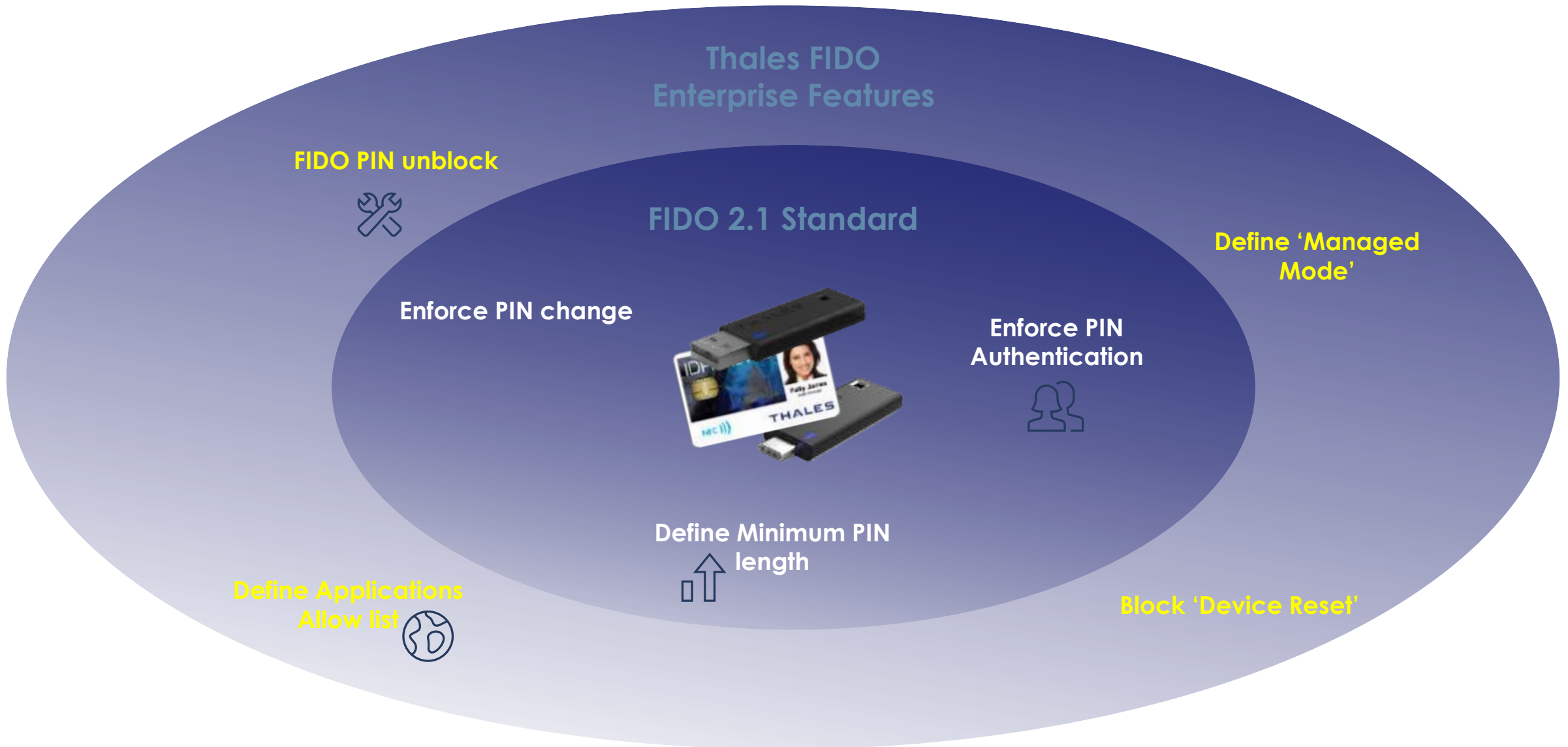
# Challenges FIDO devices

- Enrolment – out of band, end user oriented
- Unblocking Token
- Recovery Card / Token
- Revoke certificate / Disable access
  
- Enforce PIN
- PIN policy
  
- FIDO on Phone - Passkey

# Thales FIDO 2.1 Enterprise Features

- [tec-bite.ch](http://tec-bite.ch)
- FIDO 2.1
  - PIN define PIN length 
  - enforce PIN change on first use
  - Force PIN Input 
- Enterprise feature Thales
  - central Management of FIDO Credentials 
  - Provisioning of Credentials on [multiple] IdP's 
  - Restrict usage of Token on defined Services
  - Unblock Token

# FIDO 2.1 and Thales FIDO Enterprise features



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018. All rights reserved.

# Manage FIDO/PKI Token Life Cycle & Configuration

## Needs

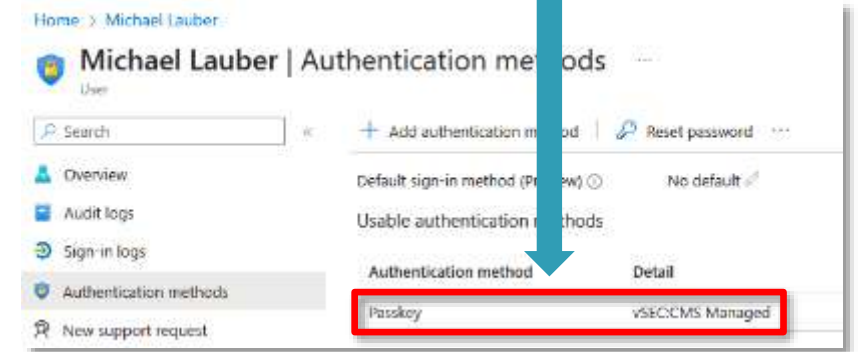
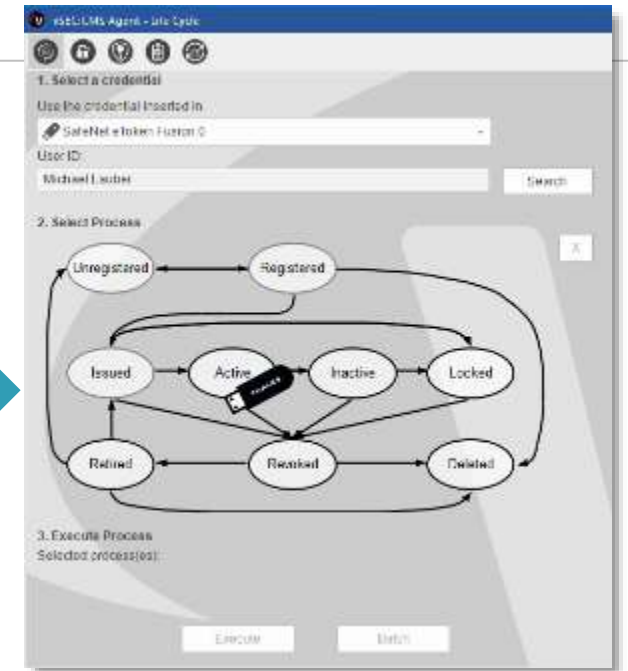
- PKI-like admin controls on FIDO authenticators/security keys
- Requires an IDP that supports FIDO authenticators

## Solution

- vSEC:CMS integrates with multiple IDPs and allows customers to use FIDO authentication



- Centralized management of FIDO security keys and PKI credentials
- Enable customers to use Thales' proprietary FIDO token management features
- On-Behalf and self-service enrollment flow



# Management von CBA + FIDO Credential – Versasec vSEC:CMS

## Verwaltung von PKI/FIDO devices

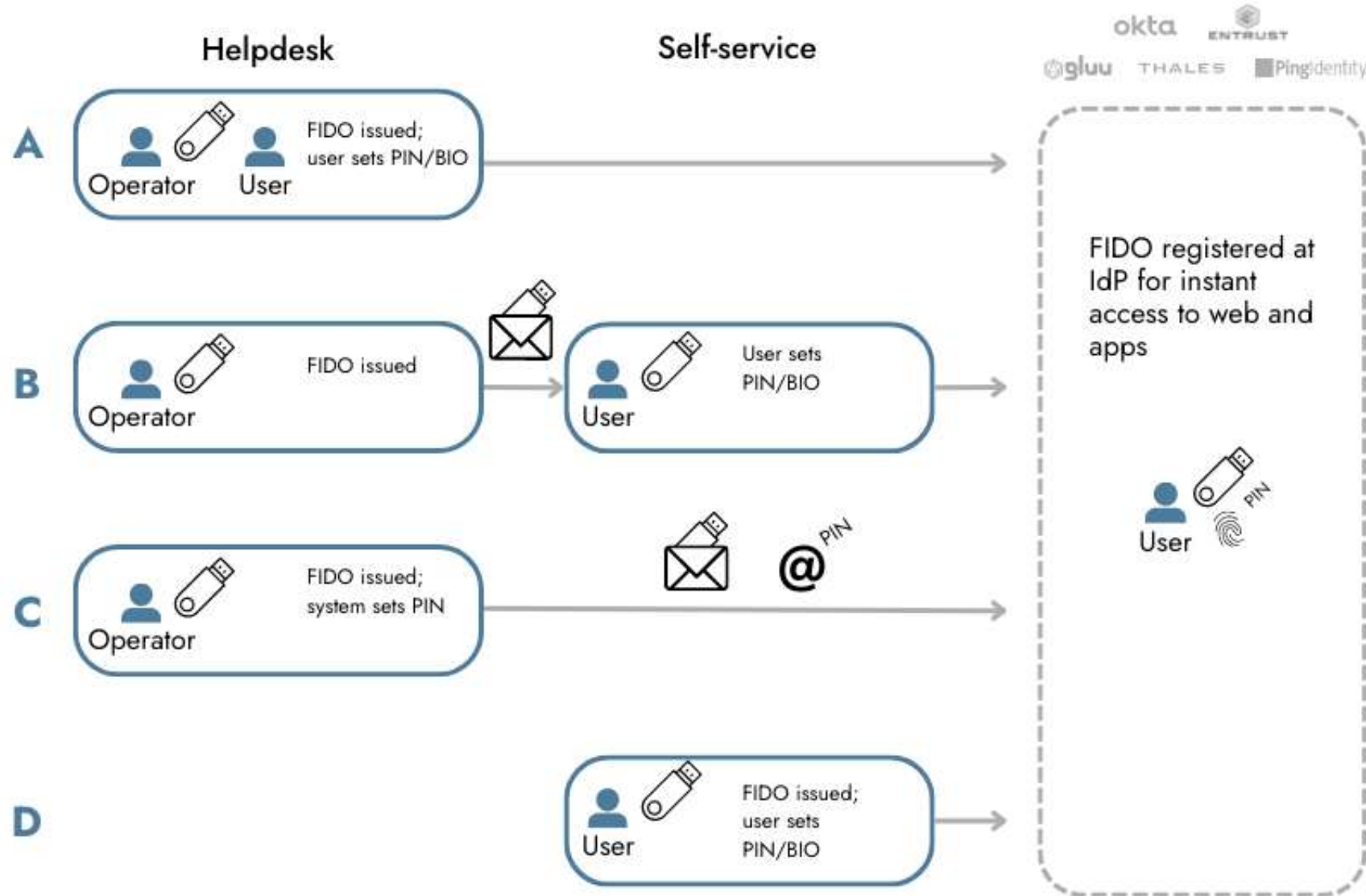
- Personalisierung
- Verwaltung der Zertifikate
  - **Beantragung** bei der CA
  - **Erneuerung** bei Ablauf
  - **Rückruf** bei Verlust oder Mitarbeiterwechsel
- Zentrale FIDO Ausstellung
  - Einbindung IDP

## Optionen für das Management

- **On-Behalf** durch Operator
- **Self-Service** durch Benutzer



# FIDO provisioning with an IDP



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2018. All rights reserved.

# Passkey

- FIDO in Software
- Ideal for consumer
  - Usability first
- Private key protection
  - Software based
  - Backup to cloud
  - Distributed
- Enrolment after successful authentication
  - Not out of band
  - On a device used for all other daily work

Good



23. April 2025

### FIDO im Unternehmen

Warum eine Consumer Technologie im Unternehmen Sinn machen kann? Die passwortlose Anmeldung ist hier der absolute...

---

 von mephisto

# Middleware / Management Tools

- SAC
- i-SCM
- FIDO Key Manager
- IdP – Thales STA oder MS EntraID
  
- CMS – Credentials Management Solutions
  
- Vesasec vSEC:CMS
  - Cloud
  - On premise
  - HSM protected
  - Integrated AD, MS EntraID, CAs, email, UserSelfService, .....

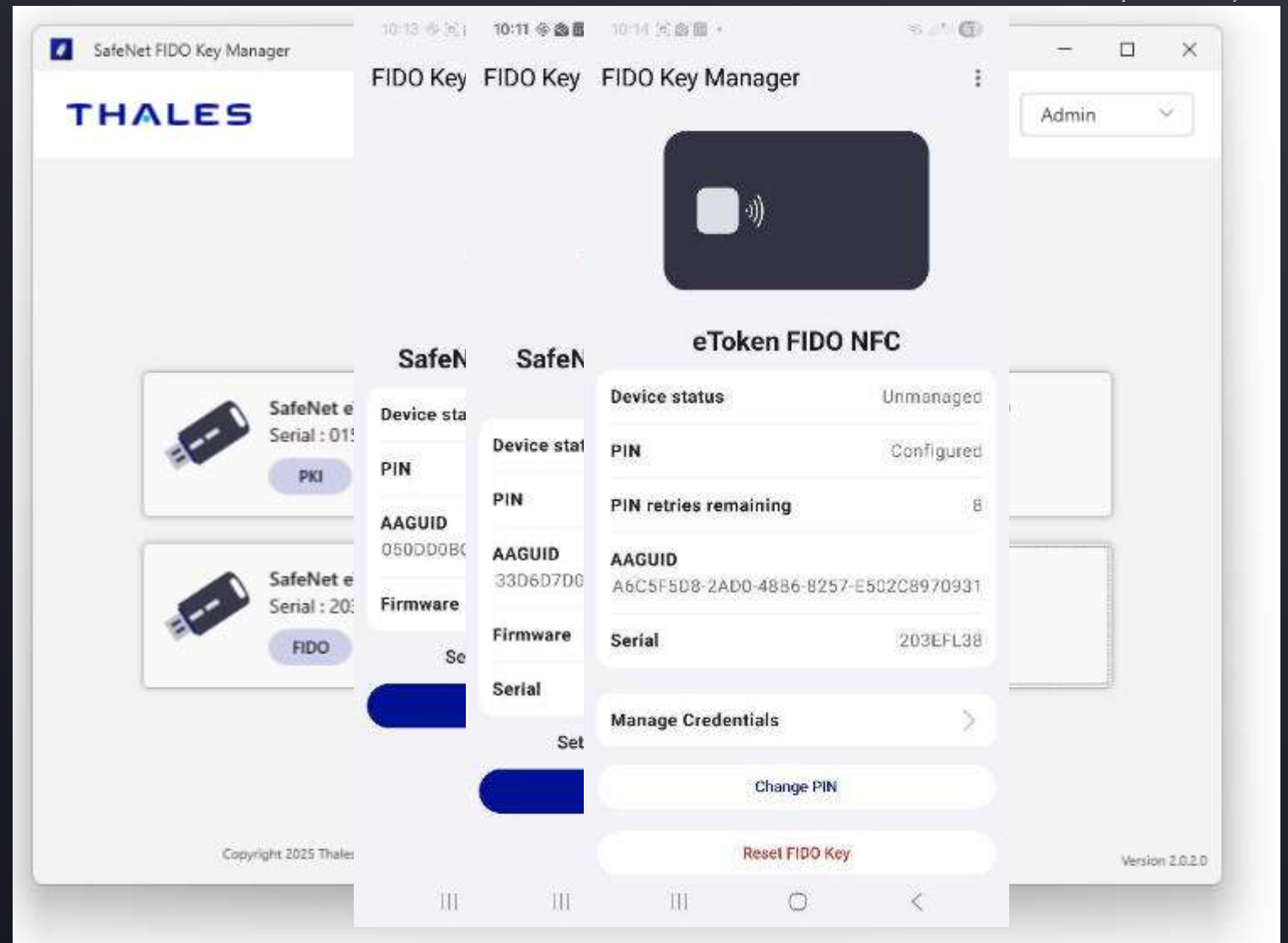
# SAC – SafeNet Authentication Client



- SAC
- Custom config
- SAC Minidriver
  
- CSP versus KSP – enforce KSP
  - [CVE-2024-30098 - Security Update Guide - Microsoft - Windows Cryptographic Services Security Feature Bypass Vulnerability](#)

# FIDO Key Manager

- Desktop
- Mobile App



# Enterprise like Management

- Managing Life Cycle of Authenticator
  - To unblock Token / Cards
  - Disable Token / Cards to block access to corporate resources
- Enrol SC & Enrol FIDO Token
  - MS EntraID or others
  - PIN Policy
  - PIN enforce
  - Unblocking Token
  - Restrict using to webservises (prevent private usage)
- <https://www.tec-bite.ch/fido-im-unternehmen/>
- <https://www.tec-bite.ch/wie-erstellt-man-smart-cards-fuer-das-zertifikatsbasierte-logon-smart-card-management-am-beispiel-von-versasec-vsec-cms/>

# SafeNet Trusted Access

- Thales IdP
  - (Authentication Service and Application Access Control System)
  - Managing Authentication
    - several OTP mechanism. Using FIDO, cba, kerberos
  - Conditional Policy based Access to Applications
  
  - But don't enroll SC, FIDO, issuing certificates
  
- MS EntraID
  - Using FIDO or SC
  
  - But do NOT enrol Token, Cards or issuing certificates
  - Just end user based FIDO registration

# SafeNet Trusted Access (STA) Workforce or SAS PCE Enterprise



# Enrollment


- SC on premise AD & CA (ADCS)
  - Registering Card for a user
  - Mastering card (registration & admin key) for unblocking card
  - Setting PIN policy
  - Initiate card (system generated user PIN)
  - User notification
  - Multiple Certificates
- Enrol SC MS EntraID and CA
- Enrol FIDO Token MS EntraID
  - PIN Policy
  - PIN enforce
  - Unblocking Token



15. April 2021

## Wie erstellt man Smart Cards für das zertifikatsbasierte Logon? Smart Card Management am Beispiel von Versasec vSEC: CMS

Wie im Artikel «Smart Card – ein kleines Kunstwerk» angedeutet, wird mit dem Begriff zu meist die ID-1 Karte...

 von mephisto

# Smart Card

- Card will be registered for a user
- Set master key (admin key) for unblocking card
- Issue certificate(s) for a user
- Manage Lifecycle
  - Revoke, unblock, recover, revoke
- Out of band
- Transfer initial PIN
- Identify the person

**cba – certificate must  
be trusted**

# FIDO Token

- Enrollment to IdP or multiple FIDO
- Register Token
- Set Master key (admin key)
- Generate keys
- Save public on IdP or resource
- Set user PIN
- Restricting - Display Name

**FIDO public must  
be provision to  
Resource / IdPs?**

# Demo Enrolment Bio Token

- Enrollment BIO T
- Using Token in M
- Revoke Token

The screenshot displays the vSEC:CMS - Lifecycle application window. The interface includes a menu bar (File, Go, Help) and a navigation pane on the left with the 'versasec' logo and 'Home > Lifecycle' path. The main content area is divided into three sections:

- 1. Select a Credential**: A form with a dropdown menu showing 'SafeNet eToken BIO 0' and a 'User ID' field containing '5746 3132 3031 354A5746 3'.
- 2. Select Process**: A flow diagram with three nodes: 'Unregistered', 'Issued', and 'Retired'. Arrows indicate a cycle: Unregistered to Issued, Issued to Retired, and Retired back to Unregistered.
- 3. Execute Process**: A field for 'Selected process(es):' with 'Execute' and 'Batch' buttons below it.

Overlaid on the main window are two smaller windows:

- A 'vSEC:CMS - FIDO2 Bio Enrollment Management' window with a 'Manage Bio Enro' button.
- A 'vSEC:CMS' dialog box with a thumbs-up icon, the text 'FIDO2 Bio Enrollment successful!', and an 'OK' button. The ID 'ID: ITHIC-8216' is visible at the bottom.

At the bottom of the main window, there are 'Execute' and 'Batch' buttons. A status bar at the very bottom shows 'Connected'.

# Comparing cba and FIDO2

## Certificate based auth with SC

- Private key not exportable
- Central policy based enrolment
- cba
  - Trust
  - Validity
  - Revocation
  - Subject / san
  - Key usage / EKU
  - RSA or ECC – key length
- PIN Policy
- Unblock card / PIN reset
- Recovery
- SC removal behaviour

## FIDO / passkey

- Key attestation
- Passkey – private key will be save to cloud and distributed across user devices
- Just private key authN – like ssh priv key auth
- Key renewing
- End user base enrolment of Token
  - Unblock Token / PIN Reset only Thales EF
- Recovery if lost / damaged → re-enrolment

# Future – QCRC or PQC

- What happen next?
  - Authentication
  - Signing / docs, code, emails, ....
- QCRC – Quantum Computer resistant cryptography or PQC
  - Swiss Government
  - NIST
  - BSI
- Changing CSP to KSP
  - [CVE-2024-30098 - Security Update Guide - Microsoft - Windows Cryptographic Services Security Feature Bypass Vulnerability](#)

# Current state September 2025

NIST name	FIPS #	Function	Based on
<b>ML-KEM</b> Module Lattice-Based Key encapsulation Mechanism / key exchange	<b>FIPS203</b> 08-13-2024	Encryption	<b>CRYSTALS-Kyber</b> (Cryptographic Suite for Algebraic Lattices)
<b>ML-DSA</b> Module-Lattice-Based Digital Signature Algorithm	<b>FIPS204</b>	Signature	<b>CRYSTALS-Dilithium</b>
<b>SLH-DSA</b> Stateless hash-based Digital Signature Algorithm	<b>FIPS205</b>	<b>Alternate</b> to FIPS204	<b>Sphincs+</b>
<b>FN-DSA</b> Lattice-based	<b>FIPS206</b> Draft 8/2025	<b>Alternate</b> Signature FIPS204	<b>Falcon</b> NTRU (n-th degree-truncated polynomial ring units)
<b>HQC</b> code-based Key encapsulation / key exchange	Expected in 2026/27	<b>Alternate</b> to FIPS203	<b>Hamming Quasi-Cyclic</b>