AVANTEC
Competence. Security. Trust.

Security Changes Everything.

Roger Mahler – PreSales Consultant Thales

Dirk Gluch (Principal Security Engineer) . gluch@avantec.ch

12 May 2026

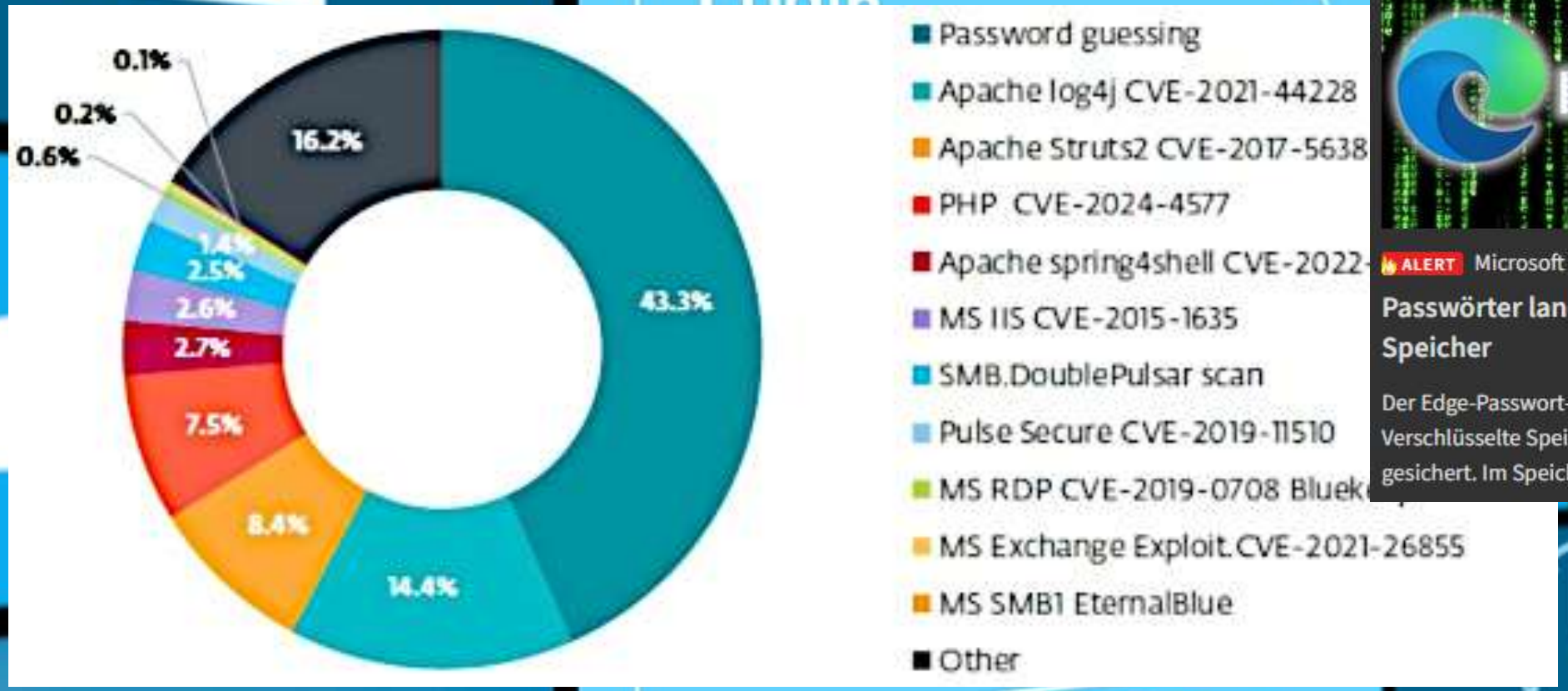
AVANTech-Day 2026

AVANTEC
Competence. Security. Trust.

Authentication – passwordless, strong, secure

Dirk Gluch
Principal Security Engineer,
AVANTEC

WORLD PASSWORD DAY



When ever possible – do NOT use passwords

12. Mai 2026

Agenda

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

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.

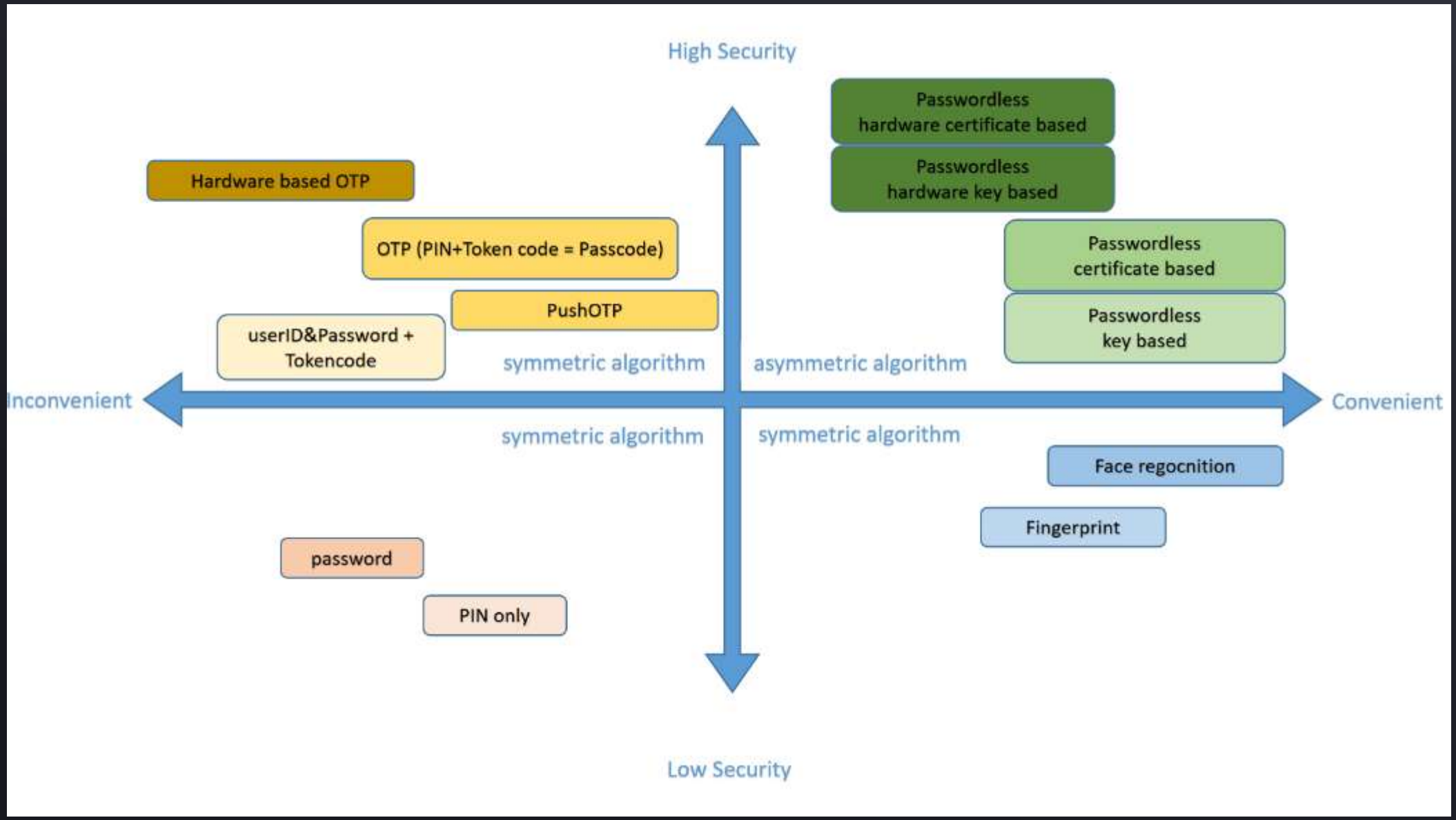
Main aspect - security

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.



Passwordless - asymmetric Authentication

IdP

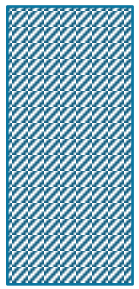
Create a nonce random string «öpes»

Lorem ipsum dolor sit amet, consete

hash

Sending cipher

encrypt
priv key



6b229a19
af9776fb6
410c9899
a0836782
fe031918
be4b0a49
55d86c6a
363b162

hash

decrypt
pub key

=?

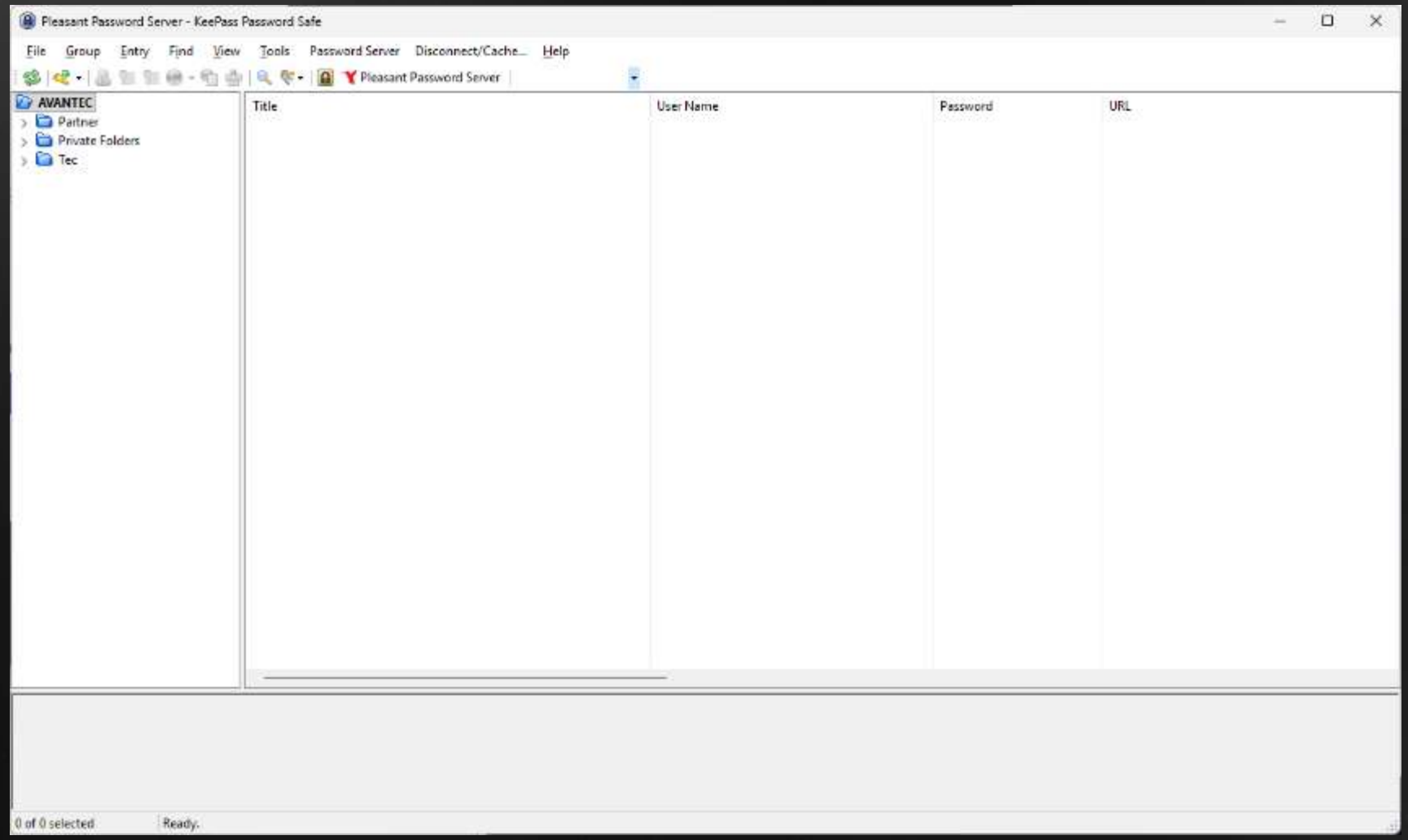
Non-repudiation

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

AVANTEC use cases

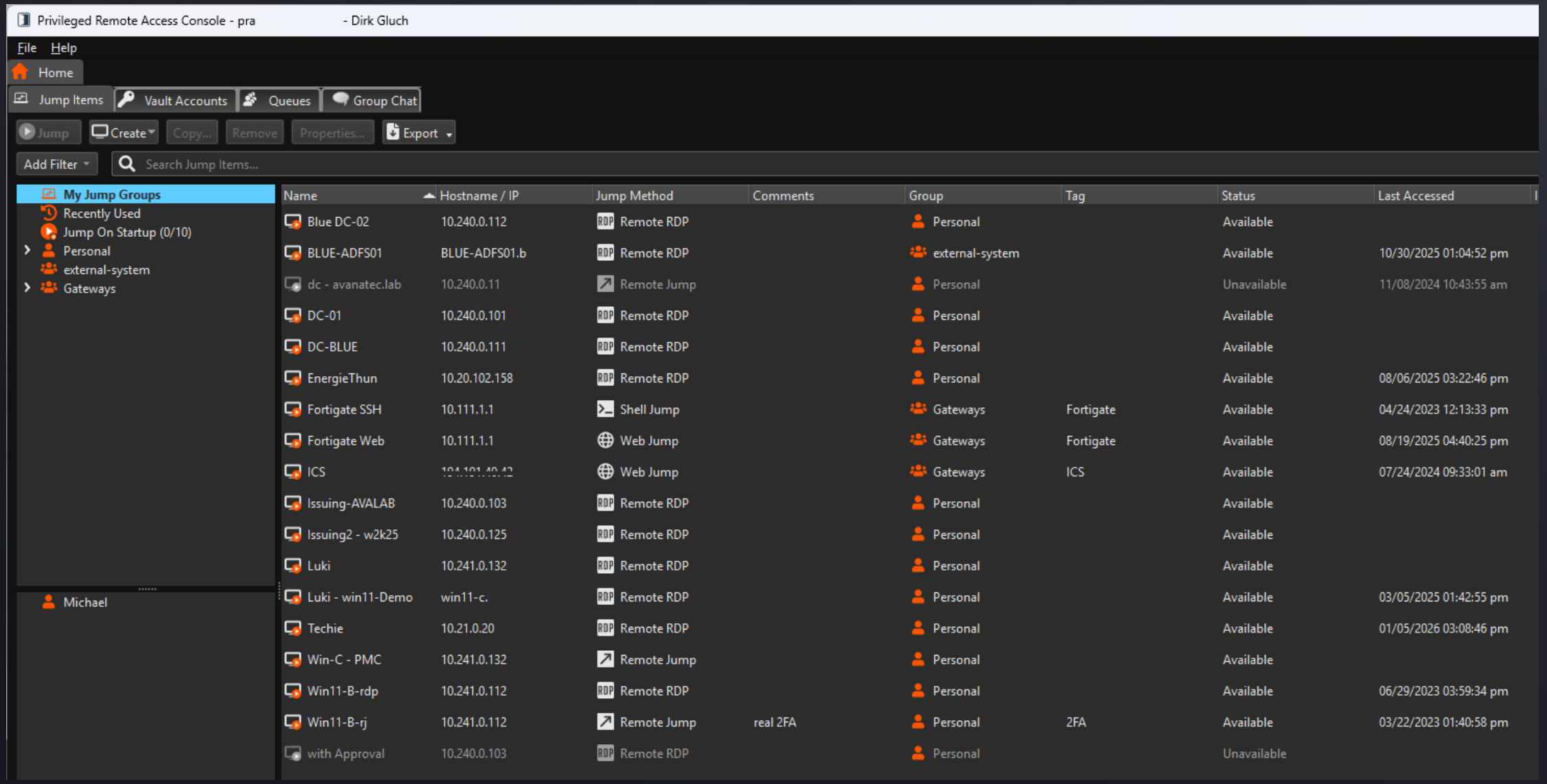
AVANTEC
Competence. Security. Trust.

- 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)
    - Asymmteric & passkey
- Challenges
    - Enrolment, unblocking, recovery token, keys


Pleasant Password Server - KeePass Password Safe
File
Group
Entry
Find
View
Tools
Password Server
Disconnect/Cache...
Help
Pleasant Password Server
AVANTEC
Partner
Private Folders
Tec
Title
User Name
Password
URL
0 of 0 selected
Ready.

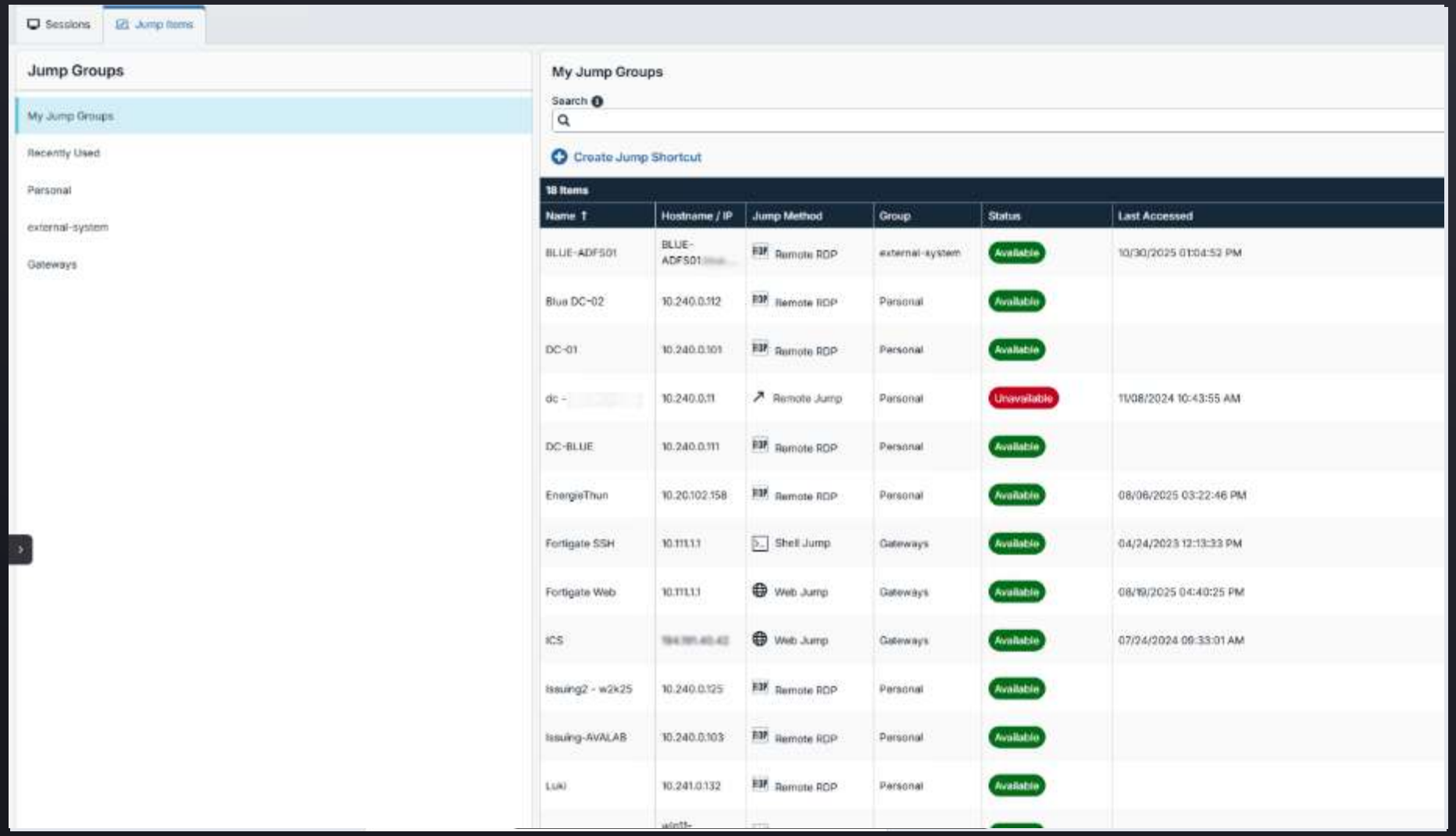
Logon PRA with FIDO-Token - ac

AVANTEC
Competence. Security. Trust.



Logon PRA with FIDO-Token - web

AVANTEC
Competence. Security. Trust.



Demo with mobile devi

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

AVANTEC
Competence. Security. Trust.

Advantages of separate hardware

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

- 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)

AVANTEC
Competence. Security. Trust.

- 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)

AVANTEC
Competence. Security. Trust.

12 May 2026

Thales IDCore & PIV

- IDCore 230 / 3230 under NIST Validation
  https://cpl.thalesgroup.com/sites/default/files/content/product_briefs/f
  024-02/safenet-idcore-230-3230-pb.pdf
- IDPrime PIV 4.0 FIDO under NIST -
  https://cpl.thalesgroup.com/de/ac
- IDPrime 930C
- https://csrc.nist.gov/Projects/cryptographic-mod gra
  process/modules-in-process-list

Custom Cards by Thales DIS BPS

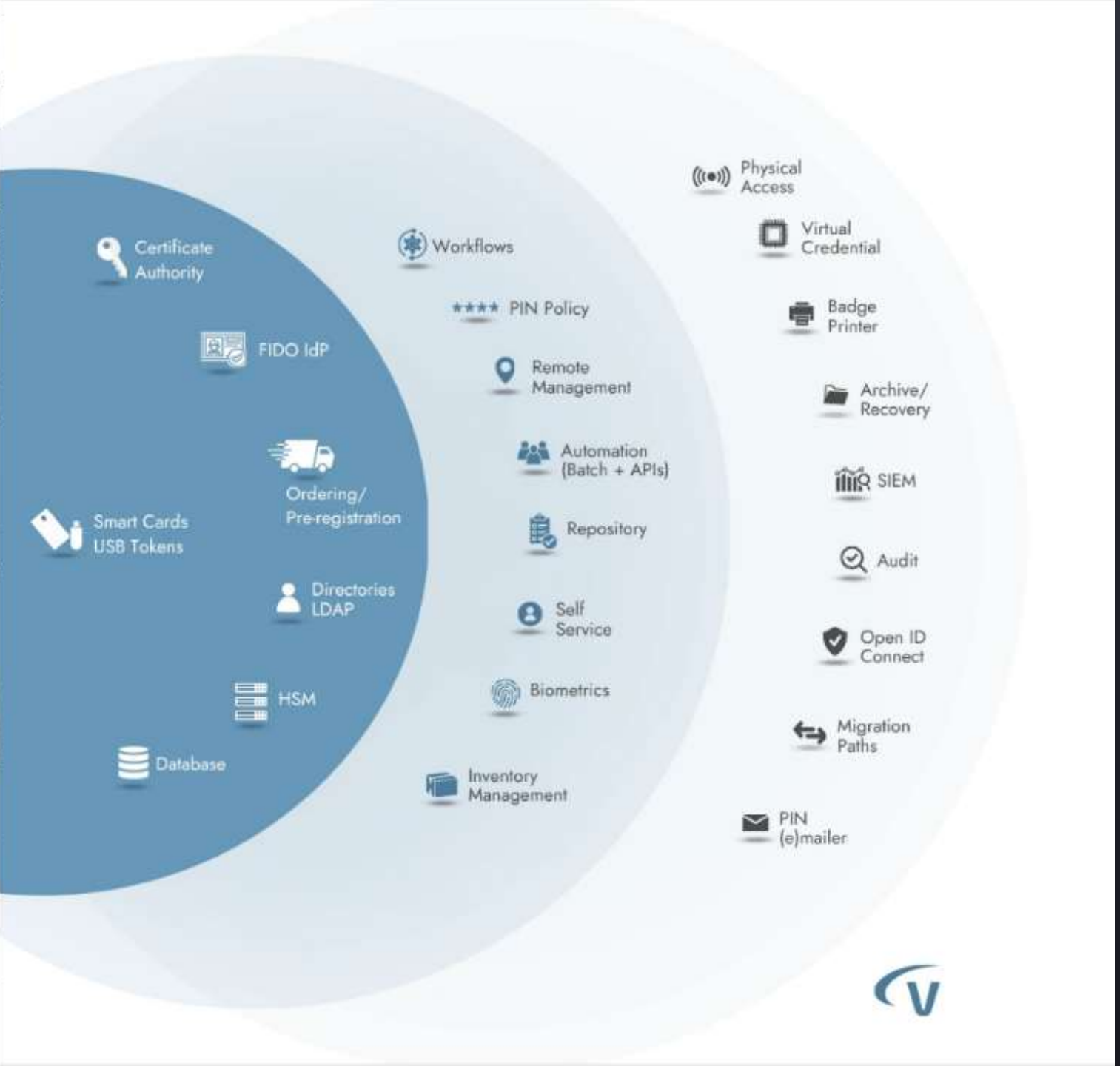
AVANTEC
Competence. Security. Trust.

- 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



AVANTEC
Competence. Security. Trust.

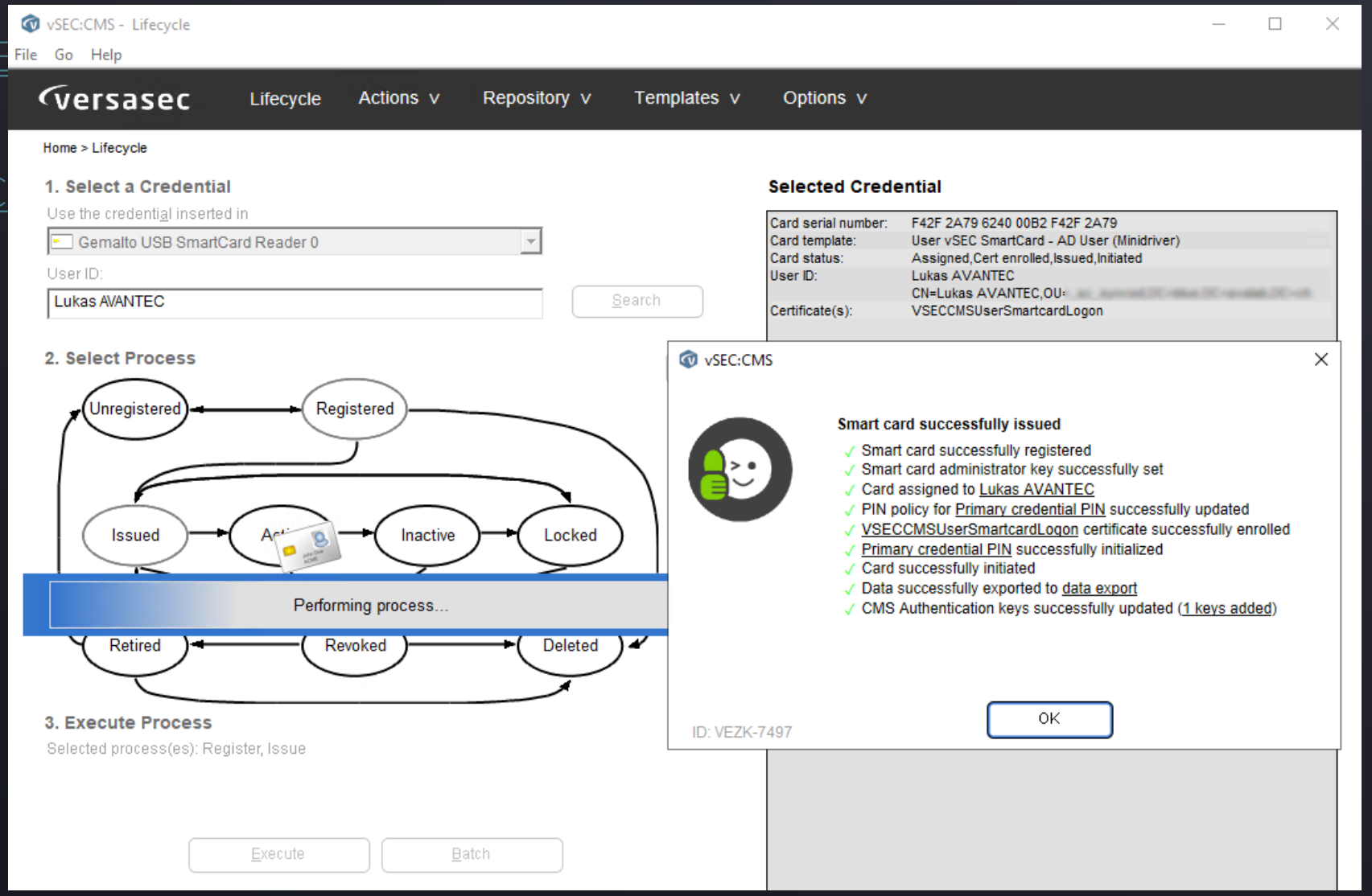
Credentials Management with

vSEC:CMD from Versasec

12 May 2026

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

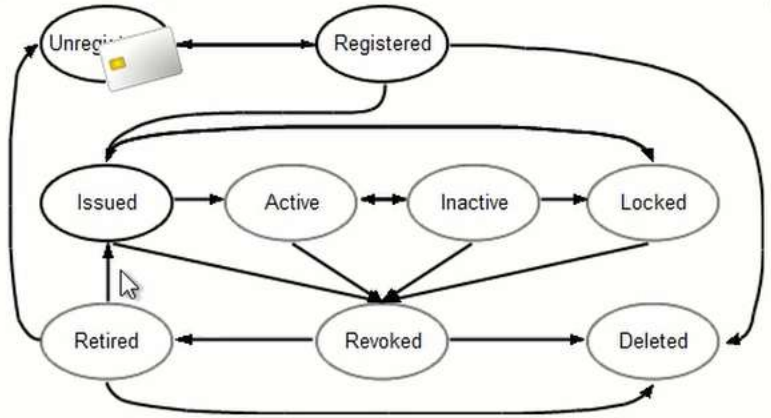
Gemalto USB SmartCard Reader 0

User ID:

F42F 2A79 6240 00B2 F42F 2A79

Search

2. Select Process



3. Execute Process

Selected process(es):

Execute Batch

Selected Credential

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

Selected Credential Template Description

NUM

smtp4dev

smtp4dev
rob@rnwood.co.uk

Messages Sessions

Received	Subject	To

Delete All Delete Save... Inspect View

Listening on port 25 Stop Listening Options

Thales IDPrime BIO (FIDO)

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

- 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)

fido ALLIANCE

FIPS VALIDATED 140-2

MADE IN FRANCE

MADE IN EU

Advantages FIDO

AVANTEC
Competence. Security. Trust.

- 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 passsword regulary
- 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

AVANTEC
Competence. Security. Trust.

- 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

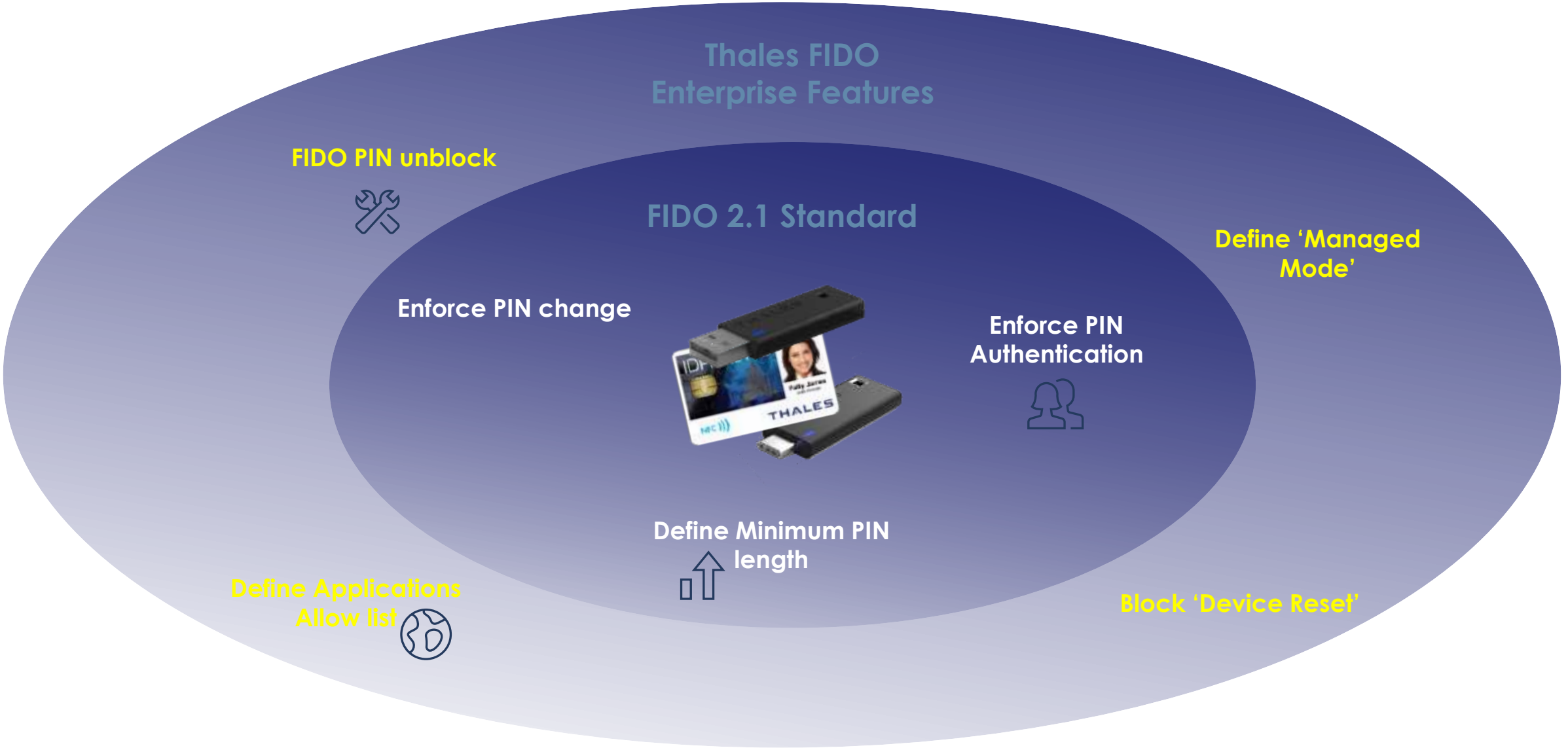
AVANTEC
Competence. Security. Trust.

- 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

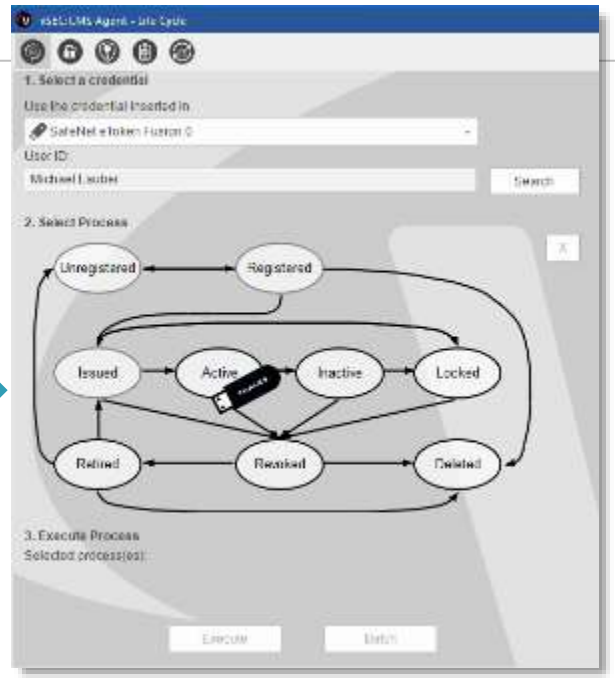
FIDO 2.1 and Thales FIDO Enterprise features



Manage FIDO/PKI Token Life Cycle & Configuration

Needs

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

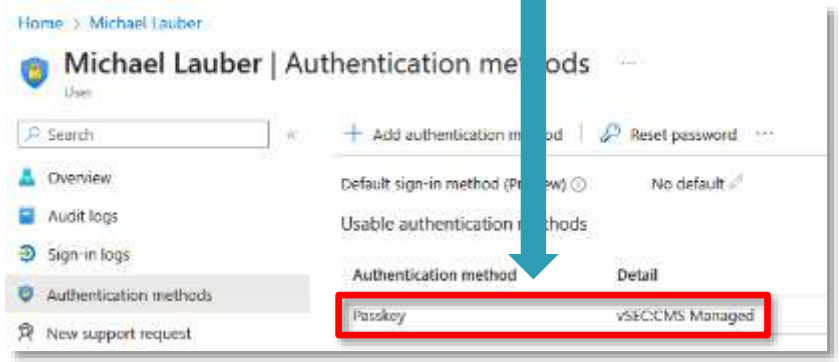


Solution

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

STA okta ENTRUST gluu Microsoft ForgeRock Ping Identity

- 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



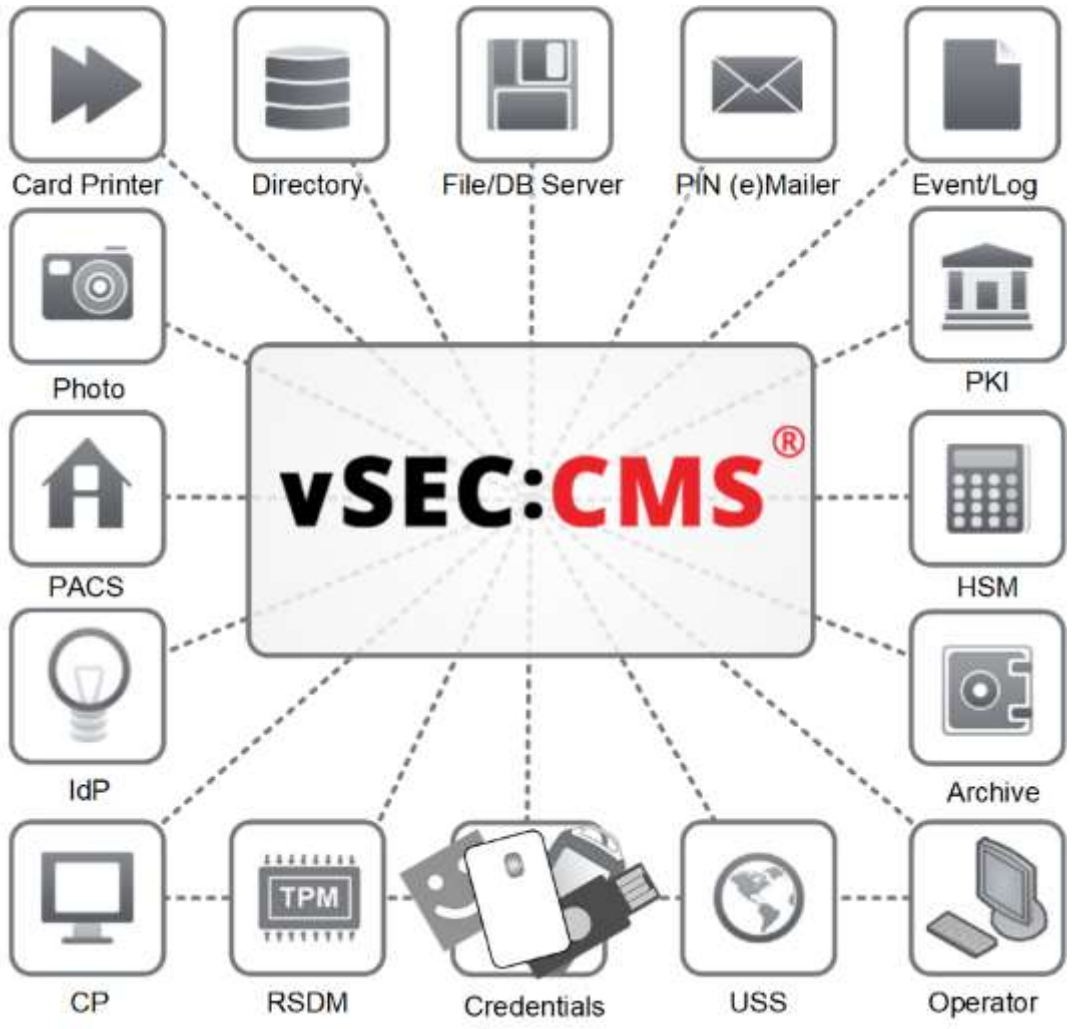
Management von CBA + FIDO Credential – Versasec vSEC:CMS

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

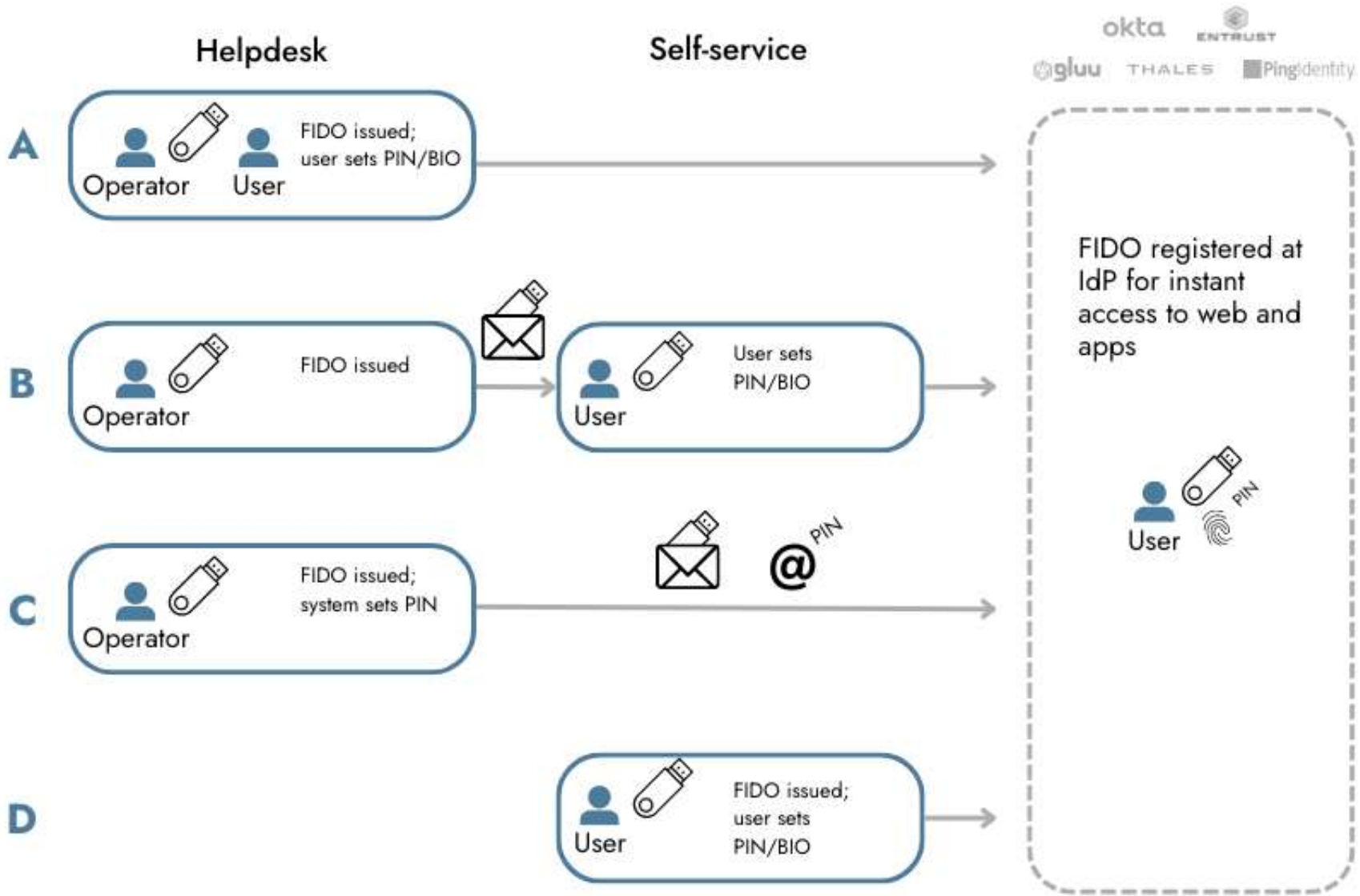
Optionen für das Management

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



THALES

FIDO provisioning with an IDP



THALES

Passkey

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

- 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

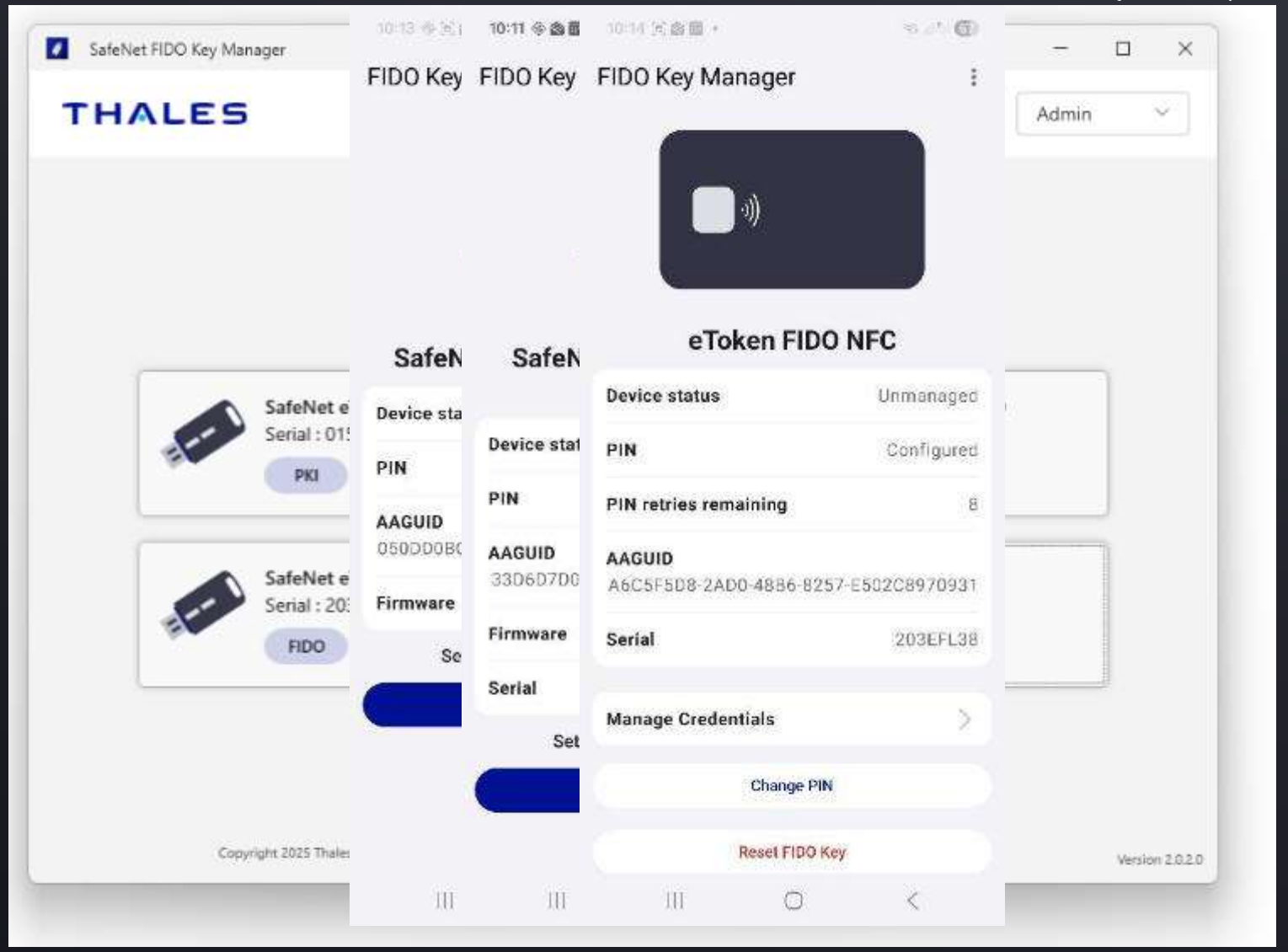
AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

- 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 webservices (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

AVANTEC
Competence. Security. Trust.

- 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, FIDOs, 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 (registrqation & 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

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

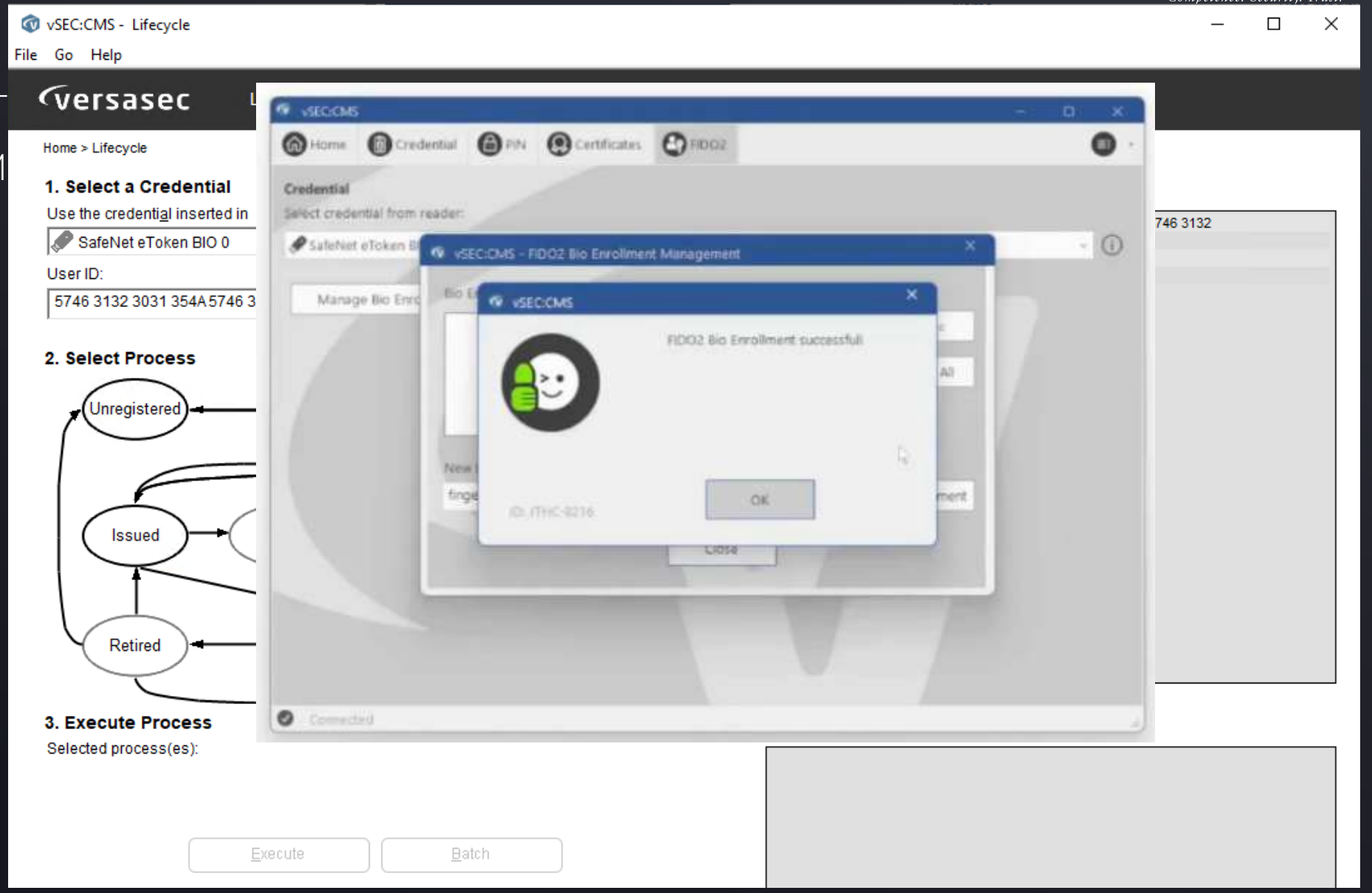
- Enrollment to IdP or multiple FIDO

- 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



Comparing cba and FIDO2

AVANTEC
Competence. Security. Trust.

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

AVANTEC
Competence. Security. Trust.

- 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

AVANTEC
Competence. Security. Trust.

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