versasec

THALES
Building a future we can all trust

Thales and Versasec Workshop

Advanced and Innovative PKI and FIDO2 based Multi-factor Authentication

www.thalesgroup.com

Presenters

Janagaran Annamalai
Regional Sales Manager – Middle East, Turkey and Africa Identity and Access Management, Thales CPL

Tatjana Suhorukova
Business Development Analyst
Versasec

Endre Pasztor
Senior Pre-Sales Consultant
Identity and Access Management
Thales DIS

Paul Rajkumar
Sales & Business Development Engineer
Versasec

Rudy Solman
IAM Pre-Sales Consultant
Digital Identity & Security
Thales CPL

John Asan
Technical Leader Worldwide
Versasec

Workshop Agenda

THALES
Building a future we can all trust

01

PKI & FIDO Passkeys market trends, use cases

Janagaran Annamalai
Paul Rajkumar

02

PKI and FIDO Authenticators

Endre Pasztor

03

Thales FIDO Keys with vSEC:CMS with STA and Entra ID

Rudy Solman
John Asan

Workshop Housekeeping Rules

All attendees muted

This workshop is being recorded

Question? Submit them via the chat

Certification: eligibility is tied to completing Knowledge Quiz

Score 100% on Knowledge Quiz and receive a special gift!

We appreciate Your participation and engagement!

THALES
Building a future we can all trust

About Thales

Janagaran Annamalai

Regional Sales Manager – Middle East, Turkey and Africa Identity and Access Management, Thales CPL

www.thalesgroup.com

From the bottom of the oceans…to the depths of space & cyberspace

THALES GLOBAL BUSINESS AREAS

#1
Worldwide in data protection

#2
Worldwide in civil satellite systems

#1
Worldwide in air traffic management

#2
Worldwide in inflight entertainment

#3
Worldwide in commercial avionics

#1
European provider of advanced sensors

#1
Worldwide in safe & smart airport solutions

Over **80,000** Employees

68 countries Global presence

€ 1bn self-funded R&D*

*Does not include externally financed R&D

Revenue of **€ 19bn** in 2023

Thales Cloud Protection & Licensing

- Data Protection
- Access Management
- Software Monetization

Worldwide leader in General Purpose, Payment & Cloud HSMs

Worldwide Leader in Data Encryption & Key Management

Worldwide Leader in Advanced Authentication

Worldwide Leader in Software Protection

2,500+ Employees

25 countries presence

750 engineers worldwide

30,000 customers worldwide

BUILDING A FUTURE WE CAN ALL TRUST

Thales' technologies and services help secure [illegible] of financial transactions between banks every day and the most valuable corporate and government information

Drivers for Passwordless Authentication

More Security

Eliminate phishing, credential stuffing & other passwords related attacks

Better User Experience

No need to remember multiple passwords. Faster & seamless login

Lower TCO

Reduce IT operations costs & support costs

Why?

P@SSW*RDS

ARE THE PROBLEM

01

The average person has approximately **38 online** accounts for work purposes (source: SC Magazine UK), secured with a username password combination

02

According to the UK National Cyber Security Centre (NCSC), **23 million account holders worldwide** still use **“123456”** as their password

03

90% of internet users are worried about getting their passwords hacked

04

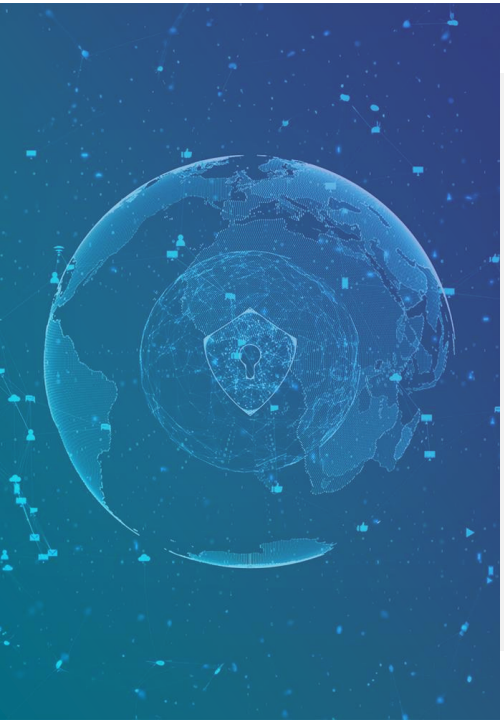
80% of hacking-related breaches are tied to passwords (source: Verizon Data Breach Investigations Report)

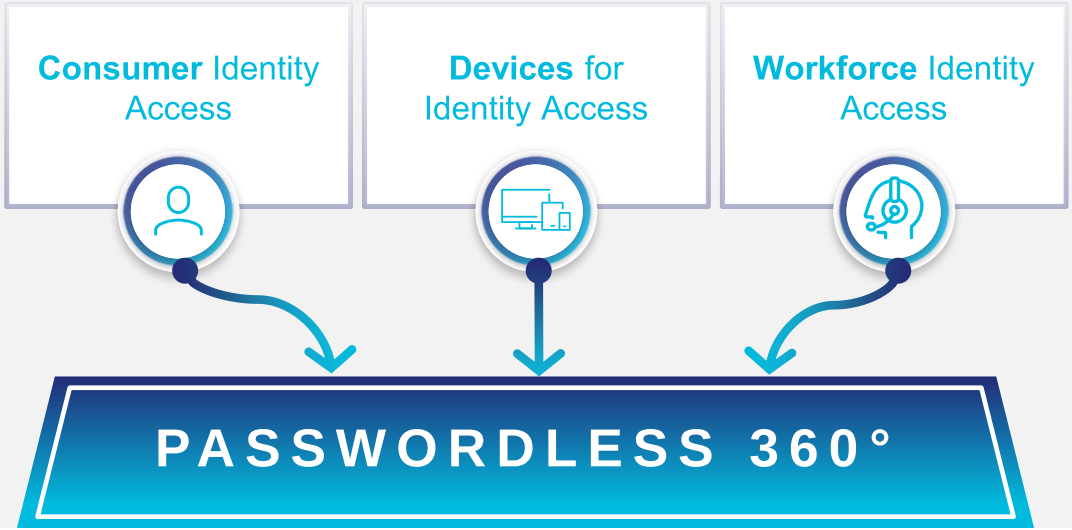
05

Slow up take on MFA.

Around 40% of employees at their organization use MFA for cloud-based applications. MFA usage for on-premises apps is even lower (source: 2024 Thales Data Threat Report)

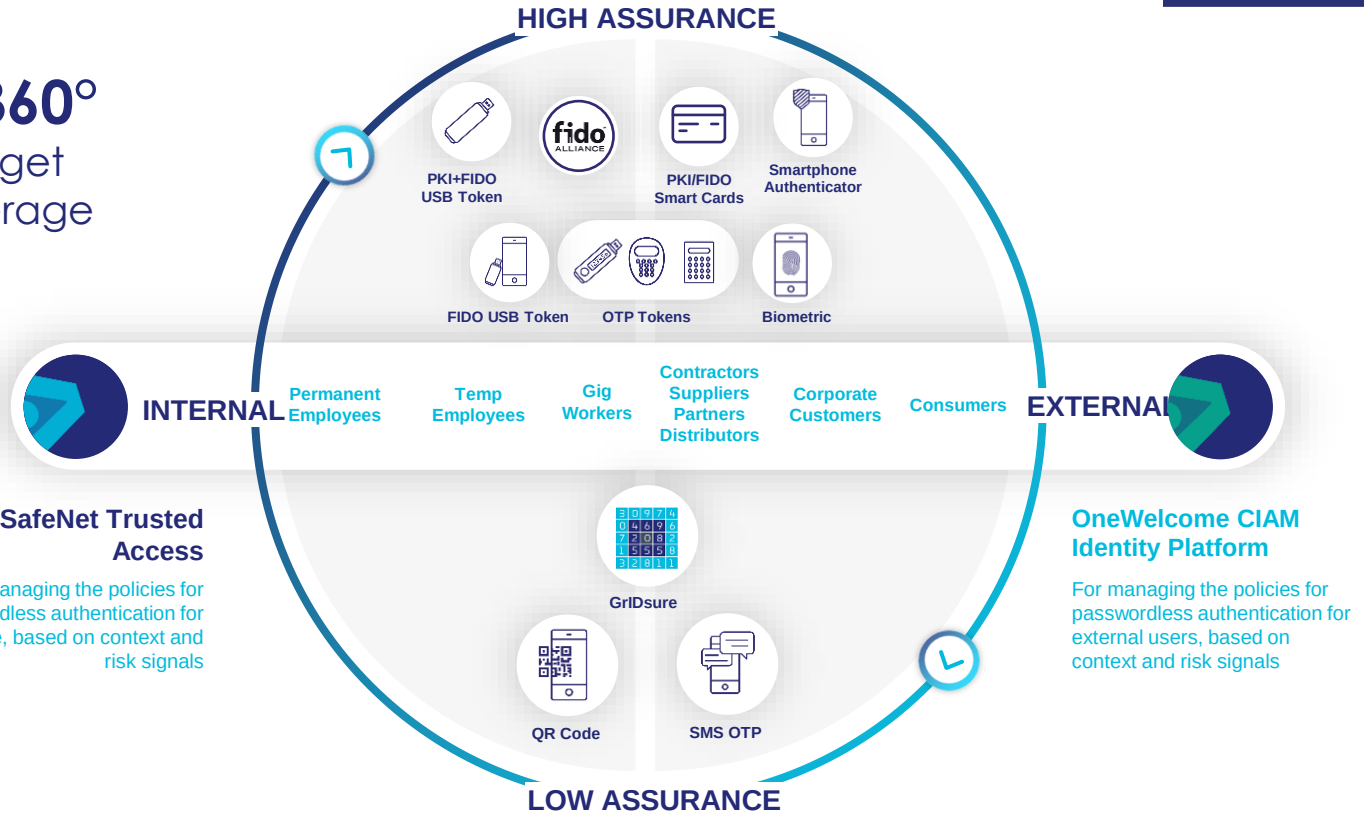
Addressing the passwordless journeys





Passwordless 360°

Thales's approach to get full Passwordless coverage



SafeNet Trusted Access

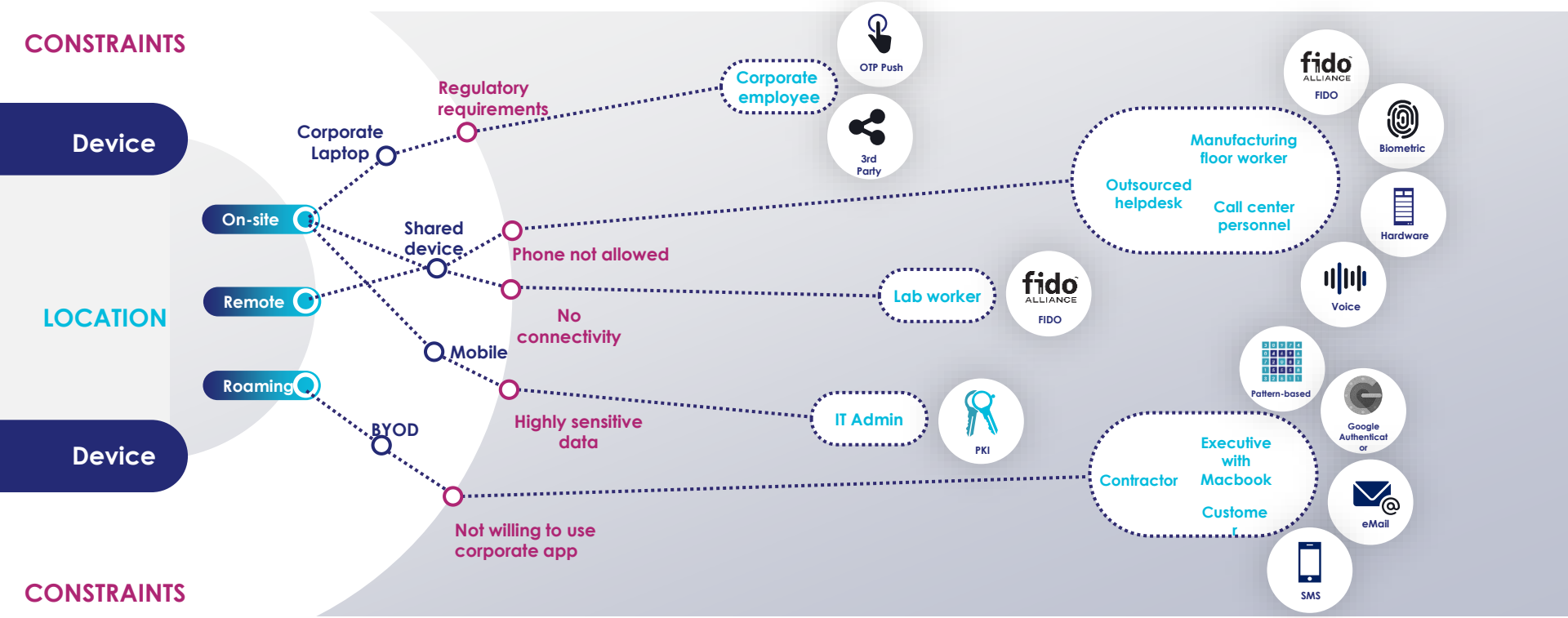
For managing the policies for passwordless authentication for workforce, based on context and risk signals

OneWelcome CIAM Identity Platform

For managing the policies for passwordless authentication for external users, based on context and risk signals

Different users, different security, different user journey

THALES
Building a future we can all trust



PKI & FIDO Passkeys market trends, use cases

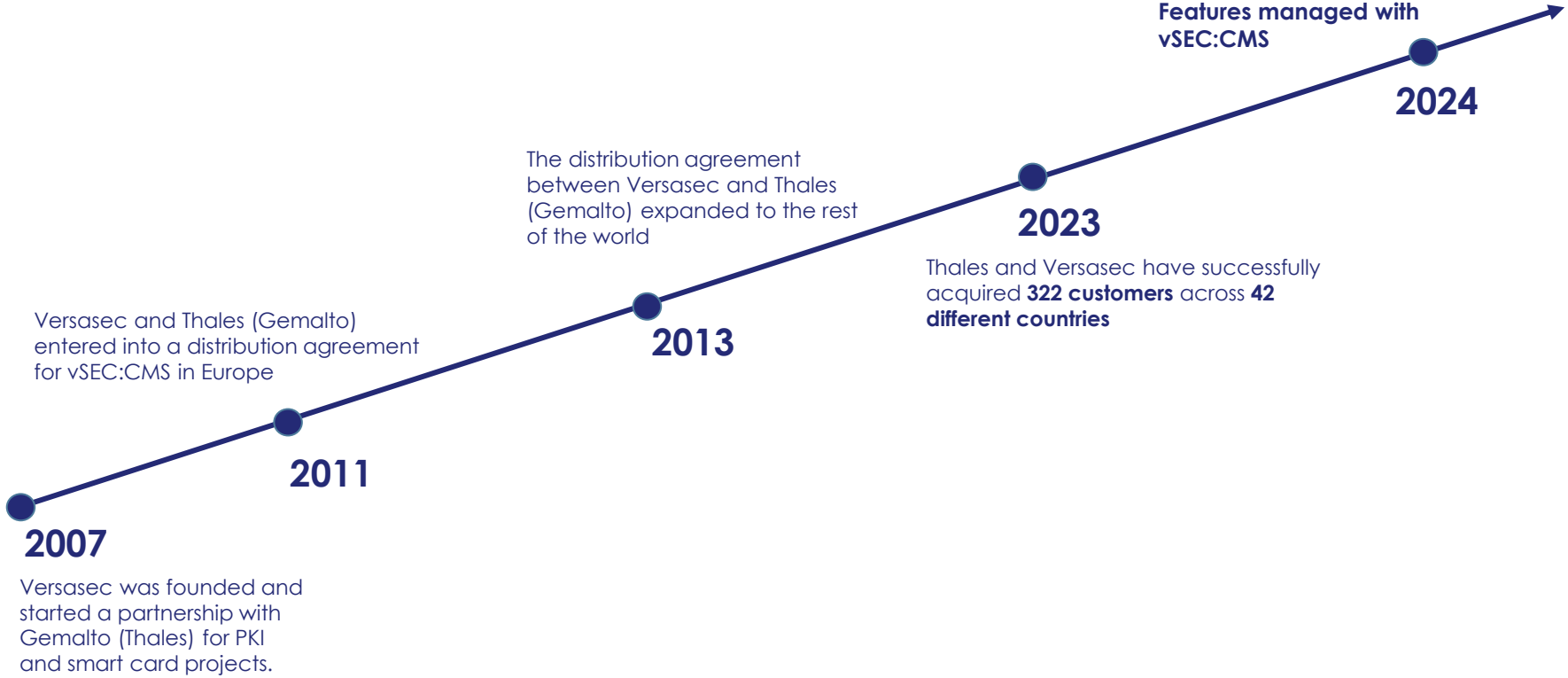
Paul Rajkumar
Business Development Manager MEA & APAC
Versasec

www.thalesgroup.com

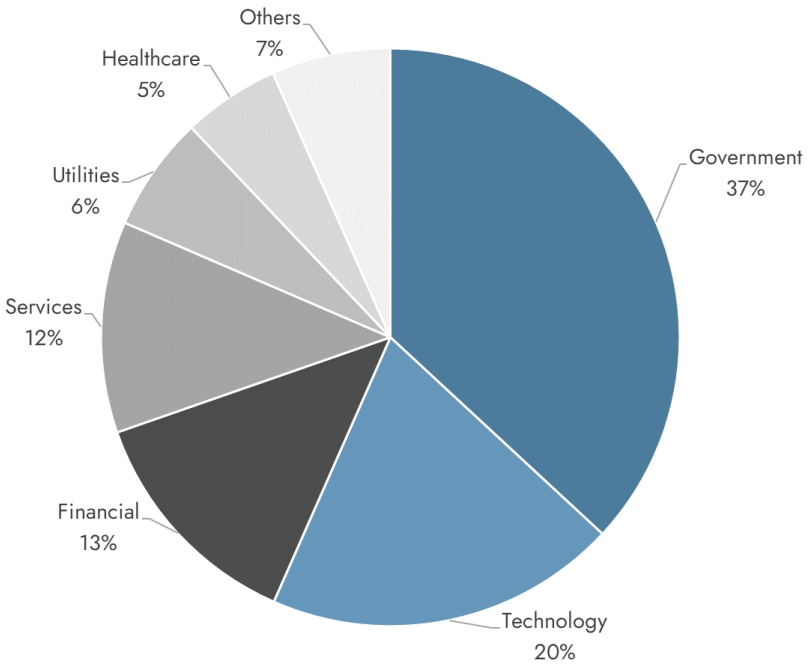
About Versasec

Versasec empowers organizations of all sizes to effortlessly manage digital identities. Our dedication lies in delivering solutions that are not only scalable and intuitive but also driven by innovation. Just as security is seamlessly woven into our products and DNA, it serves as the bedrock of our organization, enabling you to safeguard what truly matters.

Thales and Versasec: Joint History of Success



Joint Success Stories



Countries

42

Customers

300+

Avg customer lifetime (months)

94

Drivers for adopting passwordless MFA

THALES
Building a future we can all trust

- Cyber threads
- Compliance regulation
- Remote access
- Privileged access devices
- Zero Trust and passwordless
- User convenience

Phishing-resistant MFA

THALES
Building a future we can all trust

WEAKEST

SMS or Voice MFA

Text Messages (SMS)

Voice Message

App- based MFA

Mobile push notification without number matching

OTP

Mobile push notification with number matching

Token-based OTP

STRONGEST

Phishing-resistant MFA

FIDO

Public-key infrastructure (PKI)-based

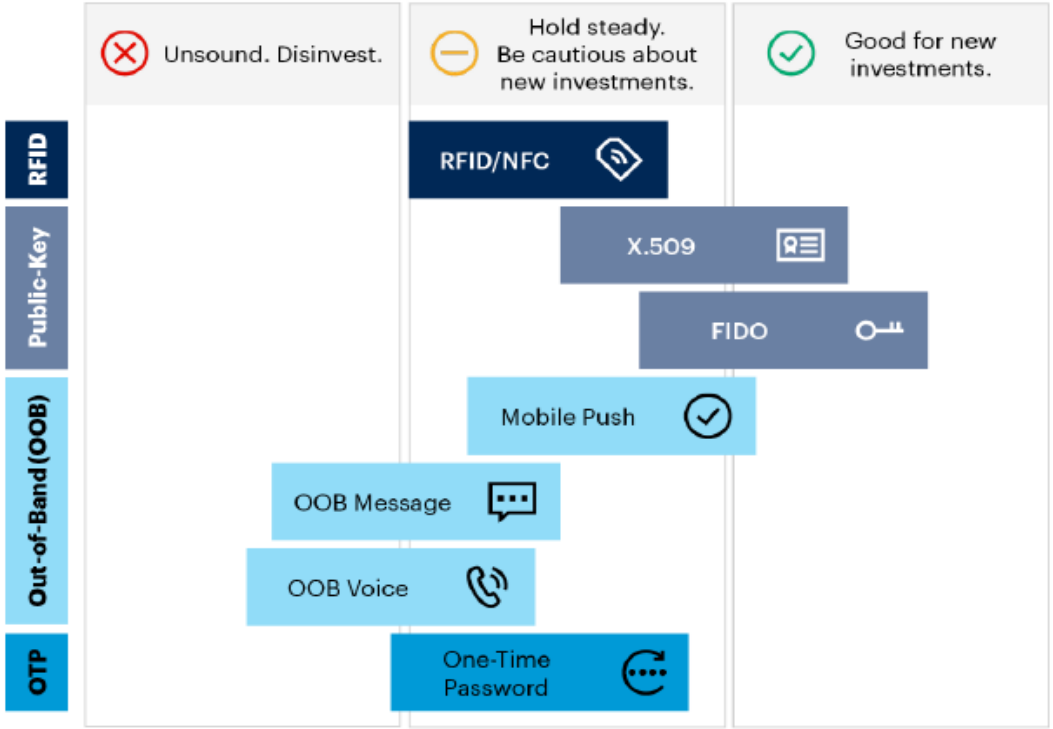
Report: Identity and Access Management: Recommended Best Practices for administrators by NSA and CISA

Follow a hybrid approach to Go Passwordless

"Go Passwordless Whenever You Can Wherever You Can"

Allan Ant, Gartner IAM Summit, March 2023,

The Strategic Value of Different Flavors of Authentication Token



Source: Gartner
778753_C

Great for Multi-factor authentication

Challenges to deploy PKI and /or FIDO in their organization

THALES
Building a future we can all trust

Configuration Management

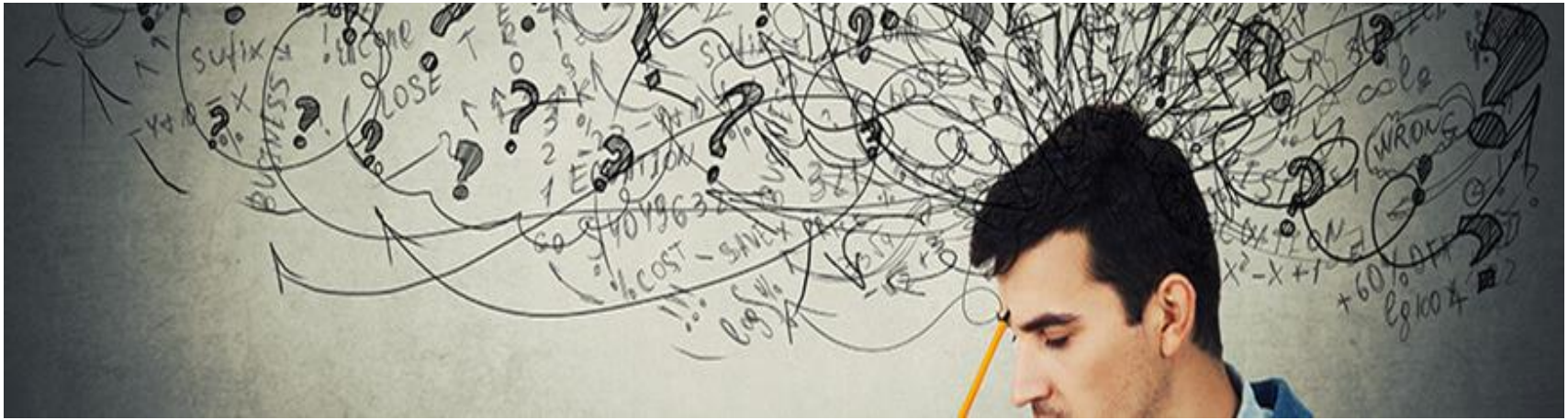
How to manage a consistent security policy?
How to associate a key to the right user?
How to avoid keys are misused?

Hybrid IT / Ecosystem

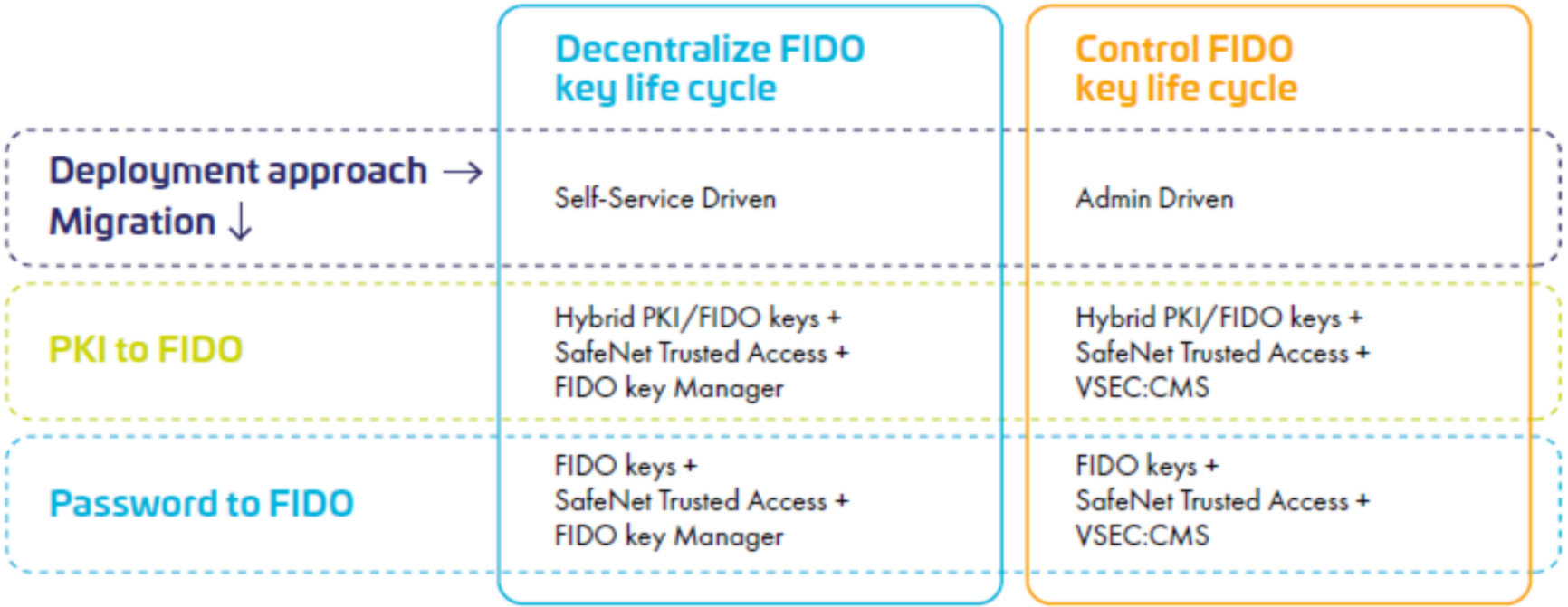
How to access non FIDO applications?
How to combine with physical access?

Services Registration

How to avoid multiple end user registrations?
How to avoid registration being a pain ?
How to revoke a FIDO / PKI key ?



How Thales and Versasec can help



THALES
Building a future we can all trust

Business Cases

www.thalesgroup.com

Corporate Badge

THALES
Building a future we can all trust

Customer Requirement

Customer requires to deploy one device for both Physical and Logical Access

Value Proposition

End to end lifecycle mgt of smart card including RFID keys encoding, integrations with printers and PACS

Sales Follow-up Questions

What physical access technology the customer uses today?
Are Physical and Logical Access managed by one or by several teams?
How many devices need to be managed?
Is this a new solution or is it replacing an existing one?

What to sell?

Authenticators: IDPrime with physical card body
Readers : IDBridge
Management : vSEC:CMS / vSEC:CLOUD
Professional Services Package
Other : SAS/STA for secondary authentication server (Optional)

Privileged Accounts

THALES
Building a future we can all trust

Customer Requirement

Implement Multi-factor Authentication (MFA) & Encryption for Privileged Account Mgt

Value Proposition

End to end solution MFA based on Public Key Infrastructure (PKI) devices for all sizes

Sales Follow-up Questions

What technology is the customer using for the authentication of privileged users?
How many devices need to be managed for your privileged users?
Can your privileged users have several active directory accounts?
What is the customer's timeline?

What to sell?

Authenticators : IDPrime or eTokens or IDPrime Virtual (PIV or combined PIV+FIDO)
Readers : IDBridge (for IDPrime)
Management : vSEC:CMS / vSEC:CLOUD
Professional Services Package
Other: SAS/STA for secondary authentication server (Optional)

PKI/CMS Migration

THALES
Building a future we can all trust

Customer Requirement

Customer is looking to migrate from the existing PKI/CMS (Microsoft MIM or FIM); Other: we can import credentials as long as we have used DN and credential admin key)

Value Proposition

Complete migration path from 3rd party CMS to vSEC:CMS without user interaction

Sales Follow-up Questions

What CMS product uses the customer today?
How many devices need to be managed?
What is the customer's timeline?

What to sell?

Authenticators & Readers & Middleware : N/A (already deployed)
Management : vSEC:CMS / vSEC:CLOUD
Professional Services Package
Other : SAS/STA for secondary authentication server (Optional)

Remote Workforce

Customer Requirement

Customer interested in strong authentication and encryption but cannot deploy hardware (missing smart card readers or USB ports

Value Proposition

Fully centralized management of virtual smart cards or WHfB on Trusted Platform Module (TPM) based on Remote Security Device Management (RSDM) capability or IDPV

Sales Follow up questions

Could you provide details about the customer's environment ?
How many devices need to be managed?
What is the customer's timeline?
What OS's are the customer's users running?

What to sell?

Authenticators: IDPrime Virtual
Readers & Middleware : N/A
Management : vSEC:CMS /vSEC:CLOUD
Professional Services Package
Other : SAS/STA for secondary authentication server (Optional)

Shared Workforce

THALES
Building a future we can all trust

Customer Requirements

Implement multi-factor authentication for shared workstations (Factories, hospitals etc…)

Value proposition

Combining RFID technology with IDPV, frontline workers can access buildings and shared workstations quickly and securely, using their existing RFID badge.

Sales Follow up questions

Could you provide details about the customer's environment ?
How many devices need to be managed?
What is the customer's timeline?
What OS's are the customer's users running?

What to sell?

Authenticators: IDPrime Virtual
Readers & Middleware : N/A
Management : vSEC:CMS /vSEC:CLOUD
Professional Services Package
Other : SAS/STA for secondary authentication server (Optional)

Email Encryption (S/MIME)

THALES
Building a future we can all trust

Customer Requirement

Customer interested in performing email encryption using S/MIME

Value Proposition

Fully centralized management of PKI device integrated with Public CA

Sales Follow up questions

Could you provide details about the customer's environment ?
How many devices need to be managed?
What is the customer's timeline?
What is the targeted use?
Has the customer already selected the type of device to be used?

What to sell?

Authenticators : IDPrime or eTokens
Readers : IDBridge
Management : vSEC:CMS / vSEC:CLOUD
Professional Services Package
Other : SAS/STA for secondary authentication server (Optional)

Compliance

THALES
Building a future we can all trust

Customer Requirement

Customer requires to to follow a regulation which forces the usage of PKI-based strong auth (DFARS, ANSSI, GDP, initiative from industry leaders…)

Value Proposition

End to end lifecycle management of certified devices

Sales Follow up questions

Could you provide details about the customer's environment ?
How many devices need to be managed?
What is the customer's timeline?
What is the targeted use?
Has the customer already selected the type of device to be used?

What to sell?

Authenticators : Complete Thales portfolio (depending on regions)
Readers : IDBridge
Management : vSEC:CMS / vSEC:CLOUD
IdP: STA
Professional Services Package
Other : SAS/STA for secondary authentication server (Optional)S

FIDO and/or PKI Management

THALES
Building a future we can all trust

Customer Requirement

Replace current MFA solution with FIDO; PKI replacement customer is missing Enterprise managemen (e.g. enrollment and revocation "on behalf of" users); Envolve the FIDO2 by adding management capabilities

Value Proposition

End user deploys combined PKI + FIDO2 credentials integrated with Thales STA allowing both CBA and Webauth

Sales Follow up questions

Could you provide details about the customer's environment ?
How many devices need to be managed?
What is the customer's timeline?
What is the targeted use?
Has the customer already selected the type of device to be used?

What to Sell?

Authenticators: IDPrime or eTokens (combined PIV +FIDO or FIDO only)
Readers : IDBridge
IdP: STA
Management : vSEC:CMS / vSEC:CLOUD
Professional Services Package
Other : SAS/STA for secondary authentication server (Optional)

Benefits of Join Solution

THALES
Building a future we can all trust

- Passwordless & Phishing-Resistant Authentication
- Transitioning Towards a Zero Trust Architecture
- Comprehensive credential management lifecycle
- Simplified Administrative experience
- Regulatory Compliance and Auditability
- Scalable and Cost effective

To know more

- Top 6 reasons for choosing SafeNet eToken Fusion Series **Infographic**

- Credential Management End-to-End Orchestration - **Product Brief**

- Control your fido key life cycle for your workforce – **Solution Brief**

versasec

THALES
Building a future we can all trust

Q&A

Janagaran Annamalai
janagaran.annamalai@thalesgroup.com

Paul Rajkumar
paul.rajkumar@versasec.com

www.thalesgroup.com

PKI and FIDO Authenticators

Endre Pasztor

Senior Pre-Sales Consultant
Identity and Access Management
Thales DIS

www.thalesgroup.com

Presentation Agenda

THALES
Building a future we can all trust

01

Current security challenges

02

Answers (PKI, PIV and FIDO

03

Smartcards and PKI

04

FIDO (Fast Identity Online)

05

IDPV (IDPrime Virtual)

06

Demo (IDPrime Virtual)

07

Q & A

08

THALES
Building a future we can all trust

What are the current security challenges?

www.thalesgroup.com

THALES
Building a future we can all trust

Password is the new mainframe

THREAT

‘12345678’
‘password’

Still the most popular passwords

84%

Data breaches related with weak or stolen passwords

COST

20-50%

Helpdesk calls are password related

HASSLE

130

Accounts associated with an email address

50-80%

Users reuse password across accounts

THALES
Building a future we can all trust

Answers

PKI, PIV and FIDO

www.thalesgroup.com

The raise of requirements for Phishing-Resistant authentication

THALES
Building a future we can all trust

Since 2021, to protect sensitive data from rising cyber threats, Governmental cybersecurity agencies are increasing their requirements and IAM market analysts are recommending the use of phishing-resistant authentication methods (US EO14028, CISA, NIST, ENISA, Gartner ..)

"Federal agencies must require their users to use a **phishing-resistant methods, FIDO2, PIV and derived PIV** to access agency-hosted account",

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

"Avoid using SMS and voice calls. Instead consider deploying **phishing-resistant** tokens such as **smart cards** and **FIDO2 security keys**,

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

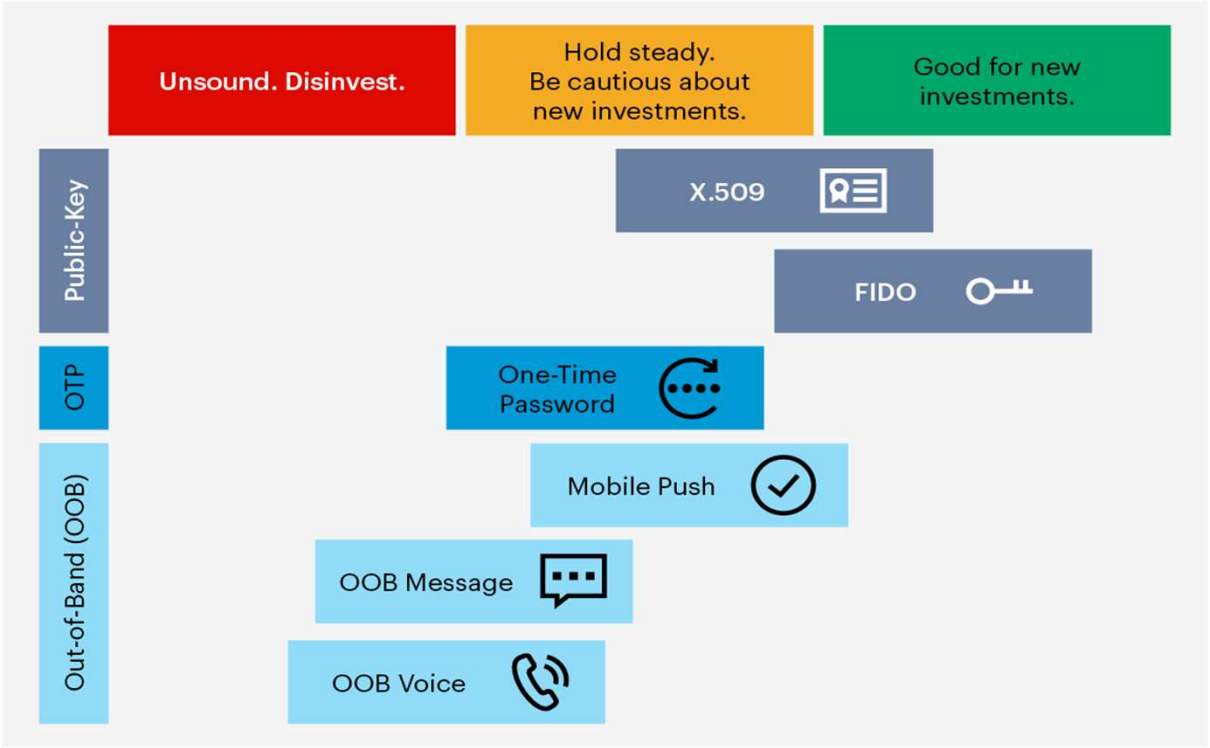
"Enforce phishing-resistant MFA to the greatest extent possible" ,

CISA Guidance on **Phishing-Resistant and Number Matching MFA**,

What Gartner says

THALES
Building a future we can all trust

The Strategic Value of Different Kinds of Authentication Token



Source: Gartner
724226_C

Gartner

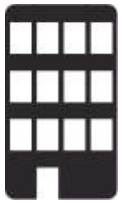
THALES
Building a future we can all trust

Smartcards and PKI

www.thalesgroup.com

Addressing security across industry segments

THALES
Building a future we can all trust



Enterprise

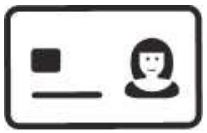
Healthcare

Law Enforcement

Critical Infrastructure

Government and Municipalities

with many use cases



Physical/Logical Access

Digital Signature

Email Encryption

Endpoint Protection

Thales Smart Card Benefits

THALES
Building a future we can all trust

Plug & Play
minidriver enabled smart cards

Different interface options
Contact / Contactless / Hybrid

High security levels
FIPS 140-2 Level 2 and Level 3
Common Criteria EAL5+ / eIDAS

Customization support
IDPrime smart cards support tailored branding and printing on the smart card, as well as serial number engraving and customized security features

Various applets
PKI / FIDO / PIV

Enhanced cryptographic
RSA (RSA 4K)& Elliptic curves (ECC 521)

Flexible security policy
Extended on-board PIN Policy

Thales Token Benefits

THALES
Building a future we can all trust

Plug & Play
minidriver-enabled tokens

Different form factors
USB-A / USB-C / Contactless

High security levels
FIPS 140-2 Level 2 and Level 3
Common Criteria EAL5+ / eIDAS

Customization support
IDPrime tokens support tailored branding and printing on the tokens, as well as serial number engraving

Various applets
PKI / FIDO / PIV

Enhanced cryptographic
RSA (RSA 4K)& Elliptic curves (ECC 521)

Flexible security policy
Extended on-board PIN Policy

Hybrid cards – Integration with major Physical Access Control vendors

NXP

- Mifare Classic
- Mifare DESFire EV1/EV2/EV3

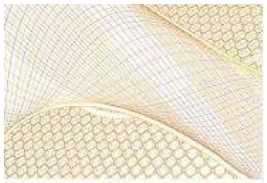
HID

- Prox
- IClass
- SeOS

Legic

- Prime
- Advant

Card body security features

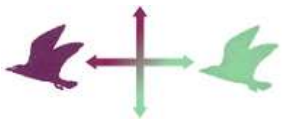


Guilloche
- Continuous thin lines
- Non-repetitive on detail level
- Provides **basic protection** for the card body **against scanning and copying**

Rainbow printing
- **Colors change continuously** along printed lines, typically from one colour to another and back
- Unlimited number of colors achieved provides **protection against copying and reproduction**

UV Printing
- Security printed element printed with special inks
- Inks become visible when illuminated with UV light

Microtext
- Basic **copy and scanning protection**
- Small characters that look like a line when looked without a loupe (200-300 microns in height)
- May consist of deliberate errors



OVI
- Special high-security printing ink typically used to print a logo or text
- Color changes when tilting the card
- The optically variable effect **cannot be copied**

Holographic overlay
- Holographic element within a plastic protective layer on top of personal data
- **Protect** the personalization **against wear and tear**

Credential Management

Versasec vSEC:CMS - Full Credential Lifecycle Management

Card Management System

- Comprehensive authentication and credential management server
- For enterprise deployments needing:
  - ✓ Life cycle management
  - ✓ Provisioning of PKI certificates and tokens
  - ✓ Provisioning of FIDO smartcards and tokens
  - ✓ PKI-based strong authentication and digital signing
  - ✓ FIDO-based strong authentication

THALES
Building a future we can all trust

Thales partners with Versasec to offer the most comprehensive identity access and authentication management solutions

THALES

Middleware

THALES
Building a future we can all trust

Advanced Management

SafeNet Authentication Client (SAC)

- Full device management solution
- Designed for large deployments needing
- Windows / Linux / Mac
- PKCS#11, CAPI / CNG

Light Management

SafeNet Minidriver

- Plug-and-Play solution in Windows environment.
- Limited device management (PIN change, card unblock)
- CAPI / CNG

THALES
Building a future we can all trust

FIDO (Fast IDentity Online)

www.thalesgroup.com

What is FIDO? (Fast Identity Online)

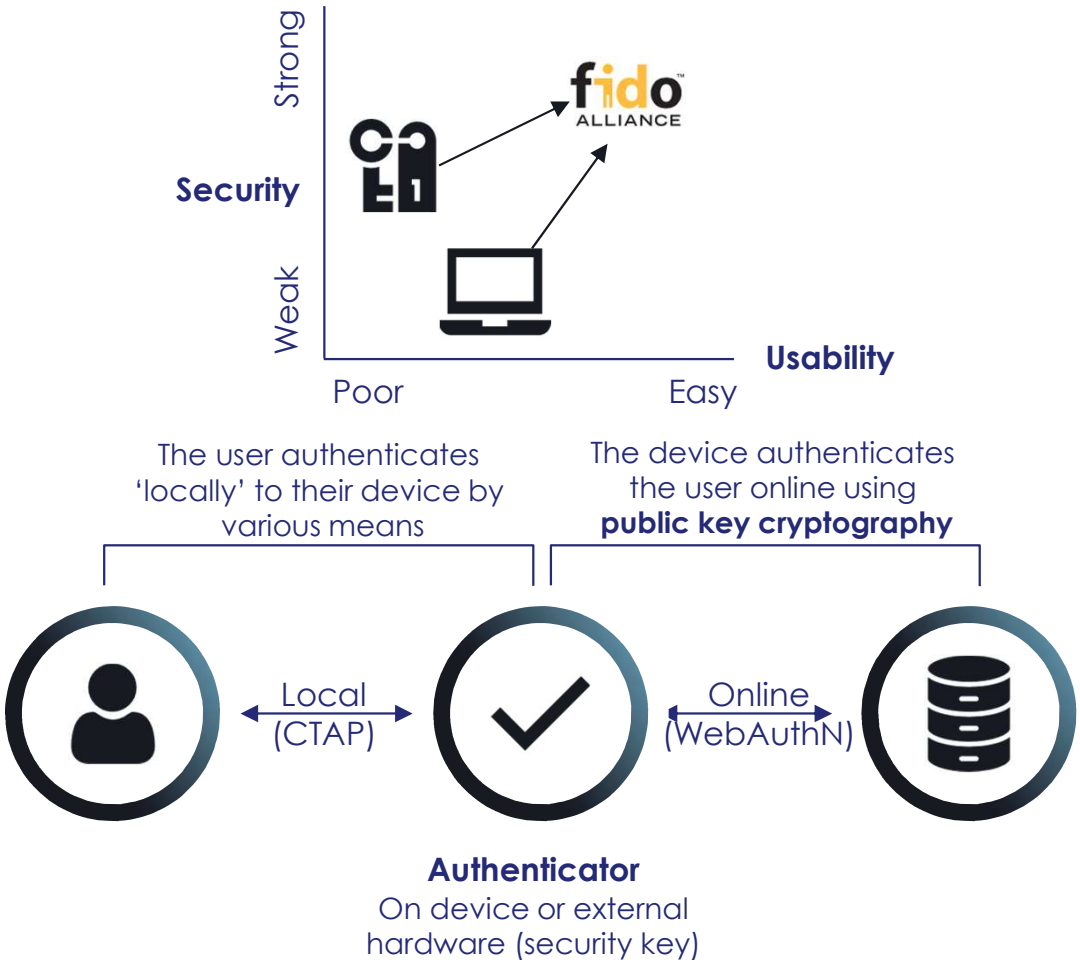
THALES
Building a future we can all trust

Mission

- Authentication standard
- Reduce world's reliance on passwords

250+
members

600
FIDO certified solutions



FIDO Authentication Benefits

THALES
Building a future we can all trust

Strong Security in Authentication

- Asymmetric Public Key Cryptography
- Possession Based Authentication

Passwordless and Anti Phishing

- Keys bound to a domain; if fake, authentication fails

Prevent MIM (Man in the Middle Attacks)

- Keys stored locally in the FIDO device
- Eliminates dependence on server-side credentials

Simple to set up and use

- Single gesture, password removed and replaced by PIN
- Open standards, no infrastructure to deploy

Thales FIDO Devices

SafeNet eToken Fusion NFC / FIDO

SafeNet IDPrime FIDO

Combined use cases

THALES
Building a future we can all trust

From PKI to FIDO

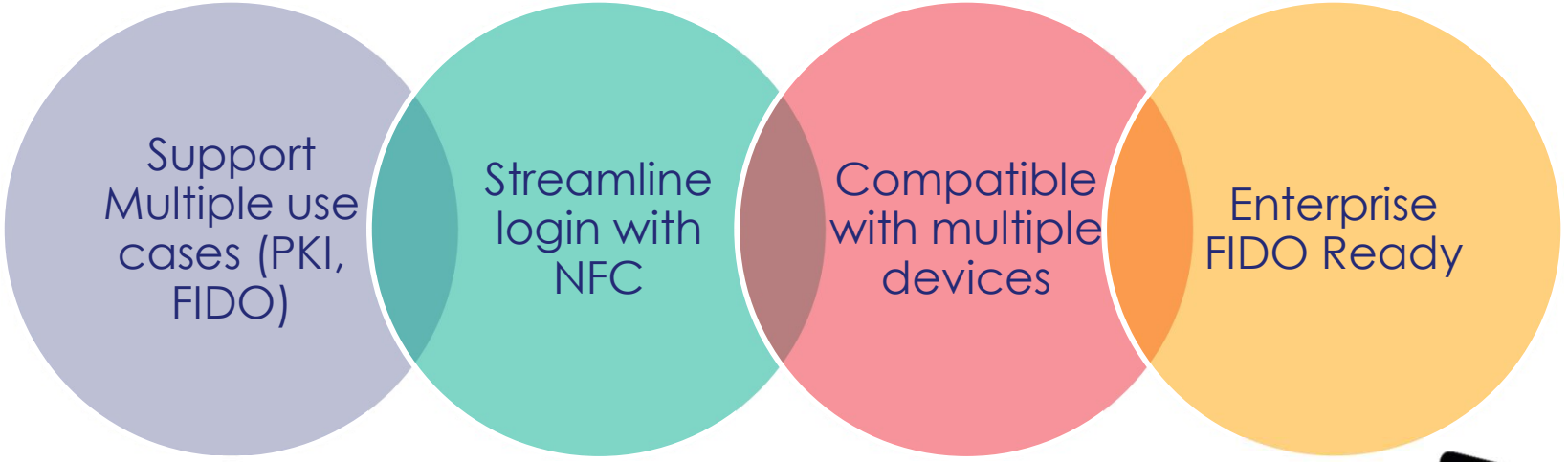
- Combined products for easy migration
- Best-in-class certifications
- Support both technologies at the same time

Converged badge

- One badge for Physical & Logical access
- Simple to use & carry
- Can also be combined with PKI

SafeNet eToken Fusion NFC

THALES
Building a future we can all trust



FIDO 2.1 Features

THALES
Building a future we can all trust

Credential Management

- Option to see which FIDO credentials were generated
- Option to delete credentials
- Only for discoverable credentials (Resident keys)

Enforce PIN Authentication

- Even if the FIDO Server is not requesting PIN for authentication, the device will enforce PIN as 2FA

Minimum PIN length

- Option to configure minimum PIN Length
- Option to enforce PIN change after configuration

FIDO 2.1 Features – Thales Proprietary Features

Non-Managed Mode

- Default FIDO Standard configuration – all configurations could be executed with the FIDO User PIN

Managed-Mode

- Thales proprietary configuration
- Specific configurations will be allowed only with additional Authentication layer – **FIDO Admin PIN**
- Option to get the Managed device either by
  - from Thales factory
  - Customer will have the option to move from the 'Non-managed' mode to 'Managed' mode

FIDO 2.1 Features – Thales Proprietary Features

Whitelist Management

- Option to decide which application s or services will be allowed to be used with the FIDO key
- Option to add/remove services

Reset Keys Block

- Option to block ‘Keys reset’ from different applications or tools

PIN unblock

- If the FIDO PIN is blocked after 5 attempts, there is an option to unblock either with Admin PIN or with Challenge response
- Feature is available only in Managed mode

THALES
Building a future we can all trust

IDPV (IDPrime Virtual)

www.thalesgroup.com

Why do we need a new PKI solution?

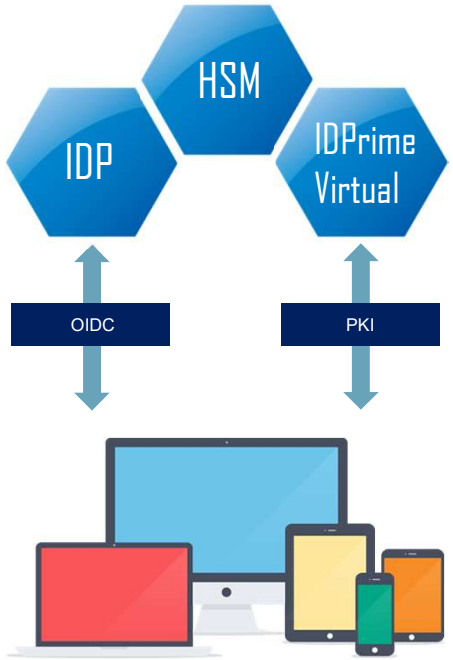
VDI & BYOD

Contractors

Backup

Mobility

Smartcards do not fit for modern use cases



Enable all use cases on any devices

Multiple solutions on the market

Thales – IDPrime Virtual

- Available on any machine upon 2FA
- Credentials follow the user

User centric

Solution

- Server-side provisioning
- No user friction
- Windows, Linux & MAC(Roadmap)

Alternatives

- Credentials deployed on a single TPM
- Provisioning required to each device

Device centric

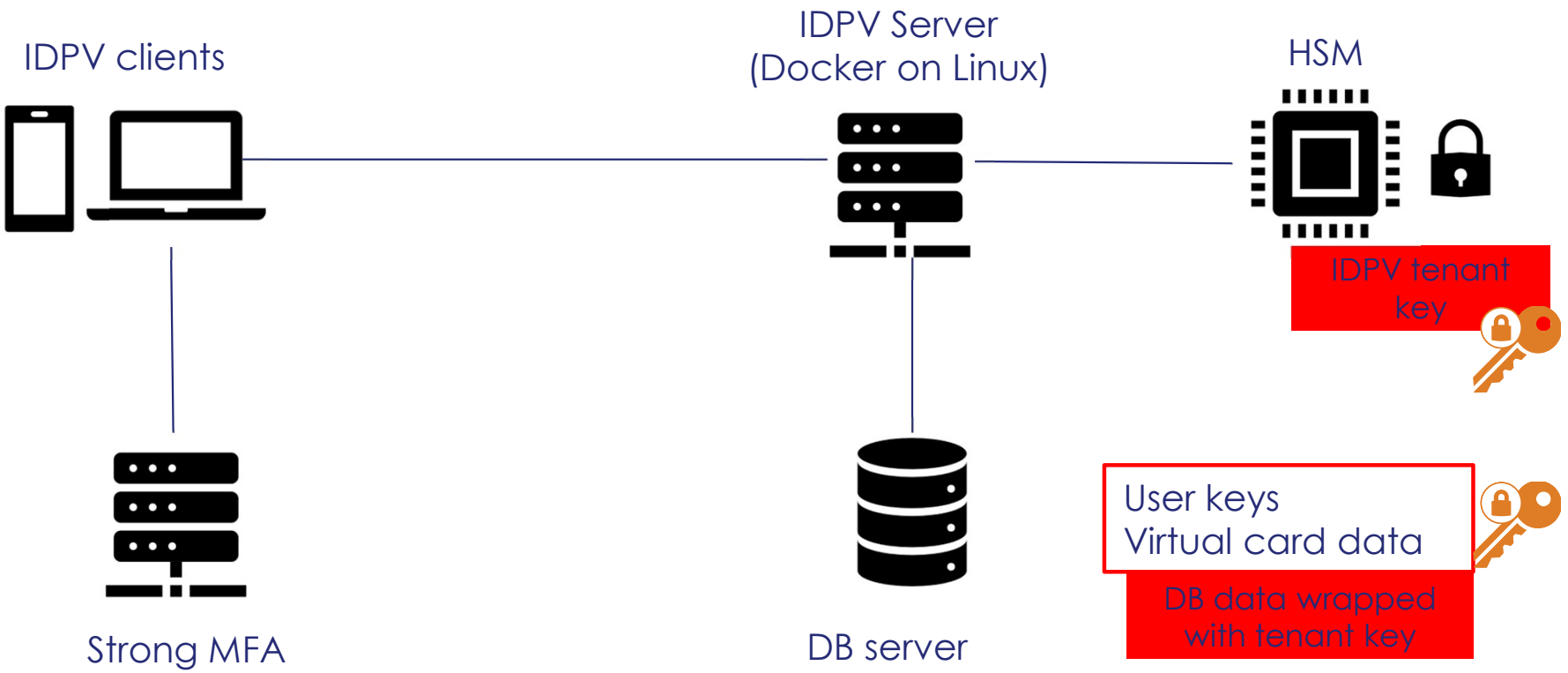
Solution

- Limited to TPM & Windows devices
- Each device must be provisioned

SafeNet IDPrime Virtual (Key Benefits)

- VDI , BYOD and mobility
- Temporary / smart card replacement
- Digital Signature Enablement
- API based smartcard management
- User Centric Approach (Use the same smartcard from any device anywhere)
- Highly Flexible Deployment (user-centric (Online)or device-centric (Offline))
- Integrations with several CMS

IDPV system architecture



VMware Workspace ONE and PIV-D

THALES
Building a future we can all trust

- The VMware Workspace ONE (WS1) platform supports the use of derived Personal Identity Verification (PIV-D) credentials on mobile devices
- The solution is based on the Workspace ONE PIV-D Manager mobile app, and integration with partners that provide PIV-D services
- The purpose of the solution is to make PIV-D certificates available to mobile apps on end user devices
- The scope of the solution is
  - Android, iOS, and iPad devices
  - VMware Workspace ONE apps, such as Boxer and Content
  - Native apps such as Chrome, Apple Mail, and Safari

THALES
Building a future we can all trust

Demo

www.thalesgroup.com

Thank you

Q&A

Endre Pasztor
endre.pasztor@thalesgroup.com

www.thalesgroup.com


THALES
Building a future we can all trust
THALES
Thales FIDO Keys with vSEC:CMS with STA & Entra ID
Thales FIDO device-Bound Passkeys & CMS offering
Rudolf Solman FIDO Pre-Sales (EMEA)
www.thalesgroup.com

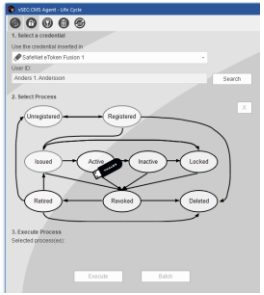
Table of contents

Our Proposed solution for customer with STA/Entra ID

1. Authentication with FIDO authenticators

- Logical Access
- FIDO BIO/Contact / Contactless

2. LIFE CYCLE Management



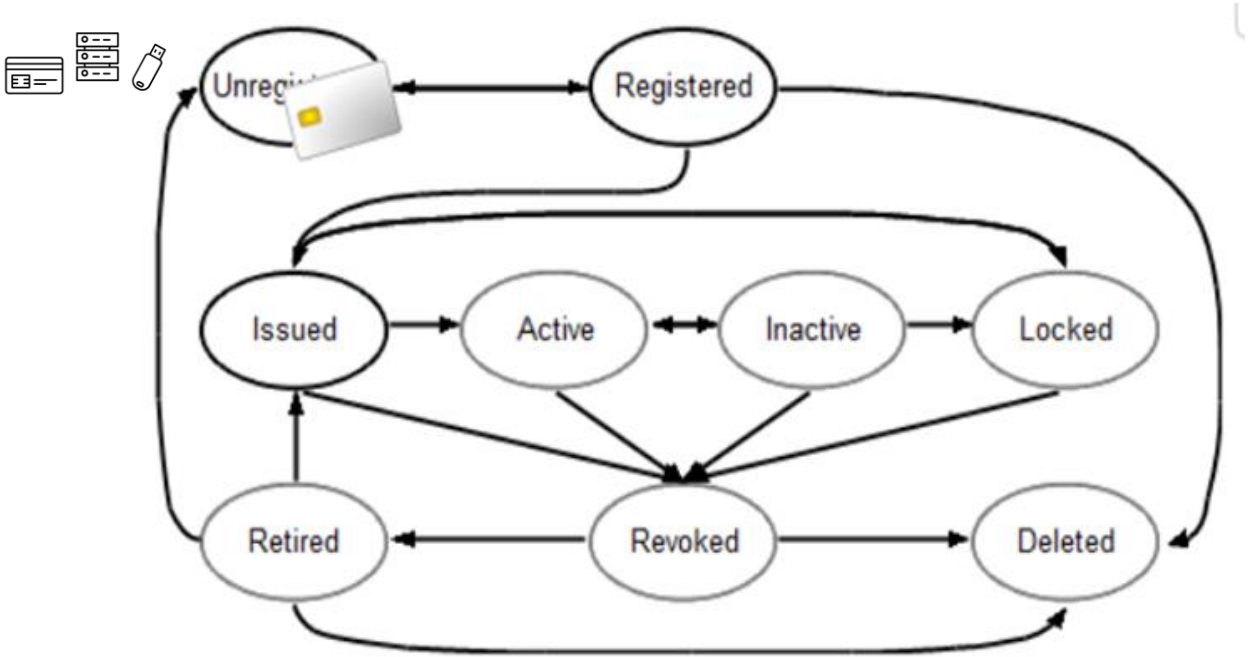
- Solution for large FIDO deployments
- Automated processes
- Integration with Entra ID IDP
- Issuance on behalf of

THALES
Building a future we can all trust

vSEC:CMS

www.thalesgroup.com

Full control over FIDO/PKI authenticator lifecycle



Hosting Environments

Versasec offers its award-winning credential management system for different hosting environments.

vSEC:CMS | On-prem

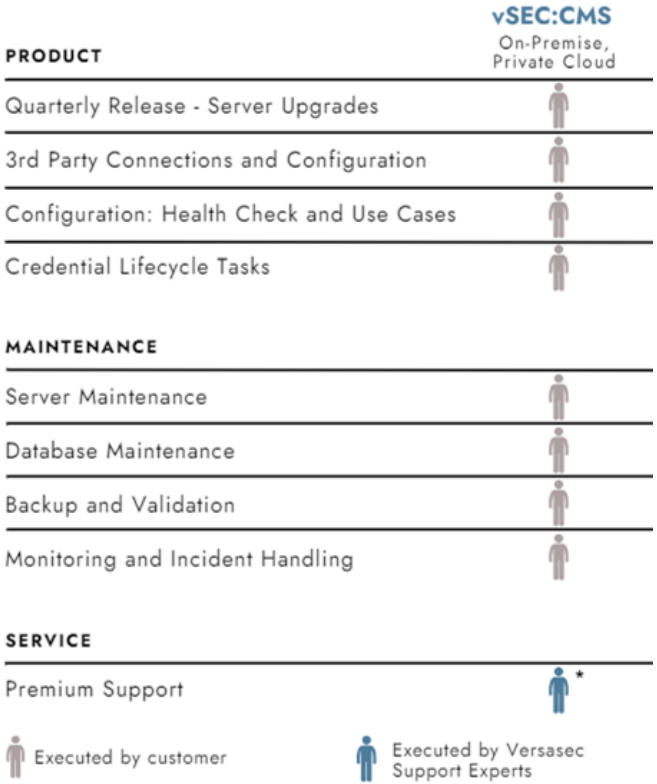
Control and flexibility while reducing external access and dependencies. Hosted in your own servers, following the security policies and guidelines established by your company.

vSEC:CMS | Private Cloud

Enable cloud benefits of high availability and scalability in your own managed cloud. Control the architecture and maintenance, security, operating systems, and software upgrades as well as all costs.

vSEC:CLOUD | Versasec Cloud

Enjoy the benefits of cloud services with flexible subscription packs. Deployed using an industry best practice architecture, managed and maintained by Versasec cloud operations experts.

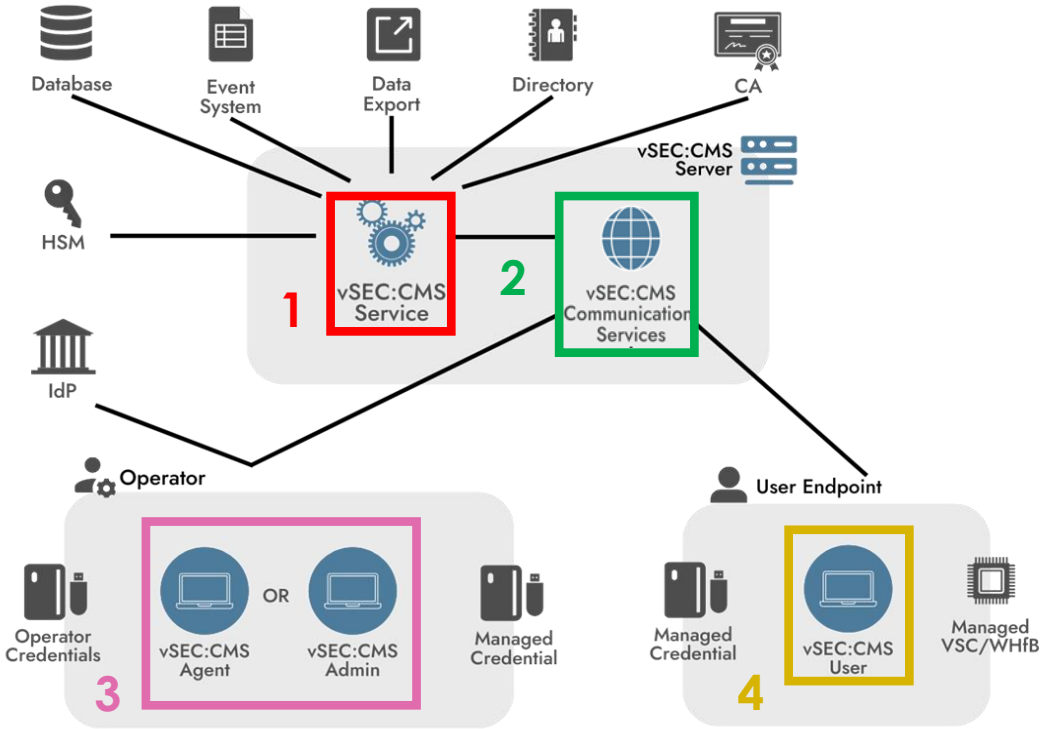


THALES
Building a future we can all trust

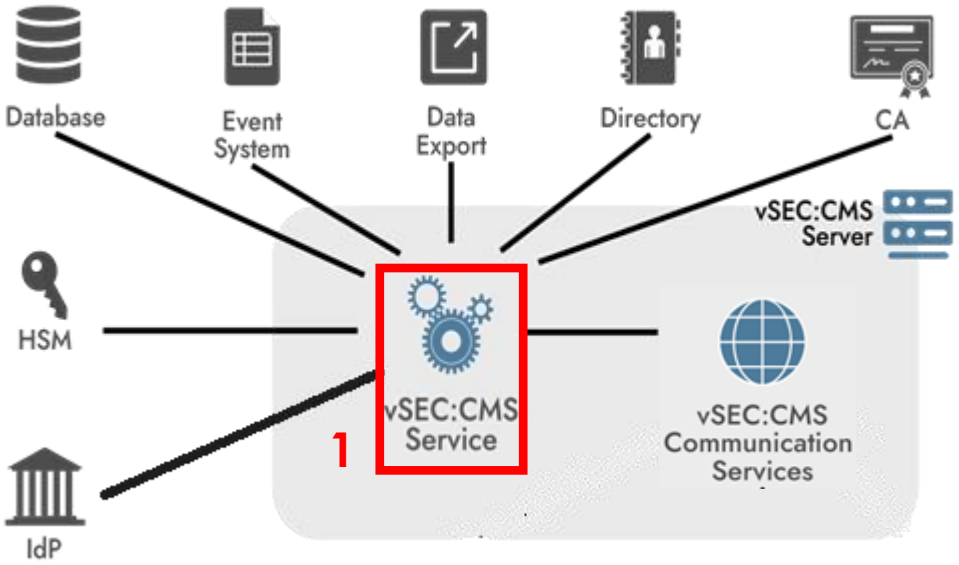
vSEC:CMS Architecture

www.thalesgroup.com

vSEC:CMS Architecture (on-prem)



1 of 4 main components: vSEC:CMS Service



Windows server 2016, 2022

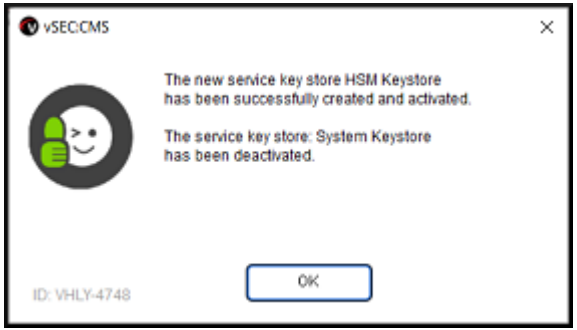
HSM

- Storage for master keys in vSEC:CMS administration key operations
- Key operations include credential registration and PIN unblocking
- vSEC:CMS leverages the PKCS#11 interface provided by HSMs

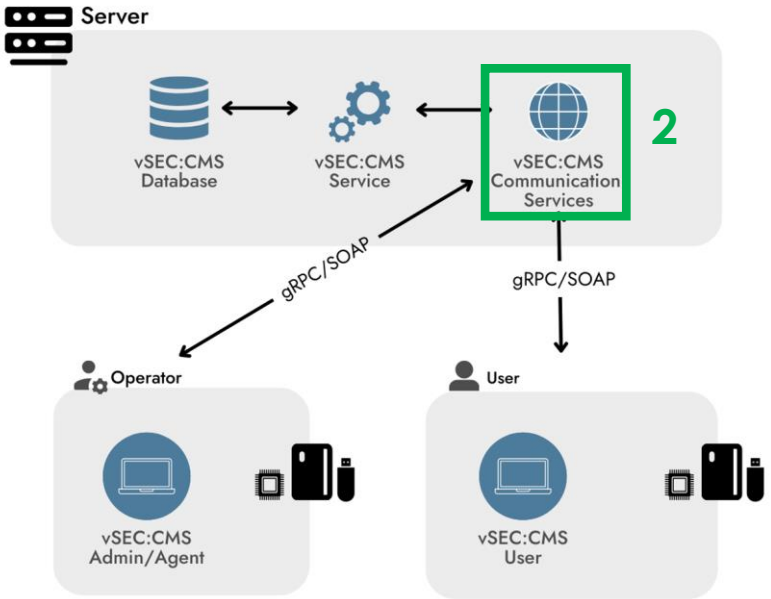
- Integration with Thales HSMs:
  - Thales Safenet Luna HSM version 7
  - Thales DPoD

- Integration with 3rd Party HSM's:

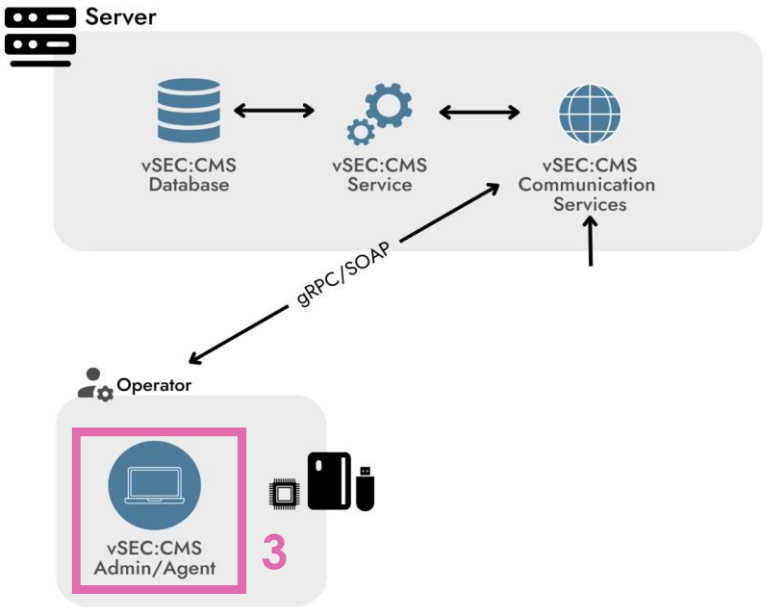
https://versasec.com/docs/versasec_credential_management.pdf



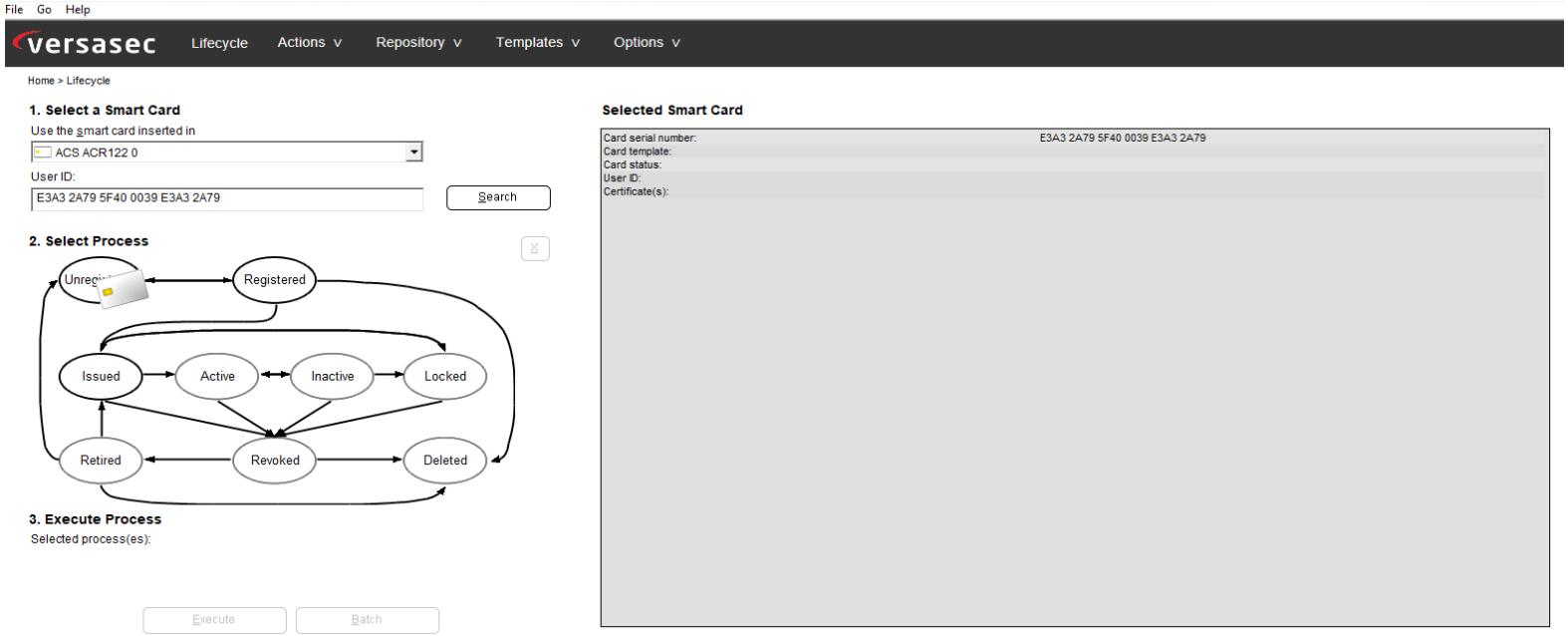
2 of 4 main components: vSEC:CMS SOAP /gRPC



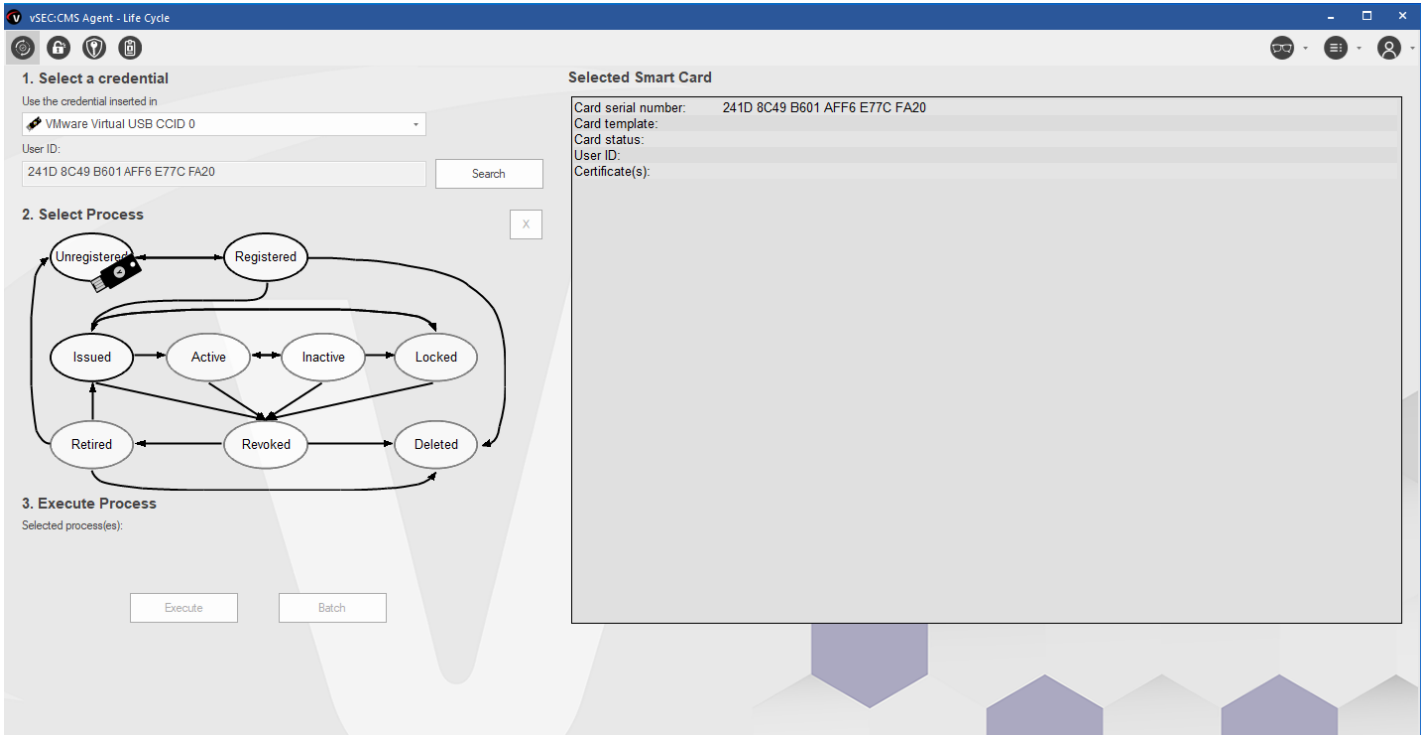
3 of 4 main components: vSEC:CMS Agent or Admin



3 of 4 main components: vSEC:CMS Admin Console

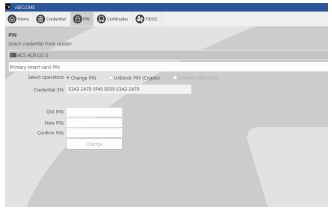


3 of 4 main components: vSEC:CMS Agent Console

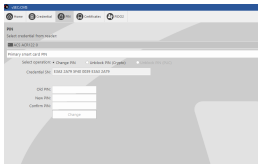


4 of 4 main components: vSEC:CMS User

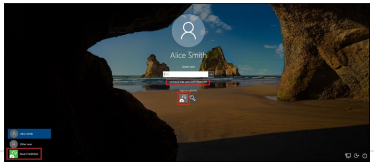
1.User App

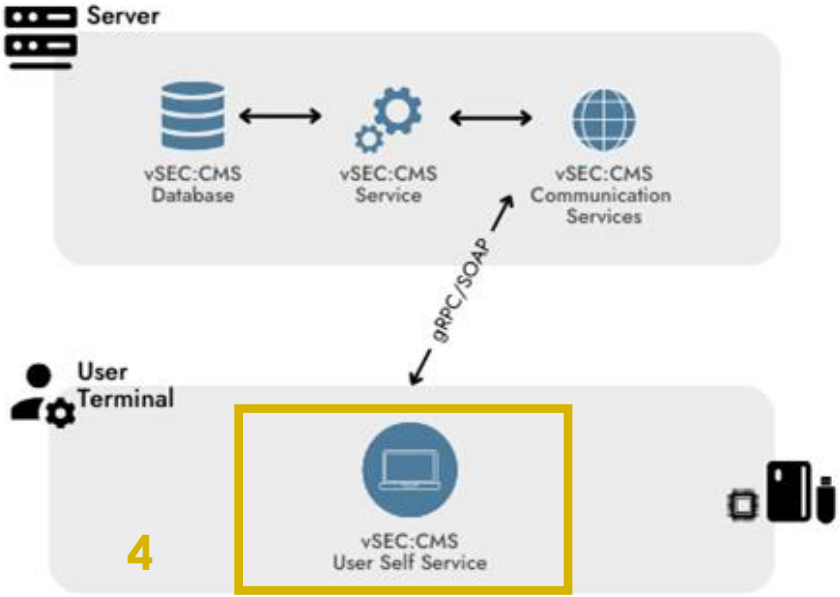


2. Webstart (API) + User App

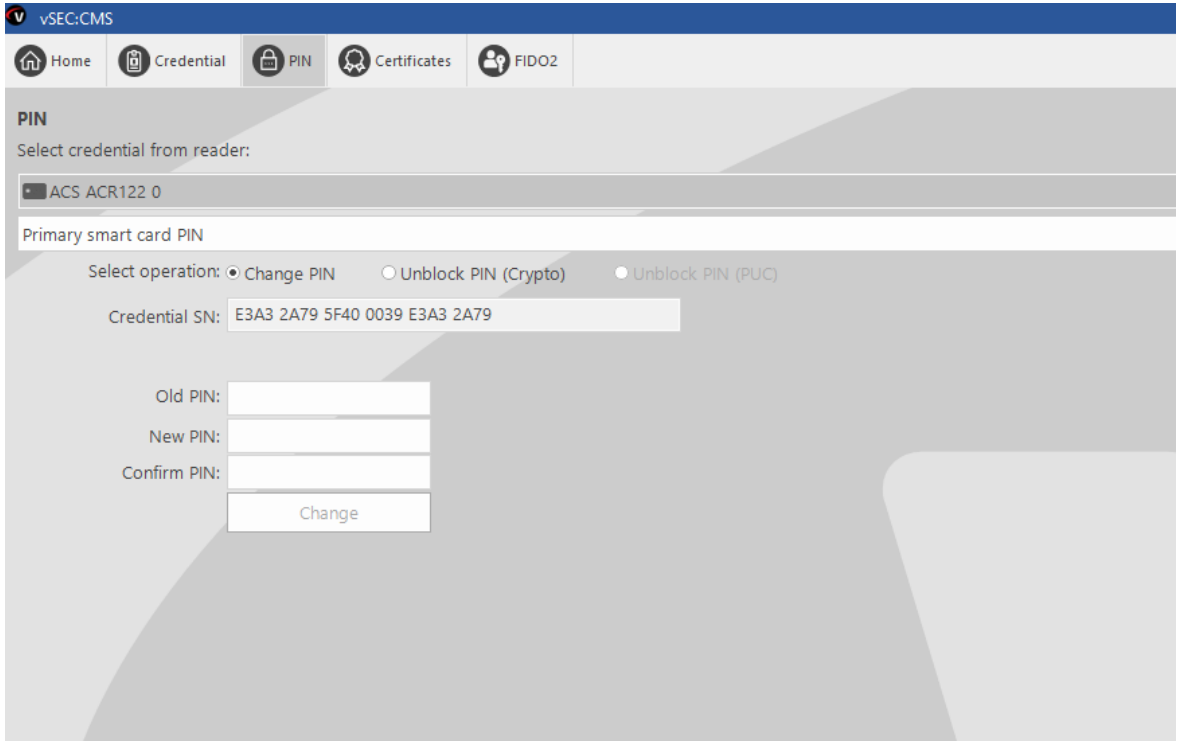


3. Credential provider App

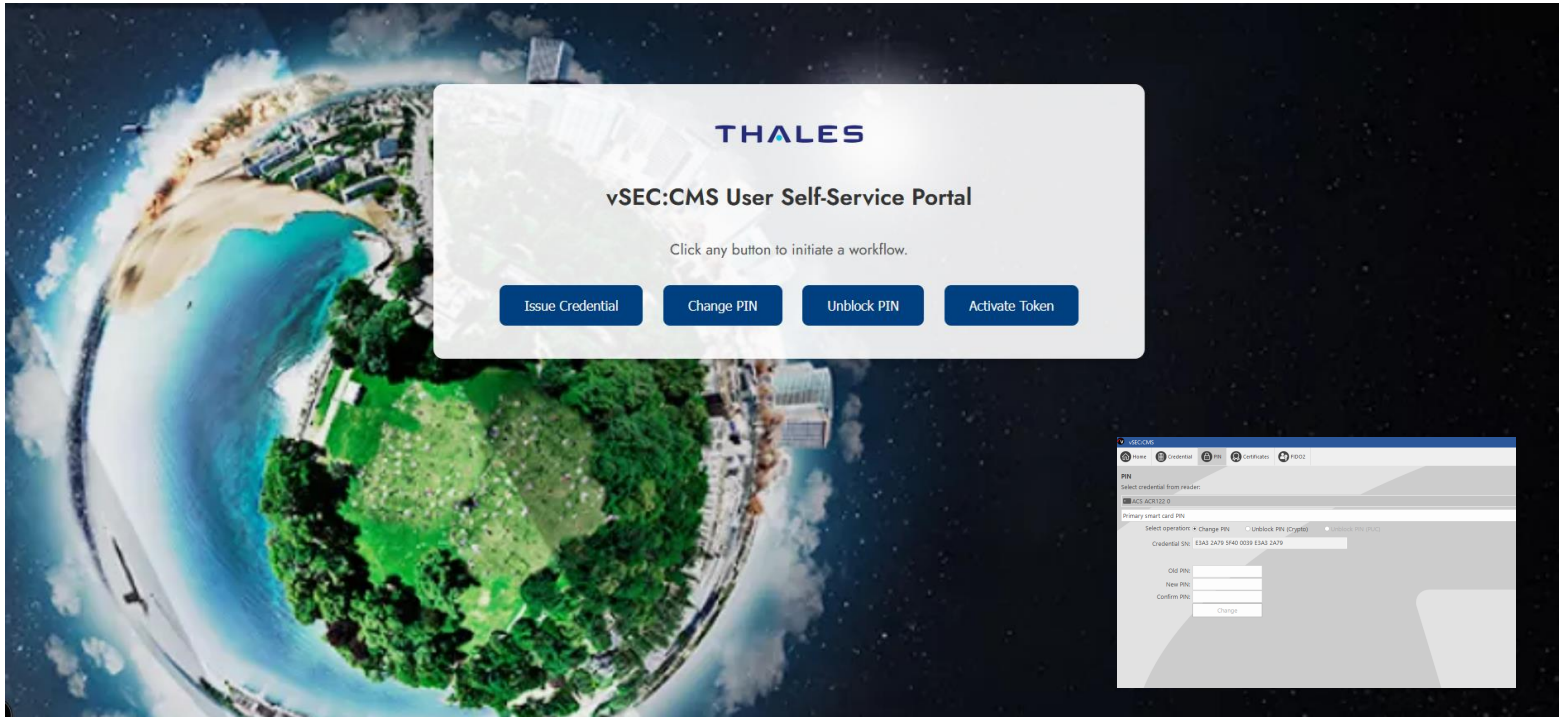




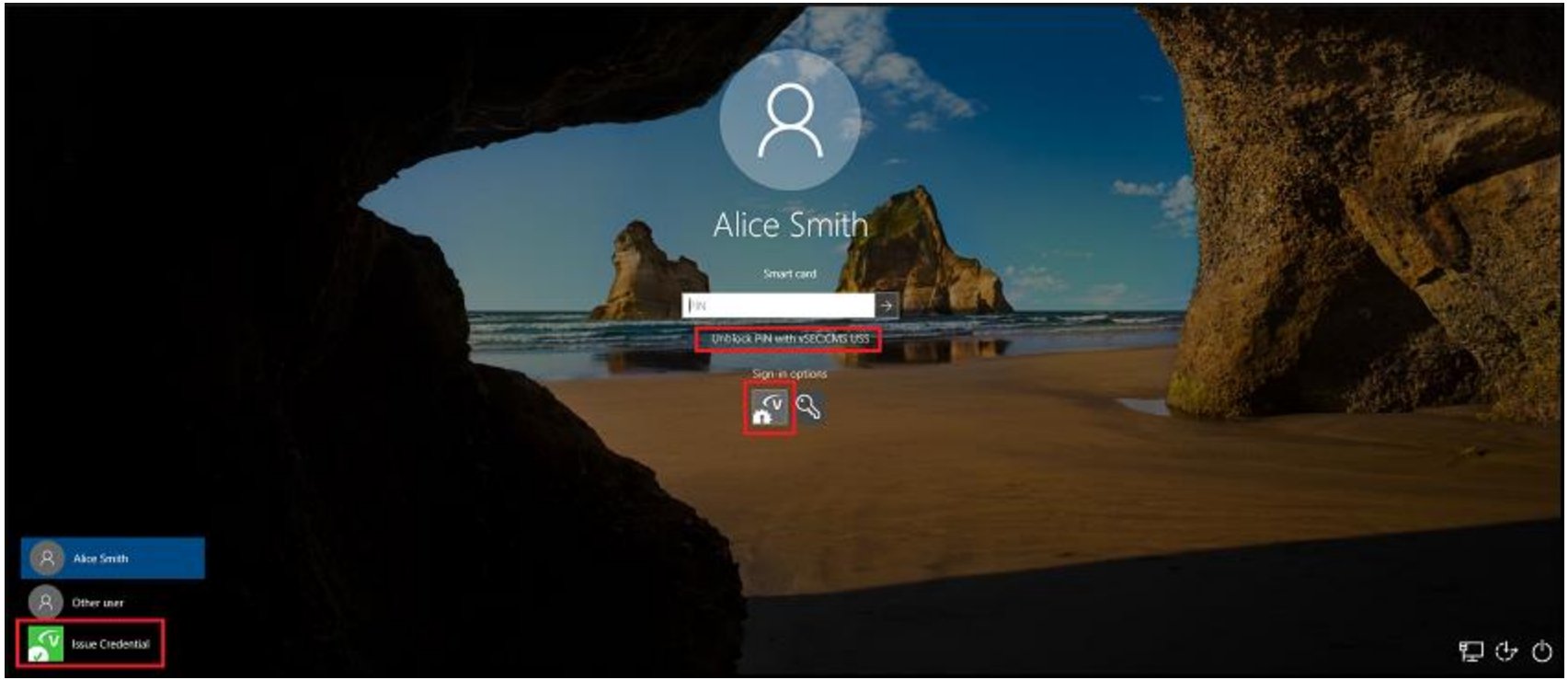
4 of 4 main components: vSEC:CMS User App



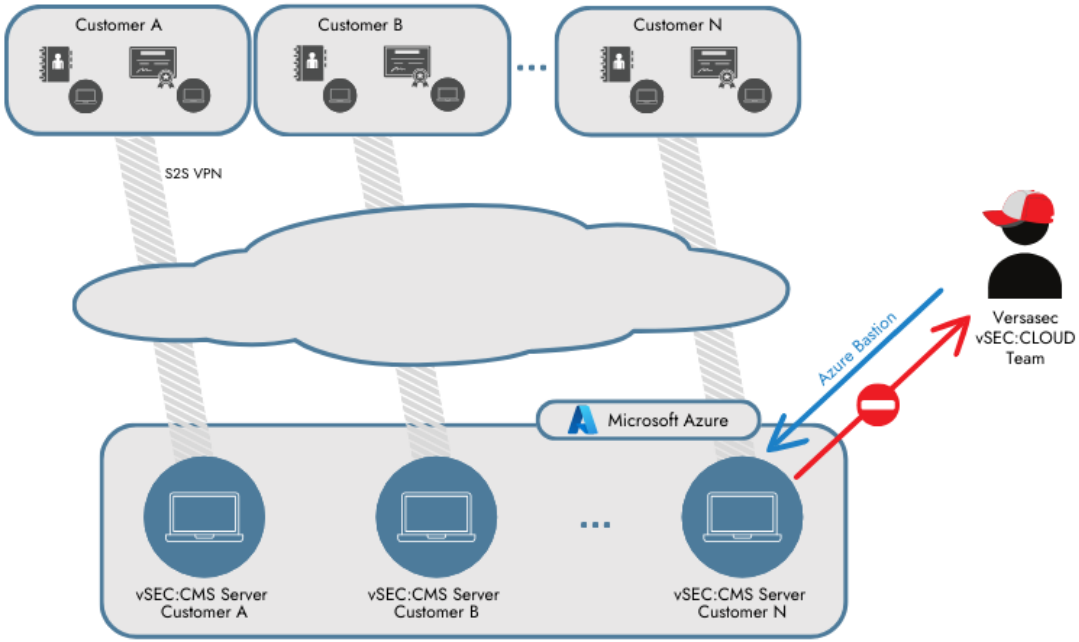
4 of 4 main components: vSEC:CMS WebStart



4 of 4 main components: vSEC:CMS Credential Provider



vSEC:CMS:CLOUD



Integration with Thales Authenticators

PKI

IDPrime.NET 510
IDPrime.NET 5500
IDPrime MD830/MD840
IDPrime MD 930/940
IDPrime MD 3810/3840
IDPrime 3930/3940
IDPrime PIV 2.1
IDPrime PIV 3.0
IDPrime Virtual
Thales MultiApp ID
Safenet eToken 5100/5110 FIPS
Safenet eToken 5300
Thales eToken 5110+CC(940C)
Thales SafeNet IDPrime 940cc

Combined PKI and FIDO

IDPrime 3940 FIDO
IDPrime 3930 FIDO
SafeNet eToken Fusion CC
SafeNet eToken Fusion

SafeNet IDPrime Virtual

FIDO only

SafeNet eToken FIDO
Thales IDPrime FIDO Bio

CMS Database and External Database

CMS Database usage

Stores information about credentials registered and managed by the vSEC:CMS along with configuration settings

Sizing

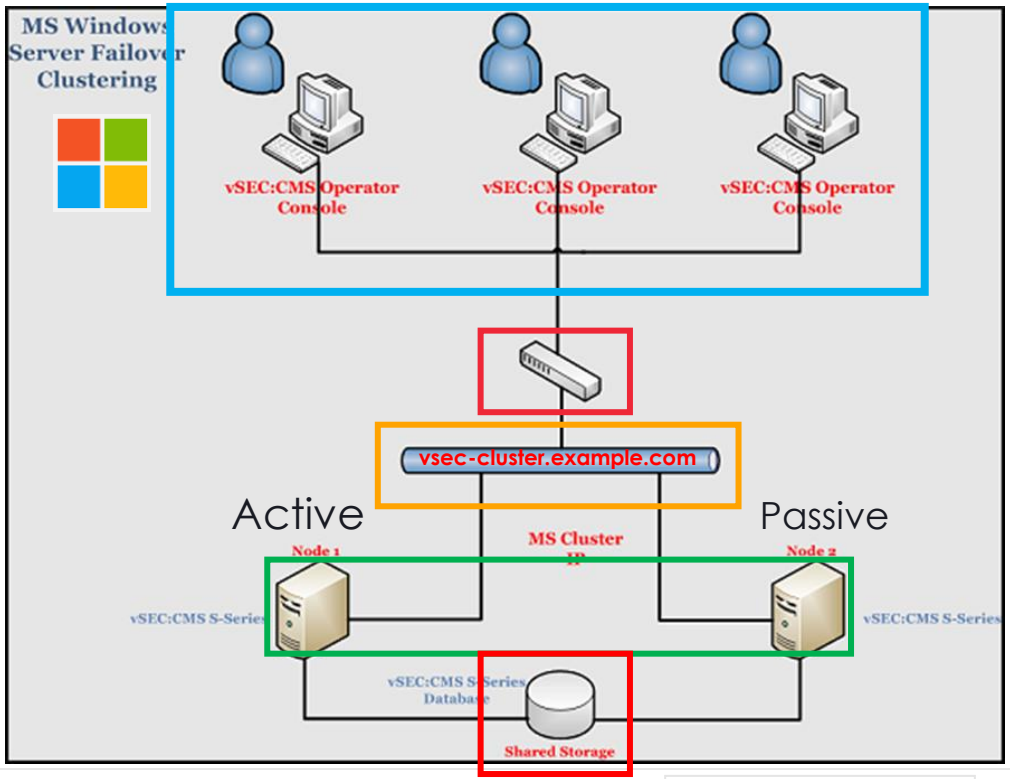
For a typical system of 1 thousand managed credentials you could expect 100 MB to be allocated for your database.

External Database

The following versions of MS SQL Server are supported 2017, 2019, 2022, Azure SQL.

https://support.versasec.com/hc/en-us/articles/360014232180-Configure-MS-SQL-as-vSEC-CMS-Database

Microsoft Windows Server Failover Clustering (WSFC)



- High Availability
- Centralised Database

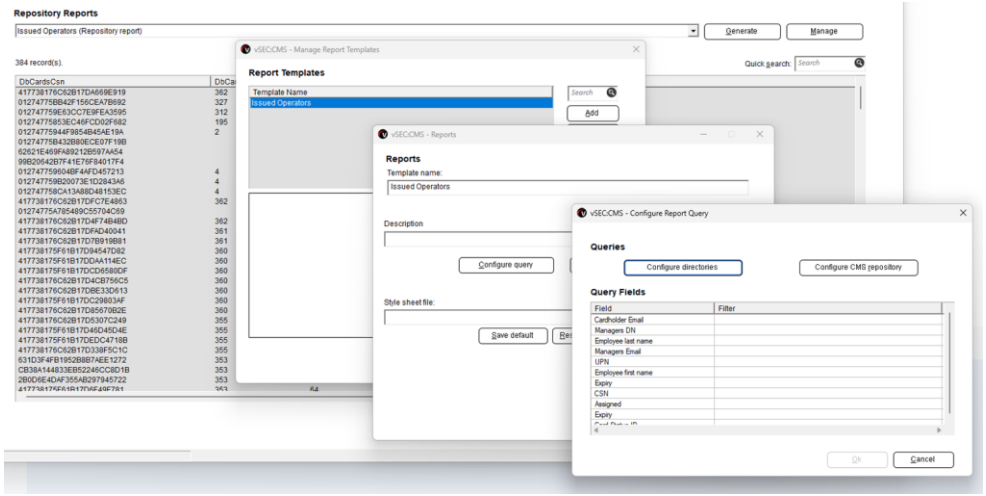
THALES
Building a future we can all trust

vSEC:CMS Features

www.thalesgroup.com

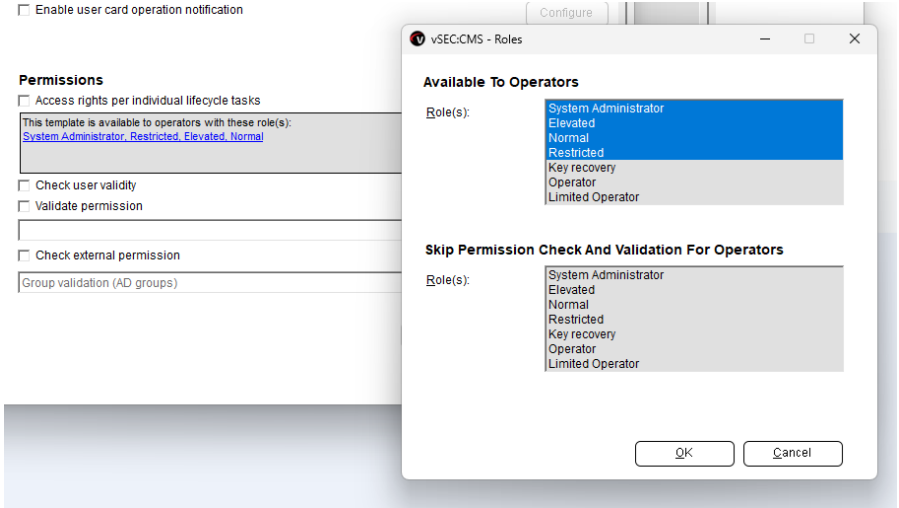
Reporting

- **Built in custom reporting**
- **Custom customer defined reporting using SQL or REST API**



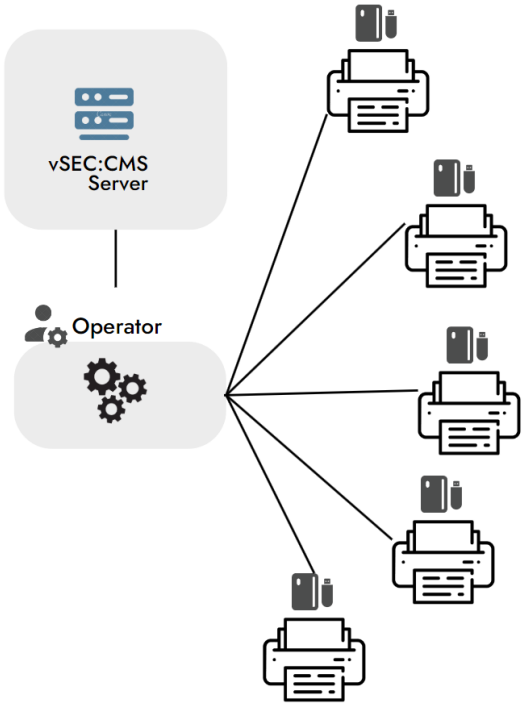
Admin Permission Roles

- Roles for least privilege access
- Configurable roles with custom permissions and access
- Issuing, Revocation, PIN Unblock, Configuration, Repositories, Key recovery …
- Windows Group Permission



Batch Issuance Station

- In parallel batch issuance
- One operator orchestrates multiple Smart Card printers
- For high volumes

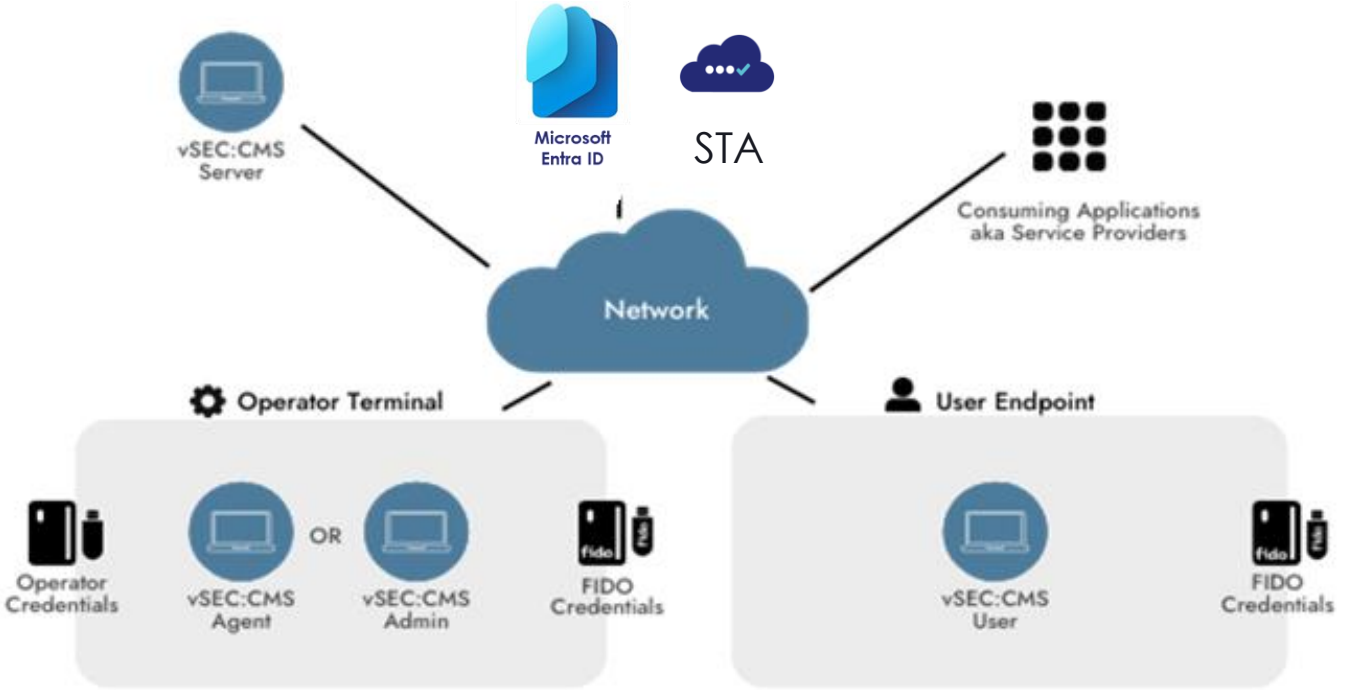


THALES
Building a future we can all trust

FIDO 2.1 with vSEC:CMS

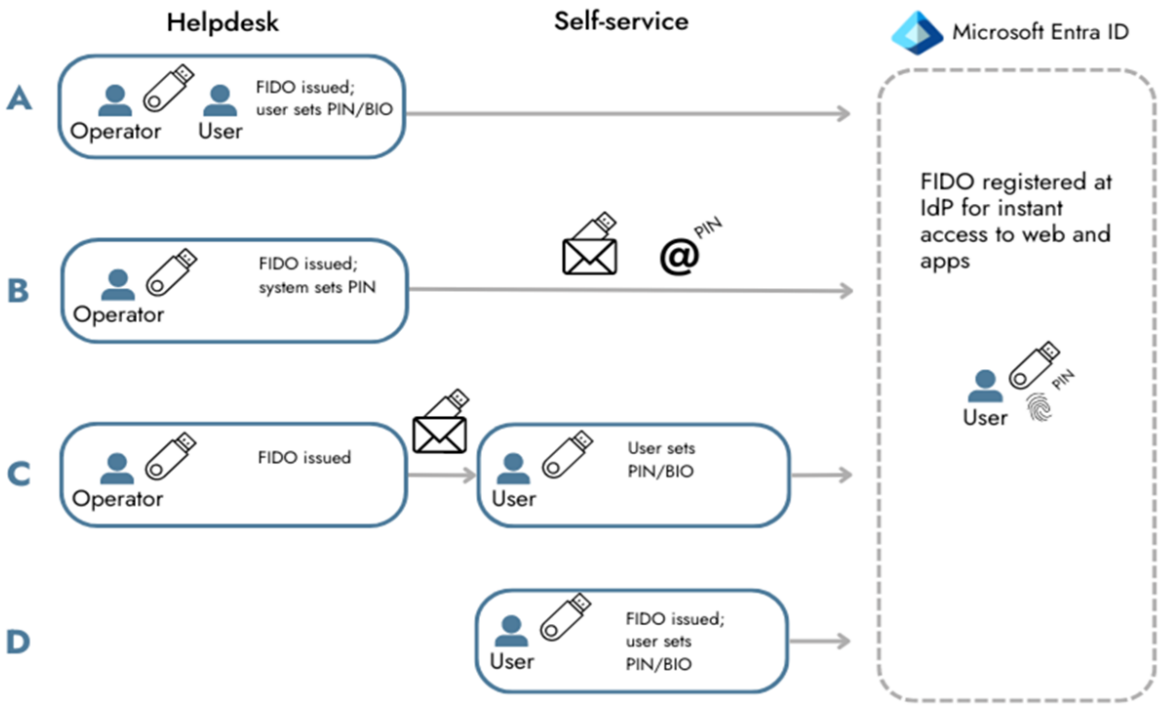
www.thalesgroup.com

vSEC:CMS FIDO Architecture

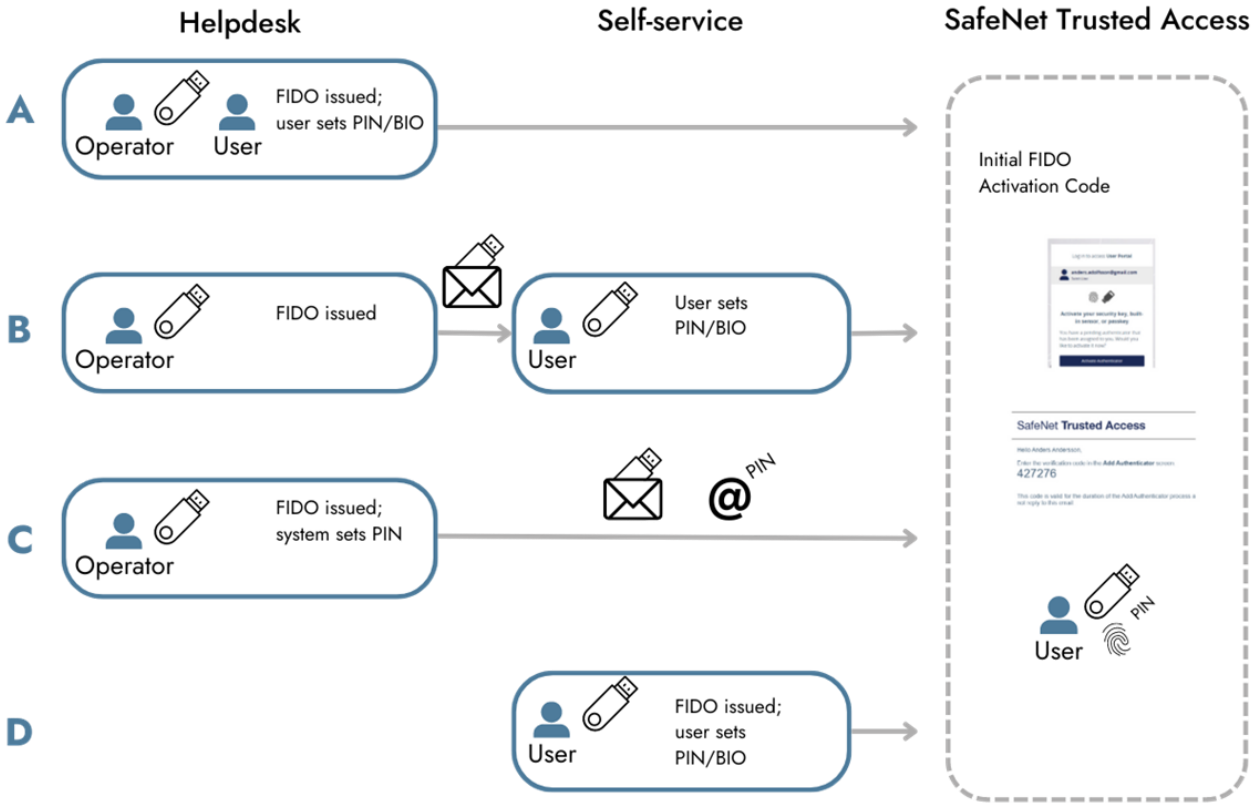


https://support.versasec.com/hc/en-us/articles/4856105329298-FIDO2-Support

Enrollment Methods with Entra ID



Enrollment Methods with STA



FIDO 2.1 with vSEC:CMS Solution

Thales FIDO
Enterprise Features

FIDO PIN unblock

FIDO 2.1 Standard

Enforce PIN change

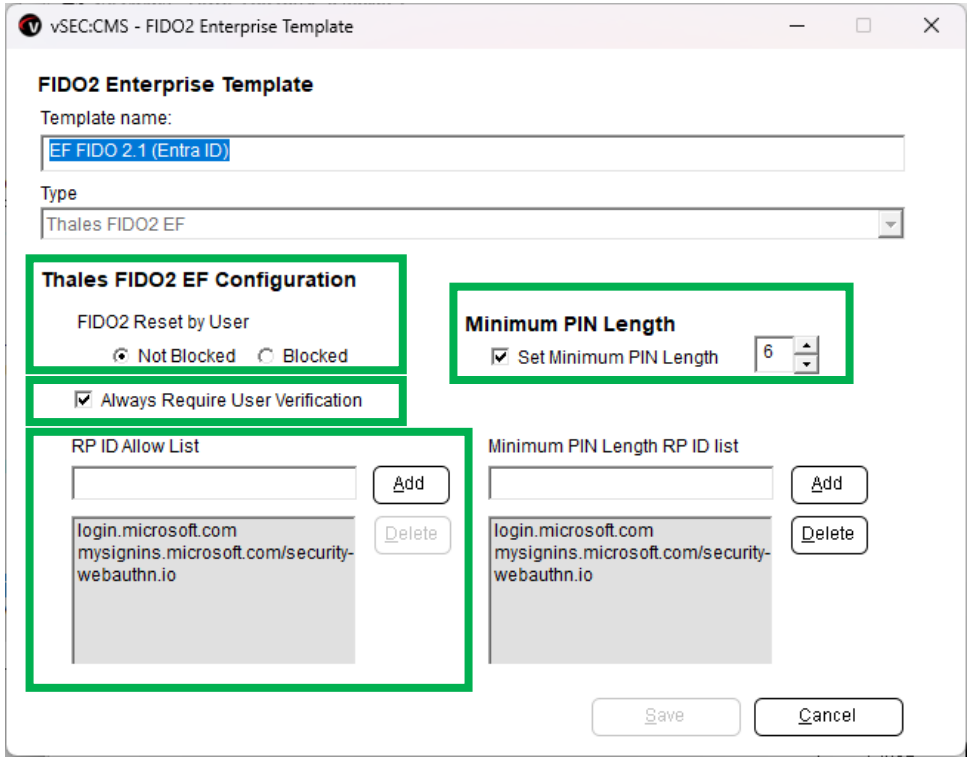
Enforce PIN
Authentication

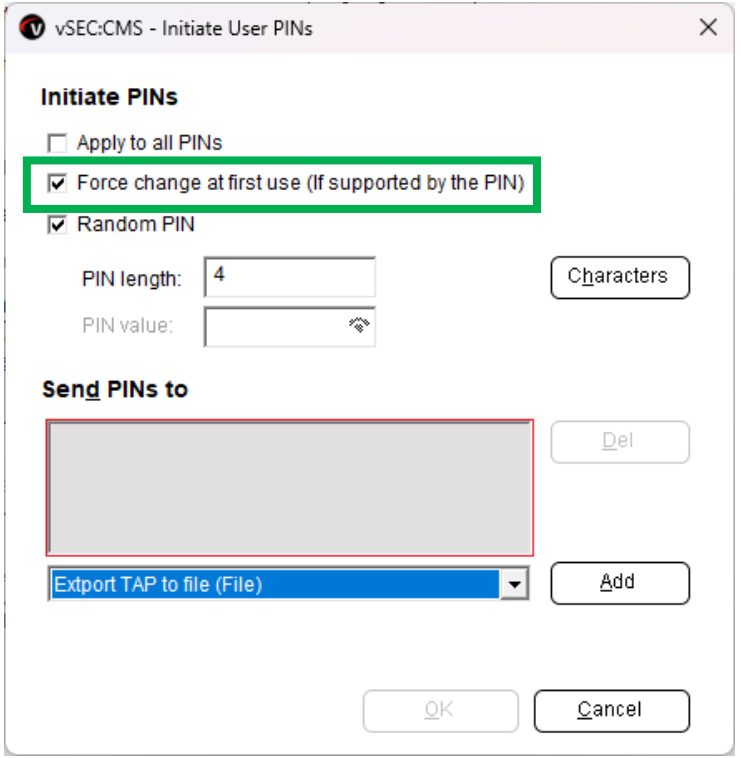
Block 'Device Reset'

Define Applications
Allow list

Define Minimum PIN
length

FIDO 2.1 EF in vSEC:CMS






THALES
Building a future we can all trust
FIDO Demo
www.thalesgroup.com


THALES
Building a future we can all trust
Live PKI Demo
www.thalesgroup.com

THALES
Building a future we can all trust

Q&A

www.thalesgroup.com

THALES
Building a future we can all trust

Thank you

www.thalesgroup.com