Solution Brief

Control the entire FIDO Authenticator Life Cycle for your Workforce

SafeNet Trusted Access and Versasec vSEC:CMS

cpl.thalesgroup.com

THALES
Building a future we can all trust

versasec

THALES
Building a future we can all trust

versasec

Summary

Thales and Versasec enable organizations using PKI to securely adopt FIDO-based authentication for their web applications, giving them full control over the entire FIDO authenticator life cycle, in the same way they manage their PKI credentials.

These organizations will get all the benefits from a modern form of authentication (FIDO2), while optionally maintaining the usage of PKI for certificate-based-authentication, digital signature, or data encryption.

Get full control over the FIDO authenticator life cycle

- Comply with your internal security policies and external market regulations.
- Let your administrators control the FIDO/PKI authenticator enrollment.
- Manage all your FIDO and PKI authenticators in the same system.
- Provide your end users a single FIDO/PKI authenticator for multiple use cases.
- Secure your web apps in no time with an easy to setup SaaS Identity Provider.

The need for phishing-resistant FIDO authentication

With sensitive data and apps dispersed across fragmented computing environments, multi-factor authentication (MFA) has emerged as the best way to authenticate and protect our digital identities in the zero-trust security framework. However, not all authentication methods are equally safe when facing complex cyberattacks. To protect sensitive data from these rising cyber threats such as phishing and Man-In-The Middle Attacks, government cybersecurity agencies worldwide[1] have increased their requirements and recommended leveraging phishing-resistant authentication methods.

Many organizations, especially in regulated markets where compliance to legal and security standards is high, have deployed extensively PKI (Public Key Infrastructure) for many years and use it for certificate-based authentication (CBA), qualified digital signatures and sensitive file encryption. CBA is recognized as phishing-resistant. However, these organizations face challenges to authenticate using CBA to modern cloud and web apps, especially from mobile devices, which are now extensively used.

FIDO (Fast Identity Online) is considered as a go-to, gold standard solution by many cybersecurity agencies, such as CISA. Future-proof, FIDO standard permits system interoperability and does not need any complex IT infrastructure.

The risks of mismanaging FIDO authenticators

The whole lifecycle of the FIDO authenticator must be considered carefully; issuance is just the first step. The authenticator must be controlled, tracked, and secured along the lifecycle which involves events such as temporary disablement, revocation, and replacement.

Unmanaged use of FIDO authenticators may have negative consequences:

- Using less secure authentication methods such as username/ password or SMS OTP for FIDO authenticator self-service leaves you open to phishing, account takeover and frauds.
- User frustration and productivity loss if the enrollment process is confusing or difficult to complete, leading to reduced user adoption and increased helpdesk burden.
- Violations of regulatory requirements or security policies if the enrollment process is not properly recorded or if unauthorized users access protected resources.
- If there is no control over the type of FIDO authenticator used, there is a risk of invalid, less secure, or even harmful authenticator being used unintentionally or intentionally.

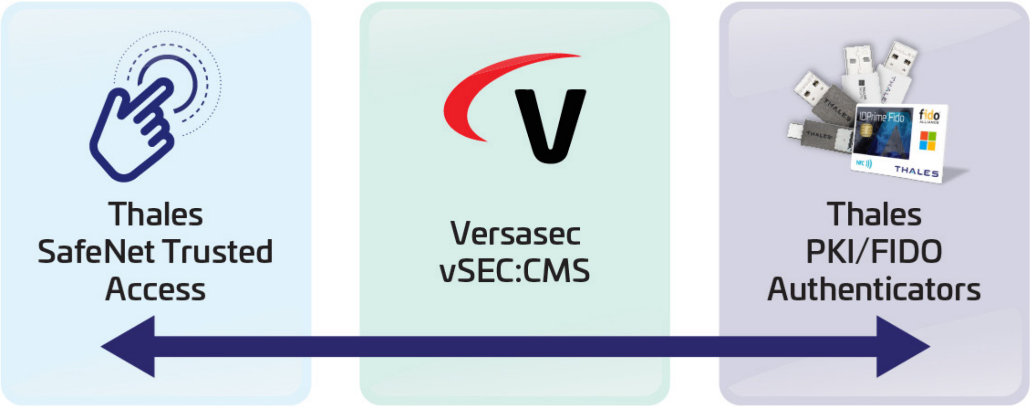
Getting phishing-resistant MFA is not enough; you need to ensure your management processes are protected, repeatable and traceable.

[1] - U.S. Executive Order 14028 on improving Nation's cybersecurity, Boosting your Organisation's cyber Resilience (European Union), Recommended best practices for administrator, CISA & NSA.

Thales-Versasec Solution for Workforce

Organizations using PKI today can now also use FIDO authentication for their web applications by deploying Thales FIDO security keys and FIDO smart cards. Thales and Versasec offer a joint end-to-end solution consisting of an Identity Provider (Thales SafeNet Trusted Access) and a centralized credential management system (Versasec vSEC:CMS). The whole solution is complemented by a large portfolio of Thales hardware authenticators supporting FIDO or both FIDO and PKI.

Get full control over FIDO authenticator life cycle



a. Enable phishing-resistant access to web apps (FIDO and CBA)

With SafeNet Trusted Access, organizations can quickly secure access to modern web apps using FIDO authentication. This Software as a Service supports FIDO2/ WebAuthn and permits to secure access to all federated webs apps using conditional access policies and risk-based authentication. FIDO authentication can be passwordless or in complement of password first authentication, based on user or device context. Thanks to the seamless integration with vSEC:CMS, IT retains full control of the FIDO authenticator life cycle.

In addition, organizations can enable Certificate Based Authentication to web apps within SafeNet Trusted Access and extend the usage of their PKI Smart card to access apps residing in virtual, public and private cloud environments.

b. Centrally manage FIDO and/or PKI authenticator lifecycle and ensure traceability.

Thanks to Versasec credential management system, organizations have a central administration of credentials. With vSEC:CMS all your hardware authenticators such as FIDO, PKI and RFID tokens are managed in one central location where IT staff takes full control over what devices are in what state, for which user and for what purpose.

Primary benefits of deploying vSEC:CMS:

- Same level of security for FIDO management as for PKI
  - All administrative tasks require phishing-resistant authentication
  - Simplified onboarding administration with single pane of glass using the same workflows
  - Proven audit trails and reporting
  - Centralized repositories for credential status and tasks
- Administrator driven "on-behalf-of" management of FIDO and/or PKI authenticators, including revocation and replacements.
- Automation of workflows and processes
- Versatile "no code" templates and workflows

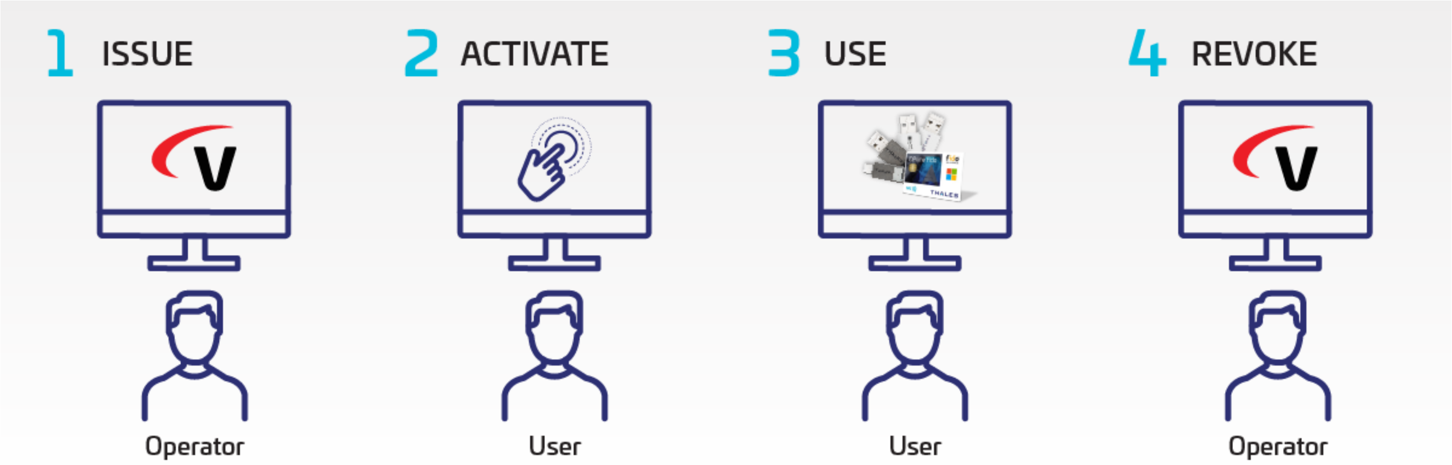
c. Adapt the authenticator to your users' needs

With Thales' broad portfolio of hardware authenticators supporting FIDO or both PKI and FIDO, organizations can equip their end users with a hardware authenticator that supports multiple use cases (phishing-resistant authentication, digital signature, file encryption, physical access to secured areas...) and can be used on different platforms and devices (shared desktops, laptops and mobile devices).

Thales FIDO and hybrid FIDO/PKI authenticators are supported by Versasec vSEC:CMS

d. FIDO authenticator enrollment overview

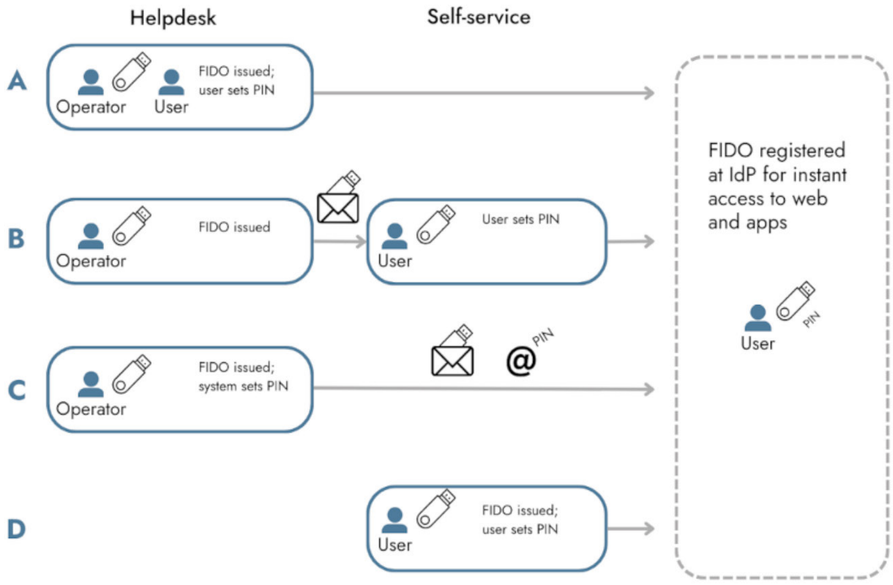
The below flow illustrates how a new FIDO authenticator can be issued and used:



1. The operator issues the FIDO authenticator in VSEC:CMS and distribute it to the user.(See the enrollment method 2 in the table below)
2. When the user receives the FIDO authenticator, he needs to activate it in SafeNet Trusted Access; he activates the authenticator within the self-provisioning flow by completing the identity verification process and setting the PIN.
3. The FIDO authenticator is now active and ready to be used for all configured authentications configured within SafeNet Trusted Access.
4. When a FIDO authenticator is lost or the user leaves the organization, it is revoked from vSEC:CMS by an operator or automated via available APIs and integrations.

During the lifecycle of the credential its status is accessible within the vSEC:CMS repositories and an audit trail is created and kept.

Issuance Options


Helpdesk
Self-service
A
Operator
User
FIDO issued; user sets PIN
B
Operator
FIDO issued
User
User sets PIN
C
Operator
FIDO issued; system sets PIN
PIN
D
User
FIDO issued; user sets PIN
FIDO registered at IdP for instant access to web and apps
User
PIN

Issuance method	Tasks	Suitable
A. Operator	Operator issues the FIDO authenticator and user is present to set the PIN	When full control of issuance and PIN setting is required
B. Operator + User	Operator issues and distributes the FIDO authenticator to the user who at a later point sets the PIN	For distributed teams that want the issuance to be done centrally
C. User	User issues and sets the PIN	For large deployments and distributed teams
D. Automation or Batch	Operator issues devices in the batch; the system sets and delivers the PIN	Ideal for large deployments that prefer centralized onboarding with no user self-service

Revocation and PIN changes can be performed by both operator and user independent of the issuance method selected. All issuance methods can be configured and used at the same time.

About Versasec

Versasec is the leading credential management software provider for organizations worldwide. The award-winning software offers a new approach to identity and credential management. Versasec enables the highest levels of security in an increasingly connected world with growing numbers of remote workers, online business, and threat actors. The security provided by Versasec serves as a cornerstone in every enterprise security system to fully take advantage of the digital transformation. Versasec's products help companies of all sizes easily deploy and manage virtual and physical smarts cards, tokens, RFID, FIDO and other PKI credentials throughout their lifecycle.

About OneWelcome Identity and Access Management Solutions

Thales's digital identity products and solutions empower billions of people and things with digital identities worldwide. The Thales OneWelcome Identity & Access Management portfolio enables organizations to build frictionless, trusted and secure digital journeys for customers, business partners and employees. The OneWelcome Identity Platform provides a variety of capabilities from identity verification, single sign-on, passwordless and multi-factor authentication to fraud management, adaptive access, dynamic authorization and consent & preference management for the highest levels of assurance. More than 30,000 organizations trust us with their IAM and data security needs, enabling them to deliver secure digital services to their users.

About Thales

Thales helps organizations protect sensitive data and software and deliver seamless digital experiences, with advanced encryption, identity and access management and software licensing solutions.