Solution Brief

Accelerate and Secure Your Passwordless Journey for Your Workforce

OneWelcome FIDO Key Lifecycle Management Solution

cpl.thalesgroup.com

THALES
Building a future we can all trust

Summary

FIDO security keys are the gold standard for securing access to sensitive data and protecting from phishing attacks, but large organizations frequently face unique challenges compared to consumers when deploying FIDO hardware security keys at scale.

That is why Thales offers an end-to-end solution called OneWelcome FIDO Key Lifecycle Management, to help CISOs accelerate and secure their passwordless journey, by managing FIDO security keys at scale, in a simple and efficient way, throughout their lifecycle, from onboarding to revocation.

Building on its years of expertise in cryptographic authentication, as well as its long-standing technology partnership with Versasec, Thales enables IT teams:

- To provide secure and seamless authentication to their users from day one by pre-registering FIDO keys on behalf of their users and configuring security policies in less than a minute.
- To manage FIDO keys easily and securely at each step of their lifecycle, from onboarding to revocation. Organizations can now avoid cumbersome re-registration for the end users who have forgotten their PIN thanks to IT-controlled key unblock, ensure appropriate usage of FIDO keys by limiting the list of web services users are allowed to access and ensure security policies are persistent through the FIDO key lifecycle.

Accelerate and Secure Your Passwordless Journey

The urgency for phishing-resistant MFA

With cloud migration and sensitive data 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 have increased their requirements and recommended leveraging phishing-resistant authentication methods such as Fast IDentity Online (FIDO).

Top Two Initial Attack Vectors for Data Breaches

Challenges faced by large organizations when deploying FIDO Authentication

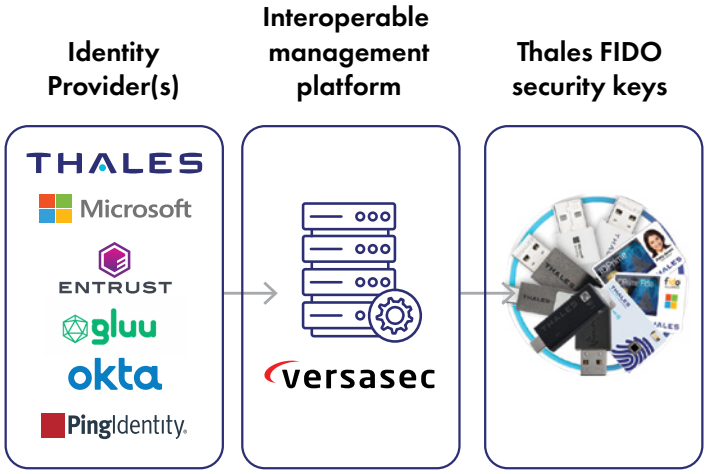
Initially designed for the consumer market, the FIDO standard aims to replace passwords with more secure authentication methods for online services. While recent versions, like FIDO2.1, have begun to address enterprise needs, there are still significant gaps that organizations must address to simplify, accelerate, and secure their deployment.

Enterprises face unique challenges compared to consumers when deploying and managing FIDO keys at scale. It impacts end users' experience, IT Administrative productivity, and security.

Weak User Experience	Administrative Overhead	Security Hole
Too complex and/or time-consuming FIDO key self-registration to enterprise resources via the Identity providers If the end user has forgotten his PIN, he must completely reset and re-register the key	How to register FIDO keys at once to multiple identity providers? How to quickly apply security policies to a large amount of FIDO keys? (e.g., fix minimum PIN length to six digits) How to easily prove that FIDO keys are managed according to policies? How to limit the usage of the keys to access enterprise resources only? How to quickly revoke a key when and employee is leaving the organization?	How to ensure a secure onboarding flow? How to ensure the applied security policies are persistent throughout the FIDO key lifecycle? How to ensure user verification (PIN or biometry) is systematically required when accessing enterprise resources?

OneWelcome FIDO Key Lifecycle Management Solution

Thales OneWelcome FIDO Key Lifecycle Management combines an interoperable management platform with Thales hardware FIDO security keys specifically designed for use in large organizations. The solution helps CISOs accelerate and secure their passwordless authentication journey by managing FIDO security keys at scale, in a simple and efficient way, throughout their lifecycle. In addition, CISOs benefit from the ultimate Thales expertise in cyber security and in complex projects.



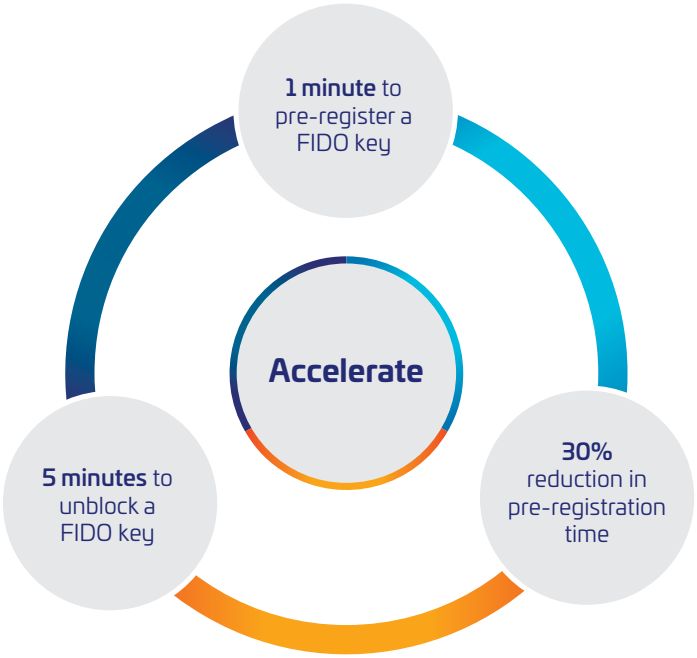
Versasec Interoperable Management Platform: Thales leverages its technical partnership with Versasec and relies on the vSEC:CMS platform to manage Thales FIDO and PKI smart cards and tokens throughout their lifecycle.

Thales FIDO Security Keys: Thales offers a broad range of FIDO2 compliant tokens and smart cards specifically designed for large deployment in the enterprise. These authenticators can be seamlessly orchestrated with Versasec's vSEC:CMS for efficient management and deployment across the enterprise.

Identity Providers Integration: The solution is designed to work with a wide range of IDPs, such as Thales SafeNet Trusted Access , Microsoft Entra ID, OKTA Workforce Identity Cloud , Ping Identity Management Platform, Entrust Identity or Gluu, providing flexibility and scalability for enterprises. Whether using on-premises or cloud-based identity providers, the integration ensures that FIDO authentication is seamlessly incorporated into existing workflows.

Accelerate your passwordless journey

With Thales OneWelcome FIDO Key Lifecycle Management, enterprises can accelerate their FIDO deployment and quickly protect their sensitive data from phishing attacks. The solution reduces IT admin overhead, improves end users' experience and productivity and then facilitates their adoption of FIDO technology.



With the solution, the IT team can:

- pre-register a FIDO key in less than 1 minute instead of the usual 10 minutes required for each user to self-register their key.
- save 30% of the pre-registration time by pre-registering FIDO keys in batch issuance mode.
- unblock a FIDO key in less than 5 minutes if the end-user has forgotten his PIN and avoid cumbersome full data reset and re-registration.

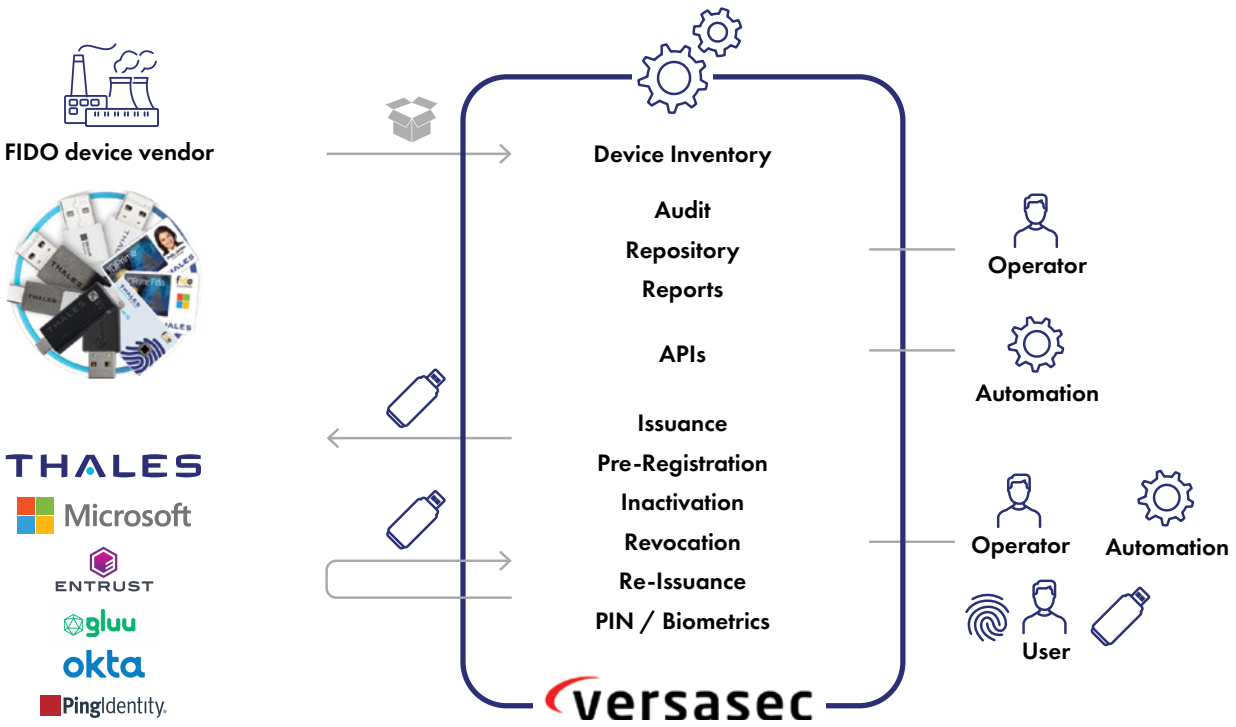
Secure Your Entire FIDO Key Lifecycle

With the Thales solution, enterprises not only secure the authentication step but also strengthen each step of the FIDO key lifecycle, from onboarding to revocation.

Secured Onboarding Flows Centrally Managed in vSEC:CMS

Thanks to vSEC:CMS, 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 takes full control over what devices are, in what state, for which user, and for what purpose.

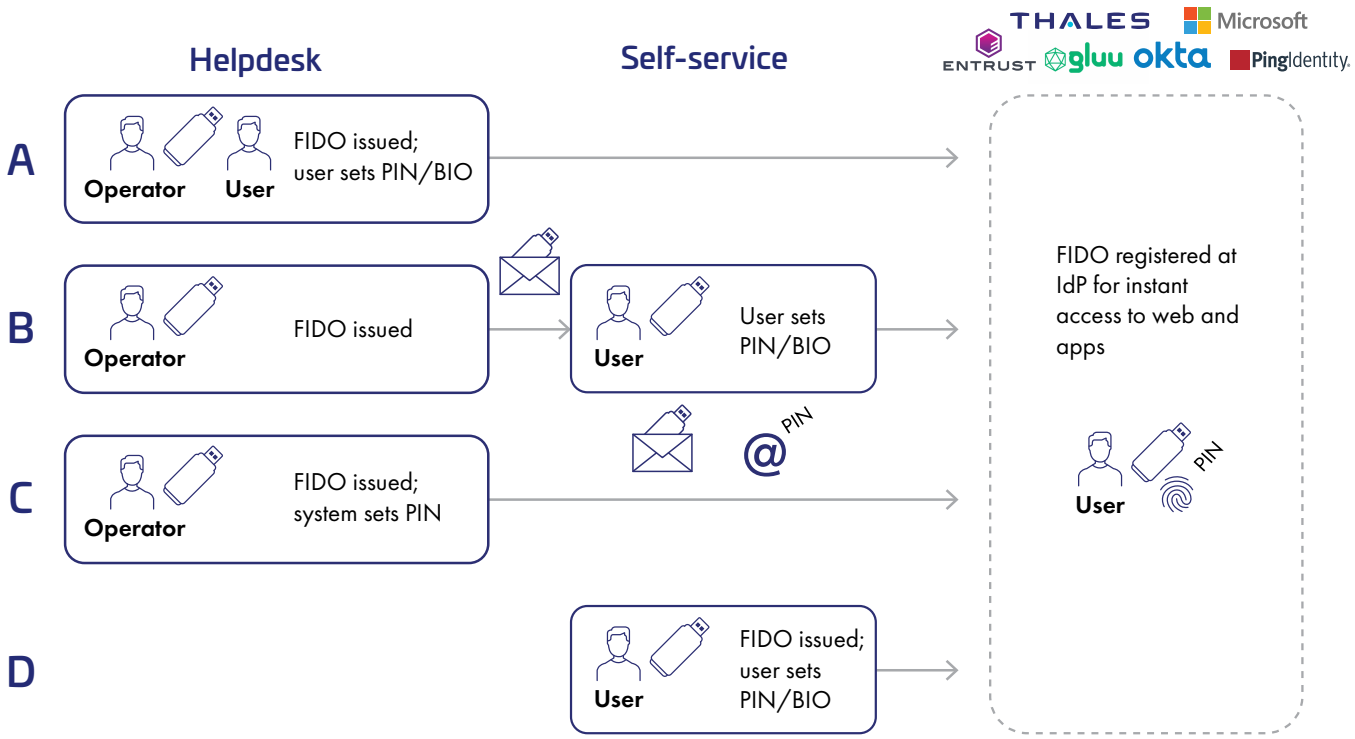
Rollout and Orchestrate FIDO keys in vSEC:CMS

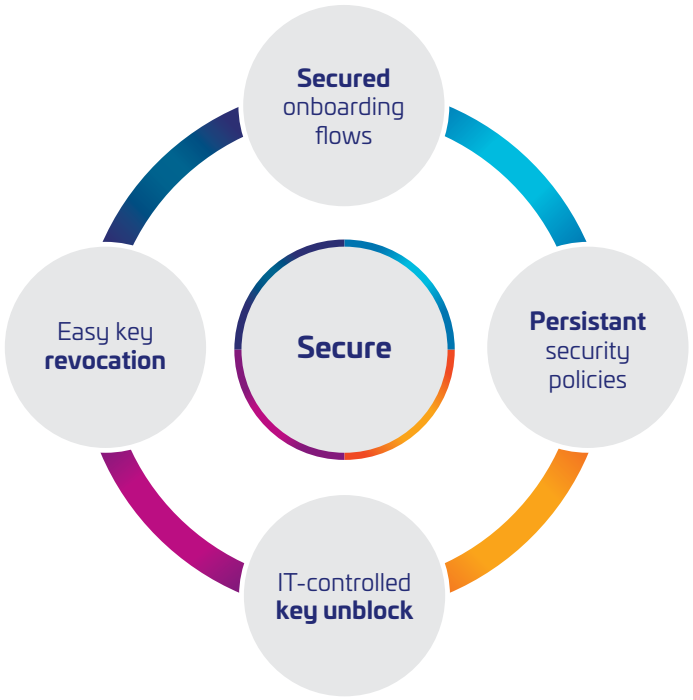


Four issuance options are available to tailor the onboarding process to the organization's security policy.

- Option A: Well-suited for when an in-person meeting before issuance is required. The operator issues the device to the user, and the user sets the PIN.
- Option B: Perfect for remote teams that want central issuance. The operator issues and distributes the credential to the user, who, at a later point, sets their PIN.
- Option C: Ideal for large deployments that prefer centralized onboarding with no user self-service. The operator issues devices in the batch; the system sets and delivers the PIN.
- Option D: Optimal for large deployments that prefer self-service and distributed teams. User issues and sets their PIN.

Versatile Enrollment Methods in vSEC:CMS





Implement Persistent Security Policies

By combining the Enterprise Edition of Thales FIDO keys and vSEC:CMS, IT teams can deploy security policies such as minimum PIN length that are persistent from key issuance to revocation, avoiding end users to change their PIN to a new PIN not compliant with the minimum PIN length defined in the security policy.

IT Controlled Key Unblock

If an end user has forgotten the PIN, the IT administrator is in full control of the operation and can verify end-user identity before authorizing him to change his PIN and regain access to sensitive data.

Easy Key Revocation

Thanks to vSEC:CMS, IT operator can revoke the FIDO key in a quick and effortless way.

Primary benefits of deploying vSEC:CMS

- All administrative tasks require phishing-resistant authentication
- Support of Thales FIDO Enterprise Features
- Simplified onboarding administration with single pane of glass
- Proven audit trails and reporting
- Centralized repositories for credential status and tasks
- Administrator driven "on-behalf-of" management of FIDO authenticators, including revocation and replacement.
- Automation of workflows and processes
- Versatile "no code" templates and workflows

Go Beyond FIDO 2.1 Standard with Thales FIDO Enterprise Features

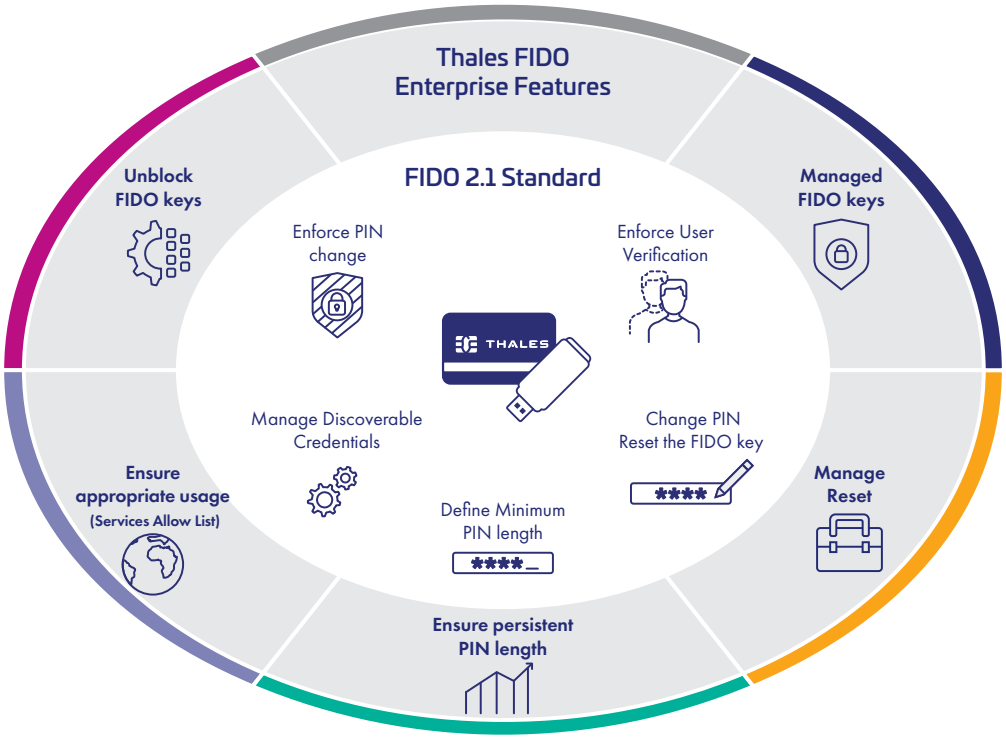
OneWelcome FIDO Key Lifecycle Management Solution offers organizations two options:

- **benefit from FIDO2.1/CTAP2.1** enterprises features and enforce PIN change, user verification and minimum PIN length. To do this, organizations need to equip their end users with Thales FIDO keys supporting FIDO2.1 and fully certified by the FIDO Alliance.
- **go beyond FIDO2.1** standard and benefit from Thales unique features on top of FIDO2.1:
  - **Managed Mode**: IT operator is the only personnel to manage security policies and sensitive operations on the FIDO keys
  - **Service Allow List** permits IT operator to limit the usage of the FIDO keys to preferred company services and by then ensure appropriate usage of the FIDO keys
  - **Unblock FIDO Keys:** allow end users to unblock their keys, under the control of the IT operator, without having to fully reset the key and re-register it to the enterprise web services.
  - **Ensure persistent PIN Length:** prevents end users from changing the minimum PIN length.
  - **Manage Reset:** prevent end users from unintentionally resetting their FIDO key.

In this case, organizations need to equip their end users with Thales FIDO keys in the Enterprise Edition, that support Thales FIDO Enterprise features and comply with FIDO2.1 standard.

SafeNet eToken Fusion NFC PIV is available in the Standard and Enterprise Editions

FIDO2.1 and Thales FIDO Enterprise Features



Conclusion

As enterprises continue to face evolving security challenges, the need for robust, phishing-resistant authentication methods has never been greater. Thales, in collaboration with Versasec and Identity Providers, offers a comprehensive solution that leverages FIDO-based authentication to enhance enterprise security and facilitate large FIDO deployments. By implementing this solution, organizations can manage FIDO security keys at scale, in a simple and efficient way, throughout their lifecycle.

For more information, contact Thales specialists.

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

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us