Thales OneWelcome FIDO Key Lifecycle Management FAQs

Simplify, Secure, and Scale the management of your FIDO security keys

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

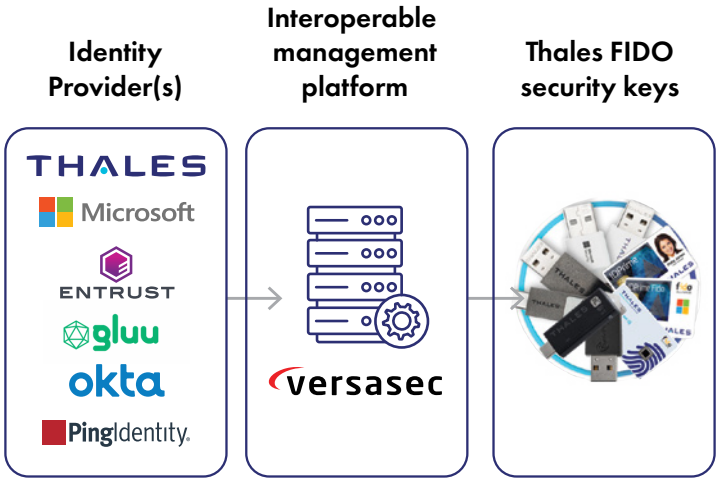
Getting Started

1. **Why is it critical for businesses to manage the lifecycle of their FIDO keys?**
   Managing the lifecycle of FIDO keys is essential for reducing cyber threats. Strengthening each step of the authenticator lifecycle - from enrolment to revocation - helps prevent account takeovers and fraudulent activities. Additionally, effective management improves user adoption by streamlining registration and key unblocking, making authentication more accessible and efficient. Furthermore, automating key configuration, revocation, and central reporting reduces administrative costs, ensuring a more secure and cost-effective authentication system.

2. **Do I need to replace my current FIDO keys to use Thales OneWelcome FIDO Key Lifecycle Management?**
   No, Thales integrates with existing FIDO keys, however, for optimal security, seamless management, and full feature access, we recommend using Thales' own FIDO devices. Our keys, especially the Enterprise Edition, such as the SafeNet eToken FUsion NFC PIV Enterprise are designed to maximise authentication security, user experience and compliance throughout their lifecycle, while ensuring smooth integration with our lifecycle management platform.

3. **How do I begin integrating Thales OneWelcome FIDO Key Lifecycle Management with my identity systems?**
   Integration is seamless and typically completed in a matter of days, thanks to pre-built connectors for major identity management platforms. The process ensures quick deployment without disrupting existing workflows or infrastructure.

4. **How can I replace our (passwordless) Multi Factor Authentication process with device bound passkeys?**
   Using Thales OneWelcome FIDO Key Lifecycle Management, you can easily implement FIDO2 support in your existing authentication system, enabling secure, phishing-resistant logins for your user devices. The solution can help you update your backend to handle passkey registration and authentication by securely storing public keys and credential metadata, while on the frontend, users can register the passkeys themselves and replace the existing MFA workflows with passkey-based authentication for multiple devices.



Operational Benefits

1. **Can Thales OneWelcome FIDO Key Lifecycle Management help manage large fleets of FIDO Authentication devices?**
   Yes, Thales OneWelcome FIDO Key Lifecycle Management provides centralised control to manage thousands of FIDO authenticators with ease, including policy enforcement and usage tracking.
2. **How does Thales OneWelcome FIDO Key Lifecycle Management minimise IT workloads?**
   The centralised FIDO key management gives IT full visibility and control. Automated provisioning, resets, and batch processes streamline fleet management t, significantly reducing manual interventions and freeing IT teams to focus on strategic priorities.
3. **How does Thales OneWelcome FIDO Key Lifecycle Management improve productivity?**
   By enabling pre-registration of a FIDO key in less than one minute, businesses can significantly cut down the usual 10-minute self-registration time for each user. Additionally, batch issuance mode allows for a 30% reduction in pre-registration time, making deployment faster and more efficient. In cases where users forget their PIN, unblocking a FIDO key in under five minutes prevents the need for a full data reset and re-registration, minimising disruptions and keeping employees productive. These efficiencies enhance security while reducing administrative overhead.

End-User Experience

1. **How does Thales OneWelcome FIDO Key Lifecycle Management reduce user friction?**
   The solution offers the option to configure and register FIDO keys on behalf of the users to various identity providers, simplifying and accelerating their onboarding. Users can also sunblock keys or manage resets with minimal IT involvement, streamlining their experience and boosting adoption.
2. **What happens if a user has forgotten their PIN?**
   End users who have forgotten their PIN can unblock their FIDO key with IT support in less than 5 minutes, avoiding the need for a full reset. This saves approximately 10 minutes per service by eliminating the re-registration process.
3. **What happens if a user loses their FIDO key?**
   Lost keys can be reported, blocked, and a new key can be configured and registered in just a few clicks, ensuring security policies are upheld while reducing frustration and downtime.
4. **Does Thales provide self-service tools for users?**
   Yes, users can resolve common issues themselves, such as setting up a key or changing the PIN, unblocking, or resetting their keys. Sensitive operations such as unblocking the key when the PIN has been forgotten or resetting the key are controlled by IT or helpdesk to ensure the appropriate level of security.

Security & Compliance

1. **What security policies can I enforce with Thales OneWelcome FIDO Key Lifecycle Management?**
   You can enforce an array of security policies such as minimum PIN length, user verification, and applications usage restrictions with the ability to push new compliance rules to the right keys instantly.
2. **How does Thales OneWelcome FIDO Key Lifecycle Management prevent accidental resets or misuse of keys?**
   Policies and workflows ensure keys are reset only when necessary and with proper authorisation.
3. **Does Thales OneWelcome FIDO Key Lifecycle Management help organisations meet compliance standards?**
   Yes, Thales supports industry standards and offers features to maintain compliance with security policies. You can also select the Thales FIDO keys certified by FIDO Alliance, NIST or Common Criteria or eIDAS.

Scalability & Flexibility

1. **Can Thales OneWelcome FIDO Key Lifecycle Management scale with my organisation as it grows?**
   Yes, Thales OneWelcome FIDO Key Lifecycle Management is designed to scale as your organisation grows. It offers flexible key management that supports a wide range of users, from small teams to large enterprises, ensuring that security remains robust as your user base expands. The system allows for batch issuance and automated key provisioning, which makes it easier to manage a growing number of FIDO keys without increasing administrative overhead. Additionally, compliance rules and security policies can be pushed out instantly to all keys, ensuring consistent security across the organisation.
2. **Is this solution suitable for hybrid or multi-cloud environments?**
   Absolutely, Thales is built for compatibility with a range of environments, supporting both on premise and cloud environments.

Cost & ROI

1. **What are the cost-saving benefits of Thales OneWelcome FIDO Key Lifecycle Management?**
   Yes, Thales OneWelcome FIDO Key Lifecycle Management provides centralised control to manage thousands of FIDO authenticators with ease, including policy enforcement and usage tracking. Reduced risk of cyberattacks, IT workload, fewer support tickets, higher user adoption rates, and faster processes all contribute to significant cost savings. For example:
   - IT can register one FIDO key in less than 1 minute and save 10 min to each end users, for self-registration per service.
   - IT admin can reduce this time by 30% using batch issuance for large volume of keys.

   On a daily basis, end users who have forgotten their PIN can unblock their key in less than 5 minutes with IT support and again save 10 mins for re-registration per service.
2. **How can this solution improve your passwordless ROI?**
   By increasing operational efficiency and minimising cyberthreats and time spent in admin, organisations save money while improving productivity.
3. **Is there a free trial or demo available?**
   Yes, a dedicated FIDO Key Lifecycle Management expert can help you set up your organisation for a free trial and book a meeting with you – completely free of charge. Contact us to explore how Thales can support your organisation.

Selecting a provider

1. **What issues arise from using separate providers for hardware and software management?**
   Using separate providers could lead to fragmented systems, integration challenges, and increased complexity, if you partner with a provider without experience across all identity sectors and flexible solutions.
2. **What support does Thales offer during deployment?**
   Thales provides expert guidance, resources, and ongoing support to ensure a smooth implementation.
3. **Why should I choose Thales over another provider?**
   Thales brings decades of expertise in identity and security solutions. As a founding member of FIDO Alliance, we have a reliable and proven track record of success. Thales also delivers comprehensive end to end solutions (hardware authenticators, management platform and identity provider) that can be adapted to your modern or legacy systems with ease.

About Thales

As a global leader in cybersecurity, Thales safeguards sensitive data, identities, applications, and software for the most trusted brands in the world. Through advanced encryption, identity access management, application security, and software entitlement, Thales secures cloud environments, defends against cyber threats, ensures compliance, and enables trusted digital experiences.

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

THALES

Building a future we can all trust

Contact us

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

cpl.thalesgroup.com

© Thales - March 2025 • MHv2