

Acelere y Asegure su Jornada Sin Contraseña para su Fuerza Laboral

Solución OneWelcome
FIDO Key Lifecycle
Management

Resumen

Las llaves de seguridad FIDO son el estándar para proteger el acceso a datos sensibles y defenderse de los ataques de phishing, pero las grandes organizaciones frecuentemente enfrentan desafíos únicos en comparación con los consumidores al implementar llaves de seguridad FIDO en escala.

Por eso Thales ofrece una solución integral denominada OneWelcome FIDO Key Lifecycle Management, para ayudar a los CISOs a acelerar y asegurar su jornada sin contraseña gestionando llaves de seguridad FIDO en escala, de forma simple y eficiente, a lo largo de todo su ciclo de vida, desde el onboarding hasta la revocación.

Basándose en años de experiencia en autenticación criptográfica y en su alianza tecnológica de larga data con Versasec, Thales permite a los equipos de TI:

- brindar autenticación segura y fluida a sus usuarios desde el primer día, pre-registrando llaves FIDO en nombre de los usuarios y configurando políticas de seguridad en menos de un minuto.
- Administre las llaves FIDO de forma sencilla y segura en cada etapa de su ciclo de vida, desde el aprovisionamiento hasta su revocación. Las organizaciones pueden evitar los complejos procesos de reinscripción cuando un usuario olvida su PIN gracias al desbloqueo de llaves administrado por TI. También pueden controlar el uso de las llaves FIDO restringiendo el acceso únicamente a los servicios web autorizados y garantizar que las políticas de seguridad se mantengan vigentes durante todo el ciclo de vida de las llaves.

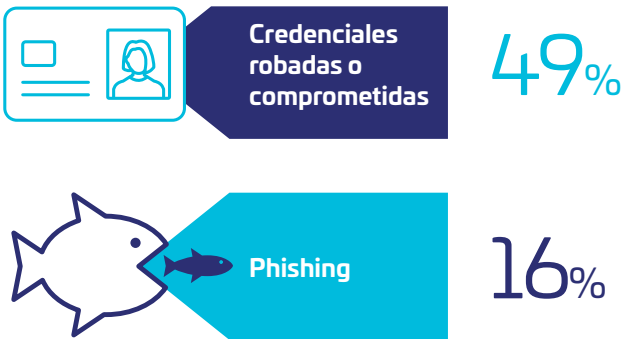
Acelere y proteja su transición hacia un entorno sin contraseñas



La Urgencia de la MFA Resistente al Phishing

Con la migración a la nube y los datos sensibles dispersos en entornos informáticos fragmentados, la autenticación multifactor (MFA) ha surgido como la mejor manera de autenticar y proteger las identidades digitales en el marco de seguridad zero-trust. Sin embargo, no todos los métodos de autenticación son igualmente seguros ante ciberataques complejos. Para proteger los datos sensibles de ciberamenazas crecientes como el phishing y los ataques man-in-the-middle, las agencias gubernamentales de ciberseguridad en todo el mundo han aumentado sus requisitos y recomendado el uso de métodos de autenticación resistentes al phishing como FIDO (Fast Identity Online).

Dos principales vectores iniciales de ataque en brechas de datos:



Desafíos de las Grandes Organizaciones al Implementar la Autenticación FIDO

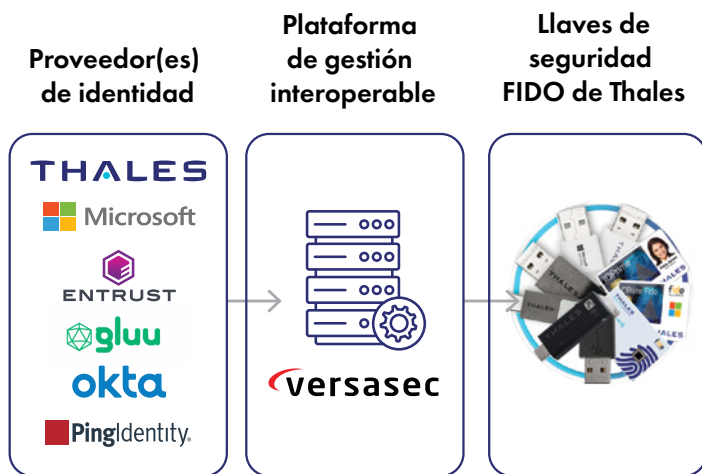
Diseñado inicialmente para el mercado de consumo, el estándar FIDO busca reemplazar las contraseñas con métodos de autenticación más seguros para servicios en línea. Si bien las versiones recientes, como FIDO2.1, han comenzado a abordar las necesidades empresariales, aún existen brechas significativas que las organizaciones deben superar para simplificar, acelerar y asegurar su implementación.

Las empresas enfrentan desafíos únicos en comparación con los consumidores al implementar y gestionar llaves FIDO en escala, con impacto en la experiencia de los usuarios finales, la productividad administrativa de TI y la seguridad.

Desafíos de Experiencia de Usuario:	Desafíos Administrativos:	Brechas de Seguridad:
Auto-registro de llaves FIDO demasiado complejo y/o lento; si el usuario olvidó su PIN, debe reiniciar y re-registrar completamente la llave.	¿Cómo registrar llaves FIDO en múltiples proveedores de identidad a la vez? ¿Cómo aplicar rápidamente políticas de seguridad a un gran número de llaves FIDO? ¿Cómo demostrar fácilmente que las llaves FIDO se gestionan según las políticas?	¿Cómo limitar el uso de las llaves solo a recursos corporativos? ¿Cómo revocar rápidamente una llave cuando un empleado deja la organización? ¿Cómo garantizar un flujo de onboarding seguro? ¿Cómo asegurar que las políticas de seguridad sean persistentes? ¿Cómo garantizar que la verificación del usuario (PIN o biometría) sea sistemáticamente requerida?

Solución OneWelcome FIDO Key Lifecycle Management

Thales OneWelcome FIDO Key Lifecycle Management combina una plataforma de gestión interoperable con llaves de seguridad [FIDO en hardware de Thales](#), diseñadas específicamente para su uso en grandes organizaciones. La solución ayuda a los CISOs a acelerar y asegurar su jornada de autenticación sin contraseña gestionando llaves de seguridad FIDO en escala, de forma simple y eficiente, a lo largo de todo su ciclo de vida. Además, los CISOs se benefician de la máxima experiencia de Thales en ciberseguridad y en proyectos complejos.



Plataforma de Gestión Interoperable Versasec: Thales aprovecha su alianza técnica con Versasec y se apoya en la plataforma vSEC:CMS para gestionar las tarjetas inteligentes y tokens FIDO y PKI de Thales a lo largo de todo su ciclo de vida.

Llaves de Seguridad FIDO de Thales: Thales ofrece una amplia gama de tokens y tarjetas inteligentes compatibles con FIDO2, diseñados específicamente para implementaciones a gran escala en empresas. Estos autenticadores pueden orquestarse de manera fluida con el vSEC:CMS de Versasec para una gestión e implementación eficientes.

Integración con Proveedores de Identidad: La solución está diseñada para funcionar con una amplia gama de IDPs, como Thales SafeNet Trusted Access, Microsoft Entra ID, OKTA Workforce Identity Cloud, Ping Identity Management Platform, Entrust Identity o Gluu, brindando flexibilidad y escalabilidad a las empresas.

Acelere su Jornada Sin Contraseña

Con Thales OneWelcome FIDO Key Lifecycle Management, las empresas pueden acelerar su implementación FIDO y proteger rápidamente sus datos sensibles contra ataques de phishing. La solución reduce la carga administrativa de TI, mejora la experiencia y productividad de los usuarios finales y facilita su adopción de la tecnología FIDO.



Con esta solución, el equipo de TI puede

- Pre-registre una llave FIDO en menos de 1 minuto, en lugar de los habituales 10 minutos necesarios para que cada usuario realice su propio registro.
- Ahorre un 30% del tiempo de pre-registro al pre-registrar llaves FIDO en modo de emisión por lotes.
- Desbloquee una llave FIDO en menos de 5 minutos si el usuario olvidó su PIN, evitando el tedioso restablecimiento completo y re-registro.

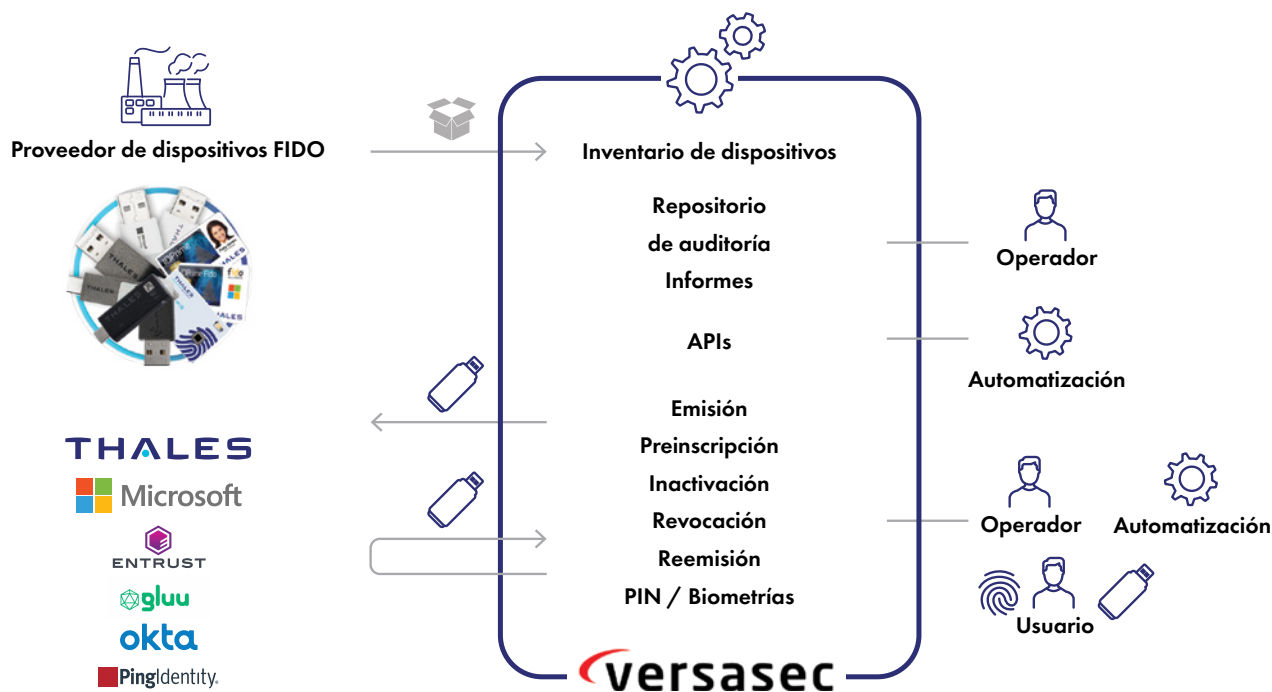
Proteja Todo el Ciclo de Vida de la Llave FIDO

Con la solución de Thales, las empresas no solo aseguran el paso de autenticación, sino que también refuerzan cada etapa del ciclo de vida de la llave FIDO, desde el onboarding hasta la revocación.

Flujos de Onboarding Seguros Gestionados Centralmente en vSEC:CMS:

CMS, las organizaciones cuentan con una administración centralizada de credenciales. Todos los autenticadores de hardware, como tokens FIDO, PKI y RFID, se gestionan en una ubicación central donde TI tiene control total sobre qué dispositivos existen, en qué estado, para qué usuario y con qué propósito.

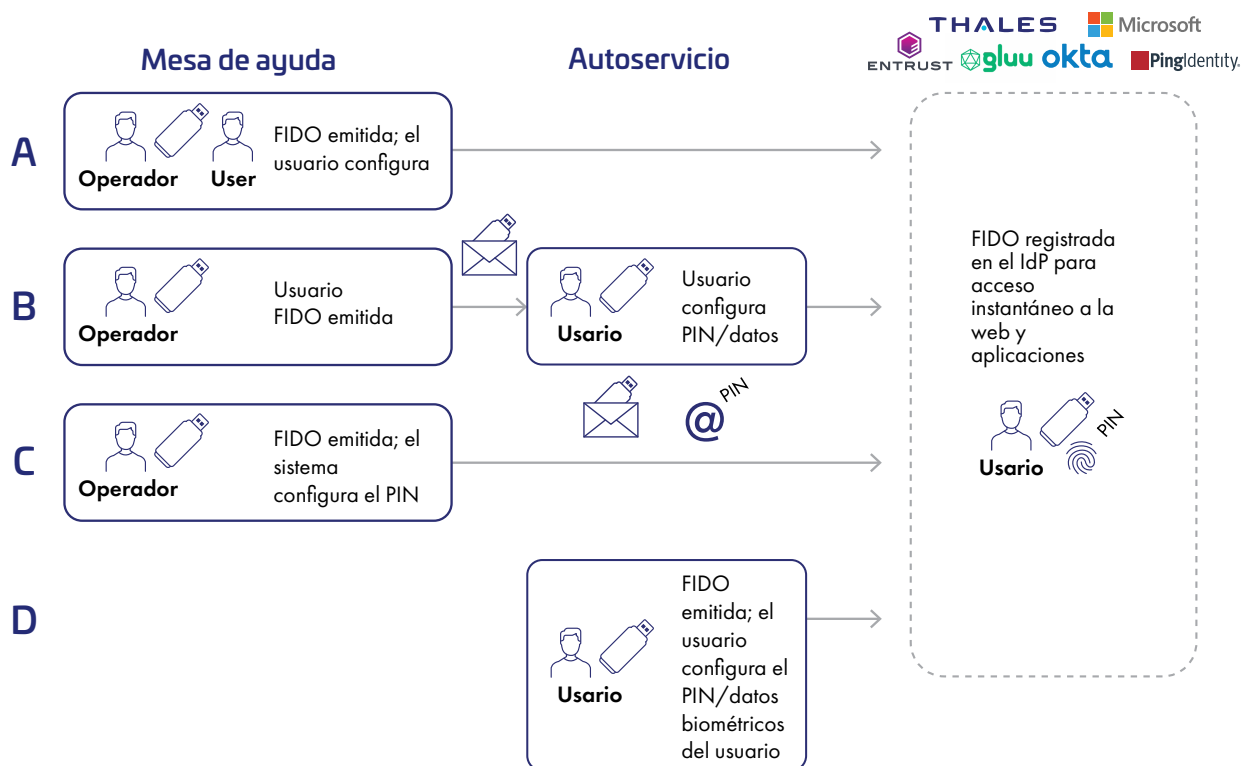
Implementación y orquestación de llaves FIDO en vSEC:CMS



Cuatro opciones de emisión están disponibles para adaptar el proceso de onboarding a la política de seguridad de la organización.

- Opción A: Indicada cuando se requiere una reunión presencial antes de la emisión. El operador emite el dispositivo al usuario, y el usuario establece el PIN.
- Opción B: Perfecta para equipos remotos que desean emisión centralizada. El operador emite y distribuye la credencial al usuario, quien establece su PIN posteriormente.
- Opción C: Ideal para grandes implementaciones que prefieren onboarding centralizado sin autoservicio. El operador emite los dispositivos en lote; el sistema establece y entrega el PIN.
- Opción D: Óptima para grandes implementaciones que prefieren autoservicio y equipos distribuidos. El usuario emite y establece su propio PIN.

Métodos de inscripción versátiles en vSEC:CMS





Implemente Políticas de Seguridad Persistentes

Al combinar la Edición Empresarial de las llaves FIDO de Thales con vSEC:CMS, los equipos de TI pueden implementar políticas de seguridad como la longitud mínima del PIN que son persistentes desde la emisión hasta la revocación de la llave, evitando que los usuarios finales cambien su PIN a uno que no cumpla con la longitud mínima definida en la política de seguridad.

Desbloqueo de Llave Controlado por TI

Si un usuario final olvidó el PIN, el administrador de TI tiene control total de la operación y puede verificar la identidad del usuario antes de autorizarlo a cambiar su PIN y recuperar el acceso a los datos sensibles.

Revocación Fácil de Llaves

Gracias a vSEC:CMS, el operador de TI puede revocar la llave FIDO de forma rápida y sin esfuerzo.

Principales Beneficios de Implementar vSEC:CMS

- Todas las tareas administrativas requieren autenticación resistente al phishing.
- Soporte de los Recursos Empresariales FIDO de Thales.
- Administración de onboarding simplificada con panel único de control.
- Trazas de auditoría y reportes comprobados.
- Repositorios centralizados para el estado de credenciales y tareas.
- Gestión 'en nombre de' dirigida por el administrador para autenticadores FIDO, incluyendo revocación y reemplazo.
- Automatización de flujos de trabajo y procesos.
- Flujos de trabajo versátiles sin código.

Vaya Más Allá del Estándar FIDO 2.1 con los Recursos Empresariales FIDO de Thales

La Solución OneWelcome FIDO Key Lifecycle Management ofrece a las organizaciones dos opciones:

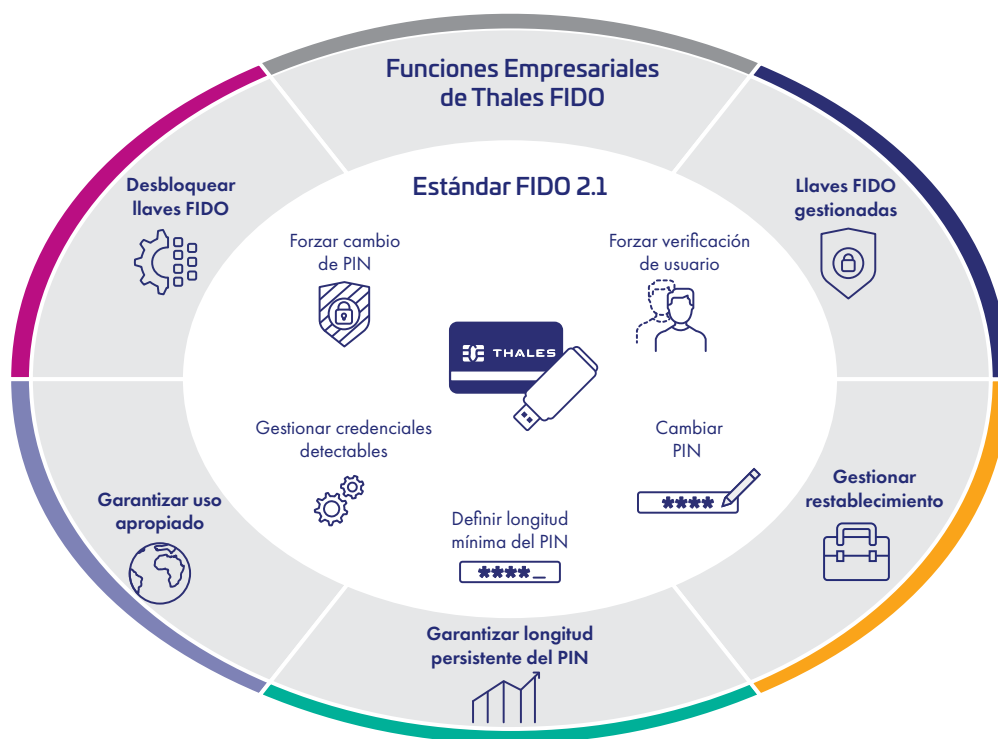
- **beneficiarse de los recursos empresariales de FIDO2.1/CTAP2.1** y aplicar cambio de PIN, verificación de usuario y longitud mínima de PIN;
- **o ir más allá del estándar FIDO2.1** y aprovechar los recursos exclusivos de Thales.
 - **Modo Administrado:** El operador de TI es el único responsable de gestionar las políticas de seguridad y las operaciones sensibles en las llaves FIDO.
 - **Lista de Servicios Permitidos:** Permite al operador de TI limitar el uso de las llaves FIDO a los servicios corporativos autorizados, garantizando su uso adecuado.
 - **Desbloqueo de Llaves FIDO:** Permite a los usuarios finales desbloquear sus llaves, bajo el control del operador de TI, sin necesidad de restablecer completamente la llave y volver a registrarla en los servicios web corporativos.
 - **Garantizar Longitud Mínima de PIN Persistente:** Impide que los usuarios finales cambien la longitud mínima del PIN.
 - **Gestionar Restablecimiento:** Impide que los usuarios finales restablezcan accidentalmente su llave FIDO.

Para ello, las organizaciones deben equipar a sus usuarios con llaves FIDO de Thales Enterprise Edition, que incorporan las funcionalidades empresariales exclusivas de Thales para FIDO y cumplen con el estándar FIDO2.1.



SafeNet eToken Fusion NFC PIV está disponible en las ediciones Estándar y Enterprise.

FIDO 2.1 y Funciones Empresariales de Thales FIDO



Conclusión

A medida que las empresas continúan enfrentando desafíos de seguridad en evolución, la necesidad de métodos de autenticación robustos y resistentes al phishing nunca ha sido mayor. Thales, en colaboración con Versasec y los Proveedores de Identidad, ofrece una solución integral que aprovecha la autenticación basada en FIDO para mejorar la seguridad empresarial y facilitar grandes implementaciones FIDO. Al implementar esta solución, las organizaciones pueden gestionar llaves de seguridad FIDO en escala, de forma simple y eficiente, a lo largo de todo su ciclo de vida.

Para más información, contacte a los [especialistas de Thales](#).

Acerca de Versasec

Versasec es el principal proveedor de software de gestión de credenciales para organizaciones de todo el mundo. El premiado software ofrece un nuevo enfoque para la gestión de identidad y credenciales. Versasec permite los más altos niveles de seguridad en un mundo cada vez más conectado, con un número creciente de trabajadores remotos, negocios en línea y actores de amenazas. Los productos de Versasec ayudan a empresas de todos los tamaños a implementar y gestionar fácilmente tarjetas inteligentes virtuales y físicas, tokens, RFID, FIDO y otras credenciales PKI a lo largo de todo su ciclo de vida.

Acerca de las Soluciones de Gestión de Identidad y Acceso de OneWelcome

Los productos y soluciones de identidad digital de Thales empoderan a miles de millones de personas y dispositivos con identidades digitales en todo el mundo. El portafolio de Gestión de Identidad y Acceso de Thales OneWelcome permite a las organizaciones construir experiencias digitales fluidas, confiables y seguras para clientes, socios comerciales y empleados. La Plataforma de Identidad OneWelcome ofrece capacidades que van desde verificación de identidad, inicio de sesión único, autenticación sin contraseña y multifactor hasta gestión de fraudes, acceso adaptativo, autorización dinámica y gestión de consentimiento y preferencias para los más altos niveles de garantía. Más de 30.000 organizaciones confían en Thales para sus necesidades de IAM y seguridad de datos.

Acerca de Thales

Las empresas y gobiernos actuales dependen de la nube, los datos y el software para ofrecer servicios digitales confiables. Por eso las marcas y organizaciones más reconocidas del mundo confían en Thales para proteger información y software sensibles dondequiera que sean creados, almacenados o accedidos — desde la nube y los centros de datos hasta los dispositivos y las redes. Como líder global en seguridad de datos, gestión de identidad y acceso, y licenciamiento de software, nuestras soluciones permiten a las organizaciones migrar a la nube de forma segura, alcanzar el cumplimiento normativo con confianza, crear más valor con su software y ofrecer experiencias digitales fluidas a millones de consumidores cada día.