

A woman with curly hair is sitting on concrete steps, looking down at a laptop. A large blue geometric shape is overlaid on the left side of the image, containing the main text.

Thales Trusted Cyber Technologies Identity and Access Management Solutions

thalestct.com

THALES

Ensure the Right Individuals Have Access to the Right Resources at the Right Times for the Right Reasons.

Identities are the cornerstone of a Zero Trust Architecture (ZTA). With apps, services and data in the cloud, everyone is literally an outsider. Establishing and enforcing a robust identity and access security policy enables agencies to safeguard the confidentiality, integrity, and availability of their assets both in the cloud and on-premises.

Thales TCT offers authentication solutions that address the evolution of identities. From traditional high assurance and commercial-off-the-shelf authentication solutions to first-of-a-kind hardware security module-based identity credentials, Thales TCT offers the most secure, certificate-based authentication platforms available to the U.S. Federal Government.

Universal Authentication Methods Widely Deployed Across Federal Agencies

Thales TCT provides universal authentication methods through wide-range authenticators including certificate-based smart cards and tokens, OTP hardware authenticators, tokenless authenticators, and more. Thales TCT offers both its own line of government-specific, high assurance authentication solutions and Thales CPL's commercial-of-the-shelf SafeNet authentication solutions.

Provide Simple, Secure Access to all your Apps with Authentication Everywhere

Allowing you to address numerous use cases, assurance levels and threat vectors, Thales TCT authenticators are supported by access management platforms which offer uniform, centralized policy management—delivered in the cloud or on premises. Supporting software solutions include SafeNet Trusted Access (STA) and SafeNet Authentication Service, access management and authentication services, and SafeNet Authentication Client Middleware, for certificate-based authentication. Thales partners with 3rd-party CMS vendors to offer the most comprehensive identity access and authentication management solutions.



PKI/CBA Smart Cards

Thales' smart cards deliver the perfect combination of convenience and robust security, leveraging PKI Certificate-Based Authentication (CBA). These versatile cards support advanced features such as preboot authentication, disk encryption, file encryption, digital signatures, and secure certificate and key storage.

In addition to their digital security capabilities, all Thales smart card authenticators can double as physical access cards, making them an all-in-one solution for securing both digital and physical assets. They also offer customizable branding and photo-badging options, with dual-interface versions compatible with NFC-enabled devices such as smartphones and tablets. These smart cards are fully supported by SafeNet Authentication Client Middleware or SafeNet Minidriver.

	Thales TCT Smart Card 650 SC650 enables strong two-factor authentication and proof-positive user identification in all PKI environments and is certified for use in Defense Networks. It supports numerous algorithms, X.509 digital certificates and on-card certificate validation.
	SafeNet IDPrime 930, 930nc, 931 SafeNet IDPrime 930 and 930nc are contact interface smart cards and are compatible with any environment through support by the SafeNet Authentication Client. SafeNet IDPrime 930 is FIPS 140 Level 2 certified for the combination of the Java platform and the PKI applet. SafeNet IDPrime 931 includes optional contactless card body for physical access control (MIFARE, DESFire, HID and others).
	SafeNet IDPrime 940, 940B, 940C and 941 SafeNet IDPrime 940 and 940C are Plug and Play contact interface smart cards and are compliant with eIDAS regulations. These cards are CC EAL5+ / PP Java Card certified for the Java platform and CC EAL5+ / PP QSCD certified for the combination of Java platform and PKI applet. They are also compliant with eIDAS regulations. SafeNet IDPrime 940C benefits from state-of-the-art security standards and relies on the latest IDCore 140C, CC EAL6+ certified. SafeNet IDPrime 941 includes optional contactless card body for physical access control (MIFARE, DESFire, HID and others).
	SafeNet IDPrime 3930 SafeNet IDPrime 3930 is a dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO 14443 interface, also compatible with some NFC readers. This smart card is FIPS 140 Level 2 certified for the combination of Java platform and PKI applet.
	SafeNet IDPrime 3940 and 3940C (Dual interface) SafeNet IDPrime 3940 and 3940C are dual-interface smart cards, allowing communication either via a contact interface or via a contactless ISO 14443 interface, also compatible with some NFC readers. These smart cards are CC EAL5+ / PP Java Card certified for the Java platform and CC EAL5+ / PP QSCD certified for the combination of Java platform and PKI applet. They are also compliant with eIDAS regulations. SafeNet IDPrime 3940C benefits from state-of-the-art security standards and relies on the latest IDCore 3140C, CC EAL6+ certified.
	SafeNet IDPrime PIV The SafeNet IDPrime PIV (Personal Identity Verification) is a FIPS 201-compliant smart card designed for U.S. government agencies and banks, Insurances or health organizations to issue trusted user credentials. Supporting both CIV and PIV-I deployments, it offers premium privacy protection with OPACITY protocol compliance, enhanced performance, and built-in biometric capabilities such as Match-on-Card for advanced user authentication.

PKI/CBA USB Tokens

Thales' SafeNet PKI USB token delivers strong multi-factor authentication in a compact USB format, ensuring secure access and data protection. Designed for PKI-based security, it supports remote and network access, password management, digital signatures, and data encryption. Available with FIPS and Common Criteria (CC) certification, it meets high security standards while enabling seamless access to critical resources.



SafeNet eToken 5110+ FIPS

The TAA-compliant eToken 5110+ is a portable USB authenticator that enhances security with two-factor authentication. Using advanced smart card technology, it securely stores credentials like private keys and digital certificates, requiring both the token and a password for access. With plug-and-play functionality, it supports secure corporate access, digital signatures, and pre-boot authentication without the need for special readers. Easy to use and customizable with branding options, it provides strong security with minimal complexity.

FIDO Smart Cards

Thales FIDO Smart Cards provide secure, passwordless multi-factor authentication for cloud services, web applications, and Windows 11+ devices. Organizations can extend FIDO authentication to additional use cases, such as physical access, PKI-based authentication, digital signatures, and file encryption, enabling seamless authentication across both digital and physical environments. These additional features are optional, allowing organizations to adopt only what suits their needs. This approach enhances ROI, improves user productivity and adoption, and supports customizable branding.

To better fit with large organization's needs, Thales offers some FIDO smart cards in the Enterprise Edition. With the Enterprise Edition, large organizations get advanced management and security features that help them accelerate and secure their FIDO deployment.



SafeNet IDPrime 3930 FIDO and IDPrime 3940 FIDO (smart cards)

Both smart cards are designed for PKI-based applications and FIDO authentication, making them an ideal choice for enterprises seeking a passwordless solution for employees while preserving PKI functionalities such as qualified digital signatures and file encryption.

With dual-interface capability, they support both contact and contactless authentication and are compatible with NFC readers, ensuring seamless and flexible integration across various environments.

SafeNet IDPrime 3930 FIDO is FIPS 140 Level 2 certified for the combined Java platform and PKI applet.

SafeNet IDPrime 3940 FIDO is CC EAL5+certified, complies with eIDAS regulation and has obtained the French "Qualification Renforcée" from ANSSI.



SafeNet IDPrime FIDO Bio Smart Card

Combining biometrics and NFC, the innovative SafeNet IDPrime FIDO Bio Smart Card allows end users to authenticate from multiple types of devices securely and easily, with just a fingerprint instead of a password. End users authenticate faster & easier by tapping the card on their device and putting their fingerprint on the biometric sensor. To protect users' data privacy, fingerprint on-device authentication ensures users' data never leaves the device. Made in France, Certified FIDO 2.1 L2.



SafeNet IDPrime FIDO

The SafeNet IDPrime FIDO is a dual-interface smart card that supports FIDO authentication in both contact and contactless mode making it compatible with a large variety of devices. It offers secure, password-free modern authentication, making it a reliable choice for businesses looking for easy compliance with FIDO and NIST regulations. FIDO2.1 L1 certified and FIPS 140-3 L2 certification in progress.

SafeNet IDPrime FIDO is also available in the Enterprise Edition.



SafeNet IDPrime CL 940 FIDO and SafeNet IDPrime CL 930 FIDO (Smart Cards)

Both cards combine physical access, PKI and FIDO use cases in contactless mode and enable FIDO authentication on mobile devices thanks to NFC.

SafeNet IDPrime CL 940 FIDO is eIDAS qualified for both eSignature and eSeal applications and is Common Criteria certified. SafeNet IDPrime CL 930 FIDO is FIPS 140 Level 2 certified.

	SafeNet IDPrime PIV FIDO The SafeNet IDPrime PIV FIDO is a secure authentication solution that can be used for either a CIV (Commercial Identity Verification) or PIV-I (Personal Identity Verification – Interoperable) based deployment depending on company policies and requirements. SafeNet IDPrime PIV FIDO (Personal Identity Verification) card supports PIV and FIDO2.1 standards. Its FIPS 201 and FIPS 140-3 level 2 certifications are in progress. Available from PIV 4.0, this Smart Card provides premium privacy protection. Made in Europe and TAA compliant SafeNet IDPrime PIV FIDO is also available in the Enterprise Edition.
	SafeNet IDPrime PIV FIDO The SafeNet IDPrime PIV FIDO is a secure authentication solution that can be used for either a CIV (Commercial Identity Verification) or PIV-I (Personal Identity Verification – Interoperable) based deployment depending on company policies and requirements. SafeNet IDPrime PIV FIDO (Personal Identity Verification) card supports PIV and FIDO2.1 standards. Its FIPS 201 and FIPS 140-3 level 2 certifications are in progress. Available from PIV 4.0, this Smart Card provides premium privacy protection. Made in Europe and TAA compliant SafeNet IDPrime PIV FIDO is also available in the Enterprise Edition.
	SafeNet IDPrime DI 940 FIDO and SafeNet IDPrime DI 930 FIDO (Smart Cards) Both cards combine physical access, PKI and FIDO use cases in both contact and contactless mode and enable FIDO authentication on mobile devices thanks to NFC. Made in France. SafeNet IDPrime DI 940 FIDO is eIDAS qualified for both eSignature and eSeal applications and is Common Criteria certified. SafeNet IDPrime DI 930 FIDO is FIPS 140 Level 2 certified.

FIDO USB Tokens

Thales offers FIDO (Fast Identity Online) security tokens that enhance authentication through passwordless and phishing-resistant methods. Complying with FIDO2 standards, these tokens provide secure access to online services using PINs or biometrics, leveraging asymmetric cryptography to protect private keys from phishing attacks. Their broad compatibility with web applications and desktop environments makes them a versatile solution for secure authentication across multiple platforms.

To better fit with large organization's needs, Thales offers some FIDO USB tokens in the Enterprise Edition.

With the Enterprise Edition, large organizations get advanced management and security features that help them, when managed in the appropriate platform, to accelerate and secure their FIDO deployment. To know more about Thales FIDO Enterprise features, read this brochure.

	SafeNet eToken FIDO The TAA-Compliant, SafeNet eToken FIDO is a USB token, and an ideal solution for enterprises looking to deploy passwordless authentication for employees. This authenticator is a compact, tamper-evident USB with presence detection sensor, which creates a third factor of authentication: Something you have (physical token), something you know (PIN), something you do (touching the token). SafeNet Etoken FIDO is Certified FIDO 2.0 L1.
	Thales SafeNet eToken Fusion The eToken Fusion Series enables organizations to utilize passwordless phishing-resistant authentication methods improving security for enterprise resources accessed from any device. eToken Fusion Series allows presence detection and supports all PKI and FIDO use cases, in contact mode. eToken Fusion Series includes an option with CC certification. eToken Fusion is available in two form factors: USB-A and USB-C. Token Fusion with USB-C enables users to authenticate to any cloud resource by plugging this token to their mobile devices (phone/tablets).

	SafeNet eToken Fusion NFC FIPS The SafeNet eToken Fusion NFC FIPS empowers organizations with a strong, passwordless authentication solution designed to resist phishing attacks, thereby enhancing the security of enterprise resources accessed across various devices. This version features NFC for effortless contactless authentication. This makes it particularly well-suited for mobile devices like phones and tablets, allowing users to authenticate easily web applications from their mobile. Manufactured in France, its secure element is certified to the FIPS 140-3 L2 standard. Based on IDPrime 930. The eToken Fusion Series offers presence detection and supports all PKI and FIDO use cases in contact mode, ensuring a comprehensive and flexible authentication solution for diverse enterprise environments. This product is available in two convenient form factors, USB-A and USB-C and Certified FIDO 2.0 L1.
	SafeNet eToken Fusion NFC PIV The eToken Fusion NFC PIV is a USB Token that enhances the existing Fusion Series by adding NFC (Near Field Communication) for contactless authentication and PIV (Personal Identity Verification) support, making it ideal for high-security environments. It also supports the latest FIDO 2.1 standard, ensuring advanced passwordless authentication across a wide range of applications. Manufactured in France and certified to the rigorous FIPS 140-3 standard, this token offers top-tier cryptographic security. It supports a broad spectrum of use cases, including PKI and FIDO, providing comprehensive protection for sensitive resources. Available USB-A and USB-C form factor. Based on IDPrime PIV 4.0 – Certified FIPS 140-3 L2 and Certified FIDO 2.1 L1. The SafeNet eToken Fusion NFC PIV is available in Enterprise edition.
	SafeNet eToken Fusion Bio The eToken Fusion NFC PIV is a USB Token that enhances the existing Fusion Series by adding NFC (Near Field Communication) for contactless authentication and PIV (Personal Identity Verification) support, making it ideal for high-security environments. It also supports the latest FIDO 2.1 standard, ensuring advanced passwordless authentication across a wide range of applications. Manufactured in France and certified to the rigorous FIPS 140-3 standard, this token offers top-tier cryptographic security. It supports a broad spectrum of use cases, including PKI and FIDO, providing comprehensive protection for sensitive resources. Available USB-A and USB-C form factor. Based on IDPrime PIV 4.0 – Certified FIPS 140-3 L2 and Certified FIDO 2.1 L1. The SafeNet eToken Fusion NFC PIV is available in Enterprise edition.

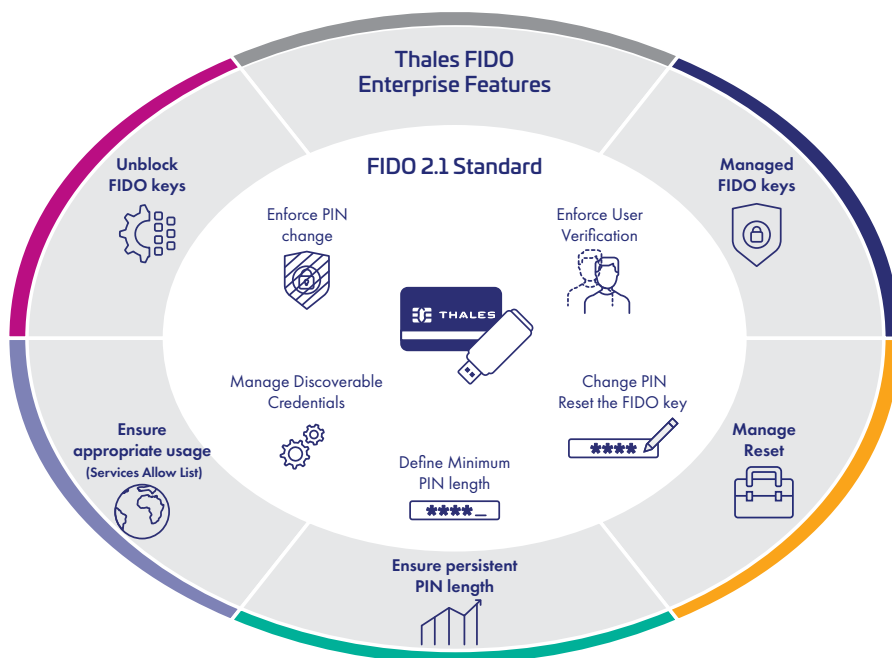
Thales Enterprise Edition

With Thales enterprise edition, Thales offers advanced management and security features tailored for large organization's needs. By going beyond the FIDO standards, Thales's devices allow greater control of the devices for Administrators and users.

What makes Thales FIDO Enterprise features unique?

Thales FIDO enterprise features allow organizations to manage their FIDO keys securely and easily throughout their lifecycle. They add an administration layer and configuration policies to help IT teams deploy, administer, and support the end user. Beyond the FIDO Alliance FIDO2.1 specifications, Thales FIDO enterprise features offer organizations:

- **Better security** - Enforcing user verification during authentication from any device, managing the minimum PIN length and protecting the PIN policy set, preventing data in FIDO keys from malicious or non-intentional deletion.
- **Appropriate usage of organization assets** - Limiting the usage of the FIDO authenticators to a list of preferred services.
- **Reduced IT costs & better user experience** - Unlocking the FIDO key without resetting all key data, allowing end users to set and change their PIN code in self-service. To benefit from these unique capabilities, consider Thales Enterprise Edition.



Hardware OTP Tokens

SafeNet's One-Time Password (OTP) Authentication products generate highly secure one-time passwords ensuring that only properly authenticated users are authorized access to critical applications and data. SafeNet OTP authenticators are available in both time- and event-based versions, never expire, and require no battery replacements. They also comply with OATH standards and are ideal for remote access solutions.

	SafeNet OTP Display Card SafeNet OTP Display Card is an OATH-compliant 2FA token designed in a convenient credit card form factor.
	SafeNet OTP 111/112 Token The SafeNet OTP 111 and SafeNet OTP 112 are OATH-certified OTP devices enabling two-factor authentication to a broad range of resources. SafeNet OTP 111 replaces SafeNet OTP 110 and SafeNet OTP 112 replaces eToken PASS.

SafeNet MobilePASS+ Mobile Authenticator App

SafeNet MobilePASS+ is a next generation authenticator app that offers secure one-time passcode (OTP) generation on mobile, wearables and windows devices, as well as single-tap push authentication for enhanced user convenience.

	SafeNet MobilePASS+ Push Authentication Technology SafeNet MobilePASS+ is an authenticator app that provides secure push and one-time passcode (OTP) authentication across mobile, desktop, and wearable devices. It offers fast, frictionless login with single-tap push approvals, biometric options, and reliable OTP fallback when push is unavailable. Designed for strong security and easy deployment, it integrates with existing infrastructure, reduces management overhead, and supports multiple platforms including Android, iOS, Windows, and Apple Watch.
---	--

Tokenless Authentication Solutions

Thales's tokenless technology enables any user to be authenticated anytime and anywhere. Thales's context-based authentication offers convenient, frictionless strong authentication while maintaining the flexibility and agility to add protection with stronger methods of security in higher risk situations. Combined with "step-up" authentication, context-based authentication optimizes a layered approach to access security by assessing user login attributes and matching them against pre-defined security policies.

	Grid or Pattern Based Authentication Thales's GrIDsure flexible authentication method allows an end-user to generate a one-time password without the requirement for hardware tokens or software applications. GrIDsure tokens work by presenting the end-user with a matrix of cells which contain random characters, from which they select a 'personal identification pattern' (PIP).
---	--

Virtual Smart Card

SafeNet IDPrime Virtual enables secure cloud transformation by building on your current PKI authentication framework for cloud access. Increase mobility by allowing users to authenticate to apps and carry out PKI operations from any device including BYOD (Bring your Own Device) via VDI within a Windows-based VDI environment. And reduce operational costs associated with hardware- based smart cards by replacing them with a virtual solution without compromising security.

	SafeNet IDPrime Virtual SafeNet IDPrime Virtual Smart Card allows users to access a software-based PKI credential within the VDI. Users can access all apps that have required PKI-based authentication and carry out PKI-based operations on any device, without the need for a physical smartcard or USB token. SafeNet IDPrime Virtual is PKI-based software authenticator, uses the latest innovation in software-based smart token technology to combine the strong two-factor security of a smart card, with the cost effectiveness, and convenience of software authentication.
---	--

HSM-Secured Identity Credentials

Thales TCT's Luna Credential System (LCS) introduces a new approach to multi-factor authentication by maintaining user credentials in a centralized hardware device that is securely accessible by endpoints in a distributed network. It unites the familiarity of certificate-based authentication with the security of a FIPS 140-2 certified hardware security module (HSM). LCS is a multi-purpose, secure credential system ideally suited for an environment in which the endpoints cannot use a traditional small form-factor token.



Luna Credential System

Composed of the Luna Credential HSM and the Luna Credential Client, LCS supports a number of use cases including Windows Logon and authentication to PK-enabled applications and websites.

Luna Credential HSM generates and protects PKI user credentials within the HSM thereby replacing individual tokens. Credentials never leave the security boundary of the HSM and can only be accessed by authorized endpoints over a secure communication link.

The Luna Credential Client, which is installed on the endpoint machine, provides an equivalent user experience to traditional multi-factor authentication login.

Luna as a Service Credential System

LCS is also available as a FedRAMP® High authorized cloud service. Thales TCT has partnered with XTec to deliver Luna as a Service Credential System to U.S. Federal Government agencies. Luna as a Service Credential System is provided through XTec's FedRAMP High AuthentX Cloud Software as a Service platform. Customers benefit from XTec's full time maintenance and support for services that reduce overhead and the burden within your agency. AuthentX Cloud is housed across three geographically separated facilities within the U.S.

Card Readers

Interface devices, or readers, are an essential component of any smart card deployment and ensure communication between smart cards and network services, but they must do so in a convenient yet secure manner. Thales's full range of smart card readers provide the perfect balance of ease of use, backed by the highest level of security.



IDBridge CT30/CT30-C

IDBridge CT30 is a USB contact reader, with a compact and transparent casing, and an optional stand accessory.

IDBridge CT30-C is USB-C contact reader, the compact and lightweight design of the IDBridge CT30 and CT30-C has the double advantage to optimize shipping expenses and to support your sustainability strategies by reducing the carbon footprint.



IDBridge CT31

IDBridge CT31 is a PIV and TAA-certified USB contact reader, with a compact and transparent casing, and an optional stand accessory.



IDBridge CT40

IDBridge CT40 is a USB contact reader, with a compact and slim-line casing



IDBridge CT700

IDBridge CT700 is a desktop pinpad for secure pin entry

Authentication and Access Management



OneWelcome Identity platform

Thales OneWelcome Identity Platform is a unified, flexible platform that manages all your use cases for Consumer (B2C), Business (B2B), Gig Worker and Workforce/Employee Identities. This core platform can be expanded with a range of identity apps that combine to meet your organization's specific needs. The platform is a scalable solution for managing digital identities, enabling seamless and compliant access for customers, employees, and partners. It combines features like customer identity and access management (CIAM), adaptive multi-factor authentication (MFA), identity federation, and consent management to enhance user experience and security. Designed for industries like banking, healthcare, and retail, it supports compliance with privacy regulations and simplifies access to digital services, making it ideal for modern enterprise



SafeNet Trust Access

SafeNet Trusted Access SafeNet Trusted Access (STA) is a comprehensive access management and authentication solution tailored for B2B use cases to secure diverse application environments for critical infrastructure organizations. It ensures robust protection for both cloud and on-premises data, addressing evolving challenges such as managing multiple authentication journeys, enabling secure access for remote workers, and reinforcing Zero Trust principles. By streamlining authentication through tailored policies and supporting advanced methods like passwordless authentication, SafeNet Trusted Access reduces risks such as phishing and credential theft. Additionally, it helps organizations achieve compliance with regulatory standards like ISO and PCI DSS, ensuring security, flexibility, and operational efficiency in an ever-changing threat landscape.



SafeNet Authentication Service Private Cloud Edition

SafeNet Authentication Service Private Cloud Edition (SAS PCE) is a comprehensive on-premises authentication solution that simplifies the user experience and allows secure access to multiple applications and systems (extending authentication to cloud/web with SAML/OIDC-based protocols) SAS PCE delivers fully automated management system that highly secure authentication with flexible token options that are tailored to the unique needs of your organization, substantially reducing the total cost of operation. An ideal solution tailored for B2E use cases. It also enables SSO support with SafeNet Access Exchange.

Management Tools



SafeNet Authentication Client (SAC)

SafeNet Authentication Client is a unified middleware client that manages Thales's extensive SafeNet portfolio of Identity and Access Management Solutions, including certificate-based authenticators such as eToken, IDPrime smart cards, USB, and software-based devices. Offering full backward compatibility and incorporating features from previous middleware versions, SafeNet Authentication Client ensures complete support for all currently deployed eToken devices, as well as IDPrime smart cards.



SafeNet Minidriver

The SafeNet Minidriver offers a simple and efficient way to use minidriver-enabled smart cards and tokens within a Windows environment. Designed for ease of use, it streamlines smart card management while minimizing administrative overhead. Ideal for organizations with smaller deployments, this lightweight solution ensures seamless integration and hassle-free management of SafeNet minidriver-enabled smart cards and eTokens, making security more accessible and efficient. More info.



OneWelcome FIDO Key Lifecycle Management

Thales offers OneWelcome FIDO Key Lifecycle Management, which is an end-to-end solution that helps CISOs streamline and secure their passwordless authentication journey. From onboarding to revocation, it simplifies FIDO security key management, ensuring efficiency, scalability, and strong security at every stage. As FIDO security keys set the gold standard for protecting sensitive data and preventing phishing attacks, large organizations often face challenges in deploying them at scale. This solution addresses those challenges by enabling seamless integration and management of FIDO hardware security keys across the enterprise.



SafeNet FIDO Key Manager

SafeNet FIDO Key Manager is a standalone offline application available on Mobile and Desktop platforms that allows administrators and end users to set up and manage Thales' FIDO USB tokens and smart cards all along their life cycle. SafeNet FIDO Key Manager is a great fit for organizations looking for a self-service app for FIDO security keys along with enterprise grade admin controls whenever needed. The application is available on Windows, macOS, Android and iOS.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com