



Thales Trusted Cyber Technologies Authentication Solutions

thalestct.com

THALES

Diverse Form Factors for Convenient Strong Authentication

Offering the broadest range of multi-factor authentication methods and form factors, Thales Trusted Cyber Technologies (TCT) facilitates and empowers enterprise-wide security initiatives for maintaining and improving secure access to enterprise resources.

Thales TCT offers authentication solutions that address the evolution of identities. From traditional high assurance and commercial-of-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.

Thales TCT's wide-range authenticators includes hardware and software OTP tokens, X.509 certificate-based USB tokens and smart cards, OOB, hybrid tokens, and phone tokens for all mobile platforms. Many Thales hardware tokens support physical access control to secure buildings and sites.

Allowing you to address numerous use cases, assurance levels and threat vectors, Thales TCT authenticators are supported by authentication 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.

Thales TCT offers both its own line of government-specific, high assurance authentication solutions and Thales OneWelcome authentication solutions. Thales TCT mitigates the risk associated with procuring data security solutions developed outside of the U.S. through our Proxy Agreement with DCSA for FOCl and CFIUS National Security Agreement.

Supported Authentication Methods



PKI



Hardware



3rd Party



OTP Push



Voice



Kerberos



Pattern Based



Passwordless



Biometric



Password



Google
Authenticator



SMS



eMail



fido



HSM
Credential System

Access Management



SafeNet
Trusted Access



SafeNet
Authentication Service

Middleware



SafeNet Authentication Client









SafeNet Minidriver

Certificate-Based Smart Cards

As convenient as any other card in your wallet, Thales's credit card-size form factors enable enhanced security with PKI Certificate-Based-Authentication (CBA). Smart cards enable other rich security features like preboot authentication, disk encryption, file encryption, digital signatures, and secure certificate and key storage.

Most Thales smart card authenticators can easily double as physical access cards to secure buildings and sites, in addition to offering rich branding options and support for photo-badging. Depending on the configuration, Thales's certificate-based authenticators are FIPS or CC certified. Thales TCT's Smart Card 650 (SC650) is certified for use in defense networks by the National Security Agency. The dual interface versions of SafeNet IDPrime smart cards comply with the ISO 14443 standard which is also compatible with some NFC readers present in smartphones and tablets. SafeNet IDPrime smart cards are supported by SafeNet Authentication Client Middleware or SafeNet Minidriver.

	<p>Thales TCT Smart Card 650</p> <p>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.</p>
	<p>SafeNet IDPrime 3940</p> <p>SafeNet IDPrime 3940 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. The smart card is 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.</p>
	<p>SafeNet IDPrime 940</p> <p>SafeNet IDPrime 940 is a Plug and Play contact interface smart card and is compliant with eIDAS regulations. IDPrime 940 is 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.</p>
	<p>SafeNet IDPrime 3930</p> <p>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 140-2 Level 2 certified for the combination of Java platform and PKI applet.</p>
	<p>SafeNet IDPrime 930/931 Series</p> <p>SafeNet IDPrime 930 series include a Plug and Play contact interface smart cards. Depending on configuration the card is compliant with FIPS regulations and FIPS 140-2 Level 2 certified for the combination of the Java platform and PKI applet.</p> <p>SafeNet IDPrime 931 includes optional contactless card body for physical access control (MIFARE, DESFire, HID and others)</p>
	<p>SafeNet IDPrime PIV</p> <p>SafeNet IDPrime PIV (Personal Identity Verification) card is a FIPS 201 standards-based card for U.S. government agencies, state and local government organizations to issue user credentials that the Federal Government can trust. The same card can be used for either a CIV or PIV-I based deployment depending on company policies and requirements. Available from PIV 3.0, this smart card provides premium privacy protection (compliant with the OPACITY protocol). Customers can benefit from enhanced performance and built-in biometric capabilities (Match-on-Card), preparing them for enhanced user authentication.</p>

Certificate-Based USB Tokens




Thales's portfolio of certificate-based USB tokens offers strong multi-factor authentication in a traditional USB form factor, enabling organizations to address their PKI security needs. SafeNet PKI USB tokens offer a single solution for strong authentication and applications access control, including remote access, network access, password management, network logon, as well as advanced applications including digital signature, data and email encryption.




Depending on their configuration, the certificate-based USB tokens can be FIPS and CC certified.

	<p>Thales TCT sKey 3250</p> <p>sKey3250, a high assurance certificate-based USB authenticator, contains a custom smart card ASIC, the SCC650, developed on-shore by Thales TCT. This SCC650 ASIC designed to the highest security principles, implements a security architecture found in other Thales TCT certified ASICs, and is fabricated at a trusted foundry.</p>
	<p>SafeNet eToken 5110+ FIPS</p> <p>TAA-compliant, ultra strong authentication, security in a convenient, portable form factor. Secure remote and network access, as well as certificate-based support for advanced security applications, including digital signature and pre-boot authentication.</p>
	<p>SafeNet eToken 5300</p> <p>SafeNet eToken 5300 is a compact, tamper-evident USB, which creates a third factor of authentication. This next generation eToken features presence detection functionality, is FIPS 140-2 certified and is available in Micro and Mini form factors. It holds CC EAL 6+ certification at the chip boundary. Depending on configuration, this token supports USB-C connection.</p>

FIDO Authenticators




FIDO authenticators enable multi-factor authentication to cloud and web services as well as Windows 11 devices. Thales offers a range of FIDO security keys, including combined PKI-FIDO smart cards and FIDO USB tokens.

	<p>SafeNet IDPrime 3930 FIDO and SafeNet IDPrime 3940 FIDO (smart cards)</p> <p>Both cards are designed for PKI-based applications and FIDO as an ideal solution for enterprises looking to deploy passwordless authentication for employees. The smart card comes with a SafeNet Minidriver that offers perfect integration with native support for Microsoft® environments, without any additional middleware. These dual-interface smart cards, allow communication either via a contact interface or via a contactless ISO 14443 interface, are also compatible with NFC readers</p> <p>SafeNet IDPrime 3930 FIDO is FIPS 140-2 Level 2 certified for the combined Java platform and PKI applet.</p> <p>SafeNet IDPrime 3940 FIDO is 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.</p>
	<p>SafeNet eToken FIDO (USB token)</p> <p>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, which creates a third factor of authentication: Something you have (physical token), something you know (PIN), something you do (touching the token).</p>
	<p>SafeNet IDCore 3121 FIDO (Smart Card)</p> <p>The SafeNet IDCore 3121 FIDO is a physical and logical smart card with FIDO. This smart card is an ideal solution for enterprises looking to deploy passwordless authentication for employees with physical access functionality (Mifare 4kb, Desfire 4kb/8kb, Mifare 4kb Desfire 4kb/8kb).</p> <p>This contactless smart card allows communication via a contactless ISO 14443 interface and is also compatible with NFC readers.</p>

	<h3>SafeNet IDPrime 941 FIDO and SafeNet IDPrime 931 FIDO (Smart Cards)</h3> <p>Both cards combine physical access, PKI and FIDO use cases in one device and enable FIDO authentication on mobile devices thanks to NFC.</p> <p>SafeNet IDPrime 941 FIDO is qualified for both eSignature and eSeal applications and is Common Criteria certified.</p> <p>SafeNet IDPrime 931 FIDO is qualified for both eSignature and eSeal applications and is FIPS 140-2 Level 2 for the combined Java platform and PKI applet.</p>
	<h3>SafeNet eToken Fusion Series</h3> <p>The SafeNet eToken Fusion Series enables organizations to utilize passwordless phishing-resistant authentication methods improving security for enterprise resources accessed from any device. SafeNet eToken Fusion is available in two form factors: USB-A and USB-C. SafeNet eToken Fusion with USB-C enables users to authenticate to any cloud resource by plugging this token to their mobile devices (phone/tablets).</p> <p>SafeNet eToken Fusion Series allows presence detection and supports all PKI and FIDO use cases, in contact mode. The SafeNet eToken Fusion Series includes an option with CC certification.</p>
	<h3>SafeNet IDPrime FIDO Bio (Biometric Smart Card)</h3> <p>Provide your end users a new passwordless authentication experience thanks to SafeNet IDPrime FIDO Bio Smart Card.</p> <p>End users authenticate faster & easier by tapping the card on their device and putting their fingerprint on the sensor. To protect users' data privacy, with fingerprint on-device authentication, users' data never leave the device.</p>


Hardware OTP Tokens

Thales's SafeNet OTP hardware tokens provide a strong and scalable foundation for securing access to enterprise, web-based and cloud applications, and complying with privacy and security regulations. Thales's SafeNet hardware tokens offer rich case-branding options, and are field-programmable by the customer, enabling organizations to maintain stringent control over their own critical OTP security data.

	<h3>SafeNet OTP Display Card</h3> <p>SafeNet OTP Display Card is an OATH-compliant 2FA token designed in a convenient credit card form factor.</p>
	<h3>SafeNet OTP 110</h3> <p>SafeNet OTP 110 is a cost effective OATH-compliant OTP hardware token that features waterproof casing, and enables two-factor authentication in time-sync and event-based modes.</p>
	<h3>SafeNet eToken PASS</h3> <p>SafeNet eToken PASS is an OATH compliant OTP hardware token that offers secure two factor authentication, in time- sync and event-based modes.</p>

Certificate-Based Virtual Smart Cards

Enable your cloud transformation securely by building on your current PKI authentication framework for cloud access. Increase mobility by allowing users to access enterprise apps with PKI credentials, from any device via Virtual Desktop Infrastructure (VDI).

	<h3>SafeNet IDPrime Virtual</h3> <p>The SafeNet IDPrime Virtual is a virtual smart card that offers the same functionality of hardware but reduce operational overheads associated with managing hardware and can be used instead of physical smart cards.</p>
---	--

SafeNet MobilePASS+ Mobile Authenticator App

SafeNet MobilePASS+ is a next generation authenticator app that offers secure one-time passcode (OTP) generation on mobile devices, single-tap push authentication for enhanced user convenience and Push with Number Matching for better protection against MFA fatigue or push bombing attacks



SafeNet MobilePASS+ Push Authentication Technology

SafeNet MobilePASS+ is a next generation authenticator app that offers secure passwordless authentication to hundreds of applications, including SaaS and VPNs. MobilePASS+ lets users authenticate with a single tap of a finger on their mobile device as well as offering secure one-time passcode (OTP) generation. For better protection against push bombing attacks, push authentication can be combined with number matching, asking the end user to select the number that appears during authentication. SafeNet MobilePASS+ offers additional protection provided by use of alphanumeric PINs or biometric PINs on all devices: iOS with Touch ID and Face ID; Android with fingerprint and facial recognition; Windows Hello for Business with fingerprint and/or facial recognition. SafeNet MobilePASS+ can support multiple authenticators, multiple languages and dark mode functionality.

SMS Out-of-Band Authentication



SMS Out-of-Band Authentication

Delivered by SMS text messages, out-of-band authentication reduces the administrative overhead of a strong authentication solution by removing the need to install software or distribute hardware. Delivery is also available via email.

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.



Pattern-based Authentication

Pattern-based, also called GrIDSure Authentication is a convenient pattern-based authentication solution that overcomes the weakness of passwords without the need for software to be installed or hardware to be provisioned.

Pattern-based Authentication works by presenting the user with a matrix of cells during enrollment containing random characters, from which the user selects a Personal Identification Pattern (PIP). Every time the challenge grid appears, the characters in the cells are different, so the user is always entering a one-time passcode.



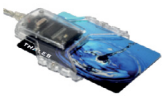
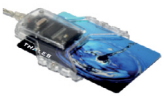


Context-Based Authentication

Context-based or contextual authentication is central to creating compliance based access policies and preventing security fatigue. Taking into account variables, such as your network, location and operating system, contextual data provides additional information on a login attempt, and fires the appropriate access policy.

By assessing a user's contextual login attributes, single sign on and access management solutions can continuously match the level of authentication required from the user with the access policy defined for each application.

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

Management

The need to securely and timely manage users and authenticators is important with any PKI-based deployment. Thales offers the most comprehensive access and authentication management systems management systems to administer, monitor, and manage strong authentication deployments and digital signing across the organization.

Middleware

Thales middleware enables strong authentication operations and the implementation of certificate-based applications such as digital signing, network logon and password management. Since every organization does not have the same needs, we have a full middleware client solution, as well as a light-weight minidriver option that is fully integrated on Windows.

Advanced Management Functionality

- SafeNet Authentication Client:
Full management solution, providing full local admin and support for advanced card and token management, events and deployment

Light Management Functionality

- SafeNet Minidriver

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.

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