

cpl.thalesgroup.com

THALES

SafeNet Authenticators

Contents

3 Diverse Form Factors for Convenient Strong Authentication

4 Hardware OTP Tokens

4 Certificate-based Virtual Smart Card

5 Certificate-based Smart Cards

6 Certificate-Based USB Tokens

6 FIDO Devices

7 Smartphone and Software Tokens

7 Tokenless Authentication Solutions

8 Card Readers

8 About SafeNet Identity and Access Management Solutions

8 About Thales

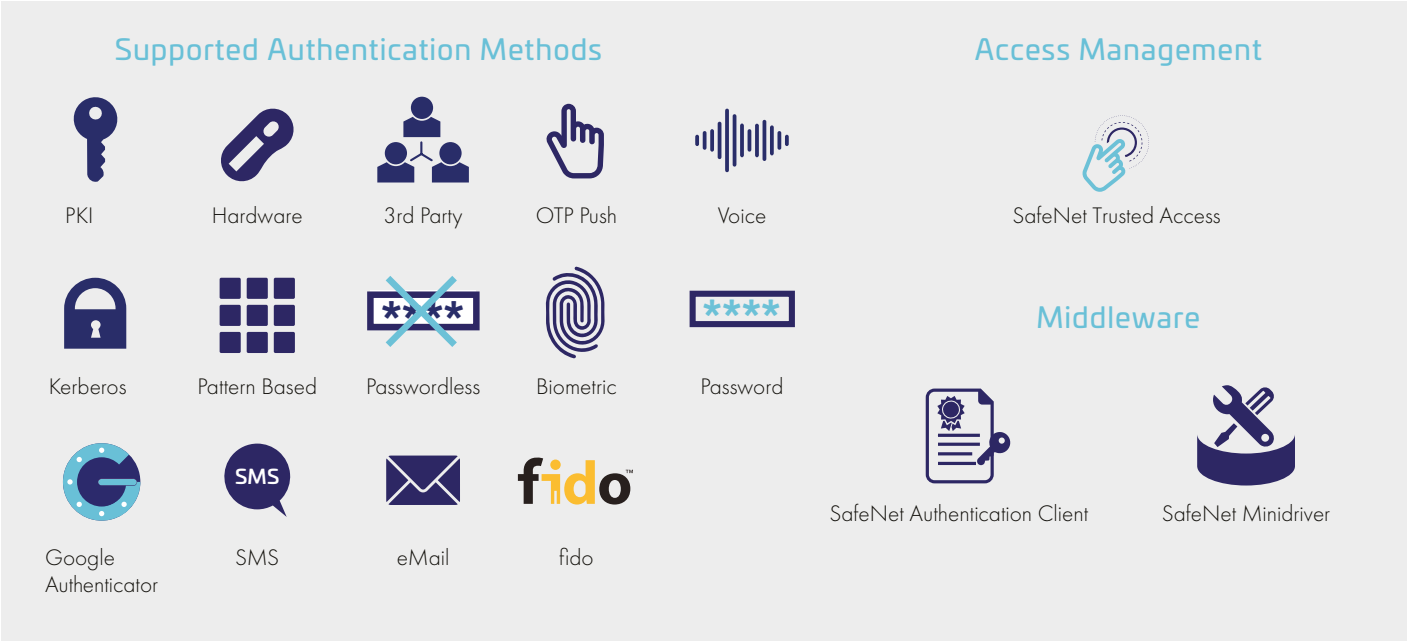
Diverse Form Factors for Convenient Strong Authentication

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

Thales's SafeNet authenticators include hardware and software OTP tokens, FIDO devices, X.509 certificate-based USB tokens , physical and virtual smart cards, OOB, hybrid tokens, and phone tokens for all mobile platforms. Many Thales SafeNet hardware tokens support physical access control to secure buildings and sites.

Allowing you to address numerous use cases, assurance levels and threat vectors, Thales's 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), an access management and authentication service, 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.

To tailor strong authentication to your business and IT needs, choose from the authenticators shown below:



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.



SafeNet OTP Display Card

SafeNet OTP Display Card is an OATH-compliant 2FA token designed in a convenient credit card form factor.



SafeNet OTP 110

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.



SafeNet eToken PASS

SafeNet eToken PASS is an OATH compliant OTP hardware token that offers secure two factor authentication, in time-sync and event-based modes.



SafeNet GOLD

Offering an additional layer of security beyond basic OTP, the SafeNet GOLD is activated with a personal identification number (PIN), which prompts the authenticator to provide an OTP. In challenge response mode, users activate GOLD with their PIN, and then must validate a numeric challenge on their GOLD authenticator.

Certificate-based Virtual Smart Card

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 VDI.

SafeNet IDPrime Virtual

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.

Certificate-based Smart Cards

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

All 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. 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.



SafeNet IDPrime 3940

SafeNet IDPrime 3940 is a dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO14443 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. It is also compliant with eIDAS regulations and qualified by the French ANSSI.



SafeNet IDPrime 940

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. It is also compliant with eIDAS regulations and qualified by the French ANSSI.



SafeNet IDPrime 3930

SafeNet IDPrime 3930 is a dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO14443 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.



SafeNet IDPrime 930

SafeNet IDPrime 930 is a Plug and Play contact interface smart card and is compliant with FIPS regulations. This smart card is FIPS 140-2 Level 2 certified for the combination of the Java platform and PKI applet.



SafeNet IDPrime PIV

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.

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.



SafeNet eToken 5110

SafeNet eToken 5110 provides PKI based two-factor authentication for secure remote and network access, as well as support for advanced security applications, including digital signature and pre-boot authentication.



SafeNet eToken 5300

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.

FIDO Devices

FIDO authenticators enable multi-factor authentication to cloud and web services as well as Windows 10 devices. Thales offers a range of FIDO devices, including a combined PKI-FIDO smart card and a FIDO USB token.



SafeNet IDPrime 3940 FIDO (Smart Card)

The SafeNet IDPrime 3940 FIDO Smart Card is designed for PKI-based applications and comes with a SafeNet minidriver that offers perfect integration with native support for Microsoft® environments, without any additional middleware. This dual-interface smart card, allowing communication either via a contact interface or via a contactless ISO14443 interface, is also compatible with some NFC readers.



SafeNet eToken FIDO (USB token)

The SafeNet eToken FIDO is a USB token, 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).

Smartphone and Software Tokens

Offering the convenience of phone-as-a-token authentication, Thales offers PUSH OTP software authentication for tablets and mobile phones.



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.



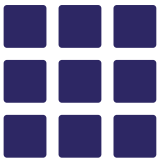
SafeNet MobilePASS+ Out of Band Push Authentication

Offering frictionless strong authentication to hundreds of applications, including SaaS and VPNs, push authentication on mobile devices lets users authenticate with a single tap of a finger print or face ID on their mobile device.

SafeNet MobilePASS+ is a next generation software token that lets users generate OTPs on their mobile devices, while also offering convenient out-of-band, single-tap push authentication.
SafeNet MobilePASS+ offers enhanced user experience, with optional QR code enrollment and optional biometric PIN: Face ID & Touch ID on iOS, fingerprint on Android and Windows Hello on Windows devices.

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 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.

About SafeNet Identity and Access Management Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policybased SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

To learn more, visit: cpl.thalesgroup.com/access-management

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Contact us

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

> cpl.thalesgroup.com <



© Thales - November 2020 • RMv46