thalescpl.com

THALES

SafeNet IDPrime PIV

Personal Identity Verification-interoperable ID credentials for federal agencies, government contractors, state and local governments and private sector organizations

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. This smart card provides premium privacy protection through mandatory and optional features of the SP800-73-4 standard. Customers can benefit from enhanced performance and built-in biometric capabilities (On Card Comparison), preparing them for enhanced user authentication.

Uses of PIV

- Based on strong multi-factor PKI authentication, SafeNet IDPrime PIV cards provide proof of cardholder identity that meets U.S. Federal Government standards
- Digitally authenticates users' identity for main information systems
- Identifies users for a variety of physical access systems
- Digitally signs and encrypts eDocuments, email and files
- Works with Federal Government PIV-based IT infrastructures, and new and legacy physical access control systems
- Biometric fingerprint and iris delivers highest level of identity assurance

Features

- Virtual Contact Interface (VCI) and Pairing code to enhance privacy through contactless interface, for physical access use cases
- PIV Secure Messaging to provide confidentiality and integrity protection to PIV card application
- Biometric Authentication (On Card Comparison), compliant to SP800-76-2, for enhanced user authentication
- Fast contactless authentication with an optimized Power-On-Self-Test mechanism as per the latest FIPS 140-2 specifications (CMVP IG 9.11)

PIV Technology and Standards

PIV card technology features a dual interface microprocessor chip for use with contact and contactless smart card readers, making it interoperable and easily adaptable for a wide range of use cases, including physical access authentication. SafeNet IDPrime PIV cards are certified FIPS 140-2, security level 2, FIPS 201-2 and listed on the GSA APL.

PIV and the U.S. Federal Government

Most U.S. federal government employees and subcontractors have a PIV card. Driven by the issuance of Homeland Security Presidential Directive 12 (HSPD-12) in 2004, the U.S. federal government has invested significant effort and resources in implementing robust, interoperable credentialing processes and technologies. The resulting standard, FIPS 201, Personal Identity Verification (PIV) for federal employees and contractors, provides a framework of the policies, processes, and technology required to establish a strong, comprehensive identity credentialing program.

Government Contractors and Critical Infrastructure Organizations

Implementing PIV-I identity credentialing and security systems helps enterprises, including those involved with the nation's critical infrastructure, to significantly upgrade the security of their information systems and networks. In addition, the fact that PIV-I credentials are trusted and interoperable with the federal government makes it much more efficient and secure for contractors to exchange information securely with their government clients. It also creates opportunities to improve business processes, such as digitally signing and encrypting contracts or specifications.

State and Local Government

State and local governments can leverage the federal PIV program by using PIV-I as the basis for their identity credentialing and information system security. Many point to the PIV standard as a way to achieve a more holistic approach to issuing identity credentials and improving their own business processes and information systems security. More than 16 states are currently planning or implementing some form of PIV-I or CIV (Commercial Identity Verification) strategy. PIV-I credentials are being used in regional and national interoperability exercises sponsored by the Federal Emergency Management Agency (FEMA) for First Responder Access Cards (FRAC). These credentials, typically issued by state and local governments, identify emergency responders for secure access to remote networks to pilot operations and access to Federal systems.

About SafeNet Access Management and Authentication 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 policy-based SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance. To learn more, please visit our website at safenet.gemalto.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.

Technical Specifications

Memory	SafeNet IDPrime PIV card is based on a Java Card platform (IDCore 3130) with 146 KB EEPROM memory with PIV v3.0 applet loaded.
Certifications	FIPS 140-2 Security level 2, FIPS 201-2, and listed on GSA APL (with the certificate #1510) • Roles, Services, and Authentication: Level 3 • Physical Security: Level 3 • EMI/EMC: Level 3 • Design Assurance: Level 3 SCP03, SCP02, SCP01 supported with scripting according to GP 2.2.1 Amendment • Amendment D ECC (256, 384) Asymmetric algorithms supported and FIPS certified
Cryptographic algorithms	**Hash -** SHA-224, SHA-256, SHA-384, SHA-512, SHA-1 **Symmetric -** AES (128-, 192-, 256-bit) **Asymmetric -** ECC (P-224, P-256, P-384, P-521 bits), RSA (up to RSA 4096 bits) using an on-card security controller with key pair generation and Deterministic Random Bit Generator (DRBG)
ISO specification compliance	• ISO 7816 contact interface (T=0 ; T=1) • ISO 14443 contactless interface compatible with NFC (T=CL) • IU high coercivity magnetic stripe (optional)
Other features	• Global PIN and local PIN • Dynamic Discovery Object management during post issuance • Dynamic Contactless interface de-activation mechanism • Fingerprint and iris biometric containers • Up to 20 Key archiving containers

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com