cpl.thalesgroup.com

THALES
Building a future we can all trust

SafeNet IDPrime Virtual

Virtual PKI Smart Card Solution

Global demand for PKI

Cyber security adoption is booming, with record IT spending on security solutions for enterprises using on-premises as well as cloud and web-based services. Along with the proliferation of vendors and solutions comes also a rise in security breaches. One of the most successful ways of stepping up on enterprise security has been through PKI-based authentication, a high assurance security framework used by many enterprises, defense departments and governments.

Pursuing Digital and Cloud Transformation Securely

With many enterprises already heavily invested and enjoying the security benefits of PKI technology, organizations face a few limitations: PKI cannot be used as an authentication method for cloud or web-based applications; cannot be used within VDI environments, and cannot be used in BYOD use cases such as mobile phones, tablets or certain laptops. In addition, hardware based smart cards are prone to be lost easily, and need to be physically delivered to users. Therefore, using virtual smart cards instead of physical ones can offer the same functionality of hardware but reduce operational overheads associated with managing hardware.

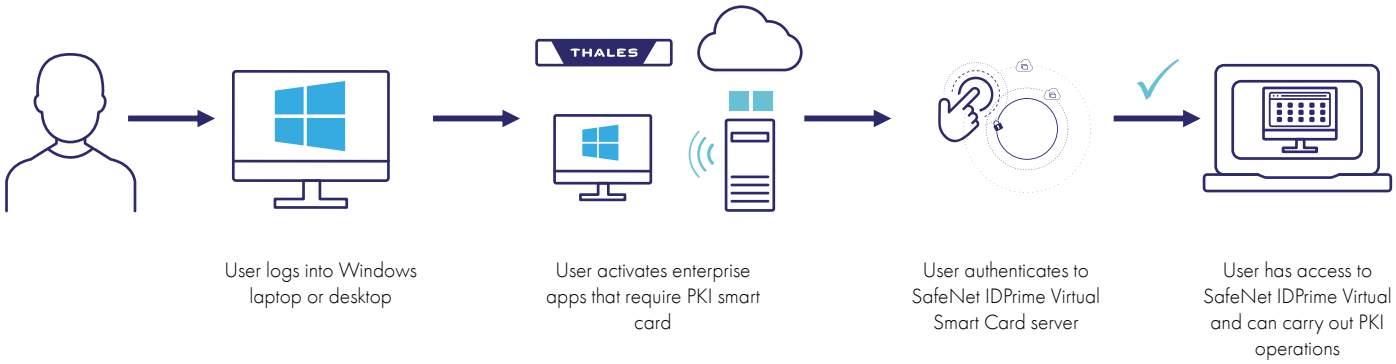
The Benefits of PKI Security in Software

With years of providing PKI-based solutions for enterprises, Thales has developed a way to serve PKI customers who need to support mobility use cases and want to reduce the use of hardware-based smart cards.

Extending PKI Security to Virtual Environments

Many organizations rely on VDI to facilitate mobility for their employees, enabling them to access enterprise applications from unmanaged devices, such as a mobile device or non-corporate issued PCs. However, in some cases, enterprise apps in the VDI require PKI authentication and other PKI based operations such as email encryption and digital signing. Since unmanaged and mobile devices don't support PKI smart cards, users may not be able to access the apps they need and carry out these PKI-based operations. The SafeNet IDPrime Virtual Smart Card overcomes this restriction, by allowing users to access a softwarebased PKI credential within the VDI. Now, 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 smart card 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.

SafeNet IDPrime Virtual Smart Card acts as hardware replacement



Benefits

- Facilitate mobility from any device, including BYOD (Bring your Own Device) while maintaining PKI-based security
- Reduce the operational overheads associated with hardware-based smart cards

Software is Simpler: Replacing hardware with a virtual token

Large customers are seeking virtual smart cards as a longterm and permanent solution for replacing hardware-based smart cards. Software-based smart cards functions are akin to hardware tokens. Virtual smart cards are simpler to handle as enterprises do not have to encounter hardships such as operational overhead, uniformity of form factors and devices, or lost tokens. By using the SafeNet IDPrime Virtual Smart Card Solution, organizations allow users to work in their usual Windows-environments, enjoying all the benefits of multifactor authentication in a high security setting. SafeNet IDPrime Virtual emulates the functionality of physical smart cards used for authentication, email & data encryption, and digital signing and enabling use cases such as VDI, BYOD, backup, and mobility on any device. It secures user private key on HSM with user authentication from OIDC compatible IDPs. What's more, organizations can also provision SafeNet IDPrime Virtual Smart Cards to temporary employees, contractors, or use it as a solution for employees who misplace or lose their hardware-based authentication devices.

SafeNet IDPrime Virtual Smart Card Solution Specifications

Key Features

- Full crypto operations support
- For desktop and web based applications
  - Import and generate certificates
  - Digital signature
- Encryption and decryption
- Certificate-based authentication
- Windows smart card authentication
- MS CAPI support by SafeNet Minidriver
- PKCS #11 support by SafeNet Authentication Client (SAC)
- BYOD (Bring your Own Device): authenticate to apps and carry out PKI operations within a Windows-based VDI environment
- Offline smart card support

Key Components

Server Components	
SafeNet IDPrime Virtual Server	• Delivered as a Docker • Provides REST based APIs • Provisioning API (for smart card provisioning) • SWS API (digital signature) • Key Management API • Client Interface API
SafeNet IDPrime Virtual Server Supported Databases	• MariaDB Database • MSSQL Database • MySQL Database • PostgreSQL Database • Oracle Database Enterprise and Express Edition
Supported HSMs	• Protects SafeNet IDPrimeVirtual database • SafeNet Luna 6/7.3/7.7Support • KeySecure • DPoD
SafeNet Trusted Access (or 3rd party IDP)	• STA • PingFederate • Okta • Keycloak Agent for SAS PCE
Client Components	
SafeNet Minidriver OR SafeNet Authentication Client (SAC)	PKI middleware/Minidriver
SafeNet IDPrime Virtual client	Launches the SafeNet IDPrime solution on the Windows client • IDPV System Tray • IDPV Windows Service • IDPV Credential Provider
Optional Components	
SafeNet IDPrime Virtual SDK	For developers who want to build proprietary apps

About Thales Cloud Protection & Licensing

Today's enterprises depend on the cloud, data and software in order to make decisive decisions. That's why the most respected brands and largest organizations in the world rely on Thales to help them protect and secure access to their most sensitive information and software wherever it is created, shared or stored—from the cloud and data centers to devices and across networks. Our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, and create more value from their software in devices and services used by millions of consumers every day.

Technical specifications

Server Operating Systems

- Red Hat Enterprise Linux (RHEL) Server 9
- Ubuntu 22.04
- CentOS-7

Client Operating Systems

- Windows 10 (64-bit)
- Red Hat Enterprise 8.3
- Ubuntu 20.04
- CentOS 8.3

Supported APIs

- PKCS#11 V2.20, PKCS#15, MS CryptoAPI and CNG(CSP,KSP), PC/SC

Supported cryptographic algorithms

- 3DES, SHA-256, RSA up to 2048

Supported CMSs

- Atos, Versasec

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