

SafeNet IDPrime Virtual Virtual PKI Smart Card Solution



PKI authentication, email & data encryption, and digital signing with a virtual smart card

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.

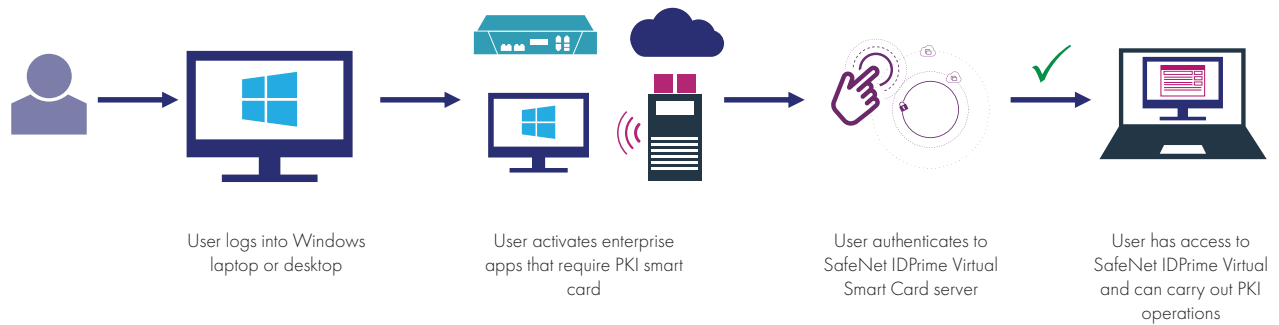
The Benefits of PKI Security in Software

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 software-based 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.

IDPrime Virtual Smart Card acts as hardware replacement



Benefits

- Facilitate mobility from any device, including BYOD while maintaining PKI-based security
- Reduce the operational overheads associated with hardware-based smart cards

Use Cases

- BYOD (Bring your Own Device): authenticate to apps and carry out PKI operations within a Windows-based VDI environment
- Digital signing
- Encryption and decryption
- Certificate-based authentication

Software is Simpler: Replacing hardware with a virtual token

Large customers are seeking virtual smart cards as a long-term 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 multi-factor authentication in a high security setting. 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
- Import certificates
- Generate certificates
- Digital signing
- Encryption and decryption
- MS CAPI support by SafeNet Minidriver
- PKCS #11 support by SafeNet Authentication Client (SAC)

Key Components	
Server Components	
SafeNet IDPrime Virtual Server	Delivered as a Docker
SafeNet IDPrime Virtual Server data base	<ul style="list-style-type: none"> • MariaDB Database • MSSQL Database
HSM	<ul style="list-style-type: none"> • Protects SafeNet IDPrime Virtual database • SafeNet Luna 7 Support
SafeNet Trusted Access (or 3rd party IDP)	Acts as an identity provider to authenticate users to the SafeNet IDPrime Virtual server
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
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.

