

# Smart Card Tokens

## *Introduction*

In an era when digital signature are fast replacing traditional hand written signature, the method in which this digital certificates are stored and operated by the holder of the certificate becomes an utmost concern for both the holder of the certificate as well the provider of the certificate. The certificates and the keys associated with the digital certificates are stored in cryptographic tokens. The tokens are protected by PINS/password only known to the holder of the digital certificate token. There are two ways in which the tokens can be provided to the end user:

- Soft Tokens (A P12 extension based cryptographic software token)

The soft token is software based cryptographic module which is directly loaded and stored into user's system. The software token is a module which protects the private key by encrypting the private key using the PIN/Password of the token. The key advantage of soft token is that it does not require any extra hardware to store it and doesn't require additional hardware driver to be installed on the system. The holder can also have backup of the token to avoid unprecedented situations arising out of loss of data from the system due to system failure or formatting of the system.

### *Disadvantages of soft token:*

- o The holder of the soft token is needed to ensure the security of the soft token file in terms of virus and malicious code access to it.
  - o The holder of the soft token is needed to assure that multiple copies of the soft token files are not taken by unwanted users. A copy of the soft token along with the knowledge of the pin can be used for fraudulent purposes by anyone having fraudulent intension.
- Hard Tokens (Built on the secured cryptographic smart card)

The hard token is built on the smart card technology wherein the keys are certificates are stored and generated on the smart card based token rather than the system. Smart card tokens are secured a cryptographic device which combines the processing capability of a smart card with its internal processors and combines the ability to perform complex cryptographic computation within the interface of the token in a secured manner. The tokens have capability to perform various cryptographic operations which includes operating on asymmetric and symmetric keys standards using various algorithms and ciphers.

*Advantages of using the hard tokens:*

- The keys are certificates are protected by the smart card operating system from any virus or malicious code attack from the user's system.
- Ability to generate Key's and Key Pairs internally and protecting the private keys using the secured microcontroller. The private key never comes out of the tokens. The tokens have the ability to generate RSA keys pairs internally and have the ability to hide the private keys from the outside world hence removing the danger of key compromise in a PKI implementation.
- Protects usage of the keys using the secured PIN or other mode of user authentication like biometrics finger prints. The operations on the private keys for generations of digital signature, encryption and decryption can only performed after the holder of the token presents the PIN or password associated with the token.
- Ability to perform PKI operations internally: The data to be signed is sent to the token and the token generates the signature internally and sends the signature outside application. Hence all operations are confined to the internal boundary of the smart card in the token.

**Types of Smart Card Tokens:**

Smart card tokens can be differentiated based on various parameters which include the following key parameters:

- Memory Capacity: Ranges from 16K to 132K for storage of keys and digital certificates.
- Operating system: The operating system is based on ISO 7816-4 to 15 specifications. There are native OS and multi application based OS like Java Card and MultOS.
- Form Factor:
  - o Plastic Card (credit card size) based format: This is standard sized card with the smart card chip embedded on it. The disadvantage of this form factor is that the user requires a smart card reader and supported devices drivers to be installed on the system. Hence the operating cost goes high. This are mainly used in the ID card based requirements where it can serve the common purpose of token and ID card.



- USB form factor: The smart card chip is embedded on the USB based reader with size and look and feel of standard thumb driver. The user can directly plug in the token into the system's USB port to use the token for digital signature purposes. Highly cost efficient and ease of use from the user's perspective.



### *Composition & Architecture of the smart card tokens:*

The smart card token is built on the secured operating system embedded into the secured microcontroller of the token architecture. The card operating system is based on the standard ISO 7816 (4-15) specifications for the file system structure and communication standards. An extra co processor is present in the smart card for performing critical security operations like generation of random number, generation of keys etc. The following table illustrates the various properties of the smart card based tokens:

Specifications	ISO 7816 (4-15)
On Board Security Algorithms	RSA 1024-bit / 2048-bit, DES, 3DES, SHA1
Memory Capacity	16K – 132 K
Memory data retention	At least 10 years
Memory cell rewrites	At least 50,000
Number of Key Pairs Supported	Minimum 2 Sets of Key Pairs
Number of Digital Certificates	Minimum 2
Secured Co-Processor	A coprocessor for generation of RSA keys and processing digital signatures.

### *E-Mudhra Supported Smart Card Tokens:*

The e-Mudhra PKI infrastructure provides user with smart card tokens based on the USB form factor. The USB form factor provided the much needed added advantage in which the user is not needed to have a smart card reader as required in traditional implementations. The USB form factor allows user to plug in the crypto module directly into the USB port of the system. E-Mudhra provides the following USB form factor based smart tokens to its user:

- Aladdin eToken Pro: Built on the proven SIEMENS embedded operating system, fully FIPS certified. Has the ability to generate up to 4 RSA keys pairs and store multiple user certificates. The e-Token pro has been deployed in many large PKI projects worldwide. More information on the token can be viewed at [http:// www.aladdin.com](http://www.aladdin.com)

