Smart Card 650

A High Assurance identification and authentication smart card that brings two-factor authentication to applications and networks where security is critical

High Assurance Security with Ultimate Flexibility

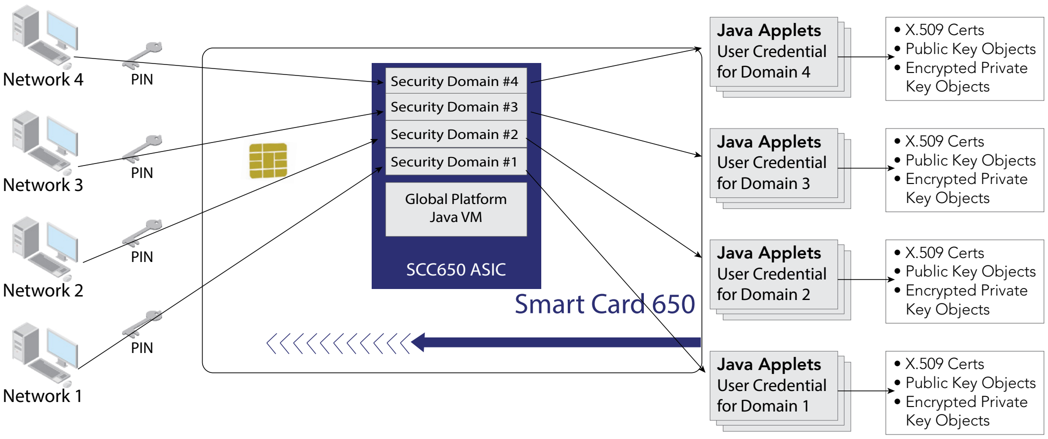
The Thales Trusted Cyber Technologies (TCT) Smart Card 650 (SC650) is the most secure, certificate-based smart card available today. Supporting numerous algorithms, X.509 digital certificates, the SC650 enables strong two-factor authentication and proof-positive user identification in all Public Key Infrastructure (PKI) environments. The smart card contains a custom smart card ASIC, the SCC650, developed by Thales TCT. This SCC650 ASIC is a highly trusted design fabricated at a trusted foundry and implements a security architecture found in other Thales TCT certified ASICs.

The SC650 operating system supports the Java card platform specification v2.2.2 and Global platform card specification version 2.1.1. This operating system incorporates Thales TCT's well-established High Assurance Suite B cryptographic eXtension (cGX) library to perform all cryptographic operations necessary for the smart card. Together, the hardware and firmware provide the user with features to facilitate and manage combined logical and physical access, while also enabling services to off-load cryptographic algorithm implementation and provide object access control.

On-board cryptographic processing including Suite B Operations

The SC650 securely stores the user's credentials, such as digitally-signed certificates, private keys, and network login credentials and seamlessly supports secure key generation, secure key storage, encryption/ decryption, and digital signature processing (sign and verify). The SC650 is capable of performing all private and public key cryptographic functions directly on the smart card, thus eliminating potential threats resulting from private key exposure. In authentication scenarios where cryptographic keys are stored locally on a computer and protected only by software, the keys are vulnerable to accidental loss and malicious acts that could greatly compromise network security and result in unfortunate economic consequences.

Additionally, the on-chip cryptographic functions enable users to perform Suite B and other FIPS- approved cryptographic operations on the card. This allows the user to carry out ECDSA, RSA (PKCS #1), or DSS (FIPS 186) digital signatures with confidence because the signing key cannot be tampered with by any software that could be running on the host computer. Similarly, security for the exchange of session encryption keys is supported by the on-board cryptographic functions, such as ECDH key agreement and key exchange.



Multi-domain Support

The SC650, combined with the Thales TCT High Assurance Client (SHAC) middleware, is designed to support multi-domain usage by allowing the user's credentials and certificates to be stored in cryptographically-separated key containers. This capability grants users more flexible and simplified access to sensitive networks and workstations because a user can use a single authentication device, the SC650, to securely authenticate to multiple independent networks (i.e., domains), each requiring its own set of unique private keys, credentials and certificates. The combination of the SC650 and SHAC middleware enables secure separation of all keys and certificates per network so appropriate access levels and network policies are enforced for each.

Easy to Integrate and Deploy

The Thales TCT SC650 has been designed to provide built-in cryptographic and data container management for all private and sensitive functions, while giving enterprises the ability to add new applications/applets to address future requirements. The SC650 may be used with Thales TCT-developed applets and middleware (SHAC). Custom application integration is facilitated by the cryptographic API support provided by the SHAC middleware and includes PKCS #11, Microsoft CAPI, and Microsoft and Apple PC/SC. The SC650 also accepts thirdparty applets to allow integration of the smart card into existing enterprise infrastructures. In addition, the SC650 interoperates with RedHat CMS 8.0 Secure channel protocol.

Benefits

- High assurance user authentication
- Multi-domain authentication support
- Secure key storage
- Signing and verifying encryption/decryption
- Private/public key generation
- Secure random number generation
- Interoperates with RedHat CMS 8.0 Secure

Technical Specifications

Cryptographic Algorithms:

- DH/ECDH/DSA/ECDSA/RSA Key Generation
- DH/ECDH Key Agreement
- ECDSA/DSA Sign & Verify
- ECC curves supported: p-256, p-384, p-521
- 3DES encryption/decryption
- AES encryption/decryption (128 and 256 key lengths)
- RSA encrypt/decrypt (1024/2048)
- RSA Sign & Verify (1024/2048)
- SHA1/256/384/512
- HMAc SHA1/256/384/512

Interface:

- ISO 7816-2 for dimensions and location of the contact for smart cards
- ISO/IEC7816 parts 3 and 4, standard for identification cards (i.e., smart cards)

Token Operating System:

- Java card v2.2.2
- Global platform 2.1.1

Host Interface

- PCI-Express X4, PCI CEM 1.0a

Reliability

- Less than 1% Failure Rate

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com