thalestct.com

THALES

sKey3250

High assurance USB authenticator that combines the capabilities of a traditional smart card and smart card reader in one easy-to-deploy device

Thales Trusted Cyber Technologies (TCT) sKey3250 is a high assurance certificate-based USB authenticator. Supporting numerous algorithms and X.509 digital certificates, the sKey3250 enables strong two-factor authentication and proof-positive user identification in all Public Key Infrastructure (PKI) environments.

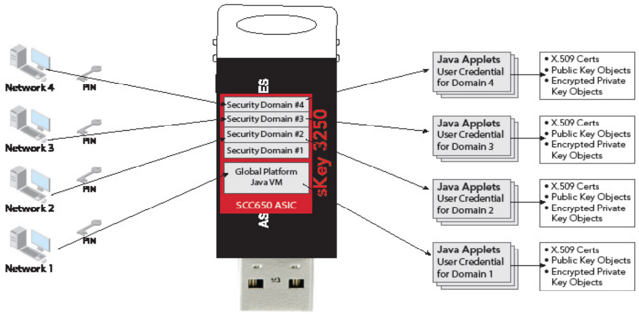
sKey3250 contains a custom smart card ASIC, the SCC650, developed on-shore by Thales TCT This SCC650 ASIC designed to the highest security principles, implements a security architecture found in other Thales TCT certified ASICs, and is fabricated at a Trusted Foundry.

sKey3250's operating system supports the Java Card platform specification v2.2.2 and GlobalPlatform 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

sKey3250 securely stores the user's credentials, such as digitally-signed certificates, private keys, and network login credentials while also seamlessly supporting secure key generation, secure key storage, encryption/decryption, and digital signature processing (sign and verify). sKey3250 is capable of performing all private and public key cryptographic functions directly on the token, 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 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

sKey3250, 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 logically separated containers when using 3rd party applets, and cryptographically-separated key containers when using the Thales TCT applets. This capability grants users more flexible and simplified access to sensitive networks and workstations because a user can use a single authentication device, sKey3250, 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 sKey3250 and SHAC middleware enables secure separation of all keys and certificates per network so appropriate access levels and network policies are enforced.

Easy to Integrate and Deploy

sKey3250 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. sKey3250 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 sKey3250 also accepts third-party applets to allow integration of the token into existing enterprise infrastructures. In addition, sKey3250 interoperates with management systems including RedHat Certificate System, Intercede MyID and Entrust Security Manager.

Benefits

- High assurance user authentication
- Multi-domain authentication support
- Device used for authentication only -- not subject to USB flash drive policy restrictions
- Secure key storage
- Signing and verifying encryption/decryption
- Private/public key generation
- Secure random number generation
- Management System Interoperability:
  - RedHat Certificate System
  - Intercede MyID
  - Entrust Security Manager

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:

- USB type A; supports USB 1.1 and 2.0
- ISO/IEC7816 parts 3 and 4, standard for identification cards

Token Operating System:

- Java Card v2.2.2
- GlobalPlatform 2.1.1

Certifications

- FIPS 140-2 validation pending

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