Trust SEC

SLCOS WHITE PAPER

CONTACT

P : +48784784 504
E : Info@TrustSec.net
www.TrustSec.net

ADDRESS

Address ul. Cyfrowa 6, 71-441 Szczecin,
Poland

linkedin.com/company/TrustSec

facebook.com/TrustSec

SLCOS

TrustSEC

About SLCOS

SLCOS sets the latest technology in smartcard operating system and secure device technology, offering an open platform that combines the best in security, flexibility Native/Java compliance and ease to use. SLCOS support contact/contactless/dual/USB interfaces. SLCOS allow preloaded or programmed with fixed applications or allow post applications upload using Card Manager Module. allow secure application upload before or after issuing. It specifies protocol with different level of security.

It supports single or multiple application vendors. SLCOS provide onboard fingerprint matching and offer it to application developers. SLCOS comply with Global Platform version 2.2.1 specifications.

SLCOS provides the following operations:

1. Manages the smart chip hardware and perform chip initialization and configuration while startup.
2. Manages single or multiple applications. Application management includes, secure download, loading, installation, selection, communication and deletion.
3. Optionally allows multiple vendors per card using multiple security domains.
4. Optionally allows On-card Java Bytecode Verification in order to defend against malicious or buggy applets not to reveal or steal sensitive data of other applets.
5. Secure application execution in multi-applications environment using firewalls.
6. Executes high level applications (i.e. Java) through internal virtual machine.
7. Provides software level implementation for cryptographic operations like RSA, ECC, DSA, DES, 3DES, AES, SHA, PRNG and DH.
8. Provides software level implementation of communication protocols like T0, T1, TCL type A.
9. Provides system level interface for different hardware modules like communication, security, storage, memory, transaction, timers and random number generator.
10. Configuration APDUs which allow application developers to configure, enable or disable many options related to the operating system.

Compliant with Standards

- ISO 7816
- ISO 14443 type A
- Global Platform Specifications 2.2.1 Amendment D, E, and supporting ID-Configuration.
- Java Card Specifications 3.0.4 with backward compatibility.
- Java Card Specifications 3.0.5 for Bio APIs.

Supporting Compliant Hardware

This system had been developed over a microprocessor (NXP SmartMX2 P60 and Infineon SLE78) that is compliant with standards and certified from known labs. Following standards are supported:

NXP SmartMX2 P60	Infineon SLE78
• FIPS 140-2 • ISO/IEC 7816 • ISO/IEC 14443 A/B • ISO/IEC 18092 Passive Mode • EMVCo Certified. • MMU memory management Unit • True Number Generator (Compliant to AIS-31) • CC EAL6+ • Crypto Library 3.1 is with CC EAL 6+ assurance level. • Enhanced Security sensors. • Electronic fuses for safeguarded mode control • Active and dynamic shielding. • Unique ID for each die. • Memory security (ROM – EEPROM- RAM). • Two Copy Machine offering fast data transfer. • Crypto Processor	• FIPS 140-2 • ISO/IEC 7816 • ISO/IEC 14443 A/B • ISO/IEC 18092 Passive Mode • EMVCo Certified. • MMU memory management Unit • True Number Generator (Compliant to AIS-31) • CC EAL6+ high (Infineon chip) • Crypto Library is with CC EAL 6+ high assurance level. • SOLID FLASH™ NVM • Peripheral Event Channel Controller • USB (Universal Serial Bus) interface • Symmetric Crypto Processor (SCP) including SPA/DPA and DFA countermeasures for triple-DES according to the DES standard (FIPS 46-3) and AES-compliant operations (FIPS 197) • An arithmetic coprocessor, the Crypto@2304T, for fast calculation of public key crypto algorithms, such as RSA or elliptic curve calculations, GF(p) and GF(2n) • Hash module supporting SHA-1/SHA-256/MD-5 • High-security Self-Test Software (STS) • Integrated Hardware Protection • Unique chip identification number for each chip • Security-optimized layout (secure wiring) • Access rights (privilege level concept and MMU functions) • Encryption of ROM, RAM and NVM contents supporting different keys • Encryption of buses for particular peripherals: SCP, Crypto@2304T, HASH, CRC and RNG modules • Temperature sensor • Voltage sensors • Frequency sensor • Implicit intelligent (I2) shield • Light-sensitive elements

Flexible Application Development

The application providers can develop their applications by developing non-native applications using Java Card APIs version 3.0.4 (also compatible with older versions) in contrast to developing natively (i.e. C or Assembly applications).

Flexible Communication supports

- The basic communication protocol, ISO 7816 T0, and alternative communication protocols, namely, ISO 7816 T1 and ISO 14443 Type A&B Contactless.
- USB (Universal Serial Bus) interface
- Extended APDUs.
- Secure messaging Via Global Platform Security Protocols (SCP02 & SCP03)

Multiple Delivery Types

- Wafer Sawn
- Contact Card
- Contactless Card
- Dual (contact and contactless) Card
- USB Stick
- Dual (USB and contactless) Card

Support Configurable Modules

- The Smart Card Operating System consists of a set of configurations for the overall system. This allows simple removal/addition/update of certain features in some modules due to business requirements or for simplicity.
- The removal/addition/update of features of the following modules is done by switching off certain values for each one:
    1. Security module
    2. Communication module
    3. JCVM module
    4. GP Module

Design Features

The operating system is designed to support several microprocessor architectures, namely, **NXP SmartMX2 P60** microprocessor and **Infineon SLE 78 /SLE 77 / SLC52**

Following points are considered:

1. The system accesses the microprocessor resources through hardware abstraction layer (HAL) to minimize the porting process to different microprocessor architectures.

2. Non-Native applications are written in high-level language, i.e. "Java Card", to be independent on the operating system itself and this leads to applications that are completely independent on the hardware.

3. Other operating system layers and native system applications are programmed using machined independent code like "C".

4. Only (HAL) layer can be programmed using machine dependent code (assembly).

SLCOS Architecture

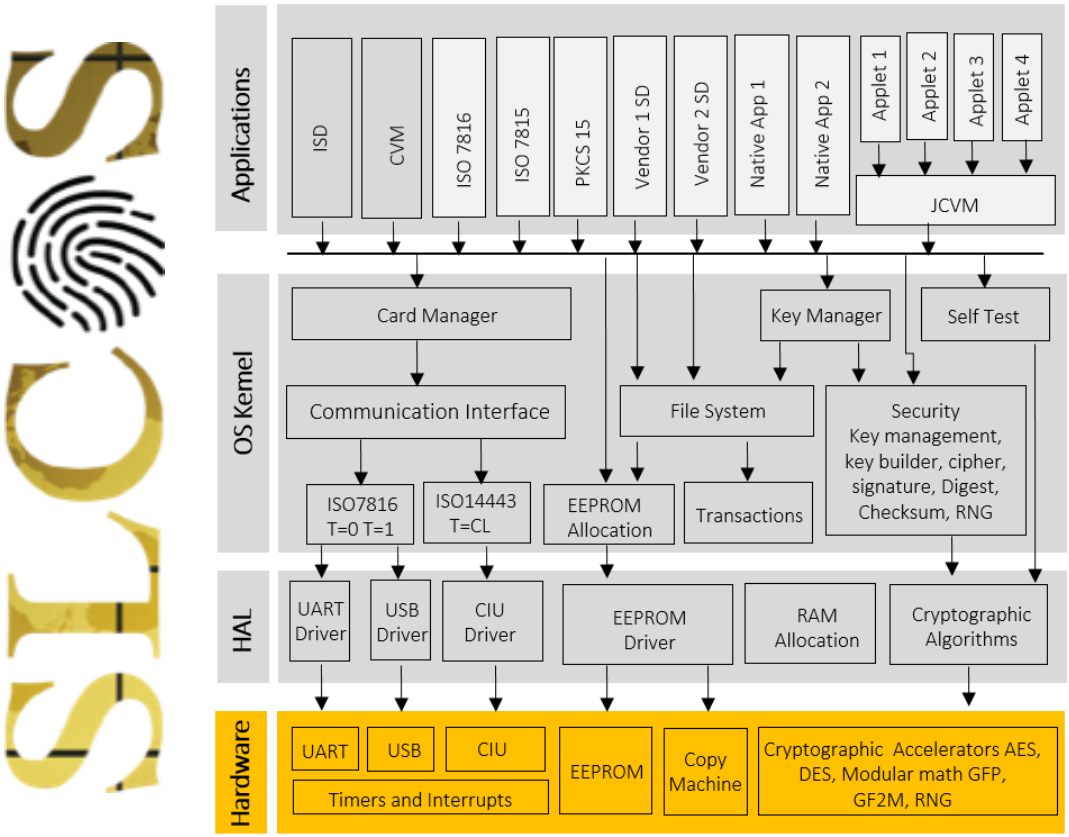

Figure 1: SLCOS Internal Architecture

SLCOS
Security Features

SECURITY FEATURES

1. **Hash**
   SHA1, SHA224, SHA256, SHA384, SHA512*

2. **Symmetric Key**
   AES (128-192-256), DES, TDES (dual key - triple key), Korean Seed*

3. **Public Key**
   RSA (up to 4,096 bits), EC over GF(p) (up to 521 bits), EC over F2M (up to 521 bits) (Infineon Only), DSA (Infineon only) (2,048 bits), EC Point Addition

4. **Key Generation**
   RSA, EC over GF(p), EC over F2M (Infineon Only), DSA (Infineon only)

5. **Random Data**
   TRNG, PRNG (SP 800-90 compliant PRNG based on AES) *

6. **Checksum**
   CRC16 (compliant with ISO/IEC 3309 16 bit CRC algorithm), CRC32 (compliant with ISO/IEC 3309 32 bit CRC algorithm)

7. **Message Authentication**
   CMAC, HMAC

8. **Key Agreement**
   ECDH

*Note: Algorithms written in Yellow are Software Implemented

TrustSEC

- Multi-application (Java) with JCRE Firewall protection.
- Protects the private data like keys and private objects against:

Offline NVM (non-volatile memory) attack: in this attack, if the attacker succeeded to penetrate the hardware security and read the EEPROM contents, he can extract the private data.

Online application-application attack: in this attack, the application can use low-level language to access the private data of other application. This attack is popular in native applications and if the hardware does not protect memory access.

Online application attack: in this attack, the application can use low-level language to access the private data from inside the operating system. This attack is popular in native applications and if the hardware does not protect memory access.

- Secure against Smart Card Attacks: protects the operating system against known Smart Card attacks like Physical Attacks, Simple Power Analysis attacks (SPA), differential fault analysis (DFA), Timing Attack, Differential Power Analysis attacks (DPA).
- On-card Java Bytecode Verification in order to defend against malicious or buggy applets not to reveal or steal sensitive data of other applets on the card.

Additional Features

- ✓ Supporting **Extended APDUs** up to a **configurable** number of bytes.
- ✓ Supporting **Garbage Collection** of unused or unreferenced objects.
- ✓ Supporting **compaction** (Defragmentation) of non-volatile memory in case of memory space shortage.
- ✓ **Automatic wait time extension** which facilitates the development of applets as the applet will not need to extend the reader's waiting time in case of processing delay.

TrustSEC

Short-term Roadmap

TrustSec believes that it should keep abreast of the latest technologies in the field of smart cards, it was mandatory for TrustSec to provide innovative solutions for the new global trend, which is a biometric smart card.

In order to achieve such goal, TrustSec has made a lot of effort including workshops, brainstorming sessions, and set agreements with most leading biometric sensor manufacture (NextBiometrics, Fingerprints, and IDEX), this was achieved through direct agreement or via partners like CardLab.

During the Journey, TrustSec used ID3 match on card module which Proves high efficiency.

Our vision is to have a Bio PKI Smart Card which results in a trusted credential for authenticating an individual's identity using one-to-one biometric verification. With the biometric template stored on the smart card, in which comparison can be made locally, without the need for connection to a database of biometric identifiers.

Choosing PKI as our recommended segment to start with was based on our long experience in PKI which is almost 25 years, but also at the same time, TrustSec worked side by side in cooperation with CardLab on the innovative Bio OTP card which will serve mainly the banking sector.

As a parallel step now our technical teams are evaluating the new chips launched by most powerful chip manufacturers Infineon and NXP to start porting TrustSec Smartcard OS SLCOS to them, After having a very good experience working with NXP P60 and Infineon SLE78, **SLE 77 / SLC52**

.

About TrustSec

TrustSec is a polish company founded by internationally recognized information security and cryptography experts. Launched in 2016, the company aims to fill the gap in the cybersecurity market, Securing data assets, and digital identity against unauthorized access, cyber-attacks, hacking, through its state of the art and innovative products and solutions.

Partnerships

TrustSec made partnerships with other booming technology leaders in the field of communication and information security to provide integrated highly secure solutions.

TrustSec

CONTACT

P : +48784784 504
E : info@TrustSec.net
www.TrustSec.net

ADDRESS

Address ul. Cyfrowa 6, 71-441 Szczecin, Poland