securosys

Auditability, confidentiality, and secure automation

IMUNES Trusted Execution Environment

- Secure execution of confidential code over confidential data
- Strong isolation of execution containers and instances
- Tamper-proof hardware platform validated to FIPS140-2 Level 3
- Input-output consistency guaranteed and verified with HSM-based hardware
- Highest availability due to cluster self-synchronization
- Integration with gRPC API and Java/C++ clients
- 2-factor authentication for Primus HSM E-Series and X-Series

Securosys IMUNES is a confidential computing platform that provides a Trusted Execution Environment (TEE). It allows users to securely run code (guaranteed unaltered) on a tamper-protected hardware platform. It can be deployed as a single unit or as cluster of multiple TEEs to facilitate numerous use-cases with focus on secure scalability, automation, trust, and confidentiality.

Automated decision making

IMUNES guarantees that only the securely loaded executable - free from tampering or malware - is executed. The executable receives signed input and returns signed output. This makes the TEE ideal for transactional programs such as automating programmable decisions in a trusted, scalable manner.

Traceability and auditability

There are multiple ways through which an external integration point can verify the consistency of operations performed by the TEE, namely:

- An internal secure counter keeps track of how many times the code has been executed
- Input and output signatures can ensure consistency of execution order
- Executions can be marked with a tamper-proof timestamp key
- The TEE provides both static and dynamic root-of-trust measurements. The complete trusted computing base of each TEE is attested with a Merkle tree

Execute Confidential Code

The executable can be encrypted with TEE's own encryption key and protected by the FIPS2-L3 certified secure enclave, providing maximum intellectual property protection.

Confidential Computing

Data inputs for the executable can be encrypted specifically for the TEE, providing maximum guarantee against the leakage of highly sensitive data.

Security Features

Security architecture

- Multilevel enterprise-grade security architecture
- Multi-barrier software and hardware architecture with supervision mechanisms
- Cryptography with protection to timing- and cache-based side-channel attacks

Runtime isolation

- Strict isolation of executable instances
- Minimum set of services subscription model

Entropy generation

- Two hardware-based true random number generators (TRNG)
- NIST SP800-90 compatible random number generator

Anti-tamper mechanisms

- Several sensors to detect unauthorized access
- Active destruction of sensitive data on tamper
- Tamper protection by digital seal during transport and (multi-year) storage

Identity-based authentication

- Multiple security officers (2 out of m)

Firmware

- Local firmware update on device or optionally via Decanus Remote Terminal

Secure Code Loading

- Local secure code loading on device or optionally via Decanus Remote Terminal

Networking and Integration

Software integration

- Java/C++ client or via custom gRPC API provider

Network Management

- IPv4/IPv6
- Monitoring and logging (SNMPv2, syslog)

Device Management

- Local configuration, remote out-of-band configuration (Decanus)
- Integrated logging
- Firmware update
- Enhanced diagnostic functions

Technical Data

Performance classes

Performance class	K2/KD2	K4/KD4	K16/KD16
Partitions (storage of executables)	1	2	4
Instances (parallel executable runtimes)	2	4	16

System architecture

- ARM-based chipset
- Cryptographic functions executed on FPGA
- 128MB of internal storage per partition
- Secure boot from ROM
- Microkernel-based operating system

VM options

- Java 9 with the following modules: java.base, java.logging, java.crypto.ec and the following native libraries: libmanagement.so, libsunec.so
- WebAssembly

Power

- Two redundant power supplies, hot pluggable (KD series)
- Built in power supply: 100 … 240 V AC, 50 … 60 Hz
- Power dissipation: 30 W (typ.), 50 W (max.)
- Backup lithium battery: Lithium Thionyl Chloride 0.65g Li, IEC 60086-4, UL 1642, 3.6V

Interfaces

- 4 Ethernet RJ-45 ports with1 Gbit/s (rear)
- 1 RS-232 management port (rear)
- 1 USB management port (rear)

Controls

- 4 LEDs for system and interface status (multicolored)
- Console interface
- Optional Decanus Terminal

Environmental test specifications (target)

- EMV/EMC: EN 55022, EN 55024, FCC Part 15 Class B
- Safety: IEC 62386-1

Specifications

- Temperature ranges (IEC 60068-2-1 Ad, IEC 60068-2-2 Bd): storage -25 … +70 °C; operation 0 … +40 °C , recommended 1 … 30 °C
- Humidity (IEC 60068-2-78 Cab): 40 °C, 93% RH, non-condensing
- Dimensions 417 x 44 x 365 mm (1U 19'' EIA standard rack)
- Weight 5,8 kg

HEADQUARTER
Securosys SA
Max-Högger-Strasse 2
8048 Zürich
SCHWEIZ
+41 44 552 31 00
info@securosys.com
www.securosys.com

GERMANY & EU
Securosys
Deutschland GmbH
Darrestrasse 9
87600 Kaufbeuren
DEUTSCHLAND
+49 8341 438620
info@securosys.de
www.securosys.de

APAC
Securosys
Hong Kong Ltd.
Unit 704B Sunbeam Centre
27 Shing Yip Street
Kwun Tong
Hong Kong
+852 8193 1646
info-apac@securosys.com
www.securosys.com

We strive to continuously improve our offerings and therefore reserve the right to change specifications without notice.
Designed and manufactured inSwitzerland.