securosys

Internal Training

Imunes Trusted Execution Environment

Content

- Introduction to Imunes TEE
- Security Architecture
- Setup and Operation
- App Development and Deployment
- Use Cases
- Resources

01/ Introduction to Imunes TEE

IMUNES Trusted Execution Environment Functionality

- Secure code execution
- 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
- IMUNES guarantees that only the securely loaded executable - free from tampering or malware - is executed. The executable receives signed input and returns signed output.

Hardware and Accessories

- The contents of the package contains the following:
  - The Imunes TEE hardware with intact hardware seal;
  - a quick-start guide;
  - 1 power cable; and
  - 1 USB memory stick.

02 / Security Architecture

Roles and Access Control

- Genesis
  - Setting up the Imunes TEE requires an initial **activation code** for the virtual “Genesis” smartcard and installation of the appropriate **license**
  - The Genesis Role is tied to a specific Imunes TEE. It prevents that anyone but the legitimate owner may set up the device.
  - The Genesis Role is received on a different delivery than the Imunes TEE. If for some reason the Imunes TEE has been replaced during delivery, the Genesis Role would not match with the Imunes TEE anymore.
- Security Officer
  - The SO Role provides access to high-privileged security functions
  - The SO role is usually split over several employees, each of which are holding SO credentials for identification

Roles and Access Control

- User
  - A User corresponds to an account with its own cryptographic storage (partition) on the Imunes TEE.
  - Each user is only able to access his own executable and the partition attestation key.
  - The number of users supported by the TEE depends on the specific model and its license options.
  - A user is created by the SOs in direct physical interaction with the Imunes TEE.
  - The User then may access the Imunes TEE through the network using his username and the matching user secret.

Clustering

- An Imunes TEE can be deployed as a single unit or as cluster of multiple TEEs
- If set up in high-availability (HA) mode, the TEEs are clustered as Master and Clones while keeping themselves automatically synchronized
- If properly set up, maintenance in an HA cluster will not be noticed by the user clients
  - Before starting a maintenance task on a specific device, the client connections need to be faded out by refusing new connections

03 / Setup and Operation

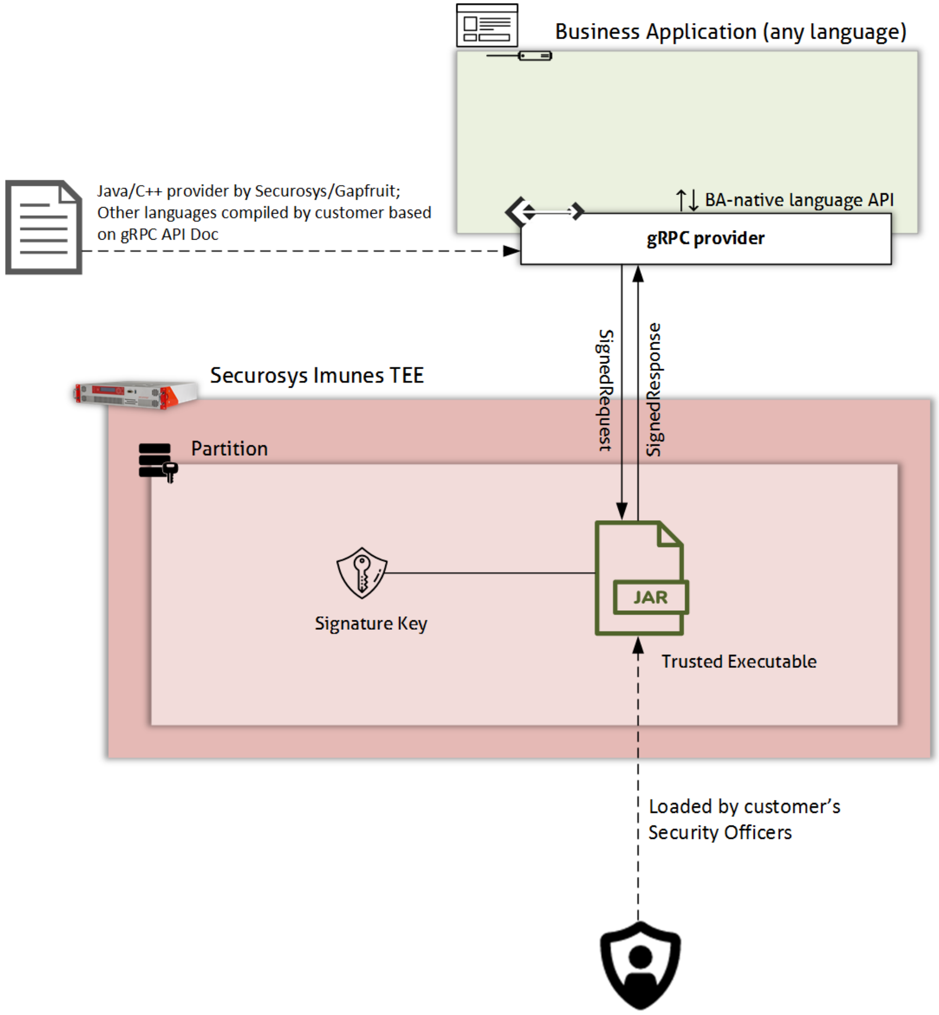
Initial Setup

- Power-up the device and wait for the blue moving light to settle into four steady blue lights
  - This indicates completion of the power-up sequence and self-tests
- Connect a PC to the TEE’s serial port. In your terminal application (like PuTTY or iTerm), set the connection parameters to speed 115'200 bps, 8 data bits, no parity bit, 1 stop bit.
- After connecting press <enter>. When you see the “Login password” prompt, type in the default password “`ABCD`”.
- To launch the initial wizard, enter `tee_intial_wizard`
  - The wizard will lead through several initial configuration settings

- Details are described in the Imunes TEE User Manual (TEE_UserGuide-v3.2_UG_E01.pdf)

Operation

- The Imunes TEE can execute Java applications, which must follow a pre-defined format and be loaded to the TEE by a Security Officer.
- The Business Application (BA) communicates with the TEE using the gRPC API.
- The API then communicates with the Java application itself using stdin and stdout.


Business Application (any language)
Java/C++ provider by Securosys/Gapfruit;
Other languages compiled by customer based on gRPC API Doc
BA-native language API
gRPC provider
SignedRequest
SignedResponse
Securosys Imunes TEE
Partition
Signature Key
JAR
Trusted Executable
Loaded by customer's Security Officers

04/ App Development and Deployment

Java

- The JAR must be compiled for Java version 9
- It must be named **app.jar** and put in a tar archive
- Put any other files that should be accessed from the code to the same tar archive
- TEE's internal JVM does only contain the following modules and native libraries:
  - java.base, java.logging, java.crypto.ec, java.xml, java.xml.crypto
  - libmanagement.so, libsunec.so

WASM

- Alternatively, the executable to be loaded might be generated using the customer’s favorite programming language and a WASM compiler
- To build the WASM binary from C source code, for example, proceed as follows:
  - Install the C-to-WASM compiler, for instance https://github.com/wasienv/wasienv
  - Compile your C code: $ wasicc app.c -o app.wasm
  - The application may also be compiled without installing a C-to-WASM compiler using the docker image at https://github.com/wasienv/wasienv/tree/master/docker:
    - $ docker run --rm -v `pwd`:`pwd` wasienv/wasienv wasic++ `pwd`/app.c -o `pwd`/app.was
- Like the Java application, the WASM application `**app.wasm**` has to be wrapped into a tar file

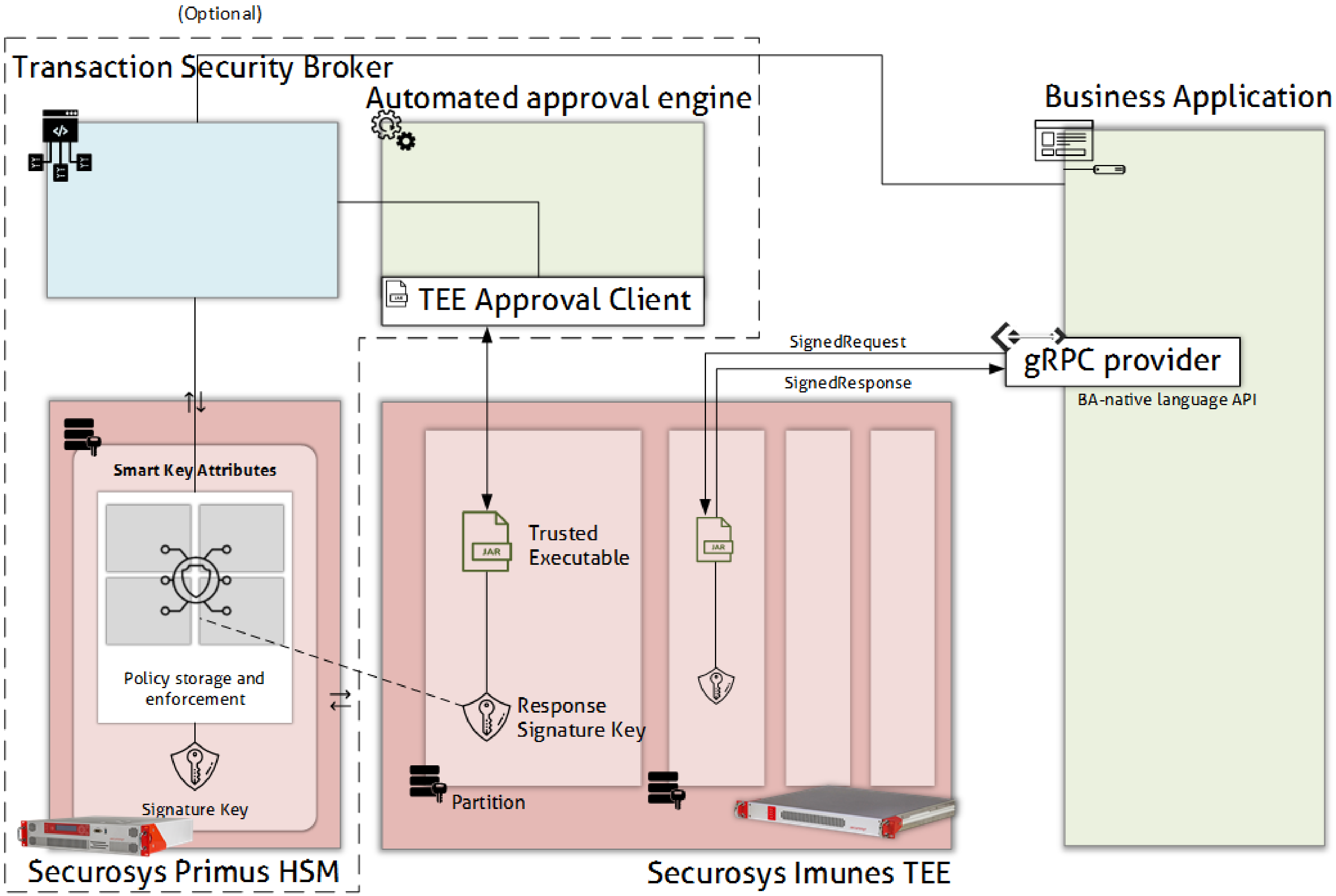
Deployment

- Log in to the Imunes TEE
- Activate the Security Officer role
  - Type the command `so` in the console
  - Enter usernames and PINs of two security officers
- Type the command `iexe` in the console
- Put the single FAT32 partition formatted USB drive with your executable into the USB port
- Confirm

05 / Use Cases

Automated Approvals

- **Automated decision making and approvals, including**
  - AML
  - Checking and updating of whitelist of recipients
  - determine the value of a crypto transaction and deciding on approval level



Other Use Cases

- To protect sensitive or highly regulated data, even while in use - and extend cloud computing benefits to sensitive workloads
- To eliminate concerns when choosing cloud providers
- To protect intellectual property
- To collaborate securely with partners on new cloud solutions
- To protect data processed at the edge

06/ Resources

Imunes TEE

Product Variants

	IMUNES K2	IMUNES K4	IMUNES K16
User partition	1	2	4
Concurrent execution images	2	2 x 2	4 x 4
Code Storage	240 MB	480 MB	960 MB

Firmware Versions, Dev Environment and Documentation

- Current firmware versions:
  - V 3.2.1 (released)
  - V 3.3.1 (experimental)
    - Includes possibility to load executable via client
- Dev environments: Developer account set up and maintained by R&D
  - geneva.securosys.ch, V 3.2.1 (released)
  - zurich.securosys.ch, V 3.3.1 (experimental)
- Docs:
  - Imunes TEE User Manual (TEE_UserGuide-v3.2_UG_E01.pdf)
  - Imunes TEE Developer's Documentation (ImunesTEE_DevDoc-v3.3-E1_DRAFT.pdf)

Thank you

for your attention.

securosys