mle
missing link electronics

Open Portable Trusted Execution Environment

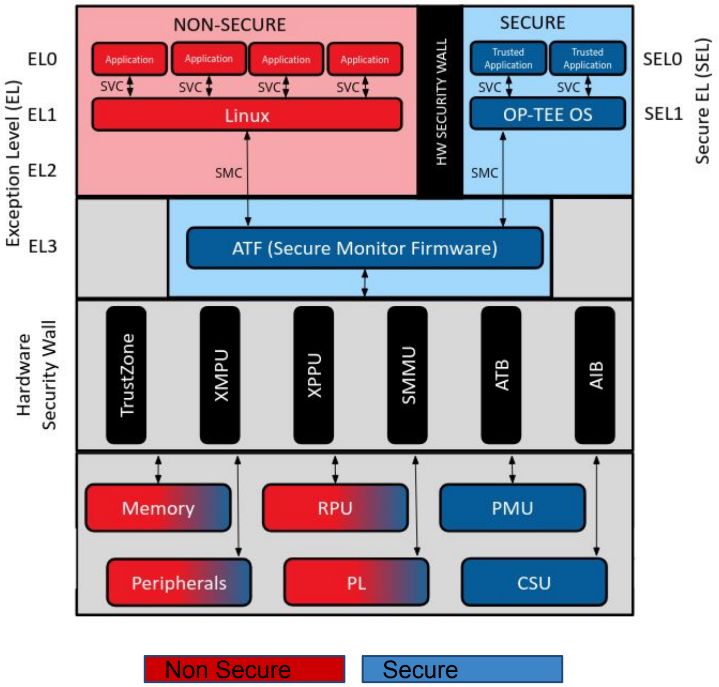
XILINX
ALLIANCE PROGRAM PREMIER

Security in Zynq Ultrascale+ is important when it comes to protecting sensitive data or functionality. OP-TEE helps to protect and secure configuration, keys, communication and functionality for a wide variety of applications: for example secure data storage, secure communication, protection of functional safe designs or simply adding another wall between sensitive data and a potential adversary.

Application Use Cases

- Secure data storage
- Secure communication
- Support for Update Over the Air
- Protect functional safety related designs
- Secure Touch inputs
- Secure key handling

Functionality supported:	Linaro OP-TEE	MLE OP-TEE
OP-TEE Basic functionality	✓	✓
Trusted Applications with your own secure application	✓	✓
Secure Paging (Hashed DDR Memory)	-	✓
Testsuite (10k+ Test Cases for selftest)	✓	✓ **(extended)**
AES-GCM (Xilinx CSU hardware accelerated)	-	✓
RSA (Xilinx CSU hardware accelerated)	-	✓
SHA3 (Xilinx CSU hardware accelerated)	-	✓
Secure Key handling with Physical Unclonable Function (PUF)	-	✓
Support for eFuse burning	-	✓
Secure/Nonsecure Bitstream Loading	-	✓
Performance Measurement of context switch or Trusted Application	-	✓
Custom Secure PL Functions	-	✓



License and Availability

- Source code with Yocto build recipes
- Pre build Demo available
- NRE or royalty-based License

Contact MLE

MLE US:
+1 (408) 475-1490 San Jose, US

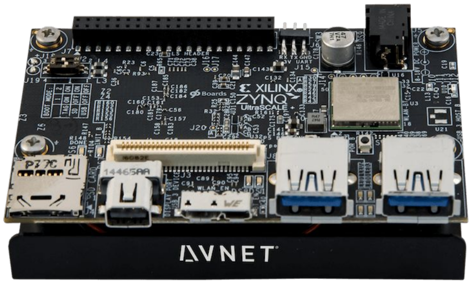
MLE Europe:
+49 (731) 141149-0 Neu-Ulm, GER

Open Portable Trusted Execution Environment

Evaluation for Zynq Ultrascale+

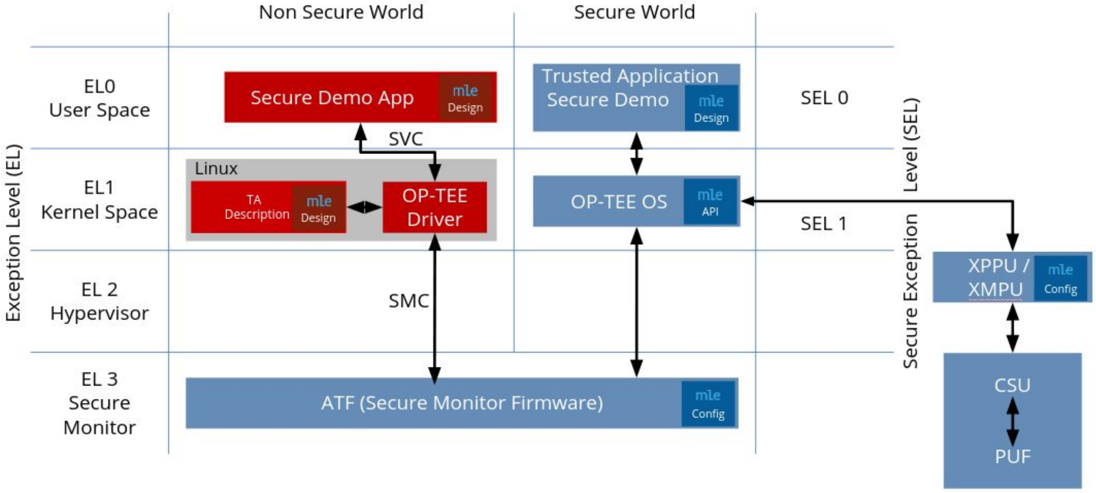
available for following platforms:

- ZCU102 (ZU9EG)
- Ultra96 V2 (ZU3EG)



Why OP-TEE?

OP-TEE is a small secure open source operating system which, after authentication and decryption, gets loaded in an secured area in the memory. A RichOS (for example Xilinx Petalinux) driver can request via a Secure Monitor Call for the execution of a trusted application. As OP-Tee sits in on chip memory / tightly coupled memory (OCM /TCM) which is additionally protected by Xilinx Memory Protection Units (XMPU) it is very hard to penetrate this HW wall to inject any malware or get access to sensitive data. Missing Link Electronics took the effort to port OP-TEE to Xilinx Zynq Ultrascale+ MPSoC Platform. Additionally the typical software implemented features like AES, RSA, SHA3 are replaced or extended by the Hardware Features of the Zynq Ultrascale+ MPSoC. Additionally other hardware features are also supported like: Secure/Nonsecure bitstream loading and burning eFuses for enabling functions or storing data in user eFuses.



Missing Link Electronics

We are a Silicon Valley based technology company with offices in Germany. We are partner of leading electronic device and solution providers and have been enabling key innovators in the automotive, industrial, test & measurement markets to build better Embedded Systems, faster.

Our mission is to develop and market technology solutions for Systems Realization via pre-validated IP and expert application support, and to combine off-the-shelf FPGA devices with Open-Source Software for dependable, configurable development platforms.

Our expertise is I/O connectivity and acceleration of data communication protocols and the integration and optimization of Open Source Linux software stacks on modern extensible processing architectures.