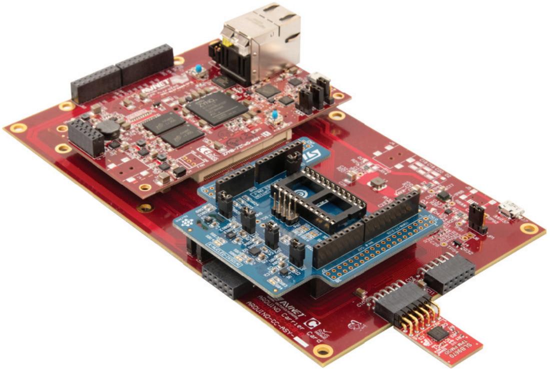
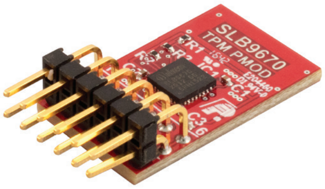
Trusted Platform Module Security for the Zynq®-7000 All Programmable SoC

The Trusted Platform Module (TPM) Security Peripheral Module (Pmod) for Zynq®-7000 All Programmable SoCs enables a root of trust for platform integrity, remote attestation, and cryptographic services as required by Industrial Internet of Things (IIoT) Applications. The TPM Pmod features Infineon's OPTIGA™ TPM SLB9670 which is compliant to the Trusted Computing Group (TCG) TPM 1.2 specification and connects to Zynq via a SPI interface. This Pmod, along with the downloadable reference design, enables measured boot functionality for the Avnet MicroZed Industrial IoT Starter Kit, featuring the Xilinx Zynq 7Z010 running WindRiver's PulsarTM Linux operating system. The system also supports additional use cases such as Device Identity, Secure Storage, Secure Communications, and Secure Firmware Upgrade. When these capabilities are coupled with Zynq's secure boot (hardware root of trust) feature, developers have the security foundation required for the Industrial Internet of Things.





FEATURES

Cost-effective, production ready TPM Pmod

- Includes Infineon OPTIGA™ TPM SLB9670 1.2
- Enhanced SPI interface to Zynq SoC
- Small 1" x 0.6" plug-in Pmod module (2x6 format)

Downloadable reference design and tutorial includes

- Zynq/Client side
    - WindRiver Pulsar 8 Linux binary image
    - Kernel built with Infineon TPM SPI Driver
    - TrouSerS Trusted Software Stack
    - strongSwan client

PC/Server side (requires Ubuntu Linux OS)

- strongSwan server

Application code examples for

- Measured boot
- Remote attestation

When paired with MicroZed Industrial IoT Starter Kit

- Cloud enabled
    - Watson IoT ready
    - Supports IBM® Bluemix™ applications & services
- Scalable Xilinx Zynq-7000 series edge compute platform
    - Dual ARM® Cortex™-A9
    - FPGA Logic
    - R3 Arduino-compatible shield expansion slot
    - Additional 2x6 Pmod expansion slot
    - User header providing access to SPI, I2C, UART, and GPIO

To purchase this TPM module or the MicroZed IIoT Starter Kit, visit www.microzed.org

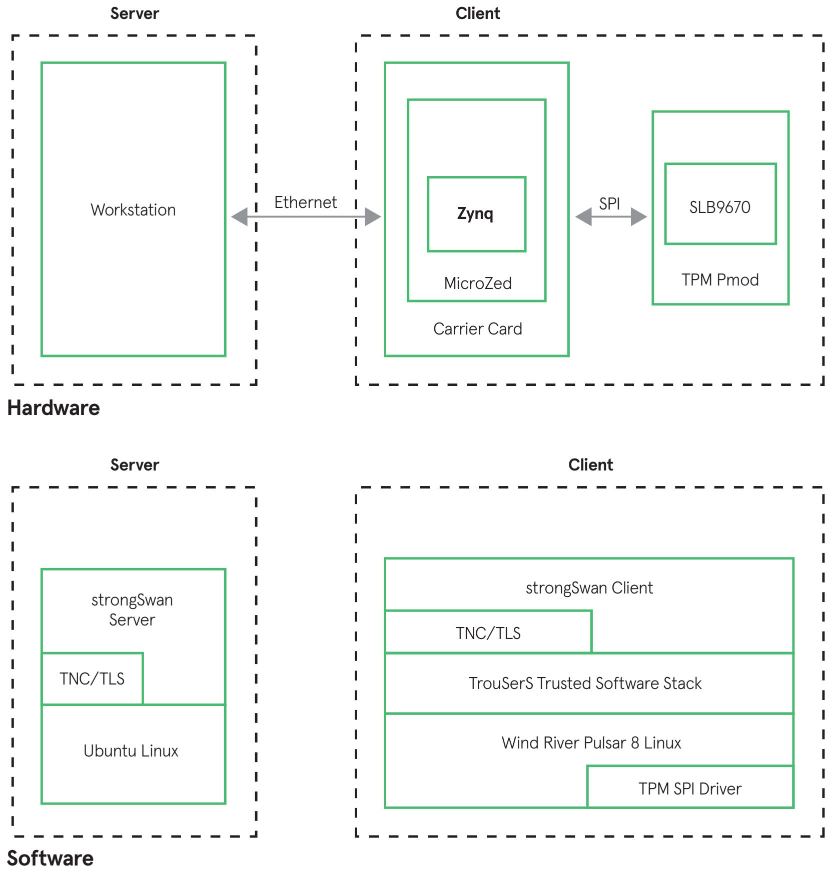
WHAT'S REQUIRED

- MicroZed IIoT Starter Kit
- Infineon TPM Peripheral Module
- Downloadable Reference Design and Tutorial

TARGET APPLICATIONS

- Any Industrial Internet of Things Application
- Factory Automation
- Smart Grid
- Healthcare
- Surveillance
- Transportation
- Smart Cities

BLOCK DIAGRAM



Hardware

Software

Functionality
Secure Boot
Measured Boot
Remote Attestation

FEATURED MANUFACTURERS

infineon XILINX ALL PROGRAMMABLE WIND

PARTS

Part Number	Description	Resale
AES-PMOD-TPM12-SLB9670-G	Infineon TPM v1.2 Peripheral Module	$29.95 USD

RELATED PARTS

Part Number	Description	Resale
AES-Z7MB-IIOT-SK-G	MicroZed IIoT Starter Kit	$299 USD
AES-Z7MB-IIOT-UP-G	MicroZed IIoT Upgrade Kit*	$129 USD

*Does not include MicroZed SOM

Countries Available for Purchase: Americas, EMEA, Asia, Japan

CONTACT INFORMATION

North America
2211 S 47th Street
Phoenix, Arizona 85034
United States of America
eval.kits@avnet.com
1-800-585-1602

Europe
Gruber Str. 60c
85586 Poing
Germany
marketing@silica.com
+49-8121-77702

Japan
Yebisu Garden Place Tower, 23F
4-20-3 Ebisu, Shibuya-ku
Tokyo 150-6023 Japan
eval-kits-jp@avnet.com
+81-(0)3-5792-8210

Asia
151 Lorong Chuan
#06-03 New Tech Park
Singapore 556741
XilinxAPAC@avnet.com
+65-6580-6000