Trusted Computing Group Measurement and Attestation RootS (TCG MARS) Work Group FAQ February 2023

Table of Contents

What is the MARS Work Group?

The MARS Work Group is a technical work group within the Trusted Computing Group focused on isolated, lightweight roots of trust for computing devices down to the microcontroller level. Beyond this FAQ, more information on the MARS Work Group can be found at https://trustedcomputinggroup.org/work-groups/mars/.

What is the purpose of the MARS Work Group?

The MARS Work Group builds upon and complements existing TCG root of trust technologies by producing technical specifications to facilitate use cases including device identity, measurement recording and measurement attestation. A MARS root of trust will support measurement and attestation in much the same way as a TPM. MARS can be implemented without the need for a discrete chip or special processor modes. See the question on “How is MARS constructed?” for more information.

How is the MARS Work Group organized?

The MARS Work Group operates under the TCG. Membership in the MARS Work Group is determined by TCG bylaws and is open to TCG members at the contributor and promoter membership levels.

What is the output of this Work Group?

The MARS Work Group deliverables include specifications that define MARS' root of trust functionality requirements, command interface, informative supporting documents and informative emulator source code and examples.

How is MARS constructed?

MARS is specified so that it could be constructed as a hardware state machine and implemented within a microcontroller as a silicon IP block. Other designs are possible, including via FPGA, as software running in integrated or discrete adjunct processors, or host software executing in a protected execution environment. The MARS specifications do not limit manufacturers' choice of construction.

How is MARS attached to its host?

MARS may be attached in a variety of ways, as appropriate for the type of construction employed. For example, it may reside within a host microcontroller and be attached to a proprietary internal bus, attach to an external bus such as I2C or SPI, or logically via an inter-process communications channel. The MARS specifications do not limit manufacturers' choice of attachment.

Are there any physical requirements for a MARS device in the MARS Library Specification?

No. MARS commands and data were designed to be simple enough to implement as on-chip integrated primitives, but they could also be useful if implemented in other ways (e.g., as a discrete chip connected to a host, integrated into a system on a chip, as part of a cryptographic accelerator, etc.).

Is everything necessary to implement a solution using MARS in the MARS Library specification?

Additional platform specific requirements contributing to the protection of the MARS roots of trust and capabilities will be included in future platform profile specifications. Implementers can also independently choose profile values and implement protections for MARS capabilities and data appropriate for their scenario.

What is a Trusted Sensor Register (TSR)?

A manufacturer incorporating MARS may include additional logic that links an onboard sensor (e.g., clock, thermistor, breathalyzer) to a MARS register - known as a Trusted Sensor Register (TSR). When a TSR is referenced by a MARS command in a register selection bit mask parameter, the additional logic is used to sample the sensor and copy its value to a TSR. The sensor reading remains in the TSR until the next sampling or when the device is reset. After the sampling is done, the selected PCR and TSR are hashed to produce a "snapshot" digest. Refer to the MARS Library specification on CryptSnapshot for more detail. MARS_Quote, for example, digitally signs the snapshot. Consequently, a signed snapshot with TSR makes it practically impossible for a device to lie about its linked sensor.

Does the MARS Library specification support the scenarios in the MARS Use Cases and Considerations reference document?

Yes, the MARS Library contains all the commands needed to implement the use cases. Some use cases may rely on functionality outside the scope of the MARS library specification (e.g., connecting a data source to a TSR). The MARS workgroup intends to publish materials detailing which MARS commands support specific use cases, and corelating the terminology used in the library specification to terms used in the earlier use case document.