Trusted Computing Group Storage Work Group
Core Spec Addendum: Secure Messaging FAQ
August 2015

Q. What is the TCG Storage Architecture Core Specification?

A. The Core Specification ("Core Spec"), officially known as TCG Storage Architecture Core Specification, developed by the Storage Work Group provides a comprehensive definition of TCG-related functions for a TCG storage device.

Q. What is the TCG Storage Core Spec Addendum: Secure Messaging?

A. The TCG Storage Workgroup has developed the TCG Storage Core Spec Addendum: Secure Messaging, an enhancement to the Core Specification that defines Secure Messaging for the TCG Storage Architecture Core Specification by mapping Transport Layer Security (TLS) v1.2 onto the TCG Storage communication protocol.

Q. What about the secure messaging defined in the Core Specification?

A. As noted in the Core Specification, "Secure session start up" is a preliminary architectural component. The Core Spec Addendum: Secure Messaging defines a mechanism for secure session start up and associated secure messaging, based on standard, well known mechanisms embodied in TLS, which supersedes the preliminary architectural definition in the Core Specification.

Q. What is the benefit of the TCG Storage Core Spec Addendum: Secure Messaging?

It specifies a means by which the host can establish a secure communication channel with a SP on the device and uses TLS as the underlying secure transport protocol to protect TCG Storage protocol payloads.

Q. What does PSK stand for?

A. Pre-Shared Key. The TLS specifications allow for multiple ways to securely establish session keys. One of these involves the use of pre-shared keys, also known as PSKs. The "TCG Core Spec Addendum: Secure Messaging" specifications rely mainly on PSKs (i.e. TLS cipher suites using PSKs) for the TLS handshake phase.

Q. What are the implications of using PSKs?

A. Although use of PSKs avoids use of more complex methods that involve Public Key Infrastructures and PKI certificates, it has its own downsides. One of those is the need to transfer the PSKs from the host to the storage device. This must be done while the device is at a trusted or secure location, as no secure channel to protect these PSKs is available at the time of this operation.

Q. What version of TLS is used in the Core Spec Addendum?

A. The Core Spec Addendum: Secure Messaging requires TLS v1.2.

Q. Where can I get the "Core Spec Addendum: Secure Messaging" specification?

A. You can download the feature set specification from Trusted Computing Group website at www.trustedcomputinggroup.org.

Contact: **Anne Price**

602-840-6495

press@trustedcomputinggroup.org