Trusted Computing Group Storage Work Group

Opal SSC Feature Set: PSK Secure Messaging FAQ

August 2015

Q. What is a Feature Set?

A. A Feature Set defines additional functionality that extends a Security Subsystem Class (SSC) specification.

Q. What is a Security Subsystem Class (SSC)?

A. The Core Specification can be further broken down in multiple subsets of functionality called Security Subsystem Classes (SSCs). SSCs explicitly define the minimum acceptable Core Specification capabilities of a storage device in a specific “class” and potentially expand functionality beyond what is defined in the Core Specification.

Q. What is the Core Specification?

A. The Core Specification, 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. Is the PSK Secure Messaging Feature Set Mandatory or Optional?

A. The PSK Secure Messaging Feature Set is Optional.

Q. What is the Opal SSC “PSK Secure Messaging” Feature Set?

A. The Opal SSC “PSK Secure Messaging” Feature Set defines an Opal SSC specific implementation for secure messaging as specified in the “TCG Core Spec Addendum: Secure Messaging”. It provides 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 Opal SSC “PSK Secure Messaging” Feature Set and the “TCG Core Spec Addendum: Secure Messaging” specifications rely mainly on PSKs (i.e. TLS cipher suites using PSKs) for the TLS handshake phase. This is to simplify the initial implementations.

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 PSK Secure Messaging Feature?

A. The PSK Secure Messaging Feature requires TLS v1.2.

Q. How can I tell if a storage device supports PSK Secure Messaging?

A. The Level 0 “Secure Messaging” Feature Descriptor is returned by the storage device.

Q. What are the benefits of the PSK Secure Messaging Feature Set?

A. The PSK Secure Messaging Feature provides a means by which the host can protect TCG Storage protocol data against anyone snooping on the wire. This avoids disclosure of sensitive information such as credentials when used during session start or host authentication. Note that any user data transferred between host and device using normal interface transport (i.e. not the TCG protocol) is not protected by this feature.

Q. Are storage devices that support the PSK Secure Messaging Feature Set backward compatible with host software which doesn’t support this Feature Set?

A. Yes. The Feature Set introduces two new Session Object methods that don’t interfere with any of the existing TCG Storage Protocol methods. The host can use regular (unprotected) session startup or select secure session startup using these new methods.

Q. Where can I get the “Opal SSC Feature Set: PSK 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