Infrastructure Work Group Specification FAQ
May 2007

Q. What are the specifications being published?
A. The specifications published are related to *integrity management* of trusted platforms. These specifications can be best understood in the following groupings by function:

Integrity Management Architecture: This document provides the architecture for the management of integrity in systems.

- Integrity Management Architecture (v1.0)

Measurement agent: This specification defines the trusted software capable of measuring, verifying and reporting software.

- PTS Interface specification (v1.0)

Integrity Schema specifications: These specifications define the XML-based schemas for reporting and verification of software.

- Core Integrity Schema (v1.0)
- Integrity Report Schema (v1.0)
- Reference Manifest Schema (v1.0)
- Security Qualities Schema (v1.0 and V1.1)
- Simple Objects Schema (v1.0)
- Verification Results Schema (v1.0)

Certificate formats: This specification defines the profiles of TPM-related certificates based on the X.509 standard.

- Credentials Profile (v1.1)

Q. What do the specifications cover?
A. The set of specifications consists of the *Integrity Management Architecture*, the interface specification for a measurement agent called the *Platform Trust Service* (or PTS), and a common XML-based data format for capturing and reporting integrity information about a system.

The Integrity Management Architecture provides the common framework for defining, collecting and reporting information pertaining to the integrity of the software and configuration of a system. Such information includes the components (software and hardware) constituting the platform, the elements that participated in its booting-up and the software that establishes the computing environment in the platform.

The *Platform Trust Service* (PTS) interface specification defines the API to a measurement agent that performs the collection, measurement and reporting of the integrity information on the platform. The PTS interface specification has been written to be platform independent, meaning that it is applicable to the various types of platforms or devices (e.g. PC client, server, mobile phones, etc).

In order for the integrity information to be meaningful and verifiable by external entities (e.g. other devices), a common XML-based data format for representing this information has been defined in the Integrity Schema specifications. The Integrity Schema itself can be understood as consisting of three major pieces derived from a single XML schema. These are the data formats for collecting and reporting integrity information, the format for representing reference measurement of known values, and the format for the verification results from evaluating a report.

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Q. What is integrity management and what is it relationship to trusted platforms?
A. The TCG uses the term "integrity management" to mean the broad aspects around the measuring, reporting and verifying of the state of a given computer system, including the infrastructure support (e.g. architectures, protocols, data formats, etc) to accomplish these tasks.

There are numerous aspects of a trusted platform that can be subject to measurements and quantification. These include the register values inside the TPM hardware, files on the system, in-memory images and others. Which aspect of a trusted platform to be measured is largely dependent on the use case of the measurement (e.g. verified boot, network access control, etc).

Q. Why were these specifications developed?
A. TCG has developed these specifications to provide the industry with a common foundation for platform integrity measurement and verification, leading to the ability to establish information security assurance, and the potential application benefits associated with that assurance. TCG security assurance directly translates into trust in a platform's capability to protect its information and functional assets, and to attest to those protections.

These new set of specifications defines the functions, roles and infrastructure to provide integrity management for platforms. This includes mechanisms to determine the integrity state (measure) of a system or platform and report the measurements regarding the system.

Q. Who benefits from this specification?
A. These specifications allow users to have confidence in the security mechanisms in their system. This stems from the fact that the integrity of these mechanisms can be verified (locally or remotely) as being free from alteration by malicious code.

Q. How do these specifications relate to the Trusted Platform Module (TPM) shipping in PCs today?
A. These specifications are directly relevant to the TPM in PCs today and represent the next phase of infrastructure support for the operations of the platforms containing the TPM.

The TPM represents the trust anchor within the platform for the truthful reporting of the state of the platform. This feature is called "attestation" of the platform and represents a core value proposition of trustworthy computing. With the PTS specification, not only can the TPM be used to protect sensitive information, it can also be used to produce irrefutable reports (in a standardized format) regarding the TPM and the platform as a whole.

Q. Is TCG working with other standardization bodies?
A. As a standardization body the TCG believes strongly in using existing standards produced by other organizations and bodies. TCG has an active liaison program with the purpose of coordinating its open specifications with other organizations. The list of these other organizations is available on the TCG website.

Additionally, many of the TCG Infrastructure Work Group members also participate in other key standards organizations such as the IETF, IEEE, DMTF, W3C and others. The TCG believes that the specifications developed by the Infrastructure Working Group are complementary to the other industry security efforts. The current set of new specifications provides the necessary building blocks to achieve high assurance in the devices or end-points that posses the TPM as root of trust.

Q. When will we see products implementing the specification?
A. Since it is an industry group that does not develop products, TCG can't forecast specific product plans. Generally products follow specs by six to eighteen months, depending on product development cycles. Implementation depends on independent companies.

Q. Do these specifications work with the TNC specifications that do not require TPMs?
A. This set of IWG specifications can be implemented without the presence of a TPM. The value of these IWG specifications is dramatically increased when the root of trust (of the platform deploying them) is based in hardware.

In the context of the TNC specifications, the Platform Trust Service (PTS) interface specification provides an agent that can be employed (called by) the TNC Client to perform measurements of the components of the TNC Client device, as well as other client components. Furthermore, the set of IWG Integrity Schema specifications provides a standardized format for TNC implementers and vendors to report on the integrity status of a target device (e.g. TNC client). This standardized format promotes greater interoperability across TNC vendors.

Q. What is the relationship of these specifications to those TCG has published for servers and mobile phones?
A. The new set of IWG specifications are platform neutral, in the sense that they represent APIs and functionalities than can be implemented across platforms, including the mobile phone and server platforms. The need for measurement and reporting using a standard data format is common to all computer systems. The intent of the TCG Infrastructure Working Group and the infrastructure specifications is to provide functions and capabilities to support these platforms throughout its lifecycle. This lifecycle includes provisioning, deployment, day to day operations and retirement of platforms.

Q. What other infrastructure specifications has TCG released and how do they relate to the PTS Specification?
A. The current set of infrastructure specifications represents a second phase of specifications, with the first phase infrastructure specifications published in 2005. The first phase specifications focused on the operational infrastructure required for a single system (containing to a TPM) to function, allowing applications to make use of the basic features of the TPM. These specifications focused on key management, backup of keying material, certificate issuance and management, and others.

In the current (second phase) specifications the focus is on the infrastructure support required for one platform to *attest* its state to another platform, which is a core value proposition of trustworthy computing. Thus, the current set of specifications includes a common architecture for understanding attestation using a TPM, as well as an interface to a measurement agent (the PTS) that can measure state, issue a report and verify attestations. The PTS builds on these previous first phase infrastructure specifications, and make use of a number of crucial functionalities provided by these specifications.

Q. What is a typical use case for using TCG infrastructure specifications?
A. One of the core value propositions of trusted computing is that of providing attestation to the integrity of a given system. Thus, in addition to user authentication, a broad use case would be that of reporting the integrity status of the system (as measured and reported by the PTS) as part of access control to resources. There are numerous specific use cases for platform attestation. These include network access control (as exemplified by TNC), remote management and control of systems, security and integrity of financial transactions, verified boot of platforms, and others.

Q. Who is your target user of the TCG Infrastructure specifications?
A. The target users of the TCG Infrastructure specifications are enterprise IT organizations that deploy platforms with a TPM, and those using applications that rely upon the trust properties of trusted platforms. The overall aim of the TCG infrastructure specifications is to seamlessly support the deployment of trusted platforms in such a way that they are easily managed by IT personnel and can be integrated into existing IT management tools based on common standards for interoperability.

Q. Are there any privacy concerns with using PTS or other infrastructure specifications from TCG?
A. Consistent with the vision and practices of the TCG and its specifications, the infrastructure specifications have been designed to preserve the privacy of users. Similar to the TPM case, users must specifically choose to opt-in to deploy the PTS and other infrastructure functions. The PTS itself can be deployed without the TPM. The PTS vendors can implement administrative interfaces that allow control over the information that may be reported by the PTS, thereby ensuring user privacy. Finally, the PTS can be configured to perform only local verifications and thus privacy sensitive data can remain local to the platform. The PTS configuration should be driven by IT policies that will ensure that privacy sensitive values are not disclosed.

Q. Will implementing PTS restrict users to any operating system or applications? Can these be changed on a platform with PTS capability?
A. The PTS specification has been written to be agnostic across platforms (PC-Client, Server, Mobile, etc), and across operating systems and applications. The need for an agent to measure and report the integrity state of devices covering the entire software stack is a fundamental need of all devices. For vendors implementing the PTS, it is important to note that each implementation may be dependent on the hardware architecture and operating system upon which the PTS is implemented. For application

developers that make use of the PTS, the same interface will be available independent of the operating system and underlying hardware platform.

For more information, go to https://www.trustedcomputinggroup.org/groups/infrastructure

Contact: Anne Price
1-602-840-6495
press@trustedcomputinggroup.org

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.