Virtualized Trusted Platform Architecture Specification and Virtualized Platform Work Group
Frequently Asked Questions
September 2011

Q. What is the TCG doing in virtualization?
A. Virtualization is rapidly growing in popularity on both client and server systems. The extension of trusted computing to virtualization is a logical next step for TCG and trusted computing in general. From the perspective of a virtual machine, it runs in a virtualized environment identically to the way it runs if it was running natively on a physical platform. The Virtual Machine’s software and trust properties should be identical in both environments. From the perspective of trusted computing software, this means that each VM and hypervisor must have its own TPM. But in a virtualized platform, there may be only one physical TPM and it is owned by the base hypervisor (also called a Virtual Machine Manager or VMM).

The TCG Virtualized Platform Workgroup has created the Trusted Virtualized Platform Architecture, which describes how to build a trusted virtualized platform. The TCG Infrastructure Workgroup is developing the associated credentials and attestation protocols that go along with it. The TCG PC Client and Server Workgroups have developed the roots of trust (SRTM and DRTM) used to launch both trusted physical platforms and virtual machines running on those platforms. The TCG TPM Workgroup defines the TPMs (Trusted Platform Modules) on which trusted computing solutions are built.

Q. What challenges does the virtualized environment present for trusted computing?
A. Virtualized environments require a VMM (Virtualized Machine Manager or hypervisor) to present an environment to a VM that behaves like a physical platform and has the same trust properties as that physical platform. Many of the trust properties we get for free in the physical world we have to work for in the virtual world (software must be written to create the required behavior equivalent to hardware).
Two examples of some of the challenges that must be addressed are:

- In a physical TPM, keys can be stored in a IC package. In the virtual environment, software is responsible for key protection.
- A physical TPM is uniquely associated with a platform by virtue of the fact it is physically soldered to the physical platform. Providing the same level of association between a VM and its vTPM is a challenge.

The specification contains a comprehensive list of the trusted computing challenges that must be solved in the virtualized environment. This is the work that TCG is focused on in the VPWG.

Q. What is the scope of the VPWG in the larger arena of virtualized system architecture?
A. The VPWG’s goal is to supplement existing VMMs with robust trusted computing capabilities. The VPWG is developing architectures that can be added to existing VMMs to add trusted computing capability to those platforms. Beyond trusted computing, the VPWG is not redefining how VMMs should be designed or implemented.

Q. Does the Virtualized Trusted Platform Architecture define the way system vendors or VMM developers must isolate virtual machines from each other?
A. No, the Virtualized Trusted Platform Architecture does not specify how virtual or physical

machines are constructed. The architecture only specifies the security requirements and implementation considerations for a TCG compatible trusted platform.

Q. What is the role of trust and the TCG in a virtualized environment?
A. The TCG is looked to by the industry to provide trusted computing architectures to a broad range of platforms. The trusted virtualized platform is the TCG's next offering in this mission. The role of trust in a virtualized environment is the same as in a non-virtualized environment, but extended in a compatible way up through the layers and into the virtual machine.

Q. How does the TPM fit into a virtualized environment?
A. The TPM fits into a virtualized environment in two ways. A physical TPM is used to establish a root of trust for the physical platform, as with all TCG trusted platforms. A virtual TPM is provided to the virtual machine to extend a root of trust to VMs providing all the TPM capabilities that a VM would have running natively. The design is to provide the same environment that TCG based applications are already programmed for. The virtual and physical TPMs are linked to provide an added measure of security.

Q. The industry is currently providing support for virtual TPMs in virtualized environments. How does TCG fit into this?
A. TCG's Virtualized Trusted Platform Architecture Specification defines both how a virtual TPM should behave and how the virtual TPM is used in conjunction with the physical TPM to determine trust in the virtual platform. Providers of virtual TPMs can follow the Virtualized Trusted Platform Architecture. To provide interoperability, the specification defines interfaces, structures and APIs.

Q. Is the TCG VPWG doing any new specifications?
A. The Virtualized Trusted Platform Architecture Specification v1.0 is being released at this time. The PC Client Specific Virtualized Trusted Platform Specification is currently being developed.

Work is now going on for v1.1 of the Trusted Virtualized Platform Architecture along with additional features and lower level specifications.
The TCG welcomes new participants who would like to develop specifications for other virtualized platforms.

Q. How will this spec be used?
A. Physical TPMs are IO devices. Virtual TPMs are presented to virtual machines as IO devices (which are typically virtual IO devices implemented in software). These new TCG specifications discuss how TPMs – both virtual and physical – are used and managed in a virtualized environment. They discuss how other TCG technologies (eg. Attestation) are implemented in virtualized environments.
Vendors can use this specification to create TCG compliant trusted virtualized platform implementations.

Q. Who is supporting this spec?
A. This is the first specification that addresses the use of trusted computing in virtualized environments. It is anticipated that a number of vendors will adopt this specification as the security requirements for virtualization and cloud computing continue to be clarified and gain momentum in the market.

Q. Who will use this specification and when?
A. Trusted computing is just now starting to migrate to virtual machines. There are a number of hypervisor and cloud computing vendors who we anticipate will use this specification going forward. This is the TCG's first offering of a specification that addresses trusted computing in virtualized environments and, as such, is expected to have a big impact as trusted computing begins to be adopted in virtualized environments.