Server Work Group Generic Server Specification Frequently Asked Qusetions

FAQs to the Server Work Group's Generic Server Specification

TCG Generic Server Specification:

Q. What is the TCG Generic Server Specification?
A. This effort defines the architecture of a trusted server and how these servers are created, managed and maintained. The specification also provides a blueprint for communication between trusted servers and clients.

Q. Why is this necessary when there already are trusted clients?
A. TCG was founded with the goal of providing the building blocks for end-to-end trusted computing. With millions of trusted clients in use and many more anticipated to be deployed in the next few years, it was logical to offer developers a complementary specification to secure the server and allow trusted communications between servers and clients for applications such as financial transactions, storing critical data and others.

Q. What kinds of servers does this specification cover?
A. Like all TCG specifications, the server specification has been created to support a variety of platforms and architectures including x86 and Itanium architectures, MIPS, Sparc, Power and others.

Q. What form factor will trusted servers take? Will blade servers be supported?
A. The specification was written to allow platform vendors to build trusted servers in all form factors, including blade servers.

Q. How does the server specification relate to the Trusted Platform Modules (TPMs)? Is a TPM required for these servers?
A. Trusted servers are required to contain TPM functionality that meets the requirements of the TPM specification (1.2 or 1.1b). The specification is complementary to the TPM specification and defines the behavior and requirements of a trusted server.

Q. Will server TPMs be different from PC ones?
A. Currently, the trusted server may be designed using the same TPMs found in trusted clients. There is no reason, however, that a TPM or system vendor could not develop TPMs with higher bandwidth capabilities, as long as the interface specifications are met. In the future, TCG may add additional TPM functionality for servers.

Q. Does a trusted server impact server throughput?
A. This will depend on the design and TPM usage of the applications built on the new trusted server features. It is assumed that early applications will not rely on the TPM for high throughput operations, but over time, as TPM performance is enhanced, more operations may be handled by the TPM.

Q. What does the specification require for servers? How much redesign is required to incorporate Trusted Computing into future servers?
A. The specification communicates baseline requirements, providing server vendors with a definition that allows for efficient transition of their server designs to trusted server designs. Much of the work in the

trusted client space can be leveraged into an x86 trusted server design, requiring minimal redesign, at the hardware, operating system and application level.

Q. When do you expect to see trusted servers on the market?
A. Trusted servers shipping with TPMs have been available since 2006 from several vendors.

Q. Will trusted servers require new or additional management tools and services?
A. There will be new tools to manage the security capabilities of trusted servers.
Q. Will trusted servers be compatible with today's applications?
A. Trusted servers will be compatible with today's applications, although to take full advantage of the new security features, updated applications will most likely be necessary.

Q. Can IT managers deploy a mix of trusted and non-trusted servers?
A. Yes. As with trusted clients, we anticipate most organizations will deploy a few trusted servers initially then gradually switch as they replace older systems.

Q. What are some of the anticipated uses for a trusted server?
A. The TCG Generic Server Specification provides for use cases including:

- Asset management
- Configuration management
- Data migration and back-up
- Distributed trusted computing
- Document management
- Financial transactions
- Management of endpoint integrity and network access control
- User and platform authentication

Q. What are some examples of these?
A. One is ensuring a trusted client is connecting to the intended server. The specification also provides for a usage model in which the server is verified to meet minimum standards before being allowed to perform sensitive transactions. Another example is to ensure that data stored on servers is sealed (using a TPM based on the 1.2 specification) to protect it from unauthorized access.

2. TCG Itanium Architecture Based Server Specification:

Q. What is the TCG Itanium Architecture Based Server Specification?
A. The TCG Itanium Architecture Based Server Specification defines trust requirements specific to Itanium Architecture based servers. The specification defines the trust measurements specific to Itanium Architecture based trusted servers and how these servers are created, managed and maintained.

Q. How does this specification relate to the TCG Generic Server Specification?
A. The TCG Itanium Architecture Server Specification is built upon the TCG Generic Server Specification. The Itanium Architecture Based Server Specification takes the more general requirements of the Generic Server Specification and creates a more specific set of requirements for Itanium Architecture based servers. In particular, it specifies the trust measurements that must be made by the PAL and SAL firmware layers.

Q. How does the TCG Itanium Architecture server specification relate to the Trusted Platform Modules (TPMs)? Is a TPM required for these servers?
A. Trusted Itanium Architecture based servers are required to contain TPM functionality that meets the requirements of the TPM specification (1.1b or 1.2). This specification is complementary to the TPM specification and defines the behavior and requirements of a trusted Itanium Architecture based server.

Q. Does the specification require Itanium Architecture-based servers? How much redesign is required to incorporate Trusted Computing specifications into future Itanium Architecture servers?

A. The specification communicates baseline requirements, providing Itanium Architecture server vendors with a definition that allows for efficient transition of Itanium Architecture server designs to trusted Itanium Architecture server designs. It specifies platform trust measurements that must be made by the PAL and SAL firmware.

Q. When do you expect to see products incorporating the server specification?
A. Trusted Itanium Architecture servers with TPMs are available today.

Q. Does the TCG Itanium Architecture Server Specification cover areas such as ACPI and EFI?
A. The Itanium Architecture server specification refers to several other specifications, such as the TCG ACPI General Specification, and an upcoming set of specifications on the EFI firmware environment. This allows these other specifications to be shared across several TCG platform types, such as trusted clients.