

Trusted Computing Platform Alliance Announces v.1.0 Specifications for Trusted Computing

Hillsboro, OR, January 30, 2001 - The Trusted Computing Platform Alliance (TCPA), an industry consortium focused on improving trust and security on computing platforms, today announced the release of its version 1.0 of the Trusted Computing Platform Specifications.

In a world increasingly influenced by the Internet, data security, information protection and user privacy have never been more important. TCPA's intention with the release of version 1.0 is to provide the industry with a clear direction that facilitates trust in computing platforms and environments.

Trusted computer platforms address the critical issues of protecting a user's personal or corporate information and protecting against break-ins, by improving the basis on which a computing environment may be trusted by the use of trusted computing platform technology.

"Consumers and businesses alike have not taken security as seriously as they should," says Roger Kay, a Research Manager at IDC. "It is only within a secure, trusted environment that e-business can really flourish, and security is only as strong as its weakest link. The industry is taking an important step by embracing the totality of the security problem, providing soup-to-nuts solutions from secure log-on to data integrity, public key infrastructure (PKI), protected storage, digital signature, and all the other necessary elements to provide an electronic business environment in which computing users realize improved safety from malicious hackers and other criminals."

The TCPA specification defines a subsystem so that it may be trusted to operate as expected. The subsystem contains an isolated computing engine whose processes can be trusted because they cannot be altered. When platforms that include this technology are available, they will measure and report information about the environment in that platform. This "integrity check" feature of the subsystem complements and enhances software-only security services.

TCPA uses a behavioral definition of trust, stating that an entity can be trusted if it always behaves in the expected manner, for the intended purpose. Version 1.0 of the specification describes the features that will enable a basic level of trust in a platform in order to be considered trustworthy by local users and by remote entities.

The TCPA 1.0 specifications add significant additional trust capability and security building blocks that can be built to supplement the computing platform that exists today. A TCPA-enabled system offers manufacturers a low cost, standardized means of embedding security functionality in a platform, translating into improved security measures and therefore enabling and encouraging the ubiquitous development and use of applications and services that use security.

These trusted processes, as described above, include protected storage, digital signature, and PKI key support. The use of TCPA described features will increase the confidence of both local users and remote entities interacting with the platform by using cryptographic processes to enhance local and remote access controls on information stored on the platform. Critical applications such as secure email, Web browsing, and file encryption will be able to leverage these capabilities through existing industry standard interfaces to enhance a user's security and privacy.

As PCs evolve, security specifications will need to also evolve to allow for greater trust in the computing environment of the future.

Customers will be able to utilize TCPA-conforming systems once PC manufacturers create a product that meets the new, more stringent security profiles; conformance to the new guidelines is the responsibility of individual vendors.

More information is available on the TCPA website: www.trustedpc.org

###

TCPA Quote Sheet

"Security and trust are critical in our increasingly connected world. Compaq's participation in the TCPA underscores our legacy of leadership in PC security. Compaq was the first PC manufacturer to ship Fingerprint Identification Technology (FIT), and today we also offer a range of smart card enabled keyboards and readers that can be used to provide enhanced security during online transactions and for authentication. As a founding member of the Trusted Computing Platform Alliance (TCPA), Compaq Computer Corporation continues to work for standards that address customer concerns about conducting business over the Internet."

John Thompson
Vice President of Marketing
Compaq Commercial PC Group

"HP is committed to delivering customers with trusted computing platforms to perform business critical e-services over the Internet with the highest level of confidentiality and integrity. The first release of the TCPA spec takes the IT industry one step closer to ensuring customers a trusted computing environment, either inside Intranets or over the Internet. This will enable customers to run their businesses with a high degree of confidence. As a founding member of the TCPA consortium, HP will work closely with its partners to bring trusted computing solutions to the market."

Ed Yang
Vice President and Chief Technology Officer
HP Computing Systems

"Building trust through client security is absolutely crucial in the world of e-business. IBM helped design the TCPA standard and was the first OEM to ship an enhanced hardware security element in a PC client. IBM will continue to establish and support industry-wide standards for improved PC client security. Today's NetVista personal systems already incorporate major aspects of the TCPA specification. Additional TCPA attributes will be added to NetVista desktop systems and Thinkpad notebooks later this year."

Harry Nicol
General Manager
IBM NetVista Desktop Systems

"TCPA Specification 1.0 is the result of an industry effort to improve trust and security on computing platforms. The specifications will help deliver a set of capabilities that customers can use to enhance the security of their computing environments."

Pat Gelsinger
Vice President and Chief Technology Officer
Intel Architecture Group

"As a founding member of the TCPA, Microsoft is pleased to see the specification ratified by such a large and diverse group of companies. This specification will allow manufacturers of PCs to enhance the trust that is already available on their platforms. Consumers have been asking for higher levels of security - for example improvements in the protection of their privacy - and a TCPA-enabled PC can help them protect their privacy."

Carl Stork
General Manager
Microsoft Windows Hardware Strategy

About TCPA

TCPA was formed in 1999 by founding promoter companies Compaq, Hewlett-Packard, IBM, Intel and Microsoft, to focus on improving trust and security across the industry via a collaboration of PC industry platform, operating system, application and technology vendors. Working together, more than 145 TCPA member companies intend to enhance existing approaches and simplify the deployment, use and manageability of security elements on future computing platforms, including PCs. The group will encourage wide industry support and adoption of the specifications, with an ultimate goal of gaining worldwide acceptance.