

可信计算组织（Trusted Computing Group）的可信平台模块规范成为ISO标准

PC和其他设备中广泛使用的安全芯片正式成为国际标准

美国商业资讯俄勒冈州PORTLAND消息——

JTC1是国际标准化委员会（ISO）和国际电工委员会（IEC）的联合委员会。JTC1已经接受可信计算组织的可信平台模块规范v1.2并将其公布为ISO/IEC标准11889。作为独立或集成的组件实施的可信平台模块(TPM)可在计算平台中实现信任。

可信计算组织的总裁Scott

Rotondo说：“ISO/IEC接受TPM规范确认了可信计算组织作为可信计算行业首要组织的地位，证实了安全数据、系统和网络正越来越多地使用此规范。对于在安全和可信计算领域工作的政府、开发者和用户而言，JTC1认可TPM规范可保证遵守公认的国际标准、保护开发投资，有助于市场发展。”

TPM的国际标准化预计将扩大TPM应用的开发和该技术的使用。预计ISO和IEC对TPM的认可还将为开发者和用户提供关于可信计算和TPM的清晰指导。

可信平台模块容易获取，价格便宜，是可在多数PC上方便使用的组件。该模块被用于在PC启动时检查用于运行计算机的软件是否出现任何变化，以帮助在PC启动和连接到网络之前检测僵尸网络、rootkit和其他可疑代码。TPM安全地存储密钥、证书和密码，支持鉴别和认证，这对于可信计算至关重要。

来自ISO的文档包括ISO/IEC 11889-

1:2009，这是TPM的概述，对TPM进行介绍并说明它如何适合于可信平台。ISO/IEC 11889-

1:2009说明可信平台的概念，例如可信边界、信任传递、完整性度量和完整性报告。附加的ISO文档提供TPM设计原理、结构和命令。

ISO文档位于：

http://www.iso.org/iso/catalogue_detail.htm?csnumber=50970

。在线的TPM规范和相关文档位于TCG网站：

http://www.trustedcomputinggroup.org/resources/tpm_main_specification

。

可信计算组织是个支持计算安全的行业组织，它创建了一系列规范以跨企业在PC、服务器、网络设备、应用程序、其他软件、存储和内嵌设备中实现更安全的计算。欲进一步了解详情和该组织的规范和工作组，敬请访问可信计算组织的网站 www.trustedcomputinggroup.org。

本文中的品牌和商标是其各自所有者的财产。

免责声明：本公告之原文版本乃官方授权版本。译文仅供方便了解之用，烦请参照原文，原文版本乃唯一具法律效力之版本。