随着人们的移动性与日俱增，对身份验证的安全性及可靠性的新需求应运而生，推动虚拟身份验证取代密钥卡门禁。为了应付无间断连接及完全分布式智能设备的爆炸式增长所带来的挑战，有必要制定一种基础架构方案来支持不断演变的门禁控制系统应用，并推动所有相关的新产品开发工作。近距离无线通信（Near Field CommunicaTIoNS，以下简称NFC）是有望实现上述目标的技术，但要确保其安全性，业界就必须建立一种基于综合监管链的身份验证方法——通过这种方法，系统或网络中的所有端点都能够得以验证，从而让各端点之间的身份验证信息在任何时候都能够可靠传输。

**1 系统简介**

　　TIP是一种安全可信的网络，可提供身份验证传输框架，实现安全产品和服务的交付。它是一种用于创建、交付和管理安全身份验证的综合性框架。简单来说，该基础架构是一个中央安全库，通过安全的网络连接，并以公开的加密密钥管理安全政策为依据，为已知端点（如凭证卡、读卡器什么是读卡器？

　　顾名思义，读卡器就是读取存储卡的设备。存储卡现在应用可谓非常广泛，从数码相机到MP3随身听，从PDA掌上电脑到时下比较流行的多媒体手机。目前在市面上比较常见的存储卡有SmartMedia（SM卡）、CompactFlash（CF卡）、MemoryStick（索尼记忆棒）、MultiMediaCard（MMC卡）、SD Memory（SD卡）、IBM Microdrive（IBM微型硬盘），以及最新的XD-Picture（XD卡）。和打印机）服务交付。HID Global将其称为“受规限”系统——连接到该系统的所有设备都是已知的，因而能够可靠安全地交换信息。TIP架构具有充分的可扩展性，其传输协议和加密模式符合各种标准，可支持多种应用。TIP系统还可以实现虚拟化及云端基础模式，因而能够在不影响安全性的情况下通过互联网提供服务交付。

　　TIP提供一种受保护的身份验证传输网络，可对网络中的所有端点或节点进行验证，因而各节点之间的信息传输都是可信的。



TIP模型图

　　TIP模型（如上图所示）包含三个核心要素，即安全库（Secure Vault）、安全通信（Secure Messaging）方法、密钥管理策略和规范（Key Management Policy and Practices）。安全库为已知且可信的端点提供加密密钥安全存储功能，安全通信方法即使用符合行业标准的对称密钥方法将信息传输至各个端点，密钥管理策略和规范即设定“安全库”的访问规则以及向各端点分发密钥的规则。

**2 如何建立端点及可靠的信息传输**

　　只有在实施了TIP节点协议后，端点才会启用，进而被“安全库”识别并注册为可靠的网络成员。而后，该端点就可与“安全库”进行通信。

　　凭证卡、读卡器及打印机等端点通过软件工作流程与“安全库”进行通信，其访问和处理规则都受到HID Global的“密钥管理策略和规范”的严格管控——只有经认证的设备才能够加入该网络（与任何计算机都可访问任何网站的互联网不同），从而形成了隐性的、严格的身份验证机制。

　　各端点之间的TIP消息采用符合行业标准的加密方法进行加密，以便进行符合公开安全政策的安全信息传输。这些TIP信息数据包由两个嵌套的对称密钥进行保护，其中含有“安全身份验证对象”（Secure Identity Object，简称SIO）信息。多个SIO可嵌套到一个TIP信息中，向各种不同的设备（如门禁卡、智能手机及计算机）提供多种指令。如有必要，每个设备都可具有不同的门禁控制特性。例如，最简单的SIO就是模拟iCLASS卡上的凭证程序数据。

　　“安全库”与端点设备之间的验证通过后，该设备在网络中就被视为是“可信的”。可信设备无需再与安全库进行通信，可以独立工作。在这种方式下，各端点（如凭证卡及读卡器）之间的信息传输是“可信的”，而由此产生的信息传输（例如打开一道门或登录到计算机）也就被视为是“可信的”。

　　在近距离无线通信技术的支持下，应用该技术的手机就可作为TIP端点而受到支持，因而能够使用不同的SIO进行编程，进而实现模拟卡片或者更为复杂的应用，不但可以获授权通过RFID/xinpin/menjinkaoqin/' target='\_blank'>门禁系统，还可实施由其自身进行解释的复杂门禁控制规则。

**3 发展现状及前景**

　　TIP在2010年底已经开始部署，并已通过宣布与HID Global的第一家合作伙伴，NCF 芯片领先企业INSIDE CONtactless的合作，朝可信、虚拟及按需式身份验证网络的宏伟蓝图迈出了第一步。INSIDE Contactless是为数不多的几家正在全球范围内推动NFC试验的公司之一。这一开创性的合作将使支持NFC的手机能像物理智能卡那样，融入iCLASS门禁控制和凭证信息。此凭证信息将通过HID Global的TIP系统提供，将来还可以实现与其他网络服务和实时通信的结合使用。HID Global 计划开展其他类似的合作伙伴关系，将HID Global和其他供应商的非接触式解决方案、NFC 技术及其他广泛应用的技术融为一体，为用户身份验证、无现金自动售货及计算机安全登录等各种应用打造一个广泛适用（涵盖从手机到笔记本电脑的各种终端设备）的平台。这些平台和应用将大幅提升非接触式智能卡凭证的价值定位。