Wi-Fi®安全状况

Wi-Fi CERTIFIED™ WPA2®为家庭、企业和移动设备提供先进安全性

Wi-Fi Alliance®

2009 年 9 月

执行摘要

Wi-Fi 是世界上应用最广、最值得信赖的技术之一，拥有强大的全球公认品牌。用户看重其可靠性能、简单性和广泛的适用性。在工作场所、家里、公共热点，Wi-Fi 无处不在。用户可用笔记本电脑、手机、相机、游戏机及越来越多的其他消费电子设备接入 Wi-Fi 网络。

Wi-Fi Alliance 通过其 Wi-Fi CERTIFIED™ 项目，致力于推动无线局域网（WLAN）设备和网络互操作性的运用与技术创新。Wi-Fi CERTIFIED 设备可带来即开即用的多厂商互操作性及出色的性能。

企业、家庭和移动用户知道，Wi-Fi 还提供尖端、标准先进的网络安全性。Wi-Fi CERTIFIED 设备满足了基本的企业网络和应用的安全需求，使住宅用户能够保护自己的网络。

自 2000 年项目推出以来，安全已成为 Wi-Fi Alliance 工作的核心。有线等效保密（WEP）是第一代解决方案。2003 年，Wi-Fi Alliance 推出了 Wi-Fi 保护接入（Wi-Fi Protected Access®/WPA）作为临时安全解决方案，以满足对日益增长的安全机制的市场需求，同时美国电气电子工程师学会（IEEE）802.11i 修正版正在制定中。WPA 通过提供双向鉴权和更强大的加密功能，弥补了 WEP 的不足。

Wi-Fi 安全大事记
2000 年，Wi-Fi Alliance 认证项目启动，包括对 WEP 的支持
在预期 IEEE 802.11i 修正版通过的情况下，WPA 认证作为临时解决方案，于 2003 年推出
采用 AES 加密并支持 EAP 的 WPA2 于 2004 年推出，并于 2006 年成为强制性要求
Wi-Fi 保护设置（ Wi-Fi Protected Setup™）作为可选认证项目，于 2007 年推出，以简化受到安全保护的家庭和小型办公网络的设置和扩建
2009 年，Wi-Fi Alliance 将所支持的可扩展认证协议（EAP）类型增加到 7 个，增加了 EAP 鉴权和密钥协议（ EAP-AKA）及 EAP-通过安全隧道灵活鉴权（ EAP-FAST）

WPA2 是新一代 Wi-Fi 安全技术。它建立在两项核心协议的基础之上：(1) 美国及其他国家政府用来保护机密信息、企业用来保护 WLAN 的加密协议——高级加密标准（AES）；(2) 企业网络中广泛用来提供强大的鉴权和精密网络接入控制功能的标准——IEEE 802.1X。WPA2 基于 IEEE 802.11i，提供 128 位 AES 加密。它还通过预共享密钥（PSK；个人模式下）和 IEEE 802.1X / EAP（企业模式下）提供双向鉴权。2004 年，Wi-Fi Alliance 推出了 WPA2 认证。2006 年，WPA2 认证成为针对所有提交认证的 Wi-Fi CERTIFIED 设备的强制性要求。此外，2007 年，Wi-Fi Alliance 推出了 Wi-Fi 保护设置项目，以简化和鼓励 WPA2 在住宅网络中的激活。

通过 WPA2，Wi-Fi 技术走向了成熟，使其能够为所有 Wi-Fi 用户提供跨越不同设备外型、厂商和地域的绝佳尖端安全性。Wi-Fi Alliance 致力于拓展现有的认证项目，创造新的认证项目，从而推动有益于用户的新型安全解决方案的运用。

引言

目录

Wi-Fi 无处不在。约三分之一拥有宽带互联网接入的美国家庭拥有 Wi-Fi 网络[1]。预计到 2009 年年底，Wi-Fi 芯片组的出货量将达到 20 亿；到 2013 年，预计这一数字将达到 70 亿[2]，这将是移动和消费电子设备领域最高的增长率之一。

自 2000 年 3 月推出其认证项目以来，Wi-Fi Alliance 一直致力于促进该技术的运用、互操作性和发展。Wi-Fi Alliance 拥有 300 多家会员和数千款认证产品，Wi-Fi Alliance 已经成为包括服务供应商、芯片组和设备厂商以及软件开发商在内的整个 Wi-Fi 生态系统的推动力。

Wi-Fi CERTIFIED 产品接受过严格的测试，以确保即开即用的互操作性和出色的用户体验。消费者和企业用户信赖 Wi-Fi CERTIFIED 品牌，知道它始终致力于为包括笔记本电脑、手机及其他移动和消费电子设备在内的各种设备提供即开即用的互操作性、可靠的性能和最佳用户体验。

市场成功不仅仅取决于用户体验和互操作性。迅速增长的家庭、企业和 Wi-Fi 移动用户需要的不仅是可互操作、可靠、简单易用的高性能设备和接入点。他们还需要一定的安全技术来保护他们在商务、个人和移动运用中的数据和控制网络接入。放心和信任是出色用户体验的关键要素。

所有环境（住宅、企业和移动环境）都需要高度保护。Wi-Fi 被用于在各种情境下发送保密和私人信息。企业用户用 Wi-Fi 来与同事、合作伙伴及客户交换高度敏感的信息。家庭及移动用户常用 Wi-Fi 来与家人朋友分享私人信息。除数据以外，各种环境下的客户正越来越多地使用 Wi-Fi 语音。

Wi-Fi 设备与网络保护功能已成为 Wi-Fi CERTIFIED 测试项目推出以来的支柱。自 2006 年年初以来，WPA2 安全支持已成为对所有 Wi-Fi CERTIFIED 设备的强制性要求。Wi-Fi Alliance 在促进 WPA2 成为所有主要厂商支持的全球公认的成熟标准的过程中发挥了主导作用。

Wi-Fi Alliance 使用标准机制，通过简单易用、推动安全最佳实践运用的安全接口工具，为 Wi-Fi 用户提供最高水平的安全性。同时，Wi-Fi Alliance 认识到有必要推出多种解决方案，以满足不同使

---

[1] 来源：Parks Associates

[2] 来源：ABI Research

用情况和设备的安全要求。因此，Wi-Fi 认证项目具有使 Wi-Fi CERTIFIED 设备满足不同类型网络（从受到高度控制的企业环境到比较灵活的家庭网络）要求以及在不同的设备外型设计下操作的灵活性。

本文对 Wi-Fi 安全状况进行评估，内容涉及认证项目的发展，以提供更加先进、简单易用的工具，以及 Wi-Fi CERTIFIED 设备所支持的密钥功能。在文章的最后，德州大学达拉斯分校的案例分析说明如何通过 WPA2 保护校园 Wi-Fi 网络。

Wi-Fi 安全的发展

Wi-Fi 技术发展迅速，以适应日新月异的市场和技术形势。全球对 WPA 和 WPA2 等先进的安全机制的运用进一步加强了世界范围内对 Wi-Fi CERTIFIED 设备的信赖（表 1）。

日期	里程碑
1997 年 9 月	IEEE 802.11 标准获批，包括 WEP
2000 年 4 月	Wi-Fi CERTIFIED 项目推出，支持 WEP
2001 年 5 月	IEEE 802.11i 工作组成立
2003 年 4 月	WPA 推出，包括 • IEEE 802.1X 鉴权 • 支持临时密钥完整性协议（TKIP）加密 • 支持 EAP 传输层安全（EAP-TLS）
2003 年 9 月	WPA 成为针对所有 Wi-Fi CERTIFIED 设备的强制性要求
2004 年 6 月	IEEE 802.11i 修正版获批
2004 年 9 月	WPA2 推出，包括： • IEEE 802.1X 鉴权 • 支持 AES 加密 • 支持 EAP-TLS
2005 年 4 月	增加对四种 EAP 类型的支持： • EAP 隧道 TLS 微软挑战握手认证协议第 2 版（EAP-TTLS/MSCHAPv2） • 保护 EAP 第 0 版（PEAPv0）/EAP-MSCHAPv2

	• 保护 EAP 第 1 版（PEAPv1）/ EAP 通用令牌卡（EAP-GTC） • EAP 用户识别模块（EAP-SIM）
2006 年 3 月	WPA2 成为针对所有 Wi-Fi CERTIFIED 设备的强制性要求
2007 年 1 月	Wi-Fi 保护设置项目推出
2007 年 11 月	IEEE 802.11w 工作组成立
2009 年 5 月	新增对 EAP-AKA 和 EAP-FAST 的支持

表 1 Wi-Fi 安全大事记

接入控制和加密技术进步以及平行的标准化工作（尤其是 IEEE 802.11i（媒体接入控制[MAC]层安全增强））和 IEEE 802.11w（保护管理框架）工作组的工作）实现了 Wi-Fi 安全的发展。

随着 Wi-Fi 运用的增长而突出的新应用和使用情况促使新型安全机制问世。几年前，Wi-Fi 在住宅和企业网络中的迅速普及增加了 WEP 审查，其局限性很快被察觉。此外，Wi-Fi 作为家庭主要接入技术的出现、公共热点的日益普及以及传送敏感和关键任务数据的企业网络的部署提高了对 Wi-Fi 的安全审查要求。

作为第一代安全解决方案，WEP 由于在重要大小（最初为 40 位，后来扩展到 104 位）上的局限性以及缺乏重播侦测功能而容易受到攻击。因此，用户不得不通过使用虚拟专用网（VPN）、IEEE 802.1X 或专有解决方案对 WEP 加以补充，以满足他们的安全需求。

到 2003 年，Wi-Fi Alliance 已改用包括 IEEE 802.11i 修正版子集的 WPA。WPA 是在预期 IEEE 802.11i 修正版通过的情况下，为弥补 WEP 的不足而设计的第二代临时解决方案；IEEE 802.11i 修正版随后被并入 IEEE 802.11-2007 标准中，对 Wi-Fi 安全机制做出了规定（表 2）。WPA 用 TKIP 进行数据加密。WPA 鉴权由 IEEE 802.1X 利用 EAP 为企业用户提供，由 PSK 为住宅和个人用户提供。

2004 年，在 IEEE 802.11i 修正版获批的同时，Wi-Fi Alliance 推出了 WPA2。起初，它是一项可选认证，但于 2006 年成为取代 WPA、针对提交认证的所有新设备的强制性要求。虽然建立在 WPA 功能的基础之上，但 WPA2 引入了更强大的加密功能，增加了使用 AES 分组密码的 CCMP 协议。2006 年以来接受测试的所有 Wi-Fi CERTIFIED 设备都支持 WPA2，为 Wi-Fi 用户提供最先进的标准安全机制。WPA2 迅速成为 Wi-Fi 设备运用最广、最值得信赖的安全框架。

	WEP	WPA	WPA2
主要加密机制	手动密钥分配，使用 Rivest 密码法 4（RC4）流密码的共享密钥	基于 RC4 流密码的 TKIP	使用 128 位 AES 分组密码的计数器模式密码块链信息认证码协议（CCMP）
数据完整性	线性哈希函数	密码哈希函数	
密钥管理	无	有	
重播侦测	无	有	

表 2 WEP、WPA 和 WPA2 之比较

WPA2 技术概述

厂商和用户对 WPA2 的广泛认可和信赖源于四个关键因素：

- **双向鉴权：**WPA2 用 IEEE 802.1X（WPA2 企业版）和 PSK（WPA2 个人版）提供双向鉴权。在单向鉴权的情况下，客户端设备发送证书，如果被批准接入，客户端设备就会连上网络。双向鉴权要求客户端设备在建立连接之前验证网络证书，以防用户连上未经授权的接入点。
- **强加密：**AES 被规定为联邦信息处理标准（FIPS Publication 197），是最早公开的加密机制，符合美国政府保护敏感机密信息的要求[3]。迄今为止，AES 已证明在面对由于 AES 的广泛运用而引发的大量已公布之攻击时极富弹性。当通过 WPA2 网络传输的数据用采用 AES 的 CCMP 算法进行加密后，就受到目前最先进的标准数据加密方法的保护。全球企业网络中所使用的很多协议和应用都要求支持 AES。
- **可互操作性：**WPA2 是基于标准的解决方案，得到 2006 年以来接受测试的所有 Wi-Fi CERTIFIED 设备的支持。无论何种设备品牌，WPA2 都可在接入点和客户端设备支持 WPA2 的任何会话中被激活。这大大提升了 WPA2 的可用性，使网络运营商和用户相信，他们的网络、设备和数据流处处受到保护。
- **使用简便：**WPA2 不但是保护 Wi-Fi 用户的强大工具，而且容易激活。2007 年，Wi-Fi Alliance 推出了独立认证项目——Wi-Fi 保护设置，以简化 WPA2 的配置，加速其在住宅网络中的运用。

[3] 保密信息可使用 128 位 AES；机密信息要求使用 192 或 256 位 AES。

WPA2企业版和WPA2个人版

根据网络要求，WPA2 有两种运行模式——企业模式和个人模式（表 3）。对 WPA2 个人版的支持是对所有 Wi-Fi CERTIFIED 客户端设备和接入点的强制性要求。对 WPA2 企业版的支持是非强制性要求，但是对在大型网络中工作的设备是建议性要求。具体的安全要求决定了在网络中使用哪一种模式。

住宅和小型办公网络一般使用 WPA2 个人版，因为它除了 Wi-Fi CERTIFIED 接入点和设备以外无需任何设备。在 WPA2 个人版中，密钥来自网络服务区标识符（SSID）和用户输入的密码。必须选择强大的密码，以充分利用 WPA2 的保护。较长、复杂、任意的密码是良好安全性的关键，而且应经常修改。

采用 IEEE 802.1X 鉴权、授权和记账（AAA）服务器的企业网络可得益于 WPA2 企业版所提供的更加复杂的功能，包括监控和管理流量、规定用户特定鉴权级别以及提供游客接入的能力。WPA2 企业版还通过共享现有的用户数据库，允许无线接入与整体网络接入控制进行整合。

WPA2 企业版	WPA2 个人版
每位用户分配到独一无二的证书	使用 PSK、不受管理的鉴权模式允许使用一般由该网络用户共享的手动输入的密码
需要支持 EAP、带有鉴权数据库的 IEEE 802.1X AAA 服务器	无需鉴权服务器
每一个会话的数据安全密钥是独一无二的	每一个会话的数据安全密钥是独一无二的

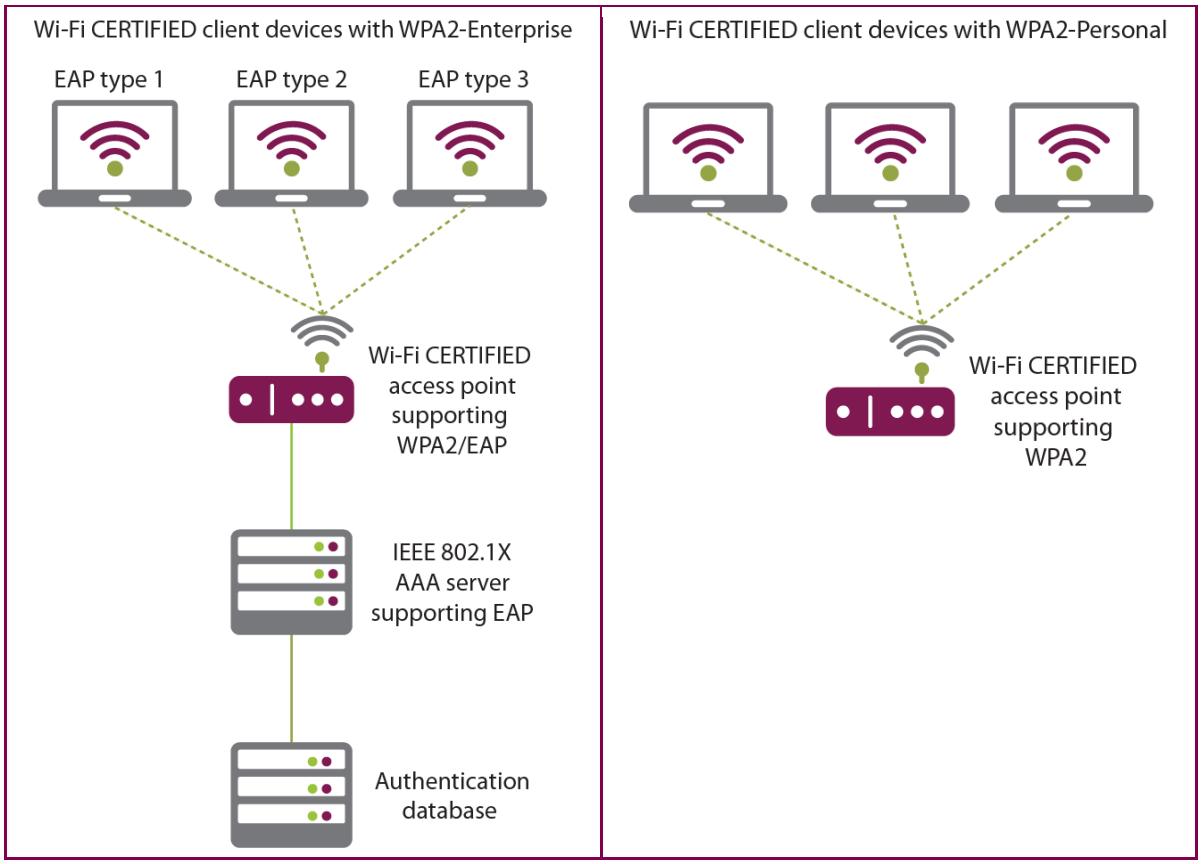

表 3 WPA2 企业版和 WPA2 个人版

采用IEEE 802.1X / EAP的鉴权

WPA2 企业版使用支持 EAP 的 EEE 802.1X 框架进行鉴权（表 4）。对多种 EAP 类型的支持使企业能够针对自己的运行环境选择最适当的鉴权技术。就网络而言，在接入点、IEEE 802.1X AAA 服务器中必须实现对一种或多种 EAP 类型的支持。客户端设备和网络（即接入点和服务器）都必须支持相同的 EAP 方法，以完成鉴权过程。

WPA2 企业版支持全球用于在企业环境中提供安全鉴权的多种 EAP 方法。WPA2 具有在新的 EAP 类型出现后支持这些新类型的灵活性。随着市场需求的增长，Wi-Fi Alliance 不断增加对新的 EAP 类型的支持，以便为用户提供最适合他们的设备、应用和网络的鉴权技术。

对 Wi-Fi 网络所支持的 EAP 类型的选择取决于设备外型设计、网络托管的应用、所使用的操作系统以及网络拥有者的具体安全要求，包括用户名和密码、令牌、认证及 PSK。

Wi-Fi Alliance 认证项目目前支持的 EAP 方法有：

- **EAP-TLS**：使用数字鉴权证书的互联网工程工作组（IETF）全球标准协议。
- **EAP-TTLS/MSCHAPv2**：在 TLS 记录内安全建立客户密码鉴权隧道。
- **PEAPv0/EAP-MSCHAPv2**：使用基于密码的鉴权

- **PEAPv1/EAP-GTC：**使用不断修改的鉴权令牌值
- **EAP-FAST：**用 TLS 安全建立任何鉴权证书隧道（如密码或令牌）
- **EAP-SIM：**基于使用全球移动通信系统（GSM）网络的手机和其他设备中所安装的 SIM
- **EAP-AKA：**使用通用移动通信系统（UMTS）用户识别模块（USIM）进行鉴权

WPA2 如何发挥作用？	
WPA2 企业版	**WPA2 个人版**
1. 客户端设备联合接入点，将其身份信息发送给鉴权服务器 2. 鉴权服务器收到客户身份信息后，向客户端设备发送证书 3. 客户端设备将该服务器识别为授权服务器，并提交用户证书进行验证 4. 客户端设备和鉴权服务器生成成对主密钥（PMK）和成对临时密钥（PTK） 5. 鉴权在客户端设备与接入点之间通过四路交接完成 6. AES 加密密钥来自 PTK，以对客户端设备与接入点之间交换的数据进行加密	1. 客户端设备联合接入点。客户端设备和接入点核实它们拥有相同的 PSK 2. 鉴权在客户端设备与接入点之间通过四路交接完成 3. 在四路交接中，PSK 被用于在客户端设备和接入点生成 PTK。 4. PTK 包括用于保护客户端设备与接入点之间所交换的数据的 AES 密钥

表 4 WPA2 企业版和 WPA2 个人版

采用AES的CCMP加密

IEEE 802.11i 和 WPA2 要求使用 CCMP 加密协议，该加密协议使用 AES 为加密和完整性保护采用相同的密钥。AES 是采用多种密钥长度和块大小的分组密码。IEEE 802.11i 和 WPA2 要求使用带 128 位密钥和 128 位块的 AES。AES 加密密钥来自使用四路交接的 PTK，基于 IEEE 802.11i 密钥管理协议。

在 WPA2 中纳入 AES，为 Wi-Fi 用户带来经过最广泛测试、运用最广的加密标准之一。如今，AES 被用于多种数据传输技术，并经过了密码学家们的严格审查。

Wi-Fi保护设置

Wi-Fi 保护设置作为可选认证项目，于 2007 年推出，以简化家庭和小型办公网络中 WPA2 的配置和激活（图 1）。到 2009 年 8 月，已有 700 多款产品通过了 Wi-Fi 保护设置认证。虽然 2006 以来接受测试的所有 Wi-Fi CERTIFIED 设备都支持 WPA2，但 WPA2 必须经过配置和激活，设备用户才能从中受益。如果需要的话，Wi-Fi 保护设置允许住宅和小型企业用户跳过详细的 WPA2 配置步骤，而且他们也不必手动输入 PSK，就能利用 WPA2 保护自己的网络。

图 1 Wi-Fi 保护设置标识帮助用户鉴别设备是否支持 Wi-Fi 保护设置

通过 Wi-Fi 保护设置，用户在设置 WPA2 方面拥有多重选择：

- **个人识别号码（PIN）：**用户输入数码。针对接入点和客户端设备的强制性要求。
- **按钮配置（PBC）：**用户在接入点和相关客户端设备上按下按钮。针对接入点的强制性要求，针对客户端设备的非强制性要求。
- **近场通信（NFC）令牌：**使用 NFC 令牌，或使接入点与客户端接触。非强制性要求。

Wi-Fi Alliance 计划扩大 2010 年测试的 Wi-Fi 保护设置认证，以纳入 ad-hoc 模式。

Wi-Fi CERTIFIED Makes It Wi-Fi

选择 Wi-Fi CERTIFIED 的优势

图 2：Wi-Fi 设备的外包装上带有 Wi-Fi CERTIFIED 标志，方便用户选择

自 2000 年以来，Wi-Fi Alliance 认证项目在建立无线局域网设备之间的可互操作性方面，发挥了积极主要作用，实现了卓越的用户体验，扩展了 Wi-Fi 功能，提升了 Wi-Fi 性能。

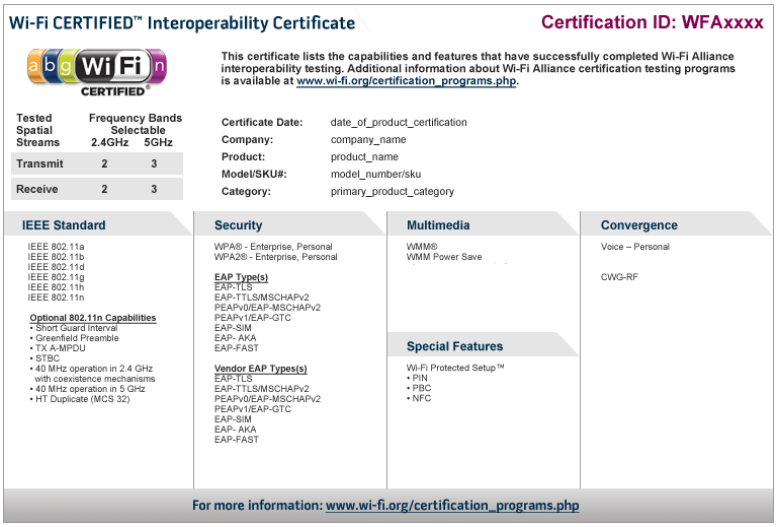

图 3 Wi-Fi 可互操作性证书列出了每个设备或接入点所支持的特性

Wi-Fi Alliance 的这些努力有助于扩大 Wi-Fi 的应用范围，确保 Wi-Fi CERTIFIED 产品成为全球知名和值得信赖的品牌。在选择新的设备或接入点时，用户会有意识的寻找 Wi-Fi CERTIFIED 标志。因为这一标志让他们相信，他们购买的产品能与任何其他厂商生产的 Wi-Fi CERTIFIED 的设备兼容。全球 Wi-Fi 设备制造商将他们的产品发送到 Wi-Fi Alliance 授权测试实验室（ATL）进行认证。

迄今为止，已有近 6000 多种产品完成认证，其中支持 WPA2 的逾半数。IEEE 802.11n 标准认证计划是非常成功的，支持这一标准的产品超过了 600 个。增长最快的是移动电话，已经有超过 375 个型号的移动电话完成了 Wi-Fi CERTIFIED 认证。

图 4 www.wi-fi.org 网站上的 Wi-Fi CERTIFIED 产品数据库

Wi-Fi 认证项目满足了不同设备对于外形的需求、给供应商以多种选择，从而满足市场需求（图 3）。有些 Wi-Fi 认证项目因为涉及最基本的 Wi-Fi 功能，所以必须通过验证，除此之外的其他项目则是可选的。

目前依然在进行中的 Wi-Fi 认证项目（星号表示可选项目）包括：

- 可互操作性及标准规则： **IEEE 802.11a, IEEE 802.11b, IEEE 802.11g 和 IEEE 802.11n***
- 安全 **：WPA2 个人版，支持 EAP 的 WPA2 企业版*，Wi-Fi Protected Setup***
- 语音 Wi-Fi： **Voice Personal***
- 借助服务质量(QoS)的应用支持 **Wi-Fi 多媒体 ™ * (WMM®)**

- 用于移动设备的节电项目： **WMM Power Save***
- Wi-Fi 和蜂窝融合： **融合无线组无线电频率（CWG-RF）概要***

Wi-Fi 安全现状

有了 WPA2，Wi-Fi CERTIFIED 设备可为全球各地的企业、家庭及移动用户使用的各种设备提供先进的安全工具。所有的新设备和新接入点都支持 WPA2，越来越多的 Wi-Fi 用户开始习惯天天使用 WPA2 功能。

如今，Wi-Fi 已成为许多企业的默认网络接入技术。许多企业的内部 IT 政策规定，必须使用 WPA2 协议，因为 WPA2 已获得广泛认可，可以保护网络以及通过 Wi-Fi 无线连接传输的机密信息。随着 Wi-Fi 技术在不同应用和多种类型的设备上使用越来越普遍，Wi-Fi 网络的安全日益成为企业整体安全策略中不可或缺的一部分。IEEE 802.1X 及 AES 等多接点技术的采用，使得 Wi-Fi 与企业 IT 基础设施之间的结合更加紧密。在美国德克萨斯大学达拉斯分校进行的案例研究表明，WPA2 可以在不增加网络复杂性的基础上融入已有的网络设施，确保无线局域网的安全。

而在家庭网络中， 用户可应用 Wi-Fi Protected Setup 搭建新网络，添加设备到现有网络，激活 WPA2。越来越多的 Wi-Fi 用户开始意识到使用网络连接技术时安全的重要性，他们希望无需惊动公司的 IT 人员或花费较多时间学习复杂的安全机制就可以实现强大的数据保护。在家庭网络中，启用 WPA2 通常只需要几分钟，用户也只需要输入一个足够复杂的密码。与安装防火墙、使用 VPN，或安装防病毒软件相似，启用 WPA2 已经成为连接家庭及公共热点中保护用户数据不可缺少的安全措施。

Wi-Fi Alliance 将继续推动安全方面的技术革新，并致力于将未来技术进步纳入到 Wi-Fi CERTIFIED 项目中来。现有的 Wi-Fi 技术已经相当成熟，可从 WPA2 技术的革新中充分获益。自 2006 年以来，所有经过 Wi-Fi CERTIFIED 认证的设备（超过 3000 种）都必须支持 WPA2。WPA2 已成为一个全球标准，在企业及家庭网络中得到了广泛应用。WPA2 有助于保护住宅、企业及热点网络免受来自黑客的诸如中间人攻击、虚假验证、虚假答复、密码冲突、防护能力低的密码、虚假包，以及病毒攻击等类型的威胁。WPA2 为 Wi-Fi CERTIFIED 设备用户提供了可靠的安全保障， 并提升了 Wi-Fi 使用的可靠性、信任度和安全性。

案例分析：德州大学达拉斯分校

应用 WPA2 为覆盖全校的 Wi-Fi 网络提供保障

德州大学（UT）达拉斯分校约有 15000 名学生及 2500 名教师及工作人员，分布在三个校区的 29 栋楼里面。德州大学达拉斯分校拥有独特的传统，该校的建立要归功于德州仪器的创立者，他们在 60 年代初发现本地区面临科学及工程技术的匮乏，因此成立了一个研究中心，以吸引全国范围内最优秀的科技人才。这个早期的人才中心最终在 1969 年成立为大学，并成为德州大学系统的一部分。今天，德州大学达拉斯分校已拥有 7 个有学位授予权点的学院，开设的科系超过 125 个。对于大学的研究任务以及学生的生活质量来说，Wi-Fi 网络都是至关重要的。

该大学使用无线局域网的历史已久，最初部署的是专用接入点（未使用 Wi-Fi 技术），之后将网络升级到 802.11b 标准，而后再次升级为 802.11a/g 标准。通过最近的升级，学校形成一个包含 450 个双无线接入点的网络，接入点和用户由五个网络控制器管理。学生将这一网络看做一种设施，用来接入国际互联网，进行在线测试，以及进行互联网语音通话(VoIP)。在无线局域网之上，该网络接入了多个更广的网络。通过北德州 Gigapop(一个科研院所互助协会），该网络连接到 Internet2 教育科研网。此外该网络还通过德州大学电信系统办公室连接到另外一个商业网络。仅无线网络的平均吞吐量就超过 50Mbps。

相对于有线以太网，无线网络对于安全的要求更高。因此，该校需要的是一个具有极好加密特性，又不会带来额外管理负担的网络系统。“我们正在寻找一个统一而安全的网络，不想增加工作人员来管理网络。”该校软件系统专家 Bruce Nunn 介绍说：“因为目前还没有专人负责无线网络安全，所以我们需要的网络系统，应尽可能多的重用现有的有线基础设施，特别是与验证相关的设施。”

学校最终选择了 Meru 系统，该系统支持 WPA2 企业版，可满足学校需求。WPA2 可与远程认证拨号用户服务（RADIUS）验证系统互用，方便无线网络连接学校的轻量目录访问协议（LDAP）数据库。用户使用 IEEE 802.1X 进行身份验证，会自动获得一个加密性好的 AES 密钥。加密对用户和 IT 部门是完全透明的，而身份验证使用的是与有线网络相同的客户端和服务器端软件。

学校使用无线网络之后，出现了许多新的应用。其中之一便是来宾访问。来宾访问也带来了具体的安全问题。来宾不属于内部用户，因此不能通过 RADIUS 数据库验证，同时依然需要保证网络的安全。Nunn 表示：“有了 WPA2，访客可使用单独的 SSID 进行安全访问。他们无需进行 IEEE 802.1X 认证，但必须接受强制网络门户的网络使用政策，而且只能访问互联网。”

SHARP. San Diego's Health Care Leader

案例分析：Sharp HealthCare

保护多设备环境下的敏感病患数据

拥有 1.1 万名员工的综合区域卫生医疗系统 Sharp HealthCare 为美国圣迭戈县 300 多万居民提供各种卫生医疗设施与服务。为提高医疗质量，Sharp 部署了 Wi-Fi 网络，覆盖 7 家医院和 40 家诊所，面积逾 50 平方英里。Sharp HealthCare 无线环境的建立起初受三个因素驱动：

1. 移动小车上电子病历（EMR）系统的部署，用于获取病患收治数据、病史和化验结果

2. 新型创新移动应用，如配备 Wi-Fi 的静脉注射（IV）泵，远程保护患者用药

3. 从医院工作人员在医院各处医治患者时偏爱使用的手持装置的高效率中受益

WLAN 必须支持同时保护无线连接、数据、核心网络和用户的多层安全解决方案。《健康保险携带和责任法》（HIPAA）中规定的美国政府患者保密新标准要求医院须保护患者病历及其它数据的无线传输。

Sharp 与 Aruba 合作，采用了带 AES 的 WPA2 以及 IEEE 802.1X 和 PEAP。Sharp HealthCare 网络管理员 Randy van Sickle 表示："对于卫生医疗提供者来说，保护患者数据，至关重要。对于 Sharp HealthCare 来说，WPA2 是显而易见的选择。WPA2 提供最佳安全性，且不会造成性能负担。"

Wi-Fi 网络支持不同安全等级的多种应用，包括免费提供患者接入。为防止病毒和潜在的网络误用，连接开放有线端口的访客在通过强制门户接入网络之前，会被要求进行鉴权。然后根据接入政策，鉴权用户可访问某些资源，而非鉴权用户则仅限于接入互联网。一个 SSID 可支持唯一用户组，各用户组有不同的鉴权要求以及接入控制。为简化配置管理，多个 VLAN 可对应一个 SSID，但用不同的政策规定各用户组的接入特权。

作为 WLAN 技术的早期采用者，Sharp 支持很多 Wi-Fi 客户端，从笔记本电脑到极其精密的医疗设备，等等。这些设备不但包括笔记本电脑，还包括 1200 种无线静脉输注泵、药房使用的无线打印机、手持扫描仪、可对无法移动的患者进行 x 光扫描的移动放射装置以及与手持设备相连以便监控的训练机等。最近，Sharp 启动了一项试验，通过中心站无线监控患者心率，并实时更新病历。

向 WPA2 的过渡平稳顺利，对用户透明，但需要与一些厂商进行协调。一开始，Sharp 就将所有接入点升级到了 WPA2。到 2010 年，Sharp 预计将使所有无线设备都支持 WPA2。在新设备支持 WPA2 的同时，Sharp 还须继续支持已经投入使用的老设备。van Sickle 补充道："WPA2 是基于标准的解决方案，这个事实至关重要，因为在医疗设备厂商也在相同时间向 WPA2 过渡的过程中，这使 Sharp 容易与他们进行软件升级协调。"





缩略语

3G	第三代网络标准
AAA	鉴权、授权和记账
AES	高级加密标准
ATL	授权测试实验室
CCMP	密码块链信息认证码协议
CWG-RF	融合无线组无线电频率
EAP	可扩展认证协议
EAP-AKA	EAP 认证和密钥协议
EAP-FAST	EAP-通过安全隧道灵活鉴权
EAP-GTC	EAP -通用令牌卡
EAP-SIM	EAP -用户识别模块
EAP-TLS	EAP -传输层安全
EAP-TTLS	EAP -隧道 TLS
FIPS	联邦信息处理标准
GSM	全球移动通信系统
IEEE	美国电气和电子工程师协会
IETF	互联网工程任务组
LDAP	轻量级目录访问协议
MAC	媒体访问控制[层]
MSCHAPv2	微软质询握手身份验证协议 版本 2
NFC	近场通信
PBC	按钮配置
PEAP	受保护的 EAP
PIN	个人识别号码
PMK	成对主密钥
PSK	预共享密钥
PTK	成对瞬时密钥
RADIUS	远程认证拨号用户服务
RC4	Rivest 密码法 4
SIM	用户识别模块
SSID	服务区标识符
TKIP	临时密钥完整性协议
UMTS	通用移动通信系统
VoIP	互联网语音协议
VPN	虚拟专用网
WLAN	无线局域网
WMM ®	Wi-Fi 多媒体™
WPA ®	Wi-Fi 受保护访问 ®
WPA2 ®	Wi-Fi 受保护访问 2 ®

关于 Wi - Fi Alliance

Wi-Fi Alliance 是一家国际非营利性行业协会，拥有数百家成员公司，共同致力于推动无线局域网（WLAN）的增长。Wi-Fi Alliance 在技术开发、市场建设以及管理项目方面的不懈努力，促进了 Wi-Fi 在全球的应用。

Wi-Fi CERTIFIED™项目始于 2000 年 3 月。该项目提供的可互操作性和质量标准得到广泛认可，可帮助 Wi-Fi 产品实现最佳用户体验。迄今为止，已经有超过 6000 种产品获得了 Wi-Fi CERTIFIED™指定认证标志，有力地拓展了 Wi-Fi 产品和服务在各个新兴和成熟市场的应用范围。

欲了解更多 Wi-Fi 安全及 Wi-Fi Alliance 认证项目的信息及下载白皮书，请访问 www.wi-fi.org