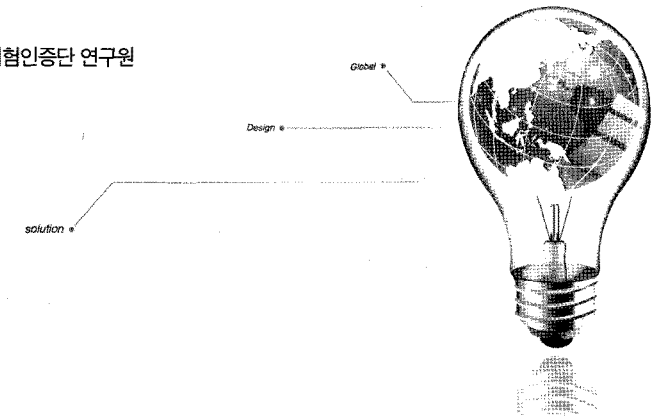
Wi-Fi CERTIFIED™ 인증 프로그램 소개

임 유 락 TTA 시험인증연구소 네트워크시험인증단 연구원



1. 머리말

Wi-Fi CERTIFIED™ 인증프로그램은 Wi-Fi Alliance의 Task Group(TG)에서 상호운용성과 역호환성 검증을 위한 시험 인증 규격을 만들어 ATL(Authorized Test Laboratory)을 통해 제공하여 운영되고 있다.

국내에서는 2009년 스마트폰 열풍과 더불어 대중적으로 Wi-Fi 기술에 대한 관심이 증대되고 있다. 스마트폰에서 시작된 Wi-Fi에 대한 관심은 개인 휴대기기뿐만 아니라 생활가전 제품 등에도 확산되어 거대한 시장이 형성되어가고 있다. Wi-Fi CERTIFIED™ 프로그램이 강제성을 가진 인증 프로그램이 아님에도 불구하고 사용자의 제품에 대한 상호운용성 및 성능에 대한 기대치가 높아짐에 따라 국내 제조사들은 Wi-Fi CERTIFIED™ 인증 프로그램에 대해 높은 관심을 갖고 있으며 시험 수요도 증가하고 있다. 본 고에서는 Wi-Fi CERTIFIED™ 인증 프로그램을 소개한다.

2. Wi-Fi CERTIFIED™ 인증 프로그램

Wi-Fi CERTIFIED™의 역사는 1999년 WECA (Wireless Ethernet Compatibility Alliance)라는 조직이 결성되어 Wi-Fi라는 브랜드를 만들며 시작되었다. 당시 기존의 802.11에 비해 고속 통신이던 802.11b 표준이 정식 발표되면서 WECA는 802.11 제품에 대한 시험과 인증 업무를 시작했다. WECA는 2002년 Wi-Fi Alliance로 조직명을 변경하고 이후 현재까지 Wi-Fi Alliance는 멤버들의 TG 활동을 통해 다양한 시험 인증 규격을 제안하고 인증 규격을 바탕으로 인증 프로그램 운영하여 Wi-Fi CERTIFIED™로고가 새겨진 제품의 신뢰성을 보장하고 있다.

2.1 WPA™/WPA2™

WPA™/WPA2™(Wi-Fi Protected Access)는 IEEE 802.11i 기반의 보안 기술을 말한다. Wi-Fi Alliance는 기존 WEP(Wired Equivalent Privacy) 보안 방식의 단점을 보완하는 WPA™를 도입한다. 기존의 WEP

방식이 스니핑(sniffing)을 통해 RC4키가 노출되는 단점이 대두되면서 이를 보완한 TKIP(Temporary Key Integrity Protocol)와 CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) 방식이 IEEE 802.11i에 제안된다.

TKIP은 WEP기반의 하드웨어를 펌웨어 업그레이드만을 통해 재사용 할 수 있고 WEP방식의 고정된 키 값을 temporal key로 변경해 보안 성능을 높였지만 여전히 해킹을 통해 RC4 키가 노출되는 단점이 있다. CCMP는 암호화 방식을 기존의 RC4가 아닌 AES(Advanced Encryption Standard)를 사용해 WEP과 TKIP에서 발생되는 보안키 유출을 차단하여 보안성능을 높인 방식이다.

Wi-Fi Alliance는 IEEE 802.11i 표준 기반의 TKIP과 CCMP를 적용해 WPA™와 WPA2™ 기술을 제안하고 이에 대한 인증 프로그램을 만들었다. WPA™는 TKIP을 적용한 보안기술이고, WPA2™는 CCMP-AES를 적용한 보안기술이다. WPA™와 WPA2™는 암호화 방식에 따라 구분되며 이는 다시 EAP(Extended Authentication Protocol)의 사용 여부에 따라 Personal과 Enterprise로 구분된다.

WPA™-Personal과 WPA2™-Personal은 PSK(Pre Shared Key)를 통해 사용자 인증을 하며 보통 가정이나 소규모 오피스 등에 적용한다. WPA™-Enterprise와 WPA2™-Enterprise는 EAP를 통해 Authentication Server가 인증 권한을 가지며 다양한 EAP 방식에 대한 인증 프로그램이 지원되고 있다. Wi-Fi CERTIFIED™ 인증 프로그램을 통해 EAP-TLS, EAP-TTLS, PEAPv0, PEAPv1, EAP-SIM, EAP-AKA, EAP-FAST 등 총 7가지의 EAP 방식에 대해 인증이 가능하다.

WPA2™ 인증 프로그램에서는 제품의 보안 기능에 대한 상호운용성 시험뿐만 아니라 802.11a/b/g 각 모드에서의 상호운용성, 802.11d(Regulatory Domain), 802.11h(Spectrum and Transmit Power Management) 등의 검증도 함께 진행된다.

〈표 1〉 Wi-Fi CERTIFIED™ 보안 인증 프로그램

보안 인증 프로그램	보안 방식	인증 방식
WEP	WEP (40/104bit key)	WEP Key
WPA™-Personal	TKIP	PSK
WPA™-Enterprise	TKIP	802.1x EAP
WPA2™-Personal	AES	PSK
WPA2™-Enterprise	AES	802.1x EAP

Wi-Fi Alliance는 보안이 취약한 WEP과 WPA™(TKIP)에 대한 인증 프로그램을 2014년까지 단계적으로 폐지할 계획에 있다.

2.2 WMM® & WMM Power Save

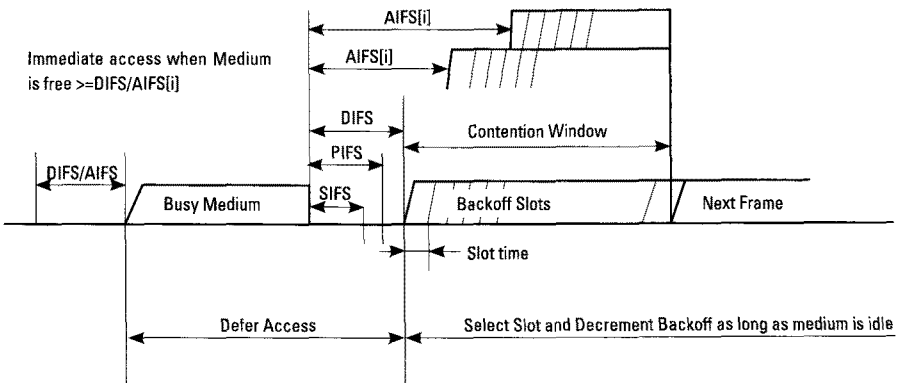
WMM®(Wi-Fi Multimedia)은 IEEE 802.11e 기반의 QoS 기능에 대한 상호운용성 검증을 위해 제안된 인증 프로그램이다. IEEE 802.11e는 EDCA(Enhanced Distributed Coordination Function Channel Access, HCCA(Hybrid Coordination Function Controlled Channel Access) 두 가지의 QoS 방식을 제안한다. Wi-Fi Alliance는 이 중 EDCA를 도입하여 WMM® 시험 인증 규격을 만들어 제품의 QoS 기능에 대한 제품 간 상호운용성을 검증한다.

EDCA는 트래픽을 4개의 AC(Access Category)로 태깅(tagging)하여 각 트래픽의 AC에 따라 차별적으로 TXOP(Transmission Opportunity)를 주어 QoS를 구현했다. 각 AC에 대해 CW(Contention Window) 구간과 AIFSN을 차별적으로 적용하여 우선 순위가 높은 트래픽이 채널 획득 경쟁에서 우선적으로 채널을 획득할 수 있도록 구현되어 있다.

WMM Power Save 인증 프로그램에서는 IEEE 802.11e에서 제안한 APSD(Automatic Power Save Delivery) 방식을 적용한 제품에 대한 상호운용성을 검증한다. APSD 전원관리 방식은 기존의 802.11의 Power Save Polling 방식에 비해 더욱 효율적으로 전

〈표 2〉 WMM 액세스 카테고리

Access Category	AC	CWmin	CWmax	AIFSN	TXOP Limit (802.11b)	TXOP Limit (802.11a/g)
Best Effort	AC_BK	aCWmin	aCWmax	7	0	0
Background	AC_BE	aCWmin	4x(aCWmax+1)-1	3	0	0
Video	AC_VI	(aCWmin+1)/2 -1	aCWmin	1	6.016ms	3.008ms
Voice	AC_VO	(aCWmin+1)/4 -1	(aCWmin+1)/2 -1	1	3.264ms	1.504ms



[그림 1] IFS에 따른 CW 차이

원을 관리한다. WMM Power save 기능은 특히 VoIP 폰이나 모바일 폰과 같이 사용시간에 비해 대기시간이 긴 제품 군에 대해 효과적이며, 대기시간을 획기적으로 늘려주는 효과가 있다.

2.3 WPS(Wi-Fi Protected Setup™)

WPS 프로토콜은 무선 네트워크의 보안 설정 과정을 간편화 시키려는 목적으로 만들어졌다. 따라서 WPS는 Wi-Fi Simple Configuration로도 표현된다. WPS 프로토콜에서는 네트워크 상에 존재하는 디바이스들을 논리적 역할에 따라 〈표 3〉과 같이 구분했다.

〈표 3〉 WPS의 역할에 따른 장치 구분

타입	역할
Registrar	네트워크에 참여할 수 있는 credential (인증서)를 제공하는 디바이스
Enrollee	네트워크에 참여하고자 하는 디바이스
AP	Registrar와 Enrollee 사이에서 AP기능을 하는 디바이스

또 인증에 사용되는 네트워크를 기준으로 WLAN을 통해 인증되는 In-band Method과 NFC, USB 등 타 네트워크를 통해 인증되는 Out-band Method로 구분할 수 있다. In-band Method의 방법으로 PIN Method와 PBC(Push Button Configuration) Method가 있고, Out-band Method으로는 NFC(Near Field Communication)과 USB(Universal Serial Bus)가 있다. WPS 기능 탑재를 위해서는 PIN과 PBC는 반드시 구현해야 하고 NFC와 USB 등의 Out-Band Method는 선택적으로 구현할 수 있다. 현재 Wi-Fi CERTIFIED™ 인증이 가능한 WPS의 인증 프로토콜은 PIN, PBC, NFC 세 가지가 있다.

Wi-Fi Protected Setup™은 Wi-Fi CERTIFIED™ 로고와는 별도로 인증 제품에 한하여 [그림 2]의 로고를 사용할 수 있다.

2.4 Wi-Fi CERTIFIED n

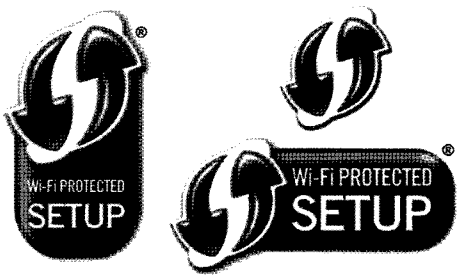
2009년 9월 802.11n 규격이 정식 릴리즈 되면서 Wi-Fi Alliance에서는 기존의 11n 드래프트 시험규격을 11n으로 개정했다. 11n 인증 프로그램을 통해 기존 802.11a/b/g에서 개선된 PHY, MAC 기능들에 대한 시험을 통해 제품의 상호운용성에 대한 검증이 가능하다. 11n 인증 프로그램에서는 11n 제품에 대한 Mixed 802.11b/g 상호운용성 시험, Association & Throughput 시험 등 기존 버전들과의 호환성에 대한 검증을 하며 A-MPDU Aggregation, STBC, 20/40MHz roaming, 20/40MHz Coexistence, 3 Spatial Streams, Block Ack, HT Greenfield, Short Guard Interval 등 11n에서 새롭게 적용된 기능들과 환경들에 대한 시험이 진행된다.

2.5 Voice over Wi-Fi Personal

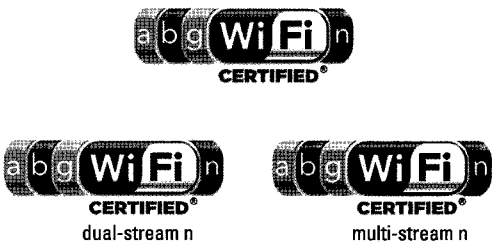
Voice Personal 인증을 받기 위해서는 인증 대상 제품은 WMM과 WPA2™-Personal을 지원하고 AP는 추가적으로 WMM Power Save를 지원해야 한다. Voice Personal 인증 시험에서는 Packet Loss, Latency, Jitter 등 통화품질과 관련된 성능 검증이 진행된다. 〈표 4〉

2.6 CWG-RF

CWG-RF 인증 프로그램은 CTIA와 Wi-Fi Alliance가 공동으로 제안하여 Wi-Fi와 이동통신 기술이 탑재된 제품에 대해 Wi-Fi에 대한 RF 성능을 확인하는 것이 목적이다. 시험은 전송전력과 수신감도에 대해 전도시험과 방사시험(TRS, TIS)으로 각각 진행되고 방사시험에 한하여 Cellular Desense 항목이 진행된다. CWG-RF에서는 시험결과에 대해 PASS/FAIL에 대한 판정은 하지 않으며 측정된 결과치를 기록해 성적서를 제공한다. CWG-RF는 Wi-Fi CERTIFIED와는 별도로 CWG 인증시험소에서 진행되며 전 세계 17곳의 시험소가 있다. 〈표 5〉



[그림 2] Wi-Fi Protected Setup 로고



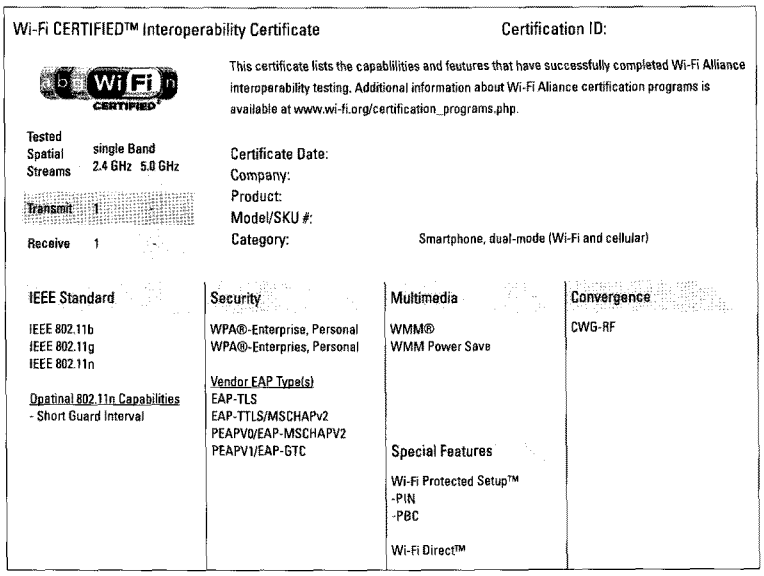
[그림 3] Wi-Fi CERTIFIED™ n 로고

〈표 4〉 Voice Personal 성능 기준

항목	기준
One way Delay	50ms 미만
Maximum Jitter	50ms 미만
Packet Loss	1% 미만
Consecutive Lost Packet	3개 미만

〈표 5〉 CWG-RF 시험 측정항목

측정항목	
TX	Conducted Power Output
	TRP(Total Radiated Power)
RX	Conducted Receiver Sensitivity
	TIS(Total Isotropic Sensitivity)
Desense	Radiated Receiver Sensitivity (Wi-Fi Desense)
	Radiated Receiver Sensitivity (Cellular Desense)



Wi-Fi CERTIFIED™ Interoperability Certificate Certification ID:

This certificate lists the capabilities and features that have successfully completed Wi-Fi Alliance interoperability testing. Additional information about Wi-Fi Aliance certification programs is available at www.wi-fi.org/certification_programs.php.

Tested Spatial Streams: single Band 2.4 GHz 5.0 GHz
Transmit 1
Receive 1

Certificate Date:
Company:
Product:
Model/SKU #:
Category: Smartphone, dual-mode (Wi-Fi and cellular)

IEEE Standard	Security	Multimedia	Convergence
IEEE 802.11b IEEE 802.11g IEEE 802.11n Opatinal 802.11n Capabilities - Short Guard Interval	WPA®-Enterprise, Personal WPA®-Enterprises, Personal Vendor EAP Type(s) EAP-TLS EAP-TTLS/MSCHAPv2 PEAPV0/EAP-MSCHAPV2 PEAPV1/EAP-GTC	WMM® WMM Power Save Special Features Wi-Fi Protected Setup™ -PIN -PBC Wi-Fi Direct™	CWG-RF

[그림 4] Wi-Fi CERTIFIED™ 인증서

2.7 Wi-Fi Direct™

2010년 10월 Wi-Fi Alliance는 Wi-Fi Direct™에 대한 인증 프로그램을 런칭한다. Wi-Fi Direct란 AP를 통하지 않고 장치 간 상호 통신이 가능한 기술이다. 장치 간 상호통신은 1:1 통신은 물론 1:n 통신도 가능하다. 이를 위해서 AP는 아니지만 AP 역할을 하는 장치가 필요하며 Wi-Fi Direct에서는 이 AP-like 장치를 P2P Group Owner로 지정한다. P2P Group Owner는 주변의 장치들의 정보를 수집하여 직접 1:1 통신의 독립체가 되거나 1:n 통신에서의 허브역할을 한다. Wi-Fi Direct™는 Wi-Fi Protected Setup™을 강제적으로 지원하도록 하여 간단한 연결과 보안 성능을 갖도록 구현했다. Wi-Fi Direct™에서는 장치를 논리적 역할에 따라 두 가지로 구분한다.

〈표 6〉 Wi-Fi Direct™의 역할에 따른 장치 구분

역할	기능
P2P Group Owner	- "AP-like" device - WPS Registrar 역할
P2P Client	- Non-AP STA 역할 - WPS Enrollee 역할

Wi-Fi Direct™ 인증을 위해서 해당 제품은 WFA2와 WMM(or 11n CERTIFIED), Wi-Fi Protected Setup™을 지원해야 하며, Wi-Fi Direct를 지원하는 P2P Device는 data 전송에 802.11b 기술을 사용할 수 없다.

Wi-Fi Direct™ 기술이 상용화되고 본격적으로 인증프로그램의 운영됨에 따라 2011년부터 Wi-Fi Direct™ 기술이 탑재된 제품들이 시장에 많이 출시될 것으로 예상된다.

3. 맺음말

본 고에서는 최근 국내에서 관심이 증폭되고 있는 Wi-Fi 기술에 대한 인증 프로그램인 Wi-Fi CERTIFIED™에 대해 간략히 살펴보았다. Wi-Fi을 탑재한 다양한 제품 군이 시장에 출시되면서 제품의 품질에 대한 사용자의 기대와 관심도 커지고 있다. 제조사는 Wi-Fi CERTIFIED™ 인증 프로그램을 통해 사용자에게 제품의 품질에 대한 신뢰도를 높일 수 있을 것으로 생각된다. TTA