Australian Competition & Consumer Commission

GPO Box 3131
Canberra ACT 2601

23 Marcus Clarke Street
Canberra ACT 2601

tel: (02) 6243 1111
fax: (02) 6243 1199

www.accc.gov.au

Our Ref: CTM1473145
Contact Officer: Joanne Palisi
Contact Phone: 02 6243 1323

26 February 2015

The Registrar of Trade Marks
IP Australia
PO Box 200
WODEN ACT 2606

By email: fep@ipaustralia.gov.au

Dear Registrar

Certification Trade Mark (CTM) Application No. 1473145
– Wi-Fi Alliance – WI-FI CERTIFIED PASSPOINT

The Australian Competition and Consumer Commission (the **ACCC**), in accordance with the provisions of the *Trade Marks Act 1995*, has completed its final assessment of Certification Trade Mark (CTM) No. 1473145 (WI-FI CERTIFIED PASSPOINT) lodged by Wi-Fi Alliance.

A certificate detailing the ACCC's assessment is attached, as is a certified copy of the CTM rules. The applicant has been notified.

If you have any inquiries about this matter, please contact Monica Lay on 02 6243 1270.

Yours sincerely

Joanne Palisi
Director
Coordination and Strategy Branch
Merger and Authorisation Review Division

Australian Competition & Consumer Commission

Final Assessment of Certification Trade Mark application 1473145 – Wi-Fi Alliance – WI-FI CERTIFIED PASSPOINT

The Australian Competition and Consumer Commission (ACCC), in accordance with the requirements of the *Trade Marks Act 1995*, has completed its Final Assessment of the above Certification Trade Mark (CTM) application.

The ACCC's Final assessment is that it is satisfied that:

(a) the approved certifiers demonstrate the attributes necessary to competently certify the products in respect of which the CTM is to be registered;

(b) the rules governing the use of the CTM would not be to the detriment of the public; and

(c) the rules governing the use of the CTM are satisfactory having regard to the principles relating to restrictive trade practices set out in Part IV of the *Competition and Consumer Act 2010* (the CCA) and the principles relating to unconscionable conduct (Part 2-2), unfair practices (Part 3-1), and safety of consumer goods and product related services (Part 3-3) in Schedule 2 (Australian Consumer Law) of the CCA.

Signed.....Michael Sleaper.....**(Deputy Chair)**

Date.....25 February 2015.....

CERTIFICATION MARK CRITERIA FOR WI-FI CERTIFIED PASSPOINT CERTIFICATION MARK

1. WHO IS AUTHORIZED TO USE THE MARK?

Wi-Fi Alliance members in good standing whose products have successfully completed certification testing under the Wi-Fi CERTIFIED PASSPOINT program may use the mark in connection with the products that have been certified.

2. THE CHARACTERISTICS THAT THE MARK IS CERTIFYING

The Wi-Fi CERTIFIED PASSPOINT mark certifies that the products with which the mark is used have completed testing for interoperability of devices and to ensure that they manage network association, authentication, sign-up, and security for public wireless hotspot connectivity as a transparent, background function.

3. HOW THE CERTIFYING BODY TESTS FOR THOSE CHARACTERISTICS

Products submitted for testing and certification under the Wi-Fi CERTIFIED PASSPOINT program are tested at one of the following independent testing laboratories according to the Hotspot 2.0 Technical Specification developed by the Wi-Fi Alliance (and available at https://www.wi-fi.org/knowledge-center/published-specifications):

- **Allion Test Labs, Inc. (Taiwan)** - Allion Test Labs, Inc. is the world leading Information Technology (IT) testing organization to conduct testing services in multiple regions of Asia and North America.
- **AT4 wireless (Spain)** - AT4 wireless provides conformance and regulatory testing, international compliance services, test systems for radiofrequency, protocols and interoperability, training and consultancy in wireless technologies.
- **Bureau Veritas ADT (Taiwan)** - Bureau Veritas ADT, a subsidiary of Bureau Veritas, provides comprehensive services including consulting for related test requirements, detailed testing, and certification process.
- **CETECOM (USA, Germany)** - a subsidiary of RWTÜV AG with headquarters in Essen (Germany), is a worldwide leading provider in testing and certification services for the mobile communications and wireless industry with several state-of-the-art testing laboratories in Europe, USA and Asia.
- **SGS Group (Taiwan, Japan, Korea)** - The SGS Group is the global leader and innovator in inspection, verification, testing and certification services. With more than 46,000 employees, SGS operates a network of over 1,000 offices and laboratories around the

world.

- **Shenzhen Institute of Telecommunications (SIT) (China)** - The Shenzhen Institute of Telecommunications is a leading high-tech, objective and independent third-part test institute, accredited by CNAS, DAKKS, and CTIA.

- **State Radio_monitoring_center Testing Center (SRTC) (China)** - The State Radio_monitoring_center Testing Center (SRTC) is a global testing and calibration laboratory with 13 domestic and foreign authority certifications and qualification accreditations that provide a variety of testing services in according with a variety of certification programs. SRTC has a first-class testing environment, equipment, scientific quality management system, professional technicians and excellent technical capabilities.

- **TA Technology (China)** - TA Technology (Shanghai) Co, Ltd. is a global certification and test service provider in Shanghai, China, specializing in communications product testing. TA was founded in 2002, and became a Wi-Fi Alliance Authorized Test Laboratory in August, 2008.

- **Telecommunication Metrology Station (TMC) (China)** - China National Telecommunication Metrology Station is a leading high-tech research and test laboratory providing open services on products inspection, verification and technical assessment as well as testing instrument metrology.

- **Telecommunications Technology Association (TTA) (Korea)** - TTA is an information technology (IT) standards organization that provides one-stop services for the establishment of IT standards and provides testing and certification for IT products. The testing and certification services cover the full suite of international and domestic standards and encompass a wide range of products related to the telecommunication industries such as digital broadcasting and mobile communication equipment and terminals as well as computer networking hardware and software.

- **TÜV Rheinland Group (USA, Japan, Korea)** - The TÜV Rheinland Group is a leading international technical service provider, with a mission of sustainable development of safety and quality. With headquarters in Cologne the TÜV Rheinland Group market activities are concentrated especially in the six fields of Industrial Services, Mobility, Products, Life Care, Education and Consulting and Systems.

- **Wipro Technologies (India)** - Wipro Technologies, a division of Wipro Limited (NYSE:WIT) is one of the largest product engineering and support service providers worldwide, providing comprehensive research and development services, IT solutions and services, including systems integration, Information Systems outsourcing,

package implementation, software application development and maintenance services to corporations globally.

4. HOW USE OF THE MARK IS SUPERVISED

The Wi-Fi Alliance polices the marketplace and identifies unauthorized uses of its certification marks, pursuing legal action under the intellectual property laws of the relevant jurisdiction, if necessary, to stop the unauthorized use. Misuse of a Wi-Fi Alliance certification mark by a Wi-Fi Alliance member can result in termination of membership.

5. HOW THE MARK IS USED

The Wi-Fi CERTIFIED PASSPOINT mark may be used only in connection with products that have successfully passed interoperability testing performed at a designated independent test facility and may only be used by companies that have been granted a usage license by the Wi-Fi Alliance.

The mark may be used on products, packaging, and associated promotional materials. Once a license is granted for use of the Wi-Fi CERTIFIED PASSPOINT mark, the authorized user may reproduce the mark in accordance with published specifications in connection with a particular product.

6. PROCEDURES FOR RESOLVING DISPUTES

The staff of the Wi-Fi Alliance, with oversight from the Board of Directors, will resolve any disputes between the manufacturer and the independent test facility regarding whether a particular product has passed interoperability testing. In the event of a dispute that can not be resolved by Wi-Fi Alliance staff, the Wi-Fi Alliance Board of Directors will take the issue under consideration and make a final decision.

Hotspot 2.0 Technical Specification Summary
(Wi-Fi CERTIFIED PASSPOINT Certification Program)

Overview

The specification provides for devices with wireless functionality to identify and associate wireless networks in the background, without any active intervention from the subscriber. Authentication does not require a browser-based sign-on. Instead, devices are authenticated automatically, using Extensible Authentication Protocols (EAP) based on a Subscriber Identity Module (SIM), a username and password, or certificate credentials.

Phases (States) of Hotspot 2.0 Connection

1. Discovery

A. Mobile devices scans for enabled networks and identifies them based on the access point's capabilities, advertised in beacon and Probe Response frames.

B. Mobile device queries Access Network Query Protocol (ANQP) server to determine network's capabilities prior to connection.

C. Mobile device checks user credentials to determine if it can access available networks.

D. If the user's credentials are valid, mobile device selects the preferred network unless overridden by the user and directly proceeds to Secure Access state

E. If the user's credentials are invalid or not present, user can select an available network for online sign-up and proceed to Registration state

2. Registration and Provisioning

Registration can be performed using pre-loaded credentials, and account creation can be done via online sign-up (OSU).

If user attempts to connect to a hotspot for the first time or without credentials, mobile device also goes through Registration and Provisioning. The OSU server registers the new subscriber and provisions a mobile device with credentials based on trusted root certificates, SIM/USIM, or username-password. Credentials for devices with a SIM are pre-provisioned, but might require metadata and policy provisioning.

If the device already has credentials for the network it is trying to connect to (such as a home service provider or a service provider that has a roaming agreement with the home provider), it goes straight to the Secure Access State and connects.

During Provisioning, a mobile device is:

- Loaded with required certificates, credentials, and related metadata, policy, and home service provider information for network discovery, selection, and access to network

- Provisioned with subscription and policy data

3. **Secure Access**

The mobile device enters the Secure Access state after it is associated to the network. In the Secure Access state the bobile device mutually authenticates with the hotspot service provider's (SP) authentication, authorization, and accounting (AAA) server using one of the allowed Extensible Authentication Protocol (EAP) methods supported by the SP's network:

Credential Type	EAP Method
Certificate	EAP-TLS
SIM or USIM	EAP-SIM or EAP-AKA
Username-Password (with server-side certificates)	EAP-TTLS with MS-CHAPv2

If authentication with the AAA server is successful, the mobile device receives full access to the network.

Requirements for Access Points

The specification requires that access points support the following:

(a) Advanced Security (Advanced Encryption Standard (AES) block cipher; user-based identification; mutual authentication between the client and the authentication server; traffic filtering until client has successfully authenticated to the network; generation of pairwise master key (PMK) and pairwise transient key (PTK) at the client device and authentication server);

(b) Each of the following standards-based Extensible Authentication Protocol (EAP) methods: EAP-Transport Layer Security (EAP-TLS), EAP-SIM, EAP-Authentication and Key Agreement (EAP-AKA), and EAP-TTLS with MSCHAPv2;

(c) Generic Advertisement Service (over-the-air transportation for frames of higher-layer advertisements between 802.11 stations or between a server in an external network and a station);

(d) Access Network Query Protocol (query and response protocol that defines services offered by an access point);

(e) Interworking and Roaming Consortium information elements and Basic Service Set load element;

(f) Traffic inspection and filtering;

(g) the capability to prevent multicast-based attacks by disabling the use of the group transient key; and

(h) Proxy Address Resolution Protocol (ARP).

Requirements for Mobile Devices

The specification requires that access points support the following:

(a) Advanced Security (Advanced Encryption Standard (AES) block cipher; user-based identification; mutual authentication between the client and the authentication server; traffic filtering until client has successfully authenticated to the network; generation of pairwise master key (PMK) and pairwise transient key (PTK) at the client device and authentication server);

(b) Each of the following standards-based Extensible Authentication Protocol (EAP) methods: EAP-Transport Layer Security (EAP-TLS), EAP-SIM, EAP-Authentication and Key Agreement (EAP-AKA), and EAP-TTLS with MSCHAPv2 (if device has SIM/USIM credentials), otherwise, EAP-TLS and EAP-TTLS with MSCHAPv2

(c) Generic Advertisement Service (over-the-air transportation for frames of higher-layer advertisements between 802.11 stations or between a server in an external network and a station);

(d) Access Network Query Protocol (query and response protocol that defines services offered by an access point);

(e) Interworking and Roaming Consortium information elements and Basic Service Set load element; and

(f) filtering of frames encrypted using the group transient key.