



The road to enhancing the public Wi-Fi access experience: FMCA and WBA spearhead an industry-wide initiative to enhance the customer experience for Wi-Fi roaming and authentication

Introduction

Over the past few years, we have witnessed an explosion in Wi-Fi usage and this trend is set to continue. According to data from research and consulting firm, Strategy Analytics, “annual wireless device sales will reach 1.2 billion units by 2014. Portable devices such as Wi-Fi enabled cell phones, consumer notebooks and games consoles are currently the most important wireless device segments.” (Source: Strategy Analytics, *Wireless Media Devices: Global Market Forecast*, 29 July 2008). Users are already able to benefit from Wi-Fi access not only in their homes and offices, but also while out and about through the deployment of public Wi-Fi hotspots and even Wi-Fi cities. Through roaming agreements between operators, people are also able to roam internationally on Wi-Fi. However, the Wi-Fi connection and log-on experience still remains far from an easy plug and play solution.

The Fixed-Mobile Convergence Alliance (FMCA) and the Wireless Broadband Alliance (WBA) launched an initiative involving 15 mobile and telecom operators and three hub providers that trialed technology that can remove this complexity for end users. A leading SIM card vendor also supported the trial by supplying innovative secured credential solutions for Wi-Fi network authentications.

“The vision of the inter-operator trial programme was to provide customers with a reliable, easy and consistent roaming experience with an automatic log-on facility, over any device, on any public Wi-Fi network,” said Gabrielle Ginér, BT, who was the project lead for the trial programme. “Together, the FMCA and WBA represent over 800 million customers around the world and this trial was the result of growing customer demand for an enhanced public Wi-Fi access experience.”

“The implementation of a full plug and play user experience over Wi-Fi devices and the ability for operators to identify its customers will open up a new trend of usage of public Wi-Fi networks”, said Tiago Rodrigues, TMN and WBA co-leader of the trial programme, “The mass adoption of 802.1x/EAP authentication will drive a new wave of Wi-Fi adoption over a vast range of services and devices”.

“The trial was conducted over the WBA’s award winning WRIX (Wireless Roaming Intermediary Exchange) platform and members from both FMCA and WBA signed bilateral agreements demonstrating the importance of collaboration amongst organisations to drive to a common goal. Through the participation of so many industry players in the project, we hope handset vendors and device manufacturers will further enhance their product features to enable an improved end user experience over public Wi-Fi networks,” said Dr Nicolas Ibrahim, Orange France and WBA project co-leader. “Ensuring that the technological requirements are established in as many devices as possible, whether it be laptops, PDA’s, mobile phones or gaming devices, will drive a more advanced and consistent customer experience. We trialed with EAP (Extensible Authentication Protocol) because it is a widely deployed technology for providing secure access control to networks.”



The trial programme specifically sought to address the following benefits:

- Allowing any Wi-Fi enabled device or gadget to work automatically on public Wi-Fi hot-spot networks without the need for complicated user interaction to access the service
- Providing customers with the same authentication experience anywhere in the world (“you just connect / like cellular”)
- Automatic authentication of devices and gadgets on public Wi-Fi hot-spots with appropriate billing and settlement (both for the home operator and international roaming partners)
- Operators with proprietary single sign-on clients will be able to support the fully standardised solution as a complementary service that delivers a seamless authentication experience for customers in-country or internationally

Although there has been sporadic use of 802.1x/EAP methods in the industry, particularly in enterprise networks, it has not been widely adopted for public Wi-Fi networks. “The advantages of using 802.1x/EAP methods are well known, but there has not been any cohesive effort to address the issues of the whole eco-system of Wireless LANs, which includes the networks and devices as well as changing user patterns. The FMCA and WBA have therefore spearheaded such an initiative through the innovative trial programme,” said Andrew Haworth, Managing Director of the FMCA.

The changing Wi-Fi landscape

While cellular mobile services were originally developed for voice applications, Wi-Fi services were developed for data applications. Although these distinctions have started to blur, this has impacted on Wi-Fi user authentication. The main authentication methods for Wi-Fi are based on credentials (a username and a password) that the user has to manually enter at least the first time the device is connected or at worst each time it connects. This requirement may become quite onerous, in particular on devices such as smart phones with small screens and small keyboards.

Even though all user services are transferred as data, they can still be divided into “data-like” and “voice-like” access. For example, “data-like” access refers to applications where an always-on continuous connection is not required as the user manually initiates usage (e.g. downloading e-mails over Wi-Fi). For “voice-like” access, automatic (and then continuous always-on) connection is required so that the application can register itself on the network, and in the case of voice, a call can be received from another user (e.g. using a cellular phone).

With the advent of dual mode services where Wi-Fi is used for both data and voice applications and where Wi-Fi usage is not only on laptops, the industry needs to simplify Wi-Fi user authentication, especially while roaming.

Seamless roaming and authentication based on 802.1x/EAP

In order to offer an enhanced user experience, the Wi-Fi industry must make the user experience simpler. Wi-Fi access via a web log in page presents many challenges to users. Adoption of seamless authentication and roaming based on the IEEE 802.1x framework supporting the agreed standard on EAP based authentication methods on devices, would provide an enhanced customer experience.



“The launch of 802.1x/EAP enabled networks will offer users of any Wi-Fi device an automatic authentication experience, similar to the one available on cellular networks. In addition, 802.1x/EAP will offer Wi-Fi users enhanced security compared to non 802.1x Wi-Fi networks,” said Shrikant Shenwai, CEO of WBA.

In addition to that, IEEE 802.1x allows a robust over-the-air connection security by ciphering the radio data exchange. This is a very valuable feature enabling the ability to efficiently address hacking and spoofing issues.

Four EAP methods were part of the trials, namely:

- EAP-SIM
- EAP-AKA
- EAP-TLS
- EAP-TTLS

EAP-SIM and EAP-AKA are popular choices for SIM card enabled devices such as dual-mode handsets. EAP-TLS and EAP-TTLS are options available for devices without the in-built SIM slot, such as media players and portable game consoles, but operators may also consider these options for dual-mode handsets, laptop computers and PDAs.

FMCA and WBA inter-operator trial overview

15 operators from the FMCA and WBA, as well as three hub providers, undertook seamless authentication and roaming trials for Wireless LANs using the 802.1x standard and the EAP framework. This was part of an industry initiative to deliver a seamless Wi-Fi roaming and authentication experience for end-users around the world.

The trial allowed participants to:

- Trial and demonstrate seamless authentication and roaming for converged devices (a dual-mode Wi-Fi enabled device or any other handheld equipment that is Wi-Fi enabled; e.g. electronic gadgets) using the EAP framework with the IEEE 802.1x standard compliance network access points and end-user devices supporting one or more of the following authentication methods: EAP-SIM, EAP-AKA, EAP-TLS, EAP-TTLS
- Collaborate towards a technical framework for the growing range of dual-mode Wi-Fi enabled devices and other electronic gadgets
- Simplify and enhance the end-user proposition by allowing users to access the services they want over multiple public Wi-Fi hotspots and devices
- Collaborate toward establishing roaming models for EAP based authentication methods



- Fine tune the provisioning process and provide a true plug and play user experience when subscribing to the service
- Discover and address potential deployment related issues
- Demonstrate the suitability of hub based roaming for EAP authentication

The trials spanned three distinct phases. Phase 1 was for establishing the trial network with 802.1x enabled access points for assessing the technical feasibility for these networks to support seamless authentication. Phase 2 was to trial devices that operators are considering launching their services on. These devices were tested on the trial network established during Phase 1. Finally, in Phase 3 some operators may move onto limited customer trials on live networks in preparation for general roll out.

Test results from FMCA and WBA trial

Participants have set up either test beds or staging platforms which form a representation of their deployed live networks. The set up of these test networks has allowed each participating operator to test their own seamless authentication solutions on 802.1x/EAP methods for home networks as well as simulated roaming networks.

The results of the trial have been obtained and are as follows:

- It is possible to authenticate using different EAP methods across different networks while roaming. Operators do not need to deploy the same type of EAP methods in their networks to enable seamless end user roaming and authentication. The 802.1x/EAP framework permits authentication using different methods (such as EAP-SIM or EAP-TTLS) across different networks while roaming
- No constraints for simultaneous 802.1x/EAP and Universal Access Method (UAM) based authentication could be identified
- The time taken for full authentication while roaming is comparable with the current cellular roaming experience for the user. Results indicate that it takes an almost equal time for 802.1x authentication as for WPA handshake signaling
- Realm or prefix stripping while RADIUS proxying fails authentication when some EAP methods are used. WBA and FMCA are currently assessing alternative methods of routing that would not strip realms in the future
- Some inconsistencies have been found in the implementation of RADIUS accounting in certain access points

There are no major issues that have been identified which would hinder the deployment of Wireless LAN networks enabling seamless authentication and roaming using the 802.1x/EAP framework. However, quite a few issues regarding the client interoperability have been identified during testing.



Opportunities for industry

The results of the FMCA and WBA inter-operator trials will be made available to industry partners for consideration.

Handset vendors have an opportunity to enhance their product features and overall roadmaps by providing a simple and consistent interface for access to public Wi-Fi networks with one or more of the above EAP authentication methods. This could be implemented in the form of a Wi-Fi network connection manager function on the device.

In order to automate the process of installing and configuring credential and connection manager settings on handsets, a set of software interfaces will be required so that these can be preformed by a self-install applet without any end user intervention.

Once the network credential is installed, the handset should be capable of authenticating itself and connecting automatically whenever it is switched on or comes within range of public Wi-Fi network. The user experience in all cases should be the same, regardless of which EAP authentication method is being used.

The EAP Settings Guideline document is available for download at either www.thefmca.com or www.wballiance.net. This document specifies the required end-user experience as well as handset behaviour when performing network auto log on. The Guideline document also covers the required steps during the initial credential provisioning and network profile configuration process.

In summary

The industry needs to respond to the growing popularity of Wi-Fi devices, to the changing usage trends of devices and to the demands of enhanced Wi-Fi user experience. The FMCA and WBA have responded to these demands and changing market conditions by initiating an inter-operator trial programme for seamless roaming and authentication based on 802.1x/EAP. Through the adoption of new technology, it is hoped that end-users will be able to capture these benefits, such as:

- Seamless access to information and communications anywhere – instant connection, without end-user intervention
- High speed wireless broadband to any handheld device – no pin or password required
- Enhanced user experience, on any device, via the best network available
- Fully standardised, interoperable, simple and secure solution
- Underpinned by leading global Wi-Fi hot spot providers in FMCA and WBA

The contents of the FMCA/WBA whitepaper 'The road to enhancing the public Wi-Fi access experience' are proprietary to the FMCA and WBA members and is - unless specifically indicated otherwise - protected by national and international copyright laws. The FMCA/WBA whitepaper 'The road to enhancing the public Wi-Fi access experience' is published for reference purposes only, and not for general copying, distribution or alteration.