NICC ND 1650 V1.1.1 (2012-12)

NICC Document

Wi-Fi Roaming Requirements

NICC Standards Limited

Michael Faraday House,
Six Hills Way,
Stevenage
SG1 2AY

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number
6613589

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC. Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by NICC Wi-Fi Working Group.

1 Scope

This document provides the high level architecture and functional requirements for a standardised approach to Security, Connectivity and Authentication within Wi-Fi networks in the UK.

2 References

For the particular version of a document applicable to this release see ND1610 [1].

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ND1610 Next Generation Networks, Release Definition

[2] WFA Passpoint programme of work

[3] WBA Next Generation Hotspot programme of work

[4] IEEE 802.11U

2.2 Informative references

[i1] RFC 4186 Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)

[i2] RFC 4187 Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA

[i3] RFC 5448 Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')

[i4] RFC 5216 The EAP-TLS Authentication Protocol

3 Definitions and abbreviations

3.1 Definitions

Authentication Storms
Excessive volume of authentication traffic generated by devices towards the network's authentication nodes. This may be caused by a large amount of genuine authentication requests or by rogue devices or applications.

Core Network
The central part of a telecom network that provides various services to customers who are connected to that network.

EAP-SIM
Authentication method used with EAP to support authentication using a SIM, as standardized in RFC 4186 [i1] (tools.ietf.org/html/rfc4186 [55])

EAP-AKA
Authentication method used with EAP to support authentication using a USIM, providing USIM Authentication and Key Agreement, as standardized in RFC 4187 [i2] (tools.ietf.org/html/rfc4187 [10])

EAP-AKA'
Authentication method used with EAP to support authentication of EAP AKA on networks that are not 3GPP compliant for 3GPP compliant devices, i.e. a device with a USIM wanting to authenticate on a Wi-Fi network would use EAP AKA', as standardized in RFC 5448 [i3] (tools.ietf.org/html/rfc5448 [13])

EAP-TLS
Authentication method used with EAP to support authentication through Transport Layer Security, in which secure digital certificates are used to mutually identify a user and a server's identity, as standardized in RFC 5216 [i4] (tools.ietf.org/html/rfc5216 [56])

EAP-TTLS
Authentication method used with EAP to support authentication through Transport Layer Security, in which secure digital certificates are used to mutually identify a user and a server's identity, as standardized in RFC 5216 [i4] (tools.ietf.org/html/rfc5216 [56])

Home Network RADIUS
The RADIUS (AAA) server in the Home Operator's network

Next Generation Hotspot (NGH)
NGH embodies standards and guidelines that enable the relationships between service providers – hotspot, cellular, cable, etc. – allowing end users to roam from one provider's hotspot to another and remain connected.

Secure Wi-Fi Roaming Network
A network that uses 802.1X to secure the air interface and uses secure connections for the backhaul between the AP and the core network.

Small Cells
Low powered radio access stations that have limited range but may operate in unlicensed and licensed spectrum

User Plane traffic
Traffic sent to and from the applications or services on a device. As opposed to traffic between the device and the network control functions.

Wi-Fi Device
A user terminal that has Wi-Fi radio used to access IP networks including the Internet.

Wireless Roaming Intermediary Exchange (WRIX)

Wireless Roaming Intermediary Exchange, a series of recommendations and operating procedures defined by the WBA to assist in the facilitation of roaming traffic on public Wi-Fi hotspots. WRIX-I defined the interchange portion, dealing with operation aspects of hotspot operation and AAA. WRIX-I deals with data exchange of traffic related information, and WRIX-f deals with financial aspects of settlement and clearing.

3.2 Abbreviations

AAA	Authentication, Authorization and Accounting
AC	Access Controller
ANDSF	Access Network Discovery and Selection Function
ANQP/GAS	Access Network Query Protocol/Generic Advertisement Service
AP	Access Provider
CP	Communication Provider
EAP	Extensible Authentication Protocol
EAP-SIM	Extensible Authentication Protocol - Subscriber Identity Module
EAP-AKA	Extensible Authentication Protocol – Authentication and Key Agreement
EAP-AKA’	Extensible Authentication Protocol - Authentication and Key Agreement Prime
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol – Tunnelled Transport Layer Security
GHz	Giga Hertz
GRE	Generic Routing Encapsulation
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPSec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	Local Area Network
NGH	Next Generation Hotspot
RF	Radio Frequency
(U)SIM	(Universal) Subscriber Identity Module
SSID	Service Set Identifier
UK	United Kingdom
WFA	Wi-Fi Alliance
Wi-Fi	Wireless Fidelity
WLC	Wireless Lan Controller
WPA	Wi-Fi protected Access
WRIX	Wireless Roaming Intermediary Exchange

4 Overview and Requirements

This document provides the high level functional requirements for a Secure Wi-Fi Roaming Network.
These requirements can be summarised as:

- Providing a Wi-Fi connection in the UK that is as secure as a cellular mobile connection.
- Enabling a seamless authentication experience, meaning no user intervention is required after a potential initial registration process.
- Allowing customers to roam in and out of various Wi-Fi networks.
- Providing a means of charging and settlement between Communication Providers.
- Being based on existing or proposed specifications, new standards and best practises in the Wi-Fi industry.

The present document provides additional requirements for interoperability which apply in addition to those in section 2.1 References; specifically -

- WFA Passpoint programme of work
- WBA Next Generation Hotspot programme of work

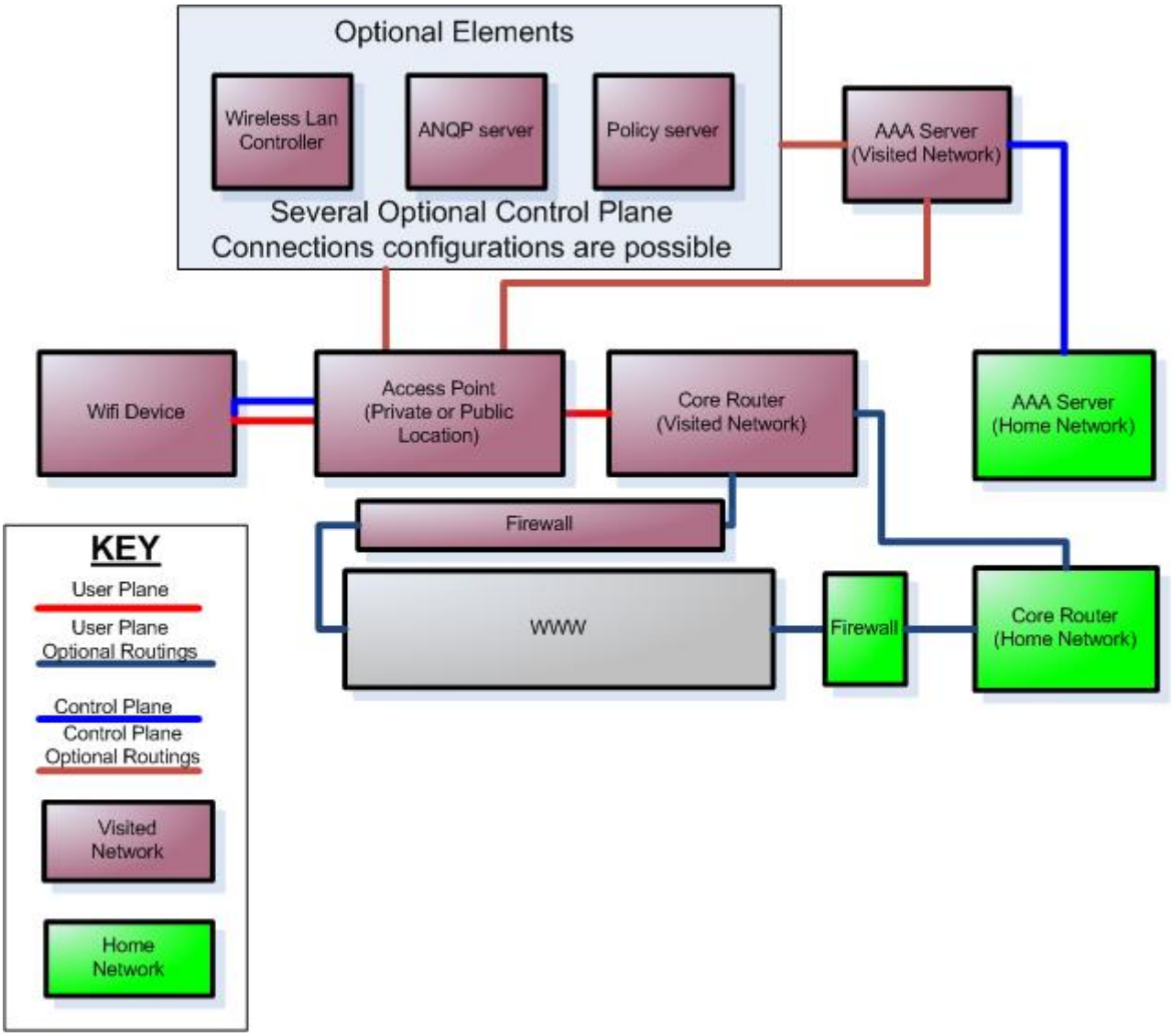
The WFA Passpoint documentation can be found at – www.wi-fi.org

The WBA Hotspot documentation can be found at – www.wballiance.com

Where the present document contradicts the referenced ones the requirements in the present document shall take precedence.

5 High Level Architecture diagram

The following diagram shows a typical WFA Passpoint compliant architecture. The use of other WFA Passpoint compliant architectures is not precluded by this specification.



5.1 Diagram Definitions

The architecture above indicates the logical functionality and in no way limits the physical implementation.

5.1.1 User Plane

This is the path of the IP session between the Wi-Fi Device and the internet or provider services

5.1.2 Control Plane

This is the set of protocols that control and manage the Wi-Fi service

5.1.3 Visited Network

The Communication Provider (CP) who controls the Wi-Fi Network to which the Wi-Fi Device connects.

5.1.4 Home Network

The CP who is providing the customer with the connection service for which there is a billing and contractual relationship.

5.1.5 ANQP Server

The ANQP server facilitates the needs for Access Network Query Protocol to provide a mobile device with additional information of the Wi-Fi network to help it choose the right network to connect, for example information about supported service providers, encryption and connection capabilities.

6 Functional Requirements

The following is a list of functional requirements for each component of a Secure Wi-Fi Roaming Architecture.

6.1 Wi-Fi Device

6.1.1 Authentication

As a minimum devices shall support an EAP authentication method as specified in WFA Passpoint certification. (Currently, April 2012, this is EAP-SIM, EAP-AKA, EAP-TLS, EAP-TTLS).

6.1.2 AP Addressing

The device shall support IP v6 or v4 addressing and may support both.

6.1.3 Connection Policy

The Connection Policy:

1. Shall allow the User to subscribe to multiple Wi-Fi CPs and have some method of the prioritising between them
2. Shall allow the User to:
    i. Manually override to a selected Access Point at any time.
    ii. Determine which Access Points to "white list" (include) and or "black list" (exclude)
3. Should enable the device to connect to the most "appropriate" Access Point based on a variety of factors, for example; signal strength, SNR, QoS and the price of the service (All criteria outside the scope of the present document.)
4. Should support ANQP/GAS
5. May support ANDSF

6.2 Access Point

6.2.1 Radio Interface

On the Radio Interface -

1. As a minimum the AP shall support EAP authentication methods as specified in WFA Passpoint certification. (Currently, April 2012, this is EAP-SIM, EAP-AKA, EAP-TLS, EAP-TTLS).
2. The number of SSIDs presented from the Access Point shall be kept to a minimum.
3. There should be radio interfaces utilising both the 2.4 GHz and the 5 GHz RF bands. Future additional spectrum, such as 60 GHz, is not be precluded when available for Wi-Fi services.

4. There may be a Radio/Airtime policy that shares Radio airtime resource across multiple Wi-Fi Devices evenly.

5. The Access Point shall conform to the proposed PassPoint Specification Release 1 as defined by the Wi-Fi Alliance (WFA), that includes:

    I. IEEE 802.11u
    II. WPA2 enterprise including EAP-SIM, EAP-AKA, EAP-TLS and EAP-TTLS

6.2.2 IP Layer

1. Shall support IP v6 or v4 addressing packet forwarding and may support both.

2. Where the Home Network Provider provides an IP address for the Wi-Fi Device then the Access Point shall tunnel/forward the User Plane traffic to the Home Network. The AP shall be capable of IP tunnelling, for example, IPSec or GRE based tunnelling.

3. There should be no Radius client at the AP. It is assumed that the public access AP is not physically secure enough to hold the actual master RADIUS secret key. A WLC or RADIUS-Proxy should be used to mitigate the risk.
4. All User traffic shall be routed via the CPs core router; no intra AP traffic shall be allowed.
5. The Visited Network shall allocate an IP address to the Wi-Fi Device where none is provided by the Home Network AAA Server after successful authentication.

6.2.3 Security and Management

1. The AP shall provide a secure network connection to Access Controller and Core Network

2. Considerations for physical security should be equivalent to cellular public access points i.e. “small cells”.

3. The AP should be controlled via some form of remote management.

6.3 Access Controller

1. The AC shall act as RADIUS Client towards the AAA Server on behalf of the Wi-Fi device.

2. Implementations should support Wireless Roaming Intermediary Exchange (WRIX) and should allow the implementation of the Next Generation Hotspot (NGH)

3. The AC shall prevent the propagation of “Authentication Storms” by an appropriate mechanism, (e.g. caching or storm control).

4. The AC should redirect new customers to a registration process or help page where Authentication fails

5. The RADIUS Accounting packets shall allow inter-CP cross charging and settlement in either a clearing house or a transactional model.

6.4 AAA Server (Home Network)

1. There shall be an AAA Server in the home Network that receives RADIUS AAA packets from the Visited Network’s Access Controller.

2. The AAA Server shall use the specification of AAA packets as defined for the Access Controller above.

3. The AAA Server shall either:

    a. provide the Wi-Fi Device with Home Network IP address if User Plane traffic is to be tunnelled to the Home Network

    b. Or provide no IP address for the Wi-Fi Device, which the visited network shall interpret as meaning that the Visited Network shall both provide the Wi-Fi Device with an IP address and terminate User Plane traffic to the internet.

6.5 Overview of Passpoint compliant network discovery and selection

End user devices will use ANQP (Access Network Query Protocol) for network discovery. The connection manager of the mobile device compares the ANQP provided data against configuration information stored in the device, including home service provider policy and user preferences, to automatically select a hotspot network.
Initially, to learn about the network environment, the end user device sends Generic Advertisement Service (GAS) query frames to learn which service providers and subscriptions are available in the area. The device can query further for details about these to make more informed network selection decisions. ANQP elements are provided by either the Passpoint compliant APs or a combination of the AP and ANQP server.
More on the Passpoint compliant deployment in the WFA best practises guide. Technical specification regarding the network discovery and selection derives from the IEEE 802.11U standard [4].

6.6 Core IP Router (Visited Network)

1. The Visited Network IP Router shall route User Plane traffic to the internet where no IP address was provided by Home Networks AAA Server.

2. User Plane traffic shall be routed to the Home network using a direct peering interconnect or via an agreed secure connection.

3. Firewall shall block all uninitiated incoming traffic requests from the internet towards the LAN.

4. The traffic between the associated devices shall be separated and any broadcast storms controlled.

6.7 Core IP Router (Home Network)

1. To enable the most secure connection between Wi-Fi Networks user Plane traffic shall be received from the Visited Network using a direct peering interconnect or agreed secure connection

2. The Home Network IP Router shall route User Plane traffic to the Internet where traffic has been received from the Visited Network.

6.8 Location information

WRIX-L Location Feed Format & File Exchange Standard provides a format and data the operators can exchange for feeds of partner service locations. This specification includes both the file format and file exchange method. It clearly describes the Mandatory and Optional fields in the WBA Location database so that there is uniformity of information across the operators. For example, geographic position is to be exchanged in WGS84 format. WRIX-L standard is available for download from the WBA website www.wballiance.com

6.9 Access to Emergency Services

Currently out of scope for this document; awaiting international standards

The potential future use of location based information for emergency services should be noted.

History

Document history		
Version	Date	Milestone
V1.1.1	17th December 2012	Initial publication