HGI-RD057

WI-FI SYSTEM REQUIREMENTS FOR HOME GATEWAYS:
NFC PAIRING, GUEST ACCESS, HOTSPOT

Publication Copy
1 CONTENTS

1 Important notices, IPR statement, disclaimers and copyright ................................................................. 1

3 Important notices, IPR statement, disclaimers and copyright ................................................................. 4
  3.1 About HGI ............................................................................................................................................... 4
  3.2 This may not be the latest version of This HGI Document ................................................................. 4
  3.3 There is no warranty provided with This HGI Document ........................................................................ 4
  3.4 Exclusion of Liability .............................................................................................................................. 4
  3.5 This HGI Document is not binding on HGI nor its member companies ................................................. 4
  3.6 Intellectual Property Rights ................................................................................................................ 4
  3.7 Copyright Provisions ............................................................................................................................ 5
    3.7.1 Incorporating HGI Documents in whole or part within Documents Related to Commercial Tenders 5
    3.7.2 Copying This HGI Document in its entirety .................................................................................. 5
  3.8 HGI Membership .................................................................................................................................. 5

4 Acronyms ................................................................................................................................................ 7
  4.1 Acronyms ............................................................................................................................................... 7
  4.2 Terms .................................................................................................................................................. 7
  4.3 Definitions of requirements terms ......................................................................................................... 8

5 Purpose and Scope of this Document ........................................................................................................ 9

6 Wi-Fi Pairing of HG and End-Devices Using NFC .................................................................................... 9
  6.1 Background ......................................................................................................................................... 9
    6.1.1 Need for Easy Pairing .................................................................................................................. 9
    6.1.2 Overview of NFC and Application to Pairing .............................................................................. 10
  6.2 Use Cases .......................................................................................................................................... 10
    6.2.1 Static Tag and Tap ....................................................................................................................... 10
    6.2.2 Connected Tag and Tap ............................................................................................................... 10
    6.2.3 Integrated Reader ....................................................................................................................... 11
    6.2.4 Connected-Tag and Mediated Connection ................................................................................. 11
  6.3 Requirements For NFC In HG .............................................................................................................. 11

7 Guest access ........................................................................................................................................... 13
2 IMPORTANT NOTICES, IPR STATEMENT, DISCLAIMERS AND COPYRIGHT

This chapter contains important information about HGI and this document (hereinafter ‘This HGI Document’).

2.1 ABOUT HGI

The Home Gateway Initiative (HGI) is a non-profit making organization which publishes guidelines, requirements documents, white papers, vision papers, test plans and other documents concerning broadband equipment and services which are deployed in the home.

2.2 THIS MAY NOT BE THE LATEST VERSION OF THIS HGI DOCUMENT

This HGI Document is the output of the Working Groups of the HGI and its members as of the date of publication. Readers of This HGI Document should be aware that it can be revised, edited or have its status changed according to the HGI working procedures.

2.3 THERE IS NO WARRANTY PROVIDED WITH THIS HGI DOCUMENT

The services, the content and the information in this HGI Document are provided on an "as is" basis. HGI, to the fullest extent permitted by law, disclaims all warranties, whether express, implied, statutory or otherwise, including but not limited to the implied warranties of merchantability, non-infringement of third parties rights and fitness for a particular purpose. HGI, its affiliates and licensors make no representations or warranties about the accuracy, completeness, security or timeliness of the content or information provided in the HGI Document. No information obtained via the HGI Document shall create any warranty not expressly stated by HGI in these terms and conditions.

2.4 EXCLUSION OF LIABILITY

Any person holding a copyright in This HGI Document, or any portion thereof, disclaims to the fullest extent permitted by law (a) any liability (including direct, indirect, special, or consequential damages under any legal theory) arising from or related to the use of or reliance upon This HGI Document; and (b) any obligation to update or correct this technical report.

2.5 THIS HGI DOCUMENT IS NOT BINDING ON HGI NOR ITS MEMBER COMPANIES

This HGI Document, though formally approved by the HGI member companies, is not binding in any way upon the HGI members.

2.6 INTELLECTUAL PROPERTY RIGHTS

Patents essential or potentially essential to the implementation of features described in This HGI Document may have been declared in conformance to the HGI IPR Policy and Statutes (available at the HGI website www.homegateway.org).
2.7 COPYRIGHT PROVISIONS

© 2013 HGI. This HGI Document is copyrighted by HGI, and all rights are reserved. The contents of this HGI Document are protected by the copyrights of HGI or the copyrights of third parties that are used by agreement. Trademarks and copyrights mentioned in this HGI Document are the property of their respective owners. The content of this HGI Document may only be reproduced, distributed, modified, framed, cached, adapted or linked to, or made available in any form by any photographic, electronic, digital, mechanical, photostat, microfilm, xerography or other means, or incorporated into or used in any information storage and retrieval system, electronic or mechanical, with the prior written permission of HGI or the applicable third party copyright owner. Such written permission is not however required under the conditions specified in Section 2.7.1 and Section 2.7.2:

2.7.1 INCORPORATING HGI DOCUMENTS IN WHOLE OR PART WITHIN DOCUMENTS RELATED TO COMMERCIAL TENDERS

Any or all section(s) of HGI Documents may be incorporated into Commercial Tenders (RFP, RFT, RFQ, ITT, etc.) by HGI and non-HGI members under the following conditions:

(a) The HGI Requirements numbers, where applicable, must not be changed from those within the HGI Documents.
(b) A prominent acknowledgement of the HGI must be provided within the Commercial document identifying any and all HGI Documents referenced, and giving the web address of the HGI.
(c) The Commercial Tender must identify which of its section(s) include material taken from HGI Documents and must identify each HGI Document used, and the relevant HGI Section Numbers.
(d) The Commercial Tender must refer to the copyright provisions of HGI Documents and must state that the sections taken from HGI Documents are subject to copyright by HGI and/or applicable third parties.

2.7.2 COPYING THIS HGI DOCUMENT IN ITS ENTIRETY

This HGI Document may be electronically copied, reproduced, distributed, linked to, or made available in any form by any photographic, electronic, digital, mechanical, photostat, microfilm, xerography or other means, or incorporated into or used in any information storage and retrieval system, electronic or mechanical, but only in its original, unaltered PDF format, and with its original HGI title and file name unaltered. It may not be modified without the advanced written permission of the HGI.

2.8 HGI MEMBERSHIP

Stollmann, Sumitomo, Swisscom AG, Technicolor, Telecom Italia, Telekom Austria, TeliaSonera, Telstra, TNO, Trac Telecoms & Radio Ltd, Vodafone, Vtech, Zarlink, ZTE, ZyXEL.
3 ACRONYMS

3.1 ACRONYMS

ACS    Automatic Channel Selection
AP     (Wi-Fi) Access Point
BSP    Broadband Service Provider
DHCP   Dynamic Host Configuration Protocol
EAP    Extensible Authentication Protocol
FQDN   Fully Qualified Domain Name
HG     Home Gateway
HGI    Home Gateway Initiative
HN     Home Network
NDEF   NFC Data Exchange Format
NFC    Near Field Communication
PSK    Pre-Shared Key
SDO    Standards development organization
SSID   Service Set IDentifier
Wi-Fi  Wireless Fidelity (IEEE 802.11)
WFA    Wi-Fi Alliance
WLAN   Wireless LAN
WPA    Wi-Fi Protected Access

3.2 TERMS

<table>
<thead>
<tr>
<th>Guest Access</th>
<th>A service which allows the primary user to share Wi-Fi bandwidth with guests, where the configuration of the service is solely under the control of the primary user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hot Spot</td>
<td>A service which allows the primary user to sharing Wi-Fi bandwidth with other users, where the configuration of the service is under the control of the service</td>
</tr>
</tbody>
</table>
provider. However, the primary user may still be able to opt-in or –out from providing the service.

| NFC Pairing | Use of Near-Field Communication to pair a client device with a Home Gateway. In this document NFC Pairing primarily refers to pairing of Wi-Fi connections, but it can also refer to Bluetooth connections. |

### 3.3 DEFINITIONS OF REQUIREMENTS TERMS

The definitions of MUST and SHOULD in this document are as follows:

**MUST**

A functional requirement which is based on a clear consensus among HGI Service Provider members, and is the base level of required functionality for a given class of HG.

**MUST NOT**

This function is prohibited by the specification.

**SHOULD**

Functionality which goes beyond the base requirements for a given class of HG, and can be used to provide vendor product differentiation (within that class).

Note: these definitions are specific to the HGI and should not be confused with the same or similar terms used by other bodies.
4 Purpose and Scope of This Document

HGI considers Wi-Fi technologies as one of the most suitable technologies for offering connectivity and services in the home network, and many Wi-Fi requirements are included in HGI documents, including the Residential Profile [1] and test specifications.

In recent years, new Wi-Fi standards have been developed by the industry, and new use cases have arisen; there are now many more Wi-Fi attached devices, tablets, smartphones etc. The success of Wi-Fi has resulted to new use cases and new requirements for in-home WLAN. The requirements document HGI-RD045v2 provides updated requirements on Automatic Channel Selection, Channel Measurement, and Repeaters.

The present document, HGI-RD057 covers system level requirements related to Wi-Fi in the Home Gateway. The aspects covered are the following:

- Pairing of Wi-Fi using NFC (Near Field Communication) technology.
- Guest Access,
- Hotspot.

Requirements for guest access and hotspot were originally described in [1], but are now updated in the present document.

5 Wi-Fi Pairing of HG and End-Devices Using NFC

This chapter provides a description of Use-Cases and Requirements for the use of NFC Pairing between a Home Gateway and end-devices such as smartphones, smart home actuators and sensors, tablets, media devices, etc.

5.1 Background

Pairing the HG with a variety of devices in a simple, effective way is especially important now (i.e., 2016) that the number of Wi-Fi equipped end-devices has increased dramatically. While many alternative smart home interface technologies exist, Service Providers anticipate that Wi-Fi will be an important technology for smart home applications, on top of the wide range of existing Wi-Fi applications.

5.1.1 Need for Easy Pairing

As the central Wi-Fi access point, easy pairing with the HG is extremely important to avoid the need for complex configurations by the customer and help-desk support by the Service Provider. The current state of the art for easy pairing is WPS PIN or WPS pushbutton. Whereas the PIN method has known security drawbacks, the pushbutton requires a physical button or other man-machine interface on the device to initiate pushbutton pairing. NFC pairing ([5]) can be an effective alternative which requires only that the paired device only be brought in proximity with the HG.
5.1.2 OVERVIEW OF NFC AND APPLICATION TO PAIRING

NFC allows communication between two devices by getting the two devices in proximity for a short moment. While in proximity (within a few centimetres), the devices can exchange data. This can be used to exchange information for subsequent Wi-Fi pairing, when both devices are Wi-Fi capable. NFC pairing for Wi-Fi is specified by the Wi-Fi Alliance “Wi-Fi Simple Configuration_Technical_Specification” (aka “Wi-Fi Protected Setup”) specification ([5]).

An NFC-capable device can be of two types

- a Tag, which exposes NFC Data Exchange Format (NDEF) formatted data to an NFC Reader
- a Reader, which can read, and write data (from/to a tag or another reader).

Note that a similar technique can be used for pairing other technology than Wi-Fi. Namely, NFC Forum have specified a pairing for Bluetooth as well ([3]). Although this document does not cover pairing for Bluetooth, HGI notes that should an HG implement Bluetooth, it may be possible to re-use integrated NFC also for Bluetooth pairing.

5.2 USE CASES

In what follows, several configuration options for integration of NFC technology to support easy pairing of Wi-Fi between the HG and end-devices are outlined, together with the use-case for each configuration.

5.2.1 STATIC TAG AND TAP

Of the three scenarios, this is the simplest: the HG gateway is equipped with a static NFC tag. The HG is provisioned with unique Wi-Fi credentials (SSID and Password) and provided with an NFC tag containing NDEF formatted credentials. To join the Wi-Fi network with NFC reader device, like a smart phone, a user needs bring the device in proximity to the HG.

While this scenario supports basic pairing with a smart phone, it has these disadvantages:

- Devices with only NFC tag can’t directly pair to the gateway. For devices hosting only a Tag, there is however a work-around, as detailed in use case “Mediated Connection” below.
- Every time an HG’s Wi-Fi credentials are changed the NFC tag needs to be re-programmed to reflect the changes. This can be done for instance by using an NFC capable smart phone application, which adds a layer of complexity to the actions that must be performed by the user.

5.2.2 CONNECTED TAG AND TAP

In order to improve the user experience of the static Tag, the gateway can be equipped with a connected Tag, which is accessible to the HG’s processor. Every time the HG’s SSID and Wi-Fi credentials are changed the tag is updated by the HG processor with NDEF data reflecting the changes. This is considerably better
than the Static Tag from a user’s point of view, however it still can’t directly pair with an NFC Tag-only device.

5.2.3 **Integrated Reader**

In this scenario, the HG would be equipped with an NFC Reader to allow direct pairing with non-reader devices, such as some IoT devices, for which hosting an NFC Reader would be too expensive.

To be noted that this case is not needed for easy pairing of smartphones, because NFC-capable smartphones do host an NFC Reader.

Again, the device can connect to the Wi-Fi network by tapping the NFC Reader integrated into the HG.

The HG is provided with an integrated NFC Reader accessible to the HG processor. Every time the gateway credentials are changed, the gateway application processor, via NFC Reader, is able to expose updated NDEF data reflecting the changes.

Although this is the most flexible scenario, it is also the most expensive as the Reader function is expected to be more costly than a tag. An alternative way is to resort to a mediated connection, as described next.

5.2.4 **Connected-Tag and Mediated Connection**

In the case where the gateway is not equipped with an NFC Reader, but only with an NFC Tag, it is still possible to benefit from NFC easy pairing even for devices hosting also only a tag. This can be achieved thanks to the mediation of a third device (typically a smartphone), which embeds an NFC Reader. This of course requires the third device to come with the right application.

This scenario can address those devices which cannot easily be brought close to the gateway (like a PC and a printer), and/or IoT devices.

5.3 **Requirements For NFC In HG**

Taking into account the scenarios described above, the following requirements are given to support Service Provider requirements for integration of NFC technology in the HG.

<table>
<thead>
<tr>
<th>N°</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFC1.</td>
<td>The HG MUST embed an NFC tag to support WPS pairing with NFC Reader devices. It MUST act according to [5].</td>
</tr>
<tr>
<td>NFC2.</td>
<td>If more than one SSID is broadcast by the HG, the NFC pairing MUST support at least the main (non-guest and non-hotspot) SSID.</td>
</tr>
<tr>
<td>N°</td>
<td>Requirement</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NFC3.</td>
<td>If Guest Access is supported by the HG, the HG MUST have the NFC pairing mechanism configured by default for the non-guest SSID.</td>
</tr>
<tr>
<td>NFC4.</td>
<td>If Guest Access is enabled by the user, the HG MUST automatically reconfigure the NFC pairing to the Guest SSID.</td>
</tr>
<tr>
<td>NFC5.</td>
<td>The HG MUST allow the user to configure the NFC pairing with regard to its SSID.</td>
</tr>
<tr>
<td>NFC6.</td>
<td>The HG MUST be able to update the embedded NFC tag with SSID and Wi-Fi security information.</td>
</tr>
<tr>
<td>NFC7.</td>
<td>Whenever the Wi-Fi settings are changed in the HG, the NFC configuration MUST be updated automatically by the HG.</td>
</tr>
<tr>
<td>NFC8.</td>
<td>The HG MUST support Mediated Connection by an external device such as Smart Phone.</td>
</tr>
<tr>
<td>NFC9.</td>
<td>The HG MUST allow the user to enable and disable NFC pairing.</td>
</tr>
<tr>
<td>NFC10.</td>
<td>The HG MUST have its NFC pairing configured by default as “enabled”.</td>
</tr>
</tbody>
</table>
6  GUEST ACCESS

The guest access service shares the residential bandwidth between a primary user and guests (connecting to the HG). Guests only have access to the Internet service connection and cannot access resources of the home network. The primary user manages the service, for example, sets the password required to access it.

Guest access is a means for the primary user to share his (Internet) access while preserving privacy:

- Devices of the home LAN are not visible by guests
- The primary user does not need to share the password that he normally uses.

6.1 USE CASE DESCRIPTION

6.1.1 USE CASE 1 (PRIMARY USE CASE)

The primary user has to allow guests to use a part of his access bandwidth. In order to do so, the gateway owner configures via the User Interface a secondary SSID, and a password of his choice. The SSID and the password are shared with granted guests, who can then use them to connect to the Internet.

6.1.2 USE CASE 2

Another use for guest access is the case of primary users willing to grant an open access to anyone, e.g. cafés willing to provide Internet access to customers. In such a case, the primary user would configure no password at all.

6.2 PROPOSED SOLUTION

In contrast to the hotspot solution, in guest access the primary user will give to the guests the credentials needed to connect. And the guests then connect to the SSID as they would for regular Wi-Fi access, i.e. guest access uses Wi-Fi Protected Access WPA-personal (aka WPA-PSK for Pre-Shared Key) to grant access.

In order to preserve privacy, the primary user’s Home network segment and the guest network segment must be isolated from each other by the HG, to prevent guests having access to the home network.

Guests are allocated a private IP address by HG.

6.3 REQUIREMENTS

<table>
<thead>
<tr>
<th>N°</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUEST1.</td>
<td>The HG MUST allow the primary user to enable and disable the guest access service.</td>
</tr>
<tr>
<td>GUEST2.</td>
<td>When enabled, the HG MUST support one SSID dedicated to the guest access service.</td>
</tr>
<tr>
<td>N°</td>
<td>Requirement</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GUEST3.</td>
<td>The HG MUST NOT forward any frames/packets between devices connected to the guest access and any other local devices connected to the HG.</td>
</tr>
<tr>
<td>GUEST4.</td>
<td>The Parental control function <strong>MUST NOT</strong> be applied to Guest Access devices</td>
</tr>
</tbody>
</table>
7 HOTSPOT

The Hotspot service shares the residential bandwidth between a primary user and hotspot users connecting to the HG. Hotspot users only have access to Internet connection and cannot access resources of the home network. The Hotspot service is managed by the Service Provider, who can enable, disable, and configure the parameters associated with the service by CWMP commands.

The primary user accepts to let visitors use a part of his access by commercial arrangement with the Service Provider, and the primary user is not involved with configuration of the service. However, the primary user may be able to opt-out of and disable the service. Hotspot users can access the hotspot service from any HG that are configured to support the service, as well as from public Access Points (APs), by commercial arrangement with the Service Provider.

7.1 USE CASE DESCRIPTION

Hotspot can operate according to two modes:

- Low-security mode: using web portal authentication through a public SSID. This is the most common mode of operation.
- High-security mode: using Wi-Fi Protected Access WPA2-Enterprise mode and providing mutual authentication between the hotspot user’s device and the service provider platform with IEEE 802.11i WPA2- Enterprise mode. In such a case, the hotspot user does not need to enter the credentials for the authentication. Instead, they are retrieved directly from their device (certificates, SIM...).

A HG may support one security mode only, or may support both security modes, including simultaneously.

Hotspot users need credentials to be able to connect to the HG; therefore they must be also customers of the Service Provider, or if there is another business arrangement which allows those customers to access the hotspot service. For example, an SP may have an arrangement to provide hotspot service access to the customers of another SP.

In high-security mode some devices will automatically reconnect to a previously visited hotspot. The user may not want this to happen. The HG is not required to support any function to prevent connection to a particular end device. Any such functionality is assumed to be on the end device.

7.2 PROPOSED SOLUTION

The primary user’s Home network segment and Wi-Fi hotspot network segment must be isolated from each other by the HG, to prevent hotspot users having access to the home network. In addition, hotspot users should be prevented from sending traffic directly to each other without passing the service
provider’s platform first. Both cases can be solved by tunnelling the hotspot traffic to the service provider’s platform.

Hotspot users consume part of the Wi-Fi bandwidth, and this could affect the primary user’s services. Therefore, high-priority services of the primary user must not be affected by the presence of hotspot users (this can be achieved by classifying traffic by SSID as per requirement R.30 of [7] along with appropriate QoS treatment of the primary and hotspot traffic). Even for best-effort traffic, the hotspot users must be constrained to a percentage of the available bandwidth under congestion (e.g. by configuring the weighting ratio of the hotspot traffic queue and that of the primary user’s lowest-priority traffic). Also it may necessary to cap the number of simultaneous connected hotspot users.

The above implies the hotspot SSID is allocated to the lowest priority level. This is consistent with the fact that the hotspot gives access to the internet (only), but is not used to give access to other services available to the gateway owner.

Note: for regulatory reasons, the service provider needs to know which traffic was originated from the hotspot, or not. Because all hotspot traffic is tunnelled towards the service provider platform, there are no additional home gateway requirements to do this.

The hotspot service is normally offered only on the 2.4G band. Hotspot service always uses a different SSID from that of the primary user, but it is possible to use more than one SSID for this service. For example:

- One SSID for the low-security access mode
- A second SSID for the high-security access mode

Attaching to the hotspot in low-security mode involves the following sequence of events:

- The hotspot user’s device associates to the public SSID
- The device sends a DHCP Discover/Request message to the HG in order to get an IPv4 address
- The HG adds option 82, sub-options 1 and 2, to the DHCP message and encapsulates it in a L2 GRE tunnel towards the service provider platform
- The service provider platform allocates an IP address through the tunnel and the HG passes the message to the device
- The HG tunnels all traffic to/from the service provider platform
- The first access by the device is redirected by the service provider platform to a login page
- Irrespective of the authentication result, all subsequent traffic continues to be tunneled to the service provider platform

Attaching to the hotspot in high-security mode involves the following sequence of events:

- The Wi-Fi beacon for the SSID advertises that 802.1X authentication is needed
- The hotspot user’s device associates to the public SSID based on 802.1X (802.11i WPA2 enterprise)
The hotspot user authenticates using Extensible Authentication Protocol EAP method as described in [IEEE Std 802.1X-2010 [2]]. The authentication process uses RADIUS messages between the gateway and the network-based authentication server; these messages generated by the gateway are routed on the internet IP session.

- If the authentication is unsuccessful then the gateway does not authorize the visitor to send traffic into the L2 tunnel.
- If the authentication is successful then the gateway sets up a GRE tunnel ([4]) towards the service provider platform and authorizes the visitor to send traffic into the tunnel.
- The visitor sends a DHCP Discover/Request message to the gateway in order to get an IPv4 address.
- The HG adds option 82 sub-options 1 and 2 to the DHCP message and encapsulates it in a L2 GRE tunnel towards the service provider platform.
- All the traffic received from the public SSID is encapsulated by the HG towards the service provider platform into the L2 GRE tunnel. All the traffic received from the hotspot L2 tunnel is de-encapsulated by the HG and sent over Wi-Fi.

### 7.3 Requirements

<table>
<thead>
<tr>
<th>N°</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOTSPOT1.</td>
<td>The HG MUST support 1 SSID dedicated to the each mode of the hotspot service that is supported.</td>
</tr>
<tr>
<td>HOTSPOT2.</td>
<td>The HG MUST NOT forward any frames/packets between devices connected to the hotspot and any other local devices connected to the HG.</td>
</tr>
<tr>
<td>HOTSPOT3.</td>
<td>The HG MUST allow the primary user to enable and disable the hotspot service (subject to any commercial limitations).</td>
</tr>
<tr>
<td>HOTSPOT4.</td>
<td>The HG MUST classify the traffic coming from the hotspot SSID into the low priority queue, as per the mechanisms in [6].</td>
</tr>
<tr>
<td>HOTSPOT5.</td>
<td>The HG MUST allow the Service Provider to remotely enable and disable the hotspot service.</td>
</tr>
<tr>
<td>HOTSPOT6.</td>
<td>The gateway SHOULD be able to limit the number of devices simultaneously connected to the hotspot</td>
</tr>
<tr>
<td>HOTSPOT7.</td>
<td>The HG SHOULD be resistant to Denial of Service attacks from hotspot users or devices attempting to connect to the hotspot</td>
</tr>
<tr>
<td>N°</td>
<td>Requirement</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HOTSPOT8.</td>
<td>The HG MUST NOT apply any firewall rules or parental control to traffic from hotspot devices</td>
</tr>
<tr>
<td>HOTSPOT9.</td>
<td>The HG MUST implement a DHCP L2 relay to insert options 82, sub-options 1 and 2, in IPv4 DHCP packets.</td>
</tr>
<tr>
<td>HOTSPOT10.</td>
<td>The HG MUST support GRE encapsulation as defined in RFC 1701 ([4]).</td>
</tr>
<tr>
<td></td>
<td>NOTE: This may have implications for HG performance unless hardware acceleration is used.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The HG needs to be provisioned with the FQDN of the service provider platform in order to setup the tunnel via DNS.</td>
</tr>
<tr>
<td>HOTSPOT11.</td>
<td>The HG MUST encapsulate all the Ethernet frames coming from the hotspot SSIDs and forward into the GRE tunnel, except EAP frames (Type=0x888e (802.1X Authentication)) that are forwarded in RADIUS messages. For the high-security mode the HG MUST encapsulate traffic if and only if prior authentication has been successful.</td>
</tr>
<tr>
<td>HOTSPOT12.</td>
<td>The HG MUST support the IEEE 802.1X protocol (authenticator role) for connectivity of wireless devices. [2]</td>
</tr>
</tbody>
</table>
8 REFERENCES

[1] HGI-RD001-R2.01 - Home Gateway Technical Requirements: Residential Profile V1.01
   http://members.nfc-forum.org/apps/group_public/download.php/18688/NFCForum-AD-BTSSP_1_1.pdf
[4] IETF RFC 2784 Generic Routing Encapsulation (GRE)