                 EAP Attributes for Wi-Fi - EPC Integration
                 draft-ietf-netext-wifi-epc-eap-attributes-14

Abstract

   With Wi-Fi emerging as a crucial access network for mobile service
   providers, it has become important to provide functions commonly
   available in 3G and 4G networks in Wi-Fi access networks as well.
   Such functions include Access Point Name (APN) Selection, multiple
   Packet Data Network (PDN) connections, and seamless mobility between
   Wi-Fi and 3G/4G networks.

   The EAP-AKA (and EAP-AKA') protocol is required for mobile devices to
   access the mobile Evolved Packet Core (EPC) via Wi-Fi networks. This
   document defines a few new EAP attributes to enable the above-
   mentioned functions in such networks. The attributes are exchanged
   between a client (such as a Mobile Node) and its network counterpart
   (such as a AAA server) in the service provider's infrastructure.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on May 18, 2015.

Copyright Notice

Table of Contents

1. Introduction

Wi-Fi has emerged as a "trusted" access technology for mobile service
providers; see [EPC2] for reference to the 3GPP description of
"trusted" access. Advances in IEEE 802.11u [IEEE802.11u] and
"HotSpot 2.0" [hs20] have enabled seamless roaming, in which a Mobile
Node can select and connect to a Wi-Fi access network just as it

would roam into a cellular network. It has thus become important to
provide certain functions in Wi-Fi which are commonly supported in
licensed-spectrum networks such as 3G and 4G networks. This draft
specifies a few new EAP attributes for a Mobile Node (MN) to interact
with the network to support some of these functions (see below).
These new attributes serve as a trigger for Proxy Mobile IPv6 network
nodes to undertake the relevant mobility operations. For instance,
when the Mobile Node requests and the network agrees for a new IP
session (i.e., a new Access Point Name or APN in 3GPP), the
corresponding attribute (defined below) acts as a trigger for the
Mobile Anchor Gateway (MAG) to initiate a new mobility session with
the Local Mobility Anchor (LMA). This document refers to [RFC6459]
for the basic definitions of mobile network terminology (such as APN)
used here.

The 3rd Generation Partnership Project (3GPP) networks support many
functions that are not commonly implemented in a Wi-Fi network. This
document defines EAP attributes that enable the following functions
in Wi-Fi access networks using EAP-AKA' [RFC5448] and EAP-AKA
[RFC4187]:

   o APN Selection

   o Multiple APN Connectivity

   o Wi-Fi to 3G/4G (UTRAN/EUTRAN) mobility

The attributes defined here are exchanged between the Mobile Node and
the EAP server, typically realized as part of the AAA server
infrastructure in a service provider's infrastructure. In
particular, the Wi-Fi access network simply conveys the attributes to
the service provider's core network where the EAP processing takes
place [EPC]. Since these attributes share the same IANA registry,
the methods are applicable to EAP-AKA', EAP-AKA, EAP-SIM [RFC4186]
and, with appropriate extensions, are possibly applicable for other
EAP methods as well. In addition to the trusted Wi-Fi access
networks, the attributes are applicable to any trusted "non-3GPP"
access network that uses the EAP methods and provides connectivity to
the mobile EPC, which provides connectivity for 3G, 4G, and other
non-3GPP access networks [EPC2].

1.1. APN Selection

The 3GPP networks support the concept of an APN (Access Point Name).
This is defined in [GPRS]. Each APN is an independent IP network
with its own set of IP services. When the MN attaches to the
network, it may select a specific APN to receive desired services.
For example, to receive generic Internet services, a user device may

   select APN "Internet" and to receive IMS voice services, it may
   select APN "IMSvoice".

   In a Wi-Fi access scenario, an MN needs a way of sending the desired
   APN name to the network. This draft specifies a new attribute to
   propagate the APN information via EAP. The agreed APN is necessary
   for the Proxy Mobile IPv6 MAG to initiate a new session with the LMA.

1.2. Multiple APN Connectivity

   As an extension of APN Selection, an MN may choose to connect to
   multiple IP networks simultaneously. 3GPP provides this feature via
   additional Packet Data Protocol (PDP) contexts or additional Packet
   Data Network (PDN) connections, and defines the corresponding set of
   signaling procedures. In a trusted Wi-Fi network, an MN connects to
   the first APN via DHCPv4 or IPv6 Router Solicitation. This document
   specifies an attribute that indicates the MN's capability to support
   multiple APN connectivity. The specific connectivity types are also
   necessary for the Proxy Mobile IPv6 signaling.

1.3. Wi-Fi to E-UTRAN mobility

   When operating in a multi-access network, an MN may want to
   gracefully handover its IP attachment from one access network to
   another. For instance, an MN connected to a 3GPP E-UTRAN network may
   choose to move its connectivity to a trusted Wi-Fi network.
   Alternatively, the MN may choose to connect using both access
   technologies simultaneously, and maintain two independent IP
   attachments. To implement these scenarios, the MN needs a way to
   correlate the UTRAN/E-UTRAN session with the new Wi-Fi session. This
   draft specifies an attribute to propagate E-UTRAN session
   identification to the network via EAP. This helps the network to
   correlate the sessions between the two Radio Access Network
   technologies and thus helps the overall handover process.

2. Terminology

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in [RFC2119].

3. Protocol Overview

3.1. Brief Introduction to EAP

   EAP is defined as a generic protocol in [RFC3748]. EAP, combined
   with one of the payload protocols such as EAP-AKA' [RFC5448] can
   accomplish several things in a network:

   o Establish identity of the user (MN) to the network.

   o Authenticate the user during the first attach with the help of an
      authentication center that securely maintains the user
      credentials. This process is called EAP Authentication.

   o Re-authenticate the user periodically, but without the overhead of
      a round-trip to the authentication center. This process is called
      EAP Fast Re-Authentication.

   This draft makes use of the EAP Authentication procedure. The use of
   EAP Fast Re-Authentication procedure is for further study. Both the
   EAP Authentication and EAP Fast Re-Authentication procedures are
   specified for trusted access network use in 3GPP. [TS-33.402]

3.2. IEEE 802.11 Authentication using EAP over 802.1X

   In a Wi-Fi network, EAP is carried over the IEEE 802.1X
   Authentication protocol. The IEEE 802.1X Authentication is a
   transparent, payload-unaware mechanism to carry the authentication
   messages between the MN and the Wi-Fi network elements.

   EAP, on the other hand, has multiple purposes. Apart from its core
   functions of communicating an MN's credentials to the network and
   proving the MN's identity, it also allows the MN to send arbitrary
   information elements to help establish the MN's IP session in the
   network. The following figure shows an example end-to-end EAP flow
   in the context of an IEEE 802.11 Wi-Fi network. We first define the
   terminology:

   o MN: Mobile Node

   o WAP: Wi-Fi Access Point

   o WAC: Wi-Fi Access Controller. In a PMIPv6 [RFC5213] network,
      hosts the MAG functionality or is assumed to have a suitable
      interface to the MAG. In the following, we simply use "WAC"
      notation. The MAG functionality within the WAC (or within the Wi-
      Fi access network), or a suitable interface to the MAG is assumed
      for PMIPv6 deployments.

   o IPCN: IP Core Network. This includes the LMA function. It
      generically also includes the AAA server function.

```
MN                           WAP                     WAC        IPCN
                                                    (MAG)      (LMA)
 1)|<----------Beacon--------|                        |          |
 2)|<----------Probe-------->|                        |          |
   |                         |                        |          |
   |             802.11 Auth| (Open System)           |          |
 3)|<---------------------->|<---------------------->|          |
   |                         |                        |          |
   |             802.11 | Association                 |          |
 4)|<---------------------->|<---------------------->|          |
   |                         |                        |          |
   |          (802.1X)       |         (CAPWAP/802.1X) |          |
 5)|<----EAP Req/Identity----|<----EAP Req/Identity----|          |
   |                         |                        |          |
 6)|----EAP Resp/Identity--->|----EAP Resp/Identity--->|          |
   |                         |                        |          |
 7)|<-EAP Req/AKA-Challenge--|<-EAP Req/AKA-Challenge--|          |
   |                         |                        |          |
 8)|-EAP Resp/AKA-Challenge->|-EAP Resp/AKA-Challenge->|          |
   |                         |                        |          |
 9)|<-----EAP Success--------|<-----EAP Success--------|          |
   |                         |                        |          |
10)|<====== 802.11 Data ====>|<=== CAPWAP(802.3 Data)=>|<=Tunnel to=>|
   |                         |                        | core network|
   |                         |                        |          |
```
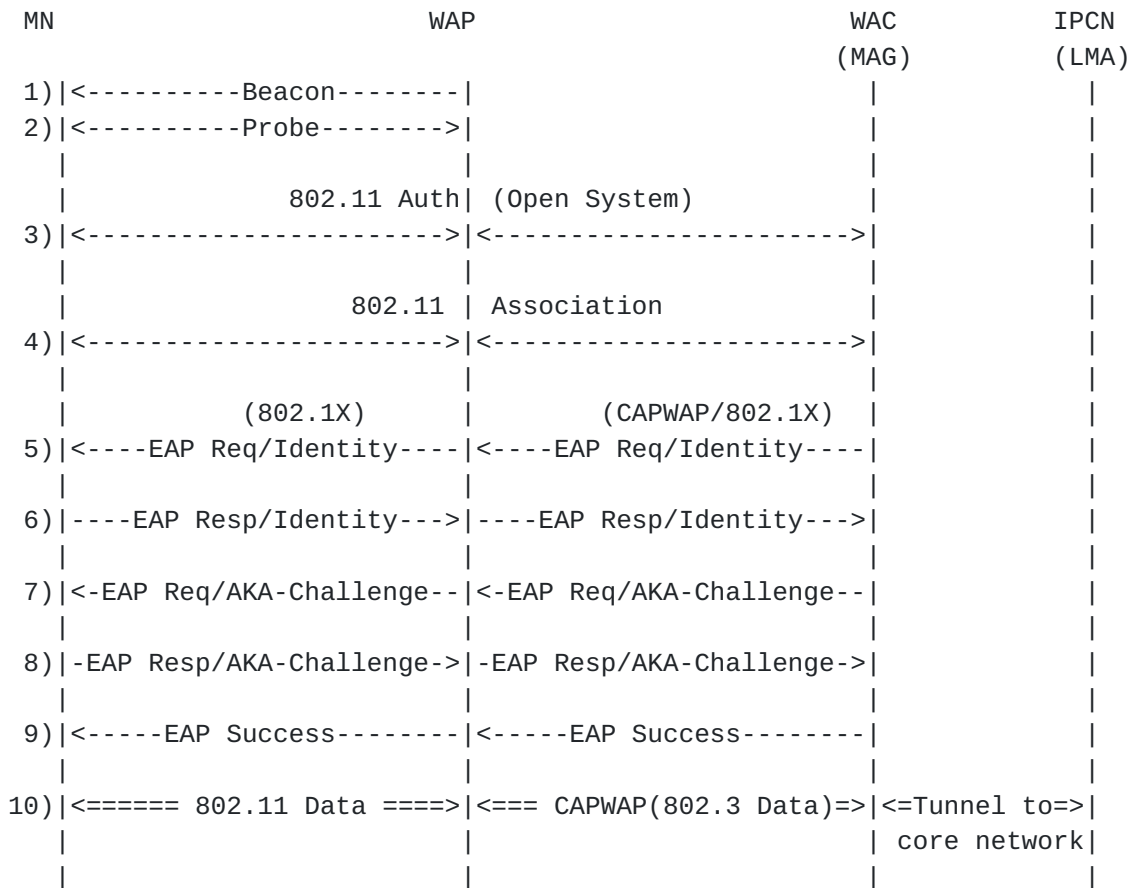
Figure 1: Example EAP Deployment

   The figure shows separate Wi-Fi Access Point and Wi-Fi Access
   Controller, following the split-MAC model of CAPWAP [RFC5415]. A
   particular deployment may have the two functions within a single
   node.

   1.   An MN detects a beacon from a WAP in the vicinity.

   2.   The MN probes the WAP to determine suitability to attach (Verify
        SSID list, authentication type and so on).

   3.   The MN initiates the IEEE 802.11 Authentication with the Wi-Fi
        network. In WPA/WPA2 mode, this is an open authentication
        without any security credential verification.

   4.   The MN initiates 802.11 Association with the Wi-Fi network.

   5.   The Wi-Fi network initiates 802.1X/EAP Authentication procedures
        by sending EAP Request/Identity.

   6.   The MN responds with its permanent or temporary identity.

7. The Wi-Fi network challenges the MN to prove its identity by
    sending EAP Request/AKA-Challenge.

8. The MN calculates the security digest and responds with EAP
    Response/AKA-Challenge.

9. If the authentication is successful, the Wi-Fi network responds
    to the MN with EAP Success.

10. An end-to-End data path is available for the MN to start IP
    layer communication (DHCPv4, IPv6 Router Solicitation and so
    on).

[4](). New EAP Attributes

The following sections define the new EAP attributes and their usage.

[4.1](). APN Selection

In a Wi-Fi network, an MN includes the AT_VIRTUAL_NETWORK_ID
attribute in the EAP-Response/AKA-Challenge to indicate the desired
APN identity for the first PDN connection.

If the MN does not include the AT_VIRTUAL_NETWORK_ID attribute in the
EAP-Response/AKA-Challenge, the network may select an APN by other
means. This selection mechanism is outside the scope of this
document.

An MN includes the AT_VIRTUAL_NETWORK_REQ attribute to indicate
single or multiple PDN capability. In addition, a sub-type in the
attribute indicates IPv4, IPv6, or dual IPv4v6 PDN connectivity.

[4.2](). Connectivity Type

An MN indicates its preference for connectivity using the
AT_CONNECTIVITY_TYPE attribute in the EAP-Response/AKA-Challenge
message. The preference indicates whether the MN wishes connectivity
to the Evolved Packet Core (the so-called "EPC PDN connectivity") or
Internet Offload (termed as "Non-Seamless Wireless Offload").

The network makes its decision and replies with the same attribute in
the EAP Success message.

[4.3](). Wi-Fi to UTRAN/E-UTRAN Mobility

When a multi-access MN enters a Wi-Fi network, the following
parameters are applicable in the EAP-Response/AKA-Challenge for IP
session continuity from UTRAN/E-UTRAN.

o AT_HANDOVER_INDICATION: This attribute indicates to the network
   that the MN intends to continue the IP session from UTRAN/E-UTRAN.
   If a previous session can be located, network will honor this
   request by connecting the Wi-Fi access to the existing IP session.

o AT_HANDOVER_SESSION_ID: An MN MAY use this attribute to identify
   the session on UTRAN/E-UTRAN. If used, this attribute contains
   P-TMSI (Packet Temporary Mobile Subscriber Identity) if the
   previous session was on UTRAN or M-TMSI (Mobile Temporary Mobile
   Subscriber Identity) if the previous session was on E-UTRAN. This
   attribute helps the network correlate the Wi-Fi session to an
   existing UTRAN/E-UTRAN session.

4.4. MN Serial ID

The MN_SERIAL_ID attribute defines an MN's serial number, including
International Mobile Equipment Identity (IMEI) and International
Mobile Equipment Identity Software Version (IMEISV). The IMEI (or
IMEISV) is used for ensuring a legitimate (and not a stolen) device
is in use. As with the others, this attribute is exchanged with the
service provider's AAA server. The MN_SERIAL_ID MUST NOT be
propagated further by the AAA server to any other node.

5. Attribute Extensions

The format for the new attributes follows that in [RFC4187]. Note
that the Length field value is inclusive of the first two bytes.

5.1. AT_VIRTUAL_NETWORK_ID

The AT_VIRTUAL_NETWORK_ID attribute identifies the virtual IP network
that the MN intends to attach to. The implementation of the virtual
network on the core network side is technology specific. For
instance, in a 3GPP network, the virtual network is implemented based
on the 3GPP APN primitive.

This attribute SHOULD be included in the EAP-Response/AKA-Challenge
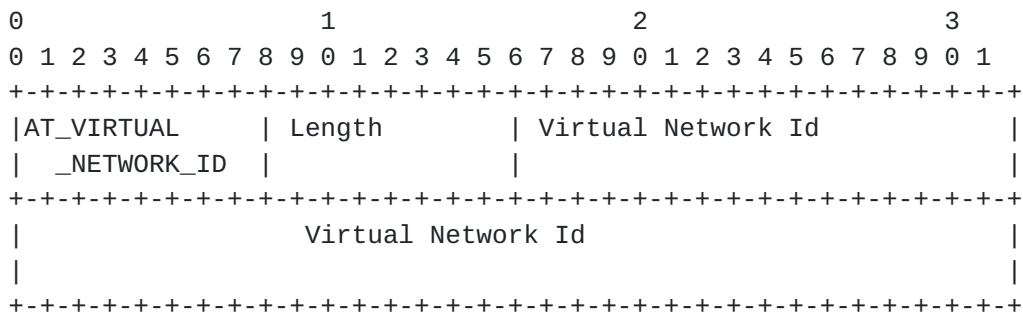message.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|AT_VIRTUAL     | Length        | Virtual Network Id            |
|  _NETWORK_ID  |               |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Virtual Network Id                         |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: AT_VIRTUAL_NETWORK_ID EAP Attribute

Virtual Network Id:

An arbitrary octet string that identifies a virtual network in the
access technology the MN is attaching to. For instance, in 3GPP
E-UTRAN, this could be an APN. See [TS-23.003] for encoding of the
field.

5.2. AT_VIRTUAL_NETWORK_REQ

When an MN intends to connect an APN, it SHOULD use this attribute to
indicate different capabilities to the network. In turn, the network
provides what is supported.

From the MN, this attribute can be included only in EAP-Response/
Identity. From the network, it SHOULD be included in the EAP
Request/AKA-Challenge message. In the MN-to-network direction, the
Type field (below) indicates the MN's request. In the network-to-MN
direction, the Type field indicates network's willingness to support
the request; a present Type field value indicates the network support
for that Type.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|AT_VIRTUAL_    |     Length    | Virt-Net-Req | Virt-Net-Req   |
|NETWORK_REQ    |               |    Type      |   Sub-type     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
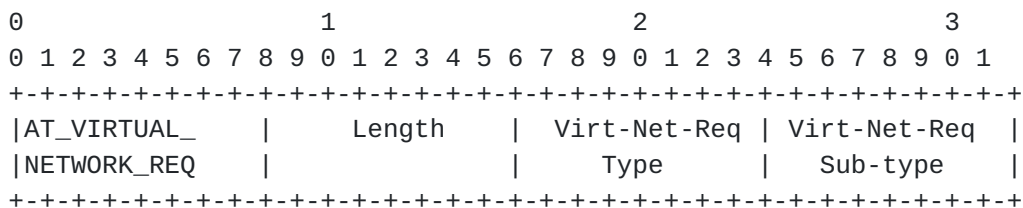
Figure 3: AT_VIRTUAL_NETWORK_REQ EAP Attribute

Virt-Net-Req Type:

Type can have one of the following values:

o   TBA IANA: Reserved

   o TBA IANA: Single PDN connection

   o TBA IANA : Multiple PDN connection. Can request Non-Seamless Wi-
      Fi Offload or EPC connectivity (see the Connectivity Type
      attribute below)

   Virt-Net-Req Sub-type:

   Sub-type can have one of the following values:

   o TBA IANA : Reserved

   o TBA IANA : PDN Type: IPv4

   o TBA IANA : PDN Type: IPv6

   o TBA IANA : PDN Type: IPv4v6

5.3. AT_CONNECTIVITY_TYPE

   An MN uses this attribute to indicate whether it wishes the
   connectivity type to be Non-Seamless WLAN Offload or EPC. This
   attribute is applicable for multiple PDN connections only.

   From the MN, this attribute can be included only in EAP-Response/
   Identity. From the network, it SHOULD be included in the EAP
   Request/AKA-Challenge message.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |AT_CONNECTIVITY|    Length     | Connectivity  | Reserved      |
   |_TYPE          |               | Type          |               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

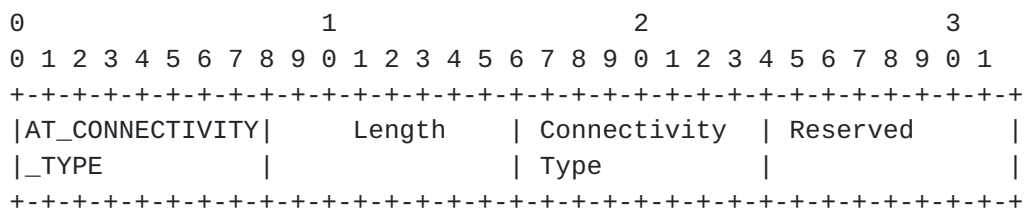   Figure 4: AT_CONNECTIVITY_TYPE EAP Attribute

   Connectivity Type:

   Connectivity Type can have one of the following values:

   o TBA IANA : Reserved

   o TBA IANA : Non-Seamless WLAN Offload (NSWO)

   o TBA IANA : EPC PDN connectivity

5.4. **AT_HANDOVER_INDICATION**

   This attribute indicates an MN's handover intention of an existing IP
   attachment.

   This attribute SHOULD be included in the EAP-Response/AKA-Challenge
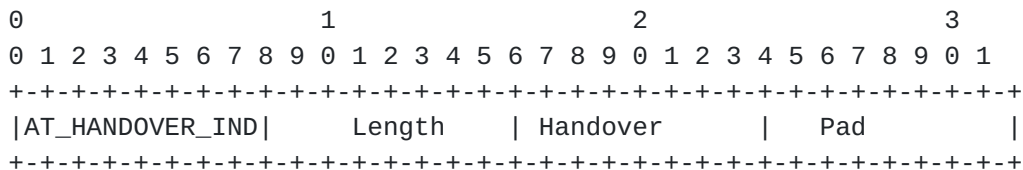   message.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |AT_HANDOVER_IND|    Length    | Handover     |    Pad         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

             Figure 5: AT_HANDOVER_INDICATION EAP Attribute

   Handover Type:

   o 0 - the MN has no intention of handing over an existing IP
      session, i.e., the MN is requesting an independent IP session with
      the Wi-Fi network without disrupting the IP session with the
      UTRAN/E-UTRAN. In this case, no Session Id (Section 5.5) is
      included.

   o 1 - the MN intends to handover an existing IP session. In this
      case, MN MAY include a Session Id (Section 5.5) to correlate this
      Wi-Fi session with a UTRAN/E-UTRAN session.

5.5. **AT_HANDOVER_SESSION_ID**

   When an MN intends to handover an earlier IP session to the current
   access network, it may propagate a session identity that can help
   identify the previous session from UTRAN/E-UTRAN that the MN intends
   to handover. This attribute is defined as a generic octet string.
   The MN MAY include an E-UTRAN GUTI if the previous session was an
   E-UTRAN session. If the previous session was a UTRAN session, the MN
   MAY include UTRAN Global RNC ID (MCC, MNC, RNC Id) and P-TMSI
   concatenated as an octet string.

   This attribute SHOULD be included in the EAP-Response/AKA-Challenge
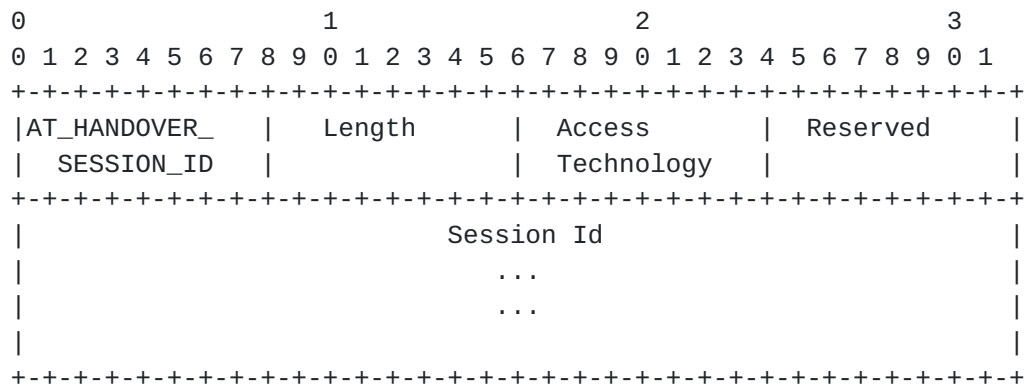   message.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|AT_HANDOVER_   |   Length      |   Access      |   Reserved    |
|  SESSION_ID   |               |   Technology  |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Session Id                           |
|                            ...                                |
|                            ...                                |
|                                                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

              Figure 6: AT_HANDOVER_SESSION_ID EAP Attribute

   Access Technology:

   This field represents the RAN technology from which the MN is
   undergoing a handover.

   o TBA IANA: Reserved

   o TBA IANA: UTRAN

   o TBA IANA: E-UTRAN

   Session Id:

   An octet string of variable length that identifies the session in the
   source access technology. As defined at the beginning of this
   section, the actual value is RAN technology dependent. For E-UTRAN,
   the value is GUTI. For UTRAN, the value is Global RNC Id (6 bytes)
   followed by P-TMSI (4 bytes). See [TS-23.003] for encoding of the
   field.

5.6. AT_MN_SERIAL_ID

   This attribute defines the MN's machine serial number. Examples are
   International Mobile Equipment Identity (IMEI) and International
   Mobile Equipment Identity Software Version (IMEISV).

   A network that requires the machine serial number for authorization
   purposes can send a request for the attribute in an EAP-Request/AKA-
   Challenge message. If the request is present, the MN SHOULD include
   the attribute in the EAP-Response/AKA-Challenge message. An MN MUST
   NOT provide the attribute unless it receives a request for it from an
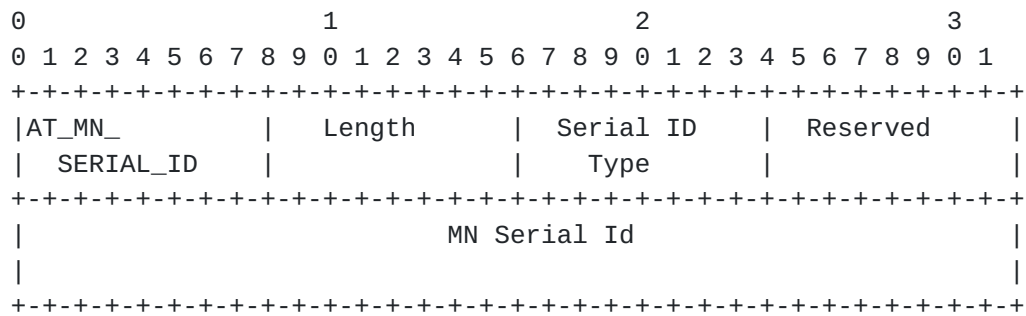   authenticated network.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|AT_MN_         |    Length     |  Serial ID    |   Reserved    |
|   SERIAL_ID   |               |    Type       |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         MN Serial Id                          |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 7: AT_MN_SERIAL_ID EAP Attribute

Serial ID Type:

This field identifies the type of the MN Identifier.

o   TBA IANA: Reserved

o   TBA IANA: IMEI

o   TBA IANA: IMEISV

MN Serial Id:

An arbitrary octet string that identifies the MN's machine serial
number. The actual value is device-specific. See [TS-23.003] for
encoding of the field. When sent by the network in the EAP-Request/
AKA-Challenge message, this field is not present, which serves as an
indication for the MN to provide the attribute in the EAP-Response/
AKA-Challenge message.

AT_MN_SERIAL_ID attribute MUST only be used with methods which can
provide mutual (network and device) authentication, such as AKA, AKA'
and EAP-SIM.

6. Security Considerations

This document defines new EAP attributes to extend the capability of
the EAP-AKA protocol as specified in Section 8.2 of [RFC4187]. The
attributes are passed between an MN and a AAA server in provider-
controlled trusted Wi-Fi networks. The document does not specify any
new messages or options to the EAP-AKA protocol.

The attributes defined here are fields which are used in existing 3G
and 4G networks, where they are exchanged (in protocols specific to
3G and 4G networks) subsequent to the mobile network authentication
(e.g., using the UMTS-AKA mechanism). For the operator-controled Wi-
Fi access which is connected to the same core infrastructure as the

3G and 4G access, similar model is followed here with the EAP-AKA (or EAP-AKA', EAP-SIM) authentication. In doing so, these attribute processing, security-wise, is no worse than that in existing 3G and 4G mobile networks.

The attributes inherit the security protection (integrity, replay, and confidentiality) provided by the paratmeters in the AKA(') or SIM methods ; see Section 12.6 in [RFC4187]. Furthermore, RFC 4187 requires attributes exchanged in EAP-Request/AKA-Identity or EAP-Response/AKA-Identity to be integrity-protected with AT_CHECKCODE; see Section 8.2 in [RFC4187]. This requirement applies to the AT_CONNECTIVITY_TYPE and AT_VIRTUAL_NETWORK_REQ attributes defined in this document.

The AT_MN_SERIAL_ID attribute MUST have confidentiality protection provided by the AKA(') or EAP-SIM methods beyond the secure transport (such as private leased lines, VPN etc.) deployed by the provider of the trusted Wi-Fi service.

7. IANA Considerations

This document defines the following new skippable EAP-AKA attributes. These attributes need assignments from the "EAP-AKA and EAP-SIM Parameters" registry at https://www.iana.org/assignments/eapsimaka-numbers

o AT_VIRTUAL_NETWORK_ID (Section 5.1) - TBA by IANA

o AT_VIRTUAL_NETWORK_REQ (Section 5.2) - TBA by IANA

o AT_CONNECTIVITY_TYPE (Section 5.3) - TBA IANA

o AT_HANDOVER_INDICATION (Section 5.4) - TBA by IANA

o AT_HANDOVER_SESSION_ID (Section 5.5) - TBA by IANA

o AT_MN_SERIAL_ID (Section 5.6) - TBA by IANA

This document requests a new IANA registry "Trusted non-3GPP Access EAP Parameters". The range for both Types and Sub types in the registry is 0 - 127, with 0 (zero) being a reserved value. The document requests IANA to make assignments in a monotonically increasing order in increments of 1, starting from 1. New assignments in this registry are made with the Specification Required policy [RFC5226].

The IANA Designated Expert should review the requirements for new assignments based on factors including, but not limited to, the

source of request (e.g., standards bodies), deployment needs (e.g.,
industry consortium, operator community) and experimental needs
(e.g., academia, industrial labs). A document outlining the purpose
of new assignments should accompany the request. Such a document
could be a standards document, or a research project description.
The Designated Expert should consider that there is sufficient
evidence of potential usage both on the end-points (e.g., Mobile
Devices etc.) and the infrastructure (e.g., AAA servers, gateways
etc.)

The document requests assignments from the new registry for the
following fields defined in this document:

o Virt-Net-Req Type (Section 5.2) - TBA by IANA

o Virt-Net-Req Sub type (Section 5.2) - TBA by IANA

o Connectivity Type (Section 5.3) - TBA IANA

o Access Technology (Section 5.5) - TBA by IANA

o Serial ID Type (Section 5.6) - TBA by IANA

8. Acknowledgment

Thanks to Sebastian Speicher for the review and suggesting
improvements. Thanks to Mark Grayson for proposing the MN Serial ID
attribute. And, thanks to Brian Haberman for suggesting a new
registry.

9. References

9.1. Normative References

[RFC4187]   Arkko, J. and H. Haverinen, "Extensible Authentication
            Protocol Method for 3rd Generation Authentication and Key
            Agreement (EAP-AKA)", RFC4187, January 2006,
            <http://tools.ietf.org/html/rfc4187>.

[RFC5226]   Narten, T. and H. Alvestrand, "Guidelines for Writing an
            IANA Considerations Section in RFCs", BCP 26, RFC 5226,
            May 2008.

[RFC6459]   Korhonen, J., Soininen, J., Patil, B., Savolainen, T.,
            Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation
            Partnership Project (3GPP) Evolved Packet System (EPS)",
            RFC 6459, January 2012.

9.2. Informative References

   [EPC]   "General Packet Radio Service (GPRS); enhancements for
              Evolved Universal Terrestrial Radio Access Network
              (E-UTRAN) access, 3GPP TS 23.401 8.8.0, December 2009.",
              <http://www.3gpp.org/ftp/Specs/html-info/23401.htm>.

   [EPC2]   "Architecture enhancements for non-3GPP accesses, 3GPP TS
              23.402 8.8.0, December 2009.",
              <http://www.3gpp.org/ftp/Specs/html-info/23402.htm>.

   [GPRS]   "General Packet Radio Service (GPRS); Service description,
              Stage 2, 3GPP TS 23.060, December 2006",
              <http://www.3gpp.org/ftp/Specs/html-info/23060.htm>.

   [IEEE802.11u]
              "802.11u-2011 - IEEE Standard for Information Technology-
              Telecommunications and information exchange between
              systems- Local and Metropolitan networks-specific
              requirements- Part II: Wireless LAN Medium Access Control
              (MAC) and Physical Layer (PHY) specifications: Amendment
              9: Interworking with External Networks", , Feb 2011,
              <http://standards.ieee.org/findstds/
              standard/802.11u-2011.html>.

   [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H.
              Levkowetz, Ed., "Extensible Authentication Protocol
              (EAP)", RFC3748, June 2004,
              <http://www.ietf.org/rfc/rfc3748.txt>.

   [RFC4186] Haverinen, H. and J. Salowey, "Extensible Authentication
              Protocol Method for Global System for Mobile
              Communications (GSM) Subscriber Identity Modules (EAP-
              SIM)", RFC 4186, January 2006.

   [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K.,
              and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

   [RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And
              Provisioning of Wireless Access Points (CAPWAP) Protocol
              Specification", RFC5415, January 2009,
              <http://www.ietf.org/rfc/rfc5415.txt>.

   [RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved
              Extensible Authentication Protocol Method for 3rd
              Generation Authentication and Key Agreement (EAP-AKA')",
              RFC 5448, May 2009.

[TS-23.003]
            "3rd Generation Partnership Project: Numbering, Addressing
            and Identification, 3GPP TS 23.003 12.2.0, March 2014.", ,
            <http://www.3gpp.org/ftp/Specs/html-info/23003.htm>.

[TS-33.402]
            "3GPP System Architecture Evolution (SAE); Security
            aspects of non-3GPP accesses, 3GPP TS 33.402 8.6.0,
            December 2009.", ,
            <http://www.3gpp.org/ftp/Specs/html-info/33402.htm>.

[hs20]   "Hotspot 2.0 (Release 2) Technical Specification Package
            v1.0.0", , <https://www.wi-fi.org/hotspot-20-release-2-
            technical-specification-package-v100>.

Appendix A. Change Log

o: Initial Draft

o: v01: status to Informational, Updated References, Revised the
Figure

o: No changes from 01 to 02

o: Per recent 3GPP updates, added the Connectivity Type attribute
to allow indicating Non-Seamless WLAN Offload or EPC connectivity

o: version-04: Revised AT_VIRTUAL_NETWORK_REQ to include 1) single
PDN vs Multiple PDN connections, 2) PDN Types, and referred to
NSWO Connectivity Type attribute

o: version 05: Added AT_MN_SERIAL_ID. Revised the IANA
Considerations section

o: version 06, 07: various edits

o: AD review revs

o: version 09: IETF LC, Directorate review revs

o: IANA Section revision, based on IANA interaction

o: version 12 - clarified/revised: 1) IMEI purpose, 2) attributes
requirement in PMIP6 signaling, 3) references to 802.11u, HotSpot
2.0 (seamless roaming) 4) References (normative/informative), 5)
editorial corrections

       o: version 13 - revised AT_MN_SERIAL_ID processing per IESG
       DISCUSS

       o: version 14 -clarified usage of AT_MN_SERIAL_ID. Provided
       additional reference to "trusted" Wi-Fi access.

Authors' Addresses

   Ravi Valmikam
   Unaffiliated
   USA

   Email: valmikam@gmail.com

   Rajeev Koodli
   Intel
   USA

   Email: rajeev.koodli@intel.com