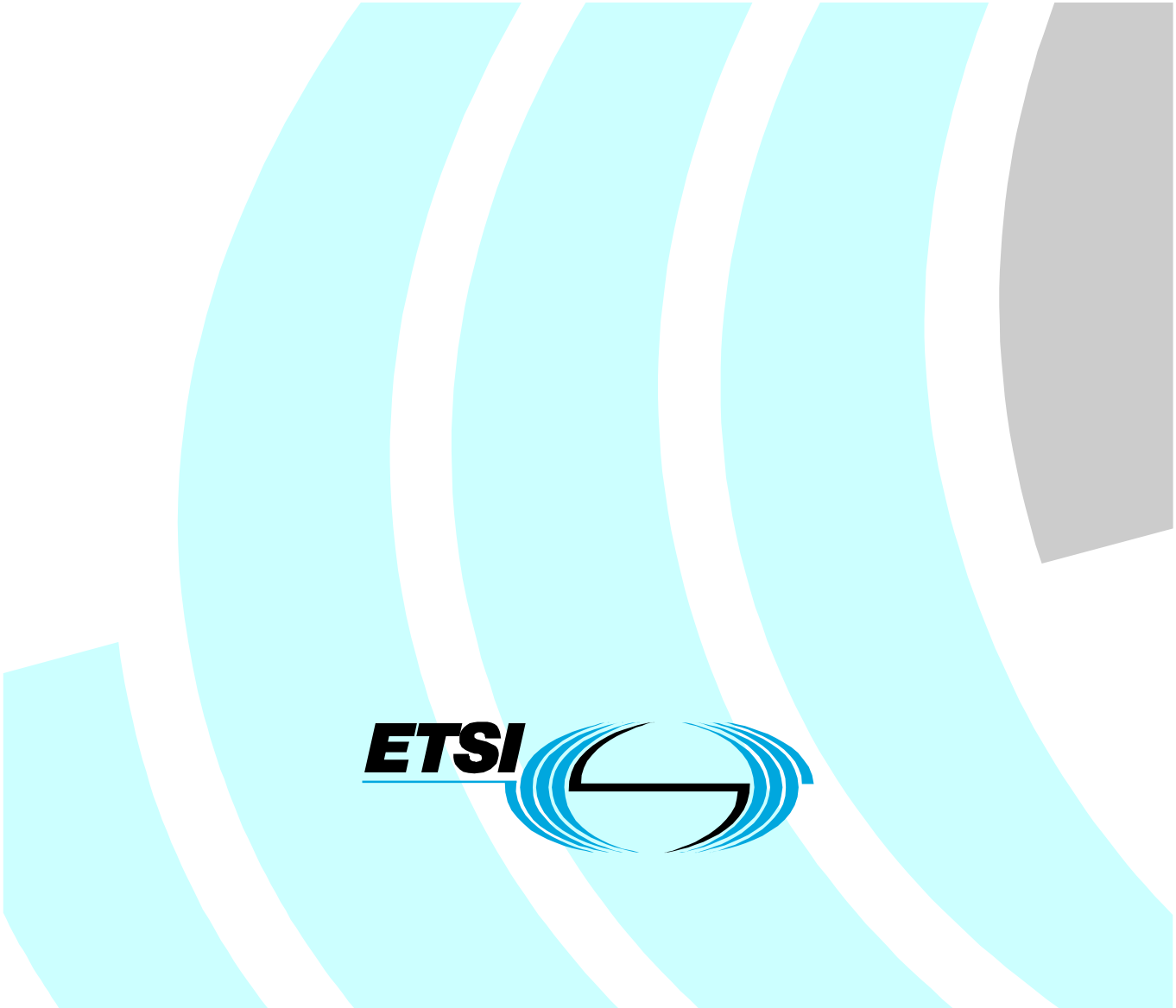
ETSI TS 183 020 V1.1.1 (2006-03)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment: Roaming in TISPAN NGN Network Accesses; Interface Protocol Definition



Reference
DTS/TISPAN-03042-NGN-R1

Keywords
access, interface, network, roaming

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document describes the protocol specifications and profiles for the interface between the UAAF in the visited NGN network (UAAF-proxy) and the UAAF in the home NGN network (UAAF-server). The specifications of this interface will be common for both xDSL and WLAN access networks, including possible other access network types as well. Specific differences, if any, will be called out.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

[2] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[3] ETSI TS 129 234: "Universal Mobile Telecommunications System (UMTS); 3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3 (3GPP TS 29.234 Release 6)".

[4] Wi-Fi Alliance: "WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks".

NOTE: http://www.wi-fi.org/OpenSection/pdf/WPA_for_Public_Access_Final.pdf

[5] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[6] IETF RFC 2486bis: "The Network Access Identifier".

[7] ETSI TS 183 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; Network Access xDSL and WLAN Access Networks; Interface Protocol Definitions".

[8] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[9] ETSI ES 283 034: "TISPAN; Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol".

[10] ETSI TS 183 017: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification".

[11] ETSI ES 283 035: "TISPAN; Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol".

[12] IETF RFC 3539: "Authentication, Authorization and Accounting (AAA) Transport Profile".

[13] IETF RFC 4005: "Diameter Network Access Server Application".

[14] IETF RFC 4072: "Diameter Extensible Authentication Protocol (EAP) Application".

[15] IETF RFC 3588: "Diameter Base Protocol".

[16] IETF RFC 4372: "Chargeable User Identity".

[17] IETF RFC 2866: "RADIUS Accounting".

[18] IETF RFC 3580: "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines".

[19] IETF RFC 2548: "Microsoft Vendor-specific RADIUS Attributes".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

access network: collection of network entities and interfaces that provide the underlying IP transport connectivity between end user devices and NGN entities

Attribute-Value Pair: see RFC 3588 [15], it corresponds to an Information Element in a Diameter message

functional entity: entity that comprises a specific set of functions at a given location. Functional entities are logical concepts, grouping of functional entities are used to describe practical physical realizations

Core Network: portion of the delivery system composed of networks, systems equipment and infrastructures, connecting the service providers to the access network

user equipment: one or more devices allowing a user to access services delivered by TISPAN NGN networks

NOTE: This includes devices under user control commonly referred to as CPE, IAD, ATA, RGW, TE, etc., but not network controlled entities such as access gateways.

visited NGN network: NGN network through which the User Equipment gains network connectivity

NOTE: The NGN Network includes both the Access Network and the Core Network. The User Equipment does not have a service relationship with the business entity that operates this network.

home NGN network: NGN network through which the User Equipment gains network connectivity

NOTE: The NGN Network includes both the Access Network and the Core Network. The User Equipment has a service relationship with the business entity that operates this network.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	Third Generation Project Partnership
AAA	Authentication, Authorization and Accounting
AAA-H	AAA-Home
AAA-V	AAA-Visited
AMF	Access Management Function
AP	Access Point
ATA	Analogue Terminal Adaptor
AVP	Attribute Value Pair
CNG	Customer Network Gateway
EAP	Extensible Authentication Protocol
EAPOL	EAP Over Lan
GSMA	Global System for Mobile communications Association
IAD	Integrated Access Device
IETF	Internet Engineering Task Force

IP	Internet Protocol
NAI	Network Access Identifier
NASS	Network Attachment SubSystem
NGN	Next Generation Network
PEAP	Protected EAP
RGW	Residential GateWay
STA	Station
TE	Terminal Equipment
TLS	Transport Layer Security
TTLS	Tunnelled TLS
UAAF	User Access Authorization Function
UE	User Equipment
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
xDSL	Digital Subscriber Line

4 NGN General Architecture

ES 282 001 [1] provides a description of the general network architecture of the NGN. The model is depicted in figure 1.

Figure 1: General NGN Network Model

Interface e1 is an access-network-specific interface, and is dependant on the access technology being used (xDSL, WLAN, and so on). Interface e5 is a roaming interface, and is independent of the access technology. Interface e5 is used to provide a consistent method for the visited NGN network to communicate with the home NGN network.

Figure 2 depicts the functional composition of the access network and the NGN core for the roaming scenario, where a UE obtains network access via a visited NGN network and authenticates back with the home NGN network. Details of this model may be found in ES 282 004 [2].

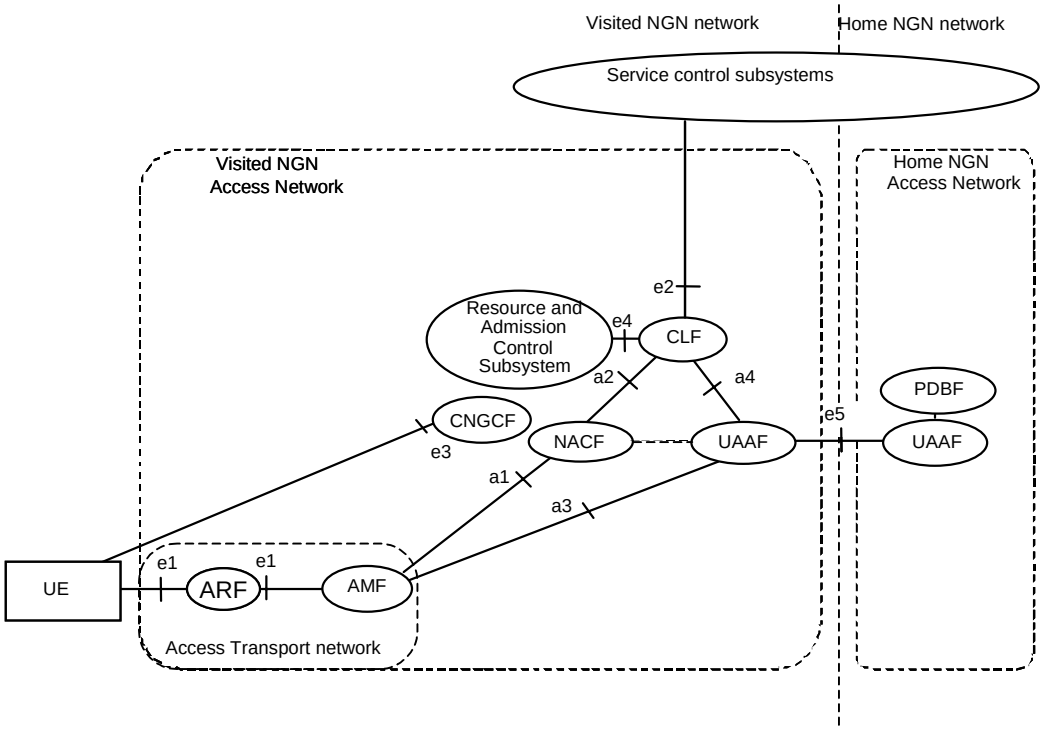


Figure 2: NASS mapped onto functional network roles - roaming scenario

4.1 Overview of Interface e5

The present document details the protocols and profiles for interface e5. This interface is intended to be used between a UAAF-proxy and a UAAF-server, which may be in different distractive domains. This interface allows the UAAF-proxy to request the UAAF-server for user authentication and authorization, based on user profiles. It also allows the UAAF-proxy to forward accounting data for the particular user session to the UAAF-server.

The UAAF-proxy will forward access and authorization requests, as well as accounting messages, received over interface a3 from the AMF, to the UAAF-server over interface e5. Responses received back in return from the UAAF-server over interface e5 will be forwarded to the AMF over interface a3. A bilateral trust relationship will need to be setup between the UAAF-proxy and the UAAF-server in order to facilitate this exchange.

The specifications for interface e5 will be similar to that of interface a3, between the AMF and the UAAF in the visited network.

This interface therefore supports AAA message exchange between the UAAF-proxy and the UAAF-server. RADIUS and Diameter are two possible options for carrier protocols on this interface, and detailed requirements are listed in the present document. Interface e5 supports both authentication/authorization and accounting message exchange.

The present document will be common for both xDSL and WLAN access networks, as well as for potential other types of access networks. Specific differences, if any, will be called out in the document.

5 Protocols and profiles for Interface e5

5.1 802.1X-based Authentication

Figure 4 depicts a typical protocol stack for 802.1X-based authentication. Further details may be found in Wi-Fi Alliance [4]. The EAP messages are carried over EAPOL (EAP over LAN) frames between the UE and the AP and then re-encapsulated in RADIUS or Diameter messages when sent from the AP to the home AAA Server (via zero or more AAA proxies). In figure 4, the UE (mobile station) acts as the 802.1X supplicant, the AP acts as the authenticator, and the RADIUS AAA server acts as the authentication server.

For security reasons, RADIUS is sometimes also carried over IPsec (RFC 3162 (see Bibliograhy) describes use of RADIUS over IPv6-IPsec, and RFC 3580 [18] also recommends use of IPsec to protect RADIUS). Diameter may also be used instead of or in addition to RADIUS.

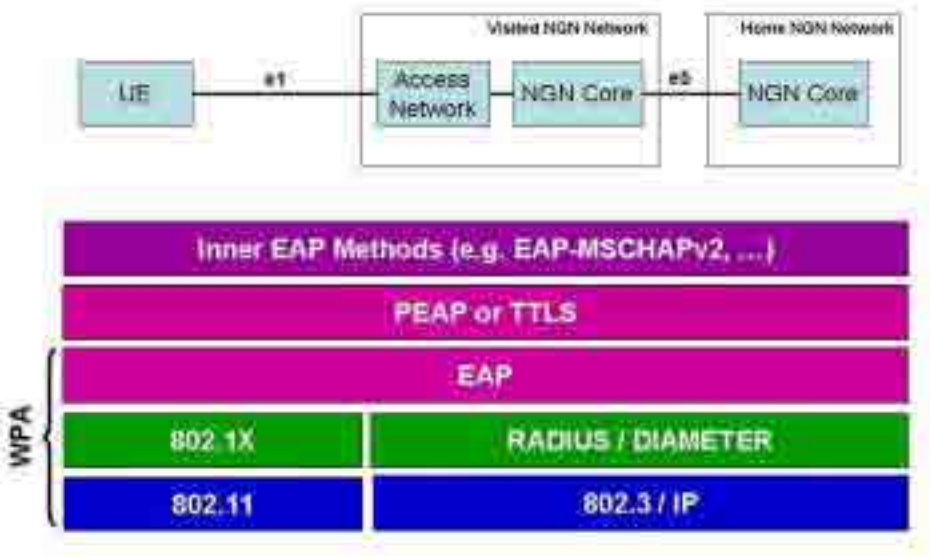


Figure 3: 802.1X/EAP Authentication Protocol Stack

Figure 5 depicts a typical 802.1X-based authentication scenario. The UE attempts to associate with an AP and is challenged to authenticate. At this point, the UE needs to indicate its user identity. There are usually two parts to this identity: the user name and the realm. Typically, these are combined into a Network Access Identifier (NAI) of the form user@realm. The realm part of the NAI is used to establish a connection with the appropriate AAA-H for that user. This presumes that the visited network recognizes that realm name. If this is not the case, then the visited network will signal an authentication failure back to the UE. The UE can then either try a different account (with a different realm) or can try to establish a new account on the visited network. If those alternatives also fail, the UE will be denied access or will be granted only limited guest access.

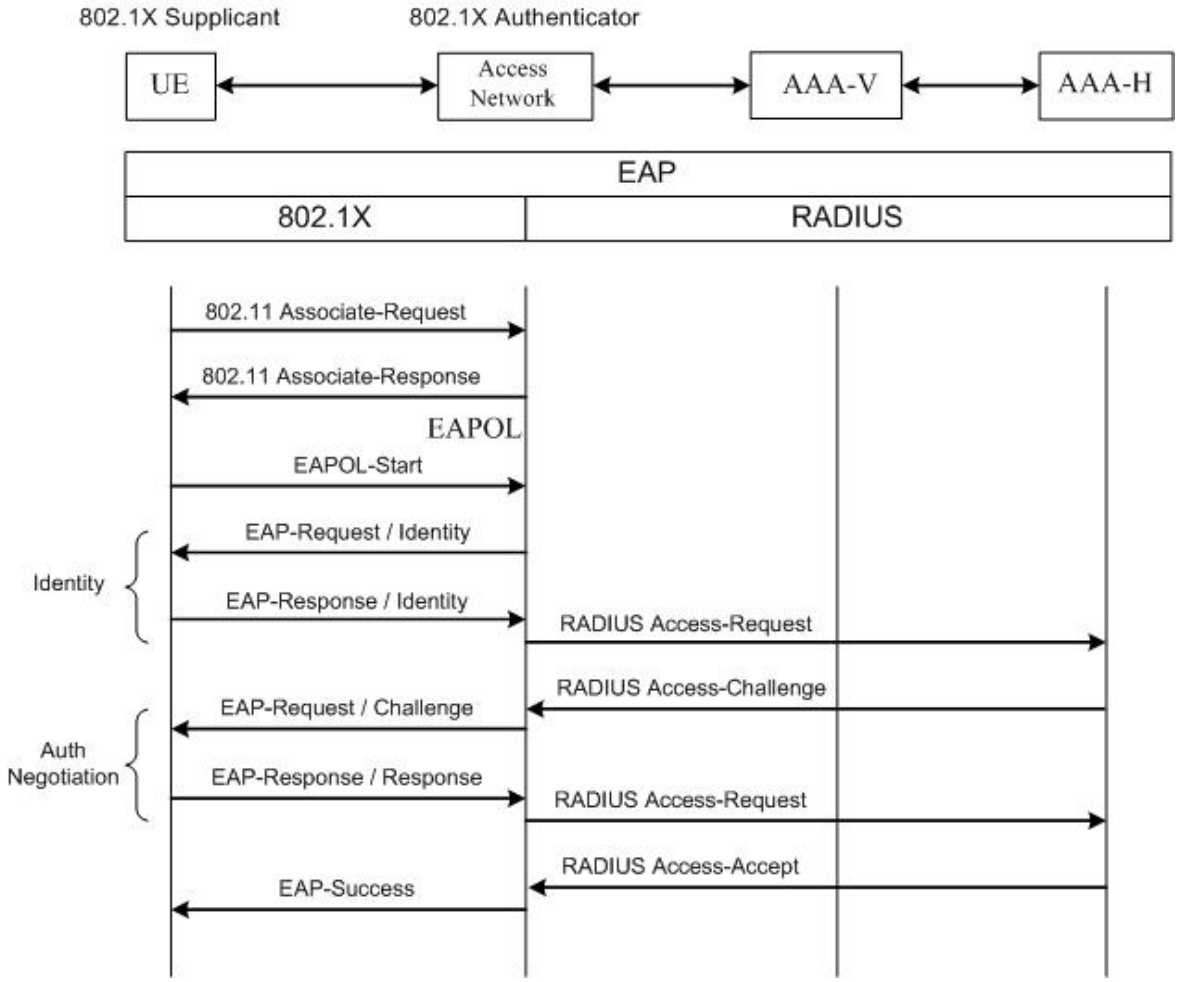


Figure 4: 802.1X-based authentication with RADIUS as AAA protocol

To avoid revealing the true user identity to an entity other than the home service provider, especially across the WLAN radio link, the UE can use a generic user name like "anonymous" or "user" in the NAI given in the initial identity exchange. The realm part of the NAI is the only information the visited network needs to know at this point. If PEAP or TTLS are used to establish a secure tunnel between the STA and the AAA-H, then the protected identity exchange will not be visible to the visited network or to any eavesdroppers. The visited network will eventually need to obtain some identity value for charging and billing purposes if the authentication is successful. The home network can provide the identity that identifies the account for charging. This account is used between the visited network and the home network. This account need not be the same as that used by the home network to bill the subscriber. Furthermore, this identity can be an alias specified by the home provider rather than information that might compromise the true identity of the UE user. The identity used for charging can be shared only with the AAA infrastructure and never needs to be sent unprotected across the WLAN radio link.

5.2 Intermediaries

An intermediary may be defined as an entity that manages and facilitates AAA transactions in real time between 2 service provider network entities. One or more intermediaries may exist between the visited and the home NGN networks, as shown in figure 5. The existence of these intermediaries should be transparent to the AAA message flow, and each intermediary shall support the requirements as noted in the following clauses.

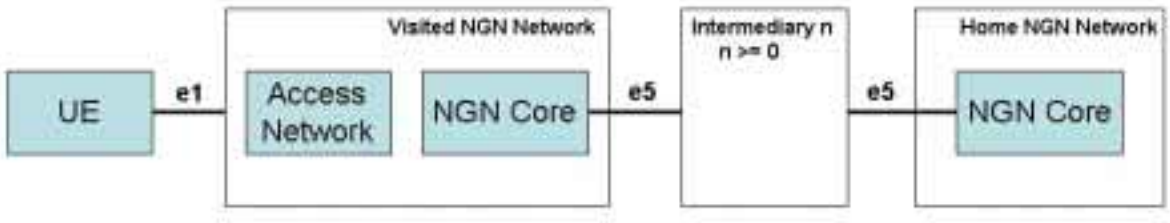


Figure 5: Inclusion of intermediaries

5.3 Requirements of the visited NGN network

One endpoint of interface e5 is the visited NGN network. Specifically, the access network within the visited NGN network should support the following requirements, and interface e5 for AAA logically extends all the way from the access network to the UAAF in the home NGN network.

1) The visited NGN network shall comply with the relevant requirement in TS 129 234 [3], clauses 4 and 5. In TS 129 234 [3], all references to "3GPP AAA Proxy" implies the requirements shall be met by the visited NGN network and all references to "3GPP AAA Server" implies the requirements are to be met by the home NGN network.

2) The visited NGN network shall support either RADIUS or Diameter as the AAA transport.

3) If Diameter is supported, the visited NGN access network shall support the following IETF standards:

   a) RFC 3539 [12], Authentication, Authorization and Accounting (AAA) Transport Profile.

   b) RFC 4005 [13], Diameter Network Access Application.

   c) RFC 4072 [14], Diameter Extensible Authentication Protocol (EAP) Application.

4) If RADIUS is supported, the visited NGN access network shall support the following IETF standards:

   a) Interpretation of Idle-Timeout attribute in RFC 2865 [8]: If a wireless station is logged on to the network but has not generated outbound IP data traffic (the definition of what constitutes this traffic is being defined in the RADEXT group in the IETF) for a specific interval of time, and if the home NGN network has specified this interval of time via the Idle-Timeout attribute, the visited access network shall proactively disconnect the wireless station and generate an Accounting-Stop message. The actual Idle-Timeout value may be set locally on the access network or via the Idle-Timeout attribute provided by the Home NGN network. If this attribute is present in the AAA message, it shall override any local timeout value set on the access network.

   b) Interpretation of Session-Timeout attribute in RFC 2865 [8]: The timeout value is typically set according to the expiration time of the prepaid account. If the wireless station remains connected until the timeout expires, the access network either automatically disconnects that wireless station or requests for a re-authentication, depending on the value of the Termination-Action attribute.

   c) The access network shall be able to appropriately process receipt of at least 5 Class attributes (defined in RFC 2865 [8]).

   d) RFC 2866 [17], RADIUS Accounting:

      I) The Accounting-Start message shall be sent when the wireless station successfully authenticates to the network and is authorized for services.

II) The access network shall detect session termination, either via user disconnect/disassociate, inactivity timer expiry, or session-timeout. When this happens, an Accounting-Stop message shall be sent.

III) The access network shall send Accounting-Interim records at the interval specified by the home network.

IV) The access network shall report the wireless station IP address in the Framed-IP-Address RADIUS attribute in the Accounting-Interim and Accounting-Stop messages. Inclusion of the wireless station IP address in the Framed-IP-Address RADIUS attribute in the Accounting-start message is optional.

V) If multiple accounting messages are generated by different physical entities within the access network for the same session, all related accounting messages shall contain the same Session-Id.

VI) The NAS shall send the appropriate Accounting On and Off messages to the home network when it undergoes a reset, to enable session state to be cleared on the home AAA server.

VII) The access network may attempt to deliver accounting records until an acknowledgement is received.

e) RFC 3580 [18], RADIUS Usage Guidelines.

f) RFC 3748 [5], Extensible Authentication Protocol (EAP).

g) The visited NGN network shall be able to accept WPA keying information contained in Microsoft vendor-specific RADIUS attributes as defined in the following sections of RFC 2548 [19]:

1) Section 2.4.2: MS-MPPE-Send-Key.

2) Section 2.4.3: MS-MPPE-Recv-Key.

h) The visited NGN network shall be able to proxy RADIUS Authentication and Accounting messages as defined in RFC 2865 [8] and RFC 2866 [17].

i) The visited NGN network shall be able to send back the Chargeable-User-Identity attribute (RFC 4372 [16]), defined in the RADEXT group in the IETF, in Accounting messages, if it was send in an authorization message by the authenticating AAA server.

5) The visited NGN access network should support IPSec for protecting AAA message flows.

5.4 Requirements of the home NGN network

1) The home NGN network shall comply with the relevant requirements in TS 129 234 [3], clauses 4 and 5. In TS 129 234 [3], all references to "3GPP AAA Proxy" implies the requirements shall be met by the visited NGN network (specifically the access network), and all references to "3GPP AAA Server" implies the requirements are to be met by the home NGN network.

2) The home NGN network shall support WPA/802.1X:

a) The home network shall support EAP methods defined in [7], clause 8.2.

b) The home network shall support NAIs as specified by RFC 2486bis [6].

3) The home NGN network may support WPA2.

4) The visited NGN network shall support either RADIUS or Diameter as the AAA transport.

5) The home NGN network shall support the following IETF standards:

a) RFC 3748 [5], Extensible Authentication Protocol (EAP)

b) RFC 2486 bis [6], Network Access Identifier

6) If Diameter is supported, the home NGN network shall support the following IETF standards:

a) RFC 3539 [12], Authentication, Authorization and Accounting (AAA) Transport Profile.

b) RFC 4005 [13], Diameter Network Access Application.

c) RFC 4072 [14], Diameter Extensible Authentication Protocol (EAP) Application.

7) If RADIUS is supported, the home NGN network shall support the following IETF standards:

a) RFC 2865 [8], RADIUS Standard.

b) RFC 2866 [17] , RADIUS Accounting.

c) RFC 3580 [18], RADIUS Usage Guidelines.

d) The home NGN network shall support the transmission of WPA keying information to the access network via Microsoft vendor-specific RADIUS attributes as defined in the following sections in RFC 2548 [19]:

1) Section 2.4.2: MS-MPPE-Send-Key.

2) Section 2.4.3.: MS-MPPE-Recv-Key.

8) The home network should support IPSec for protecting AAA message flows.

5.5 Subscriber Profile Transfer

The protocol used on the e5 interface shall support the transport of subscriber profile information as defined in ES 282 004 [2]. Table 1 provides the list of information elements to be carried over the interface for that purpose and indicates the list of Diameter attributes that shall be supported to achieve it.

Table 1: Diameter attributes for Subscriber Profile Transfer

Information Element	Description	DIAMETER attribute	Defined in
SubscriberID	The identity of the subscriber requesting IP connectivity.	User-Name	RFC 3588 [15]
GloballyUniqueAddress	This information element contains: - The IP address of the user equipment used by the subscriber for which profile information is being pushed. - The addressing domain in which the IP address is significant.	Globally-Unique-Address	ES 283 034 [9]
InitialGateSetting	This information element contains: - The list of default destination IP addresses and ports to which traffic can be sent. - The maximum amount of bandwidth that can be used without explicit authorisation in the uplink direction. - The maximum amount of bandwidth that can be used without explicit authorisation in the downlink direction.	Initiate-Gate-Setting	ES 283 034 [9]

Information Element	Description	DIAMETER attribute	Defined in
QoSProfile (NOTE 1)	For each subscribed transport service class and application class, this information element contains: - The maximum amount of bandwidth subscribed by the attached user in the uplink direction. - The maximum amount of bandwidth subscribed by the attached user in the downlink direction. - The maximum priority allowed for any reservation request.	QoS-Profile	ES 283 034 [9]
PrivacyIndicator (see note)	This information element provides policy rules for disclosure of subscriber profile elements to applications.	Privacy-Indicator	The present document (clause 5.5.1).
NOTE: This information element may be repeated.			

There is currently no standard solution defined for transferring subscriber profile data across networks where RADIUS is used instead of Diameter. This may be defined in Release 2.

5.5.1 Privacy-Indicator AVP

The Privacy-Indicator AVP (AVP code 440 13019) is of type Grouped and provides policy rules for disclosure of subscriber profile elements to applications.

AVP Format:

```
Privacy-Indicator ::= < AVP Header: 440 13019 >
          * {Requested-Information}
          * [AF-Application-Identifier]
```

Each Requested-Information AVP identifies a profile element whose disclosure is restricted to the list of applications identified by the AF-Application-Identifier AVPs. The Requested-Information AVP is defined in ES 283 035 [11] while the AF-Application-Identifier AVP is defined in TS 183 017 [10].

Annex A (informative): Tracking of Standards-related Work

A.1 Items to be tracked

These are items that are on the standards-track in the standards bodies. Their progress should be monitored, and the relevant requirements reflected appropriately.

1) Carrying Location Objects in RADIUS

   a) The GEOPRIV task group in the IETF is working on this, and draft-ietf-geopriv-radius-lo (see Bibliography) should be tracked.

2) End to end capabilities support for RADIUS

   b) The RADEXT task group in the IETF is working on this, and draft-lior-radext-end-to-end-caps (see Bibliography) should be tracked.

3) RADIUS Extensions for IEEE 802 (see Bibliography)

   c) The RADEXT group in the IETF is working on this, and draft-congdon-radext-ieee802-03X3 (see Bibliography) should be tracked.

4) Network bandwidth parameters for RADIUS

   d) The RADEXT group in the IETF is working on this, and draft-lior-radius-bandwidth-capability (see Bibliography) should be tracked.

Annex B (informative): Bibliography

IETF RFC 4284: "Identity selection hints for Extensible Authentication Protocol (EAP)".

Draft-ietf-geopriv-radius-lo-: "Carrying Location Objects in RADIUS".

Draft-lior-radext-end-to-end-caps-: "End-to-End Capabilities Support for Remote Authentication Dial In User Service (RADIUS)".

VLAN, Prority, and Filtering Attributes

NOTE: http://www.ietf.org/internet-drafts/draft-ietf-radext-ieee802-01.txt

Draft-lior-radius-bandwidth-capability: "Network Bandwidth Parameters for Remote Authentication Dial In User Service (RADIUS)".

ETSI TS 122 234: "Requirements on 3GPP system to Wireless Local Area Network (WLAN) Interworking; Release 6".

ETSI TS 123 234: "3GPP system to Wireless Local Area Network (WLAN) Interworking; System descriptions; Release 6".

International Roaming Access Protocols (IRAP): "Public WLAN Roaming Interface Specification".

NOTE: ftp://download.intel.com/technology/comms/roaming/download/Roaming_Interfaces_v0.95.pdf

ETSI TS 124 234: "3GPP system to Wireless Local Area Network (WLAN) Interworking; User Equipment to Network protocols; Stage 3; Release 6".

GSMA IR 61: "WLAN Roaming Guidelines".

IETF RFC 3162: "RADIUS and IPv6".

History

Document history		
V1.1.1	March 2006	Publication