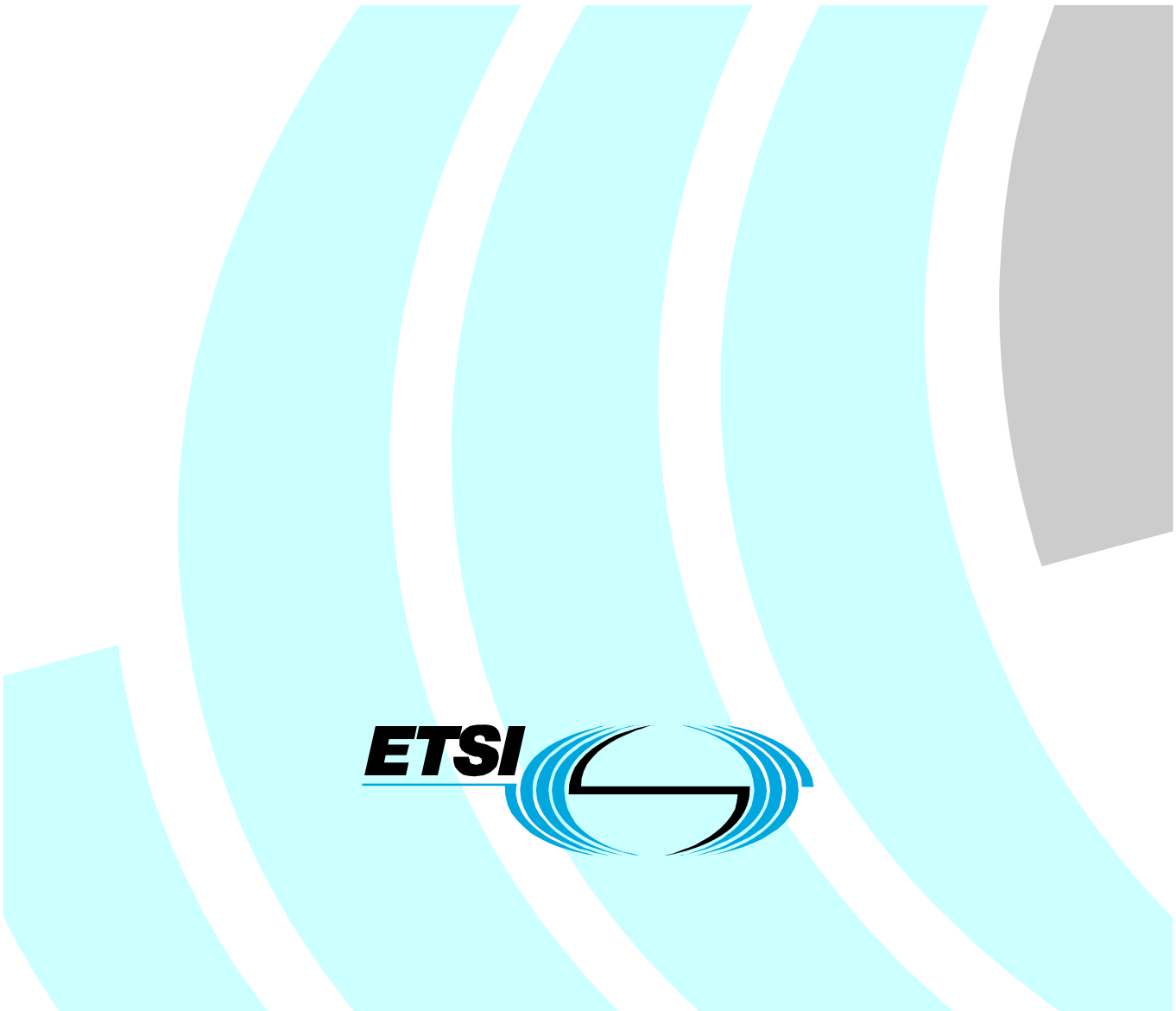
Final draft ETSI ES 282 004 V3.3.2 (2009-12)

ETSI Standard

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)



Reference
RES/TISPAN-02068-NGN-R3

Keywords
access, system

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

Contents

Intellectual Property Rights 5
Foreword 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 General Description of NASS 8
4.1 High level functional overview 8
4.2 High level concepts of NASS 9
4.3 Mobility, Nomadism 9
4.4 Access network level registration 9
4.4.1 Implicit authentication 10
4.4.1.1 Line authentication 10
4.4.2 Explicit authentication 10
4.4.3 CNG remote network configuration 10
4.4.4 TISPAN NGN Service/Applications Subsystems discovery 10
5 Functional Architecture 11
5.1 Overview 11
5.2 Functional Entities 12
5.2.1 Network Access Configuration Function (NACF) 12
5.2.2 Void 12
5.2.3 Connectivity session Location and repository Function (CLF) 12
5.2.3.1 Information Model 13
5.2.3.2 State Model 14
5.2.4 User Authentication and Authorization Function (UAAF) 16
5.2.5 Profile Data Base Function (PDBF) 16
5.2.6 CNG Configuration Function (CNGCF) 17
5.2.7 Void 17
5.3 Internal Reference points 17
5.3.1 Void 17
5.3.2 Reference Point NACF - CLF (a2) 17
5.3.2.1 Bind Indication 17
5.3.2.2 Bind Acknowledgement 18
5.3.2.3 Unbind Indication 18
5.3.2.4 Bind Information Query 18
5.3.2.5 Bind Information Query Acknowledgement 18
5.3.3 Void 19
5.3.4 Reference Point UAAF - CLF (a4) 19
5.3.4.1 Access Profile Push 19
5.3.4.2 Access Profile Pull 21
5.3.4.3 Remove Access Profile 21
5.3.5 Reference Point NACF - UAAF 21
5.3.6 Reference Point UAAF - UAAF (e5) 21
5.3.6.1 Information exchanged on e5 22
5.4 Interface with the Resource and Admission Control Subsystem (RACS) 23
5.4.1 Interface between CLF and RACF (e4) 23
5.4.1.1 Access Profile Push 23
5.4.1.2 Access Profile Pull 25
5.4.1.3 IP Connectivity Release Indication 25
5.5 Interfaces between NASS and the application plane and service control subsystems 25

5.5.1 Interface between CLF and Application Functions (e2) 25
5.5.1.1 Information Query Request 26
5.5.1.2 Information Query Response 26
5.5.1.3 Event Registration Request 27
5.5.1.4 Event Registration Response 27
5.5.1.5 Notification Event Request 27
5.5.1.6 Notification Event Response 28
5.6 Reference points between NASS and User Equipment 28
5.6.1 Authentication and IP address allocation (e1) 28
5.6.2 Interface between CNGCF and CNG (e3) 28
5.6.3 Reference points with the AMF 29

6 Mapping onto network roles 29

7 Information flows 32
7.1 High level information flows 32
7.2 PPP related procedures 33
7.4 IEEE 802 Ethernet access 39
7.5 PANA-based related 40

Annex A (informative): Physical Configurations 43

A.1 PPP case 43

A.2 PPP with DHCP configuration 44

A.3 DHCP (option 1) 45

A.4 DHCP (option 2) 46

A.5 PANA-based configuration 46

Annex B (informative): Recovery procedures for functional elements within NASS 48

B.1 Conceptual information exchange flow for CLF state recovery 48

Annex C (informative): Bibliography 49

Annex D (informative): Change history 50

History 51

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 ETSI Standard (ES) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), and is now submitted for the ETSI standards Membership Approval Procedure.

The present document describes the architecture of the Network Attachment Subsystem (NASS) identified in the overall TISPAN NGN architecture.

1 Scope

The present document describes the architecture of the Network Attachment Subsystem (NASS) and its role in the TISPAN NGN architecture as defined in ES 282 001 [2].

2 References

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.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present 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] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203)".

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

[3] IETF RFC 1661: "The Point-to-Point Protocol (PPP)".

[4] ISO/IEC 7498-2: "Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[5] IEEE 802.1X: "IEEE Standard for Local and metropolitan area networks - Port Based Network Access Control".

[6] ETSI TS 182 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Presence Service; Architecture and functional description [Endorsement of 3GPP TS 23.141 and OMA-AD-Presence-SIMPLE-V1-0]".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905 Release 7)".

[i.2] ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

3 Definitions and abbreviations

3.1 Definitions

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

authentication: property by which the correct identity of an entity or party is established with a required assurance

NOTE: The party being authenticated could be a user, subscriber, home environment or serving network (see TR 121 905 [i.1]).

authorization: granting of permission based on authenticated identification (see ISO/IEC 7498-2 [4])

NOTE: In some contexts, authorization may be granted without requiring authentication or identification e.g. emergency call services.

Customer Network Gateway (CNG): gateway between the Customer Premises Network (CPN) and the Access Network

NOTE: A Customer Network Gateway may be in its simplest form a bridged or routed modem, and in a more advanced form be an IAD.

explicit authentication: authentication that requires that the party to be authenticated performs an authentication procedure (to verify the claimed identity of the party)

NOTE: For example, in IMS security (TS 133 203 [1]), explicit authentication is provided with full AKA directed towards the IMS client entity (represented by IMPI/IMPU and USIM/ISIM) and also implicit authentication is provided by means of the IPsec security associations.

implicit authentication: authentication based on a trusted relationship already established between two parties, or based on one or more outputs of an authentication procedure already established between two parties

line identification: process that establishes the identity of the line based on the trusted configuration

NASS user: entity requesting authorization, authentication and allocation of the IP-Address from the NASS

User Equipment (UE): 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.

3.2 Abbreviations

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

AAA Authentication Authorization and Accounting
AF Application Functions
AMF Access Management Function

AN	Access Network
API	Application Programming Interface
A-RACF	Access-Resource and Admission Control Function
ARF	Access Relay Function
ASF	Application Server Functions
ATM	Asynchronous Transfer Mode
BGF	Border Gateway Function
CLF	Connectivity session Location and repository Function
CNG	Customer Network Gateway
CNGCF	CNG Configuration Function
CPE	Customer Premises Equipment
CPN	Customer Premises Network
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EP	Enforcement Point
FQDN	Fully Qualified Domain Name
IBCF	Interconnection Border Control Function
IMS	IP Multimedia SubSystem
IP	Internet Protocol
LIF	Location Information Forum
NACF	Network Access Configuration Function
NASS	Network Attachment SubSystem
PAA	PANA Authentication Agent
PaC	PANA Client
PANA	Protocol for carrying Authentication for Network Access
P-CSCF	Proxy-Call Session Control Function
PDBF	Profile Data Base Function
PNA	Presence Network Agent
PPP	Point-to-Point Protocol
RACS	Resource Admission Control Subsystem
RCEF	Resource Control Emulation Function
TE	Terminal Equipment
UAAF	User Access Authorization Function
UE	User Equipment
VC	Virtual Circuit
VP	Virtual Path

4 General Description of NASS

4.1 High level functional overview

The Network Attachment Subsystem provides the following functionalities:

- Dynamic provision of IP address and other user equipment configuration parameters (e.g. using DHCP).
- User authentication, prior or during the IP address allocation procedure.
- Authorization of network access, based on user profile.
- Access network configuration, based on user profile.
- Location management.

The location of this subsystem in the overall TISPAN architecture can be found in ES 282 001 [2] and is shown here for information in figure 4.1.

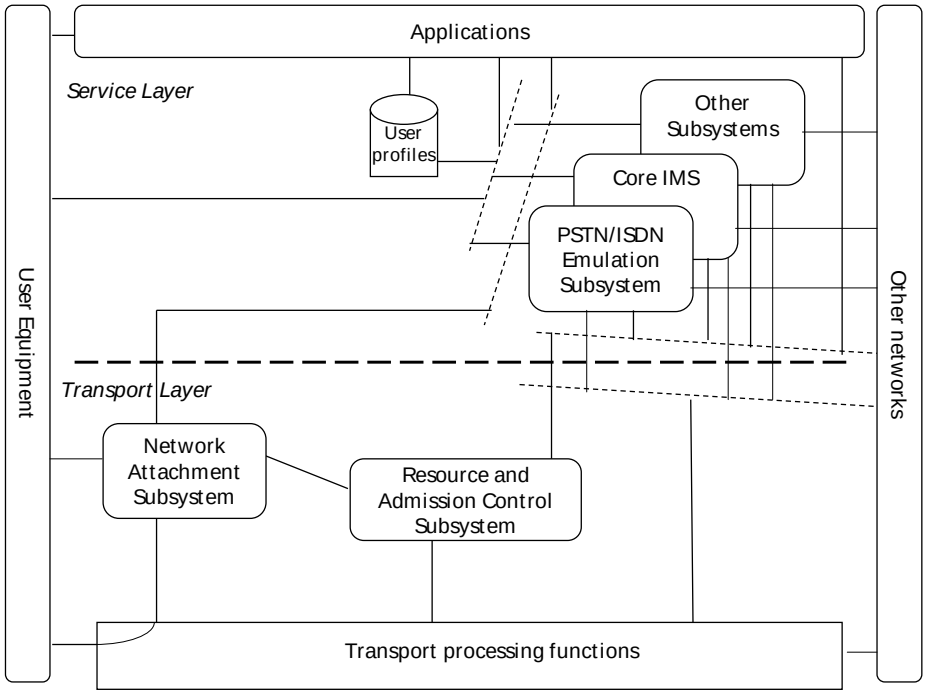


Figure 4.1: TISPAN NGN Architecture overview

4.2 High level concepts of NASS

The Network Attachment Subsystem (NASS) provides registration at access level and initialization of User Equipment (UE) for accessing to the TISPAN NGN services. The NASS provides network level identification and authentication, manages the IP address space of the Access Network and authenticates access sessions. The NASS also announces the contact point of the TISPAN NGN Service/Applications Subsystems to the UE.

Network attachment through NASS is based on implicit or explicit user identity and authentication credentials stored in the NASS.

4.3 Mobility, Nomadism

Mobility management functions provided by the NASS in the current TISPAN NGN release are limited to the ability of a terminal to be moved to different access points and access networks (which may be owned by a different access network provider) and a user to utilize different terminal, access points and access networks to retrieve their TISPAN NGN services (even from another network operator). The current TISPAN NGN release does not require the support of handover and session continuity between access networks without excluding autonomous mobility capabilities provided within the access networks.

The impact of these nomadism requirements are defined in clause 6.

4.4 Access network level registration

NASS registration involves the identification, authentication, and authorization procedures between the UE and the NASS to control the access to the NASS. Two authentication types are defined for NASS: Implicit authentication, for example based on line identification, and explicit authentication, for example based on EAP. The relationship between the identity and the credentials used for authentication must be known to the NASS for any authentication solution to be possible.

Explicit authentication is required between the UE and the NASS. It requires a signalling procedure to be performed between the UE and the NASS. Implicit authentication may be performed by the NASS based on the line identification of the connection to the UE. It is a matter of operator policy which form of authentication is applied.

Both implicit authentication and explicit authentication may be used independently as NASS authentication mechanisms.

4.4.1 Implicit authentication

Depending on the access network configuration, especially for wired broadband access networks, the implicit access authentication may rely only on an implicit authentication through physical or logic identity on the layer 2 (L2) transport layer. A UE can directly gain access to access network without an explicit authentication procedure.

A CNG shall be able to directly access an access network without an explicit authentication procedure.
Which implicit authentication method applies depends on the operator policies.

4.4.1.1 Line authentication

Line authentication is a form of implicit authentication. Line authentication ensures that an access line is authenticated and can be accessed from the CNG. Line authentication shall be based on the activation of the L2 connection between the CNG and the access network.

Line authentication ensures that an access line is authenticated and can be accessed from the CNG. The line ID shall be used for line authentication. The operator's policy shall decide whether line authentication applies.

4.4.2 Explicit authentication

In case the CNG is a routing modem and the Customer Premises Network (CPN) is a private IP realm, authentication shall be initiated from the CNG. In case the CNG is a bridge, each UE shall authenticate with the NASS as the IP realm in the CPN is known to the access network.

The relationship between the identity and the credentials used for authentication must be known to the NASS for any explicit authentication solution to be possible. The identity used for explicit authentication may depend on the authentication mechanism applied and on the access network which the UE is connected to. Two examples of these identities are:

- User identity and credentials.
- UE identity.

The type of explicit authentication mechanisms used shall depend on the access network configuration and on the operator policy.

4.4.3 CNG remote network configuration

This procedure is needed for the initialization of the CNGs accessing to the TISPAN NGN service subsystems.

4.4.4 TISPAN NGN Service/Applications Subsystems discovery

As part of the network registration process, the NASS shall have the possibility to announce the contact information of the TISPAN NGN Service/Applications Subsystems to the UE. In case the TISPAN NGN Subsystem is the IMS, the contact information provided by the NASS shall identify the P-CSCF.

The contact information provided by the NASS should either be in the form of the IP address of the contact point or in the form of the FQDN of the contact point (in which case the NASS provides the IP address of the DNS server that is able to resolve this FQDN into the IP address of the contact point).

Alternatively, the contact point to the TISPAN NGN Service/Applications Subsystems may be statically configured in the UE e.g. using Fully Qualified Domain Names (FQDN) and DNS resolution to retrieve the contact points IP addresses. This option applies in the non-roaming case.

5 Functional Architecture

5.1 Overview

The Network Attachment Subsystem (NASS) comprises the following functional entities:

- Network Access Configuration Function (NACF).
- Connectivity session Location and repository Function (CLF).
- User Authentication and Authorization Function (UAAF).
- Profile Data Base Function (PDBF).
- CNG Configuration Function (CNGCF).

The NASS has interaction with the following TISPAN NGN functional entities:

- TISPAN Service control subsystems and applications.
- Resource Admission Control Subsystem (RACS).
- Access Relay Function (ARF) and Access Management Function (AMF).
- User Equipment (UE).

One or more functional entities may be mapped onto a single physical entity. If one functional entity is implemented by two physical entities, the interface between these physical entities is outside the scope of standardization.

Functional entities in the Network Attachment Subsystem (NASS) may be distributed over two administrative domains. See clause 6 for the impact of roaming on the distribution of NASS.

Figure 5.1 provides an overview of the relationships between these functional entities and other subsystems of the NGN architecture. Interfaces to charging systems are not represented. Annex A provides informative, potential physical configurations in which the functional NASS architecture can be applied.

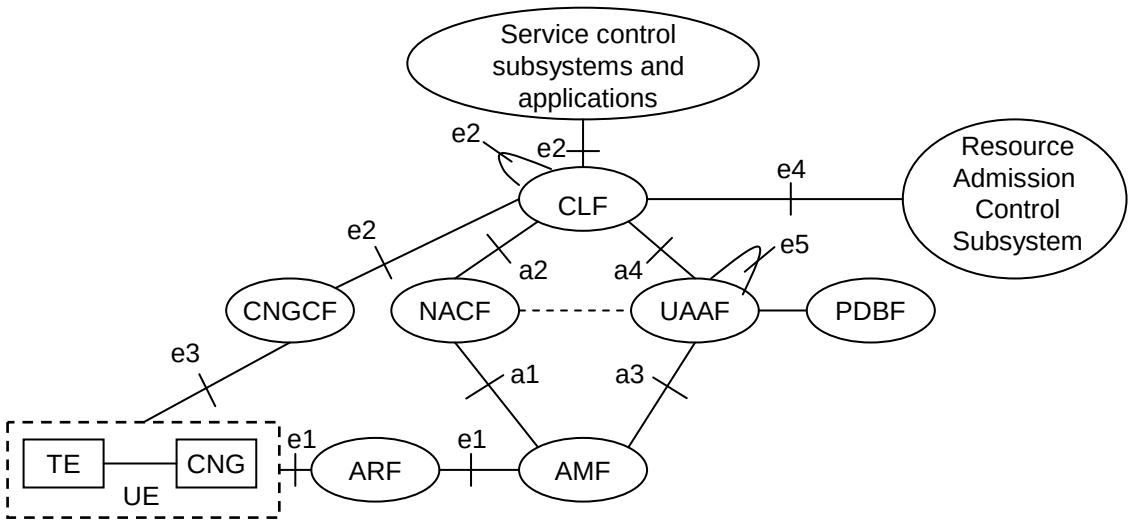


Figure 5.1: Network Attachment Subsystem architecture

5.2 Functional Entities

5.2.1 Network Access Configuration Function (NACF)

The Network Access Configuration Function (NACF) is responsible for the IP address allocation to the UE. It may also distribute other network configuration parameters such as address of DNS server(s), address of signalling proxies for specific protocols (e.g. address of the P-CSCF when accessing to the IMS).

The NACF should be able to provide to the UE an access network identifier. This information uniquely identifies the access network to which the UE is attached. The UE may send this information to applications as a hint to locate the CLF.

NOTE 1: The transport of the access identifier depends on extension in existing protocols (e.g. new DHCP option or usage of DHCP option 120). If NASS does not have the means to convey this parameter to the UE, this function will not be supported.

NOTE 2: DHCP servers or RADIUS servers are typical implementations of the NACF.

5.2.2 Void

5.2.3 Connectivity session Location and repository Function (CLF)

The Connectivity session Location and repository Function (CLF) registers the association between the IP address allocated to the UE and related network location information provided by the NACF, i.e.: access transport equipment characteristics, line identifier (Logical Access ID), IP Edge identity, etc. The CLF registers the association between network location information received from the NACF and geographical location information. The CLF may also store the identity of the NASS User to which the IP address has been allocated (information received from the UAAF), as well as the associated network QoS profile and preferences regarding the privacy of location information. In case the CLF does not store the identity/profile of the NASS User, the CLF shall be able to retrieve this information from the UAAF. For detailed CLF information model and state model see clauses 5.2.3.1 and 5.2.3.2.

The CLF responds to location queries from service control subsystems and applications. The actual information delivered by the CLF may take various forms (e.g. network location, geographical coordinates, post mail address etc.), depending on agreements with the requestor and on NASS User preferences regarding the privacy of its location. Any privacy information, that may indicate a level of accuracy of the location information to be delivered, is also sent with the actual location information.

NOTE 1: The implications and impacts of the extension of allowing the privacy indication to be sent over the e2 reference point to the application service control function on functions in the application layer and from the access (PBX networks etc.) are FFS.

NOTE 2: The decision over allowing this to change earlier versions of the present document as an essential change is FFS.

NOTE 3: The retrieval by the CLF of geographical information from related NASS User network location characteristics is outside of the scope of the present document.

NOTE 4: Geographical information may take several different forms depending on the access type and the application. The definition of this format shall also be lined up with OCG EMTEL who has decided that the LIF (Location Information Forum) is required in certain environments according to regulatory requirements. This data field is intended to be a placeholder for this information

The CLF interfaces with the NACF to get the association between the IP address allocated by the NACF to the NASS User and the Line ID.

The CLF also registers NASS User network profile information (received from the UAAF at authentication) to make this profile information available to the RACS at authentication of the UE.

The CLF is able to correlate the information received from NACF and UAAF based on the Logical Access ID.

5.2.3.1 Information Model

The CLF holds a number of records representing active sessions. These records contain information received from the NACF and the UAAF, information on the list of AFs having subscribed to particular events, and additional statically configured data. The following table identifies which information elements are stored for each of these sessions

NOTE: In case PPP is used the Physical access ID may be provided from the UAAF to the CLF.

Table 5.1

Access Session Description	
Information Received from the NACF	
Globally Unique Address	
- Assigned IP Address	The IP address of the attached NASS User.
- Address Realm	The addressing domain in which the IP address is significant.
Physical Access ID (optional)	The identity of the physical access to which the NASS User is connected.
Logical Access ID	The identity of the logical access used by the attached NASS User. In the xDSL case, the Logical Access ID may explicitly contain the identity of the port, VP and/or VC carrying the traffic.
Terminal Type	The type of user equipment to which the IP address has been allocated.
Information Received from the UAAF/PDBF	
NASS User ID	The identity of the attached NASS User.
Logical Access ID	The identity of the logical access used by the attached NASS User.
Physical Access ID (optional)	The identity of the physical access to which the NASS User is connected.
CNGCF Address (optional) (see note 6)	The address of the CNGCF entity from which configuration data may be retrieved by the user equipment.
P-CSCF Identity (optional) (see note 7)	The identity of the P-CSCF for accessing IMS services.
Privacy Indicator	Whether location information can be exported to services and applications (see note 1).
QoS Profile Information (see notes 2 and 3)	
- Transport Service Class	The transport service class subscribed by the attached NASS User. The transport service class relates to a forwarding behaviour at the transport plane.
- Media Type	The media type(s) to which the QoS profile applies.
- UL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the uplink direction.
- DL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the downlink direction.
- Maximum priority	The maximum priority allowed for any reservation request.
- Requestor Name	Identifies the requestor(s) allowed by the QoS profile.
Initial Gate Settings (optional)	
- List of allowed destinations as well as multicast flows	In case of unicast data, the list of default destination IP addresses and/or ports and/or port-ranges and/or prefixes to which traffic can be sent. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs which traffic can be received from by the attached NASS User. Address ranges are supported within the list (see note 4).
- List of denied destinations as well as multicast flows	In case of unicast, the list of default destination IP addresses, ports, prefixes and port ranges to which traffic is denied. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs for which traffic towards the attached NASS User must be denied. Address ranges are supported within the list (see note 4).

Access Session Description	
- UL Default Bandwidth	The maximum amount of bandwidth that can be used without explicit authorization in the uplink direction.
- DL Default Bandwidth	The maximum amount of bandwidth that can be used without explicit authorization in the downlink direction.
Static Information derived from the Physical access ID	
Location Information	
Default NASS User ID	
Static Information Derived from the Logical Access ID	
RACS point of contact	The address of the RACS element where the NASS User profile should be pushed.
Access Network Type	The type of access network over which IP connectivity is provided to the NASS User.
Event Management Information	
Event Management Information (see note 5)	
- Event Type	The type of event to be monitored.
- AF Identities	The list of AF to be notified of the occurrence of this event.
NOTE 1: An indication whether applications can access location information, depending on their security level. NOTE 2: The access profile may contain multiple QoS profiles. NOTE 3: The actual available bandwidth is not known by the NASS. This information can be derived by the RACS, based the logical access ID. NOTE 4: If a unicast destination and/or multicast flow does not appear in either of the two lists, gate setting decisions for those addresses is subject to control by RACS. NOTE 5: More than Event Type and associated AF Identities may be stored. NOTE 6: If the CNGCF address is configured on the CLF and the CNGCF address is received from the UAAF/PDBF, it depends on operator policy which one should be used. NOTE 7: If the P-CSCF Identity is configured on the CLF and the P-CSCF identity is received from the UAAF/PDBF, it depends on operator policy which one should be used.	

Several records may contain the same physical access ID and/or logical access ID and/or NASS User ID, as a NASS User may establish more than one IP session, over the same or different logical access (e.g. ATM VC) using the same or different physical access. The CLF does not need to establish any link between such records, although it may do it for the purpose of optimizing its storage capacity.

5.2.3.2 State Model

The behaviour of the CLF when managing access records can be represented by the state model described in the present clause. This state model is not intended to constrain implementations of a CLF. Implementations may use a different model as long as they exhibit the same external behaviour.

This state model defines a Session State Machine (SSM) that comprises five states:

- **Null:** This state represents a non existing access record.
- **Wait_For_Bind_Indication_and_Profile:** This state is entered when an access record is created as a result of receiving a request for subscription to an event (e.g. the logon event) while no session record exists for the associated NASS User identifier or globally unique address. A partial record is created and the CLF waits for a Bind_Indication event.
- **Wait_For_Bind_Indication:** This state is entered when an access record is created as a result of receiving NASS User profile information while no session record exists for the associated NASS User identifier or globally unique address. A partial record is created and the CLF waits for a Bind_Indication event.
- **Wait_For_Profile_Information:** This state represents a partial session record where NASS User profile information is missing.
- **Active_Session:** This state represents a session record where the full description of an access sessions available.

The CLF sends and receives information flows at the e2, e4, a2, and a4 reference points. Incoming information flows are routed to Session State Machines (SSM) based on the NASS User identifier or the globally unique address they contain.

An SSM instance is created when Bind_Indication or an Event_Subscription_Indication event indicating an unknown NASS User identifier or globally unique address occurs.

The following events are handled by the CLF session state machine and cause transition between the states:

- *Event_Subscription_Indication*: This event occurs when an Event Registration Request information flow (see clause 5.5.1) is received from an AF.

NOTE: When the actual CLF event occurs, a Notification Event Request information flow is sent back to the AF. This does not cause any state transition.

- *Bind_Indication*: This event occurs when the Bind Indication information flow is received at the a2 reference point (see clause 5.3.2).

- *Unbind_Indication*: This event occurs when the Unbind Indication information flow is received at the a2 reference point or when a negative acknowledgement is received in response to a Bind Information Query (see clause 5.3.2).

- *NASS_User_Profile_Received*: This event occurs when an Access Profile Push information flow is received at the a4 reference point asynchronously or as a result of sending an Access Profile Pull information flow, or when internal configuration data indicate that a default NASS User profile applies.

- *NASS_User_Profile_Removed*: This event occurs when a Remove Access Profile information flow is received at the a4 reference point.

- *Session_Data_Requested*: This event occurs when an Access Profile Pull information flow is received at the e4 reference point or an Information Query Request information flow is received at the e2 reference point. It causes an Information Query Response or an Access Profile Push information flow to be sent over the e2 or e4 reference point.

Figure 5.1a provides an overview of the state transitions based on the above events.

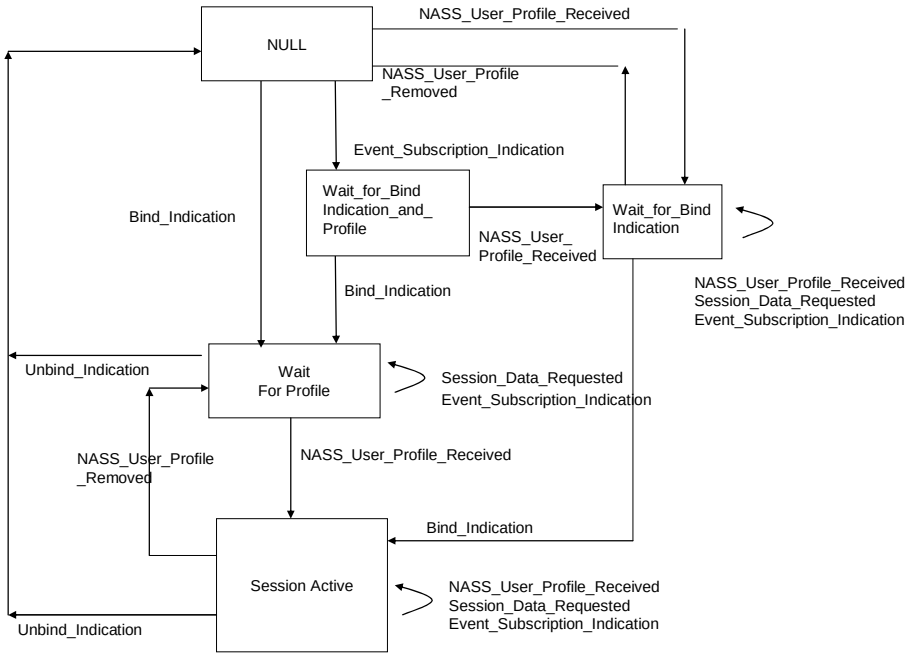


Figure 5.1a: CLF state model for access records management

5.2.4 User Authentication and Authorization Function (UAAF)

The User Authentication and Authorization Function (UAAF) performs NASS User authentication, as well as authorization checking, based on NASS User profiles, for network access. For each NASS User, the UAAF retrieves authentication data and access authorization information from the NASS User network profile information contained in the PDBF. The UAAF may also perform the collection of accounting data for each NASS User authenticated by NASS.

The User Authentication and Authorization Function (UAAF) can also act as a proxy. When acting as a proxy the UAAF can locate and communicate with the UAAF acting as server which contains the PDBF NASS User authentication data. The UAAF proxy can forward access and authorization requests, as well as accounting messages, received from the AMF, to the UAAF acting as server. Responses received back in return from the UAAF acting as server will be returned to the AMF via the UAAF proxy.

In case PPP is applied, the AMF terminates the PPP and translates it to signalling on the a3 interface. The UAAF is assumed to be able to contact the NACF via an internal interface to obtain an IP address (UAAF and NACF are in the PPP case internal functions). The a1 reference point does not carry DHCP signalling, instead the a3 interface is used to give the IP configuration information to the AMF.

NOTE: Support of nomadism entails a distinction between the user who requests access to the network and the user who owns the physical access through which the request is issued. Impact on this distinction on the UAAF requires further studies.

5.2.5 Profile Data Base Function (PDBF)

The Profile Data Base Function (PDBF) is the functional entity that contains NASS User authentication data (NASS User identity, list of supported authentication methods, key materials etc.) and information related to the required network access configuration: This data is called "NASS User network profile". The NASS User network profile may be sub-divided into sub-profiles (see figure 5.2), each of which is associated to one or more Logical Access ID. Support of the Logical Access ID is optional.

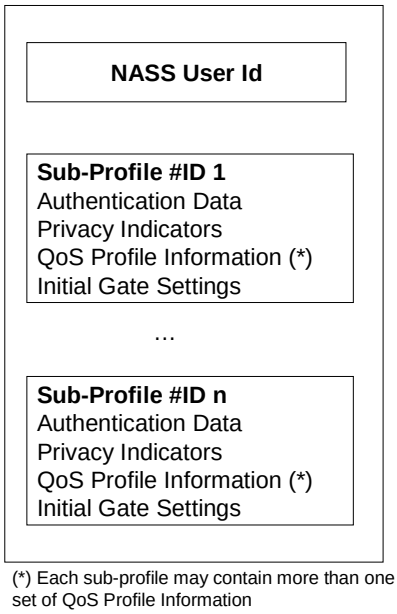


Figure 5.2: NASS User record in the PDBF

The PDBF responds to queries from the UAAF on the full profile or on a particular sub-profile. In the later case, it is the responsibility of the UAAF (or the Proxy-UAAF) to derive a Sub-Profile Id from the Logical Access ID.

In this release the interface between UAAF and PDBF is not specified, i.e. UAAF and PDBF are either co-located or connected by a non-standardized interface.

The PDBF can be co-located with the UPSF (described in ES 282 001 [2]).

5.2.6 CNG Configuration Function (CNGCF)

The CNGCF is used during initialization and update of the CNG. The CNGCF provides to the CNG additional configuration information (e.g. configuration of a firewall internally in the CNG, QoS marking of IP packets etc.), with respect to the configuration information provided by the NACF. This data differs from the network configuration data provided by the NACF.

The CNGCF may also handle notifications from the CNG on terminal equipment availability. The CNGCF may indeed provide configuration information for the TEs, indirectly via the CNG or directly to the TEs. It may also trigger maintenance tests and process results sent by the CNG or by the TEs.

The CNGCF may also interface with the CLF in order to retrieve information on the CNG and on the access it is connected to. In such cases, the CNGCF uses the procedures described in clause 5.5.1. The information retrieved from the CLF (e.g. line identifier and/or NASS User identifier) may be used as input to the selection of configuration data to be delivered to the CNG.

5.2.7 Void

5.3 Internal Reference points

5.3.1 Void

5.3.2 Reference Point NACF - CLF (a2)

This reference point allows the NACF to register in the CLF the association between the allocated IP address of the NASS User identity and the related location information (IP edge ID, Line ID).

The following information flows are used on the CLF to NACF interface:

- Bind Indication.
- Bind Acknowledgment.
- Unbind Indication.
- Bind Information Query.
- Bind Information Query Acknowledgement.

5.3.2.1 Bind Indication

The Bind Indication information flow contains the following information.

Table 5.2

Bind Indication (NACF -> CLF)	
Globally Unique Address	
- Assigned IP Address	The IP address allocated to the NASS User.
- Addressing Realm	The addressing domain in which the IP address is significant.
Physical Access ID (optional)	The identity of the physical access to which the NASS User is connected.
Logical Access ID	The identity of the logical access used by the attached NASS User (see note1).
Terminal Type (optional)	The type of user equipment (see note 2).
NOTE 1: If the NACF is implemented as a DHCP server, this parameter is mapped to the DHCP option 82, sub-option 1 and 2. NOTE 2: If the NACF is implemented as a DHCP server, this parameter is mapped to the DHCP option 77.	

5.3.2.2 Bind Acknowledgement

The Bind Acknowledgment information flow conveys information that may be sent back to the NASS User. The information returned by the CLF in response to a bind indication is received from the UAAF or retrieved by the CLF from the PDBF, via the UAAF. This information flow contains the following elements.

Table 5.3

Bind Acknowledgment (CLF -> NACF)	
CNGCF address (optional)	The address of the CNGCF entity from which configuration data may be retrieved by the user equipment.
Geographic Location Information (optional)	Geographic location information.
P-CSCF Identity (optional)	The Identity of the P-CSCF for accessing IMS services.

5.3.2.3 Unbind Indication

The Unbind Information flow is sent by the NACF on expiry of the binding between the IP address and NASS User identity or when an underlying PPP connection or layer 2 resource is released.

Table 5.4

Unbind Indication (NACF -> CLF)	
Globally Unique Address	
- Assigned IP Address	The IP address allocated to the NASS User.
- Addressing Realm	The addressing domain in which the IP address is significant.

5.3.2.4 Bind Information Query

The Bind Information Query information flow is used by the CLF to request bind information (e.g. in the context of recovery procedures) from the NACF.

Table 5.4a

Bind Information Query (CLF -> NACF)	
Globally Unique Address	
- Assigned IP Address	The IP address allocated to the NASS User.
- Addressing Realm	The addressing domain in which the IP address is significant.

5.3.2.5 Bind Information Query Acknowledgement

The Bind Information Query Acknowledgement information flow is used by NACF to inform CLF of the result of a binding information request. When the information query is successful, the acknowledgement information flow contains the following information.

Table 5.4b

Bind Information Query Acknowledgement (NACF -> CLF)	
Physical Access ID (optional)	The identity of the physical access to which the NASS User is connected.
Logical Access ID	The identity of the logical access used by the attached NASS User (see note 1).
Terminal Type (optional)	The type of user equipment (see note 2).
NOTE 1: If the NACF is implemented as a DHCP server, this parameter is mapped to the DHCP option 82, sub-option 1 and 2. NOTE 2: If the NACF is implemented as a DHCP server, this parameter is mapped to the DHCP option 77.	

5.3.3 Void

5.3.4 Reference Point UAAF - CLF (a4)

This reference point allows the CLF to register the association between the NASS User identity and the NASS User preferences regarding the privacy of location information provided by the UAAF. Reference point a4 is also used to register NASS User network profile information (QoS profile). The CLF may retrieve the NASS User network profile from the UAAF.

The UAAF - CLF relationship may be operated in pull mode or push mode. The push mode is used when the UAAF is involved in the processing of network access requests in order to authorize or deny access to the network (e.g. when explicit authentication is used). The pull mode is used when implicit authentication is used or in support of CLF recovery procedures.

The following information flows are used on the CLF to UAAF interface:

- Access Profile Push.
- Access Profile Pull.
- Remove Access Profile.

5.3.4.1 Access Profile Push

The Access Profile Push information flow is used to push Access Profile information from the UAAF to the CLF upon successful authentication of the NASS User. UAAF may decide to send in the same Access Profile Push some profiles in the form of a profile id (because the actual profile information is assumed to be available in the CLF) and some other profiles in the form of full profile descriptions. This information is retrieved from the PDBF by the UAAF. It contains the following elements.

NOTE: In case PPP is applied the UAAF may provide the Physical Access ID to the CLF.

Table 5.5

Access Profile Push (UAAF - CLF)	
NASS User ID	The identity of the NASS User requesting IP connectivity.
Globally Unique Address (see note 3)	
- Assigned IP Address	The IP address of the attached NASS User.
- Address Realm	The addressing domain in which the IP address is significant.
Logical Access ID	The identity of the logical access used by the attached NASS User.
Physical Access ID (optional)	The identity of the physical access to which the NASS User is connected.
CNGCF address (optional)	The address of the CNGCF entity from which configuration data may be retrieved by the user equipment.
P-CSCF identity (optional)	The identity of the P-CSCF for accessing IMS services.
Privacy Indicator	Whether location information can be exported to services and applications.
QoS Profile Information (see note 1) (optional)	
- QoS Profile ID (see note 5)	The identifier of a set of QoS Profile information.
- QoS Profile description (see note 5)	
- Transport Service Class	The transport service class subscribed by the attached NASS User. The transport service class relates to a forwarding behaviour at the transport plane.
- Media Type	The media type(s) to which the QoS profile applies.
- UL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the uplink direction.
- DL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the downlink direction.
- Maximum priority	The maximum priority allowed for any reservation request
- Requestor Name	Identifies the requestor(s) allowed by the QoS profile.
Initial Gate Setting (see note 2) (optional)	
- Initial Gate Setting ID (see note 6)	The identifier of a set of Initial Gate Settings.
- Initiate Gate Setting description (see note 6)	
- List of allowed destinations as well as multicast flows	In case of unicast data, the list of default destination IP addresses and/or ports and/or port ranges and/or prefixes to which traffic can be sent. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs which traffic can be received from by the attached NASS User. Address ranges are supported within the list (see note 4).
- List of denied destinations as well as multicast flows	In case of unicast, the list of default destination IP addresses, ports, prefixes and port ranges to which traffic is denied. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs for which traffic towards the attached NASS User must be denied. Address ranges are supported within the list (see note 4).
- UL Default Bandwidth	The maximum amount of bandwidth that can be used without explicit authorization in the uplink direction.
- DL Default Bandwidth	The maximum amount of bandwidth that can be used without explicit authorization in the downlink direction.
NOTE 1: The access profile may contain multiple QoS profiles. NOTE 2: This information is used by the RACS to configure the RCEF functionality, before resource reservation requests are received from services/applications. NOTE 3: In case PPP is applied, the UAAF shall provide the Globally Unique Address to the CLF. When DHCP is applied this parameter is optional. NOTE 4: If a unicast destination and/or multicast flow does not appear in either of the two lists, gate setting decisions for those addresses is subject to control by RACS. NOTE 5: Either the QoS Profile ID or the QoS Profile description may be included, but not both at the same time.	

Access Profile Push (UAAF - CLF)
NOTE 6: Either the Initiate Gate Setting ID or the Initial Gate Setting description may be included, but not both at the same time.

5.3.4.2 Access Profile Pull

The Access Profile Pull information flow is used by the CLF to request the Access Profile information from the UAAF. This information flow is used when the CLF - UAAF operates in pull mode or in the context of CLF recovery procedures. It contains the following elements.

Table 5.6

Access Profile Pull (CLF -> UAAF)	
Globally Unique Address (see note 1)	
-IP Address End Point	The IP address of the attached NASS User.
-Address Realm	The addressing domain in which the IP address is significant.
Logical Access ID (optional)	The identity of the logical access used by the attached NASS User.
NASS User ID (see note 2)	The identity of the attached NASS User.
NOTE 1: If the information flow is used for supporting recovery procedures and the interface operates in push mode, the Globally Unique Address shall be included. NOTE 2: If the interface operates in pull mode, the NASS User ID shall be included.	

The response to the Access Profile Pull information flow is an Access Profile Push information flow.

5.3.4.3 Remove Access Profile

The Remove Access Profile information flow is used by the UAAF to request the CLF to delete the information it held about a NASS User. This event occurs as a result of network management actions.

Table 5.7

Remove Access Profile (UAAF -> CLF)	
Globally Unique Address (see note)	
- IP Address End Point	The IP address of the attached NASS User.
- Address Realm	The addressing domain in which the IP address is significant.
Logical Access ID (optional)	The identity of the logical access used by the attached NASS User.
NASS User ID (see note)	The identity of the attached user.
NOTE: Either the Globally Unique Address or the NASS User Id shall be included.	

5.3.5 Reference Point NACF - UAAF

This reference point is not specified in this release.

5.3.6 Reference Point UAAF - UAAF (e5)

This reference point is intended to be used between a UAAF-proxy and a UAAF-server, which may be in different administrative domains. This reference point allows the UAAF-proxy to request the UAAF-server for NASS User authentication and authorization, based on NASS User profiles. It also allows the UAAF-proxy to forward accounting data for the particular NASS User session to the UAAF-server or to forward requests received from a CLF.

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.

The UAAF-proxy will forward requests received over interface a4 from the CLF, to the UAAF-server over interface e5. Responses received back in return from the UAAF-server over interface e5 will be forwarded to the CLF over interface a4.

A bilateral trust relationship will need to be setup between the UAAF-proxy and the UAAF-server in order to facilitate this exchange.

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. The appropriate profiles and requirements for these protocols are part of the stage 3 work for this interface.

5.3.6.1 Information exchanged on e5

The following information elements are exchanged on the e5 reference point:

Table 5.8

Information Element	Description
NASS User ID	The identity of the NASS User requesting IP connectivity.
Privacy Indicator	Whether location information can be exported to services and applications.
Globally Unique Address	
- Assigned IP Address	The IP address of the attached NASS User.
- Address Realm	The addressing domain in which the IP address is significant.
QoS Profile Information (see note 1) (optional)	
- Transport Service Class	The transport service class subscribed by the attached NASS User. The transport service class relates to a forwarding behaviour at the transport plane.
- Media Type	The media type(s) to which the QoS profile applies.
- UL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the uplink direction.
- DL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the downlink direction.
- Maximum priority	The maximum priority allowed for any reservation request.
- Requestor Name	Identifies the requestor(s) that are allowed by the QoS profile.
Initial Gate Setting (see note 2) (optional)	
- List of allowed destinations as well as multicast flows	In case of unicast, the list of default destination IP addresses and/or ports and/or port ranges and/or prefixes to which traffic can be sent. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs which traffic can be received from by the attached NASS User. Address ranges are supported within the list (see note 3).
- List of denied destination as well as multicast flows	In case of unicast, the list of default destination IP addresses, ports, prefixes and port ranges to which traffic is denied. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs for which traffic towards the attached NASS User must be denied. Address ranges are supported within the list (see note 3).
- UL Default Bandwidth	The maximum amount of bandwidth that can be used without explicit authorization in the uplink direction.

Information Element	Description
- DL Default Bandwidth	The maximum amount of bandwidth that can be used without explicit authorization in the downlink direction.
NOTE 1: The access profile may contain multiple QoS profiles. NOTE 2: This information is used by the RACS to configure the RCEF functionality, before resource reservation requests are received from services/applications. NOTE 3: If a unicast destination and/or multicast flow does not appear in either of the two lists, gate setting decisions for those addresses is subject to control by RACS.	

5.4 Interface with the Resource and Admission Control Subsystem (RACS)

5.4.1 Interface between CLF and RACF (e4)

This reference point is used to pass the association between the Globally Unique Address and/or NASS User ID on the one hand, and the Access Identifier (logical or physical) on the other hand, from the CLF to the RACS. This allows RACS to determine the amount of available network resources. The e4 reference point may also be used to pass QoS profile information and initial gate settings from the CLF to the RACS. This allows RACS to take them into account when processing resource allocation requests. The information exchanged on the e4 reference point is:

- Binding between the Logical Access ID (Line ID), the assigned IP-Address and the ID of the IP edge, NASS User network profile information in order to take them into account when processing resource allocation requests.

The following information flows are used on the CLF to A-RACF interface:

- Access Profile Push.
- Access Profile Pull.
- IP Connectivity Release Indication.

5.4.1.1 Access Profile Push

The Access Profile Push information flow is used to push Access Profile information from the CLF to the A-RACF. The CLF knows the address of the A-RACF entity where the information should be pushed, either from configuration data or from the NASS User profile (i.e. in the PDBF). This information flow occurs when resource admission control may be required for a NASS user. This can be the case:

- when an IP address has been allocated to a NASS User as part of the initial network attachment process;
- after successful completion of the authentication and authorization stage of the NASS network attachment procedure (in order to open up the gate to proceed with the second stage (IP configuration) of the network attachment procedure);
- in case a modification occurs on a profile that has already been pushed to the RACS.

A CLF may decide to send in the same Access Profile Push some profiles in the form of a profile id (because the actual profile information is assumed to be available in the A-RACF) and some other profiles in the form of full profile descriptions. It contains the following elements.

Table 5.9: Access Profile Push (CLF -> A-RACF)

Access Profile Push (CLF -> A-RACF)	
NASS User ID	The identity of the NASS User requesting IP connectivity.
Physical Access ID (optional)	The identity of the physical access to which the NASS User is connected (see note 1).
Logical Access ID	The identity of the logical access to which the NASS User is connected (see notes 2 and 3).
Access Network Type	The type of access network over which IP connectivity is provided to the NASS User.
Globally Unique IP Address	
- Assigned IP Address	The IP address of the attached NASS User.
- Address Realm	The addressing domain in which the IP address is significant.
QoS Profile Information (see note 4) (optional)	
- QoS Profile ID (see note 7)	The identifier of a set of QoS Profile information.
- QoS Profile description (see note 7)	
- Transport Service Class	The transport service class subscribed by the attached NASS User. The transport service class relates to a forwarding behaviour at the transport plane.
- Media Type	The media type(s) to which the QoS profile applies.
- UL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the uplink direction.
- DL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the downlink direction.
- Maximum priority	The maximum priority allowed for any reservation request.
- Requestor Name	Identifies the requestor(s) allowed by the QoS profile.
Initial Gate Setting (see note 5) (optional)	
- Initial Gate Setting ID (see note 8)	The identifier of a set of Initial Gate Settings.
- Initiate Gate Setting description (see note 8)	
- List of allowed destinations as well as multicast flows	In case of unicast data, the list of default destination IP addresses and/or ports and/or port ranges and/or prefixes to which traffic can be sent. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs which traffic can be received from by the attached NASS User. Address ranges are supported within the list. (See note 6).
- List of denied destinations as well as multicast flows	In case of unicast, the list of default destination IP addresses, ports, prefixes and port ranges to which traffic is denied. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs for which traffic towards the attached NASS User must be denied. Address ranges are supported within the list. (See note 6).
- UL Default Bandwidth	The maximum amount of bandwidth that can be used without explicit authorization in the uplink direction.
- DL Default Bandwidth	The maximum amount of bandwidth that can be used without explicit authorization in the downlink direction.

Access Profile Push (CLF -> A-RACF)
NOTE 1: In the xDSL case, the Physical Access ID identifies the copper line. NOTE 2: The Logical Access ID should enable the RACS to derive the following information: The identification and bandwidth capacity of the layer 2 resources over which the NASS User traffic is carried. The address of the physical node(s) implementing the BGF and RCEF. NOTE 3: In the xDSL case, the Logical Access ID may explicitly contain the identity of the port, VP and/or VC carrying the traffic. NOTE 4: The access profile may contain multiple QoS profile. NOTE 5: This information is used by the RACS to configure the RCEF functionality, before resource reservation requests are received from services/applications. NOTE 6: If a unicast destination and/or multicast flow does not appear in either of the two lists, gate setting decisions for those addresses is subject to control by RACS. NOTE 7: Either the QoS Profile ID or the QoS Profile description may be included, but not both at the same time. NOTE 8: Either the Initiate Gate Setting ID or the Initial Gate Setting description may be included, but not both at the same time.

5.4.1.2 Access Profile Pull

The Access Profile Pull information flow is used by the RACS to request the Access Profile information from the CLF (e.g. in the context of recovery procedures). It contains the following elements:

Table 5.10: Access Profile Pull (A-RACF -> CLF)

Access Profile Pull (A-RACF -> CLF)	
IP Address End Point	The IP address of the attached NASS User.
Address Realm	The addressing domain in which the IP address is significant.
NASS User ID (optional)	The identity of the attached NASS User.

The response to the Access Profile Pull information flow is an Access Profile Push information flow.

5.4.1.3 IP Connectivity Release Indication

The IP Connectivity Release Indication information flow is used by the NASS to report loss of IP connectivity. This enables the RACS to remove the access profile from its internal data base. This event occurs in case the allocated IP address is released (e.g. DHCP leased timer expiry) or due to a release of the underlying layer 2 resources.

Table 5.11: IP Connectivity Release Indication (CLF -> A-RACF)

IP Connectivity Release Indication (CLF -> A-RACF)	
IP Address End Point	The IP address of the attached NASS User.
Address Realm	The addressing domain in which the IP address is significant.
NASS User ID (optional)	The identity of the attached NASS User.

5.5 Interfaces between NASS and the application plane and service control subsystems

5.5.1 Interface between CLF and Application Functions (e2)

This reference point enables Application Functions (AF) to retrieve information about the characteristics of the IP-connectivity session used to access such applications (e.g. network location information) from the CLF. It may also be used by a CNGCF to retrieve information from the CLF.

In the context of the present document, an Application Function is a generic term representing any element of the service layer architecture offering - or providing access to - applications that require information about the characteristics of the IP-connectivity session used to access such applications. Examples of such Application Functions are the P-CSCF and the IBCF in the IMS (ES 282 007 [i.2]), certain categories of Application Server Functions (ASF) (ES 282 001 [2]) or a Presence Network Agent (PNA) as defined in TS 182 008 [6].

The form of location information that is provided by the CLF depends on the requestor.

The following information flows are used on the CLF to AF interface:

- Information Query Request.
- Information Query Response.
- Event Registration Request.
- Event Registration Response.
- Notification Event Request.
- Notification Event Response.

5.5.1.1 Information Query Request

The Information Query Request information flow contains the following information:

Table 5.12: Information Query Request (AF -> CLF)

Globally Unique IP Address (see note 1)	
- Assigned IP Address	The IP address of the NASS User.
- Address Realm	The addressing domain in which the IP address is significant (see note 2).
NASS User ID (see note 1)	The identity of the attached NASS User.
AF Identity	The identity of the requesting application function.
NOTE 1: Either the Globally Unique IP Address or the NASS User ID shall be included. NOTE 2: The addressing domain is known by the AF either using configuration data (in which case all NASS Users served by the AF belong to the same addressing domain) or from the physical or logical interface over which was received the service request that triggered the location query.	

5.5.1.2 Information Query Response

The Information Query Response information flows contain the following information:

Table 5.13: Information Query Response (CLF -> AF)

NASS User ID (optional)	The identity of the attached NASS User (see note 1).
Location Information (optional) (see note 2)	Location information (or a pointer to such information) in a form that is suitable for the requesting application.
RACS contact point (optional)	The FQDN or IP address of the RACS entity where resource request shall be sent (i.e. SPDF address).
Terminal Type (optional)	The type of user equipment.
Access Network Type (optional)	The type of access network over which IP connectivity is provided to the NASS User.
Physical Access ID (optional)	The identity of the physical access to which the NASS User is connected (see note 2).
Logical Access ID (optional)	The identity of the logical access to which the NASS User is connected. (see note 2).
NOTE 1: This identity may be used by the AF when interacting with the RACS. NOTE 2: Disclosure of this information depends on the requesting application and the NASS User's privacy restrictions. Privacy restrictions are defined in the privacy indicator stored in the CLF.	

5.5.1.3 Event Registration Request

The Event Registration Request information flow contains the following information:

Table 5.14: Event Registration Request (AF -> CLF)

Subscription Duration	Duration for which the subscription for a particular event will be active.
NASS User ID (optional), (see note 1)	The identity of the attached NASS User (in case of NASS User-specific events, such as in a NASS-User-logon event example).
Event	Event-Type (e.g. NASS User logon event) and Format for Event Relay/Notification description.
Globally Unique IP Address (optional), (see note 1)	Globally Unique address that corresponds to the UNI associated to the NASS User attached to the network.
- Assigned IP Address	The IP address of the NASS User [Ipv4 or Ipv6].
- Address Realm	The addressing domain in which the IP address is significant (see note 2).
AF Identity (optional)	The identity of the requesting application function.
NOTE 1: At least one of the two identifiers ("NASS User ID" or "Globally Unique IP Address") shall be supplied. NOTE 2: The addressing domain is known by the AF either using configuration data (in which case all NASS Users served by the AF belongs to the same addressing domain) or from the physical or logical interface over which a related service request was received.	

This information flow is not applicable if the AF is a P-CSCF.

5.5.1.4 Event Registration Response

The Event Registration Response information flow contains the following information.

Table 5.15: Event Registration Response (CLF -> AF)

Update Action	Administrative Action/Information for an event: E.g. ACTIVATED (event registration successfully received and Event Notification for "Event" activated).
NASS User ID (see note)	The identity of the attached NASS User (in case of user-specific events, such as in the NASS User-logon event example).
Event	Event-Type (e.g. NASS User logon event).
Globally Unique Address (see note)	Globally Unique address that corresponds to the UNI associated to the NASS User attached to the network.
- Assigned IP Address	The IP address of the attached NASS User.
- Address Realm	The addressing domain in which the IP address is significant.
NOTE: At least one of the two identifiers ("NASS User ID" or "Globally Unique IP Address") shall be supplied.	

This information flow is not applicable if the AF is a P-CSCF.

5.5.1.5 Notification Event Request

The Notification Event Request information flow contains the following information:

Table 5.16: Notification Event Request (CLF -> AF)

Globally Unique Address	
- Assigned IP Address	The IP address of the attached NASS User.
- Address Realm	
NASS User ID	The identity of the attached NASS User.
Event	Event (e.g. NASS User logon event).

This information flow is not applicable if the AF is a P-CSCF.

5.5.1.6 Notification Event Response

The Notification Event Response information flow contains the following information:

Table 5.17: Notification Event Response (AF -> CLF)

Globally Unique Address	Globally Unique address that corresponds to the UNI associated to the NASS User attached to the network.
- Assigned IP Address	The IP address of the attached NASS User.
- Address Realm	The addressing domain in which the IP address is significant.
NASS User ID	The identity of the attached NASS User.
Event	Event-Type.
Result	Result Code (e.g. success, permanent failure, etc.).

This information flow is not applicable if the AF is a P-CSCF.

5.6 Reference points between NASS and User Equipment

5.6.1 Authentication and IP address allocation (e1)

There is no direct reference point between the NASS and the User Equipment for supporting authentication and IP address allocation. Communication between the NASS and the User Equipment takes place via the ARF and the AMF.

The e1 interface at the UE side may either be terminated on a CNG or a TE; the latter applies when the TE has direct connectivity to the NASS.

This reference point enables the UE to initiate requests for IP address allocation and possible other network configuration parameters in order to access to the network. These requests are received by the AMF, via the ARF.

Requests for IP address allocation and network configuration parameters are either in the form of a DHCP or PPP request.

In case of a deployment leveraging DHCP, it is assumed that the IP edge in the transport plane includes an Access Relay Function (ARF) that acts as a DHCP relay between the DHCP client in user equipments and the DHCP server in the network attachment subsystem.

Before sending a request to the network attachment subsystem, the relay function may add network location information to the information received from the NASS User. This reference point enables the user equipment to provide NASS User credentials (password, token, certificate, etc.) to the Network Attachment Subsystem (NASS) in order to perform network access authentication. This reference point may also enable the NASS to provide authentication parameter to the UE to perform the network authentication when mutual authentication procedure is required. Based on the authentication result, the AMF authorizes or denies the network access to the user equipment.

NOTE: When DHCP is used for IP address allocation and user equipment configuration over the interface (e1), IEEE 802.1X [5] and PANA are candidate protocols for authentication (e1).

5.6.2 Interface between CNGCF and CNG (e3)

This reference point allows the CNGCF to configure the CNG, trigger maintenance tests, monitoring the performance, and receive notifications. The e3 interface is used during initialization and update of the CNG to provide the CNG with additional network configuration information when these information are not available over the interface (e1), in order to allow the CNG to access to the TISPAN Service/applications.

The CNGCF may also manage the TE devices connected to a CNG, indirectly via the CNG or directly to the TEs, for configuration, maintenance, performance monitoring and notification purposes.

The e3 reference point shall support the following procedures:

- CNG identification/authentication to the CNGCF (e.g. in order to send appropriate configuration information (firmware upgrade) from the CNGCF.
- CNGCF authentication to the CNG before one CNG accepts a remote configuration for instance.
- Trigger maintenance tests from the CNGF and report test results from the CNG.
- Configure the CNG.
- Notify the CNGCF about TE availability.
- Provide configuration and upgrade for the TE devices.
- Trigger maintenance tests from the CNGCF and report test results from the TEs.

NOTE: TR-069 (DSL Forum), HTTP, FTP and TFTP are candidate protocols for this interface.

5.6.3 Reference points with the AMF

This reference point (a1) allows the AMF to request the NACF for the allocation of an IP address to user equipment as well as other network configuration parameters.

This reference point (a3) allows the AMF to request the UAAF for NASS User authentication and network subscription checking.

6 Mapping onto network roles

The NASS architecture does not assume any business roles, however to cope with the requirements for nomadism and roaming the NASS architecture can be mapped onto various functional network roles present in the fixed broadband access environment as provided in figure 6.1.

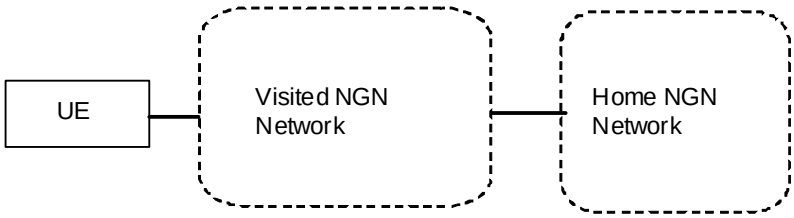


Figure 6.1: Functional network roles in TISPAN NGN

Figures 6.2 and 6.3 give the mapping of NASS. Examples of the access network in these figure is xDSL access network or a WLAN hotspot.

Figure 6.2 shows the scenario 1 whereby the service control subsystem is (partly) provided by the visited NGN network. Figure 6.3 clarifies a scenario 2 in which the home NGN network provides the service control subsystem.

Figures 6.4 and 6.5 both represent scenarios 3 and 4 in which a visiting TE is does not perform access authentication. In figure 6.4, the visiting TE is able to access its home services via roaming agreement at the level of the service control subsystems. The definition of this is however outside the scope of the present document and is specified in ES 282 001 [2]. Figure 6.5 gives a scenario in which service subsystems of the home network access the CLF in the visited network for location information via a proxy-CLF in the home network. The e2 interface is used here as a CLF to CLF interface.

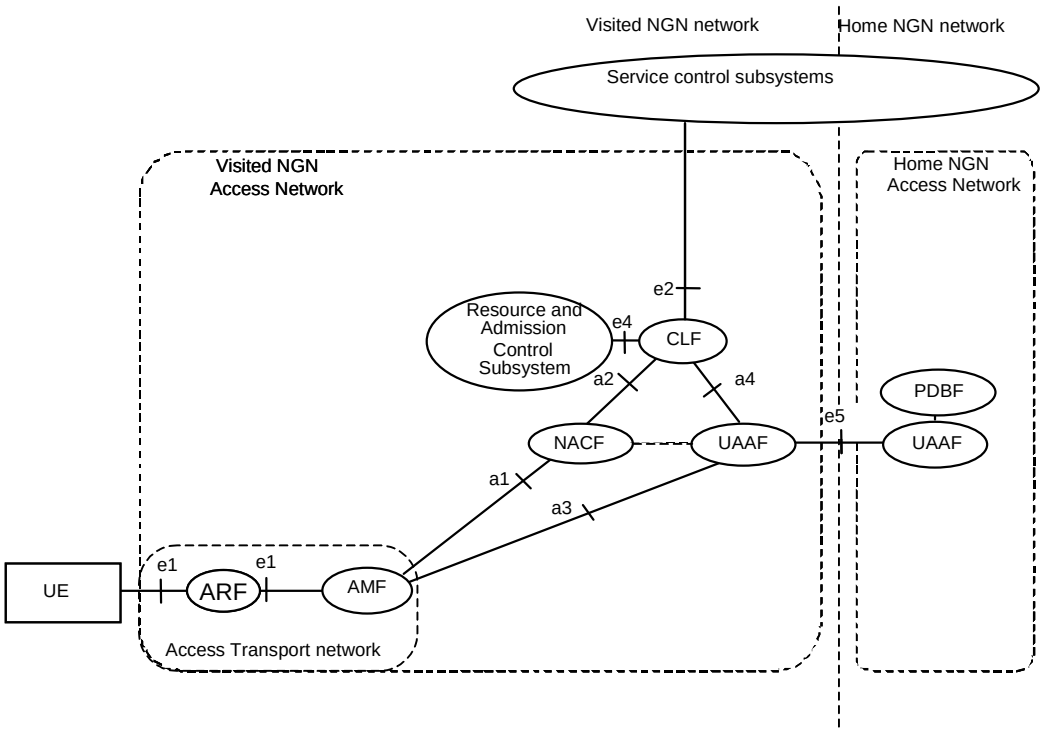


Figure 6.2: NASS mapped on functional network roles - scenario 1

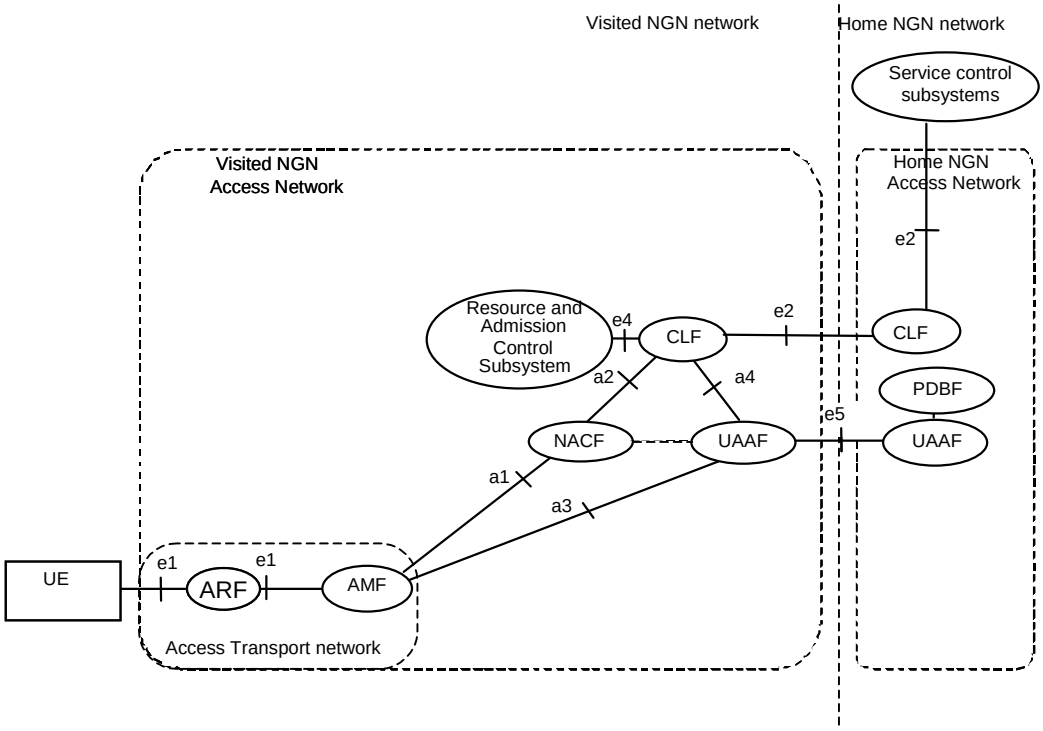


Figure 6.3: NASS mapped on functional network roles - scenario 2 (NGN services from the home network)

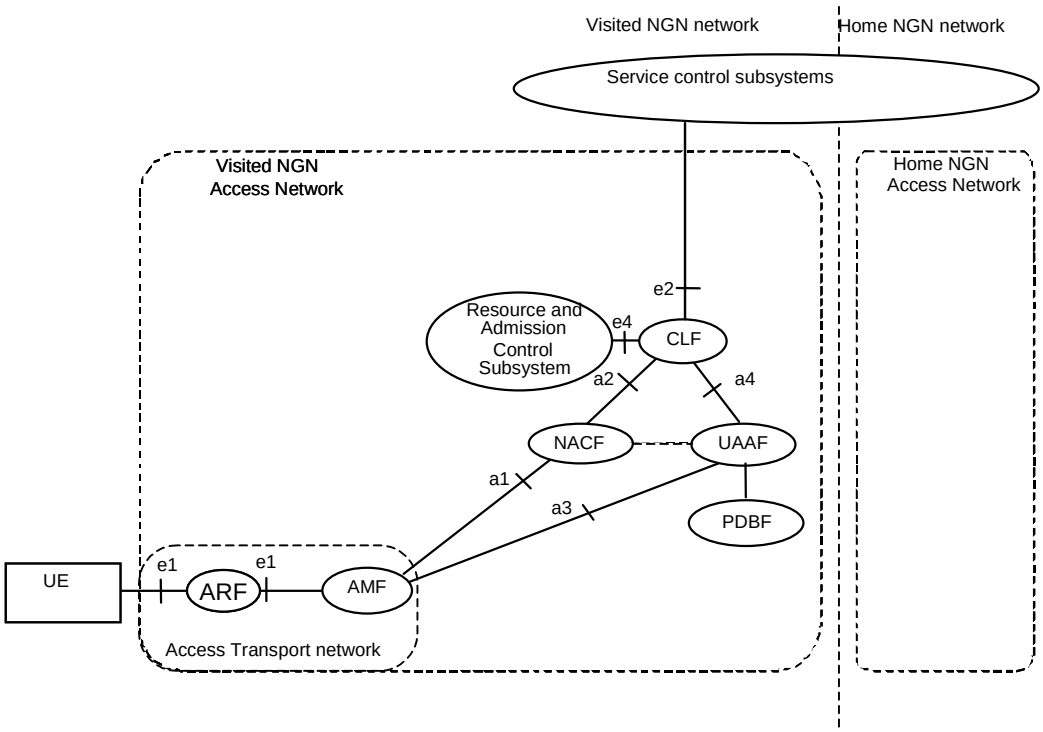


Figure 6.4: NASS mapped on functional network roles - scenario 3

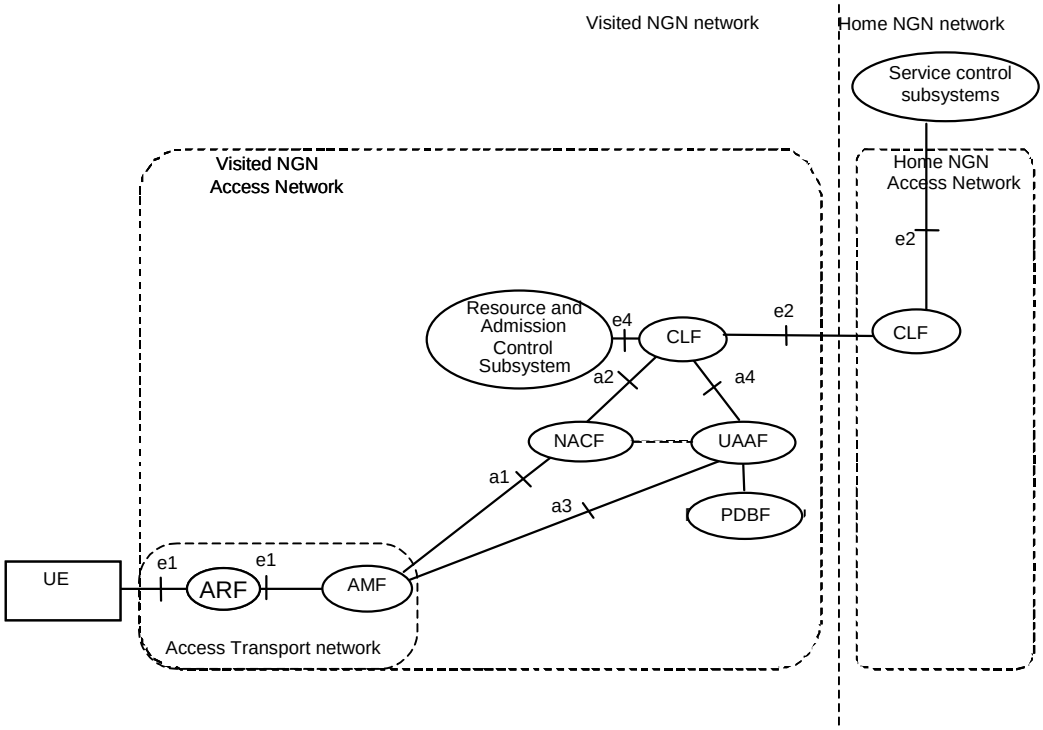


Figure 6.5: NASS mapped on functional network roles - scenario 4

7 Information flows

The procedures described in the present document are meant to provide a high level description for further Stage 3 work and are not intended to be exhaustive.

7.1 High level information flows

This clause provides high level information flows that define the network attachment process and the distribution of access NASS User network profile information within the NASS and towards the RACS.

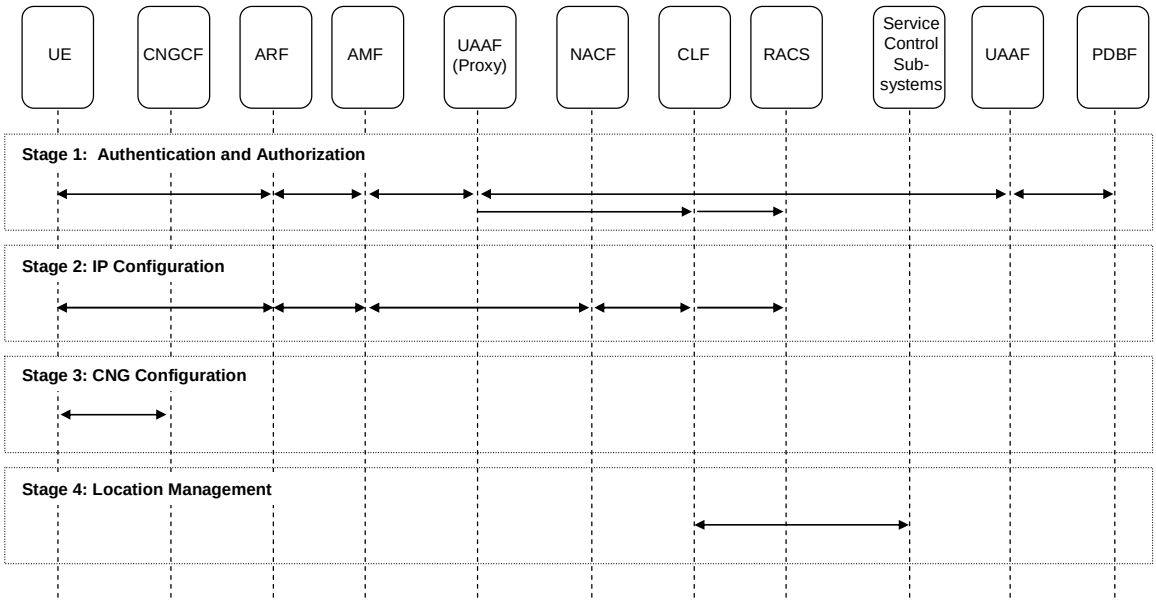


Figure 7.1: High level information flow

The NASS relies on several procedure-stages in the network attachment process. Figure 7.1 shows the high level information flow and the different procedures of NASS. Depending on the protocols (e.g. PPP, DHCP, etc.) and deployment scenarios used these procedure-stages can be applied in a different order than presented in figure 7.1, though for security reasons it needs to be ensured that the authentication procedure-stage is always successfully completed first. Different protocol procedures may be combined for the different procedure-stages of the attachment procedure (e.g. combination of PPP and DHCP procedures, combination of DHCP and PANA, etc.):

Procedure-stage 1) *Authentication and authorization:* In the first procedure-stage of the network attachment process the UE will be authenticated and authorized. The authentication process relies on the mechanisms and identities described in the previous clauses 4 and 5. This implies that line authentication and/or access authentication shall be used. The applicable identities are: NASS User identity and credentials provided by the NASS User. Procedure-stage 1 also involves the authorization for access to the network based on the NASS User profile. A NASS User specific configuration profile, related e.g. to QoS, may be downloaded from the home NGN network to the visited NGN network (from the UAAF-server to the in UAAF-proxy mode). When the authentication is successful and the UE is authorized to use access network resources, configuration of the access network based on the NASS User profile is performed. This also implies that the NASS User network profile information specific to the authenticated NASS User shall be forwarded to the CLF via the a4 reference point. The profile information shall include at least the identity of the line (line ID), NASS User identity and the NASS User network QoS profile, which may be the QoS profile downloaded from the home NGN network or a default profile, and the identity of the IP edge (IP-edge ID). If the authentication method chosen and/or the NASS User profile requires enforcement of access policies immediately after authentication (and prior to IP-address allocation), the CLF may push the NASS User profile via the e4 reference point to RACS.

NOTE 1: Procedure-stage 1 may occur as part of the IP address allocation procedure (procedure-stage 2).

Procedure-stage 2) IP configuration: IP configuration comprises "IP address allocation" (procedure-stage 2a) and "Service access point addressing information" (procedure-stage 2b):

Procedure-stage 2a): *IP-address allocation:* Dynamic provision of IP address and provisioning of IP configuration information to the UE. During procedure-stage 2a the NACF allocates the IP configuration information. The NACF receives from signalling via e1 the line identity (Line ID) and establishes the mapping between the allocated IP configuration information and the Line ID. This mapping information is forwarded to the CLF (via the a2 reference point), which correlates this with the NASS User identity and NASS User network profile and pushes this information to RACS via the e4 reference point. The RACS configures its functionality in line with the NASS User network profile information it receives from CLF.

Procedure-stage 2b): *Service subsystems contact point addressing information:* In procedure-stage 2b the UE obtains IP addressing information to access TISPAN NGN Service/Applications Subsystems (e.g. the IP address of the P-CSCF).

Procedure-stage 3) *UE configuration:* The CNGCF may configure UE parameters.

Procedure-stage 4) *Location management:* The TISPAN NGN service subsystems retrieve location information from the CLF via the e2 reference point. In case the TISPAN NGN service subsystems need to access location information in a different domain, the signalling to retrieve the location information shall be forwarded via a CLF proxy, which is located in the same network as the TISPAN NGN service subsystem that retrieves the information The primary parameter to retrieve the location information shall be the NASS User identity and/or the IP address allocated to the NASS User by NASS.

NOTE 2: Each procedure-stage may be invoked one or more times. For example, the sequence procedure-stage 1 followed by procedure-stage 2 may be invoked twice: first invocation with implicit authentication as per clause 4.4.1 followed by the allocation of a temporary IP address enabling contacting authentication servers; second invocation with explicit authentication followed by the allocation of a general purpose IP address.

NOTE 3: Different authentication steps may correspond to different NASS users (e.g. the IP address allocated during the first procedure-stage 2 invocation is considered allocated to the default NASS User associated to the line Id while the IP address allocated during the second procedure-stage 2 invocation is considered allocated to the NASS User authenticated during the second procedure-stage 1 invocation). or the same NASS user, in which case each authentication data set is associated to different sub-profiles of this NASS User in the PDBF.

7.2 PPP related procedures

This clause provides example information flows of NASS in case PPP [3] applies. These examples are not intended to cover the complete functionality of NASS.

NOTE 1: This is intended as an example only and does not prescribe stage 3 procedures.

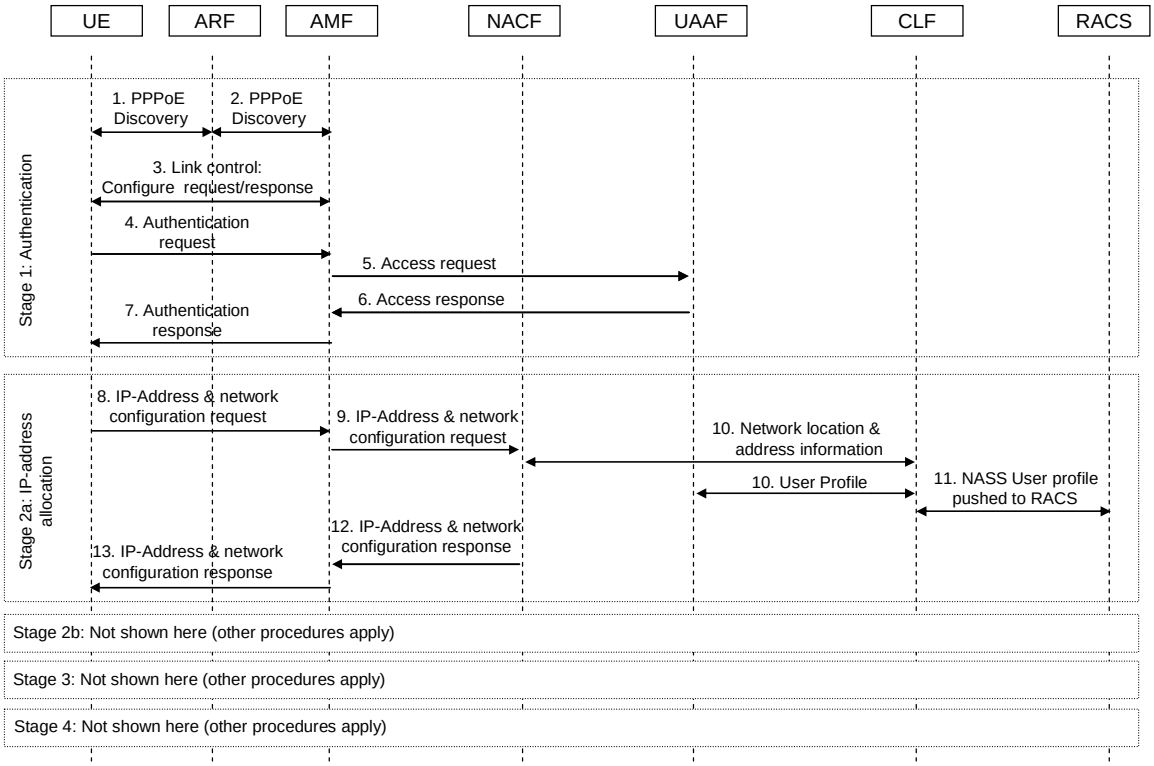


Figure 7.2: Authentication and IP-address allocation using PPP/PPPoE

This example focuses on procedure-stages 1 and 2a of the network attachment process (i.e. authentication and IP address allocation). Procedure-stages 2b, 3, and 4 are not considered here.

1.-2. UE performs PPPoE discovery procedures to identify the appropriate AMF and establish a peer-to-peer relationship with the AMF, as required by PPP. ARF implements a PPPoE intermediate agent function and inserts access line identification information into PPPoE messages.

3. Negotiation of data link parameters between UE and AMF, including the negotiation of the authentication procedure to be used.

4. UE initiates authentication and sends a corresponding information flow to AMF. The example assumes that NASS User identity and password information is supplied within the information flow.

5. AMF translates the PPP request into an access request to the UAAF which authenticates the NASS User associated to the UE.

6. UAAF responds with an access accept (assuming authentication success) to AMF.

7. AMF informs the UE about the successfully completed authentication.

NOTE 2: Steps 1 to 7 can be associated with the "PPPoE discovery" phase of PPPoE and "Link Control Protocol (LCP)" phase of PPP. The "authentication" procedure-stage of the access network attachment process is fulfilled as part of the LCP phase of PPP. Information flow steps 8 to 13 perform the "IP address allocation" procedure-stage within this call flow, typically associated with the "Network Control Protocols (NCPs)" phase of PPP, which is to configure the different network-layer protocols.

8.-9. UE sends a request to NACF to obtain IP addressing information.

10. NACF and UAAF push IP address information and the NASS User profile to CLF.

11. The CLF pushes the NASS User profile along with the associated IP addressing and location information to RACS via the e4 reference point.

12.-13. NACF supplies the IP addressing and network configuration information to the UE.

7.3 DHCP related procedures

This clause provides example information flows of NASS in case DHCP is used. These examples are not intended to cover the complete functionality of NASS.

NOTE: This is intended as an example only and does not prescribe stage 3 procedures.

7.3.1 IP configuration using DHCP

This example focuses on procedure-stage 2 of the network attachment process (i.e. IP configuration). Procedure-stages 1, 3, and 4 are not considered here.

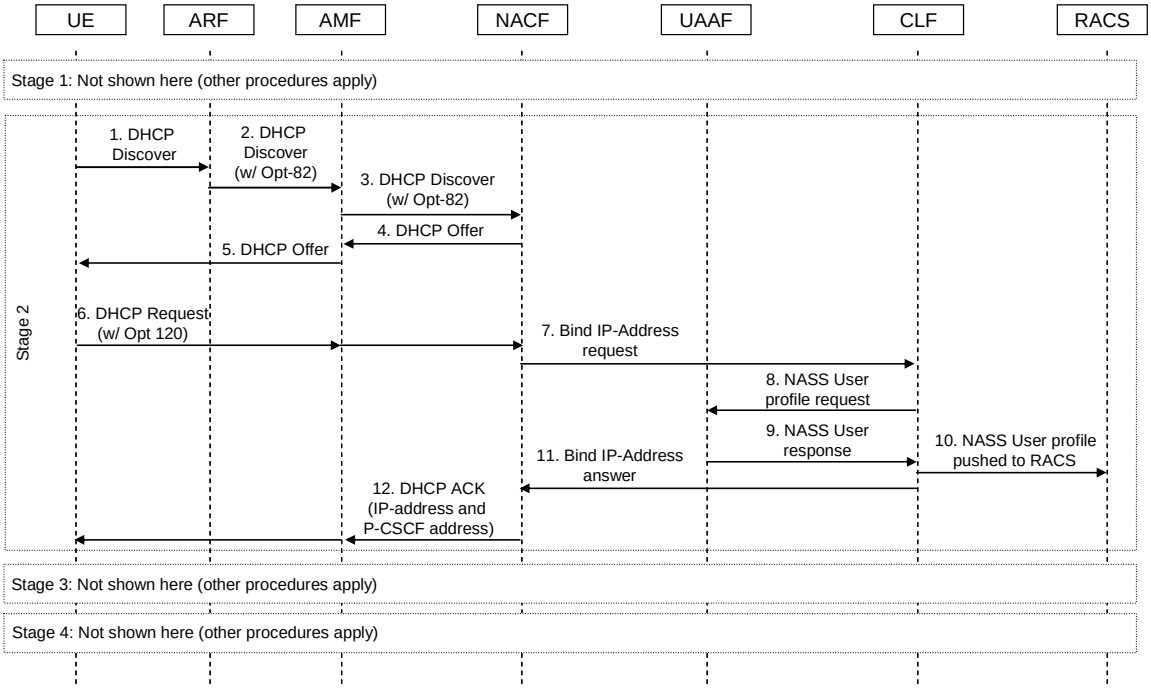


Figure 7.3: IP configuration using DHCP

1. The UE initiates the IP address allocation procedure by sending a DHCP Discover message.

2. ARF receives the message, adds additional information to the DHCP Discover (e.g. line identification), and forwards the message on to AMF. Information added by the ARF can serve multiple purposes, e.g. implicit authentication, NASS-bundled authentication, or location based services.

3. AMF receives the DHCP Discover and relays it to NACF, which operates as a DHCP server.

4.-5. NACF responds with a DHCP Offer to the UE.

6. The UE sends a DHCP Request to request an IP address and through DHCP option 120 the address of a TISPAN NGN Service/Applications Subsystem (e.g. P-CSCF). This request is relayed by the AMF to the NACF.

7. The NACF informs the CLF that an IP address is allocated to the UE.

8.-9. The CLF retrieves the NASS User profile from UAAF and associates it with the IP address received.

10. The CLF pushes the NASS User profile along with the associated IP addressing and location information to RACS via the e4 reference point.

11. CLF acknowledges to NACF the successful binding of IP address to NASS User profile. This message may also contain address information of the TISPAN NGN Service/Applications Subsystems contact point.

12. NACF provides the allocated IP address as well as the FQDN or IP address of the TISPAN NGN Service/Applications Subsystems contact point (e.g. P-CSCF), which is relayed by the AMF to the UE.

7.3.2 Implicit Authentication and IP Configuration using DHCP

This example focuses on procedure-stages 1 and 2 of the network attachment process (i.e. implicit authentication and IP configuration). Procedure-stages 3 and 4 are not considered here.

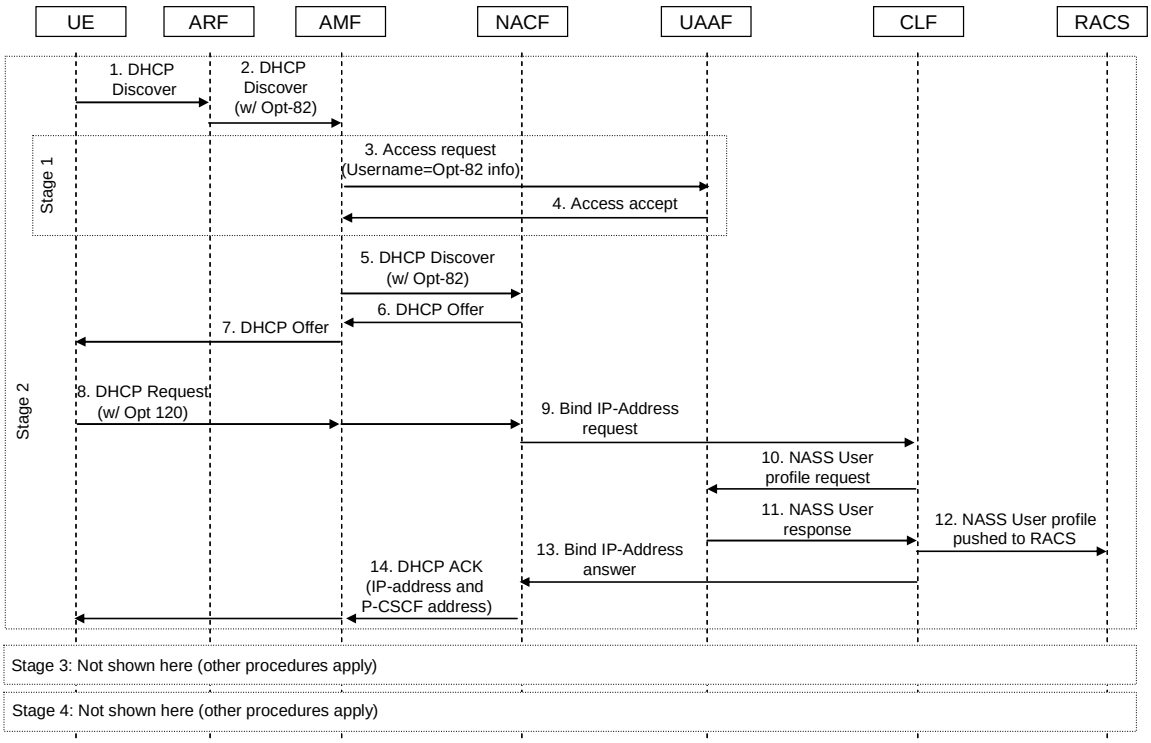


Figure 7.3a: Implicit authentication and IP configuration using DHCP

1. The UE initiates the IP address allocation and implicit authentication procedure by sending a DHCP Discover message.

2. ARF receives the message, adds additional information to the DHCP Discover (e.g. line identification), and forwards the message on to AMF. Note that the information added by ARF does not necessarily only serve implicit authentication but can be used for other purposes, e.g. location based services, NASS-bundled authentication etc. as well.

3. AMF receives the DHCP Discover and sends an access request to the UAAF to authorize the NASS User associated with the UE which sent the DHCP Discover. The association of NASS User profile and UE is facilitated by the line identification information.

4. UAAF responds with an access accept in case a NASS User profile could successfully be associated with the supplied line identification information.

   NOTE: Information flow steps 3. and 4. perform the "implicit authentication" procedure-stage of the access network attachment process within this call flow.

5. AMF sends the DHCP Discover to NACF, which operates as a DHCP server.

NOTE 1: If NACF and UAAF are collocated, procedure-stage 1 may be initiated after step 5 above.

6.-7. NACF responds with a DHCP Offer to the UE.

8. The UE sends a DHCP Request to request an IP address and through DHCP option 120 the address of a TISPAN NGN Service/Applications Subsystem (e.g. P-CSCF). This request is relayed by the AMF to the NACF.

9. The NACF informs the CLF that an IP address is allocated to the UE.

NOTE 2: Step 9 may be invoked right after step 6.

10.-11. The CLF retrieves the NASS User profile from UAAF and associates it with the IP address received.

12. The CLF pushes the NASS User profile along with the associated IP addressing and location information to RACS via the e4 reference point.

13. CLF acknowledges to NACF the successful binding of IP address to NASS User profile. This message may contain address information of the TISPAN NGN Service/Applications Subsystems contact point.

14. NACF provides the allocated IP address as well as the FQDN or IP address of the TISPAN NGN Service/Applications Subsystems contact point (e.g. P-CSCF), which is relayed by the AMF to the UE.

7.3.3 Explicit Authentication and IP Configuration using DHCP

This example focuses on procedure-stages 1 and 2 of the network attachment process (i.e. authentication and IP configuration). Procedure-stages 3 and 4 are not considered here.

NOTE 1: Other transport protocols to perform explicit authentication (e.g. PANA (see clause 7.5) or 802.1X (see clause 7.4)) can be utilized in which case DHCP is used for procedure-stage 2 only.

NOTE 2: The information flow given here is of example nature only. It does not prescribe any stage 3 procedures nor related specifications of the IETF.

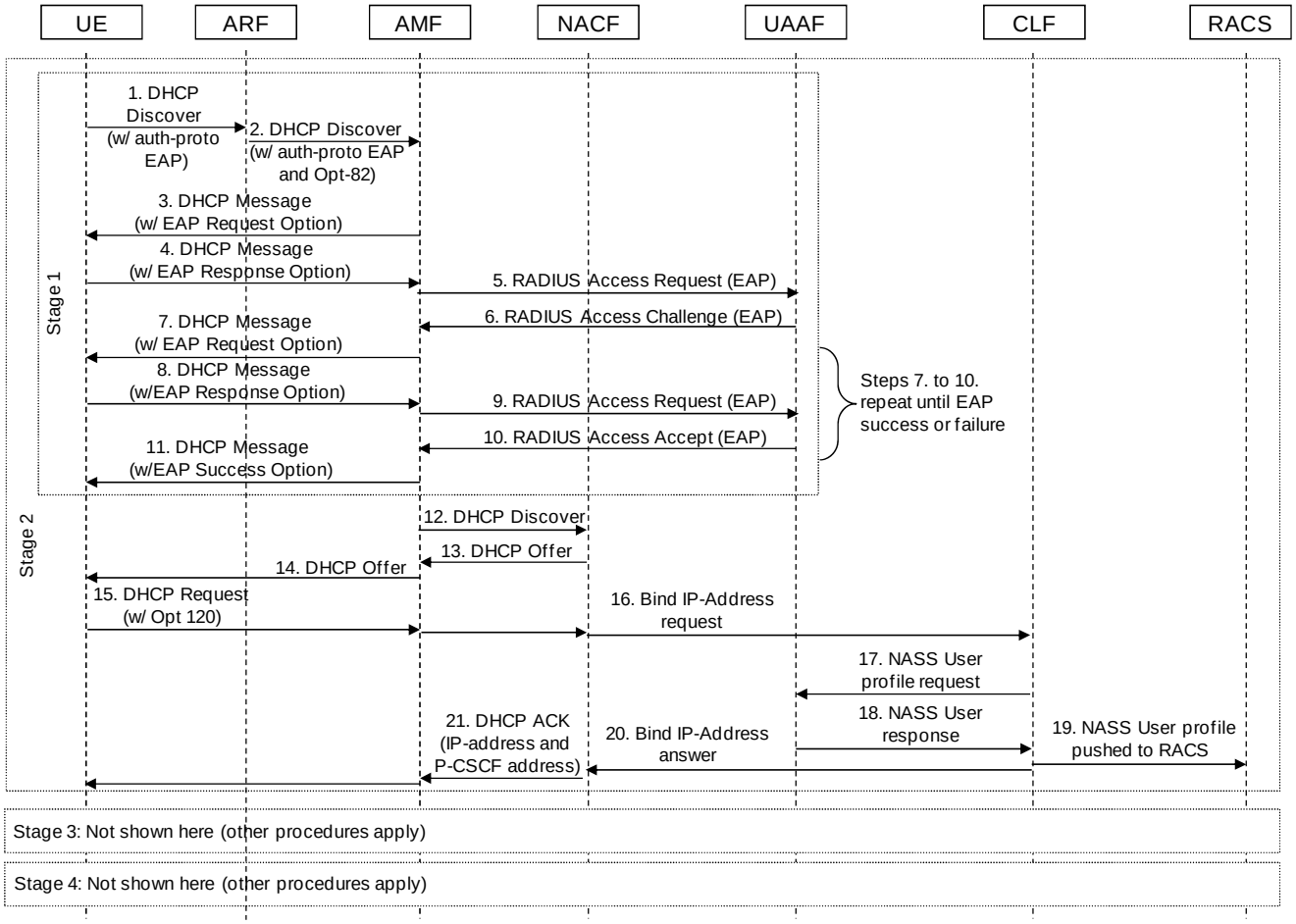


Figure 7.3b: Explicit Authentication and IP Configuration using DHCP

1. The UE initiates the IP address allocation and implicit authentication procedure by sending a DHCP Discover message with authentication protocol option EAP.

2. ARF receives the message, adds additional information to the DHCP Discover (e.g. line identification for location based services), and forwards the message on to AMF.

3. AMF responds with DHCP EAP message to UE.

4. UE responds with DHCP EAP message to AMF.

5. AMF sends Access Request to UAAF.

6. UAAF responds to AMF.

7. AMF sends DHCP EAP message to UE.

8. UE responds with DHCP EAP message to AMF.

9. AMF sends access request to UAAF.

10. UAAF responds to AMF.

NOTE: Steps 7 to 10 will be repeated until EAP success or failure. This diagram assumes a successful EAP negotiation.

11. AMF sends DHCP message with EAP success to UE.

12. AMF sends the DHCP Discover to NACF, which operates as a DHCP server.

13/14.NACF responds with a DHCP Offer to the UE.

15. The UE sends a DHCP Request to request an IP address and through DHCP option 120 the address of a TISPAN NGN Service/Applications Subsystem (e.g. P-CSCF). This request is relayed by the AMF to the NACF.

16. The NACF informs the CLF that an IP address is allocated to the UE.

17.-18. The CLF retrieves the NASS User profile from UAAF and associates it with the IP address received.

19. The CLF pushes the NASS User profile along with the associated IP addressing and location information to RACS via the e4 reference point.

20. CLF acknowledges to NACF the successful binding of IP address to NASS User profile. This message may contain address information of the TISPAN NGN Service/Applications Subsystems contact point.

21. NACF provides the allocated IP address as well as the FQDN or IP address of the TISPAN NGN Service/Applications Subsystems contact point (e.g. P-CSCF), which is relayed by the AMF to the UE.

7.3.4 Service Subsystems contact point configuration using DHCP

This example focuses on procedure-stage 2b of the network attachment process (i.e. Service Subsystems contact point addressing information). Procedure-stages 1, 2a, 3, and 4 are not considered here.

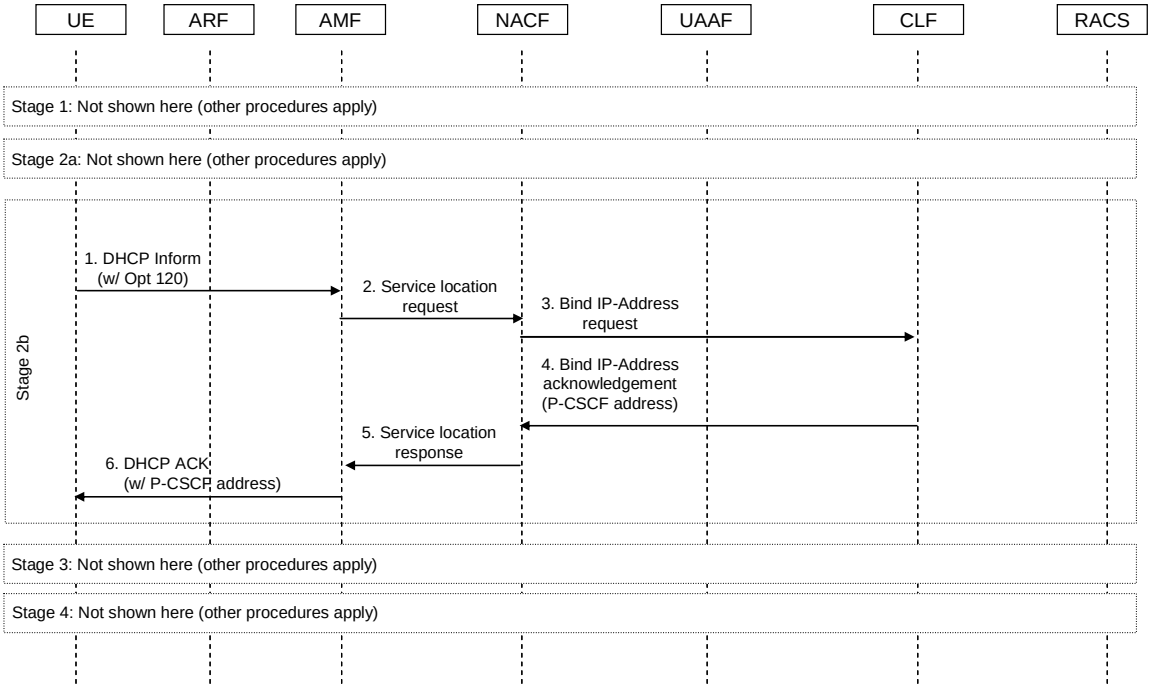


Figure 7.3c: Service Subsystems contact point configuration using DHCP

1.-2. The UE sends a DHCP Inform to request network parameters including the IP address of the TISPAN NGN Service/Applications Subsystem contact point (e.g. P-CSCF). This request is relayed by the AMF to the NACF.

3. NACF requests the IP address of the TISPAN NGN Service/Applications Subsystem contact point (e.g. P-CSCF) from CLF using the Bind information flow.

4. CLF responds with a Bind acknowledgement information flow to NACF, containing the IP address of the TISPAN NGN Service/Applications Subsystem contact point (e.g. P-CSCF).

5.-6. NACF provides the IP address of the TISPAN NGN Service/Applications Subsystems contact point (e.g. P-CSCF) to the AMF, which is then relayed by the AMF to the UE.

7.4 IEEE 802 Ethernet access based procedures

This clause provides example information flows of NASS in case IEEE 802 Ethernet procedures used. These examples are not intended to cover the complete functionality of NASS.

NOTE: This is intended as an example only and does not prescribe stage 3 procedures.

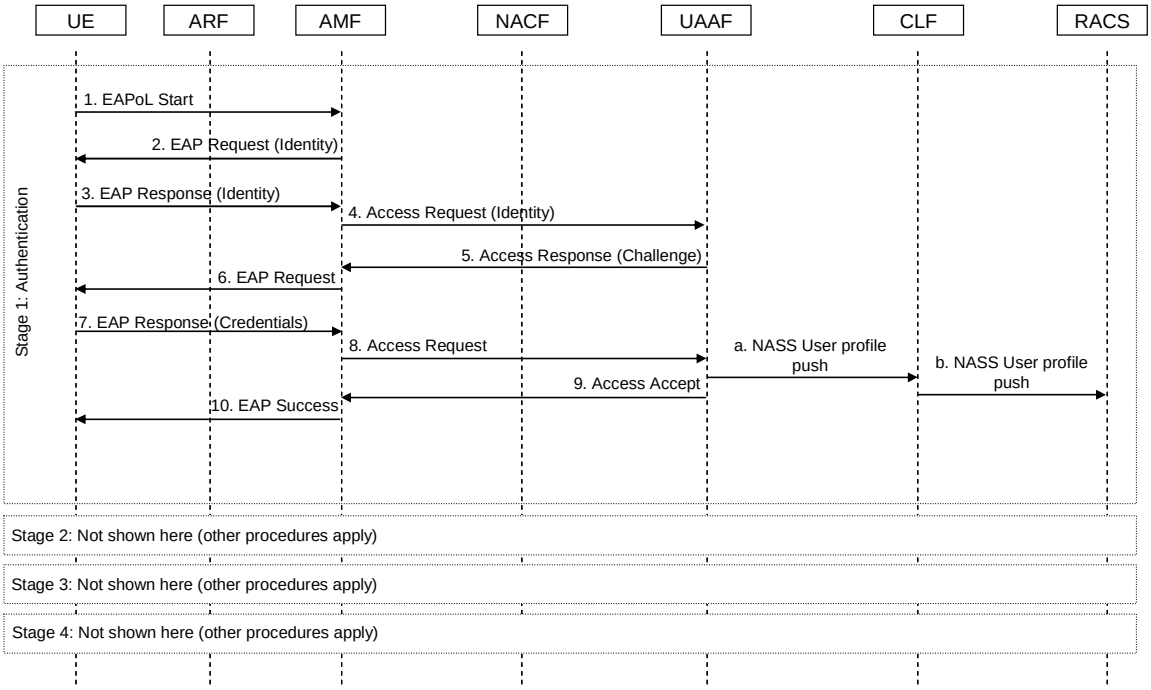


Figure 7.4a: Authentication using IEEE 802 Ethernet procedures (EAP-MD5)

This example focuses on procedure-stage 1 of the network attachment process (i.e. authentication). Procedure-stages 2, 3 and 4 are not considered here. The example information flow shown in figure 7.4a assumes the use of EAP-MD5. A shared secret associated with the NASS User which intends authentication is assumed to be available to UE and the UAAF.

1. The UE initiates the authentication conversation.

2-3. AMF retrieves the identity of the NASS User.

4. AMF provides the identity information to UAAF.

5-6. UAAF sends a random challenge to the UE.

7-8. The UE responds with a hash of the challenge, which is created by using the shared secret.

9. The UAAF verifies the hash and accepts (or rejects) the authentication. This example assumes a successful authentication, hence UAAF replies with access accept to AMF.

10. AMF informs the UE about the successful completion of the authentication procedure.

a. UAAF pushes the appropriate parts of the NASS User profile to CLF. Step a. can be carried out right after step 8 (assuming a successful access request).

b. CLF pushes the appropriate part of the NASS User profile to RACS. This allows RACS to enforce access policies (e.g. opening/closing of gates) right after authentication if so required.

7.5 PANA-based related procedures

This clause provides example information flows of NASS in case PANA is used for access network authentication. These examples are not intended to cover the complete functionality of NASS.

NOTE 1: This is intended as an example only and does not prescribe stage 3 (protocol) procedures.

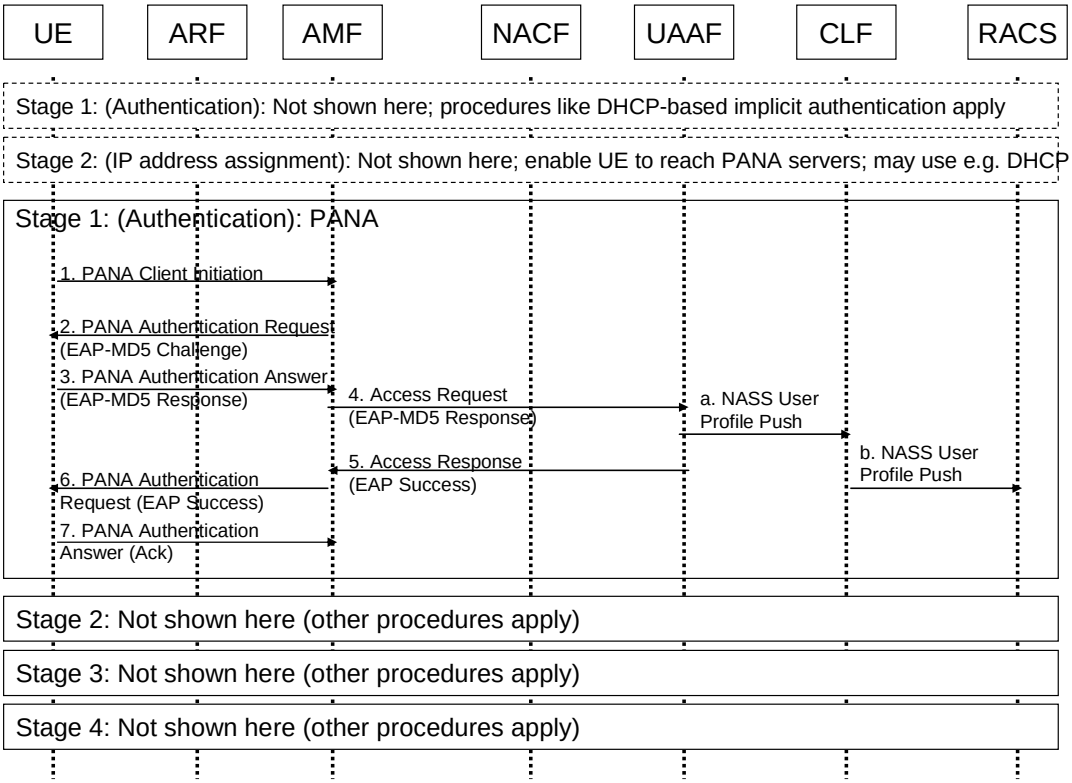


Figure 7.4b: Authentication using PANA-based procedures (EAP-MD5)

This example focuses on procedure-stage 1 of the network attachment process (i.e. authentication). Subsequent procedure-stages 2, 3, and 4 are not considered here.

NOTE 2: PANA specifications require PANA clients to obtain an IP address prior to performing PANA-based authentication. This address may be obtained through static configuration or by invoking procedure-stage 2 procedures, in which case it may be link-local address, an unspecified address or a non-link-local IP address, depending on the network configuration and the operator's policy. When the UE receives a link-local address or an unspecified address is allocated, it is an indication that a second procedure-stage 2 invocation is required after successful authentication to allocate a general purpose IP address to the UE.

The example information flow shown in figure 7.4b assumes the use of EAP-MD5 over PANA. A shared secret associated with the NASS User which intends authentication is assumed to be available to UE and the UAAF.

1. The UE initiates the authentication conversation.

2. AMF retrieves the identity of the NASS User and sends a random challenge to the UE.

3. The UE responds with a hash of the challenge, which is created by using the shared secret.

4. The AMF provides the NASS User identity, the random challenge and the associated UE response to the UAAF.

5. The UAAF verifies the hash and accepts (or rejects) the authentication. This example assumes a successful authentication, hence UAAF replies to the AMF with an access response indicating the UE has been authenticated.

6. AMF informs the UE about the successful completion of the authentication procedure.

7. The UE acknowledges the successful authentication.

a. UAAF pushes the appropriate parts of the NASS User profile to CLF. Assuming a successful authentication, step a. can be carried out right in parallel with step 5 or after.

b. CLF pushes the appropriate part of the NASS User profile to RACS. This allows RACS to enforce access policies (e.g. opening/closing of gates) right after authentication if so required. Step b may also be postponed to a later procedure-stage as the CLF may be waiting for the IP address to be allocated (procedure-stage 2) before pushing information to the RACS.

Annex A (informative): Physical Configurations

A.1 PPP case

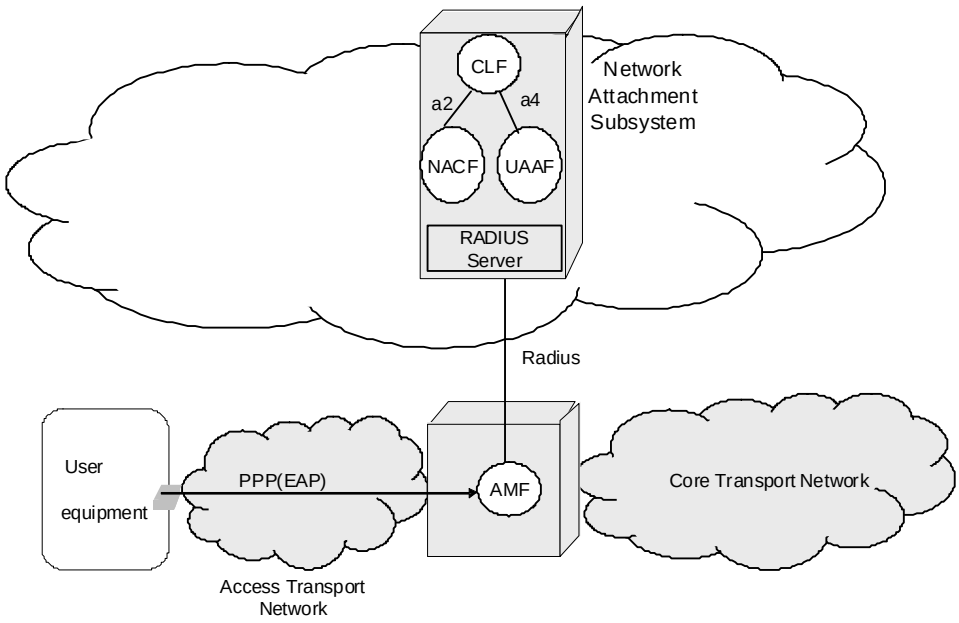


Figure A.1: PPP-based configuration

NOTE: For the sake of simplicity, interfaces to the RACS are not represented.

A.2 PPP with DHCP configuration

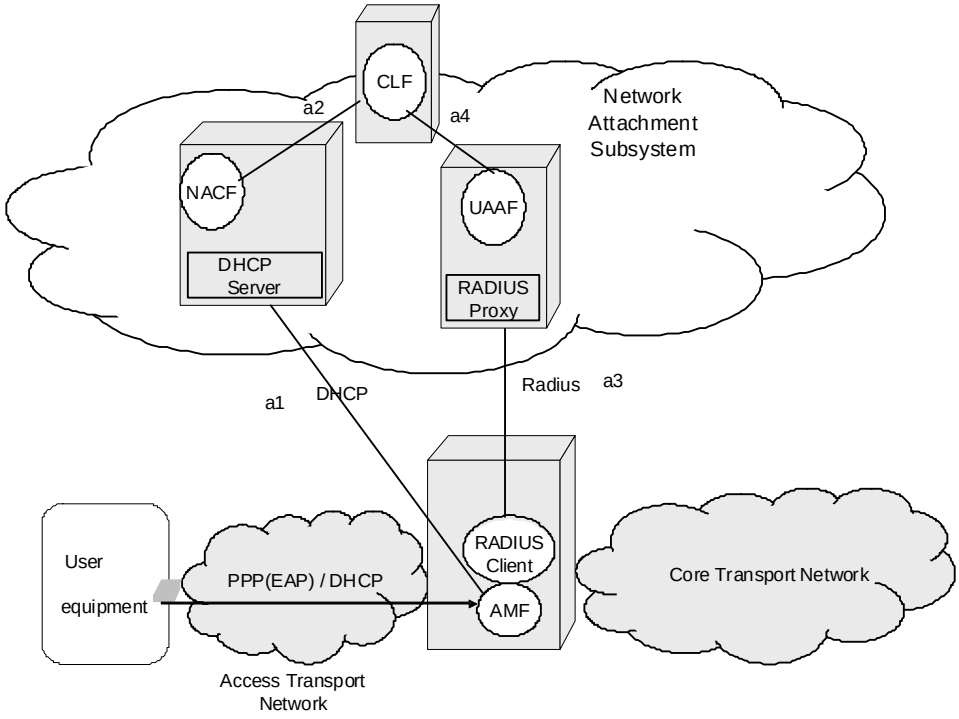


Figure A.2: PPP-based configuration with DHCP based IP configuration (allocation of the TISPAN NGN Service/Applications Subsystems contact point to the CNG)

A.3 DHCP (option 1)

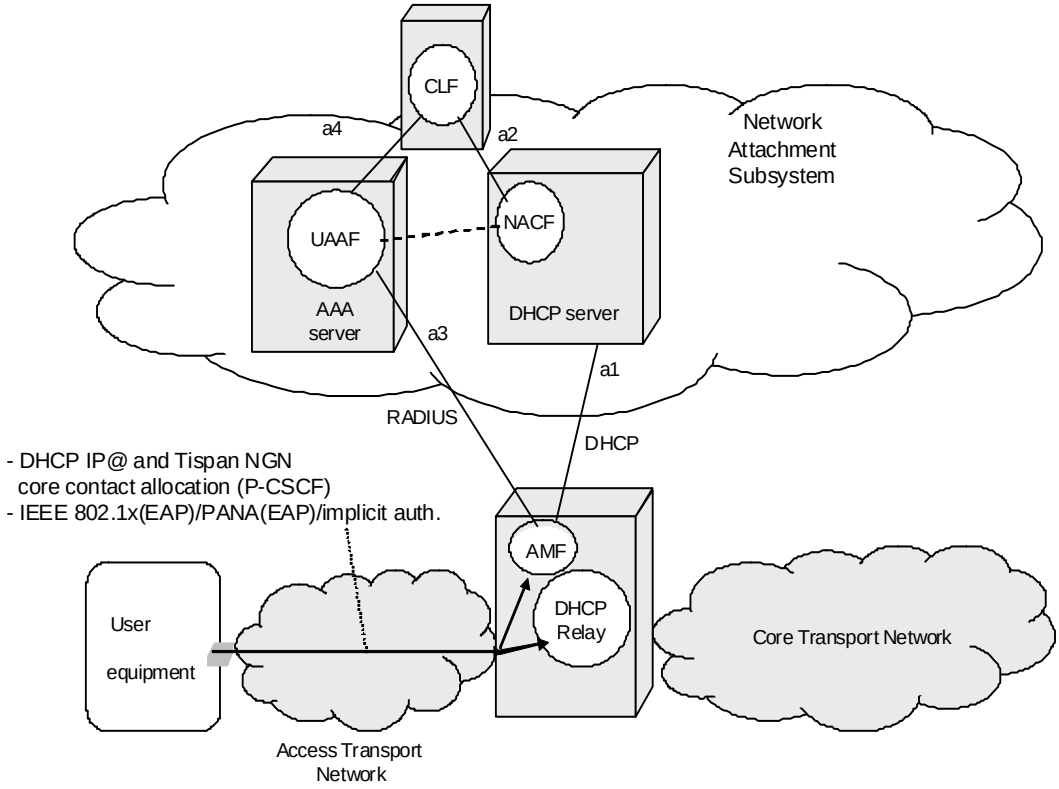


Figure A.3: DHCP-based configuration (option 1)

NOTE: For the sake of simplicity, interfaces to the RACS are not represented.

A.4 DHCP (option 2)

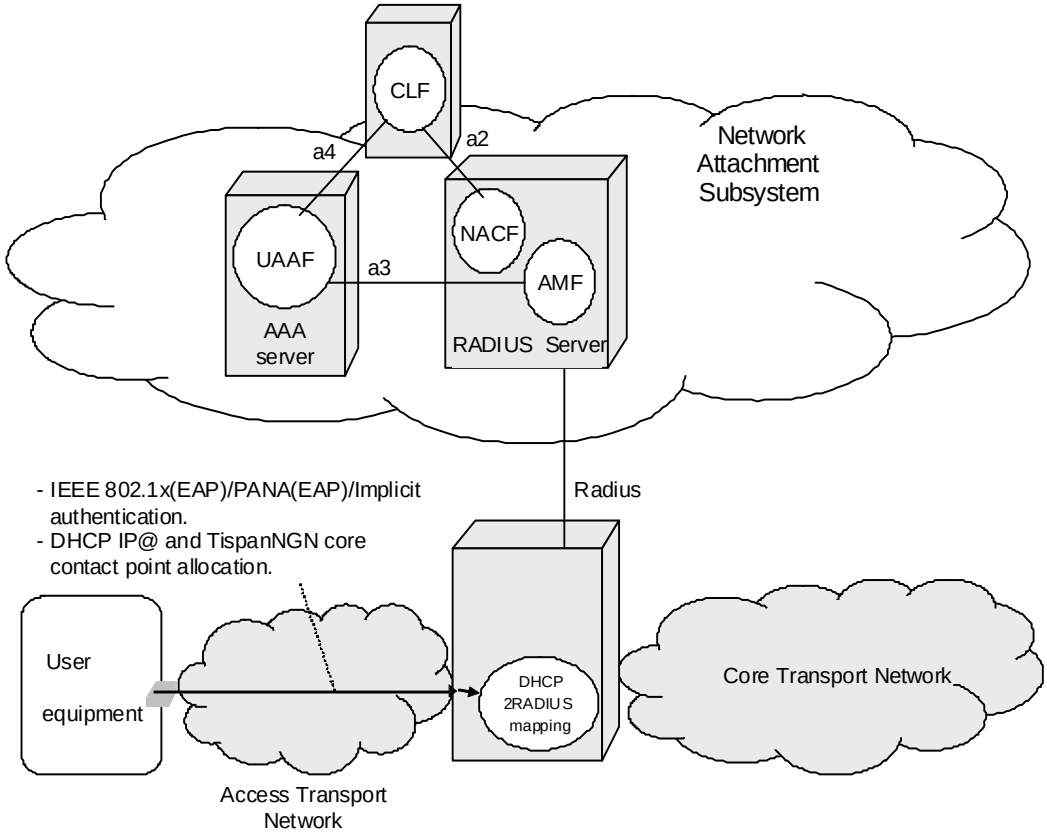


Figure A.4: DHCP-based configuration (option 2)

NOTE: For the sake of simplicity, interfaces to the RACS are not represented.

A.5 PANA-based configuration

With a DHCP-based implementation, the NASS User authentication may be provided at the IP layer by using PANA (Protocol for carrying Authentication for Network Access) defined within IETF. This IP protocol carries EAP between a PANA Client (PaC) residing in the user equipment and a PANA Authentication Agent (PAA) in the transport plane. This PANA signalling goes through an Enforcement Point (EP) that controls the access of unauthorized NASS Users to the network.

The PAA consults an authentication server in order to verify the credentials and rights of a PaC. If the authentication server resides on the same physical equipment as the PAA, an API is sufficient for this interaction. When they are separated RADIUS or Diameter may be used for this purpose.

Once the NASS User is successfully authenticated and authorized to access to the network, the PAA sends to the EP configuration information to modify the per-packet enforcement policies (i.e. filters) applied on the inbound and outbound traffic of the user equipment.

Figure A.5 describes a PANA-based implementation for the physical configuration of NASS:

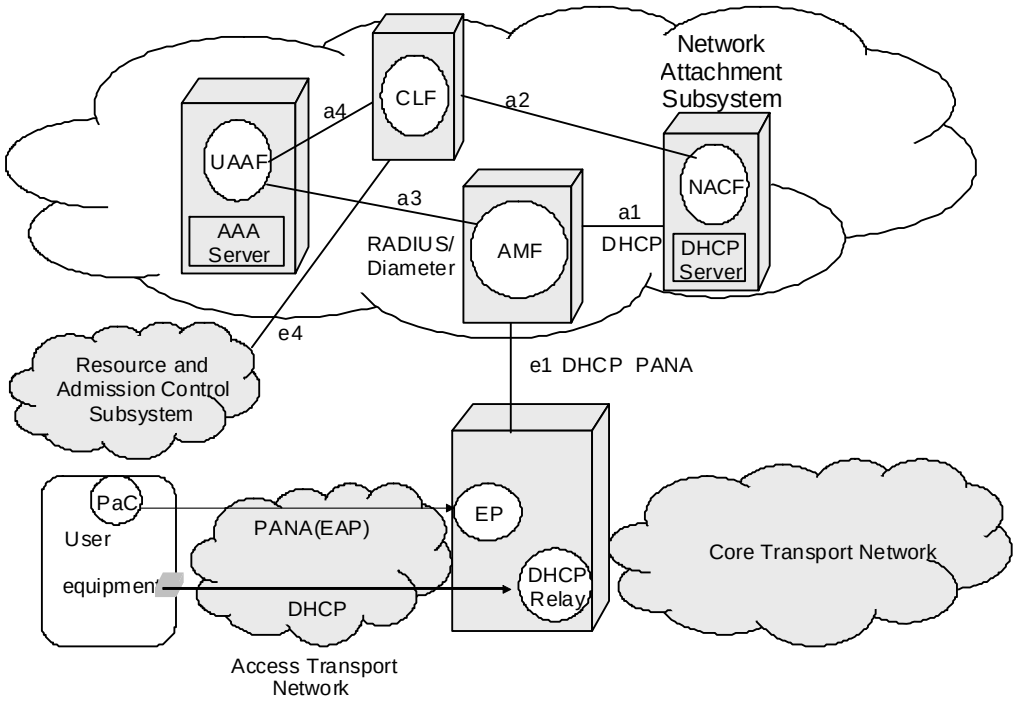


Figure A.5: PANA-based configuration

Annex B (informative): Recovery procedures for functional elements within NASS

B.1 Conceptual information exchange flow for CLF state recovery

Details for the actual flow of information exchanges for a full recovery of state of the CLF are out of the scope of the present document. Below are two examples for CLF recovery procedures if a CLF is queried for information which is not currently available within the data-base of the CLF.

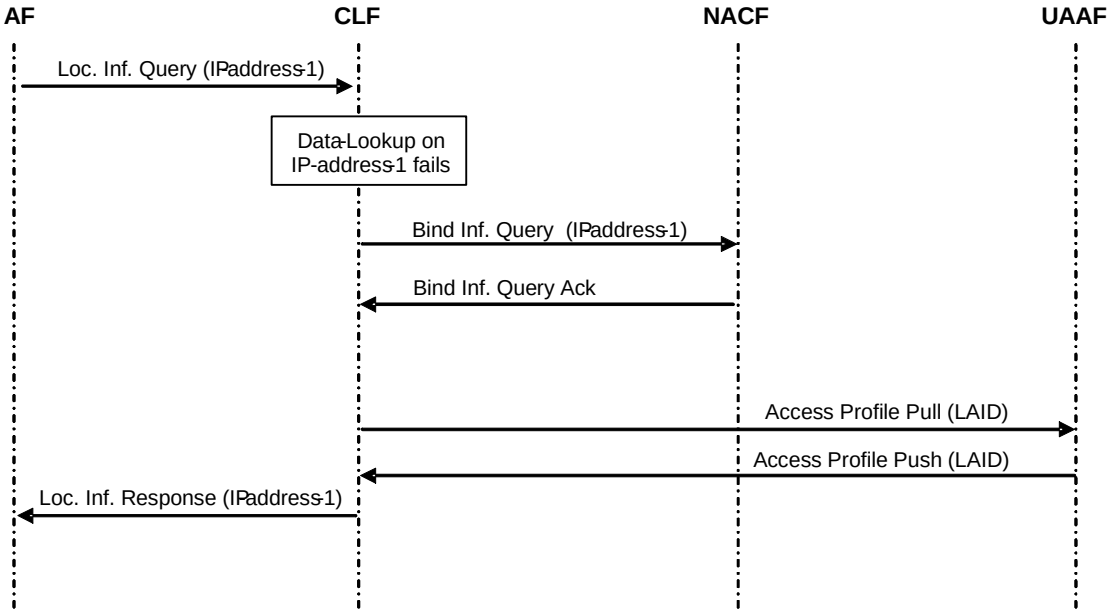


Figure B.1: CLF state recovery: Information query from AF

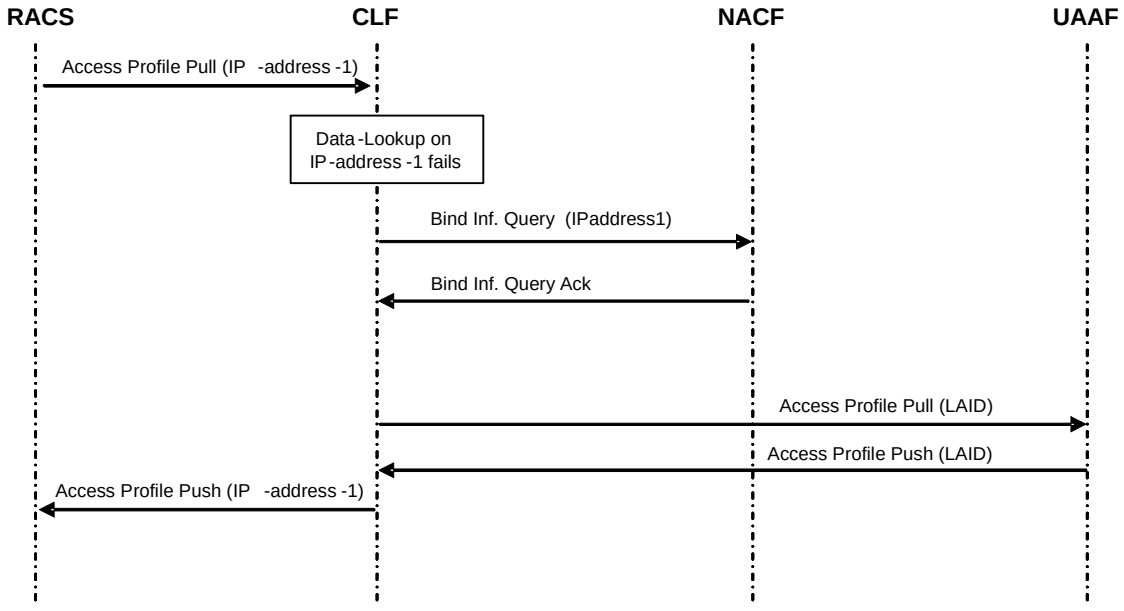


Figure B.2: CLF state recovery: Information query from RACS

Annex C (informative): Bibliography

- ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".
- IETF RFC 4058: "Protocol for Carrying Authentication for Network Access (PANA) Requirements".
- IETF RFC 2131: "Dynamic Host Configuration Protocol".

Annex D (informative): Change history

Change history							
Date	**WG Doc.**	**CR**	**Rev**	**CAT**	**Title / Comment**	**Current Version**	**New Version**
23-05-08	17bTD222r1	-			NASS Rel-3 input draft to TISPAN 17bis (based on ETSI ES 282 004 V2.0.0)		3.0.0
30-05-08	17bTD223r3	001		C	NASS high-level information flows – various improvements – clause 7.1	3.0.0	
05-07-08	17bTD328	-			Output draft of TISPAN 17bis		3.0.1
02-07-08	18WTD204r2	002		B	NASS high-level information flows – Improved PPP procedures	3.0.1	3.1.1
02-07-08	18WTD160r1	003		B	Add Physical Access ID to a4 interface	3.0.1	3.1.1
02-07-08	18WTD159r2	004		B	Add Some Information Elements to a4 interface	3.0.1	3.1.1
02-07-08	18WTD207r2	005		F	Addition of Ethernet Authentication to NASS	3.0.1	3.1.1
02-07-08	18WTD338				Output draft of TISPAN 18bis	3.0.1	3.1.1
07-07-08					All CRs approved by TISPAN#18	3.0.1	3.1.1
12-11-08	18bTD275r2	006		B	Changes to privacy rules management to allow privacy indication to the application and service control subsystems.	3.1.1	3.2.0
					CR approved by TISPAN#19	3.1.1	3.2.0
12-11-08	19bTD037				Input draft for TISPAN 19bis		3.2.0
24-02-09	20WTD219r1	007		F	WI2068 – Editorial corrections	3.2.0	3.2.1
24-02-09	20WTD290				Output draft of TISPAN 20W	3.2.0	3.2.1
10-03-09					CR 007 TB approved at TISPAN#20	3.2.1	3.3.0
19-08-09	21bTD42r2	008		F	Use of PANA	3.3.0	3.3.1
19-08-09	21bTD149r2	009		B	NASS high-level information flows – Improved DHCP procedures	3.3.0	3.3.1
19-08-09	21bTD166r1				Output draft of TISPAN 21bis	3.3.0	3.3.1
					CRs 008 and 009 TB approved and publication		3.3.1

History

Document history		
V1.1.1	June 2006	Publication
V1.3.0	June 2008	Publication
V2.0.0	February 2008	Publication
V3.3.2	December 2009	Membership Approval Procedure MV 20100220: 2009-12-22 to 2010-02-22