3GPP TR 23.862 V1.0.0 (2012-11)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
EPC enhancements to Support Interworking with Data Application Providers (MOSAP);
Stage 2
(Release 12)

Keywords
3GPP, Architecture, EPC, Data Applications

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This Technical Report describes solutions for interworking between mobile operators and data application providers. The solutions developed will describe a framework for authentication, authorization, policy and charging for various interworking scenarios.

Solutions developed as part of this work item will cover the following different relationships between mobile operators and data application providers for both roaming and non-roaming cases when

- mobile operator owns all the application layer entities;
- mobile operator does not own all the application layer entities.

The technical report will investigate charging, policy and group addressing capabilities for interworking between mobile operators and data application providers. Updates to 3GPP functions and interfaces will be specified for solutions based on IMS and/or EPC.

On-going work for authentication and other aspects in other 3GPP work items will not be duplicated. It will be investigated whether changes to 3GPP specifications are needed and if so which ones. The work item will focus on impacts to IMS and EPC.

Editor's note: The investigation of solutions based on GSMA OneAPI and Wholesale Applications Community (WAC) will be deprioritised and may be postponed to Rel-12 depending on available time for completion of this report.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 41.001: "GSM Release specifications".

[3] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[4] 3GPP TS 33.210: "3G Security; Network Domain Security (NDS); IP Network Layer Security".

[5] 3GPP TR 33.924: "Identity Management and 3GPP Security Interworking; Identity Management and Generic Authentication Architecture (GAA) Interworking".

[6] 3GPP TS 23.335: "User Data Convergence (UDC); Technical Realization and Information Flows; Stage 2".

[7] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[8] 3GPP TS 23.203: "Policy and charging control architecture".

[9] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[10] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[11] 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Bootstrapping Server Function (BSF): Definition from TS 33.220 [3].

Network Application Function (NAF): Definition from TS 33.220 [3].

OpenID Provider (OP): Definition in TR 33.924 [5].

Relying Party (RP): Definition in TR 33.924 [5].

User Data Repository (UDR): Definition in TS 23.335 [6].

Front End (FE): Definition in TS 23.335 [6].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

BSF	Bootstrapping Server Function
IdP	Identity Provider
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
NAF	Network Application Function
OP	OpenID Provider
FE	Front End
UDC	User Data Convergence
UDR	User Data Repository

4 Scenarios for interworking between mobile operators and data application providers

Several scenarios are presented in this section. They can exist simultaneously in a mobile operator's network. Figure 4-1 shows the non-roaming scenario where the mobile operator owns the EPS as well as application layer entities. Access and IP connectivity is provided by the mobile operator. Application platforms, also provided by the mobile operator, shown in the figure connect to the core network directly. Application platforms could be application servers (e.g. Video on Demand Server, PSS Server, MTC Server, etc.).

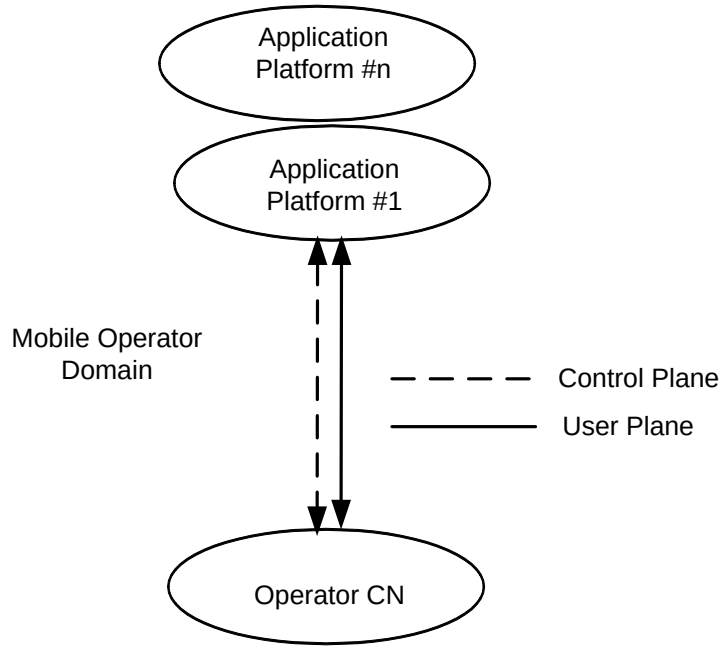

Figure 4-1: Non-roaming scenario - All entities owned by mobile operator

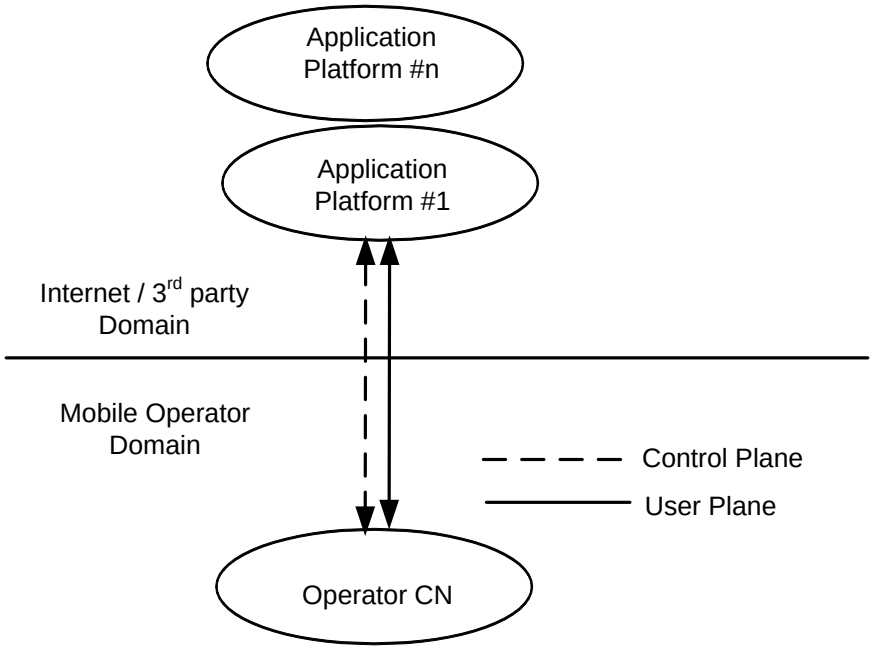

Figure 4-2: Non-roaming scenario - Application platform owned by 3rd Parties/Internet

Figure 4-2 provides the non-roaming scenario where the mobile operator does not own all the application layer entities. Access and IP connectivity is provided by the mobile operator. The 3rd party Application Platforms in this figure could be application servers (e.g. Video on Demand Server, PSS Server, MTC Server, etc.) or could be 3rd party software development platforms. The horizontal line represents the demarcation between the mobile operator domain and the 3rd party application provider domain. The mobile operator and 3rd party application providers may have agreements.

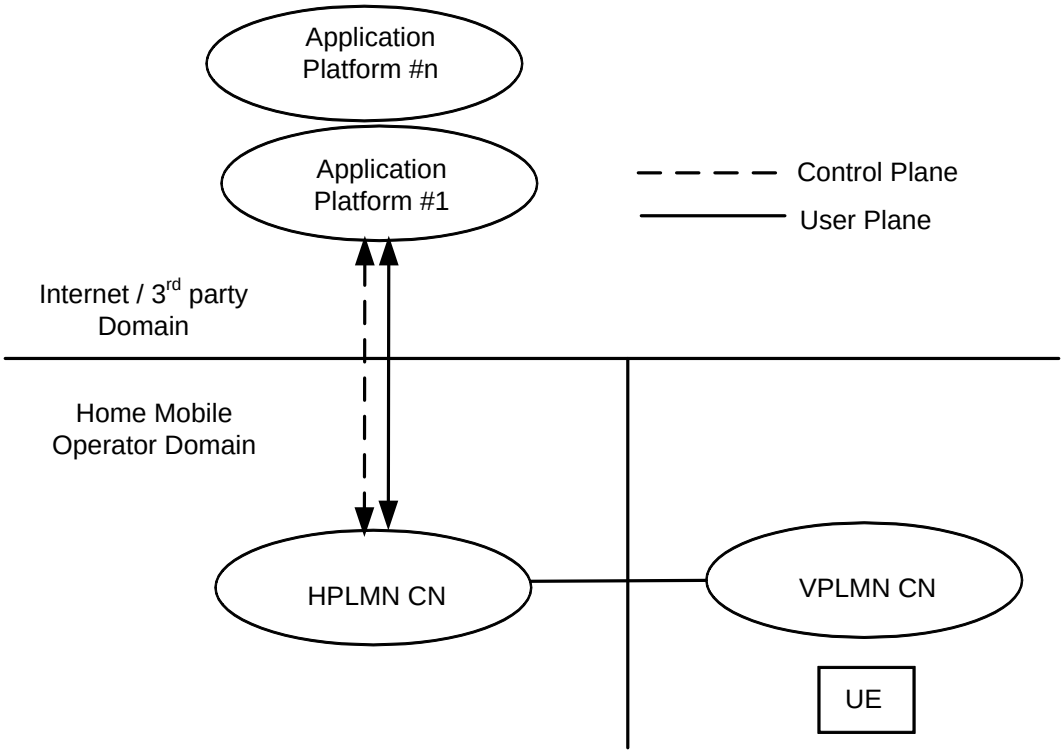

Figure 4-3: Home Routed Roaming scenario - Home Mobile Operator owned/collaborated Application Platform

Figure 4-3 provides the roaming scenario for both the above owned and collaborative scenarios. This figure shows the home-routed scenario where all traffic is routed to home mobile operator EPS and applications are delivered via roaming agreements between mobile operators.

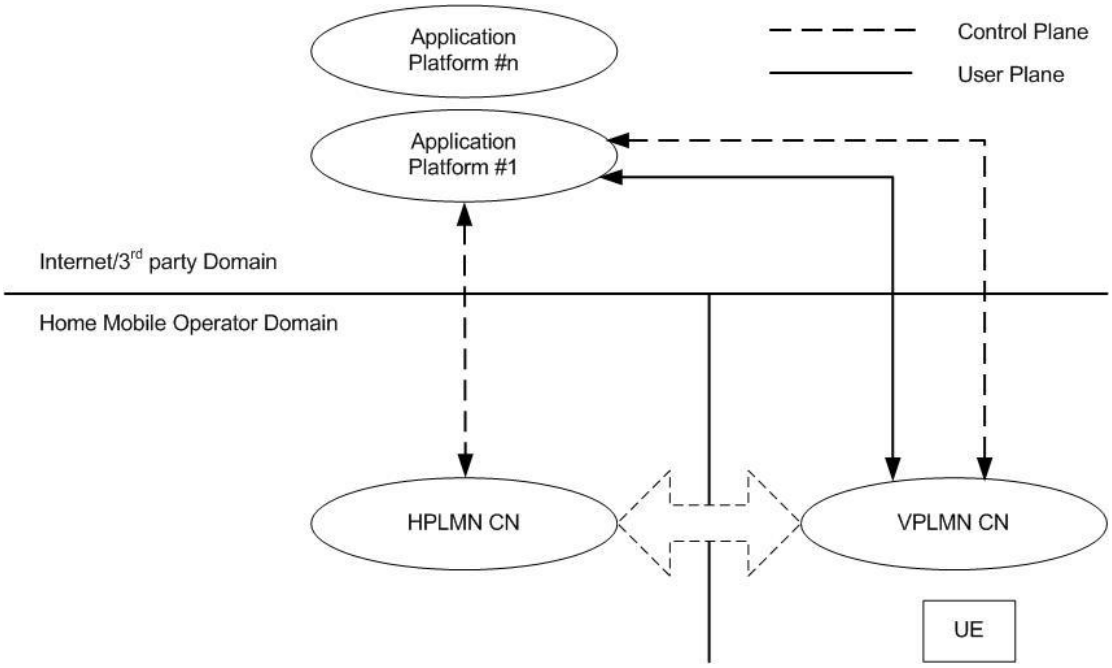

Figure 4-4: Local Breakout roaming scenario - visited mobile operator collaborative Application Platform

Figure 4-4 provides the roaming scenario between mobile operators and 3rd party application provider domains. In this scenario the application provider has agreements with visited mobile operator. This figure shows the local-breakout scenario where all traffic is routed to application domain from the visited operator network. The home network still performs authentication and authorisation of the user, and also provides policy information to the visited network using the existing mechanisms and roaming agreements.

NOTE: Application provider interaction with the visited mobile operator for the policy happens directly because of the collaboration with visited mobile operator.

Editor's Note: Other scenarios for (1) Home-routed roaming, with VPLMN owned/collaborative; (2) LBO roaming, with HPLMN owned/collaborative, (3) LBO roaming, with VPLMN owned/collaborative are for FFS.

Editor's Note: It is FFS whether it is required to have policy interactions between the Application platform and HPLMN in order to fulfil this scenario or it is possible to fulfil all the policy interactions directly with the VPLMN.

5 Architectural Requirements

This work-item shall use existing standards to achieve the objectives to the extent possible.

6 Solutions for interworking between mobile operators and data application providers

Editor's Note: This clause will describe the solution(s) for interworking between mobile operators and data application providers.

6.1 Architecture #1

6.1.1 Architecture Principles

Non-roaming and roaming home-routed/local breakout scenarios are supported.

The UDC architecture is used as a basis for user data management. UDR can be used by the non-IMS AS to store/retrieve application related data via Mh. The data model used for storing and retrieval is transparent to the UDR.

GBA and interworking between GBA and OpenID is used as a basis for security framework. Roaming scenarios are also addressed.

Network Domain Security (TS 33.210 [4]) can be used for security of reference points exposed to 3rd parties.

6.1.2 Architecture Description

Solution is based on existing EPC architecture along with UDC and GBA architectures (TS 33.220 [3], TS 33.210 [4], TR 33.924 [5], TS 23.335 [6]).

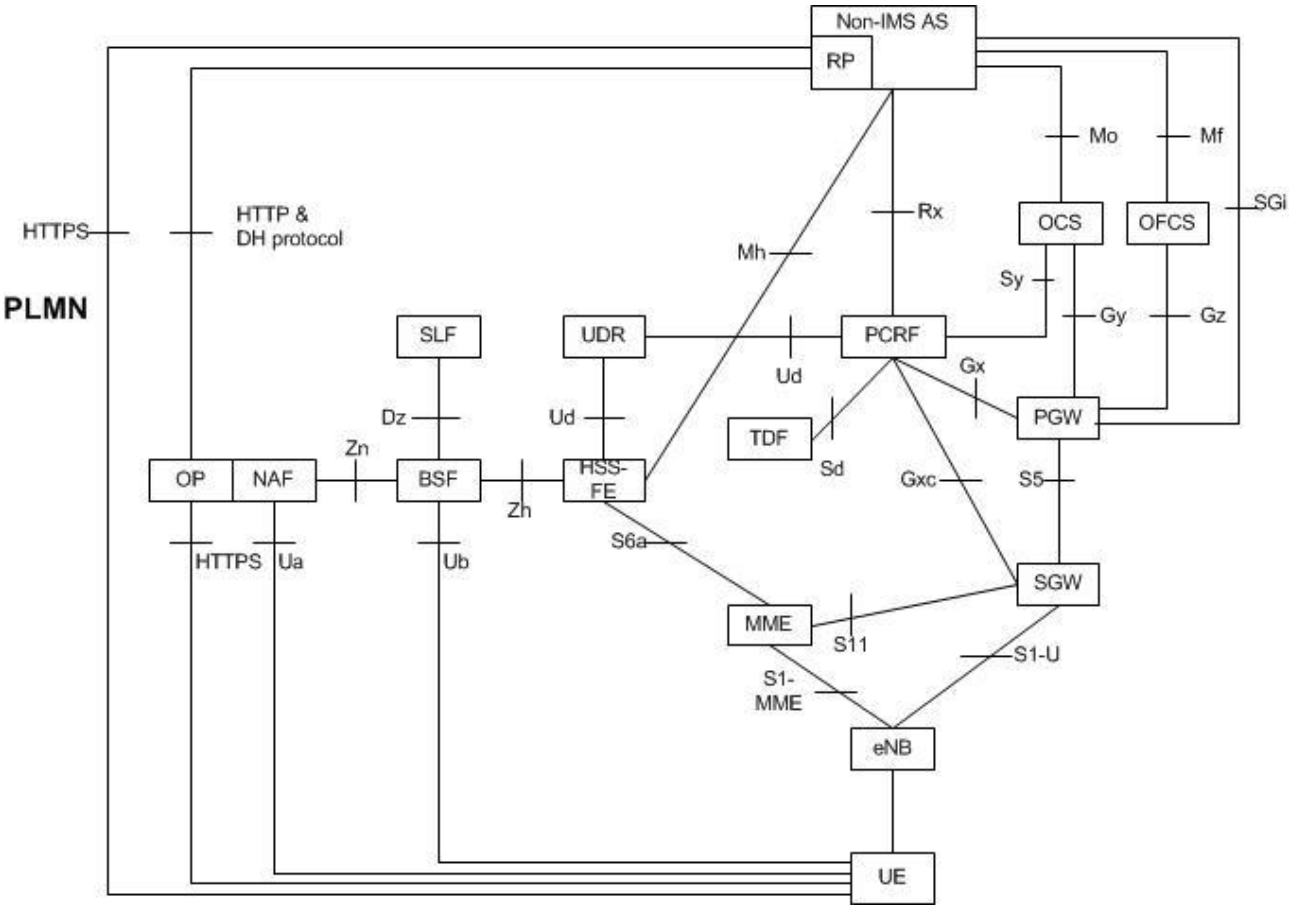

Figure 6.1.2-1: Non-Roaming Architecture - all entities owned by the Mobile Operator

Figure 6.1.2-1 shows the architecture components and the interfaces.

EPC components (eNB, SGW, PGW, MME and PCRF) are specified in TS 23.401 [7].

UDC components (UDR and HSS-FE) are specified in TS 23.335 [6].

GBA (BSF, NAF and SLF) are specified in TS 33.220 [3]. GBA and OpenID interworking components (OP and RP) are identified in TR 33.924 [5].

The non-IMS Application server can belong to the Mobile Network Operator or to a 3rd party application provider. In the latter case, appropriate security mechanisms need to be provided to protect the interfaces to PCRF, OCS, OFCS, HSS-FE and RP such as TS 33.210 [4].

The following are the associated interfaces for the architecture:

- S1-MME, S1-U, S5, S6a, Gx, S8, S9, S11, SGi are specified in TS 23.401 [7].
- Gxc is specified in TS 23.402 [9]
- Rx, Sy, Gy, Gz are specified in TS 23.203 [8].
- Ud is specified in TS 23.335 [6].
- Zh, Zn, Ua, Ub, Dz are specified in TS 33.220 [3].
- Mh is the interface between the non-IMS AS and HSS-FE and it can span beyond 3GPP (H)PLMN. It is similar to the Sh interface but it is not used by IMS application. Protocol used on Mh is assumed to be based on Sh as defined in 3GPP.
- Mo, Mf are the interfaces between the MNO owned non-IMS AS and OCS, OFCS respectively and can span beyond 3GPP (H)PLMN. They are based on the Ro and Rf interfaces specified in TS 32.240 [10] and TS 32.299 [11].

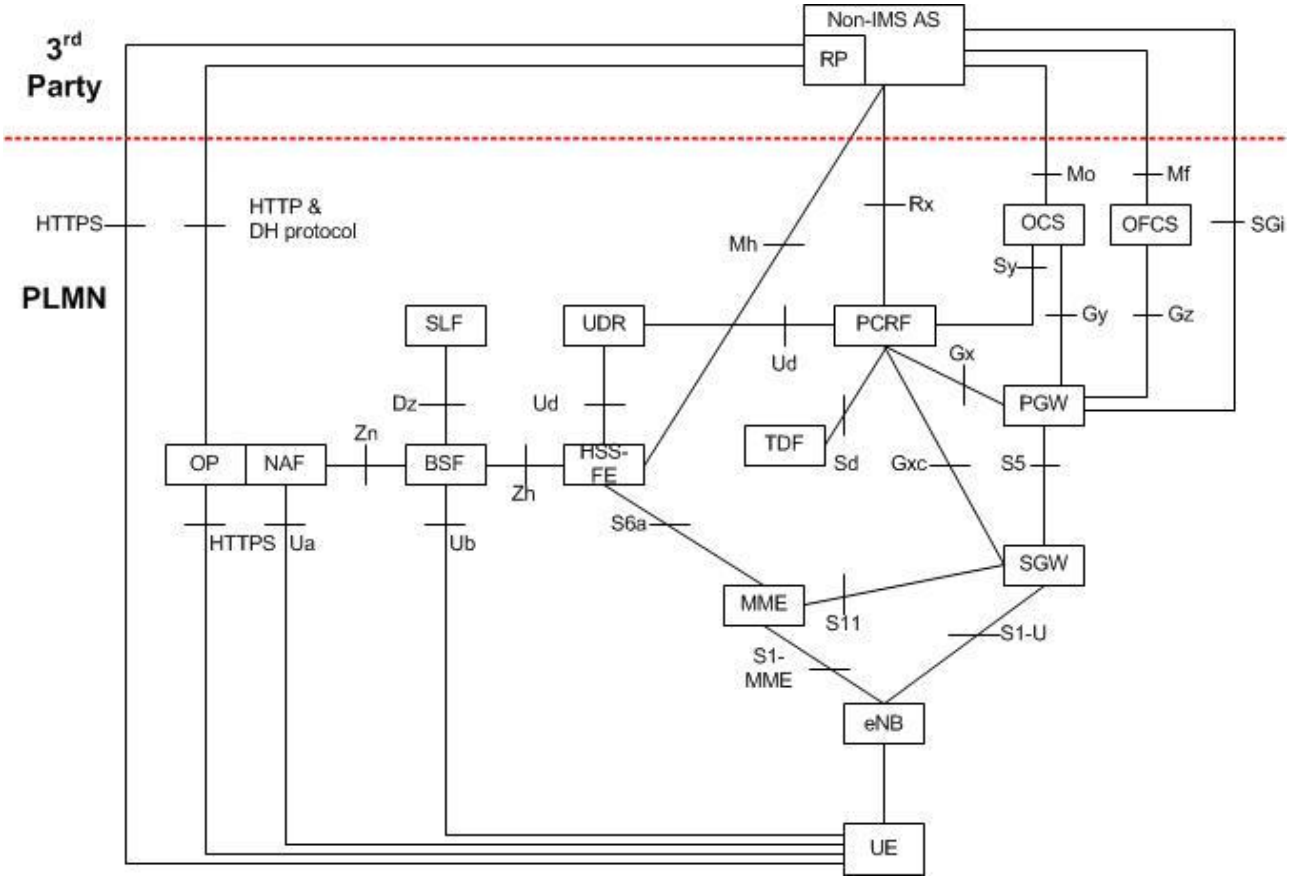

Figure 6.1.2-2: Non-Roaming Architecture - non-IMS AS owned by 3rd party Application Provider

Figure 6.1.2-2 shows the non-roaming architecture where the non-IMS AS is owned by 3rd party data application provider (DAP). Collaboration between the mobile operator and the DAP can be based on one or more of the following aspects: authentication, charging, data storage, and policies. The appropriate procedures will be used based on the collaborative aspects.

The following aspects are different than the scenario where non-IMS AS is owned by the MNO:

- Mo and Mf are interfaces between the 3rd party owned non-IMS AS and the operator owned OCS/OFCS. These could be based on Ro and Rf as agreed by MNO and 3rd party DAP. They could also be based on specifications of other SDO (e.g. oneAPI).

- All interfaces exposed to 3rd party DAP will need to have security aspects specified.

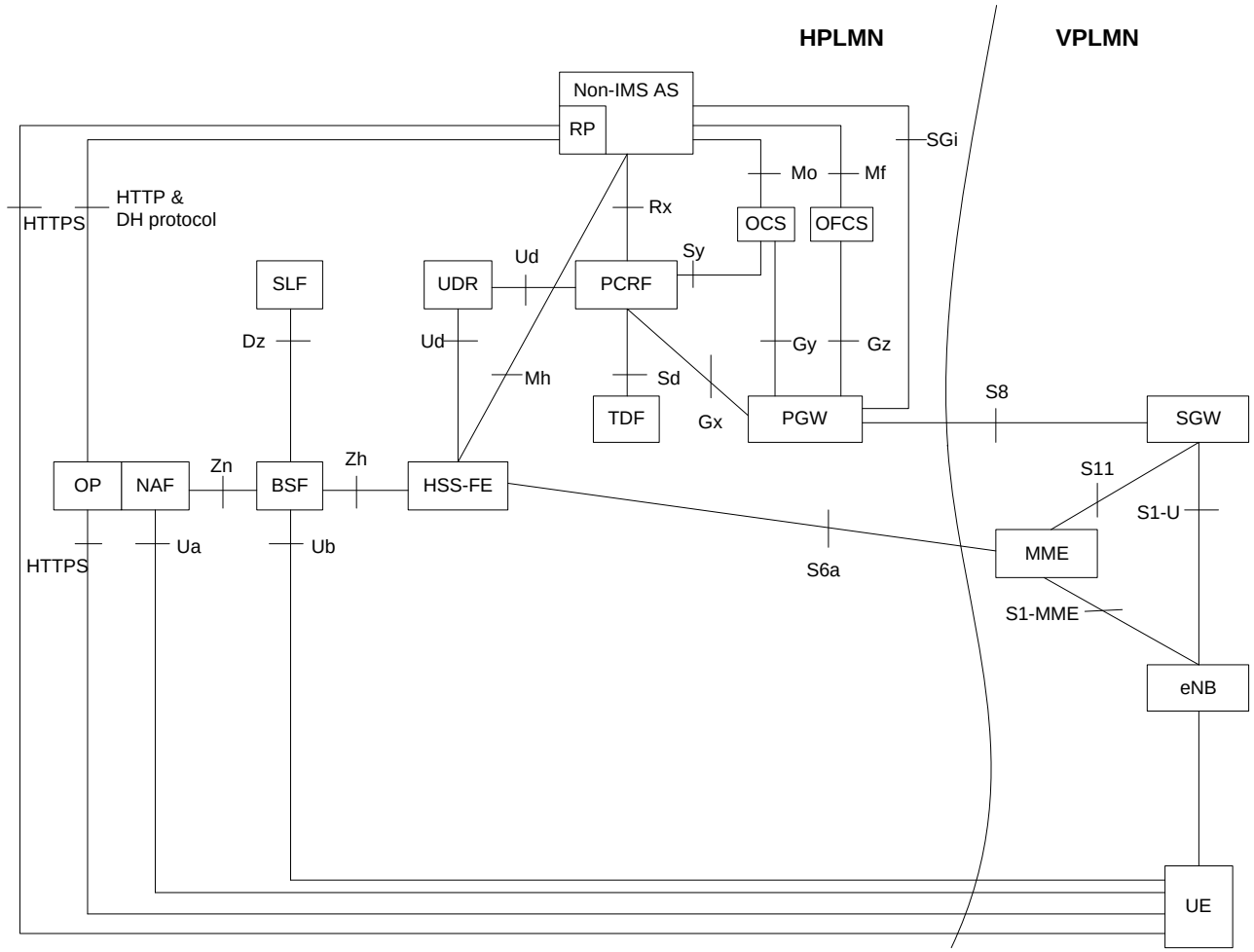

Figure 6.1.2-3: Home-Routed Roaming Architecture - non-IMS AS owned by HPLMN

Figure 6.1.2-3 shows the home routed roaming architecture where the HPLMN owns the non-IMS AS.

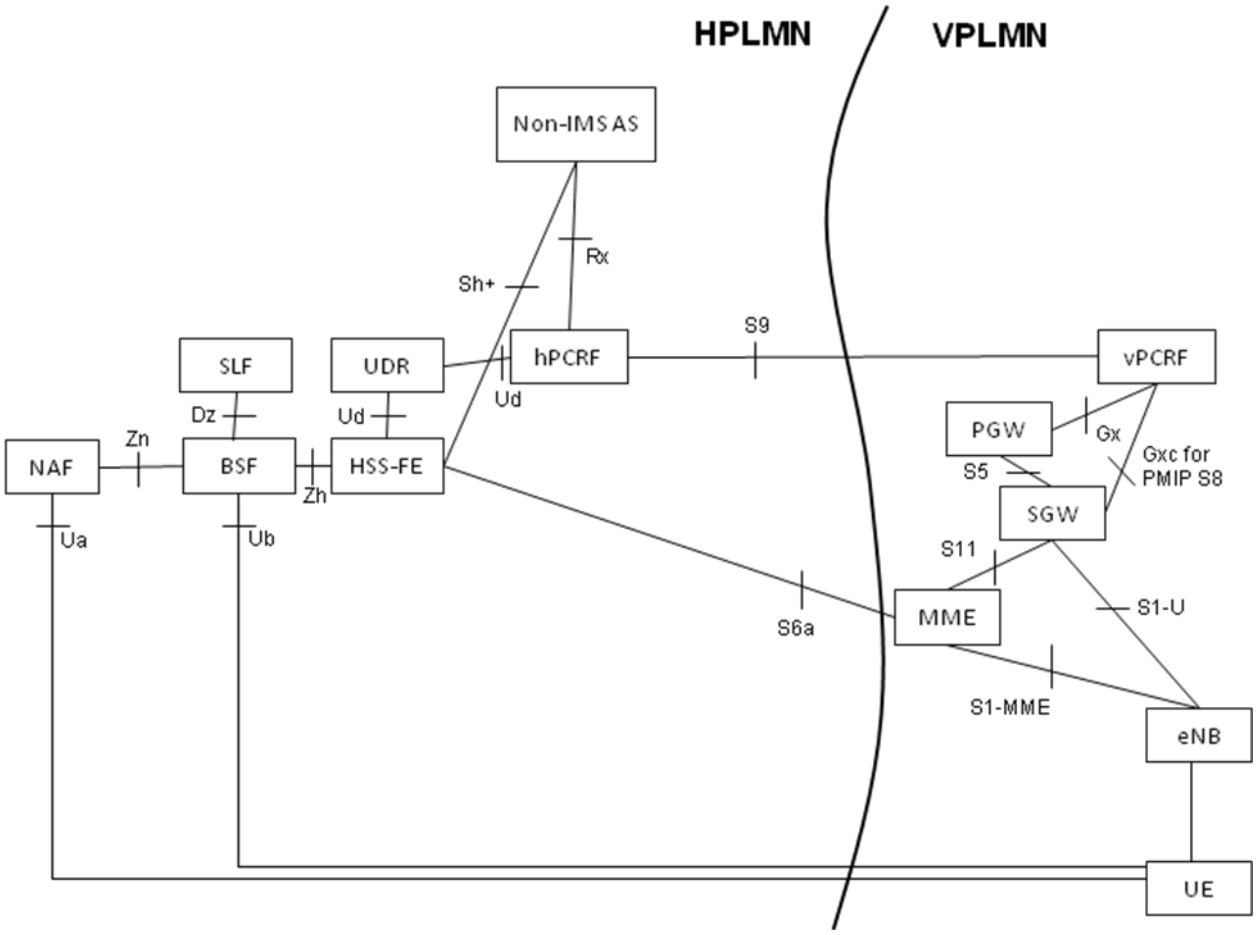

Figure 6.1.2-4: Local Breakout Roaming Architecture

Editor's Note: Charging aspect for LBO case is FFS.

Editor's Note: Architecture for LBO case is FFS.

6.1.3 Interface Enhancements

6.1.4 Impacts on existing nodes or functionality

6.1.5 Non-IMS Procedures for Non-roaming Cases

The procedures defined in this clause are applicable to the non-roaming cases where the non-IMS AS is owned by either a mobile operator or a 3rd party Data Application Provider.

6.1.5.1 Authentication Procedures

As per clause 6.1.1, GBA and interworking between GBA and OpenID is used as a basis for security framework.

For the case of non-IMS AS owned by 3rd party Data Application Provider, authentication for the user subscribing to an application service is terminated at HSS-FE in the mobile operator network. Following is the requirement addressing this case, which is specified in TS 22.278, clause 5.3.

- For scenario#2, the Evolved Packet System shall enable 3rd party data applications to rely on security derived from the security provided by the operator.

For the case of non-IMS AS owned by mobile operator, authentication is always terminated at HSS-FE in the mobile operator network.

6.1.5.1.1 Non-IMS Successful Authentication Procedure

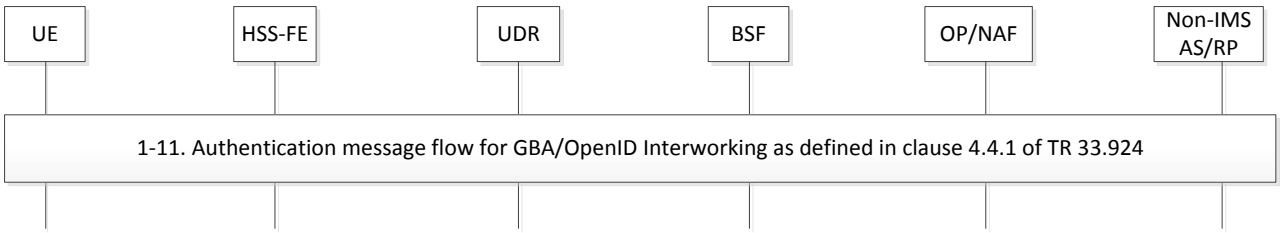

Figure 6.1.5.1.1-1: Non-IMS Successful Authentication Procedure

Figure 6.1.5.1.1-1 shows the non-IMS successful authentication procedure.

1-11. These steps are as defined in TR 33.924 [5], clause 4.4.1.

6.1.5.1.2 Non-IMS Re-authentication Procedure

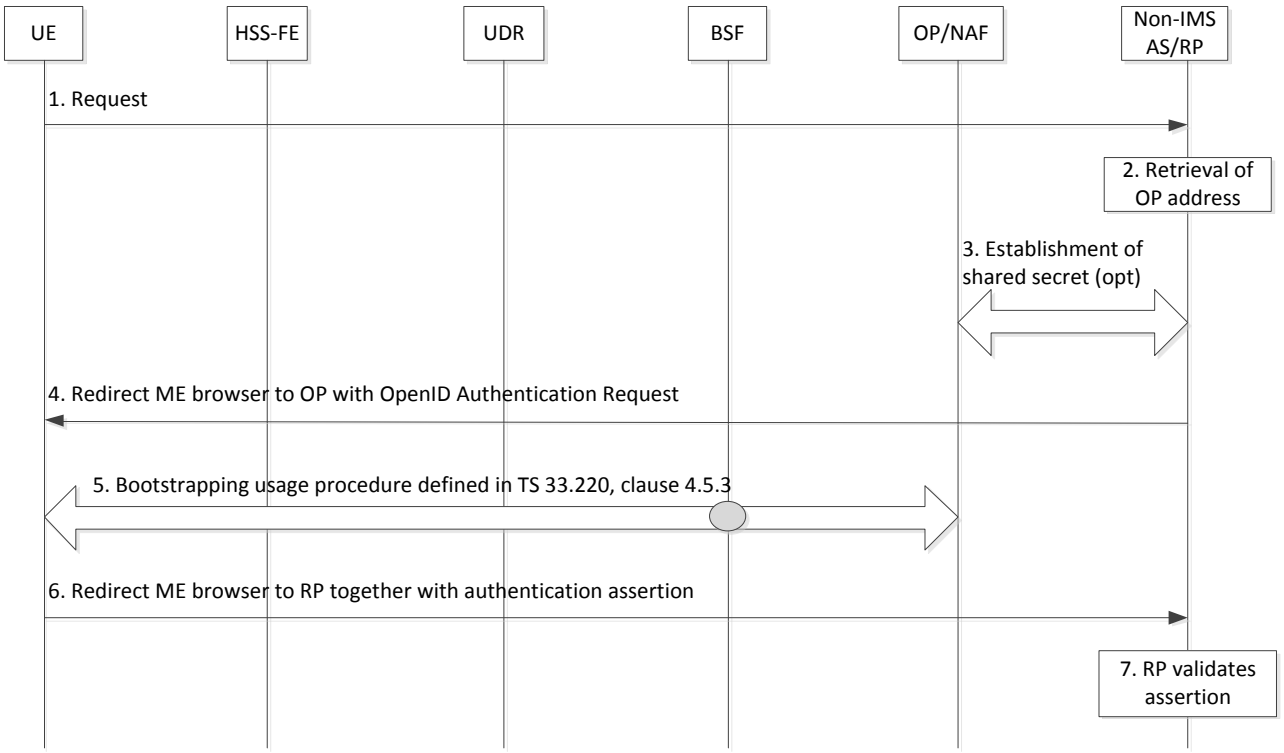

Figure 6.1.5.1.2-1: Non-IMS Re-authentication Procedure

Figure 6.1.5.1.2-1 shows the non-IMS re-authentication procedure.

1. UE sends a request for a service (e.g. HTTP Request, etc.) to the non-IMS AS/RP. Based on local policies, the non-IMS AS decides to re-authenticate the UE. The authentication information generated based on the security context established during the initial authentication is included in this message.
2. This step is as defined in step 2 of clause 4.4.1 in TR 33.924 [5].
3. This step is as defined in step 3 of clause 4.4.1 in TR 33.924 [5].
4. This step is as defined in step 4 of clause 4.4.1 in TR 33.924 [5].
5. The bootstrapping usage procedure is as defined in TS 33.220 [3], clause 4.5.3.

6. This step is as defined in step 10 of clause 4.4.1 in TR 33.924 [5].

7. This step is as defined in step 11 of clause 4.4.1 in TR 33.924 [5].

6.1.5.2 Charging Procedures

The following is the requirement for charging specified in TS 22.278, clause 5.3.

- The Evolved Packet System shall support online and offline charging models (e.g., user pays, application provider pays, etc.) for all scenarios.

To accommodate the requirement above, both online and offline charging procedures need to be supported, which are described in the following clauses.

Authentication and authorization associated with charging interfaces to 3rd party DAP are based on the business agreement between MNO and DAP and out of Release 12 MOSAP scope.

6.1.5.2.1 Non-IMS AS Assisted Offline Charging Scenarios

Offline charging for both events and sessions between non-IMS AS and OFCS is performed using the Mf interface. Two basic scenarios are supported for offline charging:

(1) Event based offline charging;

(2) Session based offline charging.

NOTE: The non-IMS AS and OFCS used in this clause are mapped to CTF and CDF used in TS 32.299 [11], clause 5.1 respectively.

6.1.5.2.1.1 Event Based Offline Charging Procedure

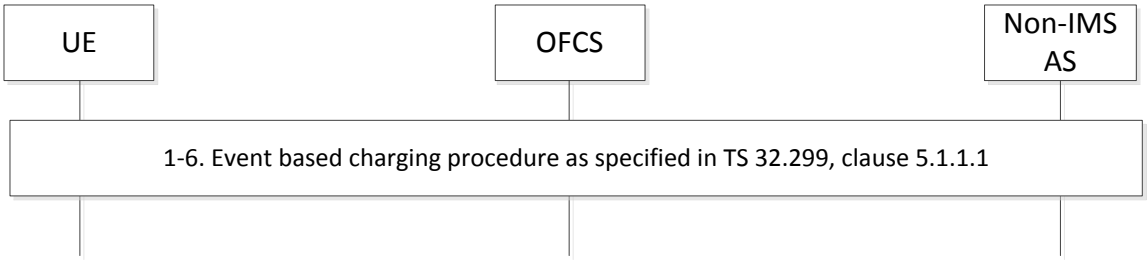

Figure 6.1.5.2.1.1-1 Event Based Offline Charging Procedure

Figure 6.1.5.2.1.1-1 describes the event based offline charging procedure assisted by the non-IMS AS.

1-6. These steps are as specified in TS 32.299 [11], clause 5.1.1.1.

6.1.5.2.1.2 Session Based Offline Charging Procedure

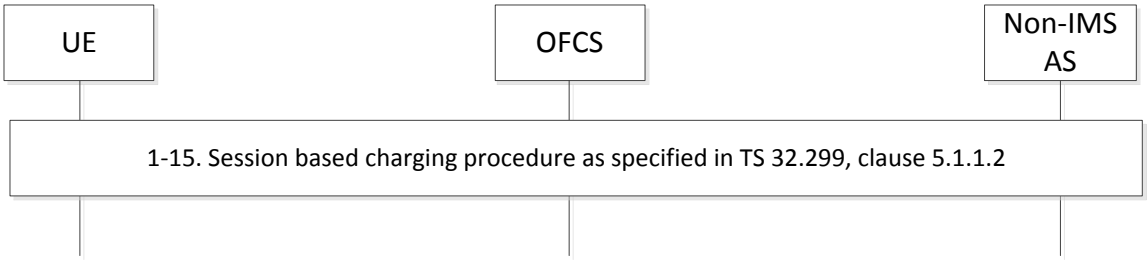

Figure 6.1.5.2.1.2-1 Session Based Offline Charging Procedure

Figure 6.1.5.2.1.2-1 describes the session based offline charging procedure assisted by the non-IMS AS.

1-15. These steps are as specified in TS 32.299 [11], clause 5.1.1.2.

6.1.5.2.2 Non-IMS AS Assisted Online Charging Scenarios

Online charging for both events and sessions between MNO owned non-IMS AS and OCS is performed using the Mo interface.

Three basic scenarios are supported for online charging:

(1) Immediate Event Charging;

(2) Event charging with Reservation;

(3) Session charging with Reservation.

For each aforementioned basic scenario, the specific cases will be studied by SA5.

NOTE: Online charging aspects between third party owned non-IMS AS and OCS are based on operator agreements.

6.1.5.3 Mh Interaction Related Procedures

As per clause 6.1.1, the UDC architecture is used as a basis for user data management. To accommodate the message interaction between HSS-FE and UDR specified in TS 23.335 [6], clauses 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8, following related message interaction over Mh interface needs to be addressed accordingly.

(1) Querying data procedure;

(2) Creating data procedure;

(3) Deleting data procedure;

(4) Updating data procedure;

(5) Subscription to Notifications procedure;

(6) Notification for data modification procedure.

6.1.5.3.1 Querying Data Procedure

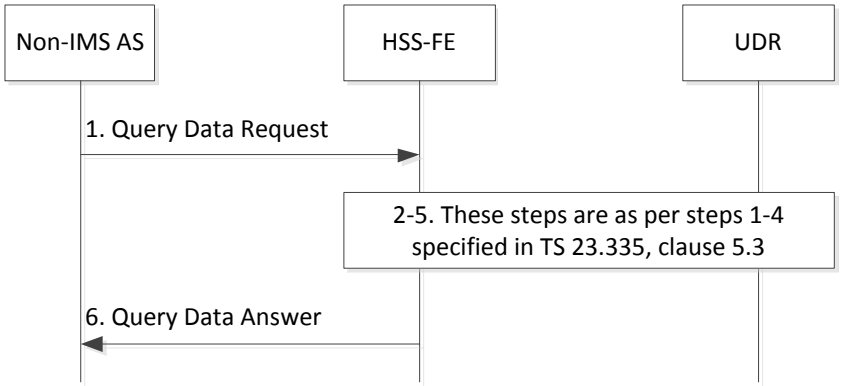

Figure 6.1.5.3.1-1: Querying Data Procedure

Figure 6.1.5.3.1-1 shows the querying data procedure.

1. The non-IMS AS sends a Query Data Request message via Mh to the HSS-FE.

   The message shall contain:

   - the user identity;
   - the identification of the user data to be queried.

NOTE: User data identification and structure comply with the HSS-FE's data view.

2-5. These steps are as per steps 1-4 specified in TS 23.335 [6], clause 5.3.

6. The HSS-FE responds to the non-IMS AS with a Query Data Answer message via Mh.

The non-IMS AS then continues processing its logic.

The message shall contain:

- the requested user data.

6.1.5.3.2 Creating Data Procedure

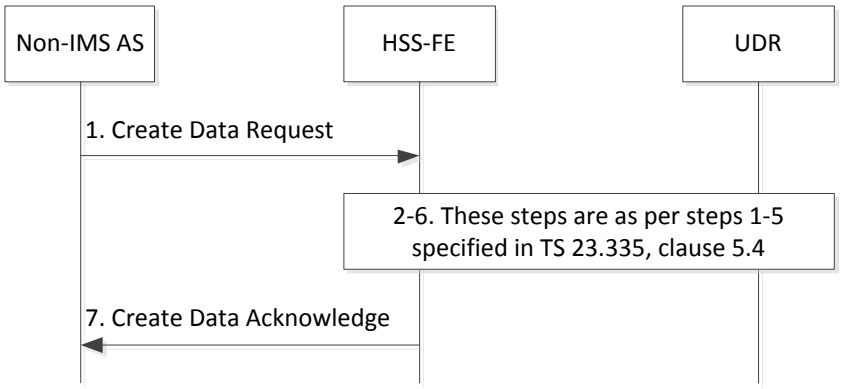

Figure 6.1.5.3.2-1: Creating Data Procedure

Figure 6.1.5.3.2-1 shows the creating data procedure.

1. The non-IMS AS sends a Create Data Request message via Mh to the HSS-FE.

   The message shall contain:

   - the user identity;
   - the new user data.

2-6. These steps are as per steps 1-5 specified in TS 23.335 [6], clause 5.4.

7. The HSS-FE responds to the non-IMS AS with a Create Data Acknowledge message via Mh. The non-IMS AS then continues processing its logic.

   The message shall contain:

   - the identification of the user data created.

6.1.5.3.3 Deleting Data Procedure

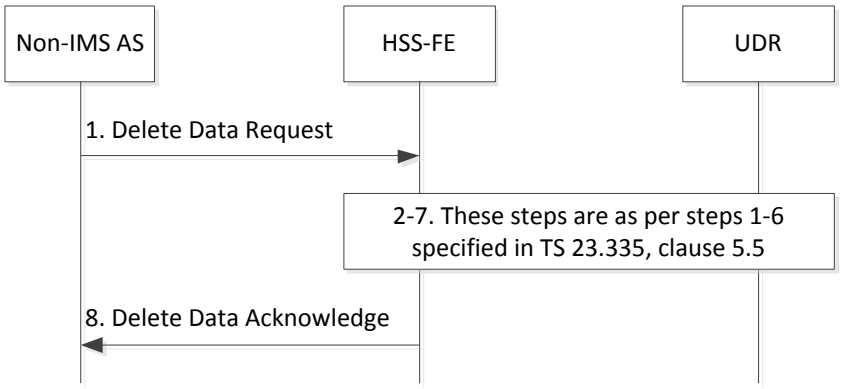

Figure 6.1.5.3.3-1: Deleting Data Procedure

Figure 6.1.5.3.3-1 shows the deleting data procedure.

1. The non-IMS AS sends a Delete Data Request message via Mh to the HSS-FE.

   The message shall contain:

   - the user identity;
   - the identification of the user data to be deleted.

   The message may contain:

   - The deletion condition, if supported by HSS-FE.

2-7. These steps are as per steps 1-6 specified in TS 23.335 [6], clause 5.5.

8. The HSS-FE responds to the non-IMS AS with a Delete Data Acknowledge message via Mh. The non-IMS AS then continues processing its logic.

6.1.5.3.4 Updating Data Procedure

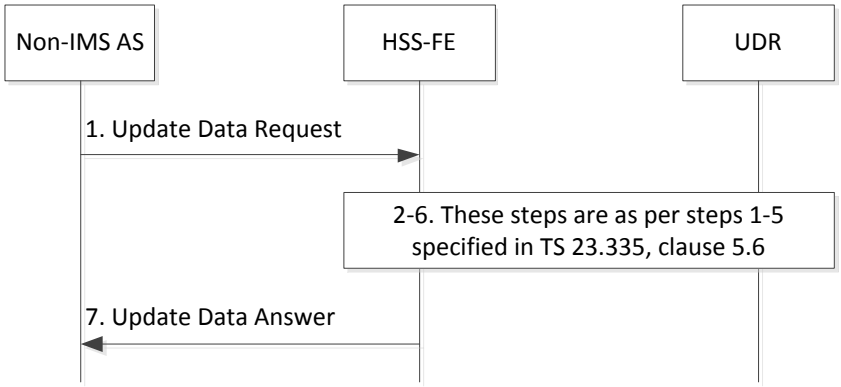

Figure 6.1.5.3.4-1: Updating Data Procedure

Figure 6.1.5.3.4-1 shows the updating data procedure.

1. The non-IMS AS sends a Update Data Request message via Mh to the HSS-FE.

   The message shall contain:

   - the user identity;
   - the identification of the user data to be updated;
   - the new data value to be written.

   The message may contain:

   - The deletion condition, if supported by HSS-FE.

2-6. These steps are as per steps 1-5 specified in TS 23.335 [6], clause 5.6.

7. The HSS-FE responds to the non-IMS AS with a Update Data Answer message via Mh. The non-IMS AS then continues processing its logic.

6.1.5.3.5 Subscription to Notifications Procedure

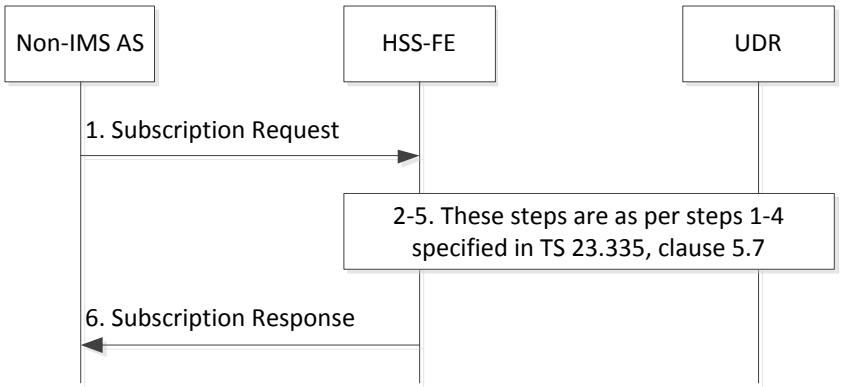

Figure 6.1.5.3.5-1: Subscription to Notifications Procedure

Figure 6.1.5.3.5-1 shows the subscription to notifications procedure.

1. The non-IMS AS sends a Subscription Request message via Mh to the HSS-FE.

   The message may contain:

   - the user identity;
   - subscription type which indicates whether this request is to subscribe or unsubscribe;
   - subscription to notification information (Identification of the requested user data, the notification condition(s), the expiry time indicating the point in time when the subscription to notification expires, the identity of the non-IMS AS).

2-5. These steps are as per steps 1-4 specified in TS 23.335 [6], clause 5.7.

6. The HSS-FE responds to the non-IMS AS with a Subscription Response message via Mh. The non-IMS AS then continues processing its logic.

6.1.5.3.6 Notification for Data Modification Procedure

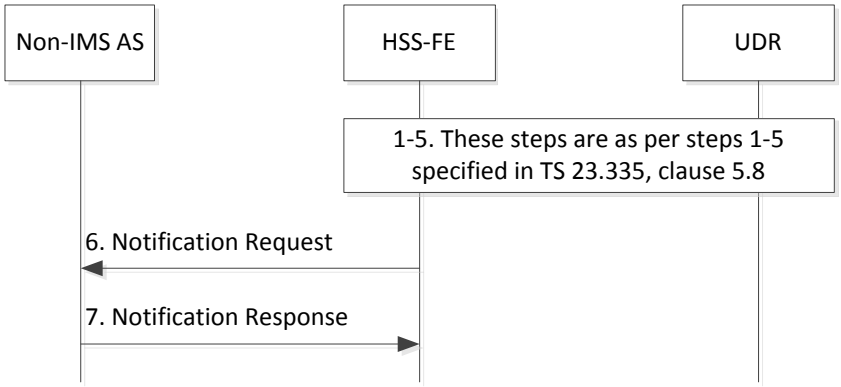

Figure 6.1.5.3.6-1: Notification for Data Modification Procedure

Figure 6.1.5.3.6-1 shows the notification for data modification procedure.

1-5. These steps are as per steps 1-5 specified in TS 23.335 [6], clause 5.8.

6. The HSS-FE sends a Subscription Response message to the non-IMS AS via Mh. This step can happen just after step 4. The non-IMS AS shall perform the relevant application logic.

7. The non-IMS AS responds to the HSS-FE with a Subscription Request message via Mh. The HSS-FE shall perform the relevant logic.

6.1.5.4 Non-IMS AS Discovery Procedure

The Non-IMS AS discovery may be performed using one of the following mechanisms:

- The UE may be configured to know the fully qualified domain name (FQDN) or the IP address of the non-IMS AS for the UE.

- The non-IMS AS discovery may be performed after the IP connectivity has been established. DHCP mechanism can be used to provide the IP address of a non-IMS AS, or alternatively, the FQDN of a non-IMS AS and the IP address of a DNS server which can resolve the FQDN of the non-IMS AS. DNS resolution is used to obtain the IP address of the non-IMS AS. This mechanism is described in clause 6.1.5.4.1

6.1.5.4.1 Non-IMS AS Discovery Procedure based on DHCP/DNS

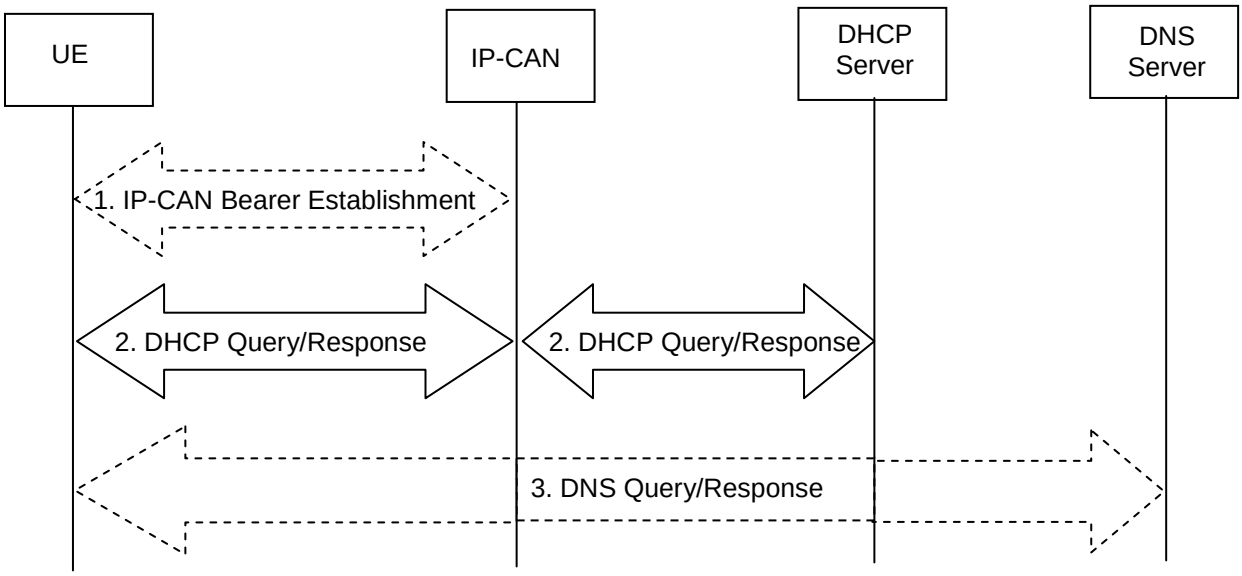

Figure 6.1.5.4.1-1 Non-IMS AS Discovery Procedure based on DHCP/DNS

1. An IP-CAN Bearer is established if not available.

2. The UE interacts with a DHCP server to request the domain name and/or IP address of the non-IMS AS and IP address of DNS server. This step may require multiple DHCP Query/Response message exchanges to retrieve the requested information. DHCP Relay within IP-CAN may be used between UE and DHCP server.

3. The UE performs a DNS Query/Response interaction with DNS server to retrieve the non-IMS AS IP address with including the FQDN of the non-IMS AS in the DNS Query message. This step is not needed if the IP address of the non-IMS AS has been obtained in step 2.

6.1.5.5 Policy Control Interaction Procedures Triggered by Non-IMS Application

6.1.5.5.1 Procedures for MNO Owned and 3rd Party Owned Non-IMS AS Cases

The following requirement is specified in TS 22.278, clause 5.3.

- The Evolved Packet System shall support policy control interactions between a mobile operator and data applications for all scenarios triggered by application layer signalling or by user plane traffic.

To accommodate the above requirement, when there is a request for a new service requiring QoS guarantee, policy control interaction procedures are as per clause 7.4 of TS 23.203 [8]. Note: The PCRF is assumed to have the knowledge about what QoS is to be authorized for the specific application.

6.1.6 Non-IMS Procedures for Home-routed Roaming Case

6.1.6.1 Authentication Procedures

Refer to clause 6.1.5.1.

6.1.6.2 Charging Procedures

Refer to clause 6.1.5.2.

6.1.6.3 Mh Interaction Related Procedures

Refer to clause 6.1.5.3.

6.1.6.4 Non-IMS AS Discovery Procedure

Refer to clause 6.1.5.4.

6.1.6.5 Policy Control Interaction Procedures Triggered by Non-IMS Application

Refer to clause 6.1.5.5.1.

6.1.7 Evaluation

6.2 Architecture #2

Editor's Note: This clause will contain functional description and interface enhancements for solution based on IMS

6.2.1 Functional Description

6.2.2 Interface Enhancements

6.2.3 Impacts on existing nodes or functionality

6.2.4 Evaluation

6.3 Other solutions and considerations

Editor's Note: This clause will contain the functional description and interface enhancements for other solutions not covered above.

7 Conclusion

Editor's Note: This clause will provide conclusions with respect to what further specification work is required in order to provide interworking between mobile operators and data application providers.

7.1 Interim Conclusions for Release 12 Specification Work

This clause contains the agreed conclusions:

a) For MNO-owned non-IMS AS, Mh interface can reuse the existing Sh and Ud interfaces for transparent user data.

b) For MNO-owned non-IMS AS, Mo and Mf interfaces will be based on the existing Ro and Rf interfaces.

c) The procedure provided in this TR will be used for re-authentication procedure for GAA/GBA and OpenID interworking.

d) The existing Rx interface will be used by non-IMS AS for all non-roaming cases and home-routed roaming case.

Annex A:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2011-07	SA2 #86				Version 0.0.0, Editor's Initial Draft, (S2-113687)		0.0.1
2011-07	SA2 #86				S2-113690, S2-113691, S2-113692, S2-113771	0.0.1	0.1.0
2012-05	SA2 #91				Inclusion of documents approved in SA2 #91. S2-122494, S2-122585. Editorial corrections.	0.1.0	0.2.0
2012-07	SA2 #92				Inclusion of documents approved in SA2 #92. S2-122824, S2-123137, S2-123138, S2-123139, S2-123140, S2-123141, S2-123143. Editorial changes on coversheet, reference number and clause number in clause 6.1.	0.2.0	0.3.0
2012-10	SA2 #93				Inclusion of papers approved at SA2 #93: S2-124100, S2-123957, S2-123958, S2-123960, S2-123961, S2-123714, S2-124101, S2-124102. Editorial changes on coversheet, clause numbers in clause 6.1.5, 6.1.6, 6.1.7.	0.3.0	0.4.0
2012-11	SP-56	SP-120729	-	-	MCC editorial update to version 1.0.0 for presentation to TSG SA for Information	0.4.0	1.0.0