

Function Specification Layered LTE EPC

Ericsson Dynamic Activation 1

FUNCTION SPECIFICATION

Copyright

© Ericsson AB 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Purpose and Scope	1
1.2	Target Group	1
1.3	Typographic Conventions	1
2	General	2
2.1	Dynamic Activation - EPS Provisioning	2
2.2	DLA HSS Overview	2
2.3	LTE/SAE Support in HSS	3
3	Overview	4
3.1	Data Model HSS	5
3.2	Data Model Management	6
3.3	Atomicity and Integrity Handling	6
3.4	Support CUDB Backup	7
3.5	Hosted Validation	7
3.6	Notification	8
3.7	HSS Provisioning Flow	9
4	Provisioning of AVG and EPS	10
4.1	Provisioning AVG Activation Interface	10
4.2	Provisioning EPS Activation Interface	12
4.2.1	Flexible Profiles - Configured Profile versus Individual Profile	13
4.2.2	Multiple Administration Area Support for EPS	14
4.2.3	Location Procedure	15
4.2.4	Auto Provisioning	15
4.2.5	Dedicated Core Network	16
4.3	IMSI Changeover	16
5	Enforcement of Subscriber Licensing	17
	Reference List	19





1 Introduction

This section is an introduction to this document. It contains information about the prerequisites, purpose, scope, and target group for the document. This section also contains explanations of typographic conventions used in this document.

1.1 Purpose and Scope

This document gives, from an Ericsson™ Dynamic Activation (EDA) perspective, a brief introduction to provisioning of EPS and AVG application data in the Data Layered Architecture (DLA) HSS.

1.2 Target Group

The target group for this document is as follows:

- Network Administrator
- System Administrator
- Application Administrator
- Network Supervision Administrator
- Application Designer
- Marketing
- Other

For information about the different target groups, see *Library Overview*, Reference [1]

1.3 Typographic Conventions

Typographic conventions are described in *Library Overview*, Reference [1].

2 General

This section contains general information about the EPS application data provisioning in DLA HSS.

2.1 Dynamic Activation - EPS Provisioning

The value of Dynamic Activation, is to simplify the activation flow, by providing one interface upstream towards BSS for provisioning of various numbers of network nodes downstream, see Figure 1.

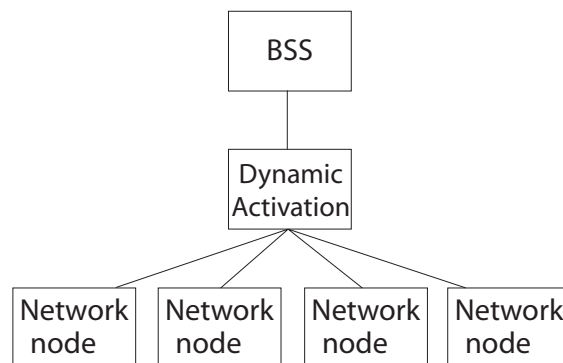


Figure 1 Dynamic Activation Provisioning Overview

2.2 DLA HSS Overview

DLA is an architecture that allows separation of application logic and data storage into different nodes. The HSS node is, in a DLA deployment, configured as Front End (FE). The FE contains the application logic and connection to an external Back End Database (BEDB). The BEDB contains the application user data storage (subscriber data) and is accessible from the HSS-FE. In the Ericsson DLA architecture the Centralized User Database (CUDB) is used as BEDB. CUDB provides a common centralized database for multiple application data.

The Dynamic Activation system is in charge of provisioning the CUDB.

The difference between an HSS-FE deployment and a classic HSS deployment is shown in Figure 2. For generic HSS-FE provisioning, see Section 3 on page 4.

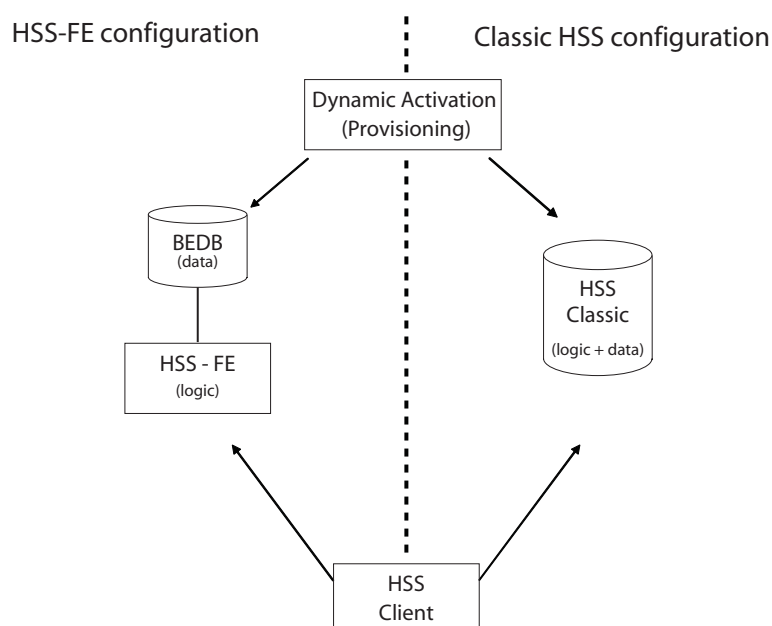


Figure 2 HSS-FE Configuration versus Classic HSS Configuration.

2.3 LTE/SAE Support in HSS

Long Term Evolution (LTE) is a new radio access platform allowing operators to achieve higher data speeds. Evolve the core network to support LTE. This has been specified by 3rd Generation Partnership Project (3GPP) in the (System Architecture Evolution (SAE) technical study for the Evolved Packet Core (EPC). The complete packet system consisting of the LTE and the SAE/EPC is called the Evolved Packet System (EPS).

The EPC is part of the core network and contains nodes such as Mobility Management Entity (MME) and SAE Gateway. These nodes controls the LTE access, routing of data packets and connectivity to external data networks, see Figure 3.

The HSS provides support to the EPC network for controlling the LTE/SAE traffic. The data is provided from the HSS EPC Subscription Management (ESM) module and the Authentication Vector Generator (AVG) function.

The ESM module provides support for subscription handling, authorization, mobility management and more, to the EPC. The AVG function provides authentication support for EPC access.

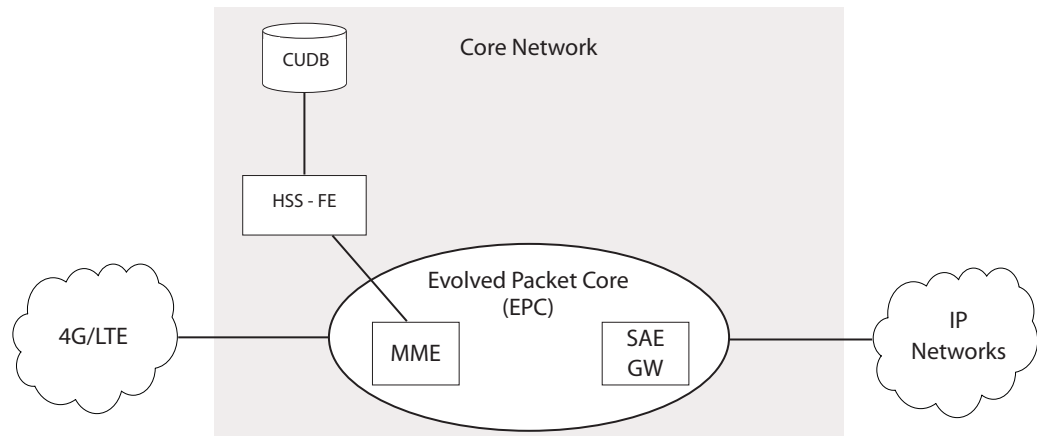


Figure 3 HSS Support the EPC with AVG and EPS Data

3 Overview

This chapter gives an introduction to the generic HSS provisioning. For provisioning of EPS and AVG data, see Section 4 on page 10.

The Ericsson solution for the HSS provisioning in DLA architecture is shown in Figure 4. Dynamic Activation exposes a CAI3G (Customer Administration Interface 3G) interface consumed by BSS (Business Support System) or any other provisioning system for management of subscribers. Dynamic Activation uses the LDAP (Lightweight Directory Access Protocol) interface towards CUDB for provisioning of subscriber data, and SOAP (Simple Object Access Protocol) towards HSS-FE for notification about changes made to a subscriber.

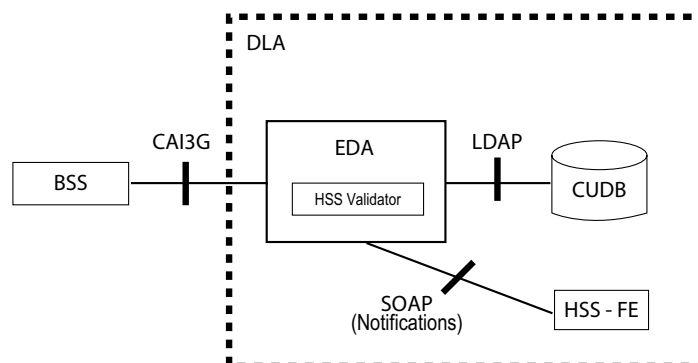


Figure 4 Ericsson Provisioning Solution in HSS

CUDB is the network entity in a layered architecture domain, serving as central storage point for subscriber data, in this context AVG and EPS data.



CUDB is built as an LDAP directory server, containing the needed entries and attributes according to the defined schema for the different services.

HSS-FE needs to inform the network nodes about changes in the subscriber data. This procedure is initiated by Dynamic Activation through the provisioning notification interface through SOAP.

Hosted in Dynamic Activation is an HSS-FE validator software which provides provisioning constraints required for subscriber data consistency.

Some data can be accessed at the same time in different network procedures. A collision detection function is provided to avoid data inconsistency in the external database.

Dedicated features in Dynamic Activation make sure that the provisioned data is of correct type, and that all mandatory parameters are present in the provisioning Customer Service Order (CSO).

3.1 Data Model HSS

The general view of the provisioning data model used in HSS is shown in Figure 5. For more information, see Reference [2].

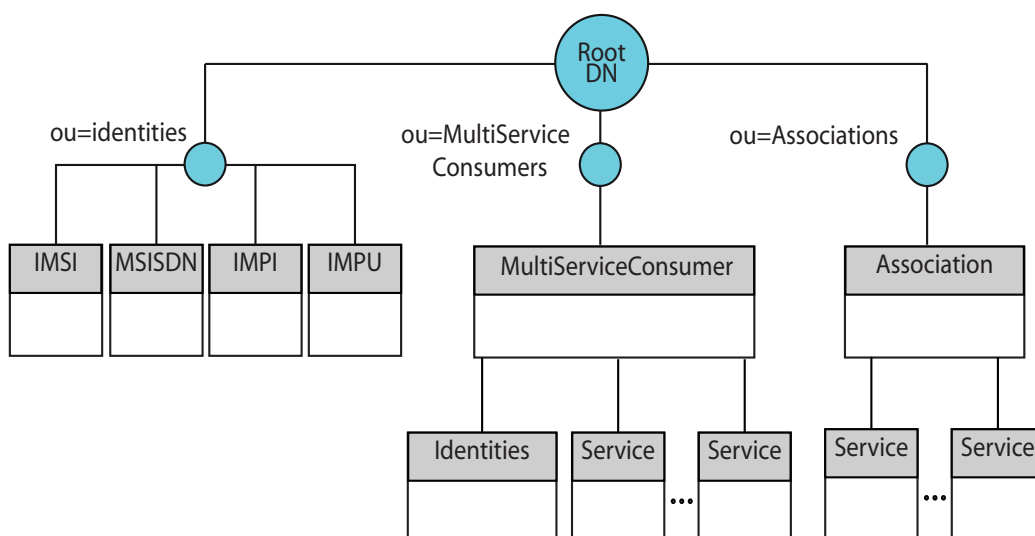


Figure 5 Provisioning Data Model HSS

- The Identities object contains all the identities related to the MultiSC. The different identities are used to identify and access MultiSC or association.
- The Association object contains information to associate several MultiSCs.
- MultiServiceConsumer (MultiSC) represents the entity which consumes one or more telecommunication services. The services it can contain below itself are the IP Multimedia Subsystem (IMS); Authentication Authorization

Accounting (AAA), Evolved Packet System (EPS), and Authentication (Auth).

- **MultiSC Identities:** A special entry in the MultiSC entry. This entry gathers all the shared identities used to identify the MultiSC for the different services. A mask per identity indicating for which services the identity has been defined.
- The Service object contains information related to the services consumed by the MultiSC. An instance of this object must be created for every service consumed by the MultiSC.

The HSS EPS data model corresponds to Identities and MultiSC objects. HSS IMS data model corresponds to Identities, MultiSC and Associations objects.

3.2 Data Model Management

Dynamic Activation is responsible to:

- Map the CAI3G order to the LDAP objects in the data model for a subscriber. There are attributes that have a different format in the CAI3G interface and in the LDAP schema.
- Check and add default values to attributes that are required (mandatory) in CUDB but optional in CAI3G.
- Handle identities and alias under root identities entry, generate identity for MultiSC (IMSI, MSISDN, and MultiSC ID) and validate their relations for a given subscriber.
- Create the service object AAA each time a MultiSC is created in the CUDB. The AAA object (and optional objects below AAA) is removed each time a MultiSC is deleted. AAA specific data is added below AAA object and an IP address alias is added by applications during traffic. The IP address is not managed by Dynamic Activation.

3.3 Atomicity and Integrity Handling

Atomicity means ensuring that any operations performed on the system are either all completed successfully or all reversed successfully to keep the data consistency.

One CAI3G CSO can imply several LDAP orders towards the CUDB. Dynamic Activation will provide atomicity in HSS EPS provisioning as below:

- Parses and validates the whole CSO before any LDAP order is sent towards the CUDB to minimize the LDAP errors received from the CUDB. For more information about data validation, see Section 3.5 on page 7.



- Retry the LDAP order when some LDAP errors are returned from CUDB, for example Function Busy and CDC Collision. The number of retries is configurable. For more information about retry setting, see *User Guide for Resource Activation*, Reference [7].
- Support fault tolerance and rollback when LDAP errors are returned from CUDB and retry failed. For more information about fault tolerance and rollback on EPS operations, see *Function Specification Resource Activation*, Reference [10].

If rollback is still failed, the atomicity is not achieved; the CUDB integrity is not assured. Dynamic Activation raises an alarm and sends back error information about inconsistent data in the CUDB.

For more information about HSS EPS alarm, see *Event and Alarm Handling*, Reference [11].

For more information about rollback failed error, see *Layered EPS Provisioning over CAI3G*, Reference [6]. In case of data inconsistency, manual action is needed.

For more information about HSS EPS actions, see *Function Specification Resource Activation*, Reference [10].

Note: Simultaneously Create, Set and Delete the same subscriber can result in inconsistent data in the CUDB, reserve sufficient time duration, with consideration to retry behavior, between the different operations.

3.4 Support CUDB Backup

When performing a backup of the CUDB, Dynamic Activation is notified to block provisioning towards it. The purpose is to ensure consistency in the CUDB during backup.

The blocking and unblocking can either be triggered from the CUDB or manually. Manually by setting the `BlockForCudbBackup` attribute to `true`, or `false` by use of a JMX client. When the backup is finished, the CUDB sets the `BlockForCudbBackup` attribute to `false`. This to allow all provisioning towards CUDB again. For more information about `BlockForCudbBackup` settings, see *Configuration Manual for Resource Activation*, Reference [12].

If a command is executing when `BlockForCudbBackup` receives the value `true`, the command is not stopped. Commands received after the `true` flag is set are rejected with an error response message. Resend the commands after CUDB backup is finished.

3.5 Hosted Validation

HSS-FE validator plug-in, hosted in Dynamic Activation, is responsible to check the constraint for the service-specific objects, that is AVG, EPS and more. The

data is not written to CUDB unless it is validated. Validation is done for `Create` and `Set CSOs`. `Get` and `Delete CSOs` are not validated.

HSS-FE validator plug-in is populated with data from Dynamic Activation and the input data for performing the validation is:

- Data to be changed for a given MultiSC (received from CAI3G).
- The current MultiSC data (read from the CUDB).
- The operations to be performed.

As a general rule, the HSS-FE validator plug-in is populated with `MultiSC`, `MultiSC Identities`, and `subscriber data`.

If validation of the populated data is successful, the HSS validator plug-in sends the result back to the HSS logic, which in turn initiates the LDAP orders towards the CUDB.

In case, the populated data does not pass the validation, the provisioning flow is interrupted with a CAI3G error respond `CONSTRAINT VIOLATION` sent back to BSS. HSS-FE validator plug-in has no logs, traces, or alarms, when there is something wrong the exception is put in a Dynamic Activation log (PAS log).

3.6 Notification

After a successful execution notification is used to inform the HSS-FE about changes made to a MultiSC. For example, changed or deleted. The HSS-FE generates a network update to the traffic nodes where the user is registered or located. The notification between Dynamic Activation and HSS-FE is performed in an asynchronous way. This means that the CSO response to BSS can be sent before the network update is performed by the HSS-FE.

Dynamic Activation maintains a list of provisioning events that triggers a notification request to the HSS-FE. The list is fetched from an HSS-FE Service Notification Configuration File. The list contains the LDAP objects or attributes or both and conditions that must be fulfilled to send the notification message.

If the HSS-FE is down, Dynamic Activation stops sending notifications and events.

Dynamic Activation can handle one or more notification files in parallel, for example one for IMS and one for EPS.

The file consists of three parts, modification logic, extra logic and sends logic.

- **Modification logic** - The modification logic part allows configuration of object classes and attributes that is included in the notification message when a MultiSC is changed or deleted. For changed data both old and new values are included, and for deleted data old values are included.



- **Additional logic (optional)** - The additional logic part allows configuration of data that is in the notification in addition to those that are configured in the modification logic. Typical data that is configured in this part is subscriber identities and addresses to network entities that needs to be informed about changes of the subscriber profile in the CUDB. The additional logic operates on the status (old values) of the MultiSC.
- **Send logic** - The send logic part allows configuration of conditions that trigger the sending of the notification message. The send logic operates on the status (old values) of the MultiSC.

Some data is stored as binary content in the CUDB. To simplify the transference of this data in HTTP, Dynamic Activation allows that `base64` encoding is used for some of the contents in the notification. There is an XML attribute to indicate that such data is formatted as binary.

Dynamic Activation detects if a notification configuration file has been updated and activates it automatically. For details, see *System Administrators Guide for Native Deployment*, Reference [3].

For more information about HSS-FE notification, see Reference [4].

3.7 HSS Provisioning Flow

A simplified and general flow for an HSS provisioning CSO sent on the CAI3G interface is shown in Figure 6.

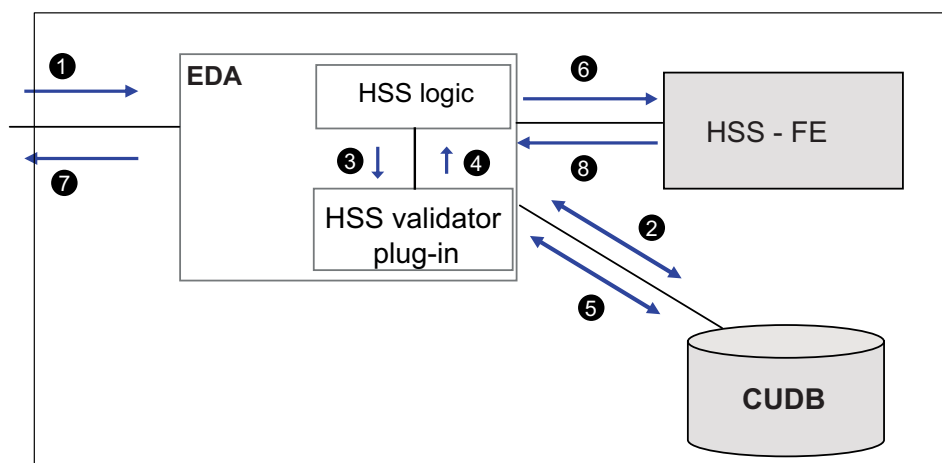


Figure 6 The General HSS-FE Provisioning Flow

1. A provisioning CAI3G request is received and its syntax validated.
2. A check if any data exists in the CUDB for the given MultiSC is performed by Dynamic Activation, if found, the data is fetched from CUDB. Dynamic Activation checks shared alias and a mask per alias, indicating already defined services for a specific MultiSC.

3. Dynamic Activation merges received data from CAI3G with fetched data from CUDB and send it to the HSS-FE validator plug-in.
4. The HSS validator plug-in validates subscriber data and sends the result back to the HSS logic.

Note: Step 3 and step 4 are only performed for `Create` and `Set` CSOs.

5. Dynamic Activation merges CAI3G data with CUDB data and possible mutation data from the HSS-FE validator plug-in. `Add`, `Delete`, or `Modify` operations are performed towards CUDB for the merged data.
6. A notification of changed data is sent to HSS-FE.
7. A CAI3G response is sent back to the originating system.
8. A notification response is received from the HSS-FE. Since the communication is asynchronous, the response can appear before the CAI3G response in step 7.

4 Provisioning of AVG and EPS

The EPS and AVG application data in the HSS-FE are provisioned by the Dynamic Activation system.

4.1 Provisioning AVG Activation Interface

This interface handles the `Create`, `Set`, `Get`, and `Delete` CSOs of AVG data.

The AVG Service requires an `IMSI` or `IMPI` as identifier to be provisioned in the system. The `IMSI` is needed if the same `mscId` is to be used for EPS and AVG.

The following CSOs are supported through the CAI3G interface:

- `Create AVGMultiSC`
- `Set AVGMultiSC`
- `Delete AVGMultiSC`
- `Get AVGMultiSC`

The Figure 7 shows the AVG data model.

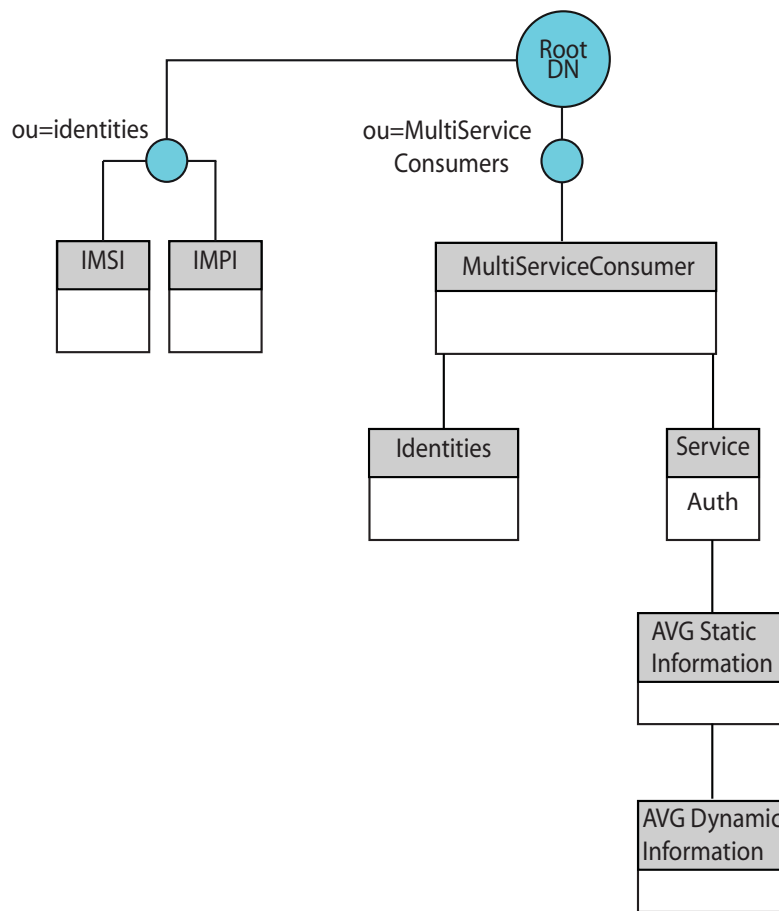


Figure 7 AVG Data Model

For a **Create** AVG CSO the LDAP objects are created in the following order in the CUDB:

1. Identifier alias object (IMSI or IMPI)
2. MultiSC object
3. Service object (AAA)
4. Identities object
5. Service object (Auth)
6. AVG Static information object
7. AVG Dynamic information object

For a **Delete** CSO the LDAP objects are deleted in the opposite order.

For information about the AVG interface, refer to *Layered AVG Provisioning over CA/3G*, Reference [5].

4.2 Provisioning EPS Activation Interface

This interface handles the `Create`, `Set`, `Get`, and `Delete` CSOs of EPS data.

The EPS Service requires an IMSI as identifier to be provisioned in the system.

The following CSOs are supported through the CAI3G interface:

- `Create EPSPMultiSC`
- `Set EPSPMultiSC`
- `Delete EPSPMultiSC`
- `Get EPSPMultiSC`

The Figure 8 shows the data model for EPS.

Note: Association is not supported.

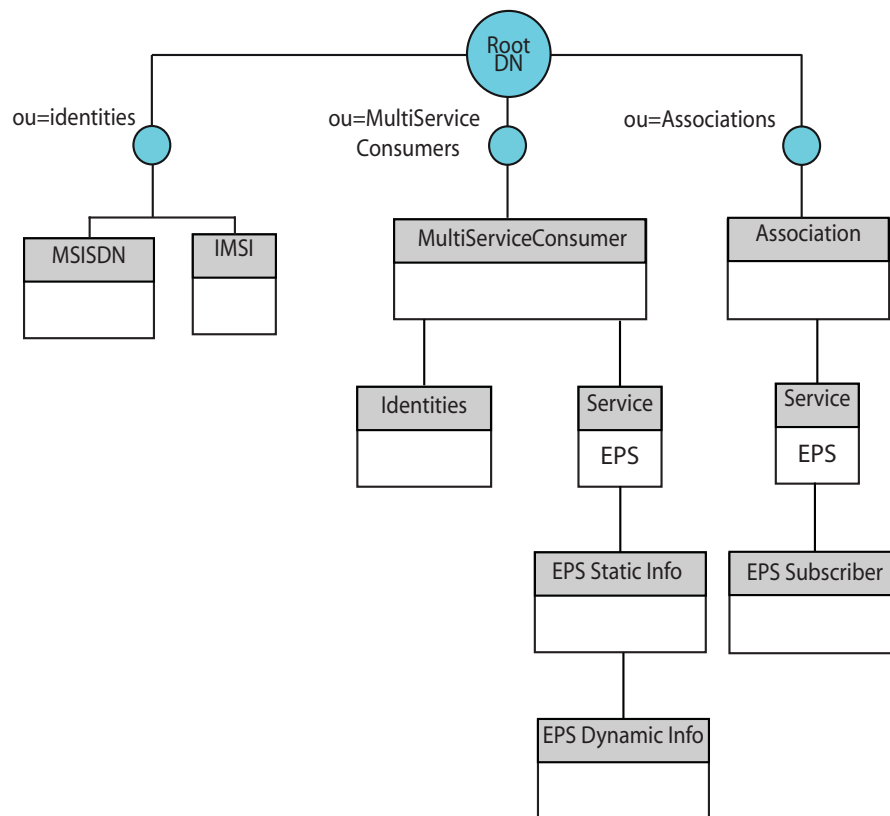


Figure 8 EPS Data Model

For a `Create` CSO the LDAP objects are created in the following order in CUDb:

1. Identifier alias object (IMSI)



2. MultiSC object
3. Service object (AAA)
4. Identities object
5. Identifier alias object (MSISDN)
6. Service object (EPS)
7. EPS Static information object
8. EPS Dynamic information object

For a `Delete` CSO the LDAP objects are deleted in the opposite order.

For information about the EPS interface, refer to *Layered EPS Provisioning over CAI3G*, Reference [6].

4.2.1 Flexible Profiles - Configured Profile versus Individual Profile

There are two different profiles used in EPS with the same set of attributes. The first is the configured profile that is stored in HSS-FE. The second is the individual profile (if it exists) that is stored among the data in EPS static information object in CUDB.

The configured profile is used as a package with settings. Every MultiSC must have a reference to one configured profile `EsmProfileId`. The same attributes included in the configured profile can however be set on individual basis, which is the profile referred to as the individual profile.

Figure 9 shows that where the two profiles are stored and how they correlate.

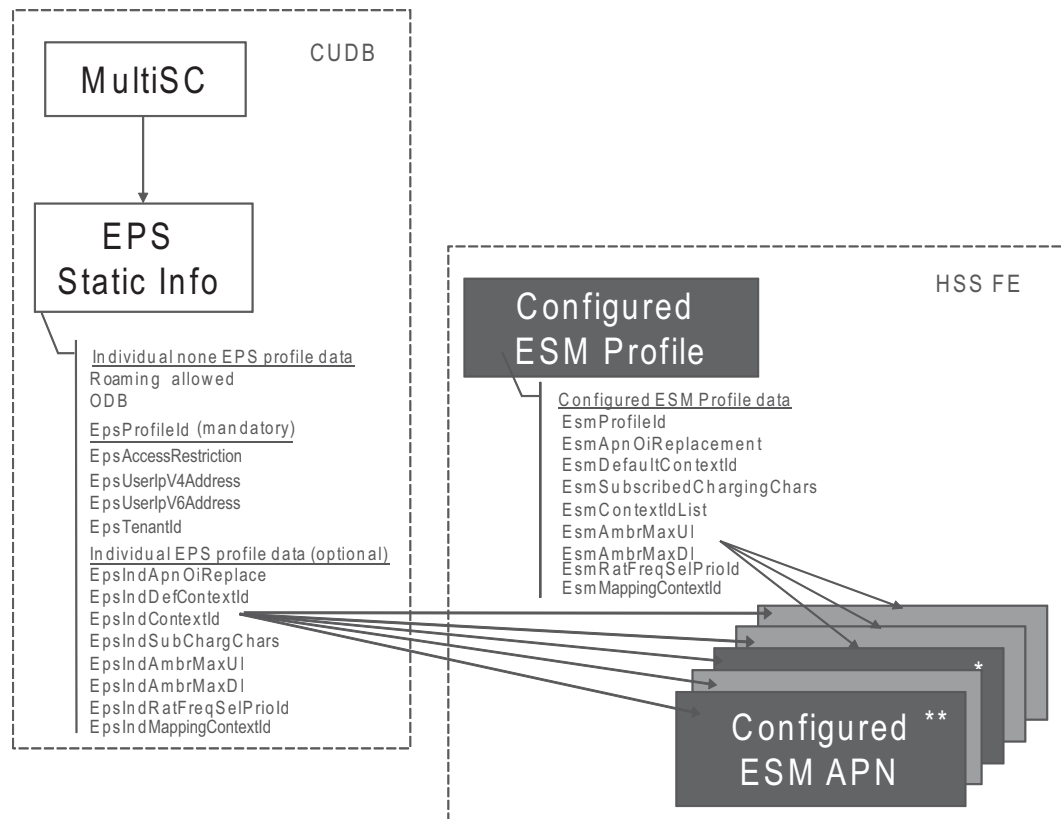


Figure 9 Flexible Profile Overview

If the individual profile for a MultiSC holds a value, that value overrides the corresponding value of the attribute in the configured profile. Hence the individual value only affects that specific MultiSC.

4.2.2 Multiple Administration Area Support for EPS

Multiple administration area support virtualizes the physical HSS resources for an operator. Any organization impact when HSS evolves from monolithic architecture to User Data Consolidation (UDC) is eliminated.

Multiple administration area support in Dynamic Activation provides the possibility to administer subscribers in different regions (Multi tenancy) separately.

An administration area is a region or a country where provisioning clients are able to perform subscriber and service data provisioning for their own subscribers only. Each administration area can be managed by one or several provisioning clients with the same or different provisioning privileges. For a specific provisioning client, provisioning privileges can be defined to allow management of subscribers in one or more administration areas.

The Access Control feature is used for defining the provisioning privileges IMSI ranges and regions (administration area identifier), that a specific provisioning



client is allowed to administer. Access restrictions can be defined on EPS CAI3G Get, Create, Set, Delete operations and also for provisioning EPS-related CLI commands.

Available functions are described in Section 4.2.2.1 on page 15.

For more information about Multiple Administration Area Support for EPS, see *User Guide for Resource Activation*, Reference [7].

4.2.2.1 Administration Area Identifier

When a subscriber is created, an Administration Area Identifier must be provisioned for the subscriber. This Administration Area Identifier is one of the attributes in the CAI3G operation for subscriber creation. The identifier is stored together with the rest of subscriber data in the CUDB.

HSS-FE uses the Administration Area Identifier to support different traffic cases (roaming/non-roaming to VPLMs).

The Access Control feature can be used to ensure that the provisioning client is allowed to administer the administration area identified by the Administration Area Identifier.

4.2.3 Location Procedure

The location procedure gathers the subscriber statistics from CUDB on per Mobility Management Entity (MME) and realm of the MME. It is possible to schedule single or recurrent location procedure.

The result statistics are stored, and can be retrieved via CLI.

For more information about Location Procedure, see *Scheduled Procedures for Layered Applications*, Reference [8]

4.2.4 Auto Provisioning

Auto provisioning is a provisioning scenario where EPS subscriber is created in CUDB by the HSS-FE when a user (USIM) has passed AKA authentication successfully, as illustrated in Figure 10.

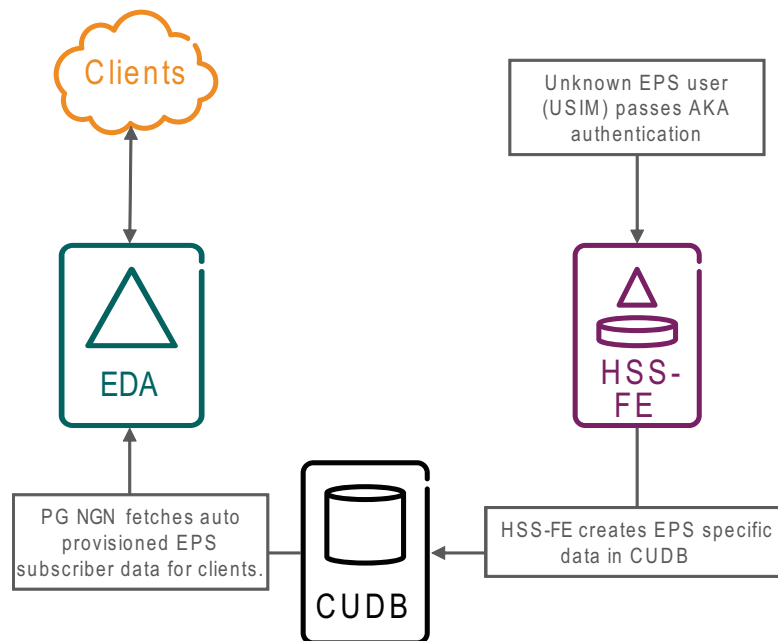


Figure 10 EPS Auto Provisioning Support

The auto provisioned EPS subscribers are marked with an auto provisioning indicator and a time stamp. In this scenario, Dynamic Activation is not involved in the subscriber creation process. However, Dynamic Activation is able to retrieve the auto provisioning indicator and the time stamp for such subscribers. Thus, the two attributes, `epsAutomaticProvisioned` and `epsLastUpdateLocationDate`, are only supported by Get operation.

4.2.5 Dedicated Core Network

The purpose with a Dedicated Core Network (DCN) is to provide specific characteristics and functions, or isolate specific User Equipments (UE)s or subscribers, for example M2M subscribers, subscribers belonging to a specific enterprise or separate administrative domain.

To specify the dedicated core network, an additional attribute is added to the EPS Individual profile, `epsIndividualUeUsageType`, to indicate the usage characteristics of the UE. If this attribute is not provisioned, a counterpart in the configured profile will be used.

This feature requires the additional Value Package EDA Shared Network.

4.3 IMSI Changeover

IMSI Changeover provides the Mobile operators and Mobile Subscribers (MS) means to replace SIM card in a flexible way. For instance when the card is lost, malfunctioning or periodically changed to prevent fraud or malfunctioning.



Dynamic Activation supports release of old IMSI, so that it becomes ready to be reused after IMSI changeover. A delayed IMSI Changeover can be reversed if the lost SIM-card has been found.

The available functions are:

- Immediate or delayed IMSI Changeover execution.
- Secure that IMSI Changeover is performed only on Subscribers (Multi Service Consumers) that has AUC, EPS, or HLR services.
- Removal of MSISDN and old IMSI relation in CUDB.

IMSI changeover is supported through the provisioning interfaces.

For more information, see *Function Specification Identity Changeover for Layered Applications*, Reference [9].

5 Enforcement of Subscriber Licensing

Several features are sold under capacity-based licenses. If the use of these features exceeds, the defined capacity levels the system reacts. If the subscriber capacity level is exceeded for a specified time, creation of new subscribers is disabled.

For more information regarding this feature, see *Function Specification Resource Activation*, Reference [10].





Reference List

Ericsson Documents

- [1] *Library Overview*, 18/1553-CSH 109 628 Uen
- [2] *Front End Provisioning Datamodel Description in HSS*, 3/155 19-2/CSH 150 0063/10 Uen
- [3] *System Administrators Guide for Native Deployment*, 1/1543-CSH 109 628 Uen
- [4] *HSS Notification Interface Description*, 11/155 19-2/CSH 150 0063/7 Uen
- [5] *Layered AVG Provisioning over CAI3G*, 10/155 19-CSH 109 628 Uen
- [6] *Layered EPS Provisioning over CAI3G*, 11/155 19-CSH 109 628 Uen
- [7] *User Guide for Resource Activation*, 1/1553-CSH 109 628 Uen
- [8] *Scheduled Procedures for Layered Applications*, 16/155 19-CSH 109 628 Uen
- [9] *Function Specification Identity Changeover for Layered Applications*, 14/155 17-CSH 109 628 Uen
- [10] *Function Specification Resource Activation*, 3/155 17-CSH 109 628 Uen
- [11] *Event and Alarm Handling*, 3/1553-CSH 109 628 Uen
- [12] *Configuration Manual for Resource Activation*, 2/1543-CSH 109 628 Uen