

Function Specification Layered IMS

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– IMS Provisioning	2
2.2	DLA HSS Overview	2
2.3	IMS Data Provisioning in HSS	3
3	Overview	4
3.1	Data Model HSS-FE IMS	5
3.1.1	Handling of Identities	7
3.2	Data Model Management	8
3.3	Atomicity and Integrity Handling	8
3.4	Support CUDB Backup	9
3.5	Hosted Validation	9
3.6	Notification	10
3.7	HSS-FE Provisioning Flow	11
4	Provisioning of AVG and IMS	12
4.1	Provisioning AVG Activation Interface	12
4.2	Provisioning IMS Activation Interface	14
4.2.1	Multiple Administration Area Support for IMS	17
5	Enforcement of Subscriber Licensing	18
	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 IP Multimedia Subsystem (IMS) and Authentication Vector Generation (AVG) application data in the Data Layered Architecture (DLA) Home Subscriber Server (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 IMS application data provisioning in DLA HSS.

2.1 Dynamic Activation– IMS Provisioning

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

In case one interface upstream is requested for the IMS solution involved nodes, it is possible by customization, for example by using Dynamic Activation Designer Studio.

A service can aggregate IMS, MTAS, IPWorks/ENUM service into one service for the northbound system.

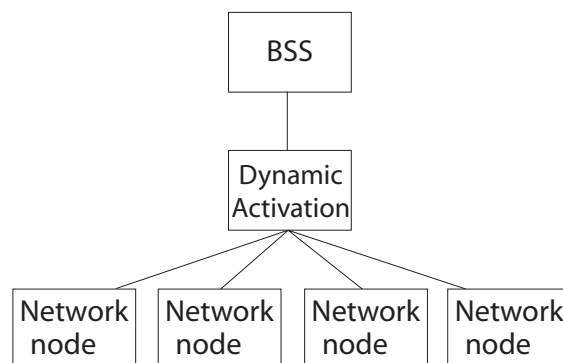


Figure 1 Dynamic Activation Provisioning Overview

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 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.

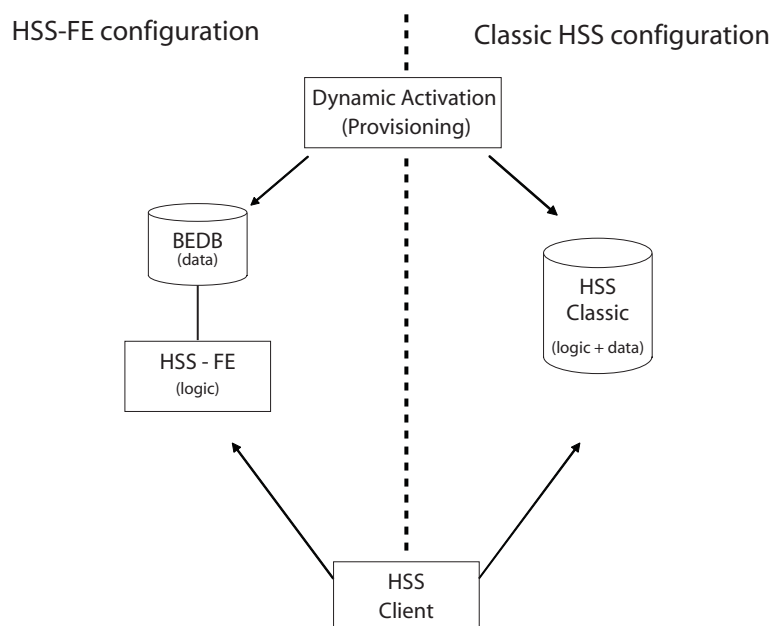


Figure 2 HSS-FE Configuration versus Classic HSS Configuration.

2.3 IMS Data Provisioning in HSS

The HSS-FE provides support to the IMS core domain for controlling the IMS traffic. The data is provided from the HSS-FE ISM (IMS Subscription Manager) module and the HSS-FE AVG (Authentication Vector Generator) function.

ISM and AVG provide data for user mobility management, session establishment procedures, authentication, user traffic protection, authorization support for IMS and more. The ISM and AVG data are used by the Call Session Control Function (CSCF) node and fetched from HSS-FE through the Cx interface. The IMS applications can fetch IMS HSS-FE data through the Sh interface. The data is provisioned to the CUDB by Dynamic Activation, see Figure 3.

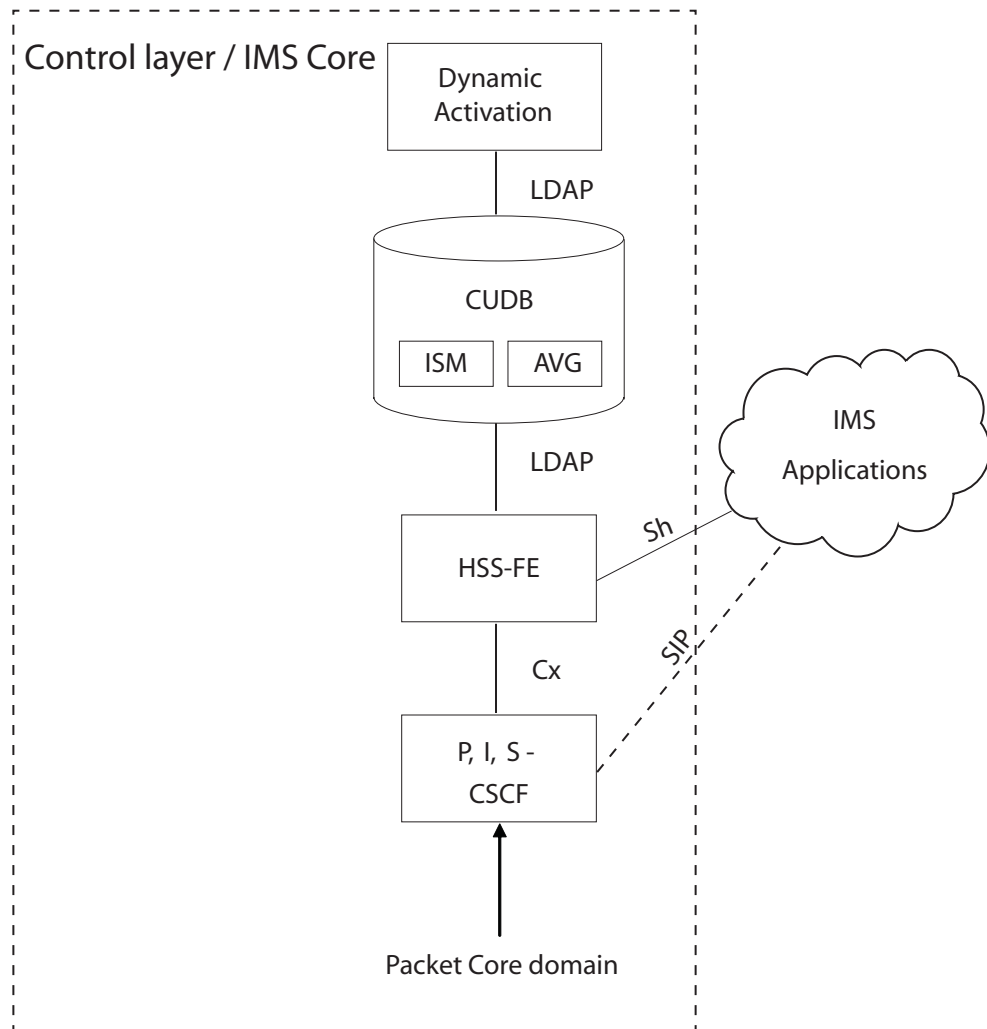


Figure 3 Simplified View of the HSS-FE IMS Core Support

3 Overview

This chapter gives an introduction to the generic HSS-FE provisioning. For provisioning of IMS and AVG data, see Section 3.7 on page 11.

The Ericsson solution for the HSS-FE provisioning in DLA architecture is shown in Figure 4. Dynamic Activation exposes a CAI3G (Customer Administration Interface 3G) interface consumed by BSS or any other provisioning system for management of subscribers. Dynamic Activation uses the LDAP (Lightweight Directory Access Protocol) interface towards CUDB, for storing subscriber data,



and SOAP (Simple Object Access Protocol) towards HSS-FE, for notification about changes made to a subscriber.

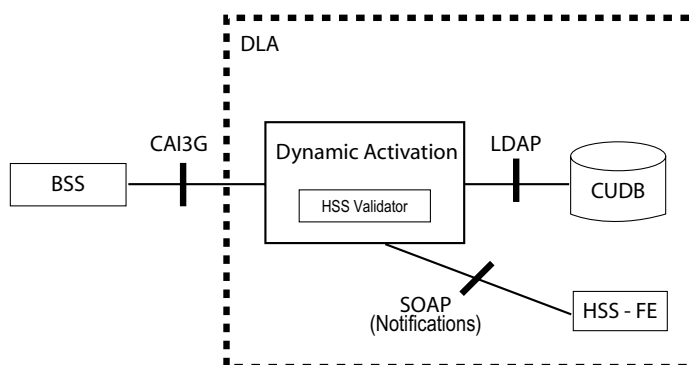


Figure 4 Ericsson Provisioning Solution in HSS-FE

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

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-FE IMS

The general view of the provisioning data model used in HSS is shown in Figure 5. For more information, refer to Reference [4].

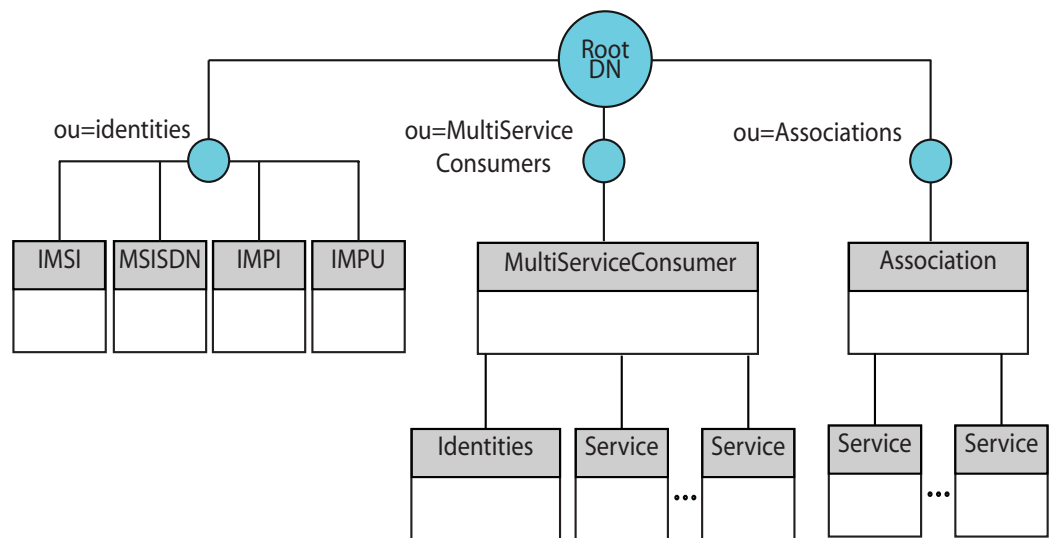


Figure 5 Provisioning Data Model UDC

For HSS the IMS data is stored under the following entries:

- The Association object contains information to associate several MultiSCs.

Note: When assigning an associationId, the recommendation is to NOT use any of the Identifiers as associationId. Use any random value or other value the customer has, except the identifier for any of the services (like IMSI, MSISDN, IMPI, IMPU) in the solution. This, since features like IMSI Changeover will only handle the service identities.

- The Identities object contains all the identities related to the MultiSC. The different identities are used to identify and access MultiSC or association. See Section 3.1.1 on page 6 for more information regarding the identities.
- MultiServiceConsumer (MultiSC) represents the entity which consumes one or more telecommunication services. Here is where all service data is connected. From HSS point of view it may contain service data for the IP Multimedia Subsystem (IMS); Authentication Authorization Accounting (AAA), Evolved Packet System (EPS), and Authentication (Auth).
- MultiSC Identities: A special entry under 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.



3.1.1 Handling of Identities

- International Mobile Subscriber Identity (IMSI): this entry can only be created, there is no explicit modification (IMSI changeover) or delete operation. To delete the IMSI, the corresponding `PrivateUserId` must be deleted.
- Mobile Subscriber ISDN Number (MSISDN): this entry can only be created, there is no explicit modification (MSISDN changeover) or delete operation. To delete the MSISDN, the corresponding `PrivateUserId` must be deleted.

There are two possibilities to assign MSISDN numbers to a `PrivateUserId`:

- Assign the number to an `msIsdn` attribute: this attribute is stored in `Identities` entry under a MultiSC. Just one MSISDN can be provisioned for a MultiSC involving several services. There is an MSISDN alias pointing to this MultiSC.
- Assign the number to an `ssoMsIsdn` attribute: a list of MSISDN numbers for Single Sign-On authentication. This data is stored under the IMPI object. Dynamic Activation does not make any cross-checking regarding this data. It has no relation to any alias or any identity for the current MultiSC or to other MultiSCs.
- IMS Private Identity (IMPI) (`PrivateUserId`): this entry can only be created and deleted, modification (IMPI changeover) is not supported.

A secondary IMPI, `secondPrivateUserId`, can be defined to support IMS Centralized Services (ICS). This entry can only be created and deleted, modification is not supported. When creating a secondary IMPI, the following rules apply:

- When IMPI is derived from an IMSI, derive the secondary IMPI from the same IMSI.
- When IMPI is not derived from an IMSI, and a `userImsi` is associated to it instead, derive the secondary IMPI from the same IMSI as the one included in the `userImsi` parameter.
- When the IMPI is not derived from an IMSI and no `userImsi` is associated with it, then, if the IMPI is already defined in CUDB and the secondary IMPI is derived from an IMSI already defined in CUDB for another service, the order is rejected. It will indicate that it is needed to delete the related privateUser (IMPI) from the IMS subscription first and then add both IMPI and secondary IMPI again.
- When secondary IMPI is not derived either from the same IMSI as primary derived IMPI, or the associated `userImsi` or not derived at all, the order is rejected.



- IMS Public Identity (IMPU) (`PublicUserId`): This entry can only be created and deleted, modification (IMPU changeover) is not supported.

Note: All identifier aliases used in provisioning orders must point to the same MultiSC, otherwise an error is returned. This enforces that subscribers with several services must be created in a certain order to guarantee that all services are stored under the same MultiSC. An IMSI must be provisioned if IMS service is provisioned for a subscriber that is defined in LTE, CSPS, AUC, or AVG.

3.2 Data Model Management

Dynamic Activation is responsible for the following:

- 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 (IMPU, IMPI, 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`), are removed each time a MultiSC is deleted. `AAA` specific data is added below `AAA` object and an IP address alias is added by services 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 IMS 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 9.
- 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 IMS operations, see *Function Specification Resource Activation*, Reference [8].

If rollback is still failed, the atomicity is not achieved; the CUDB integrity is not assured. Dynamic Activation will raise an alarm and sends back error information about inconsistent data in the CUDB. For more information about HSS IMS alarm, see *Event and Alarm Handling*, Reference [9].

For more information about rollback failed error, see *Layered IMS Provisioning over CAI3G*, Reference [10].

In case of data inconsistency, manual action is needed. For more information about HSS IMS actions, see *Function Specification Resource Activation*, Reference [8].

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 is done automatically, by CUDB sending information to Dynamic Activation and the attribute `BlockForCudbBackup` is set to `true` or `false`.

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.

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 IMS, AVG 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. Dynamic Activation reads the data from the CUDB and deletes all entries returned. This applies only for `Delete` CSO, if an entry is deleted by `Set` CSO, it is validated by the HSS-FE validation plug-in.

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

- 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 the CSO contains an `AssociationID`, the association branch and the other MultiSCs with the identities entry included in the same subscriber, must be provided to the HSS validator plug-in.

If validation of the populated data is successful, the HSS validator plug-in sends the result back to the internal Dynamic Activation 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, a notification is used to inform the HSS-FE about changes made to a MultiSC. For example, created, 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 that 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 EPS and one for IMS.

The file consists of the following parts:

- **Modification logic** - The modification logic part allows configuration of object classes and attributes that is included in the notification message when a MultiSC is created, changed, or deleted. For changed data both old and new values are included, for created data new values are included, and for deleted data old values are included.
- **Additional logic (optional)** - The additional logic part allows configuration of object classes and attributes that belong to the MultiSC and is included in the notification message, in addition to those that are configured in the modification logic. 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.

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 [5].

For more detailed information about HSS-FE notification, see Reference [6].

3.7 HSS-FE Provisioning Flow

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

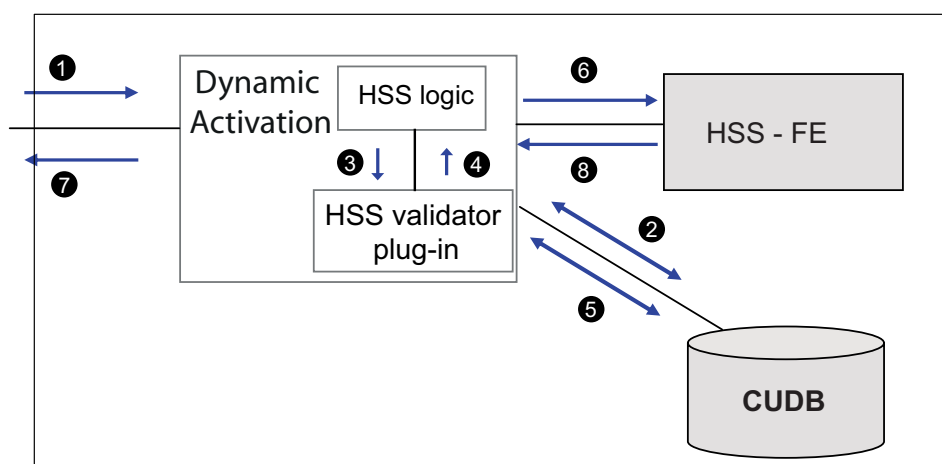


Figure 6 The General HSS-FE Provisioning Flow

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-FE validator plug-in validates subscriber data. Dynamic Activation fetches the result from the HSS-FE validator plug-in.
- 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 IMS

The AVG and IMS data in the HSS-FE are provisioned by Dynamic Activation.

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 two operations.

Communication failures during the provisioning process are in most cases resolved by resending the same command. When a `Create` command has failed, and the rollback also fails, it is not possible to resend the `Create` command without sending a corresponding `Delete` command first.

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` to be provisioned in the system.

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.

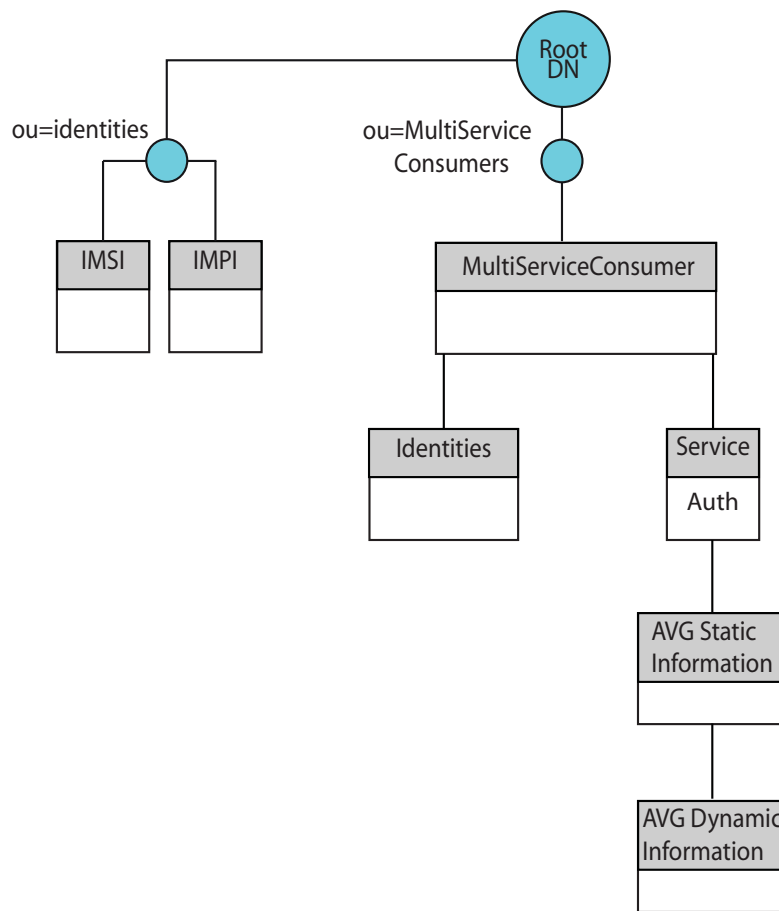


Figure 7 AVG Data Model

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

1. Identifier alias object (IMSI or IMPI)

Note: IMSI identifier to be used, if connecting several services under the same MultiSC object.

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 CAI3G*, Reference [2].

4.2 Provisioning IMS Activation Interface

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

The following CSOs are supported through the CAI3G interface:

- `Create IMSAssociation`
- `Set IMSAssociation`
- `Delete IMSAssociation`
- `Get IMSAssociation`

The Figure 8 shows the data model for IMS.

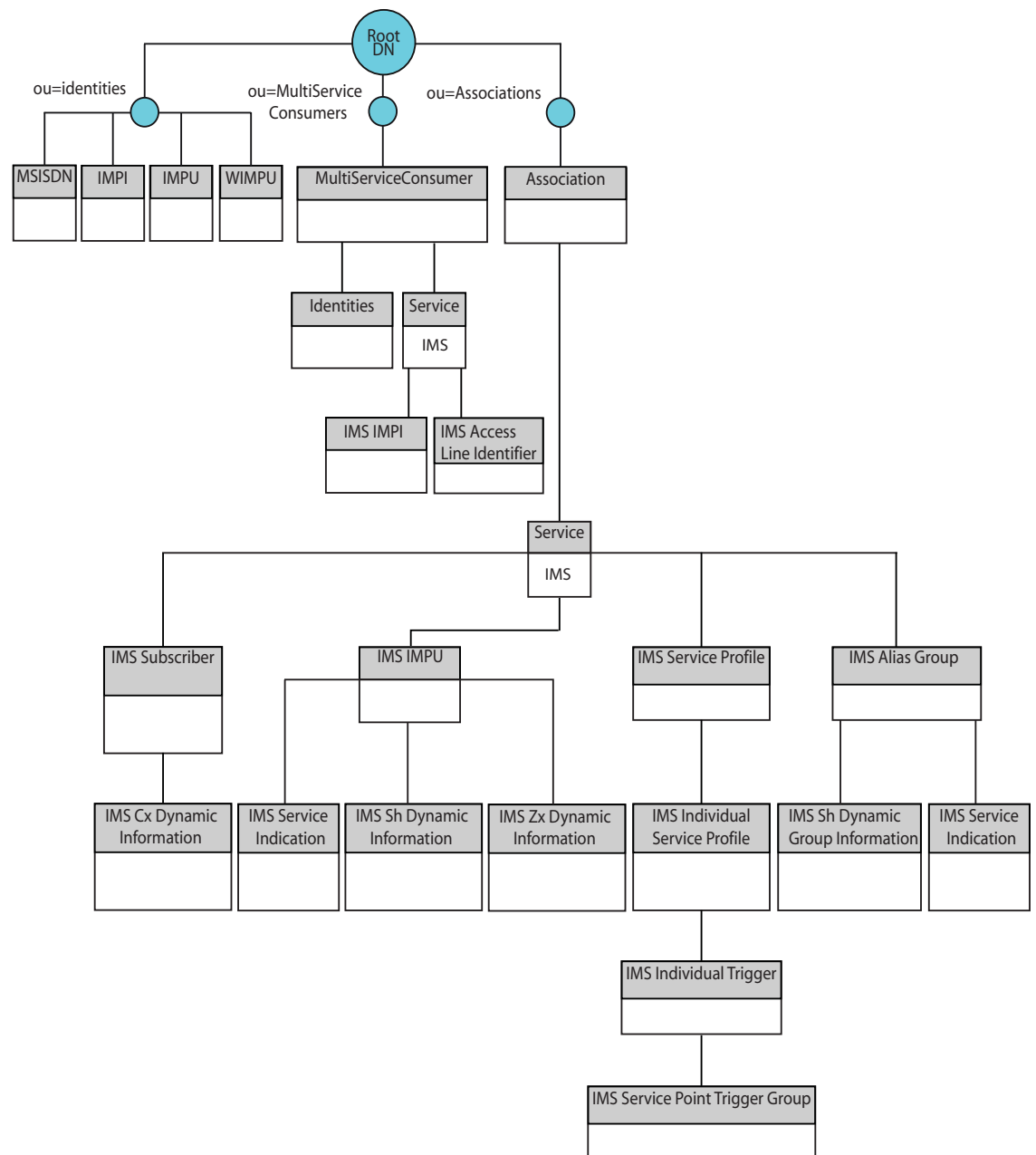


Figure 8 IMS Data Model

For a Create IMS Association CSO the LDAP objects are created in the following orders in CUDB:

1. Association object



Note: When assigning an `associationId`, the recommendation is to NOT use any of the Identifiers as `associationId`. Any random value or other value the customer has, except the identifier for ANY of the services (like IMSI, MSISDN, IMPI, IMPU) in the solution. This, since features like IMSI Changeover will only handle the service identities.

2. Service object IMS (Under Association)
3. IMS Subscriber object
4. IMS Cx Dynamic Information object

For each `IMPI`:

5. Identifier alias object (IMPI)
6. Identifier alias object (IMPI, for secondary IMPI), **Optional**
7. MultiSC object
8. Identities object
9. Service object (AAA)
10. **Optional**, IMSI alias and MSISDN alias objects
11. IMS (under MultiSC) object
12. IMS IMPI object
13. IMS Access Line Identifier object

For each `SubscriberServiceProfile`:

14. IMS Service Profile object

For every Individual Service Profile in this subscriber Service profile:

- a IMS Individual Service Profile object

For every Individual Trigger in the Individual Service Profile:

- b IMS Individual Trigger object

For every Service Point Trigger Group in the Individual Trigger object

- c IMS Service Point Trigger Group object

For each `AliasGroup`:

15. Alias Group
 - a IMS Alias Group



Note: This object is created by HSS-FE during traffic. Dynamic Activation only handles the deletion of it when last IMPU belonging to this group is deleted.

b IMS Sh Dynamic Group Information object

Note: This object is created by HSS-FE during traffic. Dynamic Activation handles updates and deletion upon validator request and deletion when the complete assoc/IMS is deleted.

c IMS Service Indication object

Note: This object is created by HSS-FE during traffic. Dynamic Activation only handles the deletion of it when corresponding IMS Alias Group is deleted.

For each IMPU:

16. IMS IMPU object

17. IMS Service Indication object

Note: This object is created by HSS-FE during traffic. Dynamic Activation only handles the deletion of it when corresponding IMS IMPU is deleted.

18. IMS Zx Dynamic Information object

19. IMS Sh Dynamic Information object

20. Identifier alias object (IMPU)

21. **Optional**, IMS WIMPU alias if `ImsIsWildcardExt = true`

Note: For a Delete IMS Association CSO, the LDAP objects are deleted in the opposite order. Step 21 is always performed, regardless if `ImsIsWildcardExt` is set to `false`.

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

4.2.1

Multiple Administration Area Support for IMS

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, the regions (administration area identifier), that a specific provisioning client is allowed to administer. Access restrictions can be defined on IMS CAI3G `Get`, `Create`, `Set`, and `Delete` operations.

Available functions are described in Section 4.2.1.1 on page 18.

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

4.2.1.1 Administration Area Identifier

For this feature to work with IMS, the Administration Area Identifier must be included in the provisioning request sent from BSS. The administration area identifier is one of the attributes in the CAI3G operation for subscriber creation. It is stored together with the rest of the subscriber data in the CUDB. Compared to the identifier used with HLR, the administration area identifier for IMS, `tenantId`, is optional in CAI3G but still mandatory for this feature.

Beyond the use for administration area, the HSS-FE uses this identifier to support different traffic cases, for example roaming/non-roaming to different GPRS location areas.

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

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 [8].



Reference List

Library References

- [1] *Library Overview*, 18/1553-CSH 109 628 Uen
- [2] *Layered AVG Provisioning over CAI3G*, 10/155 19-CSH 109 628 Uen
- [3] *Layered IMS Provisioning over CAI3G*, 13/155 19-CSH 109 628 Uen
- [4] *Front End Provisioning Datamodel Description in HSS*, 3/155 19-AVA 901 27/5 Uen
- [5] *System Administrators Guide for Native Deployment*, 1/1543-CSH 109 628 Uen
- [6] *HSS Notification Interface Description*, 11/155 19-AVA 901 27/5 Uen
- [7] *User Guide for Resource Activation*, 1/1553-CSH 109 628 Uen
- [8] *Function Specification Resource Activation*, 3/155 17-CSH 109 628 Uen
- [9] *Event and Alarm Handling*, 3/1553-CSH 109 628 Uen
- [10] *Layered IMS Provisioning over CAI3G*, 13/155 19-CSH 109 6288 Uen