

# 2

## IP Multimedia Subsystem Architecture

This chapter introduces the reader to the Internet Protocol (IP) Multimedia Subsystem (IMS). Section 2.1 explains basic architectural concepts: for instance, we explain why bearers are separated and why the home control model was selected. Section 2.2 gives a wide overview of IMS architecture, including an introduction to different network entities and main functionalities. Section 2.3 goes deeper and shows how the entities are connected and what protocols are used between them; it also describes their relationships to other domains: IP networks, UMTS and CS CN.

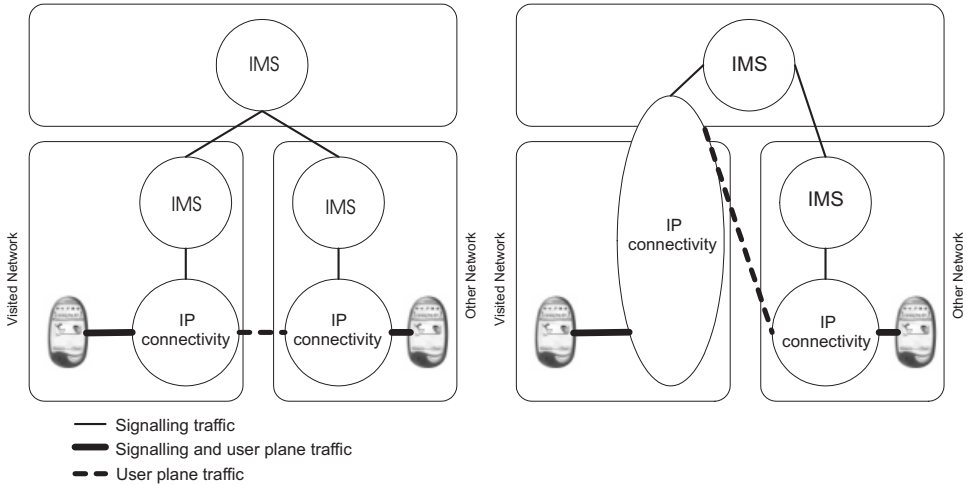
### 2.1 Architectural requirements

There is a set of basic requirements which guides the way in which the IMS architecture has been created and how it should evolve in the future. This section covers the most significant requirements. Third Generation Partnership Project (3GPP) stage 1 IMS requirements are documented in [3GPP TS 22.228].

#### 2.1.1 *IP connectivity*

A fundamental requirement is that a client has to have IP connectivity to access IMS services. In addition, it is required that IPv6 is used [3GPP TS 23.221].

IP connectivity can be obtained either from the home network or the visited network. The leftmost part of Figure 2.1 presents an option in which user equipment (UE) has obtained an IP address from a visited network. In the Universal Mobile Telecommunications System (UMTS) network this means that the radio access



**Figure 2.1** IMS connectivity options when a user is roaming.

network (RAN), Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) are located in the visited network when a user is roaming in the visited network. The rightmost part of Figure 2.1 presents an option in which a UE has obtained an IP address from the home network. In the UMTS network this means that the RAN and SGSN are located in the visited network when a user is roaming in the visited network. Obviously, when a user is located in the home network all necessary elements are in the home network and IP connectivity is obtained in that network.

It is important to note that a user can roam and obtain IP connectivity from the home network as shown in the figure. This would allow users to use new, fancy IMS services even when they are roaming in an area that does not have an IMS network but provides IP connectivity. In theory, it is possible to deploy an IMS network in a single area/country and use, say, General Packet Radio Service (GPRS) roaming to connect customers to the home network. In practice this would not happen because routing efficiency would not be high enough. Consider routing real time transport protocol (RTP) voice packets from the USA to Europe and then back to the USA. However, this deployment model is important when operators are ramping up IMS networks or, in an initial phase, when they are offering non or near-real time multimedia services.

### 2.1.2 Access independence

The IMS is designed to be access-independent so that IMS services can be provided over any IP connectivity networks (e.g., GPRS, WLAN, broadband access x-Digital

Subscriber Line). Unfortunately, Release 5 IMS specifications contain some GPRS-specific features. In Release 6 (e.g., GPRS) access-specific issues will be separated from the core IMS description. 3GPP uses the term “IP connectivity access network” to refer to the collection of network entities and interfaces that provides the underlying IP transport connectivity between the UE and the IMS entities. In this book we use GPRS as an example.

### *2.1.3 Ensuring quality of service for IP multimedia services*

On the public Internet, delays tend to be high and variable, packets arrive out of order and some packets are lost or discarded. This will no longer be the case with the IMS. The underlying access and transport networks together with the IMS provide end-to-end quality of service (QoS).

Via the IMS, UE negotiates its capabilities and expresses its QoS requirements during a Session Initiation Protocol (SIP) session set-up or session modification procedure. The UE is able to negotiate such parameters as:

- Media type, direction of traffic.
- Media type bit rate, packet size, packet transport frequency.
- Usage of RTP payload for media types.
- Bandwidth adaptation.

After negotiating the parameters at the application level, UEs reserve suitable resources from the access network. When end-to-end QoS is created, the UEs encode and packetize individual media types with an appropriate protocol (e.g., RTP) and send these media packets to the access and transport network by using a transport layer protocol (e.g., TCP or UDP) over IP. It is assumed that operators negotiate service-level agreements for guaranteeing the required QoS in the interconnection backbone. In the case of UTMS, operators could utilize the GPRS Roaming Exchange backbone.

### *2.1.4 IP policy control for ensuring correct usage of media resources*

IP policy control means the capability to authorize and control the usage of bearer traffic intended for IMS media, based on the signalling parameters at the IMS session. This requires interaction between the IP connectivity access network and the IMS. The means of setting up interaction can be divided into three different categories [3GPP TS 22.228, 23.207, 23.228]:

- The policy control element is able to verify that values negotiated in SIP signalling are used when activating bearers for media traffic. This allows an operator to verify that its bearer resources are not misused (e.g., the source and destination IP address and bandwidth in the bearer level are exactly the same as used in SIP session establishment).
- The policy control element is able to enforce when media traffic between end points of a SIP session start or stop. This makes it possible to prevent the use of the bearer until the session establishment is completed and allows traffic to start/stop in synchronization with the start/stop of charging for a session in IMS.
- The policy control element is able to receive notifications when the IP connectivity access network service has either modified, suspended or released the bearer(s) of a user associated with a session. This allows IMS to release ongoing session because, for instance, the user is no longer in the coverage area.

Policy control is further described in Section 3.9.

### *2.1.5 Secure communication*

Security is a fundamental requirement in every telecommunication system and the IMS is not an exception. The IMS provides at least a similar level of security as the corresponding GPRS and circuit-switched networks: for example, the IMS ensures that users are authenticated before they can start using services, and users are able to request privacy when engaged in a session. Section 3.6 will discuss security features in more detail.

### *2.1.6 Charging arrangements*

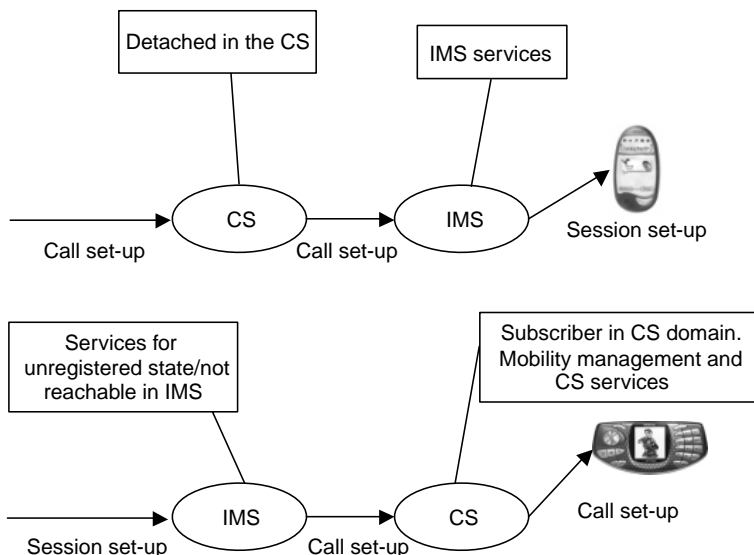
From an operator or service provider perspective the ability to charge users is a must in any network. The IMS architecture allows different charging models to be used. This includes, say, the capability to charge just the calling party or to charge both the calling party and the called party based on used resources in the transport level. In the latter case the calling party could be charged entirely on IMS-level session: that is, it is possible to use different charging schemes at the transport and IMS level. However, an operator might be interested to correlate charging information generated at transport and IMS (service and content) charging levels. This capability is provided if an operator utilizes a policy control reference point. The charging correlation mechanism is further described in Section 3.10.2 and policy control is explained in Section 3.9.

As IMS sessions may include multiple media components (e.g., audio and video), it is required that the IMS provides a means for charging per media component. This would allow a possibility to charge the called party if she adds a new media component in a session. It is also required that different IMS networks are able to exchange information on the charging to be applied to a current session [3GPP TS 22.101, TR 23.815].

The IMS architecture supports both online and offline charging capabilities. Online charging is a charging process in which the charging information can affect in real time the service rendered and therefore directly interacts with session/service control. In practice, an operator could check the user's account before allowing the user to engage a session and to stop a session when all credits are consumed. Prepaid services are applications that need online charging capabilities. Offline charging is a charging process in which the charging information does not affect in real time the service rendered. This is the traditional model in which the charging information is collected over a particular period and, at the end of the period, the operator posts a bill to the customer.

### *2.1.7 Support of roaming*

From a user point of view it is important to get access to her services regardless of her geographical location. The roaming feature makes it possible to use services even though the user is not geographically located in the service area of the home network. Section 2.1.1 has already described two instances of roaming: namely, GPRS roaming and IMS roaming. In addition to these two there exists an IMS circuit-switched (CS) roaming case. GPRS roaming means the capability to access the IMS when the visited network provides the RAN and SGSN and the home network provides the GGSN and IMS. The IMS roaming model refers to a network configuration in which the visited network provides IP connectivity (e.g., RAN, SGSN, GGSN) and the IMS entry point (i.e., P-CSCF) and the home network provides the rest of the IMS functionalities. The main benefit of this roaming model compared with the GPRS roaming model is optimum usage of user-plane resources. Roaming between the IMS and the CS CN domain refers to inter-domain roaming between IMS and CS. When a user is not registered or reachable in one domain a session can be routed to the other domain. It is important to note that both the CS CN domain and the IMS domain have their own services and cannot be used from another domain. Some services are similar and available in both domains (e.g., Voice over IP in IMS and speech telephony in CSCN). Figure 2.2 shows different IMS/CS roaming cases.



**Figure 2.2** IMS/CS roaming alternatives.

### 2.1.8 Interworking with other networks

It is evident that the IMS is not deployed over the world at the same time. Moreover, people may not be able to switch terminals or subscriptions very rapidly. This will raise the issue of being able to reach people regardless of what kind of terminals they have or where they live. To be a new, successful communication network technology and architecture the IMS has to be able to connect to as many users as possible. Therefore, the IMS supports communication with PSTN, ISDN, mobile and Internet users. Additionally, it will be possible to support sessions with Internet applications that have been developed outside the 3GPP community [3GPP TS 22.228].

### 2.1.9 Service control model

In 2G mobile networks the visited service control is in use. This means that, when a user is roaming, an entity in the visited network provides services and controls the traffic for the user. This entity in 2G is called a visited mobile service switching centre. In the early days of Release 5 both visited and home service control models were supported. Supporting two models would have required that every problem have more than one solution; moreover, it would reduce the number of optimal architecture solutions, as simple solutions may not fit both models. Supporting both models would have meant additional extensions for Internet Engineering

Task Force (IETF) protocols and increased the work involved in registration and session flows. The visited service control was dropped because it was a complex solution and did not provide any noticeable added value compared with the home service control. On the contrary, the visited service control imposes some limitations. It requires a multiple relationship and roaming models between operators. Service development is slower as both the visited and home network would need to support similar services, otherwise roaming users would experience service degradations. In addition, the number of interoperator reference points increase, which requires complicated solutions (e.g., in terms of security and charging). Therefore, the home service control was selected; this means that the entity that has access to the subscriber database and interacts directly with service platforms is always located at the user's home network.

### *2.1.10 Service development*

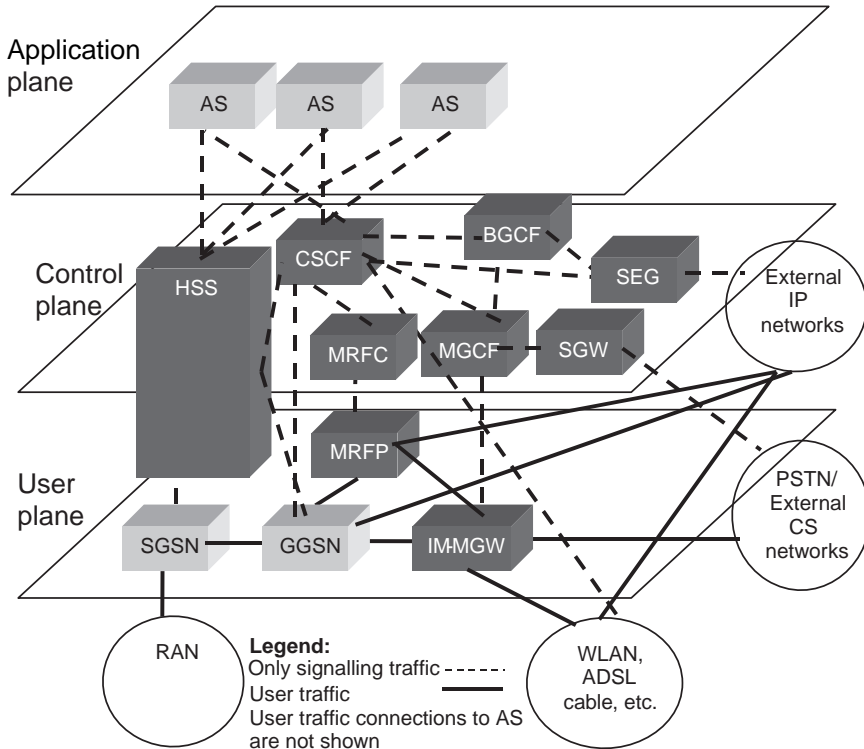
The importance of having a scalable service platform and the possibility to launch new services rapidly has meant that the old way of standardizing complete sets of teleservices, applications and supplementary services is no longer acceptable. Therefore, 3GPP is standardizing service capabilities and not the services themselves [3GPP TS 22.101]. The IMS architecture should actually include a service framework that provides the necessary capabilities to support speech, video, multimedia, messaging, file sharing, data transfer, gaming and basic supplementary services within the IMS. Section 3.12 further describes how the IMS service control works and Chapters 23–25 explain in more detail how presence, messaging and conferencing services are offered.

### *2.1.11 Layered design*

3GPP has decided to use a layered approach to architectural design. This means that transport and bearer services are separated from the IMS signalling network and session management services. Further services are run on top of the IMS signalling network. Figure 2.3 shows the design.

In some cases it may be impossible to distinguish between functionality at the upper and lower layers. The layered approach aims at a minimum dependency between layers. A benefit is that it facilitates the addition of new access networks to the system later on. Wireless Local Area Network (WLAN) access to the IMS, in 3GPP Release 6, will test how well the layering has been done. Other accesses may follow (e.g., fixed broadband).

The layered approach increases the importance of the application layer. When applications are isolated and common functionalities can be provided by the underlying IMS network the same applications can run on UE using diverse access types.



**Figure 2.3** IMS and layering architecture.

## 2.2 Description of IMS-related entities and functionalities

This section discusses IMS entities and key functionalities. These entities can be roughly classified in six main categories: session management and routing family (CSCFs), databases (HSS, SLF), interworking elements (BGCF, MGCF, IM-MGW, SGW), services (application server, MRFC, MRFP), support entities (THIG, SEG, PDF) and charging. It is important to understand that IMS standards are set up so that the internal functionality of network entities is not specified in detail. For instance, the Home Subscriber Server (HSS) contains three internal functions: IMS functionality, necessary functions for the CS domain and necessary functions for the PS domain. 3GPP standards do not describe how IMS functionality interacts with functions designed for Packet Switched (PS); instead, they describe reference points between entities and functionalities supported at the reference points (e.g., how does CSCF obtain user data from HSS). Different reference points will be described in Section 2.3. Additionally, General Packet Radio Service (GPRS) functions are described at the end of this section.



### 2.2.1 Proxy-CSCF

The Proxy-Call Session Control Function (P-CSCF) is the first contact point for users within the IMS. All SIP signalling traffic from or to the UE go via the P-CSCF. As the name of the entity indicates the P-CSCF behaves like a proxy as defined in [RFC3261]. It means that the P-CSCF validates the request, forwards it to selected destinations and processes and forwards the response. In addition, the P-CSCF may behave as a user agent (UA) as defined in [RFC3261]. The UA role is needed for releasing sessions in abnormal conditions (e.g., when a bearer loss is detected according to service-based local policy—see Section 3.9) and for generating independent SIP transactions, as explained in Section 5.12.6, which deals with registration. There can be one or many P-CSCFs within an operator's network. The functions performed by the P-CSCF are [3GPP TS 23.228, TS 24.229]:

- To forward SIP REGISTER requests to the Interrogating-CSCF (I-CSCF) based on a home domain name provided by the UE in the request. Section 5.5 gives a detailed description of what actions the P-CSCF needs to take before forwarding the SIP REGISTER request (e.g., to resolve an address of the CSCF or to let it be known that a REGISTER request was not received with a security association).
- To forward SIP requests and responses received by the UE to the Serving-CSCF (S-CSCF). Chapter 6 gives a detailed description of what actions the P-CSCF needs to take before forwarding a non-REGISTER request or response (e.g., to check that the user identity used is valid).
- To forward SIP requests and responses to the UE. Chapter 6 gives a detailed description of what actions the P-CSCF needs to take before forwarding SIP messages to the UE (e.g., to compress the message).
- To detect emergency session establishment requests. In Release 5 the P-CSCF returns a SIP error message, 380, indicating that the UE should try the CSCN instead. The work is ongoing in Release 6 and the P-CSCF behaviour is going to change in such a way that the P-CSCF will select an S-CSCF to handle an emergency session. The selection is needed because in IMS roaming cases the assigned S-CSCF is in the home network and the home S-CSCF is unable to route the request to a correct emergency centre.
- To send accounting-related information to the Charging Collection Function (CCF).
- To provide integrity protection of SIP signalling and maintain a security association between the UE and the P-CSCF. Integrity protection is provided by means of Internet Protocol Security (IPsec) Encapsulating Security Payload (ESP).

Release 6 is able to provide confidentiality protection as well. Section 3.6 explains how IMS security is designed and the security protocols are discussed in Chapter 18.

- To decompress and compress SIP messages from the UE. The P-CSCF supports compression based on three RFCs: [RFC3320], [RFC3485] and [RFC3486]. Sections 3.16 and 6.4 and Chapter 19 describe the usage of SIP compression in more detail [3GPP TS 24.229].
- To subscribe a registration event package at the user's registrar (S-CSCF). This is needed for downloading implicitly registered public user identities and for getting notifications on network-initiated de-registration events. Section 5.12.6 describes a registration event package and Section 3.14 shows how implicit registration works and Section 5.14.3 tells us more about network-initiated de-registrations.
- To execute media policing. The P-CSCF is able to check the content of the Session Description Protocol (SDP) payload and to check whether it contains media types or codecs, which are not allowed for a user. When the proposed SDP does not fit the operator's policy, the P-CSCF rejects the request and sends an SIP error message, 488, to the UE. An operator may want to use this feature for roaming users due to bandwidth restrictions.
- To maintain session timers. Release 5 does not provide a means for a statefull proxy to know the status of sessions. Release 6 corrects this deficiency by introducing session timers. It allows the P-CSCF to detect and free resources used up by hanging sessions.
- To interact with the Policy Decision Function (PDF). The PDF is responsible for implementing the Service Based Local Policy (SBLP). In Release 5 the PDF is a logical entity of the P-CSCF, and in Release 6 the PDF is a stand-alone function.

### *2.2.2 Policy Decision Function*

The Policy Decision Function (PDF) is responsible for making policy decisions based on session and media-related information obtained from the P-CSCF. It acts as a policy decision point for SBLP control. The following policy decision point functionalities for SBLP are identified:

- To store session and media-related information (IP addresses, port numbers, bandwidths, etc.).

- To generate an authorization token that identifies the PDF and the session.
- To provide an authorization decision according to the stored session and media-related information on receiving a bearer authorization request from the GGSN.
- To update the authorization decision at session modifications which changes session and media-related information.
- The capability to revoke the authorization decision at any time.
- The capability to enable the usage of an authorized bearer (e.g., Packet Data Protocol, or PDP, context).
- The capability to prevent the usage of an authorized bearer (e.g., PDP context) while maintaining the authorization.
- To inform the P-CSCF when the bearer (e.g., PDP context) is lost or modified. A modification indication is only given when the bearer is upgraded or downgraded from or to 0 kbit/s.
- To pass an IMS-charging identifier to the GGSN and to pass a GPRS-charging identifier to the P-CSCF.

### 2.2.3 *Interrogating-CSCF*

Interrogating-CSCF (I-CSCF) is a contact point within an operator's network for all connections destined to a subscriber of that network operator. There may be multiple I-CSCFs within an operator's network. The functions performed by the I-CSCF are:

- To contact the HSS to obtain the name of the S-CSCF that is serving a user.
- To assign an S-CSCF based on received capabilities from the HSS. An S-CSCF is assigned if there is no S-CSCF allocated. This procedure is described in more detail in Section 3.8.
- To forward SIP requests or responses to the S-CSCF.
- To send accounting-related information to the CCF.
- To provide a hiding functionality. The I-CSCF may contain a functionality called the Topology Hiding Inter-network Gateway (THIG). THIG could be used to hide the configuration, capacity and topology of the network from outside an operator's network.

### 2.2.4 *Serving-CSCF*

The Serving-CSCF (S-CSCF) is the brain of the IMS; it is located in the home network. It performs session control and registration services for UEs. While UE is engaged in a session the S-CSCF maintains a session state and interacts with service platforms and charging functions as needed by the network operator for support of the services. There may be multiple S-CSCFs, and S-CSCFs may have different functionalities within an operator's network. More specifically, the functions performed by the S-CSCF are:

- To handle registration requests by acting as a registrar as defined in [RFC3261]. The S-CSCF knows the UE's IP address and which P-CSCF the UE is using as an IMS entry point.
- To authenticate users by means of the IMS Authentication and Key Agreement (AKA) schema. The IMS AKA achieves mutual authentication between the UE and the home network.
- To download user information and service-related data from the HSS during registration or when handling a request to an unregistered user.
- To route mobile-terminating traffic to the P-CSCF and to route mobile-originated traffic to the I-CSCF, the Breakout Gateway Control Function (BGCF) or the application server (AS).
- To perform session control. The S-CSCF can act as a proxy server and UA as defined in [RFC3261].
- To interact with service platforms. Interaction means the capability to decide when a request or response needs to be routed to a specific AS for further processing.
- To translate an E.164 number to a SIP universal resource identifier (URI) using a domain name system (DNS) translation mechanism with the format as specified in [Draft-ietf-enum-rfc2916bis]. This translation is needed because routing of SIP signalling in IMS uses only SIP URIs.
- To supervise registration timers and to be able to de-register users when needed.
- To select an emergency centre when the operator supports IMS emergency sessions. This is a Release 6 feature.
- To execute media policing. The S-CSCF is able to check the content of the SDP payload and check whether it contains media types or codecs, which are not allowed for a user. When the proposed SDP does not fit the operator's policy or user's subscription, the S-CSCF rejects the request and sends a SIP error

message, 488. Section 3.11 shows how media policy information can be included as part of the user profile.

- To maintain session timers. Release 5 does not provide the means for a statefull proxy to know the status of sessions. Release 6 corrects this deficiency by introducing session timers. It allows the S-CSCF to detect and free resources used up by hanging sessions.
- To send accounting-related information to the CCF for offline charging purposes and to the Online Charging System (OCS) for online charging purposes.

### 2.2.5 Home Subscriber Server

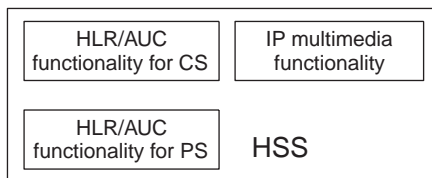
The Home Subscriber Server (HSS) is the main data storage for all subscriber and service-related data of the IMS. The main data stored in the HSS include user identities, registration information, access parameters and service-triggering information [3GPP TS 23.002].

User identities consist of two types: private and public user identities. The private user identity is a user identity that is assigned by the home network operator and is used for such purposes as registration and authorization, while the public user identity is the identity that other users can use for requesting communication with the end user. IMS access parameters are used to set up sessions and include parameters like user authentication, roaming authorization and allocated S-CSCF names. Service-triggering information enables SIP service execution. The HSS also provides user-specific requirements for S-CSCF capabilities. This information is used by the I-CSCF to select the most suitable S-CSCF for a user.

In addition to functions related to IMS functionality, the HSS contains the subset of Home Location Register and Authentication Center (HLR/AUC) functionality required by the PS domain and the CS domain. The structure of the HSS is shown in Figure 2.4. Communication between different HSS functions is not standardized.

HLR functionality is required to provide support to PS domain entities, such as SGSN and GGSN. This enables subscriber access to PS domain services. In similar fashion the HLR provides support for CS domain entities like MSC/MSC servers. This enables subscriber access to CS domain services and supports roaming to GSM/UMTS CS domain networks.

The AUC stores a secret key for each mobile subscriber, which is used to generate dynamic security data for each mobile subscriber. Data are used for mutual authentication of the International Mobile Subscriber Identity (IMSI) and the network. Security data are also used to provide integrity protection and ciphering of the communication over the radio path between the UE and the network.



**Figure 2.4** Structure of HSS.

There may be more than one HSS in a home network depending on the number of mobile subscribers, the capacity of the equipment and the organization of the network. There are multiple reference points between the HSS and other network entities.

### 2.2.6 *Subscription Locator Function*

The Subscription Locator Function (SLF) is used as a resolution mechanism that enables the I-CSCF, the S-CSCF and the AS to find the address of the HSS that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator.

### 2.2.7 *Multimedia Resource Function Controller*

The Multimedia Resource Function Controller (MRFC) is needed to support bearer-related services, such as conferencing, announcements to a user or bearer transcoding. The MRFC interprets SIP signalling received via S-CSCF and uses Media Gateway Control Protocol (MEGACO) instructions to control the Multimedia Resource Function Processor (MRFP). The MRFC is able to send accounting information to the CCF and OCS. Chapter 25 shows how the MRFC is used in conferencing services.

### 2.2.8 *Multimedia Resource Function Processor*

The Multimedia Resource Function Processor (MRFP) provides user-plane resources that are requested and instructed by the MRFC. The MRFP performs the following functions:

- Mixing of incoming media streams (e.g., for multiple parties).
- Media stream source (for multimedia announcements).

- Media stream processing (e.g., audio transcoding, media analysis) [3GPP TS 23.228, TS 23.002].

### 2.2.9 *Application server*

Keeping in mind the layered design, application servers (ASs) are not pure IMS entities; rather, they are functions on top of IMS. However, ASs are described here as part of IMS functions because ASs are entities that provide value-added multimedia services in the IMS.

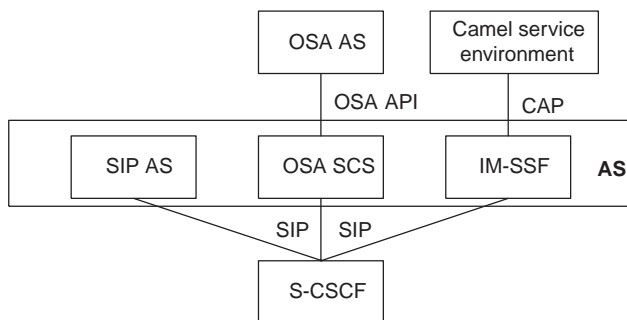
An AS resides in the user's home network or in a third-party location. The third party here means a network or a stand-alone AS. The main functions of the AS are:

- The possibility to process and impact an incoming SIP session received from the IMS.
- The capability to originate SIP requests.
- The capability to send accounting information to the CCF and the OCS.

Offered services are not limited purely to SIP-based services since an operator is able to offer access to services based on the Customized Applications for Mobile network Enhanced Logic (CAMEL) Service Environment (CSE) and the Open Service Architecture (OSA) for its IMS subscribers [3GPP TS 23.228]. Therefore, "AS" is the term used generically to capture the behaviour of the SIP AS, OSA Service Capability Server (SCS) and CAMEL IP Multimedia Service Switching Function (IM-SSF).

Using the OSA an operator may utilize such service capability features as call control, user interaction, user status, data session control, terminal capabilities, account management, charging and policy management for developing services [3GPP TS 29.198]. An additional benefit of the OSA framework is that it can be used as a standardized mechanism for providing third-party ASs in a secure manner to the IMS, as the OSA itself contains initial access, authentication, authorization, registration and discovery features (the S-CSCF does not provide authentication and security functionality for secure direct third-party access to the IMS). As the support of OSA services is down to operator choice, it is not architecturally sound to support OSA protocols and features in multiple entities. Therefore, OSA SCS is used to terminate SIP signalling from the S-CSCF. The OSA SCS uses an OSA application program interface (API) to communicate with an actual OSA application server.

The IM-SSF function was introduced in the IMS architecture to support legacy services that are developed in the CAMEL Service Environment (CSE). It hosts CAMEL network features (trigger detection points, CAMEL Service Switching



**Figure 2.5** Relationship between different AS types.

Finite State Machine, etc.) and interworks with the CAMEL Application Part (CAP) interface.

A SIP AS is a SIP-based server that hosts a wide range of value-added multimedia services. A SIP AS could be used to provide presence, messaging and conferencing services. The different functions of SIP servers are described in more detail in Sections 8.3 and 3.12.4, as part of service provisioning.

Figure 2.5 shows how different functions are connected. From the perspective of the S-CSCF SIP AS, the OSA service capability server and the IM-SSF exhibit the same reference point behaviour.

An AS may be dedicated to a single service and a user may have more than one service, therefore there may be one or more ASs per subscriber. Additionally, there may be one or more ASs involved in a single session. For example, an operator could have one AS to control terminating traffic to a user based on user preferences (e.g., redirecting all incoming multimedia sessions to an answer machine between 5 p.m. and 7 a.m.) and another AS to adapt the content of instant messages according to the capabilities of the UE (screen size, number of colours, etc.).

### 2.2.10 Breakout Gateway Control Function

The Breakout Gateway Control Function (BGCF) is responsible for choosing where a breakout to the CS domain occurs. The outcome of a selection process can be either a breakout in the same network in which the BGCF is located or another network. If the breakout happens in the same network, then the BGCF selects a Media Gateway Control Function (MGCF) to handle a session further. If the breakout takes place in another network, then the BGCF forwards a session to another BGCF in a selected network [3GPP TS 23.228]. The actual selection rules are not specified. In addition, the BGCF is able to report account information to the CCF and collect statistical information. IMS and CS interworking is described in Section 3.13.



### *2.2.11 Media Gateway Control Function*

The Media Gateway Control Function (MGCF) is a gateway that enables communication between IMS and CS users. All incoming call control signalling from CS users is destined to the MGCF that performs protocol conversion between the ISDN User Part (ISUP), or the Bearer Independent Call Control (BICC), and SIP protocols and forwards the session to IMS. In similar fashion all IMS-originated sessions toward CS users traverses through MGCF. MGCF also controls media channels in the associated user-plane entity, the IMS Media Gateway CIMS-MGW. In addition, MGCF is able to report account information to the CCF. IMS and CS interworking is described in Section 3.13.

### *2.2.12 IP Multimedia Subsystem-Media Gateway Function*

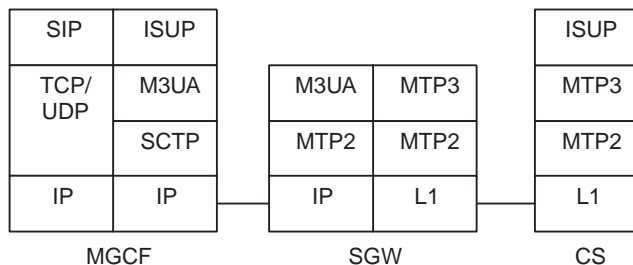
The IMS Multimedia Gateway (IMS-MGW) provides the user-plane link between CS networks (PSTN, GSM) and the IMS. It terminates the bearer channels from the CS network and media streams from the backbone network (e.g., RTP streams in an IP network or AAL2/ATM connections in an ATM backbone), executes the conversion between these terminations and performs transcoding and signal processing for the user plane when needed. In addition, the IMS-MGW is able to provide tones and announcements to CS users. The IMS-MGW is controlled by the MGCF.

### *2.2.13 Signalling gateway*

A signalling gateway (SGW) is used to interconnect different signalling networks, such as SCTP/IP-based signalling networks and SS7 signalling networks. The SGW performs signalling conversion (both ways) at the transport level between the Signalling System No. 7 (SS7)-based transport of signalling and the IP-based transport of signalling (i.e., between Sigtran SCTP/IP and SS7 MTP). The SGW does not interpret application layer (e.g., BICC, ISUP) messages. In Figure 2.6 ISUP is shown, but BICC could be shown as well.

### *2.2.14 Security gateway*

To protect control-plane traffic between security domains, traffic will pass through a security gateway (SEG) before entering or leaving the security domain. The security domain refers to a network that is managed by a single administrative authority. Typically, this coincides with operator borders. The SEG is placed at the border of



**Figure 2.6** Signalling conversion in the SGW.

the security domain and it enforces the security policy of a security domain toward other SEGs in the destination security domain. The network operator may have more than one SEG in its network in order to avoid a single point of failure or for performance reasons. The SEG may be defined for interaction toward all reachable security domain destinations or it may be defined for only a subset of the reachable destinations [3GPP TS 33.203]. The concept behind a security domain is described more thoroughly in Section 3.6.3.

### 2.2.15 Charging entities

Different charging entities and corresponding reference points will be described separately in Section 3.10.

### 2.2.16 GPRS entities

#### 2.2.16.1 Serving GPRS Support Node

The Serving GPRS Support Node (SGSN) links the RAN to the packet core network. It is responsible for performing both control and traffic-handling functions for the PS domain. The control part contains two main functions: mobility management and session management. Mobility management deals with the location and state of the UE and authenticates both the subscriber and the UE. The control part of session management deals with connection admission control and any changes in the existing data connections. It also supervises 3G network services and resources. Traffic handling is the part of session management that is executed. The SGSN acts as a gateway for user data tunnelling: in other words, it relays user traffic between the UE and the GGSN. As a part of this function, the SGSN also ensures that connections receive the appropriate QoS. In addition, the SGSN generates charging information.

### 2.2.16.2 Gateway GPRS Support Node

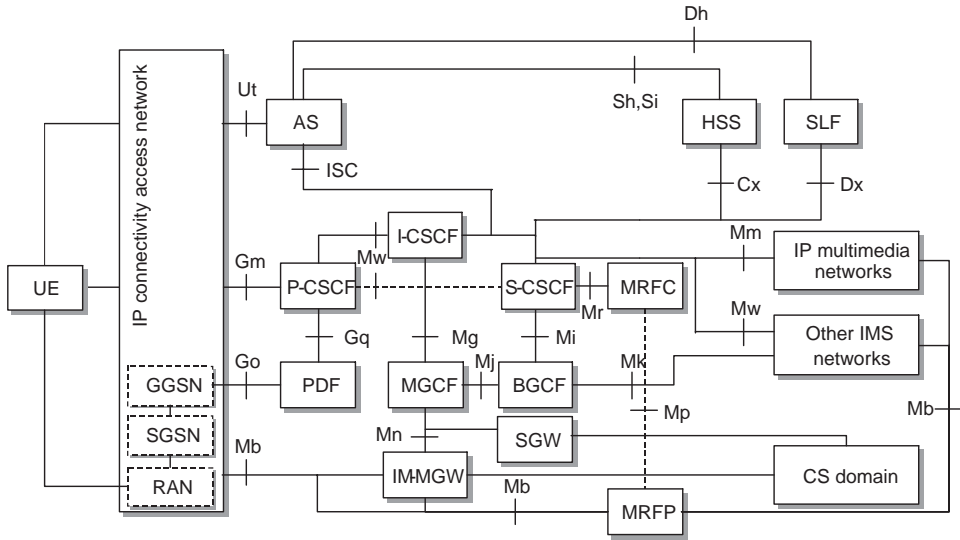
The Gateway GPRS Support Node (GGSN) provides interworking with external packet data networks. The prime function of the GGSN is to connect the UE to external data networks, where IP-based applications and services reside. The external data network could be the IMS or the Internet, for instance. In other words, the GGSN routes IP packets containing SIP signalling from the UE to the P-CSCF and vice versa. Additionally, the GGSN takes care of routing IMS media IP packets toward the destination network (e.g., to GGSN in the terminating network). The interworking service provided is realized as access points that relate to the different networks the subscriber wants to connect. In most cases the IMS has its own access point. When the UE activates a bearer (PDP context) toward an access point (IMS), the GGSN allocates a dynamic IP address to the UE. This allocated IP address is used in IMS registration and when the UE initiates a session as a contact address of the UE. Additionally, the GGSN polices and supervises the PDP context usage for IMS media traffic and generates charging information.

## 2.3 IMS reference points

This section explains how the previously described network entities are connected to each other and what protocol is used; moreover, the IMS architecture is depicted (Figure 2.7). You will also find an overview of SIP-based reference points (i.e., where SIP is used and what are the main procedures). However, you will realize that the level of description of SIP-based reference points is not so deep as with Diameter-based reference points. The reason for this division is that several chapters in this book are dedicated for SIP and SDP procedures where such descriptions are given in detail.

For the sake of clarity, it is impossible to include everything in one figure; so, please note the following:

- Figure 2.7 does not show charging-related functions or reference points (see Section 3.10 for more details).
- The figure does not show different types of ASs (see Section 2.2.9 for more details).
- The figure does not show the user-plane connections between different IMS networks and the AS.
- The figure does not show the SEG at the Mm, Mk, Mw reference points.
- The dotted line between the entities indicates a direct link.



**Figure 2.7** IMS architecture.

- ISC, Cx, Dx, Mm, Mw terminate at both the Serving-CSCF (S-CSCF) and the I-CSCF.

### 2.3.1 Gm reference point

The Gm reference point connects the UE to the IMS. It is used to transport all SIP signalling messages between the UE and the IMS. The IMS counterpart is P-CSCF. Procedures in the Gm reference point can be divided into three main categories: registration, session control and transactions:

- In the registration procedure the UE uses the Gm reference point to send a registration request with an indication of supported security mechanisms to the P-CSCF. During the registration process the UE exchanges the necessary parameters for authenticating both itself and the network, gets implicit registered user identities, negotiates the necessary parameters for a security association with the P-CSCF and possibly starts SIP compression. In addition, the Gm reference point is used to inform the UE if network-initiated de-registration or network-initiated re-authentication occurs.
- Session control procedures contain mechanisms for both mobile-originated sessions and mobile-terminated sessions. In mobile-originated sessions the Gm reference point is used to forward requests from the UE to the P-CSCF. In

mobile-terminated sessions the Gm reference point is used to forward request from the P-CSCF to the UE.

- Transaction procedures are used to send stand-alone requests (e.g., MESSAGE) and to receive all responses (e.g., 200 OK) to that request via the Gm reference point. The difference between transaction procedures and session control procedures is that a dialog is not created.

### 2.3.2 *Mw reference point*

The Gm reference point links the UE to the IMS (namely, to P-CSCF). Next, a SIP-based reference point between different CSCFs is needed. This reference point is called Mw. The procedures in the Mw reference point can be divided into three main categories: registration, session control and transaction:

- In the registration procedure the P-CSCF uses the Mw reference point to forward a registration request from the UE to the I-CSCF. The I-CSCF then uses the Mw reference point to pass the request to the S-CSCF. Finally, the response from the S-CSCF traverses back via the Mw reference point. In addition, the S-CSCF uses the Mw reference point in network-initiated de-registration procedures to inform the UE about network-initiated de-registration and network-initiated re-authentication to inform the P-CSCF that it should release resources regarding a particular user.
- Session control procedures contain mechanisms for both mobile-originated sessions and mobile-terminated sessions. In mobile-originated sessions the Mw reference point is used to forward requests both from the P-CSCF to the S-CSCF and from the S-CSCF to the I-CSCF. In mobile-terminated sessions the Mw reference point is used to forward requests both from the I-CSCF to the S-CSCF and from the S-CSCF to the P-CSCF. This reference point is also used for network-initiated session releases: for example, the P-CSCF could initiate a session release toward the S-CSCF if it receives an indication from the PDF that media bearer(s) are lost. In addition, charging-related information is conveyed via the Mw reference point.
- Transaction procedures are used to pass a stand-alone request (e.g., MESSAGE) and to receive all responses (e.g., 200 OK) to that request via the Mw reference point. As already stated, the difference between transaction procedures and session control procedures is that a dialog is not created.

### 2.3.3 IMS Service Control reference point

In the IMS architecture, ASs are entities that host and execute services, such as presence, messaging and session forwarding. Therefore, there has to be a reference point for sending and receiving SIP messages between the CSCF and an AS. This reference point is called the IMS Service Control (ISC) reference point and the selected protocol is SIP. ISC procedures can be divided into two main categories: routing the initial SIP request to an AS and AS-initiated SIP requests:

- When the S-CSCF receives an initial SIP request it will analyse it. Based on the analysis the S-CSCF may decide to route the request to an AS for further processing. The AS may terminate, redirect or proxy the request from the S-CSCF.
- An AS may initiate a request (e.g., on behalf of a user).
- The concept of service control is thoroughly described in Section 3.12.

### 2.3.4 Cx reference point

Subscriber and service data are permanently stored in the HSS. These centralized data need to be utilized by the I-CSCF and the S-CSCF when the user registers or receives sessions. Therefore, there has to be a reference point between the HSS and the CSCF. This reference point is called the Cx reference point and the selected protocol is Diameter. The procedures can be divided into three main categories: location management, user data handling and user authentication. Generally, descriptions only cover successful cases—unsuccessful ones are not covered here. The result information element could be used to carry information about why a request fails. If an error occurs, an answer message would not contain any further information elements in most cases.

#### 2.3.4.1 Location management procedures

Location management procedures can be further divided in two groups: registration and de-registration, and location retrieval.

##### *Registration and de-registration procedures between I-CSCF and HSS*

When the I-CSCF receives a SIP REGISTER request from the P-CSCF via the Mw reference point it will invoke a user registration status query, or as it is known in the standards a User-Authorization-Request (UAR) command. This command contains:

- Private User Identity—the identity to uniquely identify the user from a network perspective. It identifies subscription and correct authentication data (see Section 3.4.1.1 for further details on private user identity).
- Public User Identity—the identity to be registered (see Section 3.4.1.2 for further details on public user identity).
- Visited Network Identifier—identifies the visited IMS network in the case of IMS roaming. Based on this identifier the HSS is able to enforce roaming restrictions.
- Routing Information—contains the address of the HSS if the I-CSCF is aware of it. If the I-CSCF does not know the address of the HSS, then it contains the destination realm (i.e., the SLF is used to resolve a correct HSS).
- Type of Authorization—three possible values for the type of authorization information element are defined:
  - REGISTRATION—it is included when the expires value in the REGISTER request does not equal zero.
  - REGISTRATION\_CAPABILITIES—it is included when the expires value in the REGISTER request is not equal to zero and the I-CSCF explicitly queries S-CSCF capabilities (e.g., when a previously given S-CSCF is not responding).
  - DE-REGISTRATION—it is included when the expires value in the REGISTER request is equal to zero.

After receiving the UAR command the HSS sends a User-Authorization-Answer (UAA) command. It contains:

- Result—informs the outcome of the UAR command.
- S-CSCF Name and/or S-CSCF Capabilities (if the UAR command does not fail due, say, to the private and public identities received in the request not belonging to the same user) depending on the user's current registration status.

S-CSCF capabilities are returned if the user does not have an S-CSCF name assigned yet in the HSS or if the I-CSCF explicitly requests S-CSCF capabilities. Otherwise, the S-CSCF name is returned. When capabilities are returned the I-CSCF needs to perform S-CSCF selection as described in Section 3.8.

### ***Registration and de-registration procedures between S-CSCF and HSS***

We explained above how I-CSCF finds an S-CSCF that will serve the user. Having done this, the I-CSCF forwards a SIP REGISTER request to the S-CSCF. When the

S-CSCF receives the SIP REGISTER request from the I-CSCF it uses a Server-Assignment-Request (SAR) command to communicate with the HSS. The SAR command is used to inform the HSS about which S-CSCF will be serving the user when the expires value is not equal to zero. Similarly, if the expires value equals zero, then the SAR command is used to inform that the S-CSCF is no longer serving a user. A precondition for sending the SAR command is that the user has been successfully authenticated by the S-CSCF. The SAR command contains:

- Private User Identity—see the UAR command.
- Public User Identity—the identity to be registered/de-registered (see Section 3.4.1.2 for further details on public user identity).
- Routing Information—contains the address of the HSS if the S-CSCF is aware of it. If the S-CSCF does not know the address of the HSS, then it contains the destination realm.
- S-CSCF Name—contains the SIP URI of the S-CSCF.
- Server Assignment Type—the server assignment type contains information about why this operation is executed (e.g., due to registration, re-registration, session to unregistered user, de-registration that is user-initiated or S-CSCF-initiated and authentication failure).
- User Data Already Available—indicates to the HSS whether or not the S-CSCF has already the part of the user profile that it needs for serving the user.
- User Data Request Type—tells whether the S-CSCF wants to download a complete, registered or unregistered profile.

After receiving the SAR command the HSS will respond with a Server-Assignment-Answer (SAA) command. It contains:

- Result—inform the outcome of the SAR command.
- User Profile—based on the set values of Server Assignment Type and User Data Already Available in the SAR command the User Profile is sent (the User Profile is explained in Section 3.11).
- Charging Information—contains the addresses of the charging functions. This is an optional information element.

Previous sections have described how user-initiated registration and de-registration (user-initiated or S-CSCF-initiated) procedures are handled over the Cx reference point. There is still the need for additional operations to bring about network-initiated de-registration (e.g., due to stolen UE or when a subscription is terminated). In this case it is the HSS that starts network-initiated de-registration by using a



command called Registration-Termination-Request (RTR). The RTR command contains:

- Private User Identity—the identity to uniquely identify the user from a network perspective. It identifies the subscription and the correct authentication data (see Section 3.4.1.1 for further details on private user identity).
- Public User Identity—one or more identities to be deregistered (see Section 3.4.1.2 for further details on public user identity).
- Routing Information—contains the name of the S-CSCF that is serving the user.
- Reason for de-registration—contains a reason code that determines S-CSCF behaviour and optionally includes a textual message to be shown to the user.

The RTR command is acknowledged by a Registration-Termination-Answer (RTA) command, which simply indicates the result of the operation. Note that it is possible to deregister the public user identity in one go by only sending the private user identity.

### *Location retrieval procedures*

Previously, we have described how the I-CSCF uses a user registration status query (UAR command) to find the S-CSCF when it receives a SIP REGISTER request. Correspondingly, there has to be a procedure to find the S-CSCF when a SIP method is different than REGISTER. The required procedure is to make use of a Location-Info-Request (LIR) command. This request contains:

- Public User Identity—contains the identity from the request URI field of a SIP method.
- Routing Information—contains the address of the HSS if the I-CSCF is aware of it. If the I-CSCF does not know the address of the HSS, then it contains the destination realm.

The HSS responds with a Location-Info-Answer (LIA) command. The response contains:

- Result—inform the outcome of the LIR command.
- The S-CSCF Name or S-CSCF Capabilities—the latter are returned if the user does not have the S-CSCF name assigned, otherwise the SIP URI of the S-CSCF is returned.

#### 2.3.4.2 User data-handling procedures

During the registration process, user and service-related data will be downloaded from the HSS to the S-CSCF via the Cx reference point using SAR and SAA commands as described earlier. However, it is possible for these data to be changed later when the S-CSCF is still serving a user. To update the data in the S-CSCF the HSS initiates a Push-Profile-Request (PPR) command. This request contains:

- Private User Identity—the identity to uniquely identify the user from a network perspective (see Section 3.4.1.1 for further details on private user identity).
- Routing Information—contains the name of the S-CSCF that is serving the user.
- User Data—contains the updated user profile (the user profile is explained in Section 3.11).

Update takes place immediately after the change with one exception: when the S-CSCF is serving an unregistered user or the S-CSCF is kept for an unregistered user as described in Section 3.8.5 and there is a change in the registered part of user profile, then the HSS will not send a PPR command. The PPR command is acknowledged by a Push-Profile-Answer (PPA) command, which simply indicates the result of the operation.

#### 2.3.4.3 Authentication procedures

IMS user authentication relies on a pre-configured shared secret. Shared secrets and sequence numbers are stored in the IP Multimedia Services Identity Module (ISIM) in the UE and in the HSS in the network. Because S-CSCF takes care of user authorization, there exists the need to transfer security data over the Cx reference point. When the S-CSCF needs to authenticate a user it sends a Multimedia-Auth-Request (MAR) command to the HSS. This request contains:

- Private User Identity—the identity to uniquely identify the user from a network perspective. It identifies subscription and correct authentication data (see Section 3.4.1.1 for further details on private user identity).
- Public User Identity—the identity to be registered (see Section 3.4.1.2 for further details on public user identity).
- S-CSCF Name—contains the SIP URI of the S-CSCF.
- Routing Information—contains the address of the HSS if the I-CSCF is aware

**Table 2.1** Cx commands.

Command-Name	Purpose	Abbreviation	Source	Destination
User-Authorization-Request/Answer	User-Authorization-Request/Answer (UAR/UAA) commands are used between the I-CSCF and the HSS during SIP registration for retrieving S-CSCF name or S-CSCF capabilities for S-CSCF selection and during SIP deregistration for retrieving S-CSCF name when the SIP method is REGISTER	UAR	I-CSCF	HSS
		UAA	HSS	I-CSCF
Server-Assignment-Request/Answer	Server-Assignment-Request/Answer (SAR/SAA) commands are used between the S-CSCF and the HSS to update the S-CSCF name to the HSS and to download the user profile data to the S-CSCF	SAR	S-CSCF	HSS
		SAA	HSS	X-CSCF
Location-Info-Request/Answer	Location-Info-Request/Answer (LIR/LIA) commands are used between the I-CSCF and the HSS during the SIP session set-up to obtain the name of the S-CSCF that is serving the user or S-CSCF capabilities for S-CSCF selection	LIR	I-CSCF	HSS
		LIA	HSS	I-CSCF
Multimedia-Auth-Request/Answer	Multimedia-Auth-Request/Answer (MAR/MAA) commands are used between the S-CSCF and the HSS to exchange information to support the authentication between the end user and the home IMS network	MAR	S-CSCF	HSS
		MAA	HSS	S-CSCF
Registration-Termination-Request/Answer	Registration-Termination-Request/Answer (RTR/RTA) commands are used between the S-CSCF and the HSS when the HSS administratively de-registers one or more of the user's public identities	RTR	HSS	S-CSCF
		RTA	S-CSCF	HSS
Push-Profile-Request/Answer	Push-Profile-Request/Answer (PPR/PPA) commands are used between the HSS and the S-CSCF when user profile data are changed by a management operation in HSS and the data need to be updated to the S-CSCF	PPR	HSS	S-CSCF
		PPA	S-CSCF	HSS

of it. If the I-CSCF does not know the address of the HSS, then it contains the destination realm.

- Number of Authentication Items—information about how many authentication vectors the S-CSCF wants to download at once. Multiple authentication vectors can be downloaded (e.g., if an operator wants to re-authenticate all re-registrations).
- Authentication Data—includes authentication scheme (e.g., Digest-AKAv1-MD5) and authentication information in case of synchronization failure.

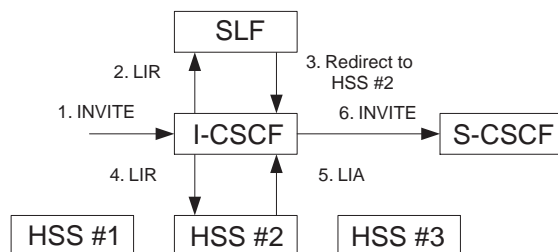
The HSS responds with a Multimedia-Auth-Answer (MAA) command. The answer contains:

- Result—informs the outcome of the MAR command.
- Private User Identity—the identity to uniquely identify the user from a network perspective. It identifies subscription and correct authentication data (see Section 3.4.1.1 for further details on private user identity).
- Public User Identity—the identity to be registered (see Section 3.4.1.2 for further details on public user identity).
- Number of Authentication Items—contains the authentication vectors.
- Authentication Data—includes an authentication vector, which is comprised of an Authentication Scheme (e.g., Digest-AKAv1-MD5), Authentication Information (authentication challenge RAND and the token AUTN), Authorization Information (expected response, or XRES), Integrity Key and, optionally, a Confidentiality Key. Additionally, it contains an Item Number, which indicates the order in which the authentication vectors are to be consumed when multiple vectors are returned.

### 2.3.5 *Dx reference point*

When multiple and separately addressable HSSs have been deployed in a network, neither the I-CSCF nor the S-CSCF know which HSS they need to contact. However, they need to contact the SLF first. For this purpose the Dx reference point has been introduced. The Dx reference point is always used in conjunction with the Cx reference point. The protocol used in this reference point is based on DIAMETER. Its functionality is implemented by means of the routing mechanism provided by an enhanced DIAMETER redirect agent.

To get an HSS address the I-CSCF or the S-CSCF sends to the SLF the Cx



**Figure 2.8** HSS resolution using the SLF.

requests aimed for the HSS. On receipt of the HSS address from the SLF, I-CSCF or the S-CSCF will send the Cx requests to the HSS. Figure 2.8 shows how the SLF is used to find a correct HSS when the I-CSCF receives an INVITE request and three HSSs have been deployed.

### 2.3.6 Sh reference point

An AS (SIP AS or OSA SCS) may need user data or need to know which S-CSCF to send a SIP request. This type of information is stored in the HSS. Therefore, there has to be a reference point between the HSS and the AS. This reference point is called the Sh reference point and the protocol is DIAMETER. Procedures are divided into two main categories: data handling and subscription/notification. The HSS maintains a list of ASs that are allowed to obtain or store data.

#### 2.3.6.1 Data handling

Data handling procedures contain the possibility to retrieve user data from the HSS. Such user data can contain service-related data (transparent or non-transparent), registration information, identities, initial filter criteria, S-CSCF name serving the user, addresses of the charging functions and even location information from the CS and PS domains. Transparent data are understood syntactically but not semantically by the HSS. They are data that an AS may store in the HSS to support its service logic. On the contrary, non-transparent data are understood both syntactically and semantically by the HSS. The AS uses the User-Data-Request (UDR) command to request data. The request contains:

- User identity—including the public user identity of the user who requires the data (see Section 3.4.1.2 for further details on public user identity).

- AS Identity—identifies the requesting AS. This information is used to check whether the AS has permission to fetch data from the HSS.
- Requested Domain—indicates the access domain for which certain data are requested. Two values are specified: CS domain and PS domain.
- Requested Data—used to indicate what kind of data is requested. The following values are defined:
  - RepositoryData—contains the transparent data stored for the user.
  - PublicIdentifiers—list of public user identities of the user.
  - IMSUserState—information about the user’s current state in IMS, defined as REGISTERED, NOT\_REGISTERED, AUTHENTICATION\_PENDING and REGISTERED\_UNREG\_SERVICES.
  - S-CSCFName—name of the S-CSCF that is serving the user.
  - InitialFilterCriteria—contains the relevant triggering information for a service that impacts the requesting AS (see Sections 3.11.1.3 and 3.12 for further information).
  - LocationInformation—consists of location information about the user in the requested domain (e.g., cell global identification).
  - UserState—information about the user’s current state in the requested domain.
  - ChargingInformation—contains the addresses of the charging functions.
- Current Location: informs whether the HSS has to perform a location retrieval procedure.
- Service Indication—unique value within the operator’s network to identify transparent data.
- AS Name—the identity that is used together with other values to identify the correct InitialFilterCriteria.

The HSS responds with the User-Data-Answer (UDA). The response contains:

- Result informs the outcome of the UDR command.
- The requested data.

The AS can update transparent data in the HSS using the Profile-Update-Request (PUR) command, which contains:

- User Identity—includes the public user identity of the user who required the data (see Section 3.4.1.2 for further details on public user identity).
- AS Identity—identifies the requesting AS. This information is used to check whether the AS has permission to fetch data from the HSS.
- Data—contains the data to be updated.

The PUR command is acknowledged by a Profile-Update-Answer (PUA) command, which simply indicates the result of the operation.

### 2.3.6.2 Subscription/Notification

Subscription/Notification procedures allow the AS to get a notification when particular data for a specific user is updated in the HSS. The AS sends a Subscribe-Notifications-Request (SNR) command to receive a notification of when a user's data indicated in the SNR command are changed in the HSS:

- User Identity—includes the public user identity of the user who requires the data change.
- Requested Data—contains the reference to the data on which notifications of change are required. Possible values are shown as part of the UDR command (RepositoryData, PublicIdentifiers, etc.).
- Subscription Request Type—informs whether the AS wants to perform a subscribe (initiates notifications) or unsubscribe (stops notifications) operation.
- Service Indication—unique value within the operator's network to identify the transparent data that require the data change.
- Application Server Identity—identifies the requesting AS. This information is used to check whether the AS has permission to fetch data from the HSS.
- Application Server Name—an identity that is used together with other values to identify the correct InitialFilterCriteria that are required for data change.

The HSS acknowledges the subscription request by a Subscribe-Notifications-Answer (SNA) command, which simply indicates the result of the operation.

If the AS has sent the SNR command and requested a notification with subscription request type, then the HSS sends a Push-Notification-Request (PNR) command to the AS when the particular data has changed. It contains the following information:

- User Identity—includes a public user identity of the user for whom the data have changed;
- Requested Data—contains the changed data.

The PNR command is acknowledged by a Push-Notification-Answer (PNA) command, which simply indicates the result of the operation.

**Table 2.2** Sh commands.

Command-Name	Purpose	Abbreviation	Source	Destination
User-Data-Request/Answer	User-Data-Request/Answer (UDR/UDA) commands are used to deliver the user data of a particular user	UDR	AS	HSS
		UDA	HSS	AS
Profile-Update-Request/Answer	Profile-Update-Request/Answer (PUR/PUA) commands are used to update transparent data in the HSS	PUR	AS	HSS
		PUA	HSS	AS
Subscribe-Notifications-Request/Answer	Subscribe-Notifications-Request/Answer commands are used to make a subscription/cancel a subscription to user's data on which notifications of change are required	SNR	AS	HSS
		SNA	HSS	AS
Push-Notification-Request/Answer	Push-Notification-Request/Answer commands are used to send the changed data to the AS	PNR	HSS	AS
		PNA	AS	HSS

### 2.3.7 *Si* reference point

When the AS is a CAMEL AS (IM-SSF) it uses the *Si* reference point to communicate to the HSS. The *Si* reference point is used to transport CAMEL subscription information including triggers from the HSS to the IM-SSF. The used protocol is Mobile Application Part (MAP).

### 2.3.8 *Dh* reference point

When multiple and separately addressable HSSs have been deployed in the network, the AS cannot know which HSS it needs to contact. However, the AS needs to



contact the SLF first. For this purpose the Dh reference point was introduced in Release 6. In Release 5 the correct HSS is discovered by using proprietary means. The Dh reference point is always used in conjunction with the Sh reference point. The protocol used in this reference point is based on DIAMETER. Its functionality is implemented by means of the routing mechanism provided by an enhanced DIAMETER redirect agent.

To get an HSS address, the AS sends to the SLF the Sh request aimed for the HSS. On receipt of the HSS address from the SLF, the AS will send the Sh request to the HSS.

### *2.3.9 Mm reference point*

For communicating with other multimedia IP networks, a reference point between the IMS and other multimedia IP networks is needed. The Mm reference point allows I-CSCF to receive a session request from another SIP server or terminal. Similarly, the S-CSCF uses the Mm reference point to forward IMS UE-originated requests to other multimedia networks. At the time of writing, a detailed specification of the Mm reference point has not been provided. However, it is very likely that the protocol would be SIP.

### *2.3.10 Mg reference point*

The Mg reference point links the CS edge function, MGCF, to IMS (namely, to the I-CSCF). This reference point allows MGCF to forward incoming session signalling from the CS domain to the I-CSCF. The protocol used for the Mg reference point is SIP. MGCF is responsible for converting incoming ISUP signalling to SIP.

### *2.3.11 Mi reference point*

When the S-CSCF discovers that a session needs to be routed to the CS domain it uses the Mi reference point to forward the session to BGCF. The protocol used for the Mi reference point is SIP. Section 3.13 contains further details about IMS-CS interworking.

### *2.3.12 Mj reference point*

When BGCF receives a session signalling via the Mi reference point it selects the CS domain in which breakout is to occur. If the breakout occurs in the same network, then it forwards the session to MGCF via the Mj reference point. The protocol used

for the Mj reference point is SIP. Section 3.13 contains further details about IMS–CS interworking.

### *2.3.13 Mk reference point*

When BGCF receives a session signalling via the Mk reference point it selects the CS domain in which breakout is to occur. If the breakout occurs in another network, then it forwards the session to BGCF in the other network via the Mk reference point. The protocol used for the Mk reference point is SIP. Section 3.13 contains further details about IMS–CS interworking.

### *2.3.14 Ut reference point*

The Ut reference point is the reference point between the UE and the AS. It enables users to securely manage and configure their network services-related information hosted on an AS. Users can use the Ut reference point to create public service identities (PSIs), such as a resource list, and manage the authorization policies that are used by the service. Examples of services that utilize the Ut reference point are presence and conferencing. The AS may need to provide security for the Ut reference point.

HTTP is the chosen data protocol for the Ut reference point. Any protocol chosen for an application that makes use of the Ut reference point needs to be based on HTTP. This reference point is being standardized in Release 6.

### *2.3.15 Mr reference point*

When the S-CSCF needs to activate bearer-related services it passes SIP signalling to the MRFC via the Mr reference point. The functionality of the Mr reference point is not fully standardized: for example, it is not specified how the S-CSCF informs the MRFC to play a specific announcement. The used protocol in the Mr reference point is SIP.

### *2.3.16 Mp reference point*

When the MRFC needs to control media streams (e.g., to create connections for conference media or to stop media in the MRFP) it uses the Mp reference point. This

reference point is fully compliant with H.248 standards. However, IMS services may require extensions. This reference point is to be standardized in Release 6.

### *2.3.17 Go reference point*

It is in operators' interests to ensure that the QoS and source and destination addresses of the intended IMS media traffic matches the negotiated values at the IMS level. This requires communication between the IMS (control plane) and the GPRS network (user plane). The Go reference point was originally defined for this purpose. Later on, the charging correlation was added as an additional functionality. The protocol used is the Common Open Policy Service (COPS) protocol. Go procedures can be divided into two main categories:

- Media authorization—as far as access is concerned, the Policy Enforcement Point (PEP) (e.g., GGSN) uses the Go reference point to ask whether a requested bearer activation can be accepted from the PDF that acts as a policy decision point. The PEP also uses the Go reference point to notify the policy decision point about necessary bearer modification and bearer releases (e.g., PDP context). As far as the IMS is concerned, the PDF uses the Go reference point to explicitly indicate when a bearer can or cannot be used; it may also request the PEP to initiate a bearer release. Media authorization is thoroughly explained in the context of the SBLP in Section 3.9.
- Charging correlation—via the Go reference point the IMS is able to pass an IMS charging identifier (ICID) to the GPRS network (user plane). In similar manner, the access network is able to pass a GPRS charging identifier to the IMS. With this procedure it is possible to later merge GPRS charging and IMS charging information in a billing system. This concept is further explained in Section 3.10.

### *2.3.18 Gq reference point*

When a stand-alone PDF is deployed the Gq reference point is used to transport policy set-up information between the application function and the PDF. The term “application function” is used because it is intended that a PDF could authorize other traffic than IMS traffic. In the IMS case the P-CSCF plays the role of an application function. This reference point is being standardized in Release 6.

The P-CSCF sends policy information to the PDF about every SIP message that includes an SDP payload. This ensures that the PDF passes the proper information to perform media authorization for all possible IMS session set-up scenarios. The

**Table 2.3** Summary of reference points.

Name of reference point	Involved entities	Purpose	Protocol
Gm	UE, P-CSCF	This reference point is used to exchange messages between UE and CSCFs	SIP
Mw	P-CSCF, I-CSCF, S-CSCF	This reference point is used to exchange messages between CSCFs	SIP
ISC	S-CSCF, I-CSCF, AS	This reference point is used to exchange messages between CSCF and AS	SIP
Cx	I-CSCF, S-CSCF, HSS	This reference point is used to communicate between I-CSCF/S-CSCF and HSS	Diameter
Dx	I-CSCF, S-CSCF, SLF	This reference point is used by I-CSCF/S-CSCF to find a correct HSS in a multi-HSS environment	Diameter
Sh	SIP AS, OSA SCS, HSS	This reference point is used to exchange information between SIP AS/OSA SCS and HSS	Diameter
Si	IM-SSF, HSS	This reference point is used to exchange information between IM-SSF and HSS	MAP
Dh	SIP AS, OSA, SCF, IM-SSF, HSS	This reference point is used by AS to find a correct HSS in a multi-HSS environment	Diameter
Mm	I-CSCF, S-CSCF, external IP network	This reference point will be used for exchanging messages between IMS and external IP networks	Not specified

Mg	MGCF → I-CSCF	MGCF converts ISUP signalling to SIP signalling and forwards SIP signalling to I-CSCF	SIP
Mi	S-CSCF → BGCF	This reference point is used to exchange messages between S-CSCF and BGCF	SIP
Mj	BGCF → MGCF	This reference point is used to exchange messages between BGCF and MGCF in the same IMS network	SIP
Mk	BGCF → BGCF	This reference point is used to exchange messages between BGCFs in different IMS networks	SIP
Mr	S-CSCF, MRFC	This reference point is used to exchange messages between S-CSCF and MRFC	SIP
Mp	MRFC, MRFP	This reference point is used to exchange messages between MRFC and MRFP	H.248
Mn	MGCF, IM-MGW	This reference point allows control of user-plane resources	H.248
Ut	UE, AS (SIP AS, OSA SCS, IM-SSF)	This reference point enables UE to manage information related to his services	HTTP
Go	PDF, GGSN	This reference point allows operators to control QoS in a user plane and exchange charging correlation information between IMS and GPRS network	COPS
Gq	P-CSCF, PDF	This reference point is used to exchange policy decisions-related information between P-CSCF and PDF	Diameter

---

media authorization concept is thoroughly explained in Section 3.9. The P-CSCF provides the following information to the PDF for each media component [3GPP TS 29.207]:

- Destination IP address and destination port number.
- Transport protocol ID (e.g., RTP).
- Media direction information (send, receive, send and receive).
- Direction of the source (originating or terminating side).
- Indication of the group that the media component belongs to.
- Media-type information (audio, video, etc.).
- Bandwidth parameters.
- Indication of forking/non-forking.

Additionally, the P-CSCF passes an ICID to the PDF when the ICID is received in SIP signalling or generated in the P-CSCF.

Similarly, the PDF sends an authorization token and GPRS charging identifier (GCID) to the P-CSCF. Section 3.9 explains further when an authorization token is generated and when the PDF receives the GCID from the GGSN.

At the time of writing, standardization of the Gq reference point was ongoing and therefore it is subject to further changes.