

CSCF Technical Description

Call Session Control Function

TECHNICAL PRODUCT DESCRIPTION

Copyright

© Ericsson AB 2016–2019. 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
2	Overview	3
2.1	Sensitive Business Information	3
2.2	CSCF Roles	4
3	CSCF Architecture	11
3.1	Network View	11
3.2	CSCF Modules	13
3.3	Architecture View	14
3.4	VNF Deployment	17
3.5	Availability and Robustness	18
3.6	Infrastructure	19
3.7	Scalability	19
3.8	Network Infrastructure and Resources	20
4	Main Functionality and Features	21
4.1	Identity and Addressing	21
4.2	Authentication	22
4.3	Registration	24
4.4	SIP Routing and Traffic	30
4.5	Wi-Fi Calling	44
4.6	Service and Application Invocation	44
4.7	Enterprise	48
4.8	Authorization	49
4.9	Distribution Control	51
5	Charging	55
5.1	General	55
5.2	Offline Charging	57
5.3	Online Charging	58
6	Life Cycle Management	61
6.1	Onboarding	63
6.2	Instantiation	63



6.3	Termination	64
6.4	Managed Scale-Out	64
6.5	Managed Scale-In	64
6.6	Time-Based Auto Scaling	64
6.7	Auto Healing	64
7	Security	67
8	Operation and Maintenance	69
8.1	Fault Management	69
8.2	Performance Management	69
8.3	Configuration Management	70
8.4	Software Notification	70
8.5	Traceability and Troubleshooting	71
9	Interfaces and Protocols	73
10	Reference Configuration and Cloud Enabled	77



1 Introduction

This technical product description describes the Ericsson Virtual Call Session Control Function (vCSCF).

Note: In this description, the term “vCSCF” refers to the product, and the term “CSCF” refers to the CSCF application.

The vCSCF product is a software-only product. It is not bundled with any hardware platform or virtualization software.

When deployed over a virtualization layer (typically included in a Cloud Execution Environment (CEE)), it is possible to deploy the CSCF application over any hardware such as the Ericsson Blade Server Platform (BSP) or any Commercial Off-The-Shelf (COTS) hardware. Contact Ericsson for further details.

The CSCF is integrated and verified using a reference configuration constituting of Ericsson CEE and BSP 8100. This documented solution is referred to as vCSCF Cloud Enabled.

The CSCF is based on the 3GPP®-defined IP Multimedia System (IMS) architecture. The Session Initiation Protocol (SIP), IETF SIP [RFC 3261](#), is used as the signaling protocol for establishing, terminating, and modifying a multimedia session.





2 Overview

The CSCF is an essential module in the IMS for processing signaling, using SIP as the signaling protocol. It supports Internet Protocols on a scalable and high-performance platform.

The CSCF handles session establishment, modification, and release of Internet Protocol (IP) multimedia sessions using the Session Initiation Protocol/Session Description Protocol (SIP/SDP) suite.

The CSCF has the following different roles in the network:

- Interrogating Call Session Control Function (I-CSCF)
- Serving Call Session Control Function (S-CSCF)
- Emergency Call Session Control Function (E-CSCF)
- Breakout Gateway Control Function (BGCF)
- Break-In Control Function (BCF)
- Emergency Access Transfer Function (EATF)

These logical entities are designed to execute traffic in either collocated or standalone mode, based on the network configuration.

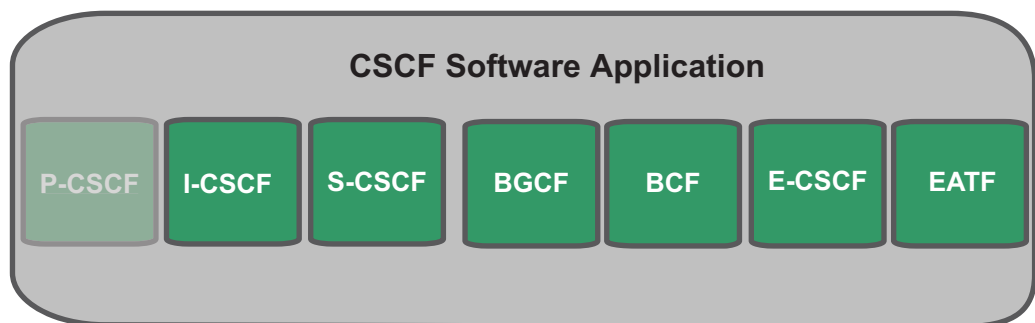


Figure 1 CSCF Logical Structure

Note: The Proxy Call Session Control Function (P-CSCF) is not part of the CSCF product.

2.1 Sensitive Business Information

This section describes the Communication Content Inspection (CCI) and the Deep Package Inspection (DPI).

The CSCF inspects sensitive information such as IP address, SIP URI (private and public), and telephone number. Most of the inspected information is used for call routing purposes in stateless and stateful mode.

In stateful mode, the inspected data, including the sensitive data, is stored in the internal database in RAM. A limited amount of inspected data, including the sensitive data, is stored temporarily internally on a Persistent Storage disk, or on a Shared Storage in the cloud Storage Area Network (SAN), for later restoration.

The inspected data, including the sensitive data, is also forwarded to trusted and non-trusted Network Elements (NEs), depending on the CSCF network configuration.

2.2 CSCF Roles

3GPP TS23.228 describes the logical modules P-CSCF, I-CSCF, S-CSCF, E-CSCF, EATF, and BGCF. Also, the BCF function is defined briefly in this document.

3GPP TS 23.237 describes IMS Service Continuity, which covers the logical module of EATF in the CSCF.

The BGCF is called from the CSCF when a message is to be routed outside the IMS network. The BGCF never acts in an own role, it is used as an extension to the CSCF.

Configuration parameters in the CSCF define if a function is to be used separately or combined. Even though the functions are configured as combined, the CSCF can take different roles depending on the traffic case and on the network topology.

2.2.1 Proxy Call Session Control Function

The P-CSCF is the first contact point within the IMS. Its address is discovered by the User Equipment (UE) using a P-CSCF discovery mechanism.

The P-CSCF functionality that Ericsson offers is implemented by the Session Border Gateway (SBG) product. The references to P-CSCF in the figures of this document are part of the SBG product. For more information, see the SBG CPI.

2.2.2 Interrogating Call Session Control Function

The I-CSCF is the contact point within a network of an operator for all connections destined to a user of that operator. The I-CSCF conforms to 3GPP TS 24.229 and supports the SIP proxy behaviors as defined in SIP [RFC 3261](#).

The I-CSCF has the following functions:

- Assigns an S-CSCF to a registration request from a user.
- Assigns an S-CSCF to handle a request for an unregistered user.
- Obtains the S-CSCF address from the Home Subscriber Server (HSS) for a registered user.



- Routes SIP messages from another network to the S-CSCF.
- Routes SIP messages to Application Servers (ASs) directly if subdomain-based routing function is started.
- Handles transit interconnection between networks.
- Handles Local Zone Policy to select only S-CSCFs included in its local zone for optimized Failover Recovery.
- Handles Onward Routing (OR), which means that Number Portability lookup is performed by the terminating I-CSCF.
- Implements the Dynamic User Association Router (DUA-R) part of the Dynamic User Identity Support (DUIS) solution by mapping the external identity of the Wholesale Partner (WP) user to the IMS internal identity for terminating request.
- Redistributes registered IMS users from their current S-CSCF to the preferred S-CSCF after a previously failed S-CSCF is back in service, or after a change in the topology, for example, when a new S-CSCF node is added to the IMS network.

The I-CSCF does not retain any session or registration state information. Multiple I-CSCFs can exist concurrently in a network of an operator.

2.2.3 Serving Call Session Control Function

The S-CSCF conforms to 3GPP TS 24.229 and performs the session control services for the UE. It maintains a session state for support of the services.

The S-CSCF has the following functions:

- Acts as a registrar according to [RFC 3261](#) at registration.
- Notifies subscribers about registration changes.
- Session control for the sessions of the registered user.
- Handles SIP requests and services them internally or forwards them on.
- Interacts with the ASs.

2.2.4 Breakout Gateway Control Function

The BGCF is used to select an outgoing gateway for a SIP request addressed to a telephone.

The BGCF complies with the 3GPP specification. It is the logical entity within the IMS network that manages the sessions initiated in the IMS network and terminated other non-IMS networks. The non-IMS networks can be Circuit

Switch (CS) networks such as Public Switched Telephone Network (PSTN) or other wireless networks.

The CSCF forwards the SIP request to a gateway; a Media Gateway Control Function (MGCF) for calls to the PSTN or a Session Border Controller (SBC) for calls to an H.323 network or other IMS networks.

The BGCF has the following features:

- Supporting break-out

It can send traffic to one out of several gateways that are defined, which is determined as a result of routing analysis in the break-out table. Extra Route headers can be added to the outgoing request to specify a specific path through the network.

- Gateway redundancy

If failed communication with a Breakout Gateway, the BGCF is able to pick another gateway.

The BGCF is a logical software implementation in the CSCF module.

The routing analysis options and selection of the outgoing gateway can be based on the following:

- Request-URI

Any information in the Request-URI, for example, telephone number of the called user, Carrier Identification Code (CIC), Routing Number (RN).

- Any standalone SIP request headers

Any information in the SIP request headers, for example, SIP method type, event and P-Access-Network-Info (PANI), P-Asserted-Identity.

- Media type in the SDP

Routing can be based on media type, for example, audio, video, that is included in the SDP.

- Coordinated Universal Time (UTC) Date information

Routing can be scheduled to be active at a certain date.

- UTC Time Information

Routing can be scheduled to be active at a certain time.

- Weight

Routing can be weighted for random but proportional routing.



The BGCF function routing logic is defined by configuring tables that correspond to the matching protocol elements, so that routing analysis can be done on the information in the received SIP request. Included protocol elements can be Request-URI information, standalone SIP headers, and SDP-media information.

The BGCF can be configured to modify the Request-URI and add SIP headers into the requests before the SIP request is routed further on.

The protocol elements are defined by table types. Also, they can be combined with operator-configured tables for UTC criteria that are configured for routing analysis based on time or date.

For the operator, the possibilities to control routing decisions are also supported by functions to use Regular Expression (RegEx) for routing analysis matching.

The routing analysis can start with any table and the operator can configure the order of sequence.

A table normally has several rows, and each table type has a “table row selection function” to select the most suitable row using the input protocol elements.

The result of the table row selection can be as follows:

- Next Table

The table navigation function continues with the identified table instance. The next table can be another instance of the same table type or an instance of another table type.

- Pool instance

The result of the table navigation function is an entry in the Pool Table. The pool entry contains either a target SIP URI or a response code and reason phrases to be used in a SIP error response.

The total sum of all the entries in all types of tables can be up to 500 000.

The BGCF supports the function to have an active and passive configuration that minimizes traffic disturbances when modifying configuration data in the passive area, and by that giving the operator the planning and preparation possibility before activating it. The switch-over from passive to active is made through a command.

The BGCF supports Crankback, which means that when there is an error or congestion from the remote Gateway, the BGCF can reselect alternative routes to reach the destination.

2.2.5

Break-in Control Function

The BCF gives the possibility for users connected to other networks to execute originating IMS services.

The BCF can be collocated with other CSCF applications. It is used when an incoming call is received from other networks (H.323, PSTN/PLMN), through a gateway.

The BCF queries the HSS to determine if the calling user is served by this IMS domain. If the calling user is served by this IMS domain, the SIP message is processed further. Otherwise, the SIP message is rejected.

The BCF does not store any SIP dialogue information, so the BCF does not Record-Route and therefore does not receive any subsequent requests within the SIP dialogue. There is no time supervision of the dialogue in the BCF.

The calling user uses the BCF for INVITE dialogues only. Other initial SIP requests than INVITE are rejected.

To register the other network users, a Registration Surrogate (RS) is used. An RS keeps registrations for other network users IDs (telephone numbers, MSISDN, SIP URI, or H.323 user IDs). The RS fetches the Public User ID and contact information for all users defined from the common directory, and then registers all these users with the CSCF using normal SIP user behavior. For the CSCF, the calling party is identified as the RS.

2.2.6 Emergency Call Session Control Function

The E-CSCF handles emergency calls according to 3GPP. It can be collocated with the other CSCF applications. If collocated, the E-CSCF communicates with the other CSCF applications through SIP signaling.

To select the Public Safety Answering Point (PSAP), the E-CSCF obtains the PSAP address using a HTTP/SOAP/XML[®] or SIP interface (MI) to the PSAP selection database, located in the Routing Determination Function/Location Retrieval Function (RDF/LRF). The HTTP version of this interface supports HTTP Digest Authentication.

The E-CSCF can handle emergency calls with a telephone number or with an emergency service Uniform Resource Name (URN) in the Request-URI from a registered user, emergency registered user, or non-registered user.

As part of emergency call situations, the E-CSCF supports the standard 3GPP procedures for the LRF to monitor the state of individual emergency calls. This can be achieved through dialog event subscription on individual dialogs from the LRF to the E-CSCF.

The E-CSCF is not aware of registration or barring state, and does not trigger any services for the user. Furthermore no authentication of the user is performed unless the user performs emergency registration.

For a Voice over LTE (VoLTE) emergency call, with Single Radio Voice Call Continuity (SRVCC) support, the E-CSCF forwards the VoLTE emergency call request to the EATF using a configured address at the E-CSCF.



For charging related information, the EATF adds the original IMS Charging Identifier (ICID) value in the P-Charging-Vector to the request to be included by the E-CSCF when generating charging information.

2.2.7 Emergency Access Transfer Function

The EATF provides IMS-based mechanisms for enabling VoLTE Single Radio Voice Call Continuity (SRVCC) in emergency call sessions. It is a function in the serving (visited if roaming) IMS network, providing the procedures for IMS Emergency Session Anchoring and Packet Switched (PS) to Circuit Switched (CS) Access Transfer.

Compliant to 3GPP 24.237, the EATF is implemented as a routing Back-to-Back User Agent (B2BUA) for coordinating the call legs (PS call leg, PSAP call leg, and CS call leg) involved in a VoLTE emergency call session and access transfer function.

The EATF identifies the VoLTE sessions by IMEI-based +sip.instance or C_MSISDN in the request.

The EATF acts as a stateful signaling reference point (anchor point) in the IMS network for the VoLTE emergency calls and it is involved in the following use cases:

- VoLTE emergency call establishment
- VoLTE emergency call transfer to CS
- PS fallback to VoLTE emergency call
- Refresh of VoLTE emergency call
- Cancellation of VoLTE emergency call
- Termination of VoLTE emergency call

Dynamic Payload Types Mapping support is a function of the EATF to detect differences between the payload types used in the access transfer request and the initial call establishment. If there is a conflict, the EATF rejects the access transfer request with 488 responses including the stored SDP of the established emergency call session. The CS UE sends a new access transfer request with the SDP provided in the 488 response.

The EATF can be collocated with the E-CSCF and deployed together. The EATF can be deployed redundantly in the IMS network.

If a primary EATF goes down, a secondary EATF takes over and anchors new emergency sessions until the primary EATF comes back to service.



2.2.8 CSCF Node Deployment

For information regarding the supported CSCF commercial node deployments, see CSCF Product Package Description, 221 03-FAP 130 4331.

3 CSCF Architecture

3.1 Network View

The CSCF is one of the core modules in the IMS System. The IMS architecture and how the CSCF fits in the IMS network is shown in Figure 2.

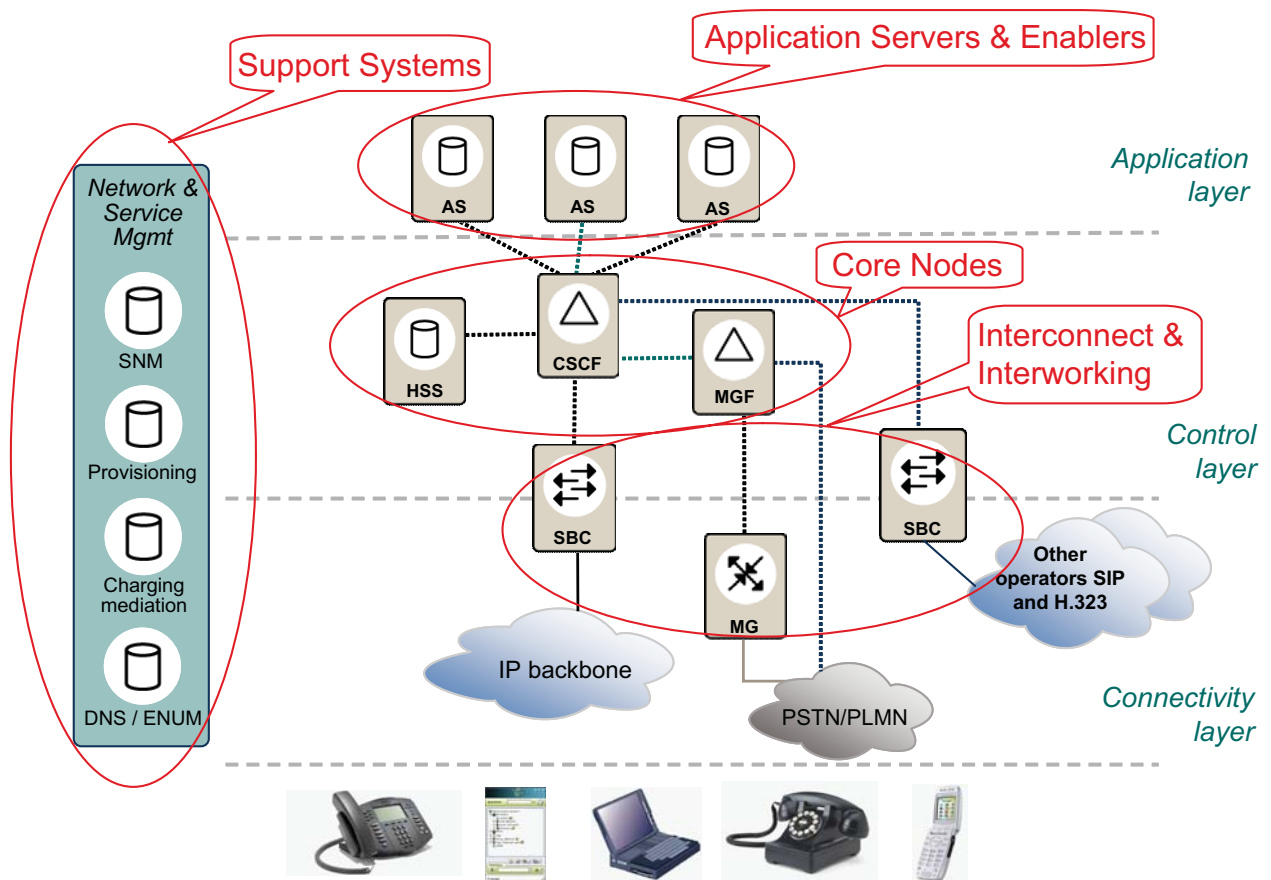


Figure 2 IMS Architecture

The CSCF implements the following 3GPP functional CSCF modules and can act as any of them:

- I-CSCF
- S-CSCF
- E-CSCF
- EATF

The CSCF also implements the following logical functional modules:

- BGCF
- BCF

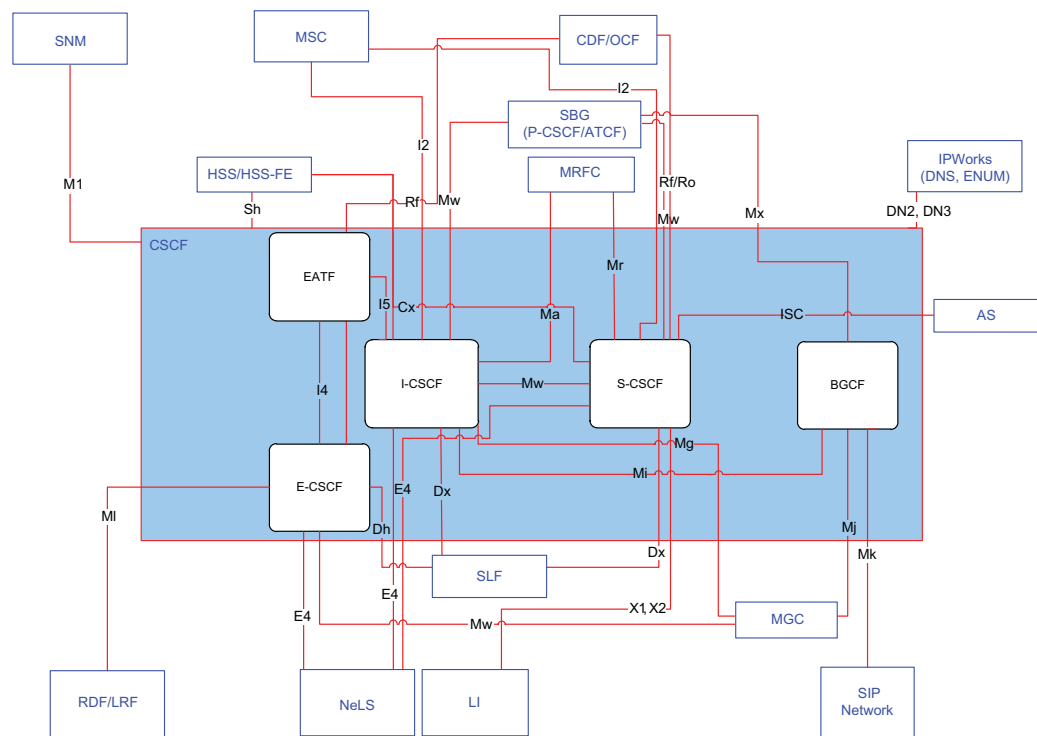


Figure 3 CSCF Architecture and Interfaces

Note: The P-CSCF is not part of the CSCF product. The P-CSCF functionality for the Ericsson offering is implemented in the SBG product.

The Cx interface supports extended functionality compared to the standard. This enables the CSCF to support extra (proprietary) features when the CSCF is deployed in a solution including an Ericsson HSS. Examples of this functionality are Roaming Awareness and Control of Max Number of Contacts.

The BCF (logic is not visualized in the picture) has the same interfaces as the I-CSCF except the following:

- The BCF only accepts the originating INVITE method (no other method supported) from a Media Gateway Controller (MGC) that is typically connected to a PSTN/ISDN network. So, the BCF is not interfacing the P-CSCF.

The MI interface between the S-CSCF and BGCF is an internal interface. Multiple CSCF modules can exist concurrently in a network of an operator.

The E4 Interface is an Ericsson proprietary interface used by the vCSCF License Management client and the Network License Server (NeLS) node. A NeLS node is a license storage and management solution that is running outside the application



environment. A NeLS node must be deployed in the customer network which must be configured with a License Key File for the required licenses, for example, Multi-Device or Wi-Fi Calling.

3.2 CSCF Modules

A CSCF module can communicate with any other CSCF module either externally or internally. The signaling between the CSCF logical functional modules, collocated in the same NE, uses internal signaling instead of external SIP signaling.

Note: The P-CSCF is not part of the CSCF product. The P-CSCF functionality for the Ericsson offering is implemented in the SBG product.

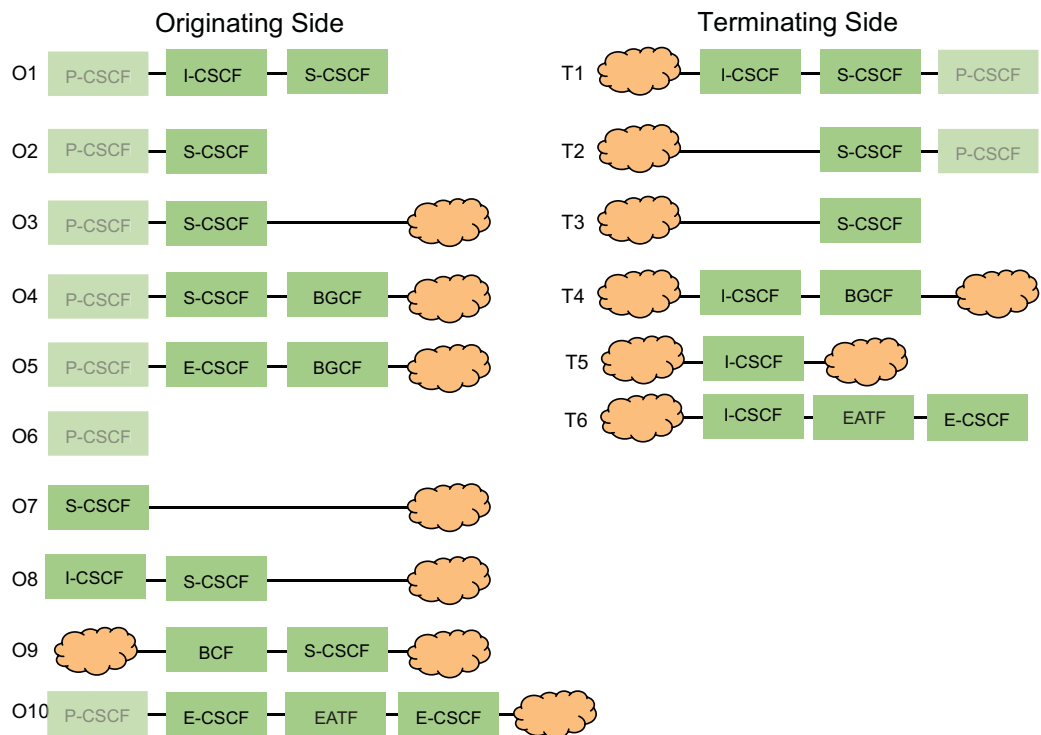


Figure 4 Interaction of CSCF Modules

- O1 During the REGISTER transactions for initial registration, re-registration, and de-registration.
- O2 All non-REGISTER SIP transactions, where either the S-CSCF or an AS acts as User Agent Server (UAS) (for SUBSCRIBE only valid if the S-CSCF is configured to stay within the dialog).
- O3 During a SIP transaction within an INVITE dialog, when the called party is located in an IMS network.
- O4 During a SIP transaction within an INVITE dialog, when the called party is located in a non-IMS network.

- O5 During a SIP transaction within an INVITE dialog with an emergency number destination.
- O6 During an initial SIP transaction within a SUBSCRIBE dialog, where the S-CSCF does not stay within the SUBSCRIBE dialog.
The P-CSCF is not included in CSCF product.
- O7 During a SIP transaction for originating Call Out Of the Blue (COOB), the AS acting as a User Agent Client (UAC).
- O8 During a SIP transaction for COOB, when the S-CSCF location is unknown to the AS.
- O9 A break-in call (an INVITE), that is, the user connects through an External Network and the services of the user are executed in IMS.
- O10 During an emergency session setup, the INVITE, initiated from a VoLTE access network, reaches the E-CSCF the same way as a normal emergency request reaches the E-CSCF, and makes it possible to handle traffic case T6.
- T1 During an initial SIP transaction, where the destination is a user agent in a UE.
- T2 During a SIP transaction within an INVITE dialog, where the destination is a user agent in a UE.
- T3 During a SIP transaction within a SUBSCRIBE dialog, where the S-CSCF is configured to stay within the SUBSCRIBE dialog.
- T4 During a SIP transaction (non-REGISTER) requiring break-out to a non-IMS network (applicable for Number Portability and transit).
- T5 For SIP to SIP transit call where HSS user lookup is not performed.
- T6 The I-CSCF forwards the INVITE to the EATF. The EATF finds PSAP call leg information and updates the PSAP call leg with the CS call leg information.

3.3 Architecture View

The vCSCF is a software-only product and it is a Virtual Network Function (VNF) as defined in the ETSI Network Functions Virtualization (NFV) specification. The relationship between the vCSCF and the ETSI NFV is outlined in Figure 5.

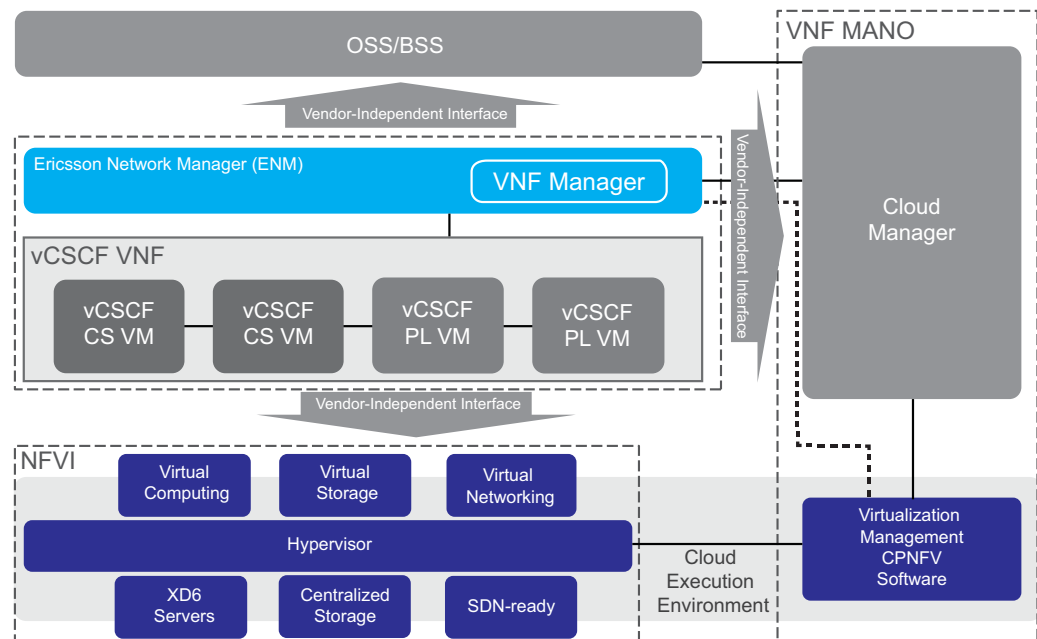


Figure 5 Outline of the Relationship between the vCSCF and the ETSI NFV

The vCSCF is not bundled with any hardware platform or virtualization software. When deployed over a virtualization layer (typically included in a CEE), it is possible to deploy the CSCF application over any hardware such as the Ericsson BSP or any COTS hardware. The O&M of the hardware platform and the virtualization layer are not included in the CSCF product.

The CSCF VNF is verified on a reference configuration constituting of Ericsson CEE and BSP 8100. This documented solution is referred to as vCSCF Cloud Enabled. See Section 10 on page 77 for more information on Cloud Enabled and the reference configuration used for verification.

The simplified internal architecture used to implement the CSCF functionality is described in Figure 6. This architecture allows for a great flexibility in obtaining physical modules by combining (collocating) various logical entities.

In the architecture, the SIP Stack component groups the entire SIP-related functionality as specified by [RFC 3261](#). The S-CSCF, I-CSCF, E-CSCF, EATF, and BGCF components implement the 3GPP-specific functionality of the respective logical entities. ASs can be accessed through the ISC interface.

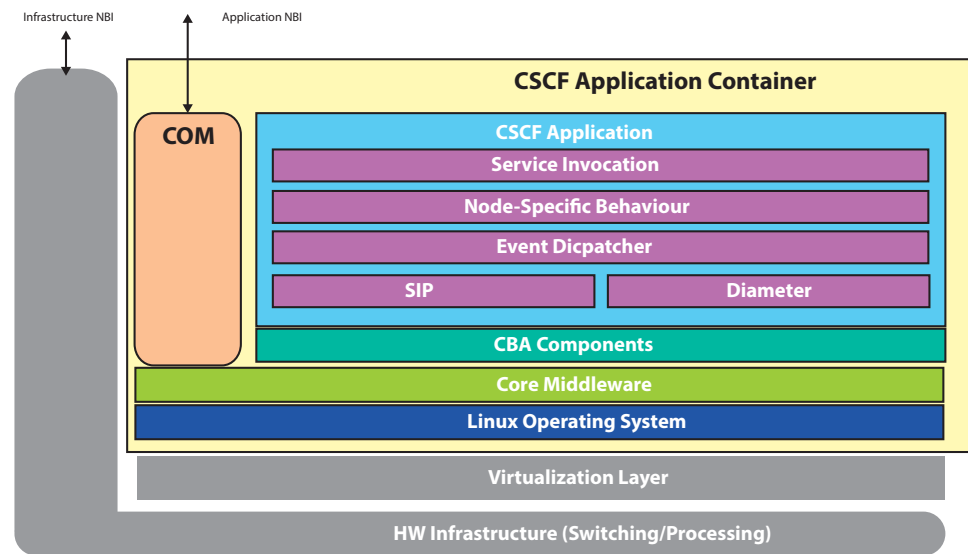


Figure 6 Simplified CSCF Logical Structure

The following is a description of the simplified internal architecture:

- The Service Invocation module is responsible for starting services that can be executed on an external SIP AS. The invocation is based on end user-specific SIP message filters.
- The Node-Specific Behavior module contains the functionality for the particular type of CSCF logic. This module incorporates SIP Proxy Server, Redirect Server, or User Agent behavior as dictated by standards.
- The Event Dispatcher module interacts with the specific SIP and Diameter events to process and serve it to the proper destination.
- The SIP stack module handles sending and receiving, construction, and parsing of SIP messages on the network.
- The Diameter stack module handles sending and receiving, construction, and parsing of Diameter messages on the network interfaces provided by the Application Support component. Diameter is also used for sending charging data.

The CSCF application container is built using the Component Based Architecture (CBA). This architecture is used in other Ericsson applications and therefore provides flexibility and standardized Northbound Interfaces (NBIs) for all these applications.

The CBA consists of several software common components providing various system functions needed by the CSCF application.



The two most central components are the Common Operation and Maintenance (COM) component and the Core Middleware (Core MW) component as follows:

- COM is a component that presents the NBIs of the CSCF application to the Network Management System. The application interfaces COM through the middleware. It provides the Operation and Maintenance. All the modules contained within the actual CSCF application interact with the COM component. The Operation and Maintenance (O&M) of the CSCF application is decoupled from O&M of the hardware infrastructure.
- Core MW is the open Service Application Framework (SAF) based middleware component of CBA, responsible for the Virtual Machine (VM) clustering functionality.

The remaining CBA components include an execution environment, an object-oriented distributed database, security functions, software management functions, O&M functions, and network and transport protocol support. High Availability of the application is supported by the intra-cluster communication of the layer and inter-processor boards communication function.

The operating system for the CSCF application consists of a Linux® distribution and the Linux Distribution Extension (LDE).

3.4 VNF Deployment

The vCSCF is delivered as a site-independent image using environment properties for site-specific data.

To support different cloud execution environments, the following different packages are available:

- A TAR file containing HOT files, a HOT environment file, and a qcow2 disk image.
- An OVA package containing a disk image in Stream-optimized VMDK format and an OVF 1.1 file.

The CSCF VNF consists of several VMs: Two instances of System Controllers (SC) VMs and two or more instances of Payload (PL) VMs depending on the capacity that is needed, see Figure 7.

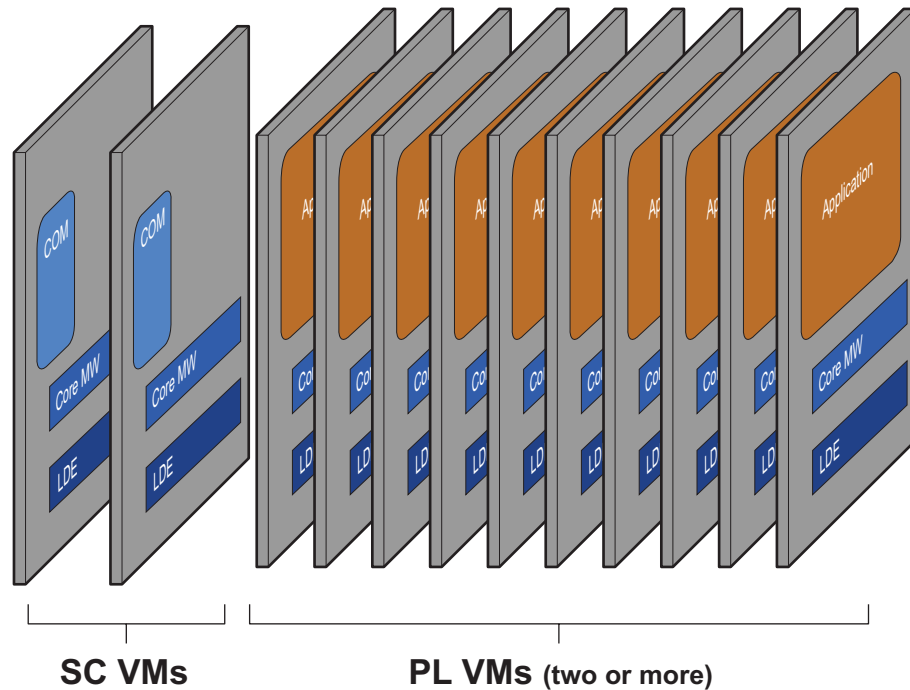


Figure 7 CSCF VNF Deployment

The PL VMs are clustered to achieve carrier grade availability and robustness by having 1+1 replication of user and session data. By doing so, a PL VM failure does not cause traffic disturbance. The PL VMs provide all the SIP and Diameter traffic-related functionality of the CSCF VNF. In the VNF, there is also a distributed load balancer function to guarantee load distribution on the PL VMs.

The CSCF VNF is managed as a cluster of PL VMs by the SCs. O&M access is through the NBI to the SC VMs, which is offering aggregation services and a unified view of the VNF towards the Network Management System.

The SC VMs, deployed in 1+1 configuration, provide administration, O&M, and aggregation functionalities for the CSCF VNF. It is an Active-Standby setup, which means that only one of the SC VMs is active at a time.

3.5 Availability and Robustness

The CSCF achieves High Availability and robustness through the cluster deployment. The main functionality of this solution can be summarized as follows:

- Automatic software recovery
- Data replication
- Overload Protection



- Load regulation
- Software updates during operation
- Upgrade of Operating System during operation
- Online backup
- Failover mechanism when a PL VM goes down

3.6 Infrastructure

The CSCF is agnostic of the cloud infrastructure and is verified in different environments, such as OpenStack® and VMware®. To reach telecom-grade availability and redundancy, the requirements of the underlying infrastructure regarding compute, networking, and storage are defined. These requirements are implemented by following configuration guidelines and are verified in the different reference configurations that are available. If the CSCF is deployed in another environment, it must be secured that the infrastructure meets these requirements.

For networking, the recommended deployment is to use Static routing with High Availability and without Bidirectional Forwarding Detection (BFD) towards the VNF. An alternative is to support a deployment without BFD or OSPF. With the alternative, the CSCF can be deployed with fewer requirements on the infrastructure and meet requests for having different routing strategies.

It is recommended to keep multiple CSCF instances in a customer deployment to secure the possibility of redundant network upgrades.

3.7 Scalability

The CSCF has been designed with scalability in mind, ensuring that the initial investment suits customer needs, and that the system can grow with the business. The modular software architecture facilitates rapid expansion of capacity when and where needed.

The CSCF VNF supports manual scaling in and scaling out by removing PL VMs from or adding PL VMs to the VNF, without traffic disturbance.

The VNF can be scaled out with new PL VMs which have the same number of virtual cores, RAM memory, and number of ports as the existing PL VMs in the cluster. When a new VM is available, the VNF populates the new VM with the necessary software, and includes it in the cluster. Scale-in is triggered from the NBI. The VNF initiates redistribution of replicated data to avoid data loss before the VM is terminated.

Time-based auto scaling is supported for Open Stack Environment.



3.8 Network Infrastructure and Resources

The CSCF VNF is a software-only product that can be deployed on several software and hardware infrastructures. To enable a commercial carrier grade deployment of the CSCF VNF, certain requirements on the minimum compute, storage resources needs, and on the network infrastructure needs must be fulfilled by the hardware and the Network Functions Virtualization Infrastructure (NFVI).

To ensure that these requirements are fulfilled, run a system integration project for the deployments diverging from the vCSCF reference configuration.



4 Main Functionality and Features

In this technical product description, a first level of technical detail is provided. Detailed information can be found in the Customer Product Information (CPI) of the product and in the Lighthouse tool (formerly known as Feature Store).

4.1 Identity and Addressing

In an IMS network, a called user is addressed using SIP addresses rather than ordinary phone numbers. If the calling users still use phone numbers, these numbers are translated to SIP URI by the CSCF by interaction with the DNS/ENUM database already on the originating network side. In case the translation fails (there was no entry in the DNS/ENUM), the call is routed to the PSTN or PLMN network through the external routing table.

If the CSCF receives a SIP request containing the parameter `user=phone`, or a tel URI, in the Request-URI, the CSCF tries to look up number to translate it into SIP URIs. If the number cannot be translated, it is routed on the tel number using BGCF.

The CSCF supports a model in which subscribers can have one or more Public User Identities where they can be reached on. The identities can be grouped into Implicit Registration Sets (IRS), which increase the user experience and limit the network traffic as several public identities can be registered or de-registered with just one single registration procedure.

The CSCF supports distinct Public Server Identities (PSI) and Wildcarded Public Service Identities (wPSIs). The PSI can either be provisioned in the HSS as a PSI user or configured in the I-CSCF as subdomain-based PSI. A PSI is used to identify services or user groups.

The CSCF supports Wildcarded Public User Identities (wIMPUs). A wIMPU represents a collection of Public User Identities that are registered from a single identity. This concept is used in an Internet Protocol Private Branch Exchange (IP-PBX) deployment where the registration is performed by IP-PBX on behalf of all its users. The IP-PBX users are then able to initiate and receive multimedia sessions.

The CSCF supports Identity convergence, which enables that multiple devices can use same Public User Identities. In addition, the CSCF supports deployments where one terminal can be used over different access network types, having the same identity and authentication credentials.

The CSCF supports Public Globally Routable User Agent URI (GRUU) as specified in 3GPP TS 24.229. A GRUU is an identity that identifies a unique combination of IMPU and sip instance. GRUU is designed to implement reliable routing to a specific device for an end user. While a SIP URI, such as `sip:bob@example.com`, is a URI that refers to a user, GRUU is a URI that refers to a specific device.

This functionality is used in solutions where multiple devices are deployed and messaging to one specific device is required, for example, RCS.

4.2 Authentication

The purpose of authentication is to ensure that the user accessing the network is authorized, by that preventing fraudulent users to use the network. The network authentication provides means to ensure that the network providing the access is the correct one and not a fake network.

4.2.1 NASS Bundled Authentication

NASS Bundled Authentication (NBA) is the standardized IMS authentication procedure for wireline networks. It allows secure authentication for any type of terminals.

The authentication procedure for wireline networks can be configured to use NBA. The CSCF compares the line identity retrieved from the terminal with the value retrieved from the HSS. This means that no password handling is needed.

If the UEs are only allowed to get access from defined Access Points, the locations are provisioned in the user profile. The properties of the access locations are called Line Profiles. The access network information is included by the P-CSCF and sent to the HSS through the S-CSCF.

4.2.2 IMS AKA Authentication

The IMS Authentication and Key Agreement (AKA) function provides mutual authentication between UE and the IMS network based on the secure AKA protocol and the USIM and ISIM of the user.

The IMS AKA authentication scheme is based on 3GPP TS 33.203.

The IMS AKA is used when a registering UE requests to use it.

The UE and the HSS share a secret key to perform the AKA authentication. The S-CSCF requests the HSS for the authentication vectors for the AKA and uses the vectors to challenge the user.

The S-CSCF allows only one contact per UE to be authenticated using AKA authentication for regular registration. The S-CSCF allows AKA authentication of an extra contact for emergency registration.

4.2.3 Digest Authentication

The Digest Authentication scheme is based on IETF [RFC 3261](#), IETF [RFC 2617](#), 3GPP TS24.229 R8, and TS33.203. The configuration determines which SIP requests are authenticated.



The Digest Authentication is password-based and available for fixed and mobile accesses. The UE and the HSS share a secret key to perform Digest Authentication. The S-CSCF requests the HSS for the authentication vectors for digest and uses the vectors to challenge the user.

It is possible to configure the number of allowed authentication attempts. When a user fails the password authentication for a configurable number of times, the user is blacklisted and subsequent attempts are rejected for a configurable period.

3GPP mandates that for digest authentication, the UEs include an Authorization header in the first REGISTER request. However, non-3GPP compliant UE only includes the Authorization header in the second round REGISTER request. The S-CSCF provides extra digest authentication support for this type of UE.

3GPP mandates that the Private User Identity of the UE used for digest authentication takes the form of a Network Access Identifier (NAI) with the specific form of `username@realm`. However, non-3GPP compliant UE does not include the realm as part of the digest username. The S-CSCF provides extra digest support for this type of UE.

4.2.4 Optimized Digest Authentication

This digest authentication mechanism authenticates the user using digest authentication at the initial registration. After the initial authentication, no subsequent authentication is performed for the user during the session, except checking and verifying the IP address of the user by the S-CSCF.

If the S-CSCF determines that authentication of the signaling traffic is no longer secure, it reauthenticates using the digest mechanism.

4.2.5 IMS-Single Sign On

The IMS-Single Sign On (IMS-SSO) relies on the access network authentication (that is, GPRS/WCDMA/CDMA authentication). The security is comparable to the security in the access network.

Note: Anti-spoofing mechanisms are required in the access network.

The standardized security solution that is used is GPRS IMS Bundled Authentication (GIBA). GIBA is applicable only for mobile terminals.

The IMS-SSO GIBA security solution works by creating a secure binding in the HSS between the Public/Private User Identity (SIP-level identity) and the IP address currently allocated to the user at the GPRS level (bearer/network level identity). Therefore, IMS level signaling, and especially the IMS identities claimed by a user, can be connected securely to the PS domain bearer level security context.

The S-CSCF performs GIBA authentication of initial registration and subsequent SIP requests. At reception of initial registration, the S-CSCF compares the UE IP

Address Information received in initial registration request in the Via header to the UE IP address received from the HSS.

The SSO process can be split into the following steps:

- 1 User authentication in the IP access network.

The access servers in the IMS system are represented by the Gateway GPRS Support Node (GGSN) (in GPRS networks), the PDSN (in CDMA networks), or by a general Network Access Server.

The IP address of the assigned user is used as the trusted token used to check the user authentication status. Therefore, the access servers must guarantee that the IP address is trusted enough for the HSS to consider it suitable for authentication purposes.

- 2 User access to the services.

The CSCF sends the received IP address to the HSS. The HSS then compares the IP address with the received one from the access network.

- 3 Non-initial registration.

At subsequent registrations, the CSCF checks that the received IP address matches the IP address that was validated at the initial registration.

The SSO session can be terminated by the HSS initiating a user profile update request to the S-CSCF that annuls the authenticated IP address.

4.3 Registration

The Registration functions allow a user to register (log on) or de-register (log off) with the network and is a requirement for allowing the user to initiate and receive SIP sessions (as well as sending and receiving standalone requests).

The functions also allow the operator to authorize the user to register or not in the network and determines if the user is allowed to use the services of the operator.

Deregistration can be initiated both by the user and the network.

4.3.1 User-Initiated Registration/Deregistration

Each user has one Private User Identity and one or more Public User Identities. Each Public User Identity can be registered from several user devices. That allows more than one contact address to be connected to the same Public User Identity. Each user is connected to a subscription. A subscription includes more than one user. A Public User Identity can be shared between several users within one subscription.



Registration is a common operation in SIP, providing the system with UE information such as contact address and current location of a user. Upon initialization, and at periodic intervals, the SIP client of the user sends SIP REGISTER requests to the home domain.

Registration always relates to a particular contact address and one or more Public User Identities. Each registration request only allows one contact at a time to be added to the Public User Identity. Registration of multiple contacts requires multiple registrations. The maximum limit of the total number of contacts per Implicit Registration Set (IRS) can either be provisioned on user level (if supported by the HSS), and downloaded to the CSCF, or locally in the CSCF.

The CSCF also uses the `+sip.instance` feature tag to identify a specific contact. The value of `+sip.instance` is a unique value in the Contact header field that uniquely identifies the device. The CSCF handles contacts with the same contact URI but different SIP instance id as different contacts.

For devices that do not send the sip instance feature tag, the CSCF Network Provided Terminal Identity (NPTI) function generates a sip instance feature tag in the Contact header, with Universally Unique Identifier (UUID) based on [RFC 4122](#), on behalf of the UE.

To de-register one or more contacts, the user sends a SIP REGISTER request where the Expires header field or the Expires parameter in the Contact header field equals the value zero. When handling a user initiated deregistration, the S-CSCF follows the behavior described in TS 24.229, that is, the de-registered contact is always included in the 200 (OK) response to the REGISTER.

The user can de-register any of its currently registered contacts or all. A Public User Identity is de-registered from the network when the last contact associated with the Public User Identity has been de-registered.

Under the condition that the P-CSCF adds the Service Route into a Route header in the re-REGISTER request, the I-CSCF can bypass the HSS, and send the re-REGISTER request directly to the S-CSCF. The S-CSCF can then bypass the authentication when there is no contact with the HSS. This functionality is On/Off configurable.

Emergency registration is a requirement for VoLTE deployments where the emergency calls are carried on a separate emergency bearer. Therefore, emergency registration is needed for the establishment of the Security Association and to establish the correct signaling priority. The UE is also required to perform an IMS emergency registration as some countries do not allow emergency calls from non-registered users.

The CSCF supports the emergency registration procedures as defined in 3GPP TS 24.229. The contact associated with the emergency registration is independent of the contacts associated to the regular (non-emergency) registration.

Note: The emergency contact is not used for callback from the emergency center.

4.3.2 Network-Initiated Deregistration

Deregistration is a process of removing the currently registered contacts of a user from the S-CSCF. It is either initiated by administrative actions or because of registration time expiration. Administrative action can be initiated from the HSS or from the CSCF. For administrative actions in the HSS, a Registration Termination Request (RTR) is received from the HSS. For registration timer expiry in the S-CSCF, the HSS is informed about deregistration in the S-CSCF.

A deregistration by network is also triggered because of administrative actions (that is, a so called administrative deregistration). The contact and its associated information are then removed from that Public User Identity. The client is not notified of this deregistration action by this function.

For network initiated deregistration, because of registration timer expiry; for each Public User Identity there is a registration timer per contact address, and the CSCF determines when registration for a contact expires. At the expiration of a contact, the CSCF terminates all ongoing sessions associated (that was used to establish dialogues) with that contact.

If the S-CSCF detects that the re-registration of the same user and same sip instance is re-registering with a new IP address, the registration is replaced by the new contact IP address.

For network-initiated deregistration that is triggered by administrative actions, all contacts for that user are de-registered.

The user can be network de-registered from one S-CSCF and moved to another S-CSCF because of a network failover or fallback after node recovery. When the S-CSCF receives an RTR from the HSS with reason code `NEW_SERVER_ASSIGNED` or `SERVER_CHANGE` and if the user has an ongoing session, the user is not de-registered immediately. In this case, the S-CSCF only de-registers the user after an operator-configurable time.

4.3.3 Implicit Registration

A user can be configured with an IRS. If at registration, the Public User Identity to be registered belongs to such a set, all Public User Identities in the IRS are fetched from the user profile, and registered at the same time. The same contact address is used for all identities. If a new contact address is added later on, it is applied on all Public User Identities within the set. The corresponding is done at deregistration, that is, the same logic is applied for all Public User Identities within the set.

One or more IRSs can be configured for a user. This set of Public User Identities is configured as subscription data and is downloaded to the S-CSCF from the HSS over the Cx reference point. This is done at registration of any of the Public User Identities within the set. Public User Identities belonging to an IRS point to different services; or some of these Public User Identities point to the same service profile.



If at registration the Public User Identity to be registered belongs to such a set, all Public User Identities in the IRS are fetched from the user profile and registered at the same time. The same contact address is used for all identities. If a new contact address is added later on, it is applied on all Public User Identities within the set.

The Public User Identities within an IRS can be a SIP URI or a tel URI. Temporary Public User Identities are supported. A temporary Public User Identity is connected to an IRS. Temporary Public User Identities are barred for session establishment.

All registered Public User Identities are sent back in the reply to the UE as associated identities. All non-temporary implicitly registered Public User Identities can be used for addressing the registered user.

All Public User Identities within an IRS share expiration timer for the same contact. At re-registration, a SIP REGISTER with a new expiration time is sent from one Public User Identity, and affects all identities within the same set. At re-registration, all Public User Identities within an IRS are updated (which is valid per contact).

Changes to the Public Identities and Wildcarded Public Identities within the IRS can be done without the need of de-registering the user.

At deregistration of a contact for one Public User Identity within an IRS, the contact is de-registered for all Public User Identities within the set with the same request. At deregistration of all contacts or the last contact for one Public User Identity within an IRS, all Public User Identities within the set are de-registered with the same request.

For VoLTE Multi-SIM and Multi-Device use cases for emergency or regular calls, the S-CSCF can send a sorted list of IMPUs in the list of P-Associated-URI (PAU) that is added to the REGISTER response to enable discovery of the right device in a call.

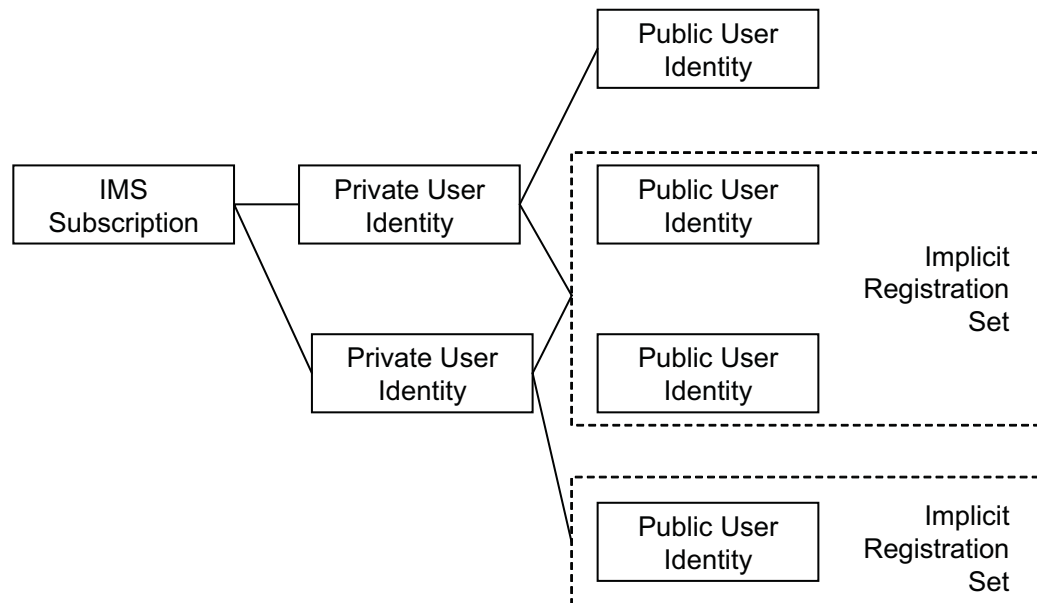


Figure 8 Relationship of Public User Identities When Implicitly Registered

4.3.4 Identity Convergence

A Public User Identity can be shared among Private User Identities. This allows also mobile users to be reached on many different terminals with the same identity – the One Number concept.

Normally, the Private User Identity is provided by the terminal as part of the SIP registration request message. But legacy terminals exclude the Private User Identity. In this case, the I-CSCF and the S-CSCF derive a Private User Identity from the registration request to be used for processing the registration request. The Public User Identity is always received from the terminal.

The user can have registration states in the CSCF and HSS for different Private/Public User Identity pairs as long as the HSS has been provisioned with the combination the user is trying to register.

A function in the registration process in the S-CSCF can be applied on either the whole IRS or one single Public User Identity in case it is not part of an IRS or applied on one Private User Identity/ Public User Identity pair.

One IRS always contains one or more Private User Identities in the S-CSCF.

4.3.5 Third-Party Registration

At registration, re-registration, and de-registration requests, an AS can be informed about the registration status of a user. This third-party registration feature is also referred to as service triggering at registration. It occurs at reception of SIP REGISTER message or network-initiated deregistration, initiating user trigger data evaluation, and the following signaling procedures to ASs.



Third-party registration occurs at reception of a SIP REGISTER request from the served user. Normal registration handling is performed. The S-CSCF then checks the value of Registration Type, if included in trigger data, to find out if service triggering is applicable. For registration query (no contact information from the user), service triggering is not performed. The user trigger data is configured as subscription data and is downloaded to the S-CSCF from the HSS over the Cx reference point.

The S-CSCF evaluates the triggers of the Served User in priority order. Third-party registration is performed to the AS defined in the AS name field in the trigger data. The SIP request is routed to the AS. Default handling is supported for third-party register. If the default handling defined in the filter criteria indicates the value SESSION_CONTINUE, the trigger evaluation continues without waiting for the response. If there is a trigger match, a SIP REGISTER is sent to the next AS. This continues until there are no more matches. If the third-party registration fails and the default handling defined in the filter criteria indicates the value SESSION_TERMINATED as specified in 3GPP TS 29.228, the S-CSCF initiates, for a registered contact, the network-initiated deregistration.

The CSCF has the possibility to include SIP Message Bodies in third-party registration requests. This means that the originally received REGISTER request or response from and to the UE can be included in the body of the third-party register to the AS. The behavior is controlled by include register request and include register response indications received from the HSS in the service triggers in the user profile.

The functionality can be optimized also with the Message Embedding option to determine when to send a registration notification to an AS. The option allows the operator to choose if a re-registration because of update of Contact header, PATH, or Feature-Caps header leads to a new registration notification.

When the Public User Identity is part of an IRS, the trigger evaluation is performed for each service profile within the IRS.

4.3.6 Registration Event Package

The registration event package allows a subscriber (in this case either a UE, a P-CSCF, or an AS) to subscribe to information about changes of the registration state for a user in the S-CSCF.

The generic SUBSCRIBE – NOTIFY mechanism, as described in [RFC 3265](#), is used for handling the subscriptions.

Using Registration Event Package the CSCF supports the possibility to initiate a network initiated reauthentication described in TS 24.229.

4.3.7 Extended Registration Event

The CSCF supports the extended registration event with information that, for example, can be used for SRVCC handover. The S-CSCF includes the

Feature-Caps header (with, for example, Access Transfer Control Function (ATCF) information or sip instance ID) and IMPI into the reginfo XML, as part of Notify message back to the AS (SCC AS).

4.4 SIP Routing and Traffic

The CSCF can route according to standard SIP mechanisms for session establishment, clearing, and modification. The CSCF supports relevant SIP routing standards from 3GPP and the Internet Engineering Task Force (IETF).

The CSCF also enhances interoperability with other SIP nodes by allowing the operator to modify the following values of SIP response messages; error code, the associated slogan phrase, and the `Retry-After` header value. The configuration is possible for SIP errors messages received from other nodes or generated by the CSCF.

4.4.1 DNS and ENUM Client

The CSCF DNS/ENUM client supports separated querying capability. This means that the CSCF is able to send DNS queries to a DNS server and ENUM queries to a separate ENUM server.

The CSCF can also keep the DNS information cached in the CSCF even when TTL is expired and no successful DNS response is received.

The CSCF also supports canonical name record (CNAME). CNAME is a type of Resource Record in DNS that specifies that a domain name is an alias of another canonical domain name.

4.4.2 Domain Routing Function

The CSCF supports internal DNS like capabilities to route SIP requests to next hop addresses. The Domain Routing Function (DRF) implements a set of CSCF local static host tables. These tables map a SIP request routing address in Fully Qualified Domain Name (FQDN) format to a new set of single or multiple next hop addresses. The host tables can be configured by the operator.

A SIP request is routed to the original next hop address if the DRF is not started, or if the function fails to return a new next hop address.

When multiple next hop addresses are configured they are only used in serial, that is, there is no forking of requests. It is also possible to use the received FQDN address, either as first or last alternative compared to the configured ones.

DRF is started by the CSCF (I/S/E) including BGCF and BCF.



4.4.3 S-CSCF Selection

The I-CSCF performs an S-CSCF selection when allocation of an S-CSCF is required at user registration. The I-CSCF contains an operator-configurable list of S-CSCF addresses and the corresponding capability of the S-CSCF called the Resource Broker Entry. For initial registrations, the I-CSCF queries the HSS for the user authorization. If the user is not registered, the HSS returns the server capabilities of the user. The I-CSCF uses the information in the Resource Broker Entry to select an S-CSCF and then forwards the SIP message to the selected S-CSCF.

For re-registrations, the I-CSCF queries the HSS for the user authorization and the HSS provides the name of the serving S-CSCF of the user. The I-CSCF forwards the request to the S-CSCF, if the S-CSCF fails to respond, the I-CSCF queries the HSS for the server capabilities of the user. The I-CSCF uses the information configured in the Resource Broker Entry to select the S-CSCF using the same mechanism as per initial registration.

The I-CSCF can be configured to select only S-CSCF located in its Resource Broker Entry for REGISTER requests. If the serving S-CSCF name returned from the HSS is not included in the configured Resource Broker table, the I-CSCF fetches the S-CSCF capabilities required by the user and then reselects an S-CSCF from its list that supports the needed capabilities. If the Resource Broker Entry is configured only with S-CSCF located in the same Geographical Area as the I-CSCF, this ensures that in failover and fallback scenarios only the S-CSCF in the same Geographical Area are selected for the registering user.

For non-REGISTER requests, the I-CSCF contacts the HSS to get the location of the user (the S-CSCF address) and then forwards the SIP message to an appropriate S-CSCF.

4.4.4 Caller Preferences

The CSCF supports serial and parallel alerting (forking) to multiple SIP endpoints. Also, the CSCF supports service-dependent alerting where the terminal capabilities of the user and calling preferences are considered.

During the registration process, the terminal capabilities and caller preferences are received and stored in the CSCF. When the terminal registers, it declares a set of features that it supports (that is, its capabilities) in the Accept-Contact header of the REGISTER request in the form of feature tags and values.

If a caller has preferences for how requests are to be handled in the network, caller preferences can be sent in any SIP request outside of a dialogue. The CSCF checks the terminal capabilities and caller preferences before accepting and forwarding requests. Sessions are not initiated to contacts that do not support a requested criterion, for example, a service.

In addition to the Accept-Contact header, the S-CSCF checks if any Reject-Contact header is received. The Accept-Contact header field contains feature tags and values that describe the UE that the caller wants to reach. The

Reject-Contact header field contains feature tags and values that, if matched by a UE, imply that the request is not to be routed to that UE.

When there is no Accept header or Reject header included in the request, Implicit Feature Set Preferences takes place. Implicit preferences are created from the SIP method (for example, INVITE) and optionally the received event (Event header) if the method is SUBSCRIBE. For example, a SUBSCRIBE request with Event=presence without Accept-Contact and Reject-Contact headers would be treated the same as a SUBSCRIBE with the following Accept-Contact header:

```
Accept-Contact: *;methods="SUBSCRIBE";events="presence";require
```

The UE capabilities of the contacts are matched against the determined implicit caller preferences. For example, if a user has two contacts registered as follows:

```
Contact: sip:u1@h.example.com;audio;methods!="INVITE";q=0.2
```

```
Contact: sip:u2@h.example.com;audio;methods="INVITE";q=0.1
```

When an INVITE request is received that does not contain any Accept-Contact headers or Reject-Contact headers, the implicit caller preference is determined as follows:

```
Accept-Contact: *;methods="INVITE";require.
```

Therefore, the first contact is not considered since this contact has explicitly stated that it does not support the INVITE method. The second contact is selected since it has explicitly stated the support of the INVITE method. In the implicit preferences case, when there are no matching contacts at all in the target set, all contacts in the target set is used for terminating the request.

4.4.5 Network Interconnection

The CSCF supports interconnection with other IMS-based networks.

The CSCF supports interconnection with non-IMS-based networks (that is, PSTN/PLMN or H.323 VoIP users). The CSCF has an external selection mechanism that selects an external gateway based on various routing criteria such as Request-URI, Any SIP request headers, Media type in the SDP, UTC Date/Time information.

4.4.6 SIP Redirect

The CSCF supports redirecting the request to the new target on received 3xx or 480 responses, defined in TS 24.229 and [RFC 3261](#).

The S-CSCF is also able to issue a redirect request when the HSS informs it that another S-CSCF is serving this user.



The CSCF support handling of SIP URI header components that are included as part of the Contact header information of a 3xx response received from a redirect server or remote target.

The received SIP URI header components are inserted as new headers of the outgoing SIP request, or are appended to or replace existing header values of the original SIP request.

4.4.7 Emergency Call Handling

The P-CSCF detects upon reception of a SIP call that it is an emergency call and routes the call to the E-CSCF or the S-CSCF. The E-CSCF is a logical module dedicated to the handling of emergency calls. An emergency call can be handled by the S-CSCF for registered users only or by the E-CSCF for registered or unregistered users.

If the S-CSCF is used to provide the emergency function, the request is prioritized higher than regular calls. If the profile of the user contains an emergency service RN, it is used to route the request to the PSAP. Otherwise regular routing logic based on the dialed digits is used to route the call.

If the E-CSCF is used to provide the emergency function, it allows a user to perform emergency calls, which are prioritized and routed to the correct emergency center (PSAP). The emergency center is selected dependent on the dialed emergency number (for example, 112) and the location (based on PANI or IP address taken from the Via header) of the user.

For selecting the PSAP, the E-CSCF obtains the PSAP address using the MI interface to the PSAP selection database (located in the RDF/LRF). The MI interface can be configured to be a SIP-based interface or an HTTP/SOAP/XML interface. The SIP MI interface is specified in the 3GPP standards. The HTTP interface is a non-standard interface and supports HTTP Digest Authentication.

The input to the RDF/LRF for the selection of the PSAP is the called number, calling number, and location.

For the SOAP-based interface, the PSAP address is returned from the LRF or a default configured PSAP address is used for routing. For the SIP-based interface, the list of available PSAP addresses is returned in the Contact header of the 3xx response from the LRF. The E-CSCF then, based on PSAP address, routes the call through the BGCF to the MGC or to the SIP-based PSAP directly. It is configurable in the E-CSCF if the user locations to be fetched from the PANI information or the IP address of the user.

To support cases when the user is located behind a SIP proxy and potentially using a private IP address, the E-CSCF can be configured to recognize which Via header belongs to the P-CSCF. The E-CSCF uses the IP address found in the Via header inserted just before the P-CSCF Via when communicating with LRF. If there are no other Via headers before the P-CSCF Via, then the P-CSCF Via is used.

If the E-CSCF cannot find the P-CSCF, the E-CSCF uses the first inserted Via header (that is, the UE Via).

The solution for Emergency Call handling complies with the emergency communication architecture recommended by 3GPP and TISPA.

If the user location from PANI is required for the selection of a PSAP and is not available (not provided from the network), the E-CSCF optionally fetches the reference location information using the Sh interface from the HSS (if HTTP/SOAP/XML is used).

A CSCF entity recognizes emergency calls by the presence of the Priority header with the value of Emergency in a SIP INVITE message header. For the SIP-based MI interface, the emergency call is detected by emergency service URN in the Request-URI. This is valid for the INVITE received on all CSCF interfaces, also including the AS to S-CSCF case. However, the originating P-CSCF has different criteria for detecting emergency calls.

Once an S-CSCF entity receives an emergency call either from a user to a PSAP or from an Emergency center to a registered user (emergency callback), it is prioritized. For emergency callback case, the Priority value must be emergency for the calls to be prioritized, otherwise, these callbacks are not prioritized in the CSCF.

For VoLTE emergency call (Emergency SRVCC), the LTE access network sends the emergency call request to the IMS network. The E-CSCF forwards the emergency call request to the EATF over the I4 interface, and then the E-CSCF connects the PSAP. The call establishment between the E-CSCF and PSAP follows the same principal as for a normal emergency call as shown in Figure 9.

When the user roams to non-LTE access network, the non-LTE access network initiates an access network transfer request to the IMS network through the I-CSCF over the Mw interface. After that the I-CSCF forwards the access transfer request to the EATF over the I5 interface. The EATF sends a request to the PSAP through the E-CSCF to update the call. Both I4 and I5 interfaces are SIP interfaces.

For Emergency SRVCC, the CSCF supports the standardized logical node EATF that is defined to coordinate the signaling exchanges for completing the access transfer of an emergency call to Circuit Switch domain and fallback to Packet Switch. The emergency session is identified using the IMEI-based sip.instance and the C-MSISDN of the terminal.

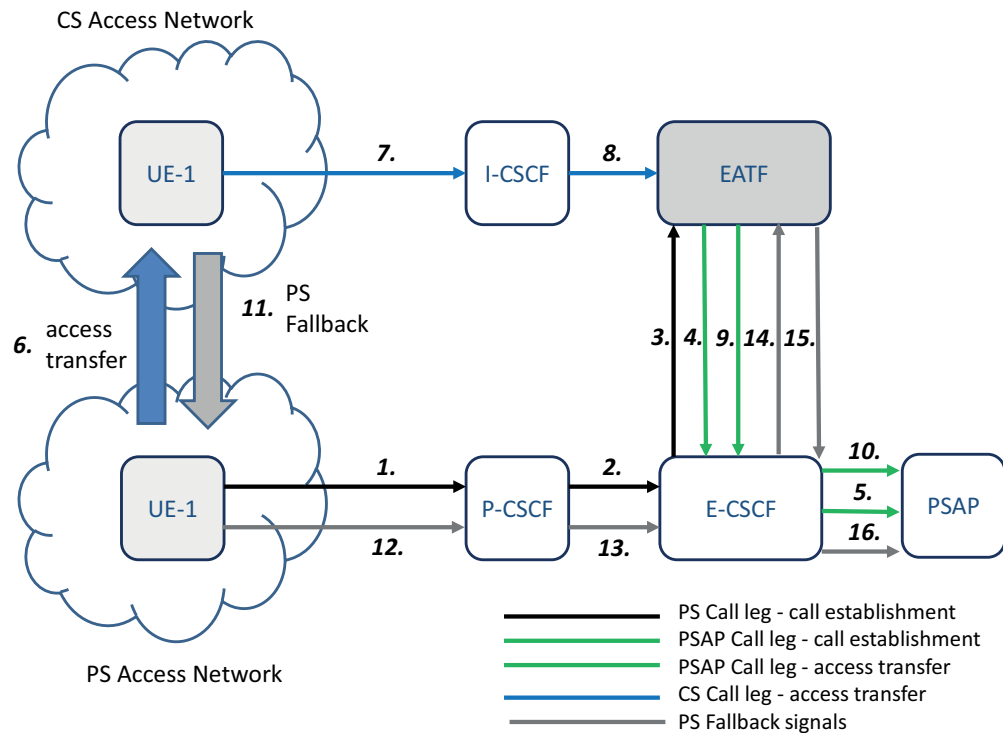


Figure 9 VoLTE Emergency Access Transfer Signaling

4.4.8

Number Portability

Number Portability is a telephony network capability which allows an end user to change Service Provider (SP) or location, or both, without having to change their telephone number.

The types of Number Portability are as follows:

- Service Provider Portability – allows an end user to change SP while retaining the telephone number.
- Location (Geographic) Portability – allows an end user to change from one Geographic Area to another while retaining the telephone number.

The supported Number Portability schemes All Call Query (ACQ), OR, and Query on Release (QoR) are described in [RFC 3482](#).

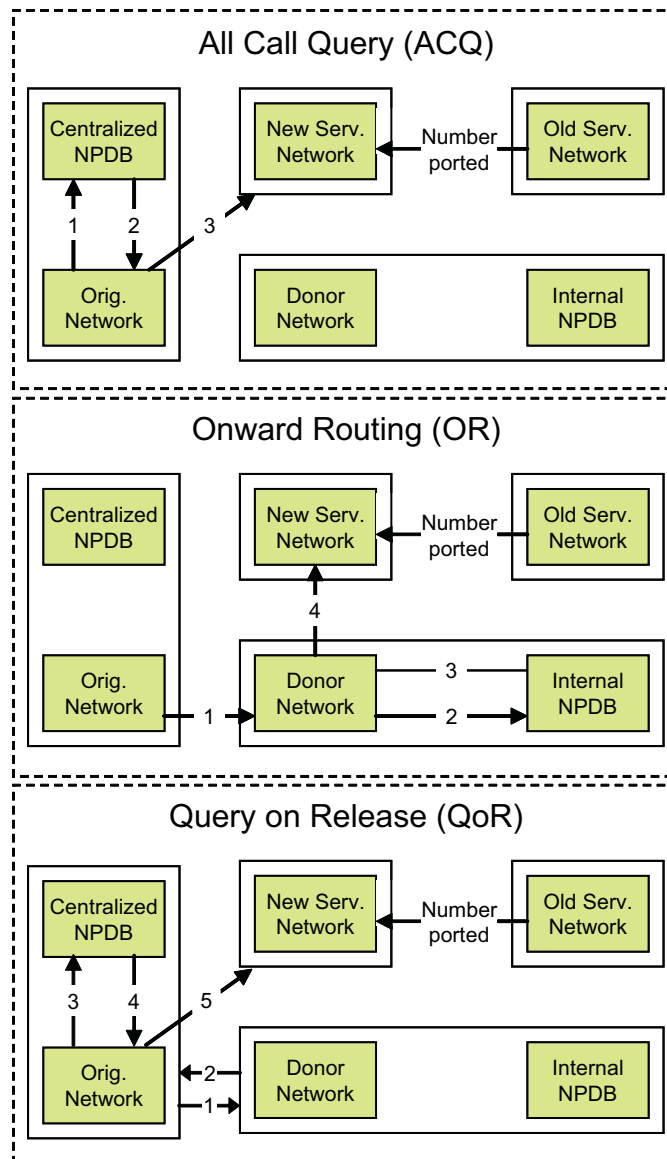


Figure 10 ACQ OR and QoR Schemes

The query to the Number Portability Database (NPDB) is done by the DNS/ENUM server. The CSCF queries the DNS/ENUM server with the telephone number as input. The Number Portability information is returned in ENUM response to the CSCF.

The ACQ scheme has the following sequence:

- 1 The Originating Network receives a call from the caller and sends a query to a centrally administered NPDB.
- 2 The NPDB returns the RN associated with the dialed Directory Number.



- 3 The Originating Network uses the RN to route the call to the new serving network.

The ACQ scheme does not involve the donor network when routing the call to the new serving network of the dialed ported number.

The OR scheme has the following sequence:

- 1 The Originating Network receives a call from the caller and routes the call to the donor network.
- 2 The donor network detects that the dialed Directory Number has been ported out of the donor network and checks with an internal network-specific NPDB.
- 3 The internal NPDB returns the RN associated with the dialed Directory Number.
- 4 The donor network uses the RN to route the call to the new serving network.

The QoR scheme has the following sequence:

- 1 The Originating Network receives a call from the caller and routes the call to the donor network.
- 2 The donor network releases the call and possibly indicates that the dialed Directory Number has been ported out of that switch.
- 3 The Originating Network sends a query to a centrally administered Number Portability Database (NPDB). A copy of the centrally administered NPDB is usually resident on a network element within its network or is provided through a third-party provider.
- 4 The NPDB returns the Routing Number associated with the dialed Directory Number.
- 5 The Originating Network uses the Routing Number to route the call to the new serving network.

4.4.9 Carrier Routing

Carrier routing means that if CIC is present in the request URI (after any service invocation), the originating S-CSCF starts External Network Selection. Or, if a CIC is received in an ENUM response, the originating S-CSCF and terminating I-CSCF also starts External Network Selection. Carrier routing can be enabled for ENUM only or SIP and ENUM.

As part of External Network Selection, the CSCF selects an External Network based on the received CIC (included in the Request-URI). When the received CIC is not found in the CIC tables, a default entry is used.

4.4.10 ICMP Support

When the CSCF sends SIP messages to other gateways/hosts, transport layer failures are reported through the Internet Control Message Protocol (ICMP). The CSCF then stores the error information and does not resend SIP messages to that destination in a configurable time. This implies that the terminals get faster SIP error response times and less load in the network.

ICMP messages are sent in several situations, for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route.

4.4.11 IMS Restoration Support

For periodic maintenance, system failure, or service interruption, the temporary session data of the user (for example, registration state, which Public and Contact identities are registered) that are important could be lost. This affects important use cases such as terminating traffic to be impossible completing. Because of this, the relevant data must be restored to provide services to registered users. With IMS Restoration Support this is achieved by retaining S-CSCF data in the HSS, and for the users to regain services, their session requests are served by a new S-CSCF or possibly the same S-CSCF (when returned into service).

If an S-CSCF failover happens, upon reception of a request, the I-CSCF selects a secondary S-CSCF based on capabilities matching. The selected secondary S-CSCF serves the user of the failed S-CSCF. By using SAR/SAA messages, the secondary S-CSCF receives the Restoration Data of the user from HSS.

The secondary S-CSCF rebuilds the user information with the restoration data (that is, to rebuild all user information with as much information as available in SCSCF-Restoration-Info). Using the rebuilt user information and user profile, the secondary S-CSCF provides services to the user.

If a user has multiple Contacts registered for the same IP Multimedia Public Identity (IMPU), as many sets of restoration data as the number of registered Contacts are sent by the HSS. If an IMPU of a user is shared by multiple IP Multimedia Private Identities (IMPIs), the S-CSCF Restoration-Info of all contacts is received from the HSS. All received Restoration-Info Attribute-Value Pairs (AVPs) are used to rebuild the user information.

The IMS Restoration support is based on 3GPP TS 23.380.

4.4.12 P-CSCF Restoration

If a P-CSCF becomes unreachable, and there is no P-CSCF restoration support, all UEs registered with that P-CSCF do not receive a terminating request until one of the following happens:

- The UE makes a new call.



- The UE re-registers.
- The UE hands off to another network.

Upon determination of an unreachable P-CSCF, the S-CSCF responds to the terminating request with an error.

The P-CSCF restoration support provides a quicker mechanism for the UE to regain services by triggering a UE re-registration on a per-user per-terminating-request basis. The session requests from the UEs are served by a new P-CSCF or possibly the same P-CSCF when it is returned into service.

When the S-CSCF receives a terminating request, destined for a UE that is served by an unreachable P-CSCF, the S-CSCF sends a P-CSCF restoration indication to the HSS. The HSS asks the Packet Core Network to force the UE to re-establish IMS Packed Data Network (PDN) connectivity, and thus perform an IMS initial registration. In this case, the UE performs an initial registration towards a reachable P-CSCF and is then reachable for terminating calls.

4.4.13 Accommodation of SIP Non-Compliant Requests

A list of illegal characters can be treated in a special way and allowed to be used in SIP Requests. These SIP requests can either come from UEs or ASs.

The [RFC 3986](#) standard states that the characters #, [,], ^, `, {, |, and } are not allowed in a URI component. It is however possible to configure that one or more characters are handled within the CSCF.

A configuration parameter in the CSCF lists illegal characters that are allowed in a URI.

4.4.14 Transit Support

The IMS provides services to end-user customers of an operator by directly supporting multimedia communications services to or from the customers of that operator. However, IMS is also used in several other configurations where the capabilities of IMS are used to support CS domain customers of an IMS operator, or in various other kinds of business arrangements where the capabilities are used to support interconnection of other networks.

The functionality enables an IMS operator to provide transit functionality for its own, non-IMS (CS domain), customers. In this case, the operator is serving its own customers, some of which have been migrated to IMS while others are still CS domain subscribers.

The functionality also enables an IMS operator to provide transit functionality to enterprise networks. In this case, the operator is serving as a transit network for an enterprise IP network and provides connectivity to both PSTN and IP endpoints.

The functionality also enables an IMS operator to provide transit functionality to other operators. In this case, the operator is serving as an IMS session-based routing backbone for a PSTN operator or another IP network and provides connectivity to both PSTN and IP endpoints.

The transit function is a role that the IMS network can take to route a session setup request, originated in another network to its destination network. This means that the transit network is not used by the calling party or the called party.

The routing analysis can consider the last forwarding user as calling party number, based on information from the History-Info SIP header.

The transit function in the I-CSCF allows calls that are destined to a user who has not been provisioned in the IMS network. The I-CSCF uses External Network Selection (BGCF) to transit the call to another network.

The following use cases are supported:

- PSTN NNI > IMS Transit > PSTN NNI
- PSTN NNI > IMS Transit > SIP NNI
- SIP NNI > IMS Transit > PSTN NNI
- SIP NNI > IMS Transit > SIP NNI

It is assumed that the charging information for the transit session is to be provided by gateways, that is, MGC or Interconnection Border Control Function (IBCF), see Figure 11.

A terminating I-CSCF can be configured to perform transit routing with bypassing HSS lookup. A terminating I-CSCF is able to handle transit and non-transit traffic.

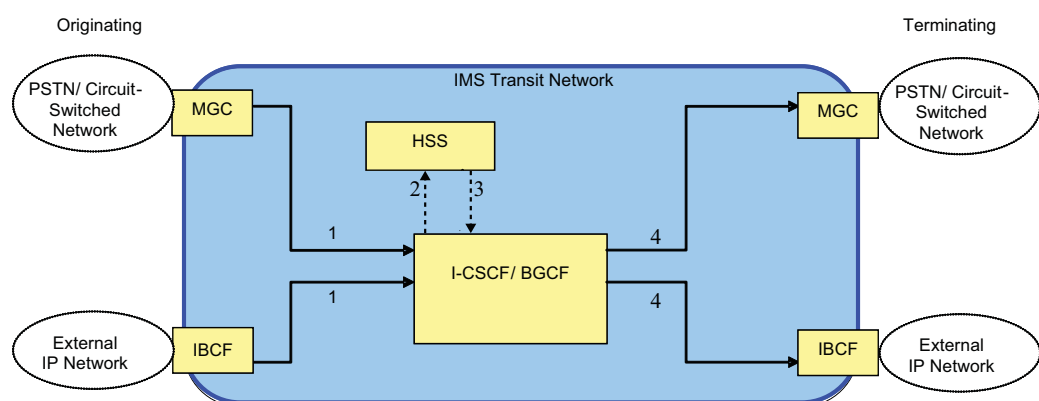


Figure 11 Transit Support

The transit session has the following sequence:

- 1 An INVITE request message arrives from the MGC for a PSTN originating case, or from the IBCF for an IP network originating case.



- 2 The I-CSCF can interrogate the HSS for the location of the terminating user, or it can be configured to suppress it for direct routing.
- 3 The I-CSCF receives the HSS response with user unknown.
- 4 The BGCF selects the External Network based on the routing criteria (see Section 2.2.4 Breakout Gateway Control Function on page 5) and routes the message to the appropriate egress gateway.

4.4.15 SIP Overload Control

The CSCF supports SIP Overload control reporting and reacting roles according to [RFC 7339](#).

The reporting role has the possibility to signal to the upstream node when the load approaches to the load regulation threshold. The CSCF indicates the percentage of the traffic that needs to be redirected to other CSCF instances or rejected by the upstream node until the traffic is normalized.

The reacting role has the possibility to react to a downstream node that is reporting overload. The CSCF redirects the received percentage of the traffic to other instances or rejects traffic on behalf of the reporting node until the traffic is normalized.

4.4.16 Failover and Fallback

It is configurable how fast the CSCF performs failovers when communication fails towards a destination. This is done by configuring various SIP failover timers depending on the interface.

When a destination has failed, it is stored in the CSCF destination blacklist for a configurable amount of time. When a destination is put on the blacklist, an alarm is raised.

It is possible to configure threshold values for blacklisting destinations whenever peer nodes do not respond or respond indicating that it is unable to process the request (SIP 503 error response). Different threshold values can be configured for transaction time-out, reception of 503 with a `Retry-After` header, reception of 503 without a `Retry-After` header, fatal transport errors, or ICMP errors.

To provide more granularity and better control for the failover and blacklisting scenarios, it is possible to configure transaction time-out timer, blacklisting thresholds, and blacklisting periods for specific FQDNs.

The CSCF has the possibility for fast fallback when the destination is in service again by starting SIP monitoring. The CSCF removes the destination from the blacklist and starts using the destination for traffic again, when the SIP monitoring detects that the destination is back in service or when the blacklisting period expires if SIP monitoring is disabled.

4.4.17 SIP Monitoring

Many IMS nodes monitor the availability of the SIP application of a peer node by sending the SIP OPTION request. The CSCF responds to the SIP OPTIONS with CSCF capabilities in the Option tags.

Option tags are used in support for SIP compatibility extensions mechanisms and identify the option to SIP endpoints.

The CSCF can be configured to send SIP OPTIONS periodically to monitor a peer node that becomes blacklisted and generate an alarm about the unavailable nodes. When a blacklisted destination responds with any SIP response except SIP 503, the destination is removed from the blacklist. When no positive SIP response is received, the SIP monitoring prolongs the blacklisting. It is possible to avoid sending SIP OPTIONS to blacklisted nodes that do not support SIP OPTIONS and to avoid that they become blacklisted forever.

The CSCF can also do periodic monitoring on preconfigured SIP nodes of which availability is sensitive or crucial and on SIP nodes that are only used as stand-by alternatives, independent if they are blacklisted.

4.4.18 IPv6

The CSCF can support UEs that are assigned an IPv4 or an IPv6 address by the access network.

IPv4/v6 dual stack is available on the I-CSCF, S-CSCF, EATF, E-CSCF, and BGCF as transport protocol for application level protocols and IPv6 addresses are supported in application logic and higher-level protocols (SIP and Diameter).

4.4.19 Loose Route Indication

The CSCF also supports loose route indication. Loose route indication is permanent subscriber data stored in the HSS and downloaded to the S-CSCF during registration. Loose route indication indicates to the S-CSCF that loose route routing mechanism is to be applied to the public identities when performing terminating routing to the user. Normally when routing a terminating non-Register request the S-CSCF takes the stored contact URI and puts it in the request URI. If loose route indication is received for the public identity during registration, the S-CSCF instead keeps the request URI as it was received and instead put the stored contact URI in a Route header when routing the request. This gives the flexibility to interwork with IP-PBX or other nodes that support different types of routing mechanisms.

4.4.20 Priority Support Session

The CSCF supports priority handling for calls in the IMS network for compliance to regulatory requirements for different markets, for example, GETS (US market).



Priority handling for Originating and Terminating calls in the CSCF gives the possibility to grant a user access to the network, even during times when the call normally is to be rejected because of overload in the network.

This enables the CSCF to support a priority service to be used in times when the network is loaded with mass emergency calls and regular calls because of, for example, a natural catastrophe like an earthquake.

Priority services are used by emergency responders, key critical infrastructure heads, key national security leaders, and emergency preparedness personnel. The objective is to provide a higher probability access to shared resources and call success at all time. A priority call can or cannot have precedence over emergency calls, depending on market requirements. Because of this the CSCF supports multiple priority levels.

The CSCF complies with [RFC 4412](#), which defines the Resource-Priority header that is used to carry priority information in SIP signaling.

Priority calls are requested by the UE using special dial strings. When the S-CSCF detects the special dial strings in the received request, the S-CSCF either verifies that the user has subscribed to priority service or forwards the request to a dedicated AS that verifies the authority of the user to use the prioritized service.

4.4.21 Crankback in I/S-CSCF and E-CSCF

The Crankback functionality supports reselecting an alternative route when a time-out or an error response indicating that congestion or a fault is received from the next hop or previously selected route. It is possible to configure several Route headers to indicate an alternative route. This makes it possible to handle crankback scenarios on behalf of the next SIP node. Thus allowing Routing Network plans to be maintained more centrally.

The CSCF provides crankback for number-based requests when the BGCF (ENS) is initiated by the S-CSCF, E-CSCF, and I-CSCF.

4.4.22 Pre-Paging

The CSCF pre-paging solution lowers the Call Setup Time by taking a mobile UE from IDLE to CONNECTED state in an early phase of the call setup.

The following scenarios are supported:

- SIP OPTIONS is sent directly towards the target UE from the terminating S-CSCF when the S-CSCF is collocated with the I-CSCF. This happens before the LIR/LIA transaction towards the HSS upon reception of a terminating INVITE.
- SIP OPTIONS is sent directly towards the target UE from the terminating S-CSCF upon reception of a terminating INVITE when the S-CSCF is not

collocated with I-CSCF. This happens before the terminating service invocations are done.

4.5 Wi-Fi Calling

The CSCF node, as part of an IMS network, supports VoLTE devices making calls over a Wi-Fi access network. The CSCF node also includes functionality that enables seamless movement from one access technology to another.

The CSCF supports registrations and re-registrations where the contact includes the currently used access type, which enables the use of the access aware configuration profiles. The access type information is also used to create PM statistics and transferred to the application servers to make it possible to have services Wi-Fi-aware.

4.6 Service and Application Invocation

4.6.1 Service Invocation

To allow value-added services to interact with a multimedia session, extension points are provided where a value-added service can take over control and extend the behavior of the session. The administrator provides service trigger information in the system. This information is specific for the value-added service. The system starts a value-added service when a trigger matches a SIP request. The SIP request is then routed to the AS that provides the value-added service.

For the IMS to start extra value-added services, the following mechanisms are involved:

- Downloading service triggers
- Service trigger match

Service triggers are downloaded from the HSS to the S-CSCF at initial registration, at an unregistered originating, terminating, or diversion (Originating CDIV) traffic case, or when changes to provisioned profile of the user are performed through the administration interface.

Users can have their own set of Differentiated Services and the service triggers for each service is explicitly defined in the user service profile, which is downloaded from the HSS to the S-CSCF.

Service triggers that can be common to multiple users, can be locally administered and stored at the S-CSCF. These are known as Shared iFC. Locally administered service triggers (or Shared iFC) are identical in structure to service triggers explicitly defined in the service profile of a subscriber. However, the user service profile downloaded from the HSS to the S-CSCF includes a reference to the locally



administered service triggers, instead of the explicit definition of the service trigger.

Service Trigger Match: upon receiving SIP requests, service invocation feature checks the service trigger information, determines if the trigger matches the SIP request.

Triggers are only applied to SIP requests that are not within an established SIP dialog.

The triggers apply at registration, Originating and Terminating side, and can be based on the following:

- SIP method
- Request URI
- SIP header
- SIP header content

The triggers can be combined also using the boolean expressions AND, OR, and NOT.

Default Handling is supported. It determines whether the dialog is to be released if the AS could not be reached.

Depending on the Default Handling specified for this AS, the S-CSCF interrupts the trigger evaluation (the final response is routed back to the served user – this is the default behavior) or the S-CSCF continues the trigger evaluation.

The CSCF is aligned with the 3GPP standard TS 24.229 R10 to distinguish when communication is to be treated as call diversion or not. The CSCF receives a Request-URI and then triggers service to an AS when the IFC is matched. The AS has changed the Request-URI before sending it back to the S-CSCF. When the S-CSCF receives such changed Request-URI, the S-CSCF checks whether the Request-URI matches the original Request-URI.

4.6.2 Node Default IFC

If no standard Initial Filter Criteria (IFCs) in the user profile are triggered (as explicit IFC downloaded from the HSS or specified as Shared IFC), then the node default IFCs are evaluated. Node default IFCs apply to all users in the S-CSCF for whom no regular IFC has been triggered and are executed in the configured priority order. When the request matches the configured node default IFC, the request can be continued to an AS, or can be rejected. It is possible to define a node default IFC without an AS, which permits the operator to allow or block specific AS-less services.

4.6.3 Application Server Initiated Requests

When the AS initiates a SIP request, such a case is often described as Call Out Of the Blue (COOB).

Two separate cases can be defined: Originating and Terminating applied sessions. The former means that the S-CSCF is acting as during a common originating case, the latter acting for the terminating side.

The AS is acting as a UAC, initiating a SIP request. The S-CSCF receives an initial SIP request outside an existing dialogue on the ISC interface. A possible SIP REGISTER request is rejected.

The IP address of the AS is checked against a list of configured ASs. If the AS is authorized, the continued processing depends on the indicated user session direction (received top Route header from the AS).

In the originating case, the S-CSCF determines the identity of the served user. If the user is registered in the S-CSCF, common originating side behavior (except for authentication) and service triggering is performed.

If the user is not registered, it performs the following:

- Informs the HSS to assign an S-CSCF name to the user in its database.
- Informs the HSS to change the state of the user to unregistered in the HSS.
- Downloads the user profile from the HSS and stores it in the local CSCF cache.
- Evaluates if there are triggers that match the received request.

If triggers match, the CSCF starts the AS indicated in the trigger. If no triggers match, the CSCF continues the originating logic and eventually routes the call to the terminating user.

The S-CSCF determines whether this physical S-CSCF serves the addressed user. If this physical S-CSCF serves the addressed user, the processing is done analogous to common terminating side procedures including service invocation. Otherwise, originating side behavior is applied without any service invocation. Further processing is done according to basic setup procedures.

The AS can also send the request to the I-CSCF to locate the S-CSCF.

The CSCF also offers support for the P-Served-User header. This header, introduced in [RFC 5502](#), is used to identify the served user in messages exchanged between the S-CSCF and an AS.

4.6.4 Public Service Identity and Wildcarded Public Service Identity

The Public Service Identity (PSI) identifies services that are hosted in ASs. The users establish sessions to these identities to use services such as conferencing and chatting.



The CSCF supports the concept of PSIs, which is used to identify services or user groups. Each PSI is hosted by an AS, which executes the service-specific logic identified by the PSI. A PSI takes the format of a SIP URI or tel URI. The same CSCF routing and triggering principles as for Public User Identities apply except registration.

The PSIs are stored either as a distinct PSI or as a Wildcarded Public Service Identity (wPSI). A distinct PSI contains the PSI that is used in routing, while a wPSI represents a collection of PSIs that matches a RegEx, but with the limitation of having the RegEx at the end of the username part. wPSIs enable optimization of the O&M of the CSCF.

wPSI is an extension of the PSI handling, and allows defining a group of PSIs with the provisioning effort of an individual PSI. For example, Tel: +1234!.*!.

If the identity received from the I-CSCF does not match any individual provisioned PSI, the HSS performs a wPSI search. The wPSI in the HSS has a profile associated like any other user public identity.

A typical use case for wPSI is in the Business Trunking solution (BT VPN) of Ericsson, where wPSIs are used to identify unregistered PBX users.

4.6.5 Service Invocation for Non-Provisioned User

The CSCF handles invocation of an AS, when a session invitation to a non-provisioned user has occurred. The application is executed at the terminating session leg by the I-CSCF.

When the CSCF receives a terminating request URI from a non-IMS user, the CSCF provides a mechanism to start an AS, based on a configurable number range or usernames for non-IMS users (unallocated routing). The CSCF translates and maps these kinds of requests to some service URIs (through the HSS), where the AS is started.

4.6.6 Application Server Dynamic Allocation

This functionality provides a dynamic mechanism to achieve load balancing and redundancy of ASs while also maintaining network efficiency without requiring complex configuration.

The ASs can be deployed in a pooled deployment achieving load balancing and redundancy and still a user throughout the registration time can be routed to the same AS instance.

The cache is updated with the new AS address when the user is redistributed. It is possible to configure a trigger to recache stored AS instances.

4.7 Enterprise

4.7.1 Dynamic User Identity Support

Multimedia services provided by IMS networks can be extended to users not provisioned within the IMS network. They can be provided to users that belong to a Wholesale Partner (WP) of the IMS operator.

The DUIS solution is composed of the DUA-R, the Dynamic User Association Server (DUA-S), and the Dynamic User Association Database (DUA-DB). The I-CSCF provides the role of the DUA-R.

The users of the WP are not provisioned in the IMS network but are assigned a dynamic user identity for the use of the services offered by the IMS system. The IMS routable identity is used for registration, originating, and terminating requests. The WP user is assigned an IMS routable identity when registered in the IMS network. The mapping between the WP user identity (also called the external identity) and the IMS routable identity within the IMS network is maintained by DUA-S.

The I-CSCF implements the DUA-R part of the DUA solution by mapping the external identity of the WP users that could either be the domain or telephone number of the user to the IMS internal identity for terminating request. DUA-R performs an LDAP query to the DUA-DB for external identity to specific IMPU mapping. Originating COOB requests from an AS are assumed to use the IMS internal identities.

A WP user is represented by a specific-IMPU within a wIMPU range. For the DUIS solution, there is no restriction for the number of simultaneous sessions for wIMPU user.

4.7.2 Wildcarded Public User Identity

A Wildcarded Public User Identity (wIMPU) represents a collection of Public User Identities that share service profile and are included in the same Implicit Registration Set. wIMPUs are introduced to support PBXs where thousands of numbers can be registered from a single identity (the PBX entity IMPU). The users can be divided in subgroups of wIMPU which share a common service profile.

When the IP-PBX SIP client registers its contact address along with the wIMPU identity, the S-CSCF downloads the common service profile associated to this wIMPU identity. Any request made from a user of the IP-PBX, triggers the originating services specified in the common service profile. Any request made to a specific user of the IP-PBX users also triggers the terminating request triggers of the common service profile.

The P-CSCF stores the wIMPUs during the registration procedure. When a non-REGISTER request generated by terminal behind PBX is received by the P-CSCF, the P-CSCF does “longest & best” (RegEx) match of Public-Identity against the wildcarded public identities. If a match is found, the P-CSCF inserts



the P-Profile-Key header in the request to the S-CSCF to indicate that the request is from a wIMPU user.

The I-CSCF also provides backward compatibility for HSS vendors who have implemented their Cx interface according to the 3GPP specification release before TS29.228 v8.8.0/v.9.1.0 and TS29.229 v8.9.0/v.9.1.0. When a wIMPU AVP (code 636) is received from HSS in a LIA message, it is processed by the I-CSCF in the same way as if the Wildcarded Public Identity AVP (code 634) is received.

4.7.3 IP-PBX Interconnection

SIP Trunking services are provided for the IP-PBX rather than for the users served by the IP-PBX.

The SIP Trunking solution can be implemented in different ways as follows:

- Static mode connection

The SIP Trunking solution enables secure connection of IP-PBX through SIP trunks to the IMS operator border in static mode connection. PSI functionality is used to route to a SIP Trunking AS.

- Dynamic mode connectivity where the IP-PBX connects with the IMS using an IMS registration. It can be achieved as well in different ways with the following:

- IMS procedures by using loose routing as specified by ETSI TISPAN TS 182 025. This is in line with the wIMPU solution, where the IP-PBX registers a main PBX identity as a Distinct IMPU which is provisioned with a wIMPU containing a regular expression where all Specific IMPUs matching the regular expression implicitly are registered.
- SIP Connect1.1 as specified by [RFC 6140](#) and in 3GPP 24.229 Bulk Number Contact is supported. This functionality enables that each of the Addresses of Record (AORs) associated to the SIP PBX are registered in bulk map to a unique set of contacts.

4.8 Authorization

4.8.1 Access Awareness

The CSCF is enabled for access awareness in the sense that the S-CSCF and other nodes can behave differently depending on the access type in the PANI header.

The way nodes in the IMS system can identify the access type is through the SIP header PANI. The P-CSCF asserts the validity, based on configuration, of the access type in the PANI header from the UE before forwarding it to the rest of the IMS nodes. If the PANI header is missing from the UE, then a correct one is generated by the P-CSCF.

During a registration, the S-CSCF identifies the configuration profile to apply both during the registration and for all other SIP requests. On a received register request, the CSCF extracts the access type from the PANI header.

The access type is matched against the configured profiles. If there is no match, or no PANI header is present in the message, the S-CSCF uses the default configuration profile.

The matching of access-types against configuration profiles is only performed for initial register requests.

The following configuration is considered to be access-aware:

- Registration Properties (Registration timer, and so on)
- Authentication Properties (Authentication type)

4.8.2 Roaming Awareness

The CSCF maintains information on the roaming status of a user, and can relay this information in charging output to charging systems. The information is also included in the PANI at message sending to ASs.

4.8.2.1 Fixed Roaming Restriction

The CSCF retrieves location-related data for further processing by roaming restriction logic in the home network. In the home network, the HSS node can use the supported CSCF information, at roaming aware restriction features.

4.8.2.2 Mobile Roaming

At wireless network access, the mobile network roaming information (MCC, MNC, roaming status) is sent by the HSS to the CSCF as part of the user service profile. This data is stored by the S-CSCF in the PANI header and included in the charging output to charging systems.

4.8.2.3 IMS Roaming

At registration and re-registration requests, the parameter P-Visited-Network-ID is added by the P-CSCF. The value is read from an operator configurable CSCF parameter. Any received P-Visited-Network-ID information is discarded by the P-CSCF. This own network identity is used by the HSS to check the roaming agreements between the home network and a possibly visited network.

4.8.3 Media Authorization

Media Authorization allows the enforcement of user level policy regarding the characteristics of the media flows, to be used during a SIP session.



The User Level Media Authorization applies operator-defined policies on SDP session descriptions that are negotiated between the endpoints.

The User Level Media Authorization procedure occurs both on Originating and Terminating half-calls. Media authorization is not performed for SIP messages received on the ISC interface, as ASs are regarded as trusted and the ASs are assumed to have knowledge about the media policies that are valid for the user.

Media policies are configured in the S-CSCF. A reference to the media policy to apply for this user is included in the user profile downloaded from the HSS.

When a user negotiates media characteristics, the S-CSCF ensures that the media components being negotiated are allowed by the Media Policy assigned to this user. The S-CSCF analyzes if all payload types are allowed according to the policy, and that the number of media components per media type is not exceeded.

If the media authorization fails, the S-CSCF rejects the session initiation attempt or session modification. Standardized emergency calls (through the E-CSCF) are not rejected by this media policy control. The charging output allows a media authorization initiated release to be distinguished from a normal session release.

4.9 Distribution Control

4.9.1 User Redistribution

The User Redistribution feature is used to redistribute registered IMS users from their current S-CSCF to the preferred S-CSCF. The User Redistribution function can be used after a previously failed S-CSCF is back in service, or after a change in the topology, for example, when a new S-CSCF node is added to the IMS network.

The following are different options on how to redistribute users:

- In the I-CSCF, the User Redistribution function is enabled and disabled by configuration. It is applicable for all REGISTER requests except Register Query. Originating and Terminating non-Register requests do not trigger the User Redistribution function. This applies to all users independently if the user is in a session or not.

When the function is triggered, the I-CSCF explicitly requests the S-CSCF capabilities from the HSS. Based on the capabilities received, the I-CSCF selects an S-CSCF using the Resource Broker List.

After the user is moved to another S-CSCF successfully, the HSS sends an RTR to the previous S-CSCF to de-register the users who have been moved to another S-CSCF.

- In the S-CSCF, the User Redistribution function is enabled and disabled by configuration. To enable the User Redistribution function in the S-CSCF, set the administrative state to Shutting Down. The Graceful shutdown function

rules are applicable. A CSCF user is redistributed only if it does not have active sessions ongoing, so the function does not disturb ongoing traffic.

The following are two variants for how to redistribute users from the S-CSCF:

- Redistribution to any S-CSCF instance:

The S-CSCF redistributes users by rejecting initial REGISTER and re-REGISTER requests, using a 480 response code. Then the I-CSCF can select a new available S-CSCF node using capabilities downloaded from the HSS.

- Redistribution to a predefined S-CSCF instance:

The S-CSCF redistributes users by redirecting initial REGISTER and re-REGISTER requests, using a 305 response code. In this case, the I-CSCF sends the original request to the S-CSCF indicated in the 305 response without involving the HSS.

4.9.2 Graceful Shutdown

The CSCF supports a procedure to shut down the S-CSCF administratively, and at the same time drain-out the users that are currently registered in the CSCF to a configured threshold without affecting the service to the users. This can be useful if one must remove the CSCF from traffic handling for example for planned maintenance, change of configuration, or update, upgrade, or move of some users to another node to reach even load between the S-CSCF instances.

When an operator puts the S-CSCF in state Shutting down, the S-CSCF starts to empty the node by activating the User Redistribution function. The S-CSCF monitors the number of registered users. When the number of registered users reaches a configured threshold, the S-CSCF changes the administrative state to Unlocked or Locked, depending on the Threshold level.

If the threshold is set to a value larger than zero, the S-CSCF changes to Unlocked state when the threshold is reached. Otherwise, the S-CSCF changes to Locked state when zero users remain in the S-CSCF.

Graceful shutdown is extended to be used in several scenarios that involve moving subscriber traffic between different CSCF instances completely or partially. To limit the signaling intensity, it is possible to configure the number of registration periods that can limit the time for moving all the subscribers from the node.

4.9.3 HSS Load Sharing

The CSCF supports several HSS configurations for load sharing of Diameter traffic by using realm-based Diameter routing for Diameter messages. The HSS-FE is stateless and not tightly connected to a range of subscribers, while the HSS monolithic is connected to the subscribers provisioned for it.



To load share between the HSS-FEs, the S-CSCF can be configured not to store the received HSS name and therefore sends all Diameter messages without Destination-Host AVP.

The quarantine functionality used when there is failure of the HSS monolithic can be disabled for HSS-FEs to reach load sharing for the remaining HSS-FEs.

Supported HSS configurations are as follows:

- Multiple HSS-FE nodes with proxy SLF
- Multiple HSS-FE nodes with redirect SLF
- Multiple HSS-FE nodes without SLF
- Single monolithic HSS
- Multiple monolithic HSS nodes with proxy SLF
- Multiple monolithic HSS nodes with redirect SLF

4.9.4 Diameter Throttling

Before routing a request to a node or a realm on Diameter Cx/Dx, the CSCF supports to check if the destination node (for example, HSS) or realm has been determined to be overloaded (based on 3004 Diameter To Busy responses), and can then, from that apply throttling at an appropriate rate.

The overloaded is monitored over a fixed window of a tunable size (in seconds). For that duration, a calculation is made for the percentage of busy responses for all requests. If the percentage is greater than a tunable upper threshold, the node/realm is determined to be overloaded.

Throttling can then be applied as a configurable percentage of the requests that are not sent to the destination node and the process that triggered the Diameter request continues as if a busy response was received from destination node.

When a Diameter request is not sent because of throttling, a SIP 500 response indicating service unavailable is sent. The `Retry-After` header is also included with a randomly generated value between the configurable minimum and maximum values.





5 Charging

5.1 General

The S-CSCF and E-CSCF are the CSCF modules that are involved in charging. The S-CSCF and the E-CSCF act as Charging Triggering Function (CTF), according to the principles outlined in the corresponding technical specifications: TS 32.260 and TS 32.299.

The S-CSCF and the E-CSCF, when performing the normal routing actions for the SIP signaling events they are handling, determine whether the SIP information represents a chargeable activity and then which type of charging mechanism to apply.

The S-CSCF supports the following charging models:

- The S-CSCF follows a centralized charging model in which the relevant charging and rating decisions are taken by the charging systems. As a CTF, the role of the S-CSCF is constrained to the determination of charging units to be used in charging and rating decisions by the centralized charging systems, controlling its use and reporting them to the charging system.
- The S-CSCF can produce charging relevant information for the Calling Party, Called Party, or both, according to the different traffic cases and configuration options defined.
- The S-CSCF can charge for both sessions and events.
- The S-CSCF supports both offline and online charging mechanisms.
- The S-CSCF maintains the notion and state machine handling of a stateful agent, supporting the notion of a fully maintained charging session associated to the user activity/service execution in place.

The E-CSCF supports offline charging only (for originating calls).

5.1.1 Charging Data and Charging Determination

The CSCF Charging Determination, for each SIP dialog, determines whether charging information is to be generated and sent to Charging Control. This is done by checking if the dialog matches defined charging triggers.

All triggers and AVPs in the following lists are not relevant for emergency calls and thus not applicable in the E-CSCF.

The following are some examples of charging triggers:

- SIP method

- Charging only on originating half-call, terminating half-call, or both
- Charging if user is roaming
- Charging if an AS is involved

When it is determined that charging information is to be generated, one or more subfunctions are activated depending on a configurable charging mode combined with the charging addresses of the user.

The charging mode can, if both offline and online charging are supported, be set to any of the following:

- No charging
- Offline charging only
- Offline charging and online charging
- Online charging has precedence
- Online charging only

The result of these charging triggers results in generated charging information sent to the Charging Server.

5.1.2 Flexible Charging

The operator can configure what SIP headers that are wanted in the charging output. If a request or response message contains the designated SIP header, the CSCF copies the header value into generic AVP, which can be used as general-purpose container of charging information to charging and billing system. This mechanism gives the operator a flexibility to generate a Call Detail Record (CDR) that contains information not previously mentioned but necessary for their business purpose.

In the E-CSCF, the generic AVP is supported, and it is enhanced to generate charging information for headers in the Provisional Requests (SIP 18x) as well.

To offload the charging system, it is possible to enable/disable event Accounting-Requests (ACRs) when receiving a SIP message and the S-CSCF performs an authentication challenge to the client. This is applicable for all SIP methods except SIP BYE.

The CSCF supports charging for Virtual Telephony Operator by logging on to the charging records the domain name of the user. The operator hosting IMS service for several virtual operators can identify and handle separately the charging records per virtual operator. The Called-Asserted-Identity and Calling-Party-Address charging AVPs are included in the charging output identifying the Virtual Operator by the domain name.

5.2 Offline Charging

Offline charging is a mechanism where charging information does not affect the service rendered. The offline charging function collects detailed information about multimedia sessions and events within IMS. The information is collected for billing, accounting, capacity and trend analysis, cost allocation, and auditing.

The charging client sends offline charging requests after final SIP responses.

The CSCF supports an AVP structure according to 3GPP Release 12.

An offline charging sequence for normal session handling without the need of Interim Reports from Charging Control Node back to the S-CSCF is shown in Figure 12. The S-CSCF also supports offline charging for event handling. This is applicable also for the E-CSCF.

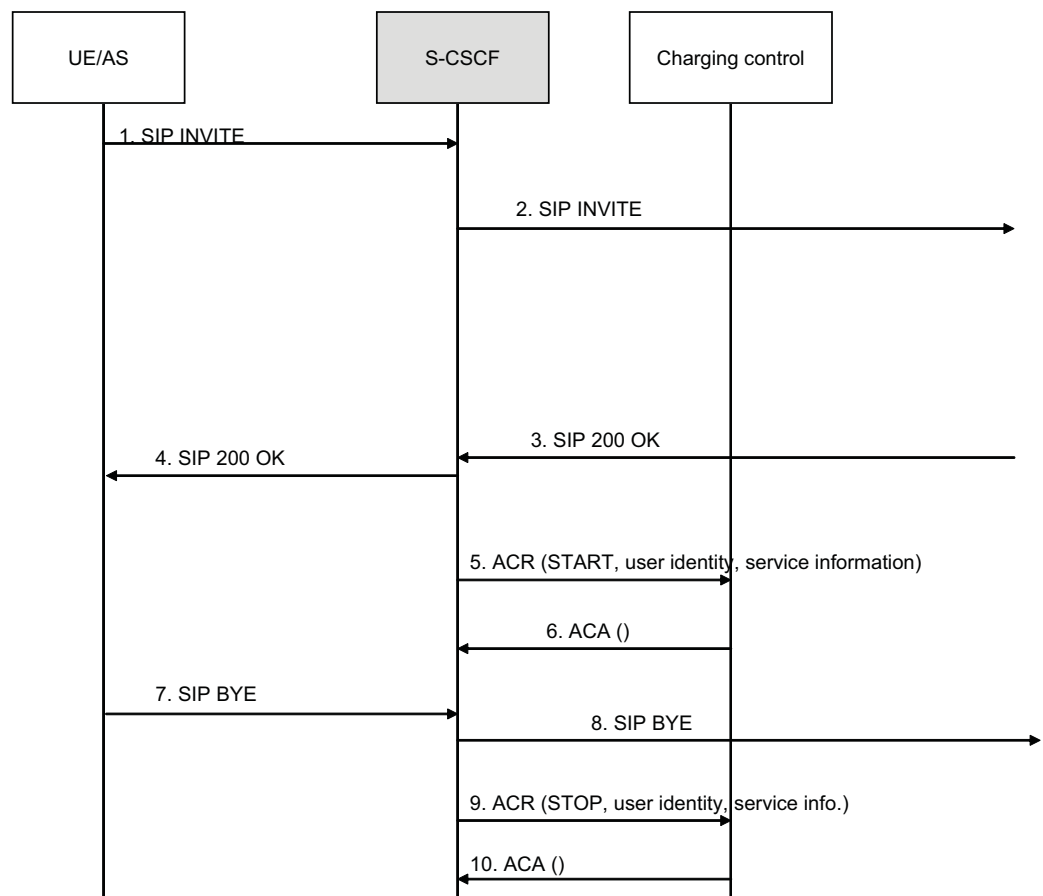


Figure 12 Offline Charging Sequence Diagram for Session Handling

5.3 Online Charging

If the charging determination process in the CSCF points to the use of online charging, an online charging session to the Online Charging System (OCS) is initiated.

The online charging is a charging mechanism, where charging information can affect, in real time, the service rendered, and therefore a direct interaction of the charging mechanisms with the session/service control is required.

The online charging feature is supported in the S-CSCF NE. The Diameter Credit Control Application (DCCA) is used.

For online charging, the basic functionality as defined by the IETF, the DCCA is used. The basic structure follows a mechanism, where the CTF, S-CSCF, requests resource allocation and reports credit control information to the OCS.

3GPP TS 32.299 defines the following three cases for online charging, where the CSCF uses Diameter credit control for sending these requests to the charging system:

- Immediate Event Charging (IEC)
- Event Charging with Unit Reservation (ECUR)
- Session Charging with Unit Reservation (SCUR)

The S-CSCF supports only ECUR and SCUR. The decision whether to apply ECUR or SCUR is based on SIP message.

The credit control messages contain service information from SIP signaling that is used for rating of the service. The OCS performs centralized rating, credit control, credit reservation, and deduction of user prepaid accounts.

An online charging sequence for normal session handling and Forwarding of the INVITE after confirmation of quota granted is shown in Figure 13.

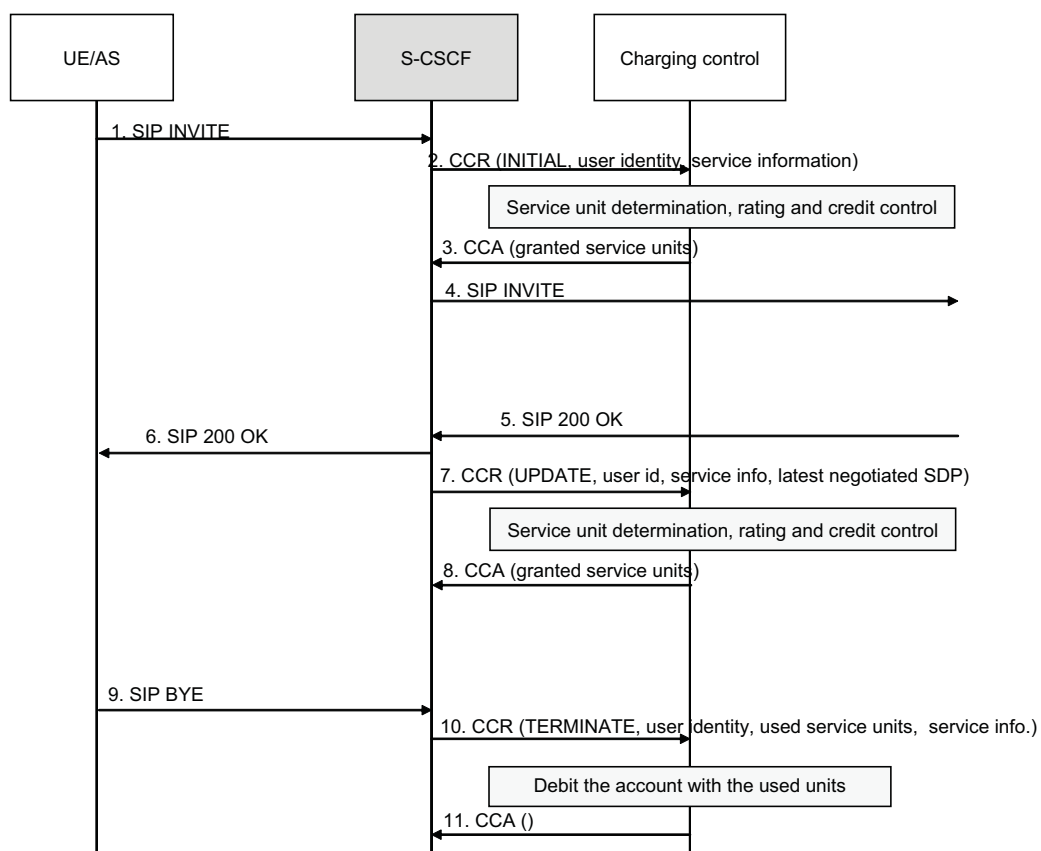


Figure 13 Online Charging Sequence for Normal Session Handling





6 Life Cycle Management

The purpose of Life Cycle Management is to automate the handling of the VNF. By enabling that VNF Life Cycle Management operations can be started with a single click (or be scheduled) and that the execution is automated, the operating expenses are reduced. Furthermore, technical VNF knowledge is no longer required to operate the VNF.

VNF Life Cycle Management is supported by providing workflow implementations (delivered with the VNF) which are deployed in a Virtual Network Function Manager (S-VNFM).

VNF Life Cycle Management is available and supported for the following deployment scenarios as depicted in Figure 14:

- 1 Full stack deployment scenario that includes vCSCFs, an Ericsson Network Manager (ENM), an Ericsson Cloud Manager (ECM), and a Cloud Execution Environment (CEE).
- 2 Small stack deployment scenario that includes vCSCFs, an ENM, and a CEE.
- 3 Small stack VMware deployment scenario that includes vCSCFs, an ENM, and a VMware.

Full Stack and Small Stack

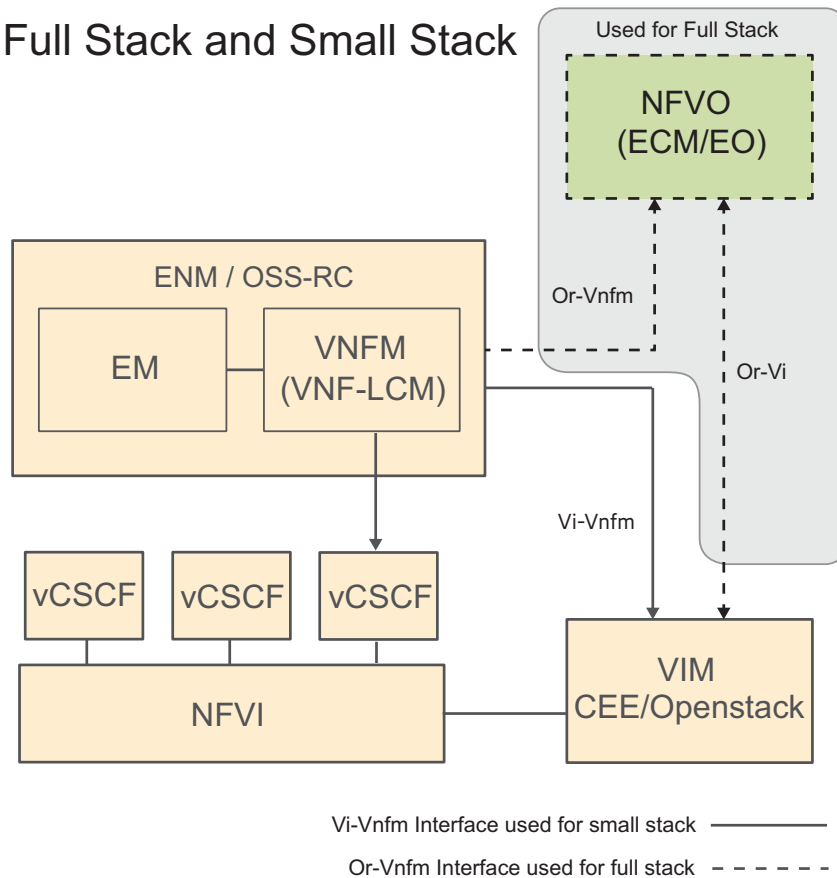


Figure 14 Full and Small Stack Deployment Scenarios

Life Cycle Management is only supported for deployments in which an ENM/OSS-RC is present and for full stack scenarios where the ECM is the only supported orchestrator. It is possible to deploy VNF-LCM separate from ENM/OSS-RC for test or proof of concept purposes.

For a small stack scenario, the workflows are triggered through the VNFM Graphical User Interface (GUI). The implementation uses the Vi-Vnfm interface for instantiation and the VNF NBI for configuration. For a full stack scenario, the workflows are triggered through the ECM using the Or-Vnfm interface. However, it is also possible to use workflows triggered on VNF-LCM in a full stack scenario.

Table 1 and Table 2 list supported workflows for VNF operations in full stack and small stack respectively. Additions of new workflows, or new functionality in existing workflows, are made in coming releases. New functionality can potentially be made available as early deliveries upon request.

Table 1 VNF Operations in a Full Stack Scenario

Operation	EO Initiated	VNF-LCM Initiated
Onboarding	Not automated	Not automated
Instantiation	Supported	Not supported



Operation	EO Initiated	VNF-LCM Initiated
Managed Scale-out (Graceful and Forceful)	Not supported	Not supported
Managed Scale-in (Graceful and Forceful)	Not supported	Not supported
Termination	Supported	Supported
Time-Based Auto Scaling	Not supported	Not supported
Auto Healing	Not supported	Not supported

Table 2 VNF Operations in a Small Stack Scenario

Operation	VNF-LCM Initiated
Onboarding	Supported
Instantiation	Supported
Managed Scale-out (Graceful and Forceful)	Supported
Managed Scale-in (Graceful and Forceful)	Supported
Termination	Supported
Time-Based Auto Scaling	Supported
Auto Healing	Supported

6.1 Onboarding

The onboarding workflow supports the preparation of the VNF for instantiation.

6.2 Instantiation

The deployment and instantiation of vCSCF becomes a simple operation using this workflow. The vCSCF is delivered containing an image file, which includes all the needed vCSCF components preinstalled. The software package is downloaded from software gateway and includes image file, hot files, and files for site configuration. Site configuration is mainly defined in a HOT environment file that must be updated before the workflow is initiated.

After that, the instantiation workflow has been executed the node can be unlocked but application-level configuration is needed before the node is operational. Application level configuration is not supported in a workflow.

The vCSCF VNF is always deployed as a 2+2 system and manual scale out is used to scale out the system to the wanted size.

6.3 Termination

The termination workflow supports termination of a VNF instance by which the VNF is taken out of service and the stack is deleted.

Termination of a VNF can either be done forcefully or gracefully. Current implementation of the workflows only supports forceful termination for which the VNF is taken out of service immediately.

6.4 Managed Scale-Out

The managed scale-out workflow makes it possible to adjust the size of the VNF in a simple way. The reason for doing this can be to adjust the size of the VNF to the actual level of traffic. Scaling is also used after instantiation to scale out the node to the wanted size.

Note: This scenario is not supported to be triggered from the ECM. It can however be used for a VNF which has been instantiated from the ECM.

6.5 Managed Scale-In

The managed scale-in workflow makes it possible to reduce the size of the VNF. It is also possible to point out which VM is to be scaled in.

The following scale-in types are supported:

- Graceful scale-in is used for minimizing the traffic disturbance.
- Forceful scale-in is used when traffic disturbance is acceptable.

Note: This scenario is not supported to be triggered from the ECM. It can however be used for a VNF which has been instantiated from the ECM.

6.6 Time-Based Auto Scaling

The customer can schedule automatic scale-in and scale-out operations based on the time of day. In this way, it is possible to use the available hardware and processing capacity efficiently. The functionality is available for CEE and OpenStack environment.

6.7 Auto Healing

Auto healing is supported to give the customer the possibility to recover a VNF, for example, when there is a hardware fault. The affected virtual machine is



recreated on another host, making sure that the VNF and the service it supports continue to run.





7 Security

The CSCF VNF is situated inside the IMS Core Network, which is part of the security Demilitarized Zone (DMZ). The DMZ in the cloud environment is achieved by traffic separation interfacing it to different Virtual Private Network (VPN) groups to restrict the CSCF VNF exposure to External Networks such as a non-IMS network or DMZ. eVIP supports internal firewall policies and packet filter rules that must be applied on Virtual IP Flow Entry (VIP FE) level. SBG (P-CSCF) in front of CSCF also enhances the protection against Denial-of-Service (DoS) and Distributed Denial of Service (DDoS) attacks. The L2 and L3 firewalls/switches deployed by the cloud infrastructure are also capable of handling DoS and DDoS attacks.

The CSCF VNF can be deployed in a Private Cloud Environment Infrastructure as a Service (IaaS), owned by an operator or an Ericsson Cloud System (ECS), based on Ericsson BSP 8100 hardware. The CSCF VNF must be always protected with External Network infrastructure and firewalls in a private cloud-only deployment and can be never put standalone in the Internet or public cloud environment.

The CSCF VNF includes hardening guidelines, which are done when the VNF is deployed. The [CSCF Hardening Guideline](#) is a document for a process to reduce the security risks by eliminating known vulnerabilities during installation, for example, removal of unnecessary software, or disabling insecure and unused services. The hardening guideline also includes what ports and listening services that must remain open and running to minimize the risk for unused ones not been used for vulnerability exploitation. Hypervisors must be hardened by the operator (the owner of the IaaS) before the CSCF VNF installation. Only security certified 3PP components are to be used by the cloud infrastructure.

The [CSCF Hardening Guideline](#) is updated with the input from the Vulnerability Analysis, which is an in-house security quality assurance test where the CSCF VNF hardening, security configuration, and characteristics are verified. The VNF is also analyzed for known vulnerabilities in 3PPs, which are mitigated during the development phase or in a Correction Package. However, 3PPs deployed in the private cloud infrastructure, owned by the operator, must be analyzed for vulnerabilities and mitigated to avoid that these are used for back-door attacks.

The CSCF VNF handles sensitive data in storage and transit such as subscribers data, user account, password, License Keys, crypto-keys, certificates, charging data, and application logs data. The data in transit signaling must be protected with IPsec tunnels and O&M with TLS. The data in storage must be protected with strict access control, data isolation, or encryption to avoid any disclosure and breach of data as storage resources are shared in a non-trusted multi-tenancy cloud infrastructure.

The CSCF VNF also supports the VNF user Identity and access management based on Role-Based Access Control RBAC centralized LDAP Authentication and Authorization Server. Audit logging and full personal accountability that cover the VNF user activities are also supported.





8 Operation and Maintenance

8.1 Fault Management

Fault Management is the detection and correction of abnormal network behavior. Each CSCF detects faults and starts recovery actions. Faults that require manual intervention are presented as alarms in the Man–Machine Interface of the CSCF and reported to the subnetwork management system over the Machine-Machine Interface, Simple Network Management Protocol (SNMP) v3.

Fault Management provides functions for detection and isolation of improper behavior within the CSCF. The CSCF modules provide fault information based on international standards, including ITU-T recommendation X.733, which defines an information model for all alarms including the alarm information structure, semantics, severity, and category and the transfer interface. The CSCF always indicates the severity of the alarm and for each fault there is an operational procedure to help correcting the fault. The Fault Management Information Model is based on the ERICSSON-ALARM-MIB. The Alarms are available on the SNMP interface.

For alarms that are tied to a specific VM instance a Universally Unique Identifier is included in the `additionalInfo` field of the alarm. This identifier is used to correlate the alarms to a specific VM.

Fault Management logs all events and alarms to files in the CSCF and can be also viewed by CLI.

The CSCF reports alarms to the external subnetwork management and Network Management System, which collects and aggregates the alarms from all nodes to give a unified view of the state of the system.

8.2 Performance Management

Performance Management is the process to produce, transfer, collect, store, aggregate, and present measurement data, which can be used to verify the physical and logical configuration of the network and to locate potential problems as early as possible. The subnetwork management system collects, stores, aggregates, and presents the measurements from all nodes to give a unified view of the state of the system.

The CSCF supports performance data transfer based on industry standards. Statistical real-time counters or scheduled data can be transferred from the CSCF modules to management applications.

The Performance Management data is used by external subnetwork managers to build performance reports. It is also used by the network administrator to assess the performance level of the managed element and subnetwork. Some examples of such reports are: SIP Traffic Summary Report, Traffic Hourly

Report, SIP Characteristics Report, and so on. The CSCF does not build any performance reports; the external subnetwork manager generates these reports. The subnetwork manager is not included with the CSCF product.

The output format of the PM counters is XML Schema Documentation (XSD), compliant with 3GPP TS 32.435 v10.0.0.

The CSCF supports many Performance Counters on access and media types which can be used for statistics or troubleshooting purposes.

8.3 Configuration Management

The CSCF supports the configuration of the CSCF application and its Managed Objects. The CSCF application provides two interfaces for Configuration Management interface: a Man–Machine Interface ECLI and a Machine to Machine XML-based interface according to the network configuration protocol (NETCONF) as described in [RFC 4741](#). NETCONF is a session-based Network Management protocol, which uses XML-encoded Remote Procedure Calls (RPCs) and configuration data to manage network devices. The managed information model is compliant to the Ericsson Common Information Model (ECIM).

Configuration Management of the hardware platform is handled outside of the CSCF application.

8.4 Software Notification

The CSCF supports notification of any changed Managed Objects through Notifications through NETCONF. The capability to support subscribing and receiving asynchronous event notifications is described in [RFC 5277](#).

The CSCF supports Configuration Management notifications, which are events that are triggered whenever changes are made to one or many configuration parameters in the system. The events result in one or many NETCONF Notifications.

The CSCF also supports General Notifications, which are events that are triggered whenever a general change occurs in the system, that is, not Configuration Management changes.

General notifications can consist of the following:

- Node administrative state changes
- Read-only parameter state changes
- Capsule Abortion (software crashes) notification



8.5 Traceability and Troubleshooting

Signaling trace (NetTrace) provides the capability to trace SIP transactions encompassing related protocol messages that traverse the CSCF, provided they match specified filter criteria. It is also possible to trace Diameter messages for the Cx interface. Transactions are represented in the XML trace data format described in 3GPP TS 32.423.

The trace level can be set to one of the following:

- Max – The protocol is traced in raw format
- Min – Only the most important headers are traced

The XML files can be transferred to the Network Management System.

This feature can be used for troubleshooting by customer support center of operator, interoperability testing, and so on, with the benefit of improved Total Cost of Ownership (TCO).

The CSCF can also perform User Trace for single public user (IMPU) communication that is traversing the CSCF. With the User Trace, the operator can define the IMPU identity together with a Trace Profile (for example, domains such as Registration or traffic sessions) that is of interest to collect the activities related to the user session for fault finding and localization of potential issues.

It is also possible with commands to, in real time, print the User Data (such as session, registration) that is cached in the CSCF from the public or private user identity of the Individual user.

For print-out of all user data in the system, an export function exists for offline processing.

To support in-depth troubleshooting, the CSCF appends a hexadecimal code specific to the generation point to the response phrase. There is also an error response and a reason catalog in the library to describe the different generation points in the node.

The CSCF provides a facility to execute automated health checks on the node. The automated procedure generates reports on key aspects of the CSCF configuration, settings, and values. The information is output into user-friendly reports which make the manual analysis quick and easy. The automated health check takes a short time to execute and can be run daily or before or after an upgrade.

The CSCF supports logging of historical event information for fault isolation. When serious events occur, for example, software process crash or other error situations, the system logs important state information. This logging function has a configurable filter for SIP Error codes, SIP Hexadecimal Error Codes, repeated errors and Log rate limitations.





9 Interfaces and Protocols

The main protocols that are used in the CSCF are the following:

- SIP/SDP

The CSCF supports the SIP/SDP signaling protocol suite as defined by the IETF [RFC 3261](#). SIP is transported using either TCP or UDP.

- Diameter

The CSCF supports the Diameter base protocol and the relevant extensions as defined by the IETF and 3GPP, along with accounting extensions specified by the relevant standards bodies. Diameter is transported using TCP or SCTP.

- Management protocols

The CSCF supports SNMPv3, LDAPv3, NETCONF, Ericsson Command-Line Interface (ECLI), HTTP, SFTP, and SSH® for management access.

- UDP

The CSCF supports the User Datagram Protocol as defined in IETF STD 6.

- HTTP/SOAP/XML

The MI reference point is the interface between the E-CSCF and the LRF to translate emergency numbers. HTTP Post message and SIP are supported.

- TCP

The CSCF supports the Transmission Control Protocol as defined in IETF STD 7.

- SCTP

The CSCF supports the Stream Control Transmission Protocol (SCTP) as defined in IETF [RFC 4960](#).

- IPv4

The CSCF supports IP version 4 according to IETF STD 5.

- IPv6

The CSCF supports IP version 6 according to [RFC 2460](#).

- LDAP v3

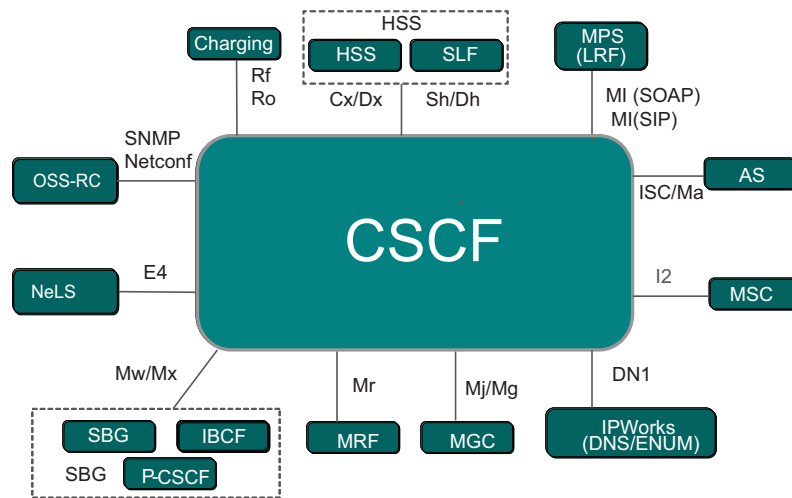


Figure 15 CSCF Logical Architecture and Interfaces

Table 3 Supported Interfaces and Protocols Used by CSCF

Interface	Protocol
Traffic	
CSCF – MRF: Mr	SIP/UDP or TCP
CSCF – MGC: Mj, Mg	SIP/UDP or TCP
CSCF – CSCF: Mw, Mx	SIP/UDP or TCP
CSCF – AS: ISC, Ma	(SIP)/UDP or TCP
CSCF – HSS: Cx, Sh	Diameter/TCP/SCTP
CSCF – SLF: Dx, Dh	Diameter/TCP/SCTP
CSCF – CDF: Rf	Diameter/TCP/SCTP
CSCF – OCS: Ro	Diameter/TCP/SCTP
(E)CSCF – RDF/LRF: MI	HTTP/SOAP/XML or SIP
CSCF – DNS/ENUM: DN1	DNS/UDP or TCP
CSCF – Network License Server (NeLS): E4	Apache® Thrift



Interface	Protocol
Operations, Administration, and Maintenance	
CSCF – OSS: Fault, performance, configuration management (secure or normal), secure remote logon	SNMP v3/TCP FTP/TCP and SFTP/TCP LDAPv3 NETCONF HTTPS SSH ECLI

Note: This list is not the exhaustive list.





10 Reference Configuration and Cloud Enabled

The CSCF software application is delivered as a software-only product. It is not bundled with a hardware platform. The CSCF is verified on a reference configuration consisting of Ericsson Cloud Execution Environment (CEE) and BSP 8100. This documented solution is typically referred to as vCSCF Cloud Enabled.

Although not being a bundled product, the Cloud Enabled concept provides the following:

- A verified installation and upgrade of the vCSCF VNF on the Cloud Enabled configuration
- A more predictable dimensioning of the CSCF VNF compared to using any hardware and any cloud infrastructure
- A verified behavior of the CSCF VNF and an IMS solution on the Cloud Enabled configuration
- A clear and described configuration including networking for the Cloud Enabled configuration
- Support for all products constituting the Cloud Enabled solution

Although the vCSCF VNF is verified using the Cloud Enabled reference configuration, the virtualization makes it possible for the CSCF software application to run over any hardware platform and cloud infrastructure.

The CSCF application has been verified with the OpenStack KVM hypervisor virtualization layer deployed on the BSP 8100 hardware platform and cloud infrastructure.