

CSCF Security User Guide

Call Session Control Function

USER GUIDE

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
1.1	Prerequisites	1
1.2	Environment	1
2	Product Security Functionality	3
2.1	Authentication	3
2.2	Authorization	4
2.3	Accountability	4
2.4	Integrity	4
2.5	Confidentiality	5
3	Security Configuration	7
3.1	Procedures	7
3.2	Recommended Periodic Operations	9
3.3	Handling of Patches	10
4	Default Parameter Values	11
5	Services, Ports, and Protocols	13
5.1	Listening Services	13
5.2	External Traffic Port Numbers	14
5.3	Operation and Maintenance Port Numbers	14
5.4	Diameter Port Numbers	15
5.5	SIP IP Flows	15
5.6	DNS IP Flows	19
5.7	Diameter IP Flows	20
5.8	IP Flow through DUA-DB LDAP	23
6	Privacy	25
6.1	Subscriber Notice	25
6.2	Consent	25
6.3	Handling of Personal Subscriber Data	26
6.4	Classification of Personal Subscriber Data	31





1 Introduction

This document describes the security functions implemented by the Call Session Control Function (CSCF). It also describes the security-related procedures that can be performed by the system administrators.

The CSCF is an essential module in the IP Multimedia Subsystem (IMS) for processing signaling data, using the Session Initiation Protocol (SIP) and Diameter as signaling protocols. It supports Internet Protocols on a scalable and high-performance platform. The CSCF can be deployed as a virtual network element in an IMS network. For details about the CSCF, the supported functionality, and the nodes it communicates with, see [CSCF Technical Description](#).

1.1 Prerequisites

This section describes the conditions required for performing security management on the CSCF.

1.1.1 Conditions

Before performing the procedures in Section 3.1 Procedures on page 7, the following conditions must apply:

- The CSCF Virtual Network Function (VNF) is installed and initially configured. The initial configuration includes the necessary settings for the authentication of the Northbound Interface (NBI) users and their authorization.
- The intended software level to be run in the CSCF is installed. The release information can be found in delivery reports, delivery specifications, delivery notes, release notes, or correction notes.
- The user has the required access privileges, and the required usernames and passwords are known.
- A System Security Administrator access role is required.

1.2 Environment

This section describes the environment requirements for product operations.

The CSCF belongs to the IP Multimedia Core Network (IMCN) and it is indirectly connected to the access network by the Session Border Gateway (SBG), which offers firewall capabilities and provides protection from external attacks.



The CSCF is placed in the Service & Control Virtual Private Network (VPN) group, which includes Network Functions handling signaling traffic without direct connection to external networks.

The following VPNs exist in the group:

- The Signaling Service Control VPN for signaling traffic to and from other IMS Network Nodes.
- The Operation and Maintenance Service Control VPN for Operation & Maintenance (O&M) traffic used for IMS Network nodes in the group.
- Charging VPN for offline (Rf) and online (Ro) traffic.

For more details, see [CSCF VNF Network Connectivity Overview](#).



2 Product Security Functionality

The following security functionality is supported in the product:

- Authentication
- Authorization
- Accountability
- Integrity
- Confidentiality

2.1 Authentication

2.1.1 Subscriber Authentication

The CSCF supports the following authentication procedures:

- IMS Authentication and Key Agreement (AKA)
- Authentication through trusted gateway
- Authentication through trusted Application Server (AS)
- NASS Bundled Authentication (NBA)
- GPRS IMS Bundled Authentication (GIBA)
- Digest authentication
- Optimized Digest

2.1.2 O&M User Authentication

The CSCF supports O&M password-based and key-based user authentication. For more information, see [User Management](#).

2.1.3 Mutual Authentication of Communication Channel Peers

The CSCF supports certificate-based mutual authentication for the following:

- Lightweight Directory Access Protocol (LDAP) over Transport Layer Security (TLS), between the CSCF and the LDAP server, see [Certificate Management](#).
- Internet Key Exchange version 2 (IKEv2) during the establishment of the IP Security (IPsec) Security Associations, between the CSCF and any peer, see [eVIP Management Guide](#).



2.2 Authorization

The CSCF supports O&M User Authorization.

Authorization is the capability to validate if the logged in user is allowed to perform a certain operation to a certain Managed Object (MO). The authorization is role-based, that is, the logged in user is mapped to a role and each role has one or several rules defining the access right to an MO.

For a description of the user management principles, user administration, and user roles, see [User Management](#).

2.3 Accountability

The audit log enables logging and tracking access to files, directories, and resources of the system, as well as tracing system calls. It enables oversight of the system for application misbehavior or code malfunctions.

For more information, see [Audit Information](#).

2.4 Integrity

2.4.1 Node Integrity

The CSCF supports node integrity in the following ways:

- Verify and protect the integrity of the system configuration files.
- Protect and prevent unauthorized modification of the selected files or folders.
- O&M Roles and Rules provide integrity protection by role and target-based access control.

2.4.2 Communication Integrity

The CSCF supports communication integrity in the following ways:

- Integrity protection of O&M traffic (also including Charging Data Records, backups, logs)
- Integrity protection of signaling traffic
- TLS provides for integrity protection



2.5 Confidentiality

The CSCF supports communication confidentiality in the following ways:

- Confidentiality protection of O&M traffic (including Charging Data Records, backups, logs)
- Confidentiality protection of signaling traffic
- TLS provides for confidentiality and integrity protection, and mutual authentication of the peers
- NETCONF is protected using Secure Shell (SSH), and TLS can be also used
- Signaling traffic like SIP and Diameter can be protected by IPsec tunnels with authentication





3 Security Configuration

3.1 Procedures

This section provides the instructions for operating the security functionality of the product.

3.1.1 Hardening

Perform hardening of the CSCF node according to the procedures, see [CSCF Hardening Guideline](#), including the following steps:

- Allow or block ports for all listening services
- Change default passwords, including predefined password for root that can be known by many persons
- Disable root access through NBI, remote logon for root user is enabled by default
- Enable strong password enforcement
- Force password change and aging
- Configure Ericsson Command-Line Interface (ECLI) inactivity timer
- Create emergency user, at least one emergency user must be configured in the system
- Delete unused local Linux® accounts, if additional users are created during installation, and they are not to be used, they must be deleted
- Block Network File System (NFS) against access from external networks

The operator can have their own security policies, where the node must be hardened according to operator requirements, for example, defining specific secure protocols or other ports different than the default ones.

After the hardening activities have been performed, create a backup of the system and upload the backup to external storage.

3.1.2 Authentication and User Management

For instructions on how to create users and user groups, and assign privileges to a group, see [User Management](#). Always use personal accounts instead of shared or generic user accounts.



The CSCF has the following predefined default roles. The roles, and the corresponding rules, cannot be modified:

- CSCF Application Administrator
- CSCF Application Operator
- CSCF Application Security Administrator
- Local Authentication Administrator
- Self
- System Administrator
- System Read Only
- System Security Administrator
- System Troubleshooter

LDAP must be configured with the strongest possible ciphers.

For details on LDAP Authentication, Local Authorization, Roles, and Rules, see [User Management](#).

3.1.3 Audit Trails

The audit log enables logging and tracking access to files, directories, and resources of the system, as well as tracing system calls. It enables oversight of the system for application misbehavior or code malfunctions.

For information about where to find the audit and syslog log files, and how to read them, see [Audit Information](#).

3.1.4 Change Logon Banner

By default, no information is provided to the user when logging on using the Command-Line Interface (CLI). The operator can define their own customized greeting message or legal message when a user logs on through the CLI.

The system provides the file `/cluster/etc/motd`, which allows a text message to be created and later displayed when user logs on to the system through CLI.

3.1.5 IPsec Support

If there are requirements to protect Signaling traffic, for example, SIP or Diameter (when transferring charging or malicious call tracing data), IPsec tunnels can be used.



For a description of the procedures for setting up IPsec tunnels to protect signaling traffic, see [eVIP Management Guide](#).

3.2 Recommended Periodic Operations

The product must be properly hardened before it is taken into use. Nevertheless, it is important that the daily operations on the product are performed in such a way that the security status of the product is not weakened.

New vulnerabilities that must be mitigated are frequently found in the existing products. Therefore it is necessary to maintain the security posture of the product in service on a regular, ongoing basis.

The recommended periodic security-related operations are the following:

- Ensure that the latest software version is installed. Get the latest available Emergency Package (EP) version of the CSCF.
- Perform system backups regularly.
- Export backups to external storage regularly.
- Export logs to external storage regularly.
- Fetch Performance Management (PM) data from the CSCF regularly and store externally.
- Check the TLS certificates regularly to ensure that they do not expire.
- Run password checkers periodically to find weak passwords. This is done using third-party software.
Note: Do not install third-party software tools as part of the CSCF distribution.
- Monitor the file system integrity periodically, either manually or as a scheduled task. For more information, see [CSCF Health Check](#).
- Ensure that no unnecessary listening ports are open, for example, by using external tools such as “Nessus” to monitor the ports and check with the system documentation or by checking the system manually.
- Ensure that the ports for the insecure protocols Telnet and File Transfer Protocol (FTP) are closed.
- Ensure that no shared user accounts are used.
- Ensure that administrative user rights are assigned only to real needs.
- Check the audit logs that are related to potential security events regularly. Check anything that can be considered as strange according to the traffic



model of the operator besides error cases, such as failures to authenticate, too much user activity, and too many dropped or rejected sessions.

- Analyze log data and counters regularly to reconsider the chosen security-related attributes.

3.3 Handling of Patches

Patches are delivered in the form of EPs. The process to load EPs is described in the upgrade instruction for the actual CSCF EP.



4 Default Parameter Values

The default values for the security parameters are listed in Table 1.

Table 1 Default Parameter Values

Parameter	Default Value
Not Applicable	No default values





5 Services, Ports, and Protocols

This section provides information about network services in the system that are available from External Networks.

5.1 Listening Services

The listening services are shown in Table 2.

Table 2 Listening Services Ports and Protocols Used by the CSCF

Port	Protocol	Description	Listening Only on the Internal Network
22	TCP	Secure Shell (SSH/Secure File Transfer Protocol (SFTP))	No, configurable
67	UDP	Dynamic host configuration service (DHCP)	Yes
69	UDP	File transfer service (TFTP)	Yes
111	TCP/UDP	Portmap service (portmap)	No. The service is listening on the External Network, but it is serving only on the internal network.
123	UDP	Time synchronization service (NTP)	No
514	UDP	Log service (syslog)	Yes
1022	TCP	SSH/SFTP (only for LDEwS)	Yes
1128	TCP	Alarm service	Yes
1129–1131	TCP/UDP	Node service	Yes
2049	TCP/UDP	Network File System (NFS)	No. The service is listening on the External Network, but it is serving only on the internal network.
7788	TCP	Disk replication service (DRBD)	Yes

The standard SSH server is started up by Linux Distribution Extensions (LDE) with a default configuration, listening on default port 22 on all networks. Also on Linux Distribution Extensions with SUSE™ Linux Enterprise Server (LDEwS), a second SSH server is listening on port 1022 on the internal network.



5.2 External Traffic Port Numbers

The ports listed in Table 3 must be available for external SIP and DNS traffic through the External Network Traffic VIP interfaces. The Access List, as part of the firewall policy in the VIP Gateway Router, is used to accomplish this availability. How to configure the router Access List depends on which router is used and is described in the documentation for the specific router chosen. These ports are used for If1, ISC, Ma, Mw, Mg/Mj, Mr, and MI interfaces. Other VIP Gateway Routers belonging to Operation and Maintenance (O&M), Charging, and Signaling Networks must block the access to the listed external ports in Table 3.

Table 3 External Access Ports and Protocols Used by the CSCF

Port Number	Protocol	Server Side	Use (Comment)
53	TCP	DNS server	DNS
53	UDP	DNS server	DNS
5060	TCP	CSCF	For SIP used by I-, S-, or E-CSCF, or EATF, or BCF, other port numbers can be used.
5060	UDP	CSCF	For SIP used by I-, S-, or E-CSCF, or EATF, or BCF, other port numbers can be used.

5.3 Operation and Maintenance Port Numbers

The ports listed in Table 4 must be available through O&M VIP Interface. The Access List, as part of the firewall policy in the O&M VIP Gateway Router, is used to accomplish this availability. How to configure the router Access List depends on which router is used and is described in the documentation for the specific router chosen. All the VIP Gateway Routers belonging to Charging and HSS/SLF must block the access to the listed external ports in Table 4.

Table 4 Standard O&M Ports and Protocols Used by the CSCF

Port Number	Protocol	Server Side	Use (Comment)
161	UDP	CSCF O&M	SNMP requests to Platform (Fault Management).
162	UDP	OSS	SNMP traps (messages) from Platform to SNMP Manager. Port number is configurable in Platform.
830	TCP	CSCF O&M	NETCONF



Table 4 Standard O&M Ports and Protocols Used by the CSCF

Port Number	Protocol	Server Side	Use (Comment)
2022	TCP	CSCF O&M	Ericsson Command-Line Interface (ECLI) over SSH
2028	TCP	CSCF O&M	SFTP over SSH
6513	TCP	CSCF O&M	NETCONF over TLS

5.4 Diameter Port Numbers

The ports listed in Table 5 must be available through the Charging or Signaling Diameter VIP interface. The Access List, as part of the firewall policy, in the Charging or Signaling Diameter VIP Gateway Router is used to accomplish this availability. How to configure the router Access List depends on which router is used and is described in the documentation for the specific router chosen. These ports are used for Charging or Signaling Diameter networks. All the VIP Gateway Routers belonging to Traffic and O&M Networks must block the access to the listed external ports in Table 5.

Table 5 Standard Diameter Ports and Protocols Used by the CSCF

Port Number	Protocol	Server Side	Use (Comment)
3868	TCP or SCTP	CSCF Diameter	Default Diameter port
3869 ⁽¹⁾	TCP or SCTP	CSCF Diameter	Additional Diameter port
3870 ⁽¹⁾	TCP or SCTP	CSCF Diameter	Additional Diameter port
3871 ⁽¹⁾	TCP or SCTP	CSCF Diameter	Additional Diameter port
3872 ⁽¹⁾	TCP or SCTP	CSCF Diameter	Additional Diameter port

(1) Port numbers 8700–8732 can be also used.

5.5 SIP IP Flows

SIP IP flows are described in Section 5.5.1 Ma Interface on page 16, Section 5.5.2 Mw Interface on page 16, Section 5.5.3 Mg/Mj Interface on page 16, Section 5.5.4 Ml Interface on page 17, Section 5.5.5 Mr Interface on page 18, Section 5.5.6 ISC Interface on page 18, Section 5.5.7 I4 Interface on page 19, and Section 5.5.8 I5 Interface on page 19.

The ports listed in the following subsections are configurable for all the external interfaces. The default port for SIP is 5060 according to [RFC 3261 SIP: Session Initiation Protocol](#).

Note: The CSCF originating port for TCP is ephemeral for outgoing traffic to the remote nodes. Therefore, the origin port for the TCP is not applicable in the tables in the subsections.



5.5.1 Ma Interface

The flows that must be available on the Ma interface are shown in Table 6.

Table 6 Ma Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
AS to CSCF (SIP)	IP address range or ranges allocated to AS.	Allocated ports to the AS	I-CSCF VIP	I-CSCF port	UDP and TCP
CSCF to AS (SIP)	I-CSCF VIP	I-CSCF port	IP address range or ranges allocated to AS.	Any	UDP and TCP

5.5.2 Mw Interface

The flows that must be available on the Mw interface are shown in Table 7.

Table 7 Mw Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
I-CSCF to S-CSCF (SIP)	I-CSCF VIP	I-CSCF Mw port	S-CSCF VIP	S-CSCF port	UDP and TCP
BCF to S-CSCF (SIP)	BCF VIP	BCF Mw port	S-CSCF VIP	S-CSCF port	UDP and TCP
I-CSCF to P-CSCF (SIP)	I-CSCF VIP	I-CSCF Mw port	IP address range or ranges allocated to P-CSCF.	Any	UDP and TCP
S-CSCF to P-CSCF (SIP)	S-CSCF VIP	S-CSCF Mw port	IP address range or ranges allocated to P-CSCF.	Any	UDP and TCP
P-CSCF to E-CSCF (SIP)	IP address range or ranges allocated to P-CSCF.	P-CSCF Mw port	E-CSCF VIP	E-CSCF port	UDP and TCP

5.5.3 Mg/Mj Interface

The flows that must be available on the Mg/Mj interface are shown in Table 8.



Table 8 Mg/Mj Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
MGC to I-CSCF (SIP)	IP address range or ranges allocated to MGC.	MGC Mj port	I-CSCF VIP	I-CSCF port	UDP and TCP
MGC to S-CSCF (SIP)	IP address range or ranges allocated to MGC.	MGC Mj port	S-CSCF VIP	S-CSCF port	UDP and TCP
MGC to E-CSCF (SIP)	IP address range or ranges allocated to MGC.	MGC Mj port	E-CSCF VIP	E-CSCF port	UDP and TCP
MGC to BCF (SIP)	IP address range or ranges allocated to MGC.	MGC Mj port	BCF/I-CSCF VIP	BCF/I-CSCF port	UDP and TCP
I-CSCF to MGC (SIP)	I-CSCF VIP	I-CSCF Mj port	IP address range or ranges allocated to MGC.	Any	UDP and TCP
S-CSCF to MGC (SIP)	S-CSCF VIP	S-CSCF Mj port	IP address range or ranges allocated to MGC.	Any	UDP and TCP
E-CSCF to MGC (SIP)	E-CSCF VIP	E-CSCF Mj port	IP address range or ranges allocated to MGC.	Any	UDP and TCP

5.5.4 MI Interface

The flows that must be available on the MI interface are shown in Table 9.



Table 9 MI Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
E-CSCF to LRF	E-CSCF VIP	E-CSCF MI port	Location Repository Function (LRF) IP address.	LRF Port number	HTTP/SIP
LRF to E-CSCF	LRF IP address	LRF MI port	E-CSCF VIP	E-CSCF Port Number	HTTP/SIP

5.5.5 Mr Interface

The flows that must be available on the Mr interface are shown in Table 10.

Table 10 Mr Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
MRF to I-CSCF (SIP)	IP address range or ranges allocated to MRF.	MRF Mr port	I-CSCF VIP	I-CSCF port	UDP and TCP
MRF to S-CSCF (SIP)	IP address range or ranges allocated to MRF.	MRF Mr port	S-CSCF VIP	S-CSCF port	UDP and TCP
I-CSCF to MRF (SIP)	I-CSCF VIP	I-CSCF Mr port	IP address range or ranges allocated to MRF.	Any	UDP and TCP
S-CSCF to MRF (SIP)	S-CSCF VIP	S-CSCF Mr port	IP address range or ranges allocated to MRF.	Any	UDP and TCP

5.5.6 ISC Interface

The flows that must be available on the ISC interface are shown in Table 11.



Table 11 ISC Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
AS to CSCF (SIP)	IP address range or ranges allocated to AS.	AS ISC port	S-CSCF VIP	S-CSCF port	UDP and TCP
CSCF to AS (SIP)	S-CSCF VIP	S-CSCF ISC port	IP address range or ranges allocated to AS.	Any	UDP and TCP

5.5.7 I4 Interface

The flows that must be available on the I5 interface are shown in Table 12.

Table 12 I4 Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
E-CSCF to EATF	E-CSCF IP Address	E-CSCF I4 port	EATF VIP	EATF Port number	SIP
EATF to E-CSCF	EATF VIP	EATF I4 port	E-CSCF IP address	E-CSCF Port number	SIP

5.5.8 I5 Interface

The flows that must be available on the I5 interface are shown in Table 13.

Table 13 I5 Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
I-CSCF to EATF	I-CSCF IP Address	I-CSCF I5 port	EATF VIP	EATF Port number	SIP
EATF to I-CSCF	EATF VIP	EATF I5 port	I-CSCF IP address	I-CSCF Port number	SIP

5.6 DNS IP Flows

DNS IP flows are described in Section 5.6.1 If1 Interface on page 20.

The ports listed in the following subsections are configurable for all the external interfaces. The default port for SIP is 5060 according to [RFC 3261 SIP: Session Initiation Protocol](#).



Note: The CSCF originating port for TCP is ephemeral for outgoing traffic to the remote nodes. Therefore, the origin port for the TCP is not applicable in the tables in the subsections.

5.6.1 If1 Interface

The flows that must be available on the If1 interface are shown in Table 14.

Table 14 If1 Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
I-CSCF to DNS	I-CSCF VIP	I-CSCF If1 port	IP address range or ranges allocated to DNS.	Any	UDP/TCP
S-CSCF to DNS	S-CSCF VIP	S-CSCF If1 port	IP address range or ranges allocated to DNS.	Any	UDP/TCP
E-CSCF to DNS	E-CSCF VIP	E-CSCF If1 port	IP address range or ranges allocated to DNS.	Any	UDP/TCP
EATF to DNS	EATF VIP	EATF If1 port	IP address range or ranges allocated to DNS.	Any	UDP/TCP
BCF to DNS	BCF VIP	BCF If1 port	IP address range or ranges allocated to DNS.	Any	UDP/TCP

5.7 Diameter IP Flows

Diameter IP flows are described in Section 5.7.1 Cx and Dx Interfaces on page 21, Section 5.7.2 Rf Interface on page 22, Section 5.7.3 Ro Interface on page 22, and Section 5.7.4 Sh and Dh Interface on page 23.

The ports listed in the following subsections are configurable for all the external interfaces. The default port for SIP is 5060 according to [RFC 3261 SIP: Session Initiation Protocol](#).

Note: The CSCF originating port for TCP is ephemeral for outgoing traffic to the remote nodes. Therefore, the origin port for the TCP is not applicable in the tables in the subsections.



5.7.1 Cx and Dx Interfaces

The flows that must be available on the Cx and Dx interfaces are shown in Table 15.

Table 15 Cx and Dx Interfaces

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
Cx					
HSS to I-CSCF (Diameter)	IP address range or ranges allocated to HSS.	HSS Cx stack port	I-CSCF CSCFCX stack VIP	I-CSCF CSCFCX stack port	TCP or SCTP or both
HSS to S-CSCF (Diameter)	IP address range or ranges allocated to HSS.	HSS Cx stack port	S-CSCF VIP	S-CSCF CSCFCX stack port	TCP or SCTP or both
HSS to BCF (Diameter)	IP address range or ranges allocated to HSS.	HSS Cx stack port	BCF VIP	BCF CSCFCX stack port	TCP or SCTP or both
I-CSCF to HSS (Diameter)	I-CSCF CSCFCX stack VIP	I-CSCF CSCFCX stack port	IP address range or ranges allocated to HSS.	Any	TCP or SCTP
S-CSCF to HSS (Diameter)	S-CSCF CSCFCX stack VIP	S-CSCF CSCFCX stack port	IP address range or ranges allocated to HSS.	Any	TCP or SCTP
BCF to HSS (Diameter)	BCF CSCFCX stack VIP	BCF CSCFCX stack port	IP address range or ranges allocated to HSS.	Any	TCP or SCTP
Dx					
SLF to I-CSCF (Diameter)	IP address range or ranges allocated to SLF.	SLF Dx stack port	I-CSCF CSCFDX stack VIP	I-CSCF CSCFDX stack port	TCP or SCTP
SLF to S-CSCF (Diameter)	IP address range or ranges allocated to SLF.	SLF Dx stack port	S-CSCF VIP	S-CSCF CSCFDX stack port	TCP or SCTP



Table 15 Cx and Dx Interfaces

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
I-CSCF to SLF (Diameter)	I-CSCF CSCFDX stack VIP	I-CSCF CSCFDX stack port	IP address range or ranges allocated to SLF.	Any	TCP or SCTP
S-CSCF to SLF (Diameter)	S-CSCF CSCFDX stack VIP	S-CSCF CSCFDX stack port	IP address range or ranges allocated to SLF.	Any	TCP or SCTP

5.7.2 Rf Interface

The flows that must be available on the Rf interface are shown in Table 16.

Table 16 Rf Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
Offline Charging System to S-CSCF (Diameter)	IP address range or ranges allocated to Offline Charging system.	Offline Charging System CSCFRF stack port	S-CSCF CSCFRF stack VIP	S-CSCF CSCFRF stack port	TCP or SCTP or both
Offline Charging System to E-CSCF (Diameter)	IP address range or ranges allocated to Offline Charging system.	Offline Charging System CSCFRF stack port	E-CSCF CSCFRF stack VIP	E-CSCF CSCFRF stack port	TCP or SCTP or both
S-CSCF to Offline Charging System (Diameter)	S-CSCF CSCFRF stack VIP	S-CSCF CSCFRF stack port	IP address range or ranges allocated to Offline Charging system.	Any	TCP or SCTP
E-CSCF to Offline Charging System (Diameter)	E-CSCF CSCFRF stack VIP	E-CSCF CSCFRF stack port	IP address range or ranges allocated to Offline Charging system.	Any	TCP or SCTP

5.7.3 Ro Interface

The flows that must be available on the Ro interface are shown in Table 17.



Table 17 Ro Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
Online Charging System to S-CSCF (Diameter)	IP address range or ranges allocated to Online Charging System.	Online Charging System CSCFRO stack port	S-CSCF CSCFRO stack VIP	S-CSCF CSCFRO stack port	TCP or SCTP or both
S-CSCF to Online Charging System (Diameter)	S-CSCF CSCFRO stack VIP	S-CSCF CSCFRO stack port	IP address range or ranges allocated to Online Charging System.	Any	TCP or SCTP

5.7.4 Sh and Dh Interface

The flows that must be available on the Sh and Dh interfaces are shown in Table 18.

Table 18 Sh/Dh Interfaces

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
HSS to E-CSCF (Diameter)	IP address range or ranges allocated to HSS.	HSS Sh/Dh port	E-CSCF VIP	E-CSCF CSCFCX stack port	TCP or SCTP or both
E-CSCF to HSS (Diameter)	E-CSCF CSCFCX stack VIP	E-CSCF CSCFCX stack port	IP address range or ranges allocated to HSS.	Any	TCP or SCTP

5.8 IP Flow through DUA-DB LDAP

The flows that must be available on the DUA-DB LDAP interface are shown in Table 19.

Table 19 DUA-DB LDAP Interface

Traffic Flow	Origin IP	Origin Port	Destination IP	Destination Port	Protocol
I-CSCF to DUA-DB (LDAP)	I-CSCF IP Address	I-CSCF LDAP port	IP address range or ranges allocated to DUA-DB.	LDAP Port number	TCP





6 Privacy

The CSCF handles personal subscriber data to be able to provide services in the network. The personal subscriber data is handled in a secure way and the product supports different measures to protect the privacy of the subscribers. The CSCF stores personal subscriber data that is read from the Home Subscriber Server (HSS) when a subscriber registers and uses the personal subscriber data received through signaling for IMS session handling. Charging data is collected and sent to an external system for billing. Personal subscriber data can be also stored in logs when specific events happen in the system. For a description of the personal subscriber data that is handled by the CSCF, see Section 6.4 Classification of Personal Subscriber Data on page 31.

6.1 Subscriber Notice

This product processes personal subscriber data. Depending on the local legislation where the product is deployed and operated, the use of this product can require providing notice of the privacy policy of the operator to subscribers.

Ericsson discloses personal subscriber data to customers, professional advisors, suppliers, or other third parties engaged to perform administrative or other business management services. This disclosure is always on a confidential basis or otherwise in accordance with law. Ericsson may also disclose personal subscriber data with the consent of the individual or if disclosure is required or authorized by law.

Ericsson takes reasonable steps in all circumstances to ensure that the personal subscriber data it holds is protected from misuse, from interference and loss, and from unauthorized access, modification, or disclosure. Ericsson holds personal subscriber data in both hard copy and electronic forms in secure databases on secure premises, accessible only by authorized personnel.

Ericsson destroys or deidentifies personal subscriber data in circumstances where it is no longer required, unless Ericsson is otherwise required or authorized by law to retain that data.

6.2 Consent

This product processes personal subscriber data. Depending on the local legislation where the product is deployed and operated, the subscriber must give consent upon buying this service to do the following:

- Collect and maintain personal subscriber data, aimed at holding securely this information.
- Fulfill the purpose of installing, upgrading, and administering the CSCF.



The system can be required to activate trace information. The purpose of these traces is only for troubleshooting. Depending on the trace level, it can contain personal subscriber data.

The collected data is only be accessed by Ericsson personnel or specific third parties that are in charge of these activities. The collected data is not distributed to third parties for other purposes.

When the personal subscriber data is no longer required, this data is disposed of.

6.3 Handling of Personal Subscriber Data

6.3.1 Personal Subscriber Data in Logs

6.3.1.1 Personal Subscriber Data in the CSCF Cache

Subscriber data is cached by the CSCF during call handling. The REGISTRATION message has a time limit for the cached data. After the time expires, the data is deleted.

The CSCF also removes the cached subscriber data when the user deregisters successfully.

6.3.1.2 Personal Subscriber Data in the CSCF Console Logs

The CSCF writes events that are used during troubleshooting to log files. These log files are reused and overwritten when the maximum file size limit and the maximum number of log files are reached.

The following are the CSCF console logs and their storage locations:

- Syslog: `/var/log/<system_controller>`
- CSM log: `/storage/no-backup/coremw/var/log/<system_controller>/clustermonitor`
- vDicos console logs: `/storage/no-backup/cdclsv/log/lpmsv/`
These log files can contain privacy data.
- Application logs: `/storage/no-backup/coremw/var/log/saflog/`
These log files can contain privacy data.
- Crash collector: `/storage/no-backup/cdclsv/dumps/`
These log files can contain privacy data.

The management policy of the CSCF console log files is described in [Handling Files](#).



6.3.1.3 Personal Subscriber Data in Other CSCF Logs

The data collections from ACDC and Health Check are generated by operator interaction only. These log files are not reused or overwritten.

Additional logs can be found in the following locations:

- Data Collection (ACDC): /storage/no-backup/vcscf_<CSCF_Product_Number>/acdc/

For example: /storage/no-backup/vcscf_CXP9034345/acdc/

- Health Check Reports: /storage/no-backup/vcscf_<CSCF_Product_Number>/healthcheck/

For example: /storage/no-backup/vcscf_CXP9034345/healthcheck/

For more details on how to collect data using the Aggregated CSR Data Collection (ACDC) script, see [Data Collection Guideline for CSCF](#).

6.3.2 CSCF Functions with Privacy Impact

The following CSCF functions collect personal subscriber data:

- Offline and Online Charging

The CSCF collects offline and online charging data for billing purposes. Normally, the CSCF directly transfers offline charging data. When a connectivity problem occurs, offline charging data is temporarily stored before it is forwarded to an external Charging Data Function. The CSCF does not analyze the collected charging data.

- Traceability and Troubleshooting

In the CSCF, the Network Tracing, and User Tracing functions collect personal subscriber data for troubleshooting purposes. When an incident occurs, that data is analyzed to resolve it.

- User Data Output

The CSCF functionality User Data Output collects and prints user data for troubleshooting purposes. For more information about User Data Output, see [CSCF User Data Output Guideline](#).

6.3.3 Personal Subscriber Data Collection and Removal

The following personal subscriber data types are collected by the CSCF:

- Semi-permanent data



This type of data is downloaded from the HSS when a subscriber registers and stored in the CSCF to enable processing of subscriber requests.

- Dynamic data

This data includes dynamic registration data and dynamic session data related to subscriber activities. Dynamic data is stored in the CSCF.

- Personal subscriber data in Event History

Event History collects and logs personal subscriber data for troubleshooting.

- Personal subscriber data in Network Tracing

Network Tracing collects and logs personal subscriber data for troubleshooting.

- Personal subscriber data during a system crash

During a crash of the system, the core dump can include personal subscriber data. Activation of the CSCF Health Check can start the collection of the core dump.

The CSCF removes semi-permanent and dynamic data when the user deregisters successfully.

Removing stored personal subscriber data can be done in the following ways, depending on the type of log or file:

- The data is overwritten at regular intervals.
- Automatic file removal is configured, see Section 6.3.4.5 File Removal on page 30.
- The operator removes the files manually, see Section 6.3.4.5 File Removal on page 30.

6.3.4 Overview of Personal Subscriber Data Handling Configuration

6.3.4.1 Role-Based Access

Role-Based Access Control can be used to limit and control the access to personal subscriber data. For more information about Role-Based Access Control, see [User Management](#).

The default Role-Based access per File Management directory is described in Table 20.



Table 20 Default Access per File Management Directory and Role

File Management Directory	Roles							
	CSCFApplicationAdministrator	CSCFApplicationOperator	CSCFApplicationSecurityAdministrator	Local Authentication Administrator	Self	System Administrator	System Read-Only	System Security Administrator
AlarmLogs	RWX	R	R	Deny	Deny	RWX	Deny	R
AlertLogs	RWX	R	R	Deny	Deny	RWX	Deny	R
BackupAndRestoreManagementFiles	RWX	R	Deny	Deny	Deny	Deny	Deny	Deny
Cscf	RWX	R	Deny	Deny	Deny	Deny	Deny	Deny
InServicePerformance	Deny	Deny	Deny	Deny	Deny	R	Deny	Deny
PerformanceManagementReportFiles	RWX	R	Deny	Deny	Deny	RWX	Deny	Deny
SoftwareManagement	RWX	R	R	Deny	Deny	RWX	Deny	Deny

6.3.4.2 Privacy Event Logging

All privacy events, such as access to or modification of personal subscriber data, are logged in the audit trail log. For more information about the audit trail log, see [Audit Information](#).

The syslog can be read from `/var/log/messages`. This is a symbolic link to the messages directory on the System Controller. For example: `/var/log/SC-2-1/messages`.

Note: Automatic encrypted streaming of log files to a secure external server can be enabled and disabled by NBI users. For more information, see [Configure Automatic Log Streaming](#).

6.3.4.3 Data Level Minimization

The level of logged data can be reduced by setting the NetTrace trace level to minimum. For more information about setting the trace levels in NetTrace, see [CSCF Network Tracing](#).

The following levels of Nettrace output types exist:

- Machine-readable at Min Level
- Machine-readable at Max Level
- Human-readable at Min Level
- Human-readable at Max Level



Specific SIP methods can be also logged. The default setting is that all SIP methods are applied.

6.3.4.4 File Access Limitation

Access to log files that contain sensitive data can be limited through Security Management rules. See [Handling Files](#) for more information.

The default configuration is described in Table 21.

Table 21 Default Policies for File Access Limitation

File Management Directory	Default Policy
AlarmLogs	The maximum number of log files is 11. The maximum size of each alarm log file is restricted to 500 KB.
AlertLogs	The maximum number of log files is 11. The maximum size of each alert log file is restricted to 500 KB.
BackupAndRestore ManagementFiles	No default preventive maintenance policy.
Cscf	No default preventive maintenance policy.
InServicePerformance	InServicePerformance XML [®] report files are kept for 6 months. As a preventive maintenance policy, the system automatically cleans the old InServicePerformance reports. This activity happens once per month at the time of creation of a new InServicePerformance XML report.
Performance Management ReportFiles	The maximum number of Performance Management report files is 1000.
SoftwareManagement	No default preventive maintenance policy.

6.3.4.5 File Removal

It is important to clean up files that are no longer needed. It is possible to clean up files automatic and manual.

To remove files automatically, follow the instructions in [Configure Preventive Maintenance Policy Deleting Files in Logical File System](#).

To remove a file manually, follow the instructions in [Delete File in Logical File System](#).

There is no default configuration for file removal.



6.4 Classification of Personal Subscriber Data

Table 22 lists the personal subscriber data handled by the CSCF.

Table 22 Personal Subscriber Data Handled by the CSCF

Personal Subscriber Data Category	Data Item	Comments
Basic data	IP address	
	MSISDN	
	IMSI	
	IMEI code	
	Mobile Number	MSISDN
	Mobile Device Serial Number	IMEI
	First name	Display Name
	Last name	Display Name
	User ID	
	SIP address	
	Logon details	Authentication Information
Other Basic Data	Access-type	
	Authentication information (digest, AKA)	
	Public ID (IMPU)	
	Private ID (IMPI)	
	NoOfContacts/Contact	
	Registered status	



Personal Subscriber Data Category	Data Item	Comments
Sensitive Data	Call history	
	Event Monitoring: event-based monitoring, call trace recordings, general performance event handling, and so on.	
	Metadata showing user activity	
	Content of communication: text	Short Message
	Location: LAC / CellID	
	Location History	
	Barred calling subscribers (Blacklist)	