

# Session Context Exposure User Guide

Ericsson Service-Aware Policy Controller

User Guide

## **Copyright**

© Ericsson AB 2018. 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

<b>1</b>	<b>Session Context Exposure Introduction</b>	<b>1</b>
<b>2</b>	<b>Session Context Exposure Function</b>	<b>2</b>
2.1	Session Context Exposure Overview	2
2.2	Session Context Collection	5
2.2.1	Session Context in External Database	7
2.3	Update Session Context Triggered by External System	9
2.4	Automatic Removal of Closed Session Context	9
2.5	Retrieval of IMSI with IP Address Mechanism	10
<b>3</b>	<b>Session Context Exposure Operation and Maintenance</b>	<b>12</b>
3.1	Session Context Exposure Configuration	12
3.1.1	Enable or Disable Session Context Exposure	12
3.1.2	Configure Automatic Removal of Closed Session Context	13
3.2	Retrieval of IMSI with IP Address	15
3.3	Session Context Retrieval	15
3.3.1	Retrieval of Session Context from External Database	16
3.3.2	Retrieval of Session Context from SAPC Internal Database	16
3.4	Session Context Exposure Fault Management	16
3.4.1	Session Context Exposure Alarms	16
3.4.2	Session Context Exposure Notifications	16
3.4.3	Session Context Exposure Error Handling	16
3.5	Session Context Exposure Logging	17
<b>4</b>	<b>Restrictions</b>	<b>18</b>
<b>5</b>	<b>Reference List</b>	<b>19</b>





# 1 Session Context Exposure Introduction

This document is intended to be used as guide to configure the Session Context Exposure function in the SAPC and consult the session context from external or internal database.



## 2 Session Context Exposure Function

### 2.1 Session Context Exposure Overview

The Session Context Exposure enables the user to store ongoing and closed IP-CAN sessions into the external or internal database and access them by REST API for consulting. If desired, this function removes the obsolete closed session context automatically according to the configuration.

[Table 1](#) shows elements of the session context stored and published in the external or internal database.

Table 1 Elements in session context

Session Context Elements		Type	Possible Values	(O) Optional / (M) Mandatory	Comments
trafficId (1) (2)	idType	String	IMSI or MSISDN	M	The subscriber identifier received by the SAPC in the traffic query.
	idValue	String	Any		
apn <sup>(2)</sup>		String	Any	M	Access point name.
ipv4Addr		String	Any	O	UE's IPv4 address.
ipv6Prefix		String	Any	O	UE's IPv6 prefix.
startTime		String	Format: dd-mm-yyyyThh:m m:ss	O	Start date and time when the IP-CAN session is established.
updateTime <sup>(3)</sup>		String	Format: dd-mm-yyyyThh:m m:ss	O	Session update time.



mnc		String	Any	0	It is obtained from 3GPP_SGSN-MCC-MNC AVP.
mcc		String	Any	0	It is obtained from 3GPP_SGSN-MCC-MNC AVP.
ratType		String	RAT-Type values	0	-
pccRules	pccRuleIds <sup>(4)</sup>	Array	Any	0	Identify all authorized PCC rules in the IP-CAN session.
	time	String	Format: dd-mm-yyyyThh:mm:ss	0	Last update date and time when a PCC rule list is modified.
qos	qci	Integer	1 - 254	0	Authorized QoS Class Identifier for the default bearer.
	apnAmbrDL	Integer	Any	0	Authorized maximum aggregate bit rate (in Kbits per second) for the downlink.
	apnAmbrUL	Integer	Any	0	Authorized maximum aggregate bit rate (in Kbits per second) for the uplink.



bearerId	String	Any	O	The identifier for the IP-CAN bearer. It is in hexadecimal format with 0x as the prefix.
mbrDl	Integer	Any	O	Authorized maximum bit rate (in Kbits per second) for the downlink of the default bearer.
mbrUl	Integer	Any	O	Authorized maximum bit rate (in Kbits per second) for the uplink of the default bearer.
arpPrio	Integer	1 - 15	O	Priority for Allocation Retention Priority (ARP).
arpPvi	Boolean	true false	O	Pre-emption vulnerability indication for ARP:  —true: DISABLED  —false: ENABLED
arpPci	Boolean	true false	O	Pre-emption capability





					indication for ARP:  —true: DISABLE D  —false: ENABLE D
pra	praId	Integer	0 - 16777215	0	Name of Presence Reporting Area (PRA).
	praStatus	String	PRA Status used:  —Unknown  —In  —Out	0	Indicates whether the UE is inside or outside of the PRA. Before the report from the PCEF is received, the status is Unknown.

- (1) If Subscription-Id AVP includes IMSI, IMSI is used as the trafficId. Only when Subscription-Id AVP includes MSISDN but does not include IMSI, MSISDN is used as the trafficId. Value NAI is not supported.
- (2) The SAPC uses the combination of apn and trafficId as the key of the session context.
- (3) It is updated if any session context element or accumulated usage is changed when an IP-CAN session is modified or terminated. When a GET operation for subscriber state from external system is received, the updateTime of ongoing sessions without fair usage is also updated.
- (4) For a static or preconfigured PCC rule, the charging rule name or base name is included. For a dynamic PCC rule, the service name is included.

**Note:** The SAPC supports to expose session context and accumulated usage together in the external or internal database.

## 2.2 Session Context Collection

Next figure shows an overview of the session context collection mechanism.

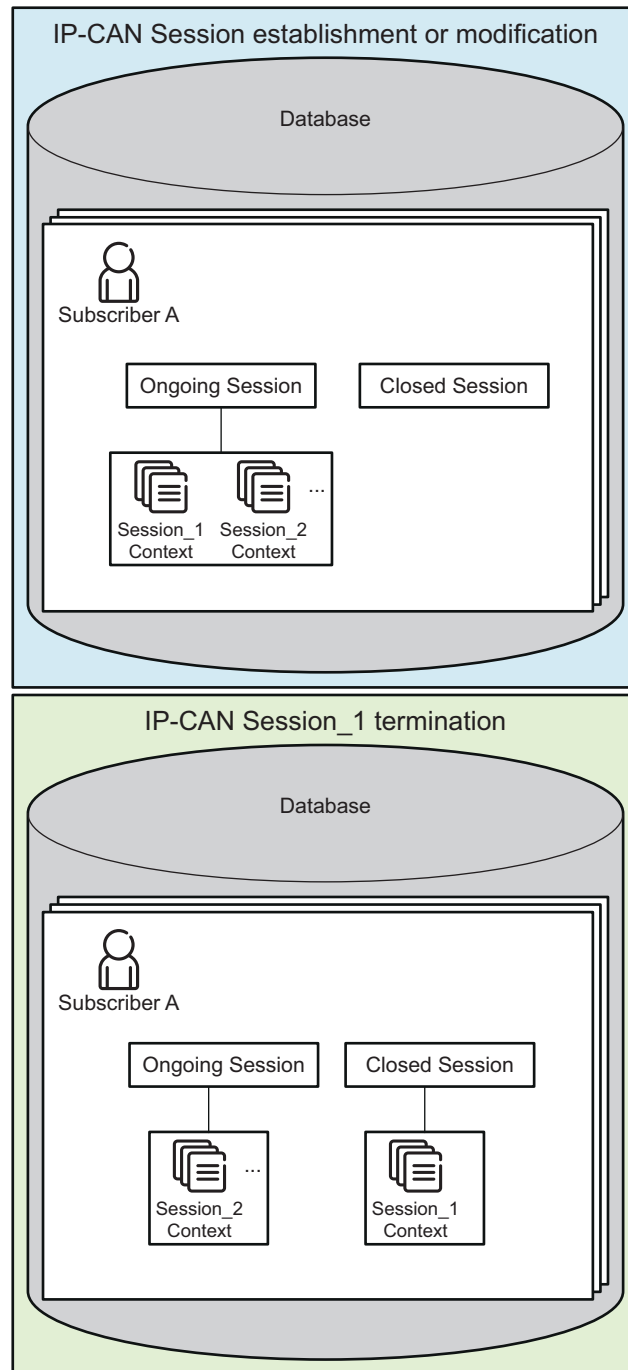


Figure 1 Session context collection

The session context is collected and overwritten per combination of APN and trafficId. At the IP-CAN session establishment, the session context is created and stored to the SAPC external or internal database. At IP-CAN session modification or reauthorization, the session context is updated based on the latest authorized data. At the IP-CAN session termination, the session context is also updated and stored persistently.



## 2.2.1 Session Context in External Database

The SAPC can read and write the session context in the external database by LDAP operations:

- At the IP-CAN session establishment, the SAPC writes the session context into the `OngoingSession` attribute of the external database by LDAP modify.
- At the IP-CAN session modification or reauthorization, the SAPC reads the session context by LDAP search and updates the ongoing session context including session update time into the external database by LDAP modify whenever authorized data or accumulated usage is changed.
- At the IP-CAN session termination, the SAPC updates the session update time and moves the session context from the `OngoingSession` attribute to the `ClosedSession` attribute in the external database by LDAP modify.

For more information about interworking with external database, see [Integration in User Data Consolidation](#).

[Figure 2](#) shows how the SAPC saves and updates session context in the external database at IP-CAN session establishment, modification and termination.

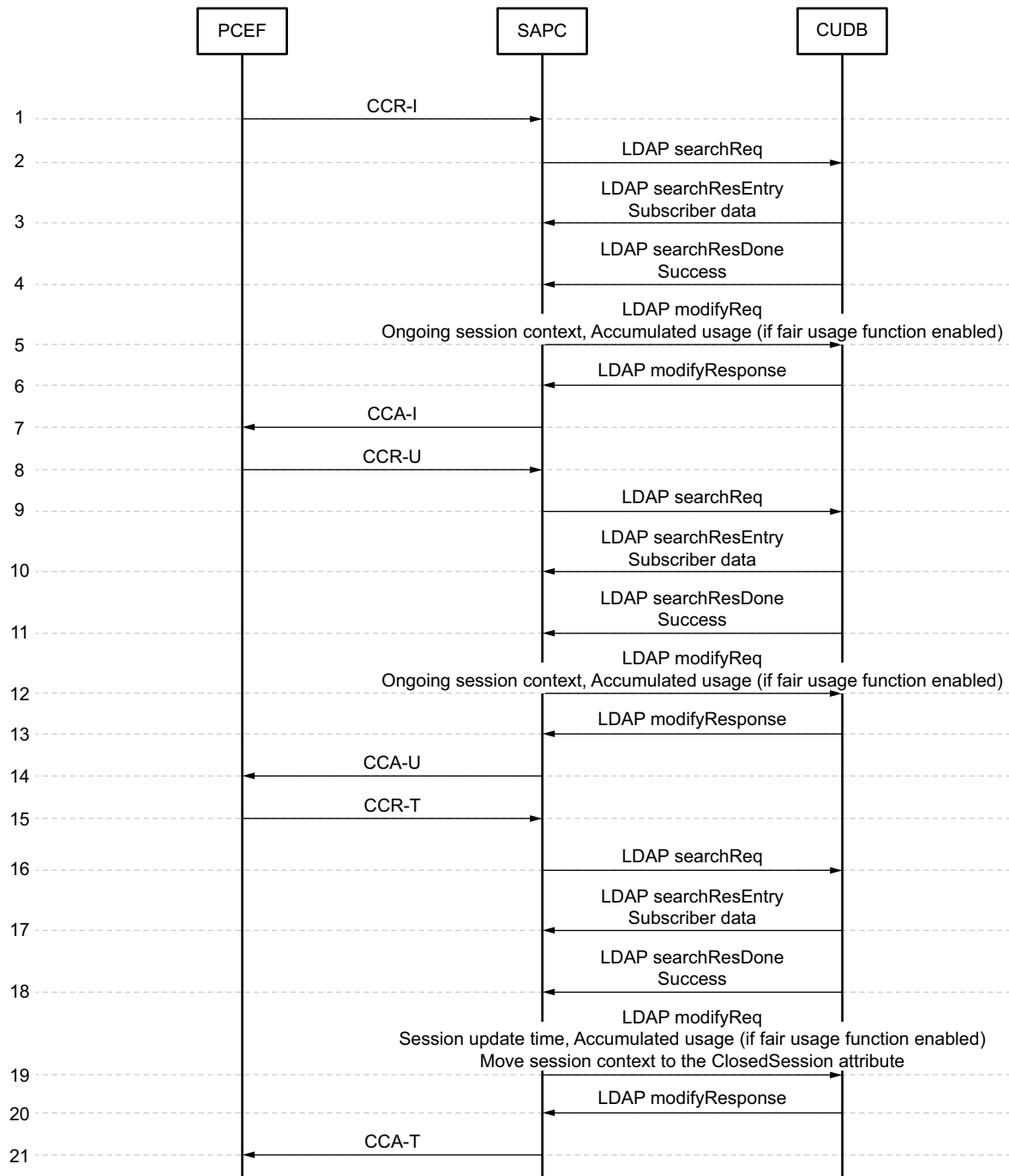


Figure 2 Session context storage and update in the external database



## 2.3 Update Session Context Triggered by External System

It is possible for the external system to trigger the usage reporting in ongoing IP-CAN sessions and update session update time together by a GET operation for requesting subscriber state. For details, see [Session Context Retrieval](#) on page 15.

When receiving a GET operation for subscriber state, the SAPC checks if any ongoing IP-CAN session exists for the subscriber:

- If any ongoing IP-CAN session is found, the SAPC sends GET response to the external system with online state.
  - For the ongoing IP-CAN session with usage information, the SAPC sends a forced RAR to the PCEF for the usage reporting. After the usage reporting is received, the SAPC updates the accumulated usage and the session update time.
  - For the ongoing IP-CAN session without usage information, the SAPC only updates the session update time.
- If no ongoing IP-CAN session is found, the SAPC sends GET response to the external system with offline state.

## 2.4 Automatic Removal of Closed Session Context

This clean-up functionality protects SAPC external and internal databases from storing obsolete closed session contexts (such as when an IMSI is deprecated). This functionality is disabled by default and can be enabled by configuration. For configuration details, see [Configure Automatic Removal of Closed Session Context](#) on page 13.

**Note:** When this functionality is disabled, closed session contexts are stored persistently but updated when the user terminates a new IP-CAN session established with same combination of APN and trafficId.

Next figure shows the mechanism for the automatic removal of closed session context.

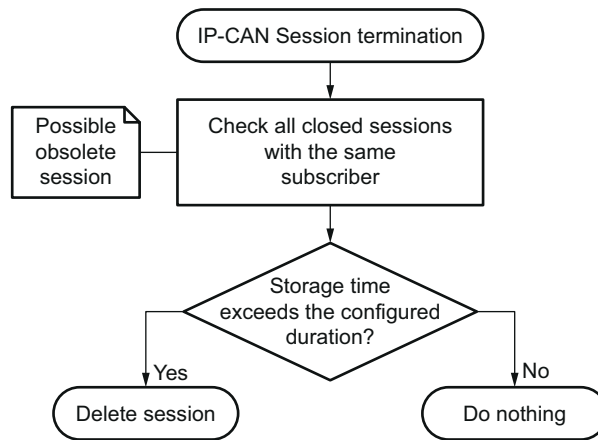


Figure 3 Automatic removal of closed session context

When receiving an IP-CAN session termination request from the PCEF, the SAPC checks the storage time (the difference between current time and session update time) of all closed sessions belonging to the same subscriber and moves the session context into closed session attribute simultaneously. If the storage time exceeds the configuration duration, the SAPC removes these obsolete closed session contexts from external or internal database.

## 2.5 Retrieval of IMSI with IP Address Mechanism

Some IT systems need to find out IMSI from a known IP address in order to access the session information, so the SAPC supports to query IMSI by IP address in case IMSI is unknown. This functionality can be operated based on a primary key (single input argument) or a composed key (multiple input arguments), see [page 10](#).

Table 2 IMSI retrieval related input arguments

Query arguments	Type	(O) Optional / (M) Mandatory	Comments
ipaddr	String	M	IPv4 and IPv6 prefix addresses are supported.
apn	String	O	See <a href="#">Table 1</a> .
pcef	String	O	The PCEF identifier.

The SAPC returns a list of IMSI values from IP-CAN sessions matching the input arguments. An empty list is returned in case of none IP-CAN session for the input arguments.



**Note:** If there is no IMSI for the corresponding IP-CAN session (such as no IMSI received from the PCEF at IP-CAN session establishment or this IP-CAN session is terminated), the SAPC also returns an empty list.



## 3 Session Context Exposure Operation and Maintenance

### 3.1 Session Context Exposure Configuration

#### 3.1.1 Enable or Disable Session Context Exposure

The Session Context Exposure is disabled by default in the SAPC, and can be enabled by setting `enableSessionInfoPublication` attribute to true in `SessionInfoPublicationConfig` object class.

Example 1 Enable session context exposure

```
<edit-config>
  <target>
    <running />
  </target>
  <config>
    <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop">
      <managedElementId>1</managedElementId>
      <dnPrefix>dc=ManagedElement</dnPrefix>
      <networkManagedElementId>1</networkManagedElementId>
      <userLabel>Managed Element</userLabel>
      <PolicyControlFunction xmlns="urn:com:ericsson:ecim:sapcmom">
        <policyControlFunctionId>1</policyControlFunctionId>
        <AppConfig xmlns="urn:com:ericsson:ecim:appconfigmom">
          <appConfigId>1</appConfigId>
          <SessionInfoPublicationConfig xmlns="urn:com:ericsson:ecim:sessioninfopublicationconfigmom">
            <sessionInfoPublicationConfigId>1</sessionInfoPublicationConfigId>
            <enableSessionInfoPublication>true</enableSessionInfoPublication>
          </SessionInfoPublicationConfig>
        </AppConfig>
      </PolicyControlFunction>
    </ManagedElement>
  </config>
</edit-config>
```

To disable Session Context Exposure if it has been previously enabled, set `enableSessionInfoPublication` attribute to false in `SessionInfoPublicationConfig` object class.





## Example 2 Disable session context exposure

```
<edit-config>
  <target>
    <running />
  </target>
  <config>
    <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop">
      <managedElementId>1</managedElementId>
      <dnPrefix>dc=ManagedElement</dnPrefix>
      <networkManagedElementId>1</networkManagedElementId>
      <userLabel>Managed Element</userLabel>
      <PolicyControlFunction xmlns="urn:com:ericsson:ecim:sapcmom">
        <policyControlFunctionId>1</policyControlFunctionId>
        <AppConfig xmlns="urn:com:ericsson:ecim:appconfigmom">
          <appConfigId>1</appConfigId>
          <SessionInfoPublicationConfig xmlns="urn:com:ericsson:ecim:sessioninfopublicationconfigmom">
            <sessionInfoPublicationConfigId>1</sessionInfoPublicationConfigId>
            <enableSessionInfoPublication>false</enableSessionInfoPublication>
          </SessionInfoPublicationConfig>
        </AppConfig>
      </PolicyControlFunction>
    </ManagedElement>
  </config>
</edit-config>
```

For details about the object and attributes, refer to [Managed Object Model \(MOM\)](#).

### 3.1.2 Configure Automatic Removal of Closed Session Context

To remove closed session context automatically, configure the `durationSessionInfoPublication` in `SessionInfoPublicationConfig` object class.

Depending on your needs, execute one of the actions described in [Table 3](#).

Table 3 Automatic removal options

Action	Command
Remove the obsolete closed session stored more than one week	Set <code>durationSessionInfoPublication</code> attribute to 1.
Remove the obsolete closed session stored more than one month	Set <code>durationSessionInfoPublication</code> attribute to 2.



Remove the obsolete closed session stored more than three months	Set durationSessionInfoPublication attribute to 3.
Remove the obsolete closed session stored more than one year	Set durationSessionInfoPublication attribute to 4.

**Note:** The default value of durationSessionInfoPublication attribute is 0. If this attribute is not configured or set as the default value, the removal of closed session context does not execute automatically.

Next an example to configure the removal of the obsolete closed session stored more than one week.

#### Example 3 Remove the obsolete closed session stored more than one week

```
<edit-config>
  <target>
    <running />
  </target>
  <config>
    <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop">
      <managedElementId>1</managedElementId>
      <dnPrefix>dc=ManagedElement</dnPrefix>
      <networkManagedElementId>1</networkManagedElementId>
      <userLabel>Managed Element</userLabel>
      <PolicyControlFunction xmlns="urn:com:ericsson:ecim:sapcmom">
        <policyControlFunctionId>1</policyControlFunctionId>
        <AppConfig xmlns="urn:com:ericsson:ecim:appconfigmom">
          <appConfigId>1</appConfigId>
          <SessionInfoPublicationConfig xmlns="urn:com:ericsson:ecim:sessioninfopublicationconfigmom">
            <sessionInfoPublicationConfigId>1</sessionInfoPublicationConfigId>
            <enableSessionInfoPublication>true</enableSessionInfoPublication>
            <durationSessionInfoPublication>1</durationSessionInfoPublication>
          </SessionInfoPublicationConfig>
        </AppConfig>
      </PolicyControlFunction>
    </ManagedElement>
  </config>
</edit-config>
```



## 3.2 Retrieval of IMSI with IP Address

**Note:** The operation GET-IMSI-List is disabled by default and can be enabled by setting enableSessionInfoPublication attribute to true, see [Enable or Disable Session Context Exposure](#) on page 12.

To obtain an IMSI list from IP-CAN sessions, use the operation GET-IMSI-List in the analytics REST API. For more information, see [Analytics REST API](#).

Depending on the inputs, execute one of commands described in [page 15](#).

Table 4 Retrieval of IMSI with IP address

Command	Description
<code>/sessions/{ipaddr}/imsi-list</code>	The SAPC retrieves IMSI identified by IP address, the returned IMSI list may include zero, one or multiple values.
<code>/sessions/{ipaddr}/imsi-list?apn=&lt;APN&gt;&amp;pcef=</code>	The SAPC retrieves IMSI identified by IP address and APN, the returned IMSI list may include zero, one or multiple values.
<code>/sessions/{ipaddr}/imsi-list?apn=&amp;pcef=&lt;PCEF&gt;</code>	The SAPC retrieves IMSI identified by IP address and PCEF, the returned IMSI list may include zero, one or multiple values.
<code>/sessions/{ipaddr}/imsi-list?apn=&lt;APN&gt;&amp;pcef=&lt;PCEF&gt;</code>	The SAPC retrieves IMSI identified by IP address, APN and PCEF, the returned IMSI list may include zero or one value.

Example 4 Retrieval of IMSI with IPv6 prefix address, APN and PCEF

```
request := {
  client_id := omit,
  method := "GET",
  uri := "/analytics/v1/sessions/467C:94FA:9125:F696/imsi-list?apn=APN1&PCEF=ggsnNodeHostname.nodeHostRealm.com",
  version_major := 1,
  version_minor := 1,
}
```

## 3.3 Session Context Retrieval

The session context can be obtained by external systems at any time. It is possible to query the session context and accumulated usage together.

To ensure the accumulated usage is up to date before retrieving, use the GET operation for `/subscribers/{subscriberId}/subscriber-state` URI in the analytics REST API.



The external system receives GET subscriber state response from the SAPC:

- If the subscriber state is online, the external system waits some time for the SAPC updating the accumulated usage and the session update time. The detailed waiting time is measured according on the real network status (the suggested value is 3 seconds). And then it retrieves the session context and the accumulated usage from external or internal database of the SAPC.
- If the subscriber state is offline, the external system retrieves the session context and the accumulated usage from external or internal database of the SAPC immediately.

### 3.3.1 Retrieval of Session Context from External Database

When the session context of a known subscriber is stored in the external database, it is possible to obtain session context with the ldapsearch request. For more information, see [Integration in User Data Consolidation](#).

### 3.3.2 Retrieval of Session Context from SAPC Internal Database

To retrieve session context of a known subscriber from the internal database, use the GET operation for `/subscribers/{subscriberId}/subscriber-info` URI in the analytics REST API.

When the SAPC receives this GET operation, it responds with the session context (ongoing and closed sessions) and accumulated usage (if available) to the external system.

## 3.4 Session Context Exposure Fault Management

### 3.4.1 Session Context Exposure Alarms

Not alarms are raised.

### 3.4.2 Session Context Exposure Notifications

No notifications are sent.

### 3.4.3 Session Context Exposure Error Handling

Table 5 Session context exposure error handling

Error Condition	Action	Code
-----------------	--------	------



The SAPC receives an REST GET message and cannot query state or session context of a known subscriber.	The SAPC returns a response indicating an error.	Result-Code set to 400 Bad Request
The SAPC receives an REST GET-IMSI-List message with invalid URI.	The SAPC returns a response indicating an error.	Result-Code set to 400 Bad Request
The SAPC receives an REST GET-IMSI-List message with wrong IP format.	The SAPC returns a response indicating an error.	Result-Code set to 400 Bad Request
The SAPC receives an REST GET message and cannot detect the specific subscriber.	The SAPC returns a response indicating an error.	Result-Code set to 404 Not Found
The SAPC receives an REST PUT or DELETE message.	The SAPC returns a response indicating an error.	Result-Code set to 405 Method Not Allowed
The SAPC receives an REST GET-IMSI-List message but this functionality is not activated.	The SAPC returns a response indicating an error.	Result-Code set to 405 Method Not Allowed
The SAPC encounters an unexpected condition which prevented to fulfill the request.	The SAPC returns a response indicating an error.	Result-Code set to 500 Internal Server Error

## 3.5 Session Context Exposure Logging

See Database Access.



## 4 Restrictions

The following restrictions apply to the Session Context Exposure:

- In multiple IP-CAN sessions scenario, if the different sessions have the same combination of APN and trafficId, the SAPC only supports to store the last updated IP-CAN session and expose its session context.
- In multiple Gx scenario, if several Gx sessions belonging to the same IP-CAN session have the same combination of APN and trafficId, the SAPC only supports to store the last updated Gx session and expose its session context.
- The SAPC does not support session context exposure for non-authorized PCC rules.



## 5 Reference List

### **Ericsson Documents**

1. Analytics REST API
2. Integration in User Data Consolidation
3. Managed Object Model (MOM)
4. Database Access

### **Standards**

1. Lightweight Directory Access Protocol RFC 4511