

Policy Control for Wi-Fi Calling

Ericsson Service-Aware Policy Controller

FACILITY DESCRIPTION

Copyright

© Ericsson España, S.A. 2016. 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.

Abstract

This document describes the policy control provided by the SAPC for the Ericsson SIM-based Untrusted Wi-Fi Calling Solution.



Contents

1	Introduction	1
1.1	Document Purpose and Scope	1
1.2	Revision Information	1
1.3	Concepts	1
2	Function	2
2.1	Overview	2
2.2	Wi-Fi Calling	3
2.2.1	Use Case: Bill Shock Prevention	5
3	Network Deployments	5
4	Traffic Cases	5
4.1	Wi-Fi Calling Setup	5
4.2	Handover between VoLTE and Wi-Fi	8
4.2.1	Handover from Wi-Fi to VoLTE	8
4.2.2	Handover from VoLTE to Wi-Fi	10
4.3	Error Handling	12
5	Operational Conditions	12
5.1	External Conditions	12
	Glossary	13
	Reference List	15





1 Introduction

1.1 Document Purpose and Scope

This document describes the policy control provided by the SAPC for the Ericsson SIM-based Untrusted Wi-Fi Calling Solution.

1.2 Revision Information

Rev. A This is the first release of this document.

1.3 Concepts

Access Point (AP)

A device that allows Wi-Fi capable devices to connect to a wired network using Wi-Fi technology.

Gating

A process of blocking or allowing packets belonging to a service data flow, to pass to the desired endpoint.

Seamless Handover

A method that ensures mobility of the user equipment in the network without affecting a call session, previously established. To secure continuity of the call connection during the handover, the “make before break” principle is applied. According to that principle, the UE attaches to new radio access point establishing a new connection. Once the traffic starts being conveyed through the new connection, the old one is released.

Untrusted Wi-Fi

A Wi-Fi access network that is not managed by the operator or does not provide sufficient security mechanisms. For example, a public open hotspot, a private Wi-Fi AP at home or any other Wi-Fi AP that does not fulfill security mechanism such as authentication and encryption.



2 Function

2.1 Overview

Ericsson SIM-based Untrusted Wi-Fi Calling Solution allows subscribers to make Wi-Fi calls using their SIM-based devices, when the subscribers attach to either a public or residential Wi-Fi access network.

This solution supports the following two functions:

- Wi-Fi calling for SIM-based devices

This function enables SIM-based devices entering the packet core network through an untrusted Wi-Fi network to use IMS voice services. The Wi-Fi calling feature is natively integrated in the device, which avoids the drawbacks of existing over-the-top applications and provides the subscribers with a carrier-grade performing service. The subscribers only need to turn on the Wi-Fi calling feature rather than any other specific settings.

- Seamless handover between VoLTE and Wi-Fi

This function enables voice session continuity without interruption for a UE attached to LTE moving to Wi-Fi and the other way around. The PCEF acts as anchor point for the session providing key support for seamless mobility. When the UE decides to handover, authentication and authorization are triggered for IMS APN on the destination access. Once connectivity is established over the destination access, session and bearers over the source access are released. Finally, the SIP Registration procedure for the new access is triggered.

The solution has the following advantages:

- Wi-Fi calling at public or residential areas achieves better data coverage.
- Wi-Fi calling uses the same phone number that the phone uses for cellular calls.
- Wi-Fi calling can be seamlessly handed off to the cellular network when the UE leaves Wi-Fi range, and the other way around.
- Wi-Fi calling can be made to any cell phone or landline phone, regardless of which network the other end is using.
- Wi-Fi calling capability works overseas to avoid cellular roaming charges.
- Voice quality of Wi-Fi calling is the same as on standard cellular calls.

Figure 1 shows the Ericsson Network Integrated Wi-Fi (ENIW) architecture that enables the seamless integration of untrusted Wi-Fi access networks in 3GPP



networks. This architecture allows subscribers to securely access the packet core network through an untrusted Wi-Fi network.

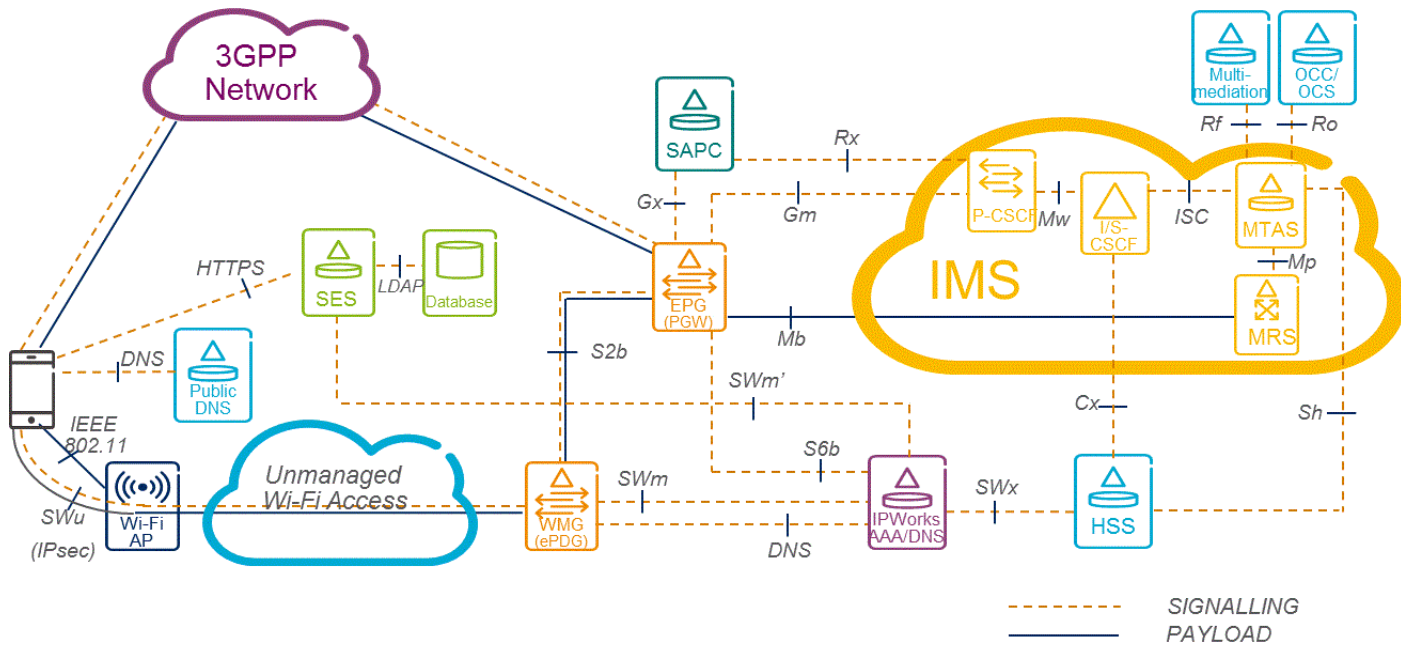


Figure 1 ENIW Architecture

The Wi-Fi calling can be made or received only when the untrusted Wi-Fi access network, the IMS network, and S2b capable EPG are deployed.

2.2 Wi-Fi Calling

Figure 2 shows a high-level flow for the establishment of the Wi-Fi calling.

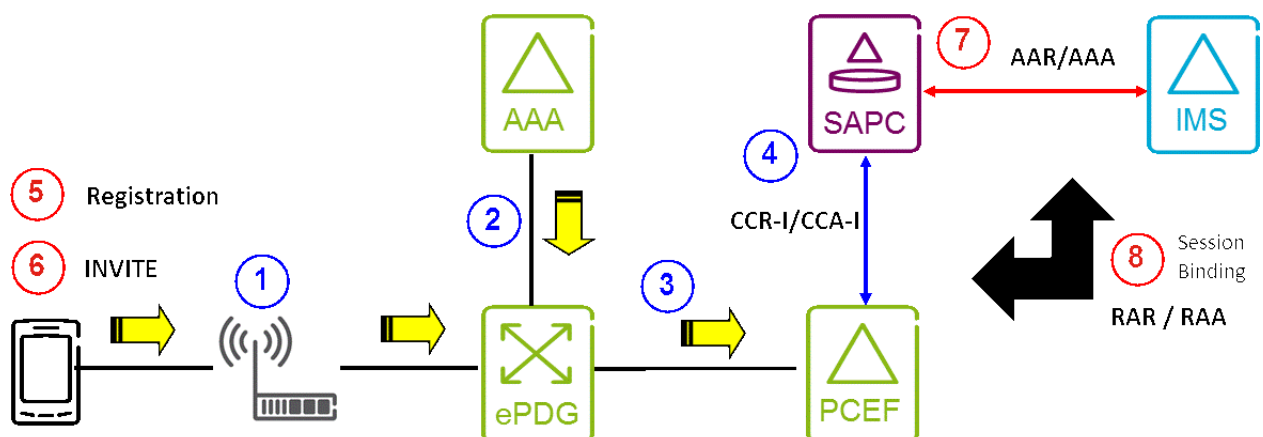


Figure 2 Overview of Wi-Fi Calling



- 1. When the UE wants to establish the Wi-Fi calling, the UE attaches to the Wi-Fi access and requests the IPsec tunnel by sending the IKE messages.
- 2. The IPWorks AAA server then authenticates the UE using the EAP-AKA method.
- 3. The ePDG triggers the establishment of the S2b GTP tunnel to the PCEF.
- 4. The PCEF allocates an UE IP address and initiates the Gx session establishment. Upon reception of the IMS APN, IP-CAN type “Non-3GPP-EPS” and RAT type “WLAN”, the SAPC identifies that the IP-CAN session is for the Wi-Fi calling service. The SAPC then installs PCC rules to the PCEF with the authorized QoS that applies to the default EPS bearer for the Wi-Fi calling service.
- 5. Once the IPsec tunnel and the S2b GTP tunnel are established, the UE initiates the SIP Registration procedure to the IMS network.
- 6. Once the SIP Registration procedure is completed, the UE initiates the Wi-Fi calling by sending the INVITE request to the IMS network and subsequent application layer signaling.
- 7. The P-CSCF establishes an Rx session to the SAPC indicating in an AAR message that the new AF session relates to Wi-Fi service and requesting authorization and reservation of resources for the Wi-Fi service.
- 8. The SAPC performs session binding and ensures that the AF session relates to the Wi-Fi calling service. The SAPC then performs dynamic service classification, authorization, and qualification, and provides the PCC rules with the authorized QoS and charging for the Wi-Fi calling service.

The SAPC allows the operator to use the application identifier and media information received from the P-CSCF in the dynamic service classification. Example of typical service classification patterns for Wi-Fi calling is as follows:

Table 1 Example of Dynamic Service Classification Patterns for Wi-Fi Calling

AF Application Identifier	Media Type	Service-Id
urn:urn-7:3gpp-service.ims.icsi.mmtel	audio	Wi-Fi calling

At IP-CAN session reauthorization and events received from AF, the SAPC performs dynamic service authorization, service QoS control, service charging control, and service qualification for the Wi-Fi calling service. After that the SAPC downloads PCC rules with the authorized QoS data and charging data.

In addition, the SAPC supports the following uses cases for Wi-Fi calling:

- Bill shock prevention, as described in Section 2.2.1 on page 4.



2.2.1 Use Case: Bill Shock Prevention

Bill shock is the negative experience that subscribers have if they are faced with unexpected high charges. Bill shock can happen when the subscribers use a mobile device while roaming without understanding the voice or data roaming charges involved.

To prevent bill shock, the SAPC can reject the service authorization for the Wi-Fi calling according to policies when the SAPC detects the handover from Wi-Fi to VoLTE and the subscriber is roaming. The SAPC, for this purpose, must subscribe to the IP-CAN change event trigger.

3 Network Deployments

The SAPC can provide policy control for the Wi-Fi calling in the following network deployments:

- In the bearer plane (PCEF) side:
 - Ericsson EPG, through Ericsson Gx+ Rel9 onwards.
 - Non-Ericsson PCEF, through standard Gx Rel9 onwards.
- In the application plane (AF) side:
 - Ericsson SBG, through Rx Rel9 onwards.
 - Non-Ericsson P-CSCF, through Rx Rel9 onwards.

4 Traffic Cases

4.1 Wi-Fi Calling Setup

The following traffic case occurs when the UE is setting up the Wi-Fi calling. Before this traffic case, the UE has registered in the IMS network.

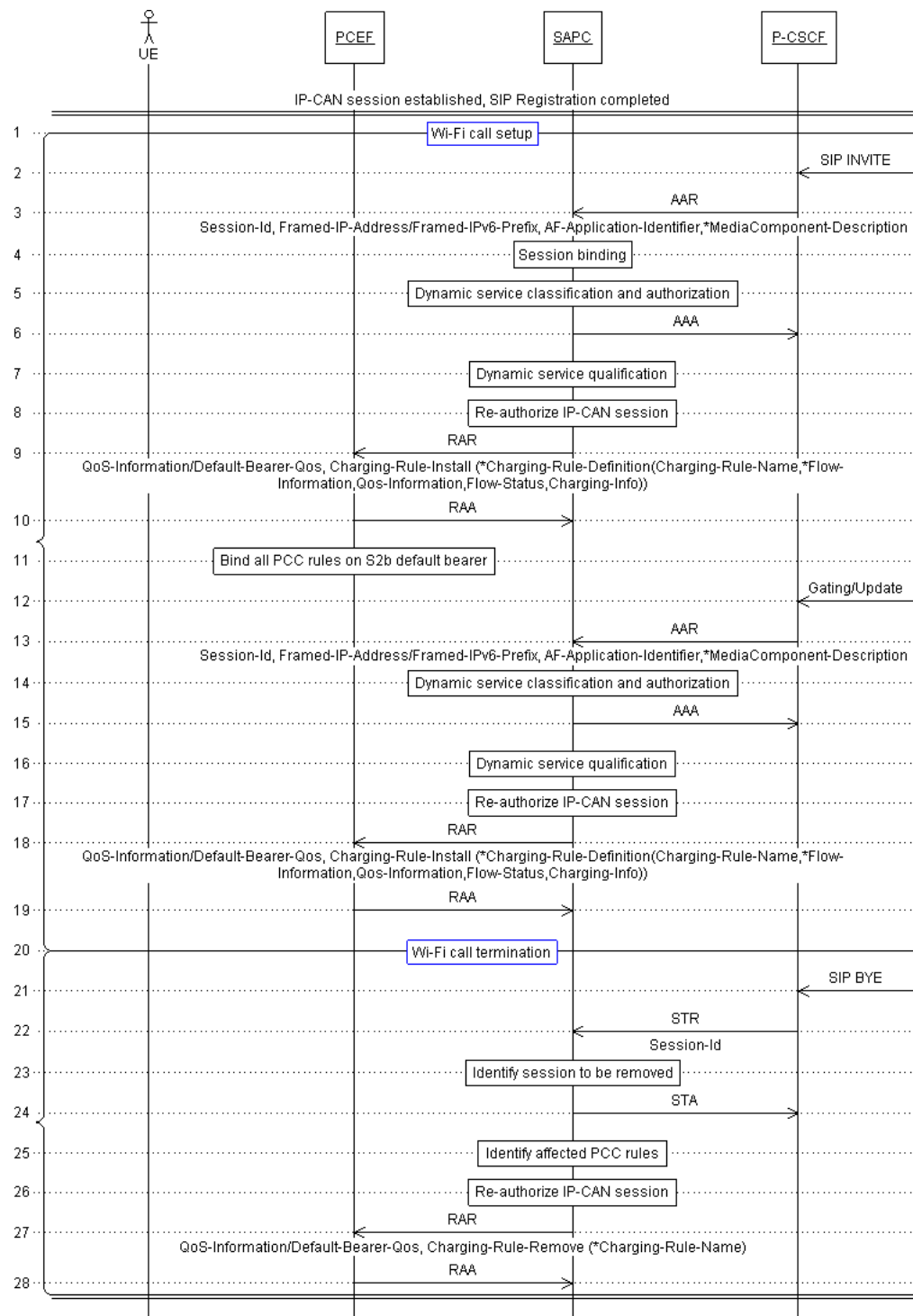


Figure 3 Wi-Fi Calling Setup



Wi-Fi Calling Setup

- 2. The P-CSCF receives a SIP INVITE message indicating the SIP call setup.
- 3. The SAPC receives an AAR message from the P-CSCF including the AF-Application-Identifier AVP to indicate that the new AF session relates to the Wi-Fi calling service.
- 4. The SAPC performs the session binding to associate the IP flows in the AF session information with the existing IP-CAN session for the Wi-Fi calling service. For more information about session binding, refer to [Dynamic Policy Control \(Rx\)](#), Reference [3].
- 5. The SAPC performs dynamic service classification and authorization for the Wi-Fi calling service.
- 6. The SAPC sends an AAA message to the P-CSCF as a response.
- 7. The SAPC performs dynamic service qualification for the Wi-Fi calling service.
- 8. The SAPC performs a reauthorization of the IP-CAN session.
- 9. The SAPC generates the dynamic PCC rules and sends a Gx RAR message to the PCEF to enforce the PCC rules including the QoS information.
- 10. The SAPC receives a Gx RAA message from the PCEF as a response.
- 11. The PCEF accepts the installation of PCC rules and binds all PCC rules on the S2b default bearer.
- 12. The P-CSCF receives a gating or update message.
- 13. The SAPC receives an AAR message from the P-CSCF indicating the AF session modification.
- 14. The SAPC performs dynamic service classification and authorization for the Wi-Fi calling service.
- 15. The SAPC sends an AAA message to the P-CSCF as a response.
- 16. The SAPC performs dynamic service qualification for the Wi-Fi calling service.
- 17. The SAPC performs a reauthorization of the IP-CAN session.
- 18. The SAPC updates dynamic PCC rules including the QoS information and sends a Gx RAR message to the PCEF to update PCC rules including the QoS information.
- 19. The SAPC receives a Gx RAA message from the PCEF as a response.



Wi-Fi Calling Termination

- 21. The P-CSCF receives a SIP BYE message indicating the SIP call termination.
- 22. The SAPC receives an STR message from the P-CSCF to remove the AF session for the Wi-Fi calling service.
- 23. The SAPC identifies the session to be removed.
- 24. The SAPC sends an STA message to the P-CSCF as a response.
- 25. The SAPC identifies the affected dynamic PCC rules to be removed.
- 26. The SAPC performs a reauthorization of the IP-CAN session.
- 27. The SAPC sends a Gx RAR message to the PCEF to remove the dynamic PCC rules for the Wi-Fi calling service.
- 28. The SAPC receives a Gx RAA message as a response.

4.2 Handover between VoLTE and Wi-Fi

4.2.1 Handover from Wi-Fi to VoLTE

The following traffic case occurs when the UE loses the Wi-Fi signal and determines to handover current sessions from Wi-Fi to LTE.

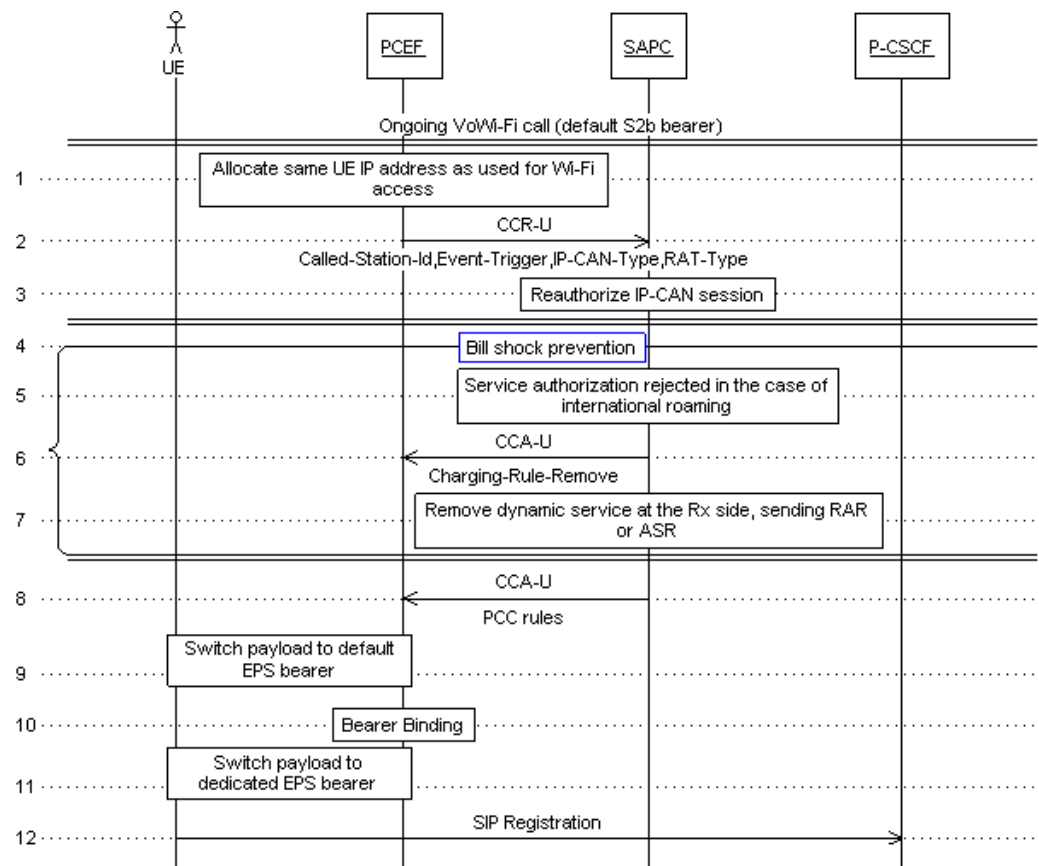


Figure 4 Handover from Wi-Fi to VoLTE

The UE moves from Wi-Fi access to LTE:

- 1. The PCEF allocates the same UE IP address for the LTE access as used for Wi-Fi access.
- 2. The SAPC receives a Gx CCR-U from the PCEF indicating the IP-CAN session modification. The main information that the PCEF includes:

- Called-Station-Id AVP: This indicates the IMS APN for the IP-CAN session.
- Event-Trigger AVP: This indicates the events IP_CAN_CHANGE (7).
- IP-CAN-Type AVP: This indicates the IP-CAN type “3GPP-EPS” (5).
- RAT-Type AVP: This indicates the RAT type “EUTRAN”.

Note: When the SAPC subscribes the IP_CAN_CHANGE (7) event trigger and the IP-CAN type is changed, the SAPC receives the IP-CAN-Type AVP and the RAT-Type AVP regardless of whether the SAPC subscribes the RAT_CHANGE (2) event trigger.



- 3. The SAPC reauthorizes the IP-CAN session.
- 4-7. When the SAPC detects the handover from Wi-Fi to VoLTE and the subscriber is roaming, the SAPC can reject the service authorization for the Wi-Fi calling according to policies:
 - 5. The SAPC rejects dynamic service authorization for the service at the Gx side.
 - 6. The SAPC sends a Gx CCA-U message to the PCEF including dynamic rules for the Wi-Fi calling service to be removed.
 - 7. The SAPC removes the associated flows at the Rx side, sending RAR or ASR message (refer to [Dynamic Policy Control \(Rx\)](#), Reference [3]).
- 8. If the subscriber is not roaming, the SAPC then sends a Gx CCA-U message to the PCEF to enforce the dynamic PCC rules including the QoS for the Wi-Fi calling service.
- 9. The PCEF installs the dynamic PCC rules on default EPS bearer before the dedicated EPS bearer is established. In the PCEF, the payload is switched to the default EPS bearer.
- 10. The PCEF performs the bearer binding.
- 11. The PCEF evaluates whether it is possible to use one of existing bearers to fulfill the QoS requirements of the dynamic PCC rules. If it is not possible, the PCEF initiates the establishment of a dedicated EPS bearer and installs dynamic PCC rules on dedicated EPS bearers. In the PCEF, the payload is switched to the dedicated EPS bearer.
- 12. Once the IPsec and GTP tunnels are established, the UE initiates the SIP Registration procedure to the IMS network to inform of the new access type for the ongoing session.

4.2.2 Handover from VoLTE to Wi-Fi

The following traffic case occurs when the UE detects the presence of an untrusted Wi-Fi network and determines to hand over current sessions from LTE to Wi-Fi.

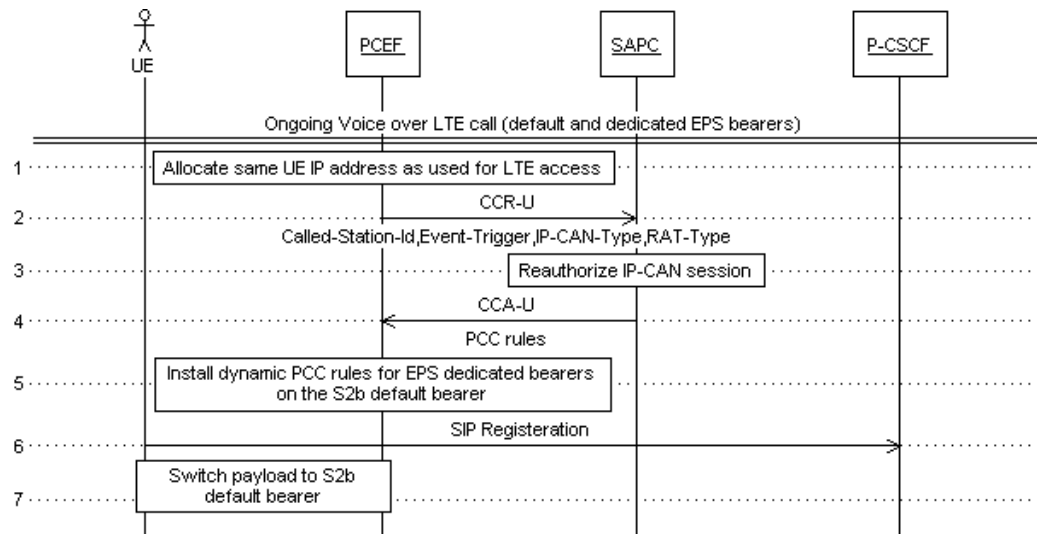


Figure 5 Handover from VoLTE to Wi-Fi

The UE moves from LTE to Wi-Fi access:

- 1. The PCEF allocates the same UE IP address for the Wi-Fi access as used for LTE access.
- 2. The SAPC receives a Gx CCR-U message from the PCEF indicating the IP-CAN session modification. The main information that the PCEF includes:
 - Called-Station-Id AVP: This indicates the IMS APN for the IP-CAN session.
 - Event-Trigger AVP: This indicates the events IP_CAN_CHANGE (7).
 - IP-CAN-Type AVP: This indicates the IP-CAN type “Non-3GPP-EPS” (6).
 - RAT-Type AVP: This indicates the RAT type “WLAN” (3).

Note: When the SAPC subscribes the IP_CAN_CHANGE (7) event trigger and the IP-CAN type is changed, the SAPC receives the IP-CAN-Type AVP and the RAT-Type AVP regardless of whether the SAPC subscribes the RAT_CHANGE (2) event trigger.

- 3. The SAPC reauthorizes the IP-CAN session evaluating controls configured for the PCEF, such as service access control, bearer QoS control, service QoS control, and service charging control.
- 4. The SAPC sends a Gx CCA-U message to the PCEF to enforce the dynamic PCC rules including the information previously computed.
- 5. The PCEF installs the dynamic PCC rules on the S2b default bearer.
- 6. Once the IPsec and GTP tunnels are established, the UE initiates the SIP Registration procedure to the IMS network to inform of the new access type for the ongoing session.



- 7. In the PCEF, the payload is switched to the S2b default bearer.

4.3 Error Handling

For information about error handling, refer to [Access and Charging Control \(Gx\)](#), Reference [1], and [Dynamic Policy Control \(Rx\)](#), Reference [3].

5 Operational Conditions

5.1 External Conditions

Not applicable.



Glossary

AF

Application Function

ENIW

Network Integrated Wi-Fi

ePDG

Evolved Packet Data Gateway

EPG

Evolved Packet Gateway

EPS

Evolved Packet System

GTP

GPRS Tunneling Protocol

IMS

IP Multimedia Subsystem

P-CSCF

Proxy Call Session Control Function

PCC

Policy Charging and Control

PCEF

Policy and Charging Enforcement Function

QoS

Quality of Service

SAPC

Ericsson Service-Aware Policy Controller

SIP

Session Initiation Protocol

UE

User Equipment

VoLTE

Voice over LTE

Wi-Fi

Wireless Fidelity





Reference List

Ericsson Documents

- [1] Access and Charging Control (Gx)
- [2] Subscription and Policy Management
- [3] Dynamic Policy Control (Rx)

Standards

- [4] Policy and Charging Control over Gx reference point, 3GPP TS 29.212