ETSI TS 123 380 V12.1.0 (2015-01)

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
IMS Restoration Procedures
(3GPP TS 23.380 version 12.1.0 Release 12)

Reference
RTS/TSGC-0423380vc10

Keywords
GSM,LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights 2
Foreword 2
Modal verbs terminology 2
Foreword 5
Introduction 5
1 Scope 6
2 References 6
3 Definitions, symbols and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 Restoration of Data in the S-CSCF 7
4.1 General 7
4.2 Registration Procedure 7
4.2.1 Introduction 7
4.2.2 S-CSCF Restoration after Failure 7
4.2.3 S-CSCF Restoration during Registration Process 8
4.3 UE Terminating Procedure 8
4.3.1 Introduction 8
4.3.2 S-CSCF Restoration after Restart 9
4.3.3 S-CSCF Restoration after Failure 9
4.4 UE Originating Procedure 9
4.4.1 Introduction 9
4.4.2 S-CSCF Restoration after Restart 9
4.4.3 S-CSCF Restoration after Failure 10
4.5 SIP-AS Originating Procedure 10
4.5.1 Introduction 10
4.5.2 S-CSCF Restoration after Restart 10
4.5.3 S-CSCF Restoration after Failure 10
4.6 S-CSCF Data Restoration Information Backup and Update Procedures 11
4.6.1 Introduction 11
4.6.2 Backup and Update of S-CSCF Restoration Information during Registration Process 11
4.6.3 Backup and Update of S-CSCF Restoration Information after UE"s Subscription 11
5 Recovery after P-CSCF failure 12
5.0 General 12
5.1 Update PDP context/Bearer at P-CSCF failure 12
5.1.1 General requirements 12
5.1.2 Network recovery information flow - Update PDP context / Bearer 12
5.1.3 Network recovery information flow with S5 PMIP 14
5.2 Inform UE about P-CSCF failure 15
5.2.1 General requirements 15
5.2.2 Network recovery information flow – Inform UE at P-CSCF failure 15
5.2.3 Network recovery information flow – Inform UE at P-CSCF failure with S5 PMIP 17
5.3 Network recovery information flow – UE uses keep alive mechanism 18
5.4 HSS-based P-CSCF restoration 19
5.4.1 Introduction 19
5.4.2 Description 19
5.4.2.1 General 19
5.4.2.2 P-CSCF restart/failure detection by S-CSCF 21
5.4.2.2.1 General 21
5.4.2.2.2 Direct connection from S-CSCF to P-CSCF 21
5.4.2.2.3 S-CSCF connection to P-CSCF via IBCF/ATCF 21

5.4.2.3 MME/SGSN mechanism support 21
5.4.3 PCO-based optional extension 21
5.4.3.1 Introduction 21
5.4.3.2 Description 22
5.4.4.3 UE indication of support for "Update PDP context/bearer at P-CSCF failure" Restoration 24
5.4.5 Coexistence with "Update PDP context/bearer at P-CSCF failure" mechanism 24
5.4.6 HSS based P-CSCF restoration in roaming scenarios 24
5.5 PCRF-based P-CSCF restoration 24
5.5.1 Introduction 24
5.5.2 PCRF-based P-CSCF restoration information flow - deactivate PDN connection/PDP context 25
5.5.3 PCO-based optional extension 28
5.5.3.1 Introduction 28
5.5.3.2 Description 28
5.5.3.3 UE indication of support for "Update PDP context/bearer at P-CSCF failure" Restoration 28
5.5.4 Coexistence with "Update PDP context/bearer at P-CSCF failure" mechanism 28
5.5.5 P-CSCF restoration in roaming scenarios for PCRF based solution 28

Annex A (informative): Change history 30

History 32

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

Although network nodes in the IMS Core Network should have a very high availability, some maintenance downtime and occasional failures are unavoidable. Communication links although designed with robust protocols between the network elements are also subject to failures. This document specifies a set of standardized procedures for automatic restoration after loss or corruption of data reducing the impact of these problems in order to improve service to the users. The scenarios covered here for the IMS Domain are similar to those covered in 3GPP TS 23.007 [2] for the CS and PS Domains.

1 Scope

The present document specifies the procedures required in 3GPP IMS to handle a S-CSCF or a P-CSCF service interruption scenario with minimum impact to the service to the end user.

NOTE: IMS Restoration Procedures covering service interruption of other network elements are not defined in this version of the specification.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.007: "Restoration procedures".

[3] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[4] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification".

[5] 3GPP TS 29.213: "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping".

[6] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[7] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[8] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[9] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[10] 3GPP TS 29.274: "3GPP Evolved Packet System. Evolved GPRS Tunnelling Protocol for EPS (GTPv2)".

[11] IETF RFC 3361: "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[12] IETF RFC 1034: "Session Initiation Protocol (SIP): Locating SIP Servers".

[13] IETF RFC 3319: "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[14] IETF RFC 6223: "Indication of Support for Keep-Alive".

[15] 3GPP TS 29.275: "Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3".

[16] IETF RFC 7077: "Update Notifications for Proxy Mobile IPv6".

[17] 3GPP TS 23.401: "GPRS Enhancements for E-UTRAN Access".

[18] IETF RFC 3261: "SIP: Session Initiation Protocol".

[19] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[20] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[21] GSMA PRD IR.65: "IMS Roaming and Interworking Guidelines, version 14.0".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Service Interruption: A period of time in which one or more network elements do not respond to requests and do not send any requests to the rest of the system.

S-CSCF Restoration Information: Information required for the S-CSCF to handle traffic for a registered user. This information is stored in HSS and if lost, retrieved by the S-CSCF.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

LIR	Location Information Request
LIA	Location Information Answer
SAR	Server Assignment Request
SAA	Server Assignment Answer
UAR	User Authorization Request
UAA	User Authorization Answer

4 Restoration of Data in the S-CSCF

4.1 General

The following clauses describe the IMS Restoration Procedures for the S-CSCF service interruption in each of the scenarios where they apply.

4.2 Registration Procedure

4.2.1 Introduction

The following clauses specify the behaviour of HSS and S-CSCF if they support the IMS restoration feature.

4.2.2 S-CSCF Restoration after Failure

If the UE initiates a SIP REGISTER and the S-CSCF returned by the HSS during user registration status query procedure fails, the I-CSCF is unable to contact the S-CSCF. In this case, regardless of this registration is an initial registration, a re-registration or a de-registration, the I-CSCF shall send UAR with Authorization Type set to

REGISTRATION_AND_CAPABILITIES to the HSS to explicitly request S-CSCF capabilities. After re-assignment of another S-CSCF according to the S-CSCF capabilities, the I-CSCF shall forward the REGISTER to the new S-CSCF. For registrations and re-registrations, S-CSCF shall proceed with the registration procedure as for initial registration, except for the clauses specified in 4.2.3.

For de-registrations, S-CSCF shall proceed as for user-initiated de-registration.

4.2.3 S-CSCF Restoration during Registration Process

During the registration procedure, the HSS shall send all the registered Private User Identities sharing the same Public User Identity which is being registered in the SAA, in addition to the basic user data to the S-CSCF. Then the S-CSCF compares the registered Private User Identities received from the HSS with the ones it stores. If there are any registered Private User Identities the S-CSCF does not have their registration data, the S-CSCF shall send SAR with Server Assignment Type set to NO_ASSIGNMENT to the HSS to retrieve the S-CSCF restoration information for the registered Public User Identity. If there are S-CSCF restoration information related to the Public User Identity stored in the HSS, the HSS shall send the S-CSCF restoration information together with the user profile in the SAA to the S-CSCF. The result code shall be set to DIAMETER_SUCCESS.

If there are more than one group of S-CSCF restoration information related to the Public User Identity stored in the HSS, which may happen if the Public User Identity is shared by multiple Private User Identities, the HSS shall include all of the S-CSCF restoration information in the SAA. One group of S-CSCF restoration information corresponds to one Private User Identity.

If the S-CSCF receives an initial registration request for a Public User Identity that does not match any Public User Identity currently registered with the same Private User Identity as in the request at this S-CSCF, the S-CSCF shall check whether there is a reg-id parameter in the Contact header in the SIP REGISTER message and whether there is an "sos" SIP URI parameter in the SIP REGISTER message. Only when a reg-id parameter exists and an "sos" SIP URI parameter does not exist, the S-CSCF shall indicate to the HSS that the registration is related to a multiple registration.

If the HSS receives an SAR request with multiple registration indication, and the Public User Identity is stored as registered in the HSS, and there is restoration information related to the Private User Identity, the HSS shall not overwrite stored restoration information, instead, it shall send the stored S-CSCF restoration information together with the user profile in the SAA. The result code shall be set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE. The S-CSCF shall send a new SAR with Server-Assignment-Type set to RE_REGISTRATION and the User Data Already Available parameter set to USER_DATA_ALREADY_AVAILABLE to update the restoration information in the HSS in accordance to the current registration event.

If the S-CSCF receives a user-initiated deregistration request for a Public User Identity that does not match any Public User Identity currently registered with the same Private User Identity as in the request at this S-CSCF, the S-CSCF shall check whether there is a reg-id parameter in the Contact header in the received SIP REGISTER message,

- if a reg-id parameter exists, the S-CSCF shall:

    - 1. Send SAR with Server-Asignment-Type set to NO_ASSIGNMENT to retrieve the S-CSCF restoration information associated with the Public User Identity. The Result-Code shall be set to DIAMETER SUCCESS.

    - 2. Compare the contact address(es) received in SAA with the contact address(es) in REGISTER request:

    - If they are not the same, the S-CSCF shall send SAR with Server-Asignment-Type set to RE_REGISTRATION to update the S-CSCF restoration information in HSS with the Contact address(es) still associated with the Public User Identity after the deregistration event.

  Otherwise, the S-CSCF shall send SAR with Server-Asignment-Type set to USER_DEREGISTRATION.

4.3 UE Terminating Procedure

4.3.1 Introduction

The following clauses specify the behaviour of HSS, I-CSCF and S-CSCF if they support the IMS Restoration feature.

4.3.2 S-CSCF Restoration after Restart

The S-CSCF lost all user data if it restarts after a failure or it is unable to trust any data after it resumes operation, due to the fact that it may have lost profile updates from the HSS in the service interruption period. If such a S-CSCF receives a terminating service request from the I-CSCF, it sends an SAR to the HSS for unregistered service data. In this case, HSS and S-CSCF proceed as indicated in 3GPP TS 29.228 [3], except that

- if the Public User Identity is stored as registered in the HSS, and there are S-CSCF restoration information related to the Public User Identity stored in the HSS, the HSS shall send the S-CSCF restoration information together with the user profile in the SAA. The result code shall be set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE. The S-CSCF shall trigger matched registered services for the Public User Identity.

If there are more than one group of S-CSCF restoration information related to the Public User Identity, which may happen if the Public User Identity is shared by multiple Private User Identities, the HSS shall include all of the S-CSCF restoration information in the SAA. One group of S-CSCF restoration information corresponds to one Private User Identity.

If the S-CSCF restoration information received includes the UE"s subscription information, the S-CSCF shall construct a NOTIFY message according to the information and send it to the UE (or UEs if the IMPU is shared between several IMPIs) to trigger a new registration at anytime after normal processing of the terminating request.

4.3.3 S-CSCF Restoration after Failure

If the S-CSCF returned by the HSS during location query procedure fails, the I-CSCF is unable to contact the S-CSCF during terminating procedure. In this case, the I-CSCF shall send LIR to the HSS to explicitly request S-CSCF capabilities. If the HSS returns the S-CSCF capabilities to the I-CSCF, after re-selection of another S-CSCF according to the S-CSCF capabilities, the I-CSCF shall forward the service request to the new S-CSCF. The HSS and this new S-CSCF shall behave as described in clause 4.3.2, except that the HSS shall overwrite the S-CSCF name when receiving the SAR request, only if there is a previous explicit LIR request for S-CSCF capabilities.

NOTE: If the HSS indicates during location query procedure that the server name returned corresponds to an AS, then the service request is for PSI direct routing. In this case, IMS Restoration Procedures will not be executed and I-CSCF will reject the service request.

4.4 UE Originating Procedure

4.4.1 Introduction

The following clauses specify the behaviour of HSS, S-CSCF and P-CSCF if they support the IMS Restoration feature.

4.4.2 S-CSCF Restoration after Restart

The S-CSCF lost all user data if it restarts after a failure or it is unable to trust any data after it resumes operation, due to the fact that it may have lost profile updates from the HSS in the service interruption period. If such a S-CSCF receives an originating request different from SIP REGISTER coming from the UE, the S-CSCF shall send SAR to the HSS with Server Assignment Type set to NO_ASSIGNMENT to restore the user data. If the S-CSCF name sent in the Server-Assignment-Request command and the previously assigned S-CSCF name stored in the HSS are different, which may happen if S-CSCF reassignment occurred during a terminating restoration before, the HSS shall not overwrite the S-CSCF name; instead it shall send a response to the S-CSCF with result code set to DIAMETER_UNABLE_TO_COMPLY, as specified in the 3GPP TS 29.228 [3]. If there are S-CSCF restoration information related to the Public User Identity stored in the HSS, the HSS shall send the S-CSCF restoration information together with the user profile in the SAA to the S-CSCF. If the HSS returns an error DIAMETER_UNABLE_TO_COMPLY to the S-CSCF, the S-CSCF shall then return a specific error response to the UE to trigger a new registration.

If there are more than one group of S-CSCF restoration information related to the Public User Identity stored in the HSS, which may happen if the Public User Identity is shared by multiple Private User Identities, the HSS shall include

all of the S-CSCF restoration information in the SAA. One group of S-CSCF restoration information corresponds to one Private User Identity.

If the S-CSCF receives SAA with the service profile of the user, the S-CSCF shall continue the originating service as normal.

If the S-CSCF receives SAA with S-CSCF restoration information and the S-CSCF restoration information includes the UE"s subscription information, the S-CSCF shall construct a NOTIFY message according to the information and send it to the UE (or UEs if the IMPU is shared between several IMPIs) to trigger a new registration at anytime after normal processing of the originating request.

4.4.3 S-CSCF Restoration after Failure

If the UE initiates an originating service request different from SIP REGISTER and the P-CSCF is unable to contact the S-CSCF in the Route, the P-CSCF shall return a specific error response to the UE to trigger a new registration.

4.5 SIP-AS Originating Procedure

4.5.1 Introduction

The following clauses specify the behaviour of HSS, I-CSCF and S-CSCF if they support the IMS Restoration feature.

4.5.2 S-CSCF Restoration after Restart

The S-CSCF lost all user data if it restarts after a failure or it is unable to trust any data after it resumes operation, due to the fact that it may have lost profile updates from the HSS in the service interruption period. If such S-CSCF receives an originating request on behalf of a user (i.e. top-most route header in request contains "orig" parameter) coming from an AS, the S-CSCF shall send SAR to the HSS with Server Assignment Type set to UNREGISTERED_USER to inform the HSS that the user is unregistered. HSS and S-CSCF proceed as indicated in 3GPP TS 29.228 [3], except that:

- if the Public User Identity is stored as registered in the HSS, and there is S-CSCF restoration information related to the Public User Identity stored in the HSS, the HSS shall send the S-CSCF restoration information together with the user profile in the SAA. The result code shall be set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE. The S-CSCF shall trigger matched originating services for the Public User Identity.if the Public User Identity is stored as registered in the HSS, and there is no S-CSCF restoration information related to the Public User Identity stored in the HSS, the HSS shall send the user profile in the SAA and set the registration state for the Public Identity to unregistered. The result code shall be set to DIAMETER_SUCCESS. The S-CSCF shall trigger matched originating unregistered services for the Public User Identity.

- if the S-CSCF name sent in the Server-Assignment-Request command and the previously assigned S-CSCF name stored in the HSS are different, the HSS shall not overwrite the S-CSCF name. Result Code will be DIAMETER_IDENTITY_ALREADY_REGISTERED. The S-CSCF shall return a specific error response to AS. The AS shall resend the request to the I-CSCF.

NOTE: The address of the S-CSCF can be obtained by AS either by querying the HSS on the Sh interface or during third-party registration. It may happen that if AS is using third party registration and a reassignment occurred during a terminating request, AS will have the wrong S-CSCF name.

4.5.3 S-CSCF Restoration after Failure

If the application server sends the originating service request on behalf of the user to the S-CSCF, and the S-CSCF can not be contacted, after timeout, the application server shall resend the originating service request to the I-CSCF.

If the application server sends the originating service request directly to the I-CSCF, or resends the originating service request to the I-CSCF due to the S-CSCF can not be contacted, the I-CSCF shall behave as in section 4.3.3. The S-CSCF and HSS shall behave as in section 4.5.2, except that the HSS shall overwrite the S-CSCF name when receiving the SAR request, only if there is a previous explicit LIR request for S-CSCF capabilities.

4.6 S-CSCF Data Restoration Information Backup and Update Procedures

4.6.1 Introduction

The following clauses specify the behaviour of HSS and S-CSCF if they support the IMS Restoration feature.

4.6.2 Backup and Update of S-CSCF Restoration Information during Registration Process

The S-CSCF shall backup the following data in the HSS during the initial registration process.

- the list of SIP proxies in the path (normally it would be just the P-CSCF address)
- the Contact Information (Contact Addresses and Contact Header parameters)
- the Authentication Information (SIP-Authentication-Scheme)

The S-CSCF may backup the following data in the HSS during the initial registration process.

- the Initial-CSeq-Sequence-Number and the Call-ID used if used for temporary GRUU generation (see IETF RFC 3261 [18])

This is done with an additional information element in the SAR requesting user information, in addition to the basic set of information required to handle traffic, as specified in the 3GPP TS 29.228 [3]. The information is associated with the Private User Identity and the Implicit Registration Set that is affected by the SAR request. The HSS shall store this information.

If any of the above data is changed, the S-CSCF shall update it in the HSS using SAR request with Server-Assignment-Type set to RE_REGISTRATION and the User Data Already Available parameter set to USER_DATA_ALREADY_AVAILABLE, as specified in the 3GPP TS 29.228 [3].

4.6.3 Backup and Update of S-CSCF Restoration Information after UE"s Subscription

If the S-CSCF receives the UE"s subscription to notification of the reg-event for the first time, the S-CSCF shall send an SAR to the HSS to store the following UE"s subscription information.

- Call-ID, From, To, Record-Route, Contact

To avoid frequent storing of the subscription information in the HSS, the CSeq should not be included in the S-CSCF restoration information. Instead, the CSCF shall ensure that subsequent notification after retrieving this data includes a sufficiently large Cseq value so that the UE is able to accept it.

This is done with Server Assignment Type set to RE_REGISTRATION and the User Data Already Available parameter set to USER_DATA_ALREADY_AVAILABLE in the SAR, as specified in the 3GPP TS 29.228 [3]. The information is associated with the Private User Identity affected by the SAR request. The HSS shall store this information.

If any of the above data is changed, the S-CSCF shall update it in the HSS using SAR request with Server-Assignment-Type set to RE_REGISTRATION and the User Data Already Available parameter set to USER_DATA_ALREADY_AVAILABLE, as specified in the 3GPP TS 29.228 [3].

The S-CSCF shall send the registration data together with the subscription data as one S-CSCF restoration information. Each time the HSS receives the S-CSCF restoration information related to the same Private User Identity in the SAR with Server-Assignment-Type set to RE_REGISTRATION, the HSS shall overwrite the previous S-CSCF restoration information.

5 Recovery after P-CSCF failure

5.0 General

The following clauses show the requirements and information flows of IMS Restoration Procedures for the P-CSCF service interruption in each of the scenarios where they apply.

Procedures over S9 between V-PCRF and H-PCRF are not supported in this release of the specification.

5.1 Update PDP context/Bearer at P-CSCF failure

These flows show the procedures performed by the network at P-CSCF failure after user initiated registration..

5.1.1 General requirements

The following points are considered as requirements for the purpose of these procedures.

1. P-CSCF discovery is performed by requesting and provisioning P-CSCF address(es) within Protocol Configuration Options (PCO), as specified in 3GPP TS 29.061 [9], subclause 13a.2.1

2. The UE supports PCO IE, as specified in 3GPP TS 24.008 [4], subclause 10.5.6.3.

3. For the GTP based S5 interface, GTPv1, as specified in 3GPP TS 29.060 [8] or GTPv2, as specified in 3GPP TS 29.274 [10] are supported by the GGSN/PDN-GW.

4. For the PMIP based S5 interface, PMIPv6, as specified in 3GPP TS 29.275 [15] is supported by the PDN-GW.

5.1.2 Network recovery information flow - Update PDP context / Bearer

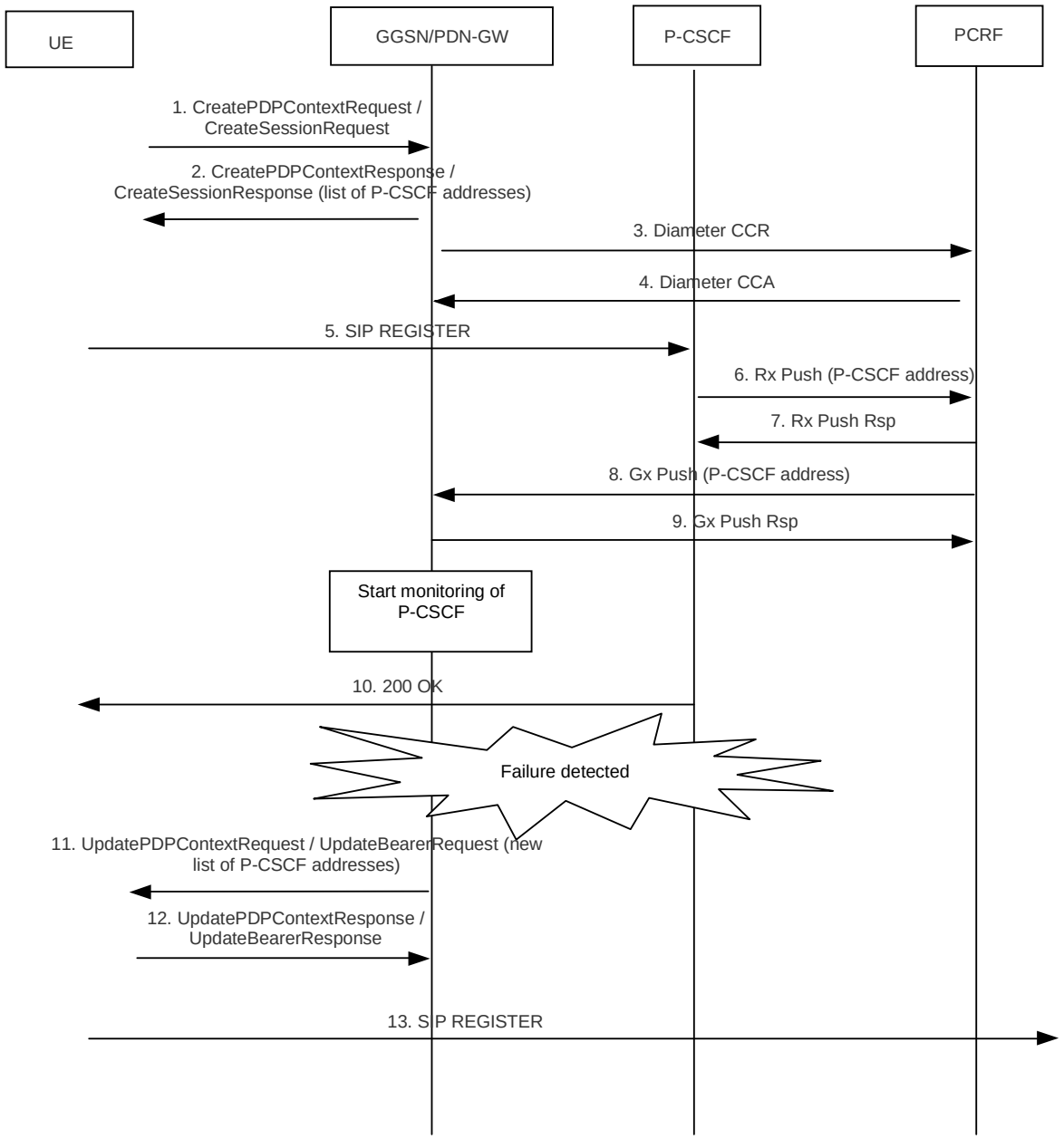

Figure 5.1.2a: P-CSCF failure (new list of P-CSCFs in PCO)

1. The UE initiates an IP-CAN session.
2. P-CSCF discovery is performed. A list of P-CSCF addresses is received in CreatePDPContextResponse / CreateBearerResponse within the PCO IE.
3. The GGSN/PDN-GW sends CCR to request for PCC rules, as specified in 3GPP TS 29.212 [6].
4. The PCRF provides PCC rules to be applied in CCA.
5. The UE performs an initial registration towards a P-CSCF from the received list.
6. The P-CSCF sends Rx Push (see 3GPP TS 29.214 [7]) to provide the PCRF with the P-CSCF selected by the UE.
7. The PCRF sends Rx Push reponse.
8. The PCRF uses a Gx push procedure to provide the GGSN/PDN-GW with the P-CSCF address.

9. The GGSN/PDN-GW stores this address for the UE and sends Gx Push Rsp. Also, the GGSN/PDN-GW starts monitoring the health of the P-CSCF if not already done.

10. The P-CSCF sends 200 OK to the UE.

11. A failure in P-CSCF is detected via Gi/sGi by the GGSN/PDN-GW. The GGSN/PDN-GW sends a new PCO IE with a new list of P-CSCF addresses (which does not include the failed P-CSCF) to all UEs associated to the failed P-CSCF address.

12. The UEs acknowledge the request.

13. Upon receiving the new list of P-CSCFs, if the P-CSCF in use is missing, each UE performs an initial registration towards a new P-CSCF.

5.1.3 Network recovery information flow with S5 PMIP

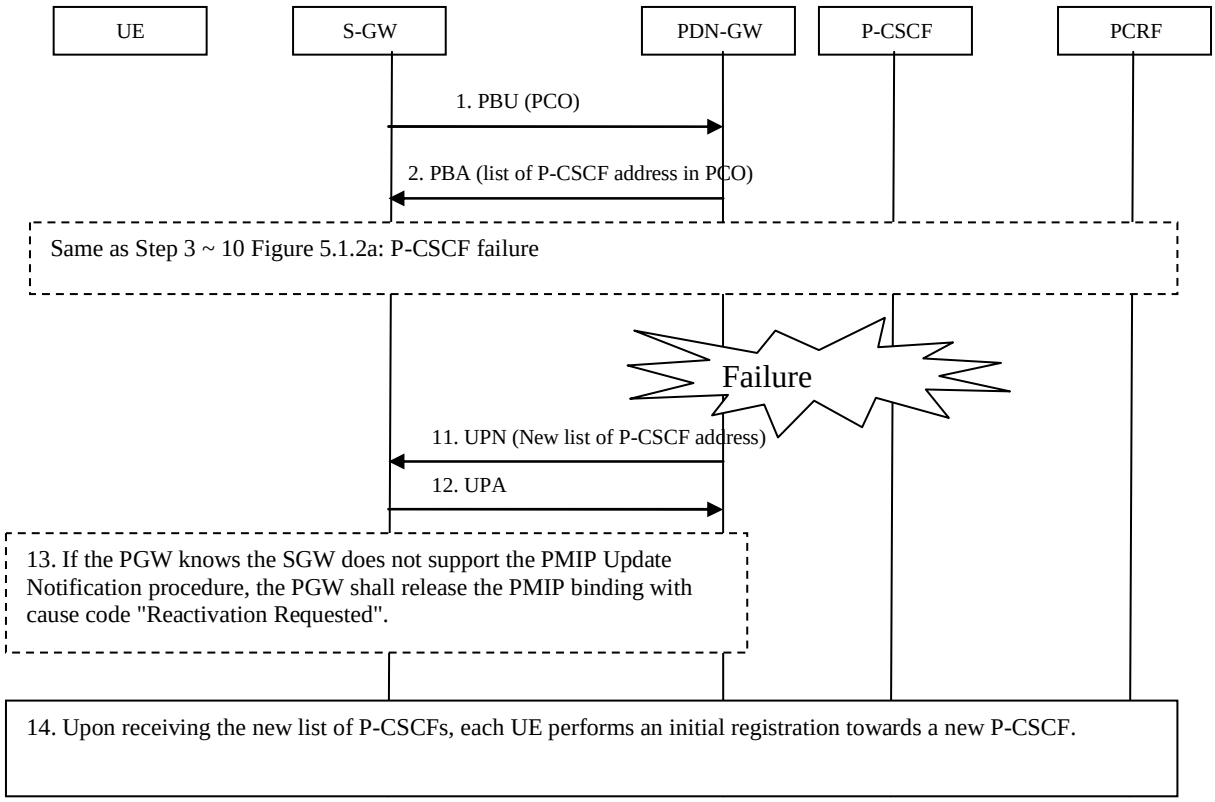

Figure 5.1.3: P-CSCF failure with S5 PMIP

1 ~ 10. The IMS session is setup as described in subclause 5.1.2 except S5 PMIP procedure is used between SGW and PGW.

11. Once a P-CSCF failure is detected via Gi/sGi by the PDN-GW, the PDN-GW shall send a PMIP UPN message (MN ID, APN, PDN connection ID, PCO, and Additional parameters) as specified in 3GPP TS 29.275 [15] and IETF draft-ietf-netext-update-notifications-12 [16]. The PCO contains a new list of P-CSCF address. The Notification reason shall indicate that update Bearer Context at P-CSCF failure is needed.

12. If the SGW supports the PMIP Update Notification message, it shall send Update Bearer Request message with the new list of P-CSCF address in the PCO to the MME/SGSN as part of the PGW initiated bearer modification without QoS update procedure as specified in 3GPP TS 23.401[17].

    Once the Update Bearer Response message is received, the SGW shall response with a PMIP UPA message (MN ID, APN, PDN connection ID, PCO, and Additional parameters) as specified in 3GPP TS 29.275 [15] and IETF RFC 7077 [16].

13. If the PGW knows the SGW does not support the PMIP Update Notification procedure, the PGW shall skip step 11 and release the PMIP binding with cause code "Reactivation Requested".

14. Upon receiving the new list of P-CSCFs, the UE may perform an initial registration towards a new P-CSCF.

5.2 Inform UE about P-CSCF failure

These flows show the procedures performed by the network at P-CSCF failure after user initiated registration..

5.2.1 General requirements

The following points are considered as requirements for the purpose of these procedures.

1. P-CSCF discovery is performed by requesting P-CSCF address(es) via DHCP method, as specified in 3GPP TS 29.061 [9], subclause 13a.2.1

2. The UE supports PCO IE, as specified in 3GPP TS 24.008 [4], subclause 10.5.6.3.

3. For the GTP based S5 interface, GTPv1, as specified in 3GPP TS 29.060 [8] or GTPv2, as specified in 3GPP TS 29.274 [10] are supported by the GGSN/PDN-GW

4. For the PMIPv6 based S5 interface, PMIPv6, as specified in 3GPP TS 29.275 [15] is supported by the PDN-GW.

5.2.2 Network recovery information flow – Inform UE at P-CSCF failure

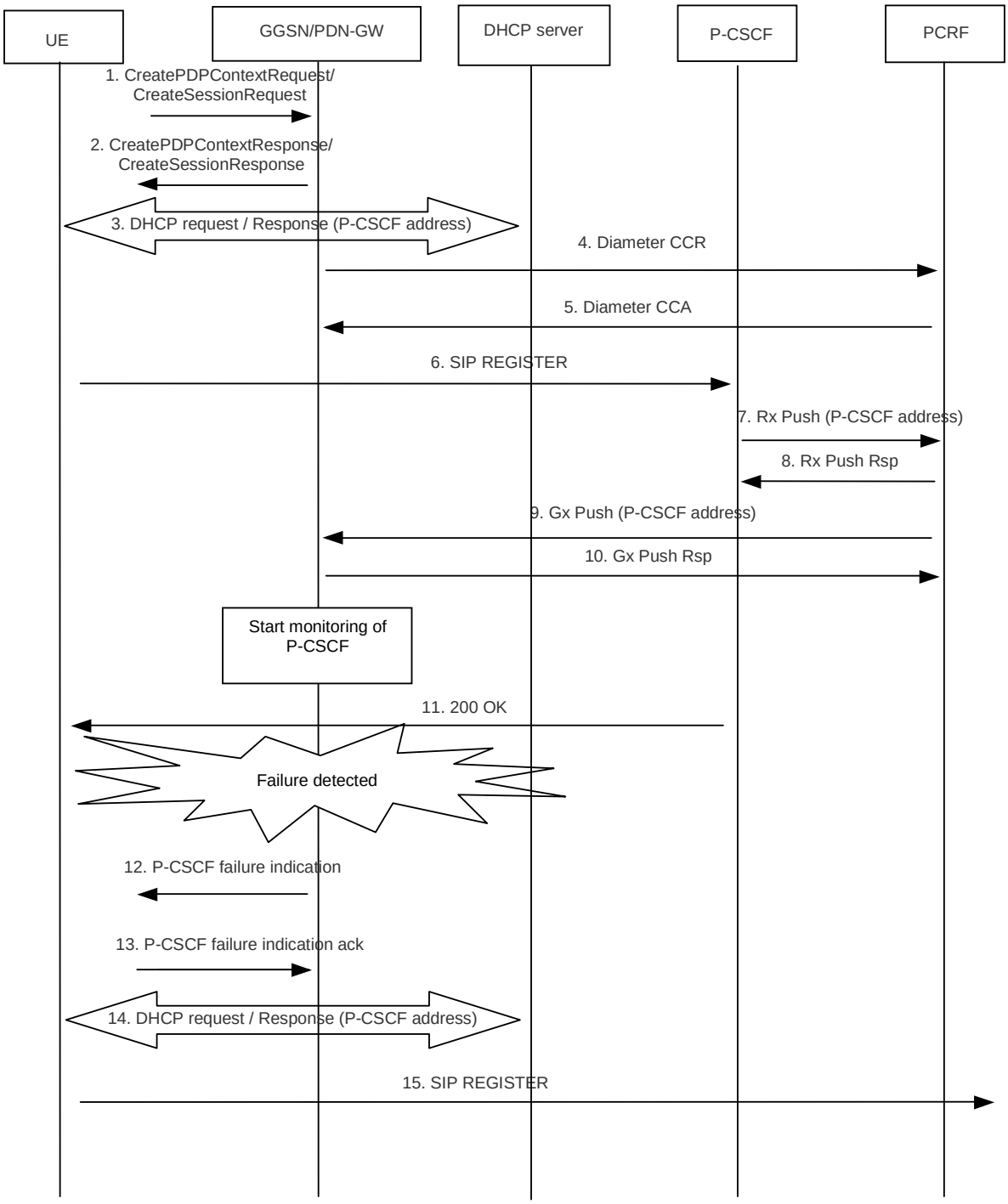

Figure 5.2.2a: P-CSCF failure for DHCP based scenarios

1-2. The UE initiates an IP-CAN session.

3. P-CSCF discovery is performed using DHCP based method. The GGSN/PDN-GW relays/send the list of P-CSCF addresses in DHCP response.

NOTE: The DHCP response can include either a list of P-CSCF IPv4/IPv6 addresses or a list of FQDNs (see IETF RFC 3361 [11] and IETF RFC 3319 [13]). If P-CSCF FQDNs were provided, the UE uses DNS SIP server resolution mechanism (see IETF RFC 3263 [12])

4. The GGSN/PDN-GW sends CCR to request for PCC rules, as specified in 3GPP TS 29.212 [6].

5. The PCRF provides PCC rules to be applied in CCA.
6. The UE performs an initial registration towards the P-CSCF received.
7. The P-CSCF sends Rx Push (see 3GPP TS 29.214 [7]) to provide the PCRF with the P-CSCF selected by the UE,
8. The PCRF sends Rx Push reponse.
9. The PCRF uses a Gx push procedure to provide the GGSN/PDN-GW with the P-CSCF address.
10. The GGSN/PDN-GW stores this address for the UE and sends Gx Push Rsp. Also, the GGSN/PDN-GW starts monitoring the health of the P-CSCF if not already done.
11. The P-CSCF sends 200 OK to the UE.
12. A failure in P-CSCF is detected via Gi/sGi by the GGSN/PDN-GW. The GGSN/PDN-GW informs to all UEs associated to the failed P-CSCF address that the P-CSCF is not available.
13. The UEs acknowledge the request.
14. The UE requests P-CSCF addresses (if needed) via new DHCP request.
15. The UE selects a new P-CSCF and initiates an initial IMS registration.

5.2.3 Network recovery information flow – Inform UE at P-CSCF failure with S5 PMIP

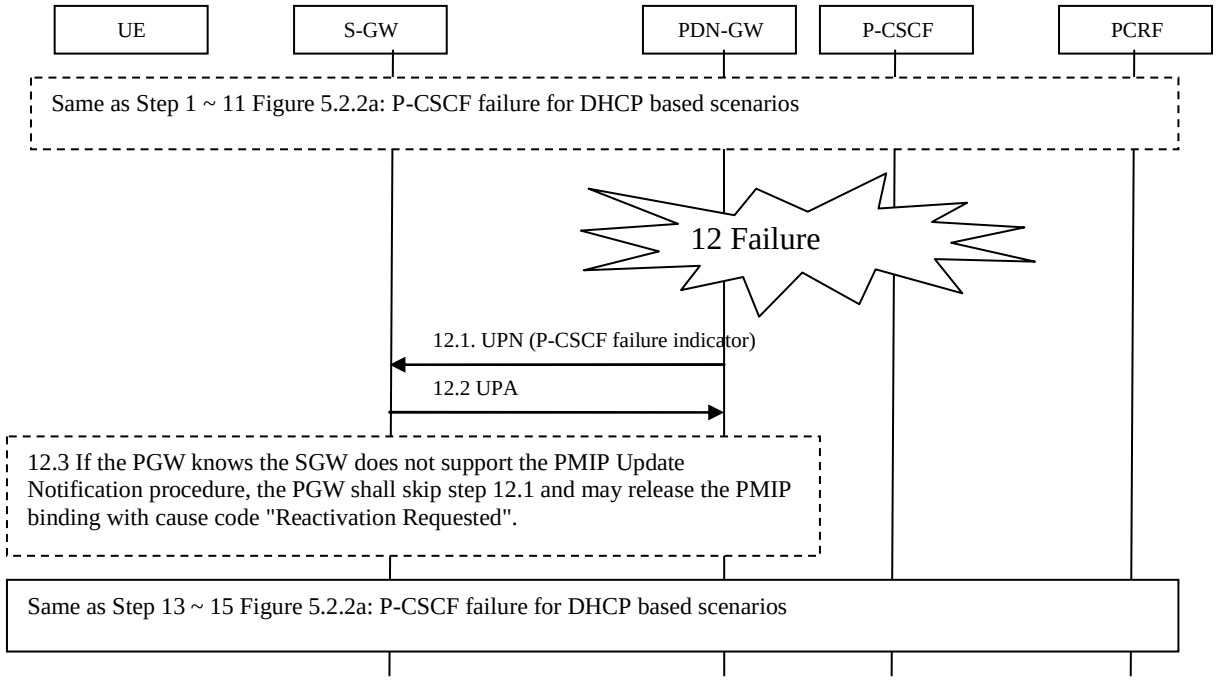

Figure 5.2.3-1: P-CSCF failure for DHCP based scenarios with S5 PMIP

1 ~ 11. Same as figure 5.2.2a step 1 ~ 11

12. A failure in P-CSCF is detected via Gi/sGi by the GGSN/PDN-GW. The GGSN/PDN-GW informs to all UEs associated to the failed P-CSCF address that the P-CSCF is not available.

    - The PDN-GW shall send a PMIP UPN message (MN ID, APN, PDN connection ID, PCO, and Additional parameters) as specified in 3GPP TS 29.275 [15] and IETF RFC 7077 [16]. The PCO contains a P-CSCF failure Indicator. The Notification reason shall indicate that there is a P-CSCF failure.

- If the SGW supports the PMIP Update Notification message, it shall send Update Bearer Request message with the P-CSCF failure Indicator in the PCO to the MME as part of the PGW initiated bearer modification without QoS update procedure as specified in 3GPP TS 23.401 [17]. Once the Update Bearer Response message is received, the SGW shall response with a PMIP UPA message (MN ID, APN, PDN connection ID, PCO, and Additional parameters) as specified in 3GPP TS 29.275 [15] and IETF RFC 7077 [16].

- If the PGW knows the SGW does not support the PMIP Update Notification procedure, the PGW may release the PMIP binding with cause code "Reactivation Requested".

13 ~ 15. Same as figure 5.2.2a step 13 ~15.

5.3 Network recovery information flow – UE uses keep alive mechanism

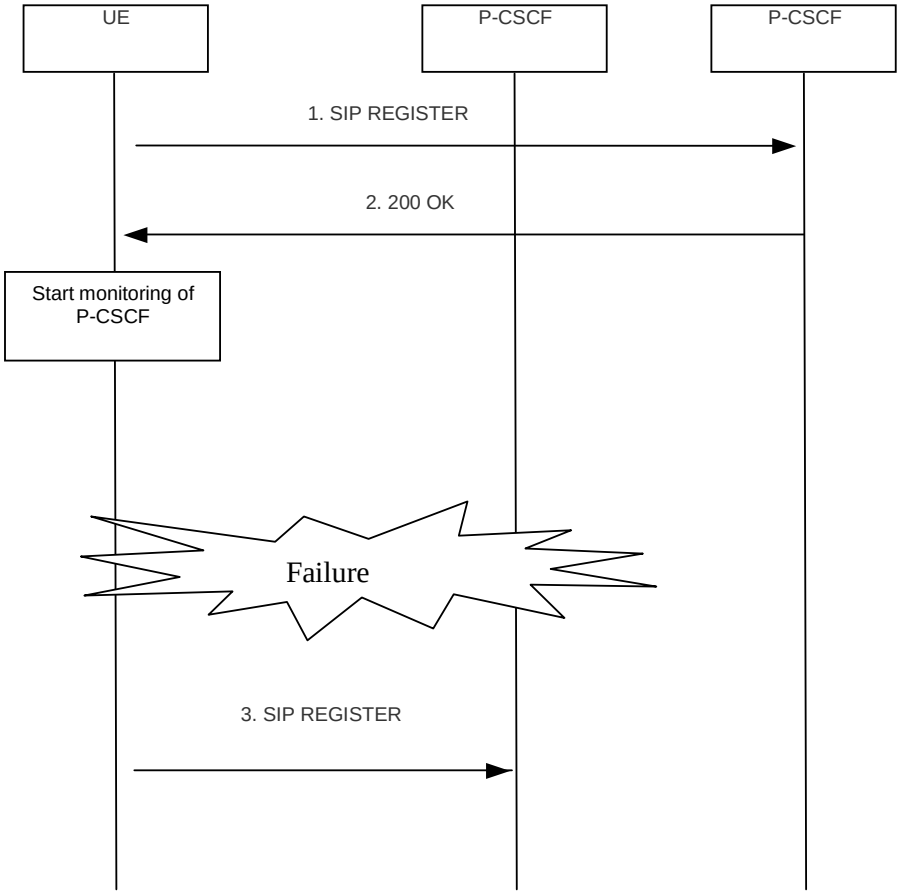

Figure 5.3a: P-CSCF failure detected by UE

1. After establishment of an IP-CAN session and acquiring P-CSCF addresses, the UE performs initial registration towards a P-CSCF.

2. If registration is successful, the UE monitors the P-CSCF health according to IETF RFC 6223 [14]

3. When a failure is detected, the UE acquires new P-CSCF addresses (if needed) and performs an initial registration.

5.4 HSS-based P-CSCF restoration

5.4.1 Introduction

The HSS-based P-CSCF restoration is an optional mechanism and applies only when the UE is using 3GPP access technologies.

When supported, this mechanism shall be executed when a terminating request cannot be serviced due to a P-CSCF failure, as long as there are no other registration flows for this terminating UE using an available P-CSCF.

The HSS-based P-CSCF restoration consists of a basic mechanism that makes usage of a path through HSS and MME/SGSN to request the release of the IMS PDN connection to the corresponding UE, as described in subclause 5.4.2; and an optional extension that avoids the IMS PDN deactivation and re-activation, as described in subclause 5.4.3.

5.4.2 Description

5.4.2.1 General

The call flow for the HSS-based P-CSCF restoration mechanism is described in figure 5.4.2.1-1. The nodes included in this call flow shall execute following procedures if they support the HSS-based P-CSCF restoration mechanism.

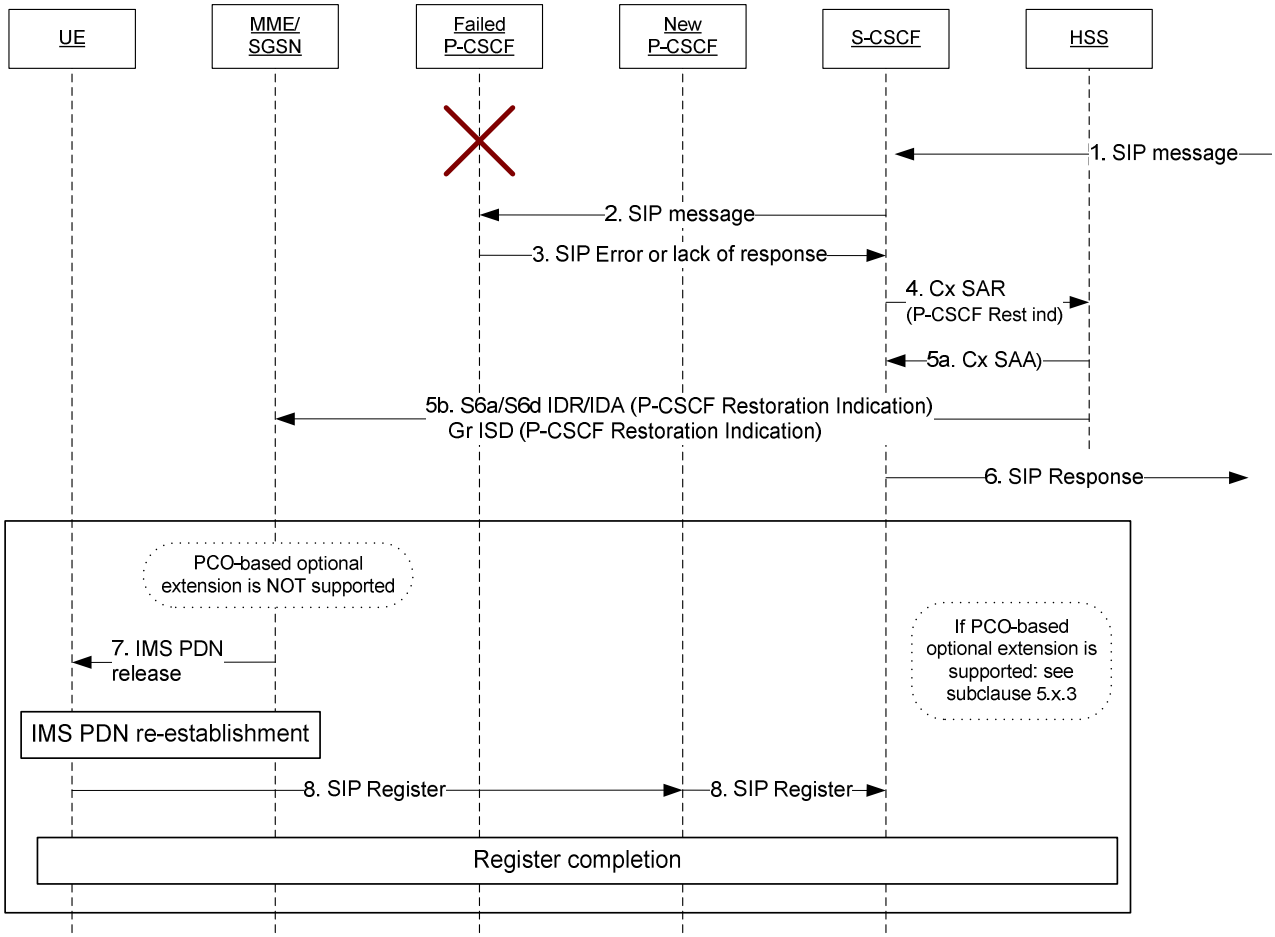

Figure 5.4.2.1-1: HSS-based P-CSCF restoration

1. The terminating S-CSCF receives a SIP message for a destination UE.

2. The S-CSCF forwards the SIP message to this called UE"s terminating P-CSCF.

3. The S-CSCF shall identify whether the called UE"s terminating P-CSCF is not able to process this request, based on received error codes (i.e. the UE registration data is not present) or no response. In this case, if the terminating UE uses a 3GPP access technology, the following steps shall apply to execute the HSS-based P-CSCF restoration. For more information about S-CSCF failure detection, see subclause 5.4.2.2.

4. The S-CSCF shall check the registration status of the Public User Identity associated to the called UE. If the registration state of the Public User Identity is Registered, the S-CSCF shall check if the Public User Identity is currently registered with one or more Private User Identities.

   - If the Public User Identity is currently registered with only one Private User Identity, the S-CSCF shall unregister this Public User Identity by sending a Cx SAR to the HSS, including a P-CSCF Restoration indication.

   - If the Public User Identity is currently registered with more than one Private User Identity, the S-CSCF shall send a deregistration request to the HSS for the corresponding Public User Identity and Private User Identity pair via Cx SAR, including a P-CSCF Restoration indication.

5. The HSS shall identify whether the MME/SGSN supports HSS-based P-CSCF restoration based on feature support information provided by the MME/SGSN as described in subclause 5.4.2.3, then when the HSS receives a Cx SAR with a P-CSCF Restoration indication, it shall check whether the serving node(s) for corresponding user support this feature:

   - if at least one of the serving nodes support the feature:

     - the HSS shall send a P-CSCF restoration indication to the supporting serving node(s) where the IMSI associated to the received Private Identity is registered, i.e. SGSN and/or MME, using S6a/S6d IDR/IDA or Gr ISD request/answer; and

     - the HSS shall perform either the unregistration or deregistration requested and it shall send a successful response to the S-CSCF via Cx SAA. The S-CSCF shall set respectively this Public User Identity as Unregistered or this UE as not registered.

   - otherwise, the HSS shall provide an error response back in Cx SAA to the S-CSCF.

NOTE 1: In case there is not homogeneous support of this feature in corresponding user serving nodes, the P-CSCF Restoration procedure may be triggered as long as one serving node supports this feature, but if the UE is only reachable in the non-supporting serving node, the restoration procedure is not successful.

6. The S-CSCF shall send a SIP response back to the originating side. This shall be an error response if only one Private User Identity is registered, since the S-CSCF is not able to progress the request; otherwise the S-CSCF shall select the best possible response following normal forking procedures.

   Subject to an operator policy, the error response sent by S-CSCF may in addition inform the originating side that a terminating request reattempt is possible based on timer expiration.

NOTE 2: Steps 4 and 6 above are not required to be in this order, reverse order is also possible.

7. Upon reception of the P-CSCF Restoration indication from the HSS, the MME/SGSN from the received IMSI shall identify if the MM context of the UE exists and if the UE has an IMS PDN connection context. If either the MM context or the IMS PDN connection context does not exist, the MME/SGSN shall discard the P-CSCF Restoration indication without further processing; otherwise the MME/SGSN shall continue as below.

NOTE 3: GSMA PRD IR.65 [21] clause 2.3 recommends one single IMS APN in case of simultaneous usage of VoLTE and RCS.

   The MME/SGSN shall check the UE state:

   - If the UE is in ECM-IDLE state, the MME/SGSN shall page the UE.

   - If the UE is initially in ECM-CONNECTED state or when it gets a response from the UE after paging:

     - If ISR is active, the MME/SGSN shall send a message, via the S3 interface, to stop paging the UE at the other ISR-associated node; and

- The MME/SGSN shall execute the optional PCO-based optional extension to this mechanism as described in subclause 5.4.3, if this optional extension is supported by the MME/SGSN and by the serving SGW/PGW; otherwise it shall proceed as below.

NOTE 4: The support of this feature by the serving SGW/PGW is determined based on the local configuration at the MME/SGSN.

- The SGSN, or the MME if this is not the last PDN connection of the UE, shall release the UE"s IMS PDN connection towards the UE by initiating a PDN disconnection procedure with the NAS cause "reactivation requested". If this is the last PDN connection of the UE, the MME shall initiate a detach procedure with the NAS cause code "reactivation requested". Additionally, the MME/SGSN shall also release the same PDN connection towards the SGW/PGW by sending Delete Session message (not shown in the figure).

8. As a result of the release of the IMS PDN connection, the UE shall activate the IMS PDN connection, select an available P-CSCF and perform a new initial IMS registration, as per 3GPP TS 29.061 [9].

5.4.2.2 P-CSCF restart/failure detection by S-CSCF

5.4.2.2.1 General

If the P-CSCF is not reachable, the S-CSCF does not receive any SIP response when it sends a request. In this case, the S-CSCF shall consider the P-CSCF to be non-reachable. As long as the S-CSCF considers the P-CSCF to be non-reachable, the S-CSCF shall not try to contact again this P-CSCF for subsequent terminating requests. The S-CSCF shall consider the P-CSCF to be reachable as soon as a SIP request, including REGISTER, is received from that P-CSCF.

Various mechanisms can be used for the S-CSCF to detect a non-reachable P-CSCF, e.g. keep-alive mechanisms or expiry of timers.

If the P-CSCF is reachable, but it is not able to process the request, it shall send an error indication to the S-CSCF.

5.4.2.2.2 Direct connection from S-CSCF to P-CSCF

This is the normal case when the terminating user is not roaming.

When the S-CSCF receives a terminating request towards a UE registered to a P-CSCF that is not considered non-reachable, the S-CSCF shall forward the request to the P-CSCF. If the P-CSCF does not respond, after a pre-defined number of retransmissions, the S-CSCF shall consider the P-CSCF to be non-reachable.

5.4.2.2.3 S-CSCF connection to P-CSCF via IBCF/ATCF

This is the normal case when the terminating user is roaming and there are IBCFs between the S-CSCF and the P-CSCF. It can also be that an ATCF is inserted between the S-CSCF and the P-CSCF.

In this case, the SIP node closest to the P-CSCF shall identify when the P-CSCF is not reachable. It rejects the request with a SIP error response with an indication that the P-CSCF is not reachable.

5.4.2.3 MME/SGSN mechanism support

If the MME/SGSN supports this mechanism, it shall indicate support of this feature to the HSS in S6a/S6d ULR. If support is indicated, this information shall be stored by HSS per MME/SGSN.

5.4.3 PCO-based optional extension

5.4.3.1 Introduction

The HSS-based P-CSCF basic mechanism is optionally extended by reusing part of the "Update PDP context/bearer at P-CSCF failure" mechanism described in subclause 5.1, in order to avoid the need to deactivate and reactivate the IMS PDN connection.

This extension is based on the possibility for the P-GW/GGSN to know whether or not the UE supports the "Update PDP context/bearer at P-CSCF failure" mechanism. This is described in subclause 5.4.3.3.

5.4.3.2 Description

This procedure is described by figure 5.4.3.2-1 (for EPC) and 5.4.3.2-2 (for GPRS). The nodes included in this call flow shall execute following procedures if they support the HSS-based P-CSCF restoration mechanism.

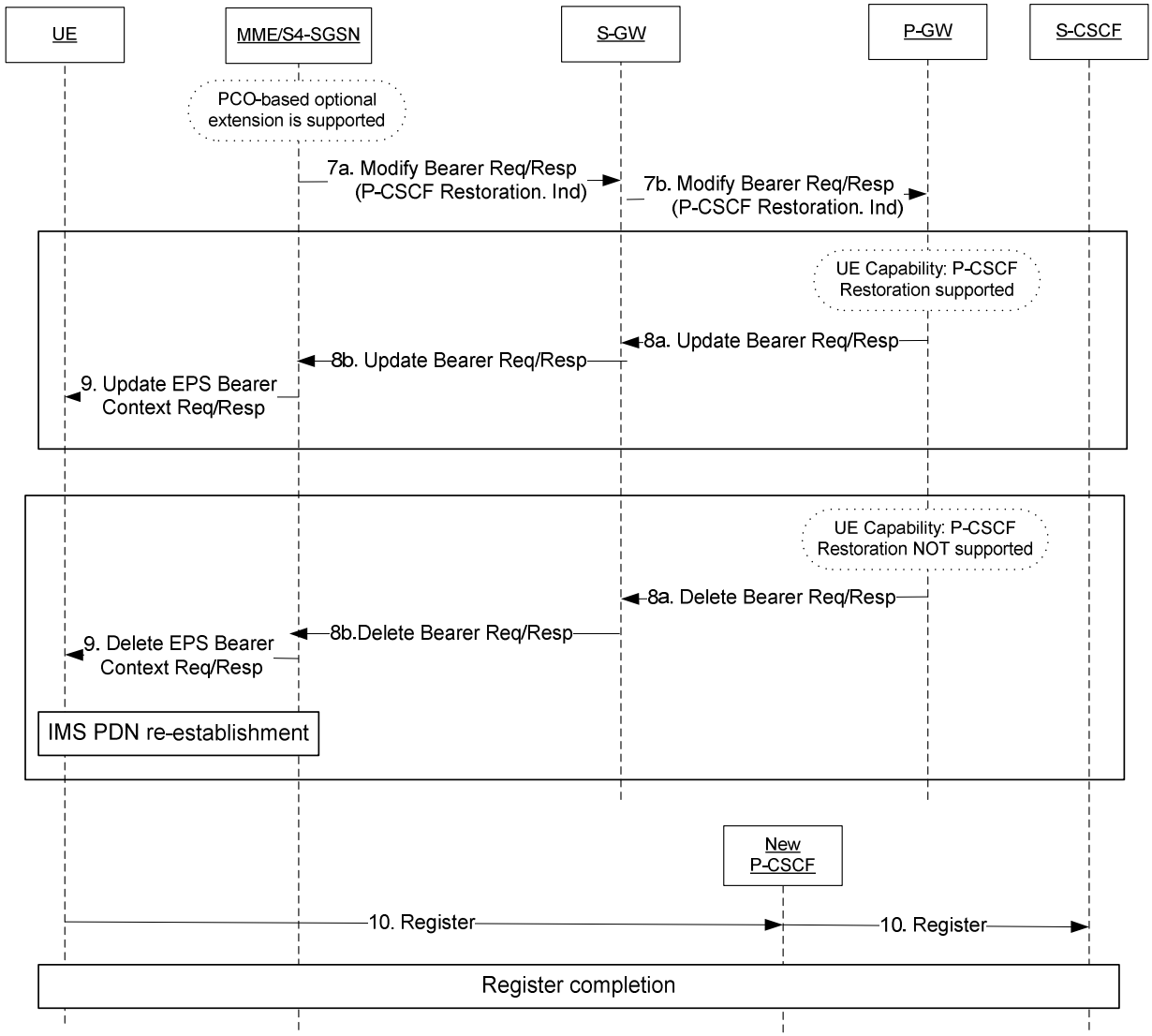

Figure 5.4.3.2-1: PCO-based optional extension - EPC

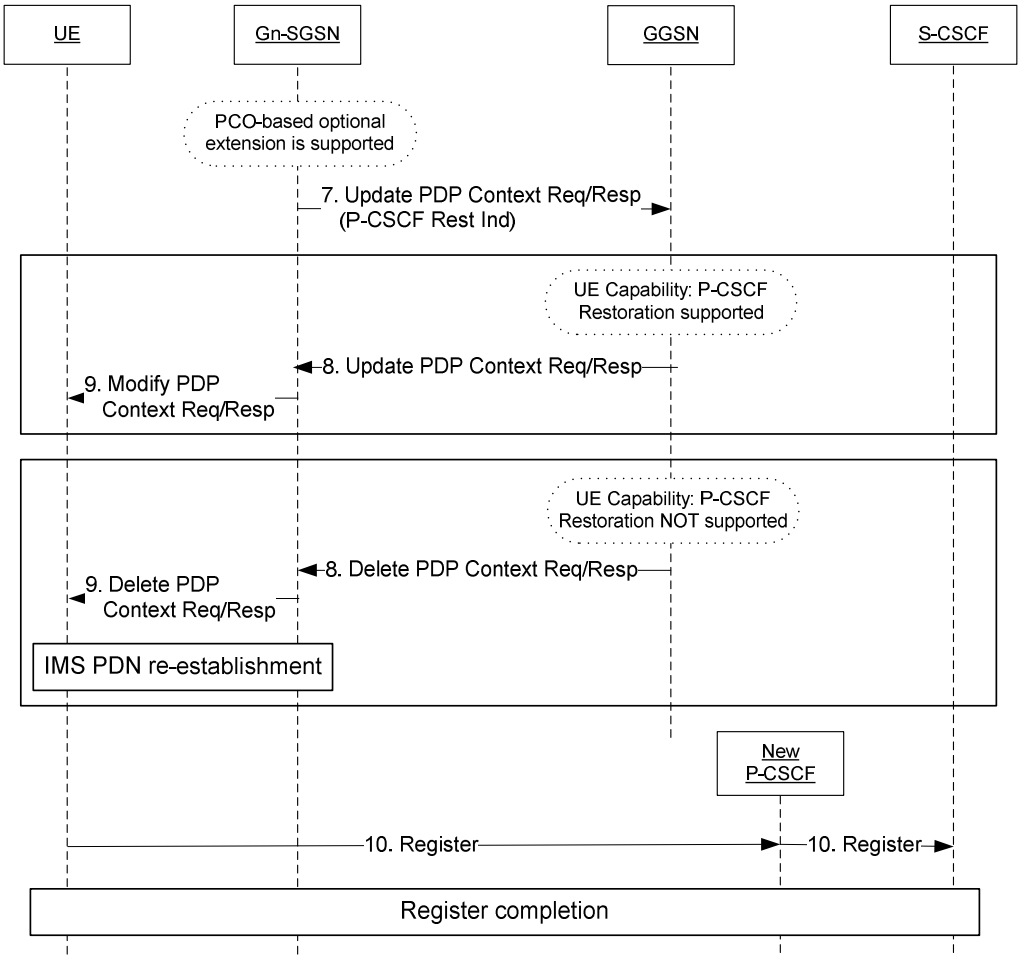

Figure 5.4.3.2-2: PCO-based optional extension - GPRS

Steps from 1 to 6 are the same as explained in figure 5.4.2.1-1 above.

7. The MME/SGSN shall send Modify Bearer Request / Update PDP Context Request to the P-GW/GGSN for this associated PDN connection with a P-CSCF Restoration indication.

   The MME/S4 SGSN shall provide this indication to the P-GW via the S-GW. When the Modify Bearer Request is received by the S-GW with the P-CSCF Restoration indication, this message shall be forwarded to the P-GW.

8. Upon reception of the P-CSCF Restoration indication, the P-GW/GGSN shall check whether the UE has indicated it supports 'Update PDP context/bearer at P-CSCF failure" mechanism, as described in subclause 5.4.4.3:

   - if supported, the PGW/GGSN shall send Update Bearer Request / Update PDP Context Request to the MME/SGSN with the list of available P-CSCF addresses within PCO IE to update destination UE. The list of available P-CSCFs may contain the address of the P-CSCF used by the UE if this P-CSCF has restarted and is again available.

   - if not supported, the P-GW/GGSN shall release the IMS PDN connection/PDP context by sending a Delete Bearer Request / Delete PDP Context Request to the MME/SGSN with GTP cause "reactivation requested".

9. Upon reception of the Update Bearer Request / Update PDP Context Request, the MME/SGSN shall send an Update EPS Bearer Context Request / Modify PDP Context Request to the UE, including the PCO with the list

of available P-CSCF addresses; otherwise, upon reception of a Delete Bearer Request / Delete PDP Context Request, the MME/SGSN shall send a Delete EPS Bearer Context Request / Delete PDP Context Request to the UE with the NAS cause "reactivation requested", then once the PDN connection is released, the UE shall re-activate the IMS PDN connection.

10. The UE selects an available P-CSCF. If the UE has received a Modify EPS Bearer Context Request / Modify PDP Context Request, the UE shall select one available P-CSCF from the list for IMS registration and perform a new initial IMS registration.

5.4.4.3 UE indication of support for "Update PDP context/bearer at P-CSCF failure" Restoration

This optional extension is based on the possibility for the P-GW/GGSN to identify whether or not the UE supports "Update PDP context/bearer at P-CSCF failure", as described in subclause 5.1 and 3GPP TS 24.229 [19] (subclauses B.2.2.1C and L.2.2.1C).

The UE shall indicate this capability to the P-GW/GGSN at the activation of the IMS PDN connection /PDP context, in a PCO parameter as described in 3GPP TS 24.008 [4] subclause 10.5.6.3. The P-GW/GGSN shall store this UE capability.

This method has no impact on the MME/SGSN or SGW, as PCO information is transparently transferred through these network elements.

5.4.5 Coexistence with "Update PDP context/bearer at P-CSCF failure" mechanism

If the "Update PDP context/bearer at P-CSCF failure" mechanism is deployed, as soon as a P-CSCF failure is detected, as described in subclause 5.1, it triggers massive radio signalling first and then massive IMS registration. Therefore, the HSS-based P-CSCF restoration triggering use case does not occur in most cases, and benefits are minimal; i.e., in case of coexistence, the "Update PDP context/bearer at P-CSCF failure" mechanism takes precedence over the HSS-based P-CSCF restoration mechanism in most cases. Hence, if the optional HSS-based P-CSCF restoration is deployed in a network, the recommendation is to only deploy the HSS-based P-CSCF restoration.

5.4.6 HSS based P-CSCF restoration in roaming scenarios

The considered roaming scenarios are the ones described in 3GPP TS 23.401 [17], clause 4.2.2.

For these roaming scenarios, when the VPLMN and the HPLMN both support the HSS based P-CSCF restoration mechanism, this mechanism shall be used for P-CSCF restoration. The HPLMN shall be aware that the VPLMN supports the HSS based P-CSCF restoration mechanism by signalling from the VPLMN. The HPLMN should not trigger a P-CSCF restoration otherwise.

For the roaming scenarios when either the VPLMN or the HPLMN does not support the HSS based P-CSCF restoration mechanism, then the PGW/GGSN which is located in network supporting the HSS based mechanism, depending on operator policy, may apply:

- no P-CSCF restoration mechanism; or
- another existing mechanism e.g. the "Update PDP context/bearer at P-CSCF failure" mechanism described in subclause 5.1. The PGW/GGSN shall be aware (e.g. by local configuration) that the HSS based P-CSCF restoration mechanism cannot be used.

NOTE: The PGW/GGSN identifies the roaming or non-roaming scenario based on the serving PLMN-ID and IMSI received from the MME/SGSN at the PDN connection establishment.

5.5 PCRF-based P-CSCF restoration

5.5.1 Introduction

The PCRF-based P-CSCF restoration is an optional mechanism.

This mechanism is executed when a terminating request does not proceed due to a P-CSCF failure, as long as there are no other registration flows for this terminating UE using an available P-CSCF.

The PCRF-based P-CSCF restoration consists of a basic mechanism that makes usage of a path through an alternative P-CSCF and PCRF to request the release of the IMS PDN connection to the corresponding UE, as described in clause 5.5.2; and an optional extension that avoids the IMS PDN deactivation and re-activation, as described in clause 5.5.3.

5.5.2 PCRF-based P-CSCF restoration information flow - deactivate PDN connection/PDP context

The following figures illustrate the details of PCRF-based P-CSCF restoration information flow.

The nodes included in this call flow shall execute following procedures if they support the PCRF-based P-CSCF restoration mechanism.

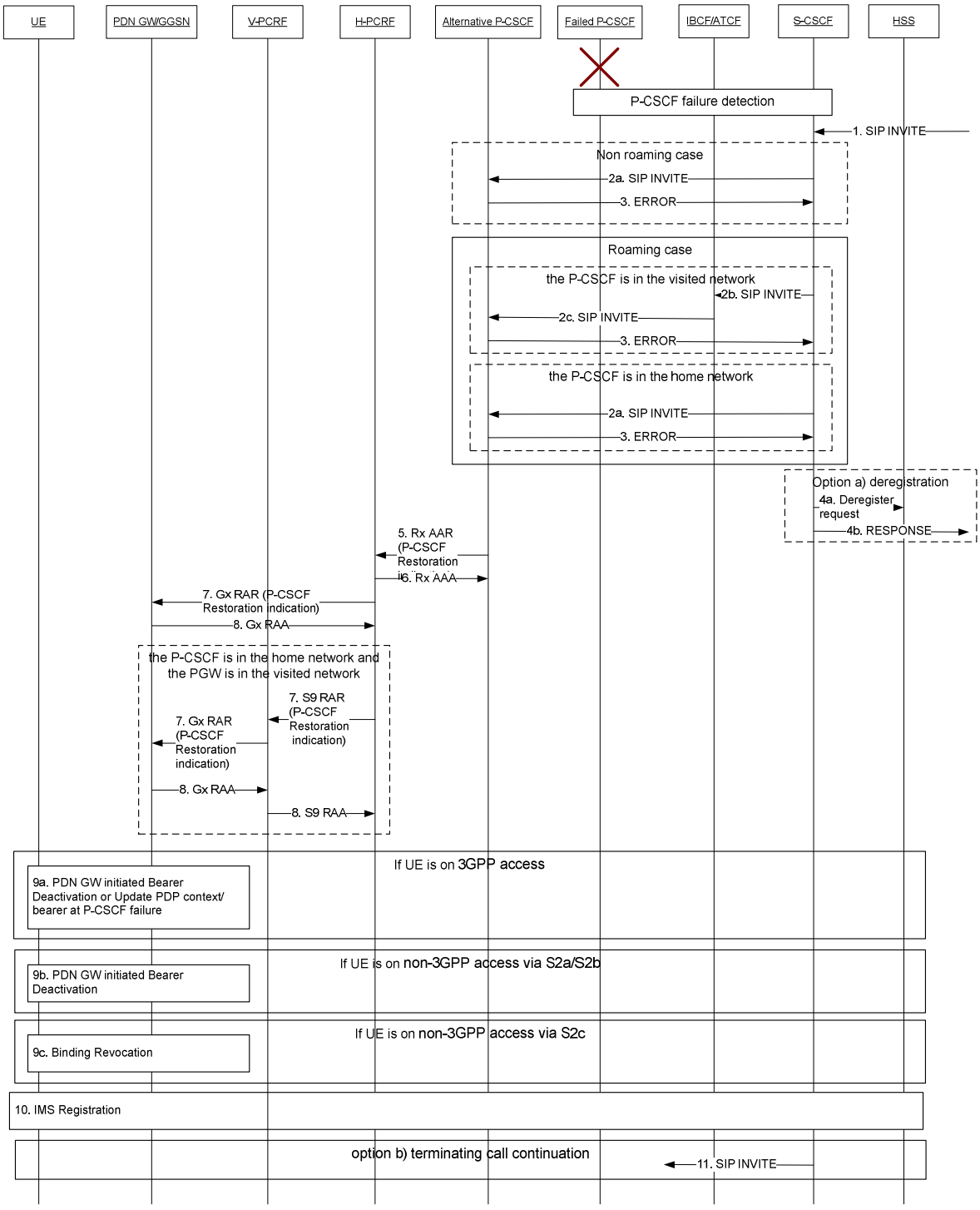

Figure 5.5.2-1: PCRF based P-CSCF restoration

This call flow provides two options for termination call being treated.

Option a) makes terminating UE to be deregistered until next re-registration.

Option b) continues terminating call after successful re-IMS registration.

1. The S-CSCF receives a terminating INVITE message.

2a. The S-CSCF shall populate IMSI into the terminating INVITE message. IMSI is maintained in the S-CSCF, which is obtained from HSS when the UE registers. Then the S-CSCF shall forward the Terminating INVITE message to alternative P-CSCF. The alternative P-CSCF is chosen by local configuration.

NOTE 1: The IMSI is used by the alternative P-CSCF to find the associated PCRF associated for the UE. The IMSI information is subtracted in P-CSCF.

2b. The S-CSCF shall populate IMSI into the terminating INVITE message. IMSI is maintained in the S-CSCF, which is obtained from HSS when the UE registers. Then the S-CSCF shall forward the terminating INVITE message to visited network.

2c. If IBCF or ATCF next to the failed P-CSCF has detected the P-CSCF failure, IBCF or ATCF shall forward the terminating INVITE message to alternative P-CSCF. The alternative P-CSCF is chosen by local configuration.

3. The alternative P-CSCF shall send SIP ERROR message to the S-CSCF.

4a. If option a) is chosen, the S-CSCF shall check the registration status of the Public User Identity associated to the called UE. If the registration state of the Public User Identity is registered, the S-CSCF shall check if the Public User Identity is currently registered with one or more Private User Identities.

- If the Public User Identity is currently registered with only one Private User Identity, the S-CSCF shall unregister this Public User Identity sending a Cx SAR/SAA to HSS. If the response is successful, the S-CSCF shall set this Public User Identity as Unregistered.

- If the Public User Identity is currently registered with more than one Private User Identity, the S-CSCF shall send a deregistration to HSS for the corresponding Public User Identity and Private User Identity pair via Cx SAR/SAA. If the response is successful, the S-CSCF shall set this UE as not registered.

4b. If option a) is chosen the S-CSCF shall send a SIP response back to the originating side. This shall be an error response if only one Private User Identity is registered; otherwise the S-CSCF shall select the best possible response following normal forking procedures.

5. The alternative P-CSCF shall send an Rx AAR message with the P-CSCF restoration indication to the associated PCRF, the associated PCRF is found by UE"s IP address (if available), IP Domain (if UE"s IP address is provided and IP address overlapping can occur), IMSI and APN. The APN and IP Domain are set based on local configuration and additionally referring to the SDP information, e.g. media field, on the received SIP INVITE message.

NOTE 2: When the UE"s IP address is not available, the P-CSCF has to include both IMSI and APN in the Rx AAR command.

NOTE 3: When IMSI is not available, the associated PCRF for the UE can be found by IP address of the UE with the condition that there is no IP translation function in the P-CSCF.

6. The PCRF shall send an Rx AAA to the P-CSCF

7. The PCRF shall find the IP-CAN session related to that UE based on the available information received in step 5 and shall send a Gx RAR including the P-CSCF restoration indication to the PDN GW/GGSN that has been associated with that IP-CAN session. In case where the alternative P-CSCF is located in the HPLMN and the associated PDN GW/GGSN is located in the VPLMN, in this case both S9 interface and Gx interface are used.

8. The PDN GW/GGSN shall send Gx RAA to the PCRF.

9. Then the PDN GW/GGSN shall perform one of following procedures.

- For 3GPP accesses, the PDN GW/GGSN initiates bearer deactivation procedure for the default bearer with "reactivation requested", if the PDN GW/GGSN has no knowledge whether the UE supports the "Update PDP context/bearer at P-CSCF failure". If the UE supports the "Update PDP context/bearer at P-CSCF failure" mechanism, step 11 and 12 in the procedure that is described in clause 5.1 is reused instead.

- For the S2a and S2b, the PDN GW initiates bearer deactivation procedure to the trusted non 3GPP access domain and the ePDG, respectively.

- For the S2c, the PDN GW/GGSN initiates detach procedure.

NOTE 4: For the S2a/b/c, it should be noted that although this procedure does not request UE to re-attach to the IMS explicitly by signalling, it is assumed that IMS compliant UE shall re-attempt to obtain IMS service soon after detached from the IMS service.

10. UE activates the PDN connection and registers to IMS. As a result of the release of the IMS PDN connection, the voice centric UE activates the IMS PDN connection, selects a new available P-CSCF and performs a new initial IMS registration.

11. If option b) is chosen, the S-CSCF shall send the suspended terminating SIP INVITE message to a newly selected P-CSCF after the successful SIP registration for the UE.

5.5.3 PCO-based optional extension

5.5.3.1 Introduction

The PCRF-based P-CSCF basic mechanism is optionally extended by reusing part of the "Update PDP context/bearer at P-CSCF failure" mechanism described in clause 5.1, in order to avoid the need to deactivate and reactivate the IMS PDN connection.

This extension is based on the possibility for the P-GW/GGSN to know whether or not the UE supports the "Update PDP context/bearer at P-CSCF failure" mechanism. This is described in clause 5.5.3.3.

5.5.3.2 Description

This procedure is described by figure 5.4.3.2-1 (for EPC) starting with step 8a and 5.4.3.2-2 (for GPRS) starting with step 8. The nodes included in this call flow shall execute following procedures if they support the PCRF-based P-CSCF restoration mechanism.

5.5.3.3 UE indication of support for "Update PDP context/bearer at P-CSCF failure" Restoration

This function is identical to the HSS-based P-CSCF restoration. Refer to 5.4.4.3.

5.5.4 Coexistence with "Update PDP context/bearer at P-CSCF failure" mechanism

If the "Update PDP context/bearer at P-CSCF failure" mechanism is deployed, as soon as a P-CSCF failure is detected, as described in clause 5.1, it triggers massive radio signalling first and then massive IMS registration. Therefore, the PCRF-based P-CSCF restoration triggering use case does not occur in most cases, and benefits are minimal; i.e., in case of coexistence, the "Update PDP context/bearer at P-CSCF failure" mechanism takes precedence over the PCRF-based P-CSCF restoration mechanism in most cases. Hence, if the optional PCRF-based P-CSCF restoration is deployed in a network, the recommendation is to only deploy the PCRF-based P-CSCF restoration.

5.5.5 P-CSCF restoration in roaming scenarios for PCRF based solution

In a home routed scenario, i.e., S-GW(or any other gateway node) is in VPLMN and P-GW and P-CSCF are in HPLMN, the PCRF based solution can work sorely within HPLMN that supports the PCRF based solution, no matter VPLMN supports the solution or not.

The following procedures only apply to the local breakout scenario.

In roaming scenarios, the VPLMN and HPLMN operators may deploy the same or different P-CSCF restoration mechanisms, amongst those described in subclause 5.1 (Update PDP context/bearer at P-CSCF failure), subclause 5.4 (HSS based P-CSCF restoration) and subclause 5.5 (PCRF based P-CSCF restoration), independently from each other.

The PCRF based P-CSCF restoration can work in roaming scenarios if:

1) Both HPLMN and VPLMN support the PCRF based P-CSCF restoration; or

2) When the HPLMN does not support the PCRF based P-CSCF restoration but VPLMN does and NAT is not performed.

NOTE: If the HPLMN does not support the PCRF based P-CSCF restoration, IMSI may not be available on terminating INVITE message.

Alternatively, based on the operator policy or roaming agreement, the VPLMN can use the "Update PDP context/bearer at P-CSCF failure" mechanism described in subclause 5.1.

For a terminating call to outbound roamers, the S-CSCF may not populate IMSI to terminating INVITE message if HPLMN knows, e.g. by configuration in the S-CSCF according to roaming agreements, that VPLMN for outbound roamer does not support the PCRF based P-CSCF restoration.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
	CT#41				V1.0.0 was approved in CT#41	1.0.0	8.0.0
2008-12	CT#42	CP-080698	0003	-	Re-selection of S-CSCF at de-registration	8.0.0	8.1.0
		CP-080698	0004	1	Subscription to registration information recover		
		CP-080963	0007	3	AS originating procedures		
		CP-080698	0008	-	Multiple contacts restoration at re-registration		
		CP-080698	0009	1	Multiple contacts restoration at de-registration		
2009-03	CT#43	CP-090026	0010	-	Multiple Registrations in De-Registration	8.1.0	8.2.0
			0011	-	Multiple Registrations in Registration		
2009-06	CT#44	CP-090303	0019	-	Contact storage in reg event subscription	8.2.0	8.3.0
2009-12	CT#46	CP-090796	0020	1	P-CSCF restoration procedures: stage 2	8.3.0	9.0.0
2010-03	CT#47	CP-100045	0022	1	P-CSCF failure indication removal	9.0.0	9.1.0
			0023	1	P-CSCF failure handling for DHCP based scenarios		
			0024	1	P-CSCF monitoring performed by UE		
			0025	1	S9 interface procedures		
2010-06	CT#48	CP-100285	0027	-	Notification is to be sent to all UEs sharing the IMPU	9.1.0	9.2.0
2010-09	CT#49	CP-100462	0030	1	Restoration Data Backup	9.2.0	9.3.0
2011-03				-	Update to Rel-10 version (MCC)	9.3.0	10.0.0
2011-06	CT#52	CP-110356	0033	-	Emergency Restoration	10.0.0	10.1.0
2012-09	CT#57	CP-120440	0040	1	Emergency registrations do not affect registration status	10.1.0	10.2.0
2012-09	CT#57	CP-120458	0037	1	P-CSCF failure procedure with S5 PMIP	10.2.0	11.0.0
		CP-120458	0041	1	Reference list correction to align with the corrected TS 29.212 title		
2012-12	CT#58	CP-120745	0042	1	Alignment on the Network recovery procedure at P-CSCF failure	11.0.0	11.1.0
		CP-120743	0046	1	PSI direct routing with restoration procedures		
2013-12	CT#62	CP-130609	0047	1	Correction of reference to Update Notifications for Proxy Mobile IPv6	11.1.0	11.2.0
2014-03	CT#63	CP-140017	0051	1	Update the reference of draft-ietf-sipcore-keep-01 to RFC 6223	11.2.0	11.3.0
2014-03	CT#63	CP-140020	0048	1	Update the reference of IETF draft Update Notifications for Proxy Mobile IPv6 to RFC 7077	11.2.0	11.3.0
2014-09	CT#65	CP-140515	0053	1	T-GRUU restoration	11.3.0	12.0.0
		CP-140506	0054	3	HSS-based P-CSCF restoration		
		CP-140506	0055	2	P-CSCF restoration in roaming scenarios for the HSS based mechanism		
		CP-140506	0056	5	PCRF based P-CSCF restoration		
		CP-140506	0057	3	P-CSCF restoration in roaming scenarios for PCRF based solution		

2014-12	CT#66	CP-140794	0059	1	HSS-based P-CSCF restoration, ISR implications	12.0.0	12.1.0
			0060	3	HSS-based P-CSCF restoration, MME/SGSN lack of support		
			0061	1	HSS-based P-CSCF restoration, response back to UE with retry option		
			0062	2	P-CSCF Restoration for single IMS APN		
			0065	1	P-CSCF restoration in a roaming scenario that P-GW and P-CSCF are in HPLMN for PCRF based solution		
			0066	1	A correction in figure of PCRF based P-CSCF restoration		
			0069	2	P-CSCF Restart		
			0070	-	Addition of P-CSCF restoration in the scope		
			0071	2	P-CSCF as non-reachable clarification		

History

Document history		
V12.0.0	October 2014	Publication
V12.1.0	January 2015	Publication