ETSI TS 128 204 V18.1.1 (2024-08)

TECHNICAL SPECIFICATION

5G; Charging management; Network slice-specific authentication and authorization charging in the 5G System (5GS) (3GPP TS 28.204 version 18.1.1 Release 18)

Reference

RTS/TSGS-0528204vi11

Keywords

5G

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Intellectual Property Rights

Essential patents

Trademarks

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**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

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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not	indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is	(or any other verb in the indicative mood) indicates a statement of fact
is not	(or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies the Converged Charging description for network slice-specific authentication and authorization charging in the 5G System (5GS) based on Network Slice-Specific Authentication and Authorization Function (NSSAAF) of 5GS architecture and procedures specified in 3GPP TS 23.501 [3] and 3GPP TS 23.502 [4].

The scope is the Network Slice-Specific Authentication and Authorization as specified in TS 23.502 [4] with a AAA Server (AAA-S).

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 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[3] 3GPP TS 23.501: "System Architecture for the 5G System (5GS); Stage 2".

[4] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[5] 3GPP TS 32.256: "Telecommunication management; Charging management; 5G connection and mobility domain charging; stage 2".

[6] 3GPP TS 32.290: "Telecommunication management; Charging management; 5G system; Services, operations and procedures of charging using Service Based Interface (SBI)".

[7] 3GPP TS 32.291: "Telecommunication management; Charging management; 5G system; Charging service, stage 3".

[8] 3GPP TS 32.298: "Telecommunication management; Charging management; Charging Data Record (CDR) parameter description".

[9] 3GPP TS 32.295: "Telecommunication management; Charging management; Charging Data Record (CDR) transfer".

[10] 3GPP TS 32.297: "Telecommunication management; Charging management; Charging Data Record (CDR) file format and transfer".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP 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 3GPP TR 21.905 [1].

5G System: 3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE.

Network Slice: A logical network that provides specific network capabilities and network characteristics.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Bnssaa	Reference point for the CDR file transfer from the NSSAAF CGF to the BD
Ga	Reference point for CDR transfer between a CDF and the CGF
Nchf	Service based interface exhibited by CHF
N103	Reference point between NSSAAF and the CHF

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

3GPP	3rd Generation Partnership Project
5GS	5G System
AAA	Authentication Authorization Accounting
AAA-S	AAA Server
AMF	Access and Mobility Management Function
CDR	Charging Data Record
CGF	Charging Gateway Function
CHF	CHarging Function
EAP	Extensible Authentication Protocol
ECUR	Event Charging with Unit Reservation
GPSI	Generic Public Subscription Identifier
IEC	Immediate Event Charging
NSSAA	Network Slice-Specific Authentication and Authorization
NSSAAF	Network Slice-Specific Authentication and Authorization Function
PDU	Protocol Data Unit
PEC	Post Event Charging
S-NSSAI	Single Network Slice Selection Assistance Information
SUPI	Subscription Permanent Identifier
UE	User Equipment

4 Architecture considerations

4.1 High-level 5G System architecture

4.1.1 Non-roaming reference architecture

Figure 4.1.1-1 shows the Non-roaming 5G System high level architecture in the service-based representation, as defined in 3GPP TS 23.501 [3], with Network Slice-Specific Authentication and Authorization (NSSAAF):

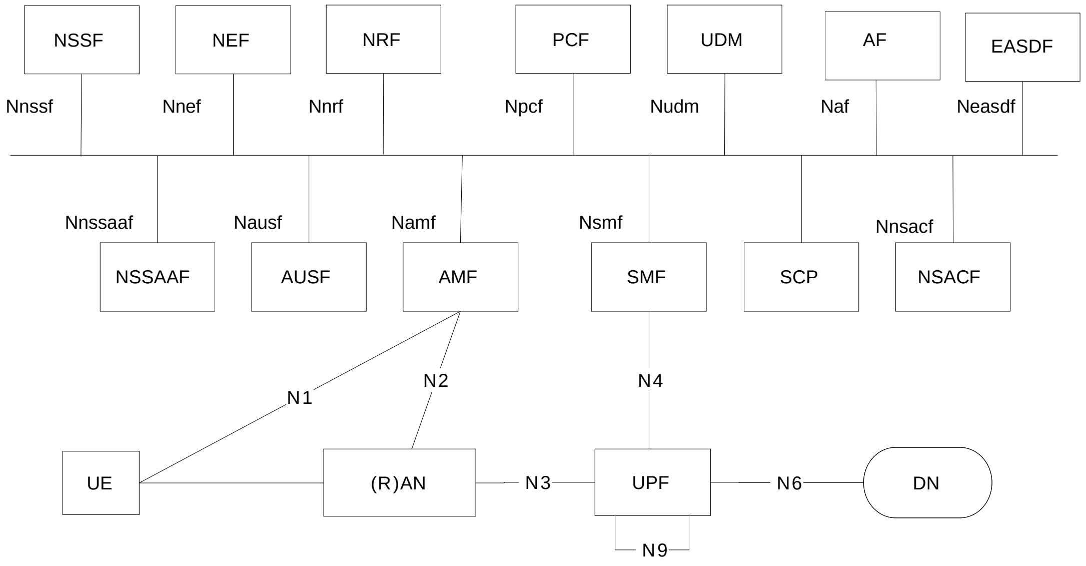

Figure 4.1.1-1: Non-Roaming 5G System architecture

4.2 Network Slice-Specific Authentication and Authorization converged charging architecture

4.2.1 Non-roaming

Architectural options for Network Slice-Specific Authentication and Authorization converged charging in service-based representation are depicted in figure 4.2.1-1.

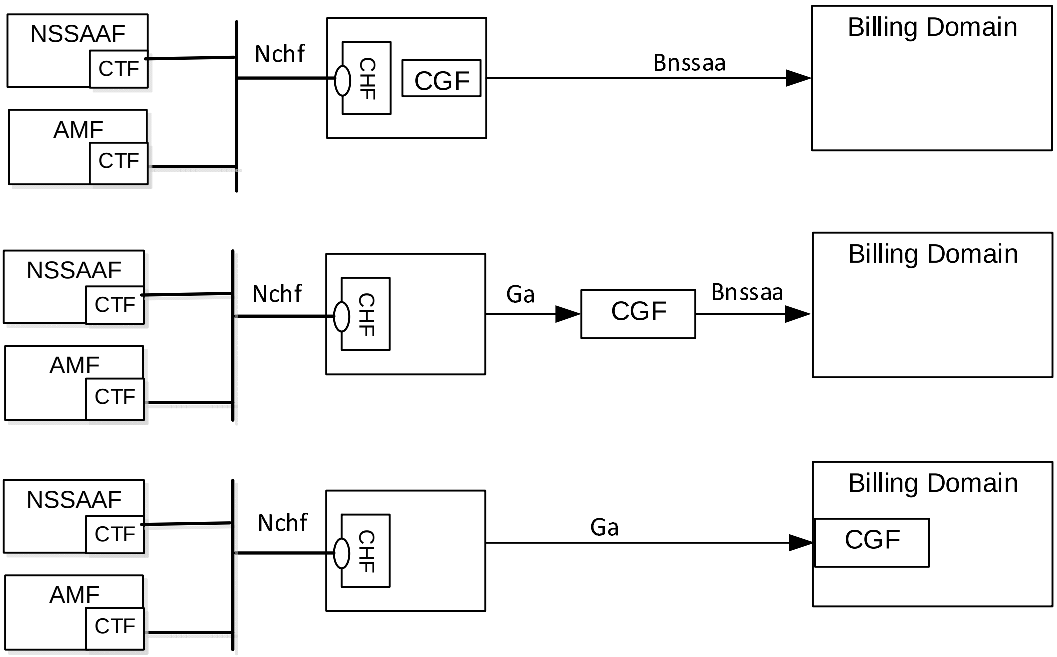

Figure 4.2.1-1: Non-Roaming Network Slice-Specific Authentication and Authorization converged charging architecture

Architectural options of figure 4.2.1-1 apply to any Network Slice-Specific Authentication and Authorization converged charging architecture of this clause.

AMF is part of this architecture for the purpose of Network Slice-Specific Authentication and Authorization converged charging. For AMF 5G connection and mobility converged charging see TS 32.256 [5].

Details on the interfaces and functions can be found in 3GPP TS 32.240 [2] for the general architecture components, Ga is described in clause W and Bnssaa in clause Z of this document, and Nchf is described in 3GPP TS 32.290 [6].

Figure 4.2.1-2 shows the Network Slice-Specific Authentication and Authorization converged charging architecture in reference point representation for non-roaming:

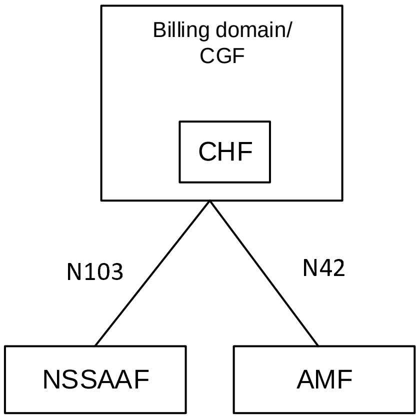

Figure 4.2.1-2: Non-Roaming Network Slice-Specific Authentication and Authorization converged charging architecture - reference point representation

5 Network Slice-Specific Authentication and Authorization charging principles and scenarios

5.1 Network Slice-Specific Authentication and Authorization charging principles

5.1.1 General

The charging functions specified for Network Slice-Specific Authentication and Authorization charging, are based on Network Slice-Specific Authentication and Authorization with a AAA Server (AAA-S) functionality as specified in TS 23.501 [3], supported by:

- NSSAAF; and
- optionally AMF.

The network slice is identified by a S-NSSAI.

For AMF the present specification only covers Network Slice-Specific Authentication and Authorization charging. For AMF 5G connection and mobility charging see TS 32.256 [5].

5.1.2 Requirements

The following are high-level charging requirements specific to Network Slice-Specific Authentication and Authorization charging:

- The NSSAAF shall support converged charging using service based interface.
- The NSSAAF shall support converged charging for Network Slice-Specific Authentication and Authorization procedure per S-NSSAI per UE.
- The AMF shall support converged charging for Network Slice-Specific Authentication and Authorization procedure per S-NSSAI per UE.

5.1.3 Charging information

The charging information for Network Slice-Specific Authentication and Authorization charging are:

- GPSI;
- SUPI;
- S-NSSAI;
- AAA-S address.

5.1.4 CHF selection

The CHF selection by the NSSAAF is based on the following options and with this priority order (highest to lowest):

- NRF based discovery;
- pre-configured CHF address(s).

The CHF selection by the AMF for the purpose of Network slice-specific authentication and authorization charging is based on the following options and with this priority order (highest to lowest):

- NRF based discovery;
- pre-configured CHF address(s).

5.2 Network Slice-Specific Authentication and Authorization charging converged charging scenarios

5.2.1 Basic principles

5.2.1.1 General

Network Slice-Specific Authentication and Authorization converged charging, may be performed by the NSSAAF and AMF interacting with the Charging Function (CHF) using Nchf specified in 3GPP TS 32.290 [6] and 3GPP TS 32.291 [7]. In order to provide the data required for the management activities outlined in 3GPP TS 32.240 [2], the NSSAAF and AMF shall be able to perform converged charging for each of the following:

- Charging information related to Network Slice-Specific Authentication and Authorization procedure per UE per S-NSSAI.
- Charging information related to the "AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization" procedure per UE per S-NSSAI.
- Charging information related to the "AAA Server triggered Network Slice-Specific Authorization Revocation" procedure per UE per S-NSSAI.

The NSSAAF and AMF shall be able to perform converged charging by interacting with the CHF, for charging data related to Network Slice-Specific Authentication and Authorization, AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization and AAA Server triggered Slice-Specific Authorization Revocation procedures.

The Charging Data Request and Charging Data Response are exchanged between the NSSAAF and the CHF based on IEC, PEC, or ECUR scenarios as specified in TS 32.290 [6]. The Charging Data Request and Charging Data Response are exchanged between the AMF and the CHF, based on PEC scenario. IEC, PEC and ECUR scenarios are specified in TS 32.290 [6].

The Charging Data Request is issued by the NSSAAF towards the CHF, and by the AMF towards the CHF, when certain conditions (chargeable events) are met.

The contents and purpose of each charging event that triggers interaction with CHF, as well as the chargeable events that trigger them, are described in the following clauses.

A detailed formal description of the converged charging parameters defined in the present document is to be found in 3GPP TS 32.291 [7].

A detailed formal description of the CDR parameters defined in the present document is to be found in 3GPP TS 32.298 [8].

5.2.1.2 Applicable Triggers

5.2.1.2.1 General

When a charging event is issued towards the CHF, it includes details such as Subscriber identifier (e.g. SUPI).

Each trigger condition (i.e. chargeable event) defined for the Network Slice-Specific Authentication and Authorization converged charging functionality, is specified with the associated behaviour when they are met.

Table 5.2.1.2.1-1 summarizes the set of default trigger conditions and their category which shall be supported by the NSSAAF when charging is active for the corresponding Network Slice-Specific Authentication and Authorization functionality. For "immediate report" category, the table also provides the corresponding Charging Data Request message sent from NSSAAF towards the CHF.

Table 5.2.1.2.1-1: Default Trigger conditions in NSSAAF

Trigger Conditions	Trigger level	Default category	CHF allowed to change category	CHF allowed to enable and disable	Message when "immediate reporting" category
Network Slice-Specific Authentication and Authorization request	-	Immediate	Not Applicable	Yes	IEC: Charging Data Request [Event] ECUR: Charging Data Request [Initial]
Network Slice-Specific Authentication and Authorization completed	-	Immediate	Not Applicable	Yes	PEC: Charging Data Request [Event] ECUR: Charging Data Request [Termination]
AAA-S Network Slice-Specific Re-auth request	-	Immediate	Not Applicable	Yes	IEC: Charging Data Request [Event] ECUR: Charging Data Request [Initial]
AAA-S Network Slice-Specific Re-auth completed	-	Immediate	Not Applicable	Yes	PEC: Charging Data Request [Event] ECUR: Charging Data Request [Termination]
AAA-S Network Slice-Specific Revocation request	-	Immediate	Not Applicable	Yes	IEC: Charging Data Request [Event] ECUR: Charging Data Request [Initial]
AAA-S Network Slice-Specific Revocation completed	-	Immediate	Not Applicable	Yes	PEC: Charging Data Request [Event] ECUR: Charging Data Request [Termination]

Table 5.2.1.2.1-2 summarizes the set of default trigger conditions and their category which shall be supported by the AMF when charging is active for the corresponding Network Slice-Specific Authentication and Authorization functionality. For "immediate report" category, the table also provides the corresponding Charging Data Request message sent from AMF towards the CHF.

Table 5.2.1.2.1-2: Extended Default Trigger conditions in AMF

Trigger Conditions	Trigger level	Default category	CHF allowed to change category	CHF allowed to enable and disable	Message when "immediate reporting" category
Network Slice-Specific Authentication and Authorization completed	-	Immediate	Not Applicable	Yes	PEC: Charging Data Request [Event]
AAA-S Network Slice-Specific Re-auth Notification	-	Immediate	Not Applicable	Yes	PEC: Charging Data Request [Event]
AAA-S Network Slice-Specific Revocation Notification	-	Immediate	Not Applicable	Yes	PEC: Charging Data Request [Event]

NOTE: If the same triggers are enabled in the NSSAAF and the AMF, the respective CHF CDRs will be associated to the same procedure.

5.2.2 Message flows

5.2.2.1 General

The flows in the present document specify the interaction between the NSSAAF and the CHF and between the AMF and the CHF, for Network slice-specific authentication and authorization converged charging functionality, in different scenarios, based on 3GPP TS 23.501 [3] and 3GPP TS 23.502 [4] procedures and flows.

This interaction is based on Charging Data Request /Response specified in 3GPP TS 32.290 [6], exchanged between the NSSAAF embedding the CTF and the CHF, and between the AMF embedding the CTF and the CHF.

If both NSSAAF and AMF generate CHF CDRs, for the same procedure, they will be the same.

The following scenarios are supported by NSSAAF:

- PEC;
- IEC;
- ECUR.

The PEC scenario is supported by AMF.

As a general principle, the steps in the figures for the message flows below correspond to the steps of figures in 3GPP TS 23.502 [4], which is the reference. The present document specifies the charging specific extension part.

5.2.2.2 Network slice-specific authentication and authorization charging

5.2.2.2.1 General

The subclauses below describe Network slice-specific authentication and authorization charging message flows based on figure 4.2.9.2-1 of 3GPP TS 23.502 [4].

5.2.2.2.2 Network slice-specific authentication and authorization – AMF - PEC

The following figure 5.2.2.2.2-1 describes a Network slice-specific authentication and authorization charging in PEC scenario for AMF:

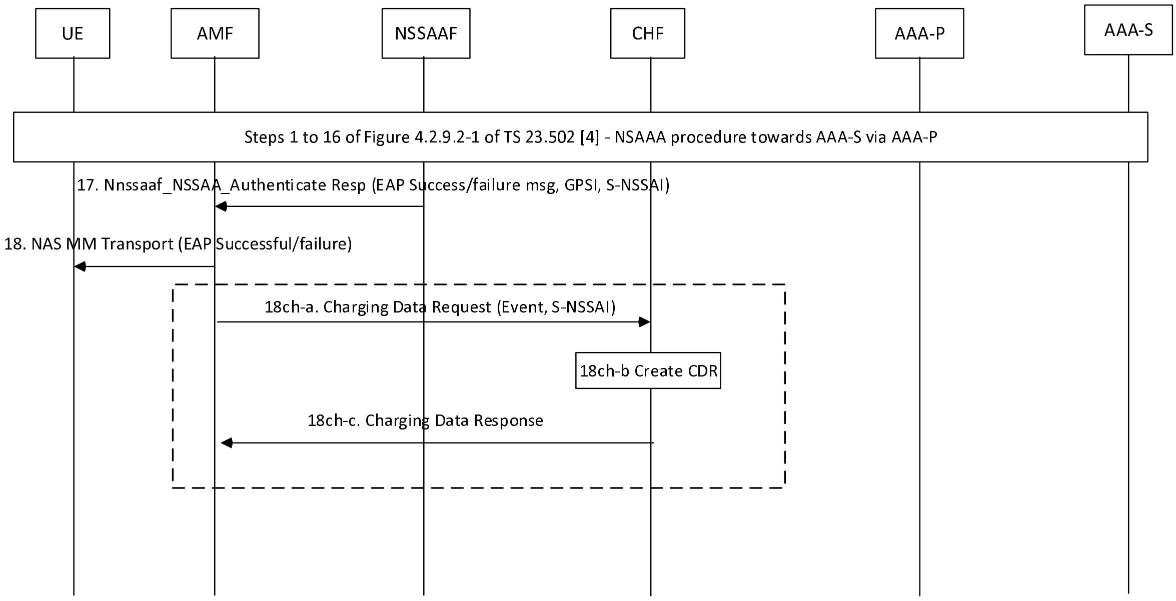
UE
AMF
NSSAAF
CHF
AAA-P
AAA-S
Steps 1 to 16 of Figure 4.2.9.2-1 of TS 23.502 [4] - NSAAA procedure towards AAA-S via AAA-P
17. Nnssaaf_NSSAA_Authenticate Resp (EAP Success/failure msg, GPSI, S-NSSAI)
18. NAS MM Transport (EAP Successful/failure)
18ch-a. Charging Data Request (Event, S-NSSAI)
18ch-b Create CDR
18ch-c. Charging Data Response

Figure 5.2.2.2.2-1: Network slice-specific authentication and authorization – AMF - PEC

Steps 1 to 18: per 3GPP TS 23.502 [4] Figure 4.2.9.2-1 Network Slice-Specific Authentication and Authorization procedure.

18ch-a: NSSAA procedure in AMF completed: AMF sends Charging Data Request [Event] to CHF with EAP-Success/Failure, GPSI and S-NSSAI.

18ch-b: The CHF creates a CDR.

18ch-c: CHF provides response to AMF.

5.2.2.2.3 Network slice-specific authentication and authorization – NSSAAF - PEC

The following figure 5.2.2.2.3-1 describes a Network slice-specific authentication and authorization charging in PEC scenario for NSSAAF:

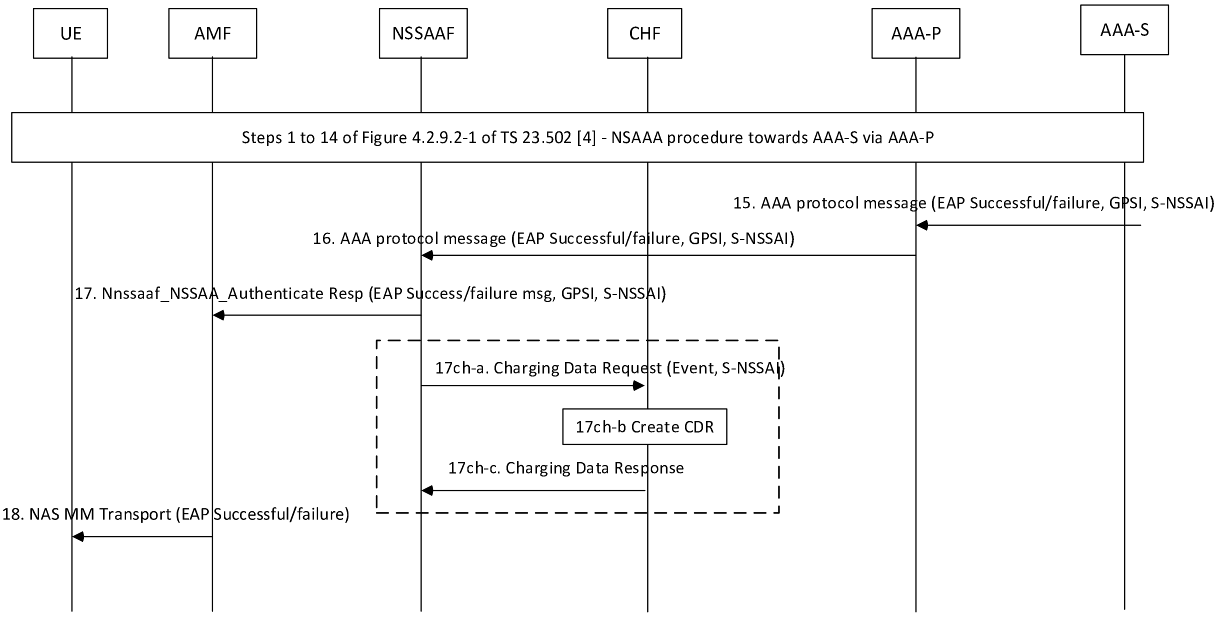
UE
AMF
NSSAAF
CHF
AAA-P
AAA-S
Steps 1 to 14 of Figure 4.2.9.2-1 of TS 23.502 [4] - NSAAA procedure towards AAA-S via AAA-P
15. AAA protocol message (EAP Successful/failure, GPSI, S-NSSAI)
16. AAA protocol message (EAP Successful/failure, GPSI, S-NSSAI)
17. Nnssaaf_NSSAA_Authenticate Resp (EAP Success/failure msg, GPSI, S-NSSAI)
17ch-a. Charging Data Request (Event, S-NSSAI)
17ch-b Create CDR
17ch-c. Charging Data Response
18. NAS MM Transport (EAP Successful/failure)

Figure 5.2.2.2.3-1: Network slice-specific authentication and authorization - PEC

Steps 1 to 17: per 3GPP TS 23.502 [4] Figure 4.2.9.2-1 Network Slice-Specific Authentication and Authorization procedure.

17ch-a: NSSAAF procedure with AAA-S for NSSAA is completed: NSSAAF sends Charging Data Request [Event] to CHF with EAP-Success/Failure, GPSI and S-NSSAI.

17ch-b: The CHF creates a CDR.

17ch-c: CHF provides response to NSSAAF.

Step 18: per 3GPP TS 23.502 [4] Figure 4.2.9.2-1 Network Slice-Specific Authentication and Authorization procedure.

5.2.2.2.4 Network slice-specific authentication and authorization – NSSAAF - IEC

The following figure 5.2.2.2.4-1 describes a Network slice-specific authentication and authorization charging in IEC scenario for NSSAAF :

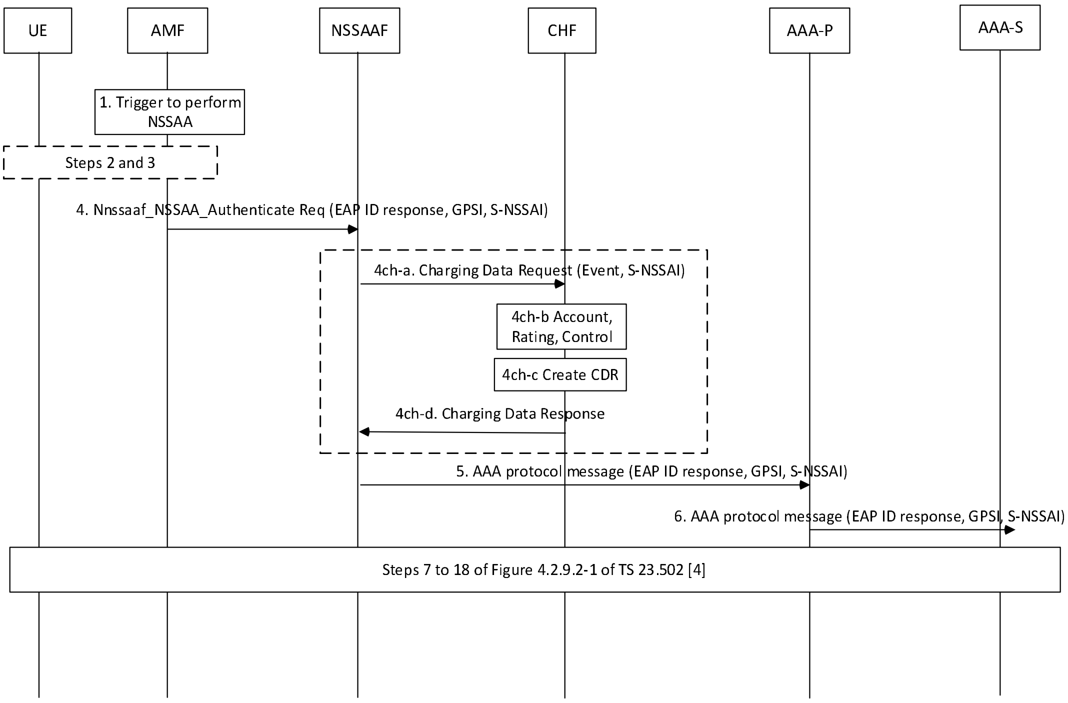
UE
AMF
NSSAAF
CHF
AAA-P
AAA-S
1. Trigger to perform NSSAA
Steps 2 and 3
4. Nnssaaf_NSSAA_Authenticate Req (EAP ID response, GPSI, S-NSSAI)
4ch-a. Charging Data Request (Event, S-NSSAI)
4ch-b Account, Rating, Control
4ch-c Create CDR
4ch-d. Charging Data Response
5. AAA protocol message (EAP ID response, GPSI, S-NSSAI)
6. AAA protocol message (EAP ID response, GPSI, S-NSSAI)
Steps 7 to 18 of Figure 4.2.9.2-1 of TS 23.502 [4]

Figure 5.2.2.2.4-1: Network slice-specific authentication and authorization – NSSAAF - IEC

Steps 1 to 4 per 3GPP TS 23.502 [4] Figure 4.2.9.2-1 Network Slice-Specific Authentication and Authorization procedure, AMF sends the EAP Identity Response to the NSSAAF.

4ch-a: NSSAAF sends Charging Data Request [Event] to CHF with GPSI and S-NSSAI.

4ch-b: Account, Rating, control by the CHF.

4ch-c: The CHF creates a CDR.

4ch-d: CHF provides response to NSSAAF.

Steps 5 to 18 per 3GPP TS 23.502 [4] Figure 4.2.9.2-1 Network Slice-Specific Authentication and Authorization procedure.

5.2.2.2.5 Network slice-specific authentication and authorization – NSSAAF - ECUR

The following figure 5.2.2.2.5-1 describes a Network slice-specific authentication and authorization charging in ECUR scenario for NSSAAF:

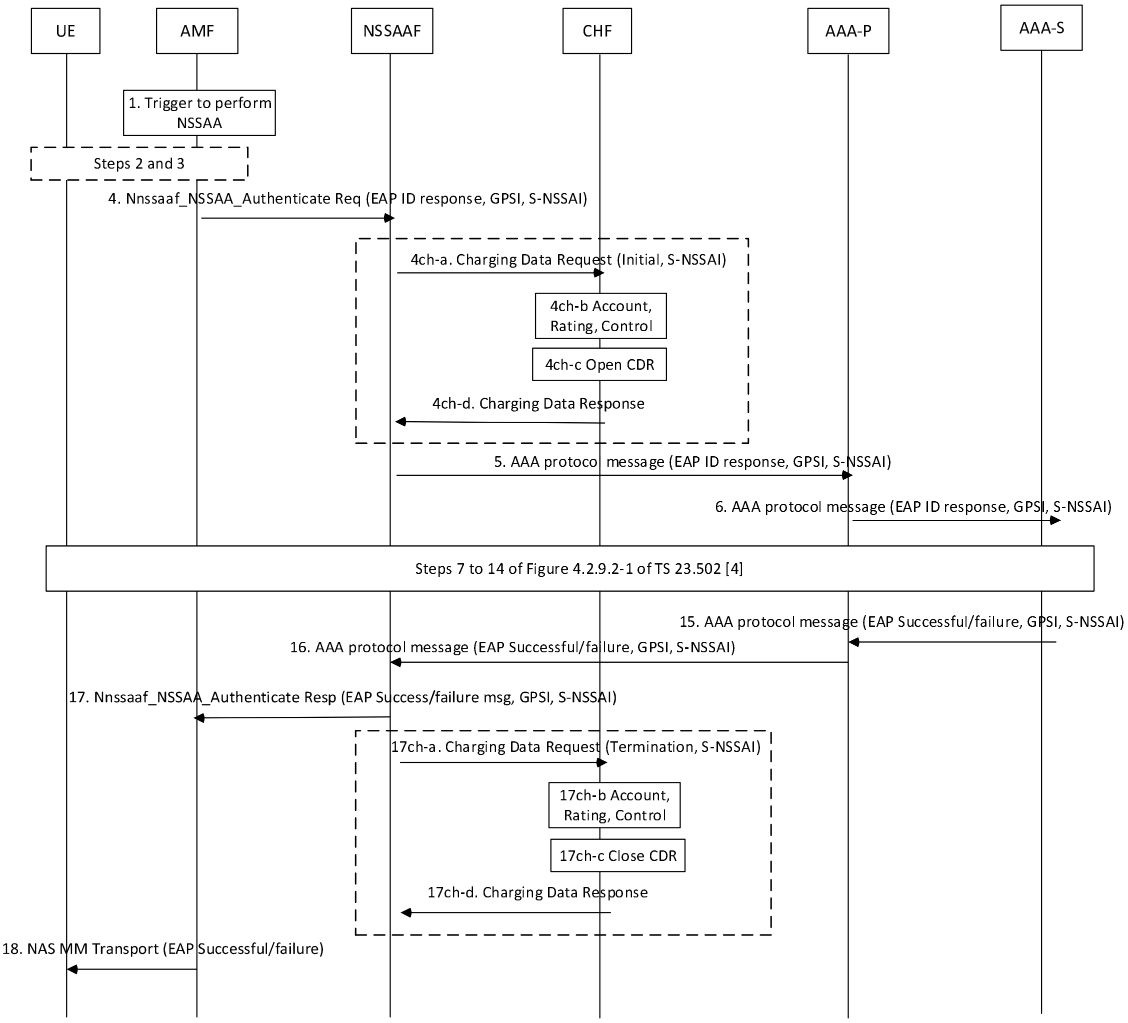
UE
AMF
NSSAAF
CHF
AAA-P
AAA-S
1. Trigger to perform NSSAA
Steps 2 and 3
4. Nnssaaf_NSSAA_Authenticate Req (EAP ID response, GPSI, S-NSSAI)
4ch-a. Charging Data Request (Initial, S-NSSAI)
4ch-b Account, Rating, Control
4ch-c Open CDR
4ch-d. Charging Data Response
5. AAA protocol message (EAP ID response, GPSI, S-NSSAI)
6. AAA protocol message (EAP ID response, GPSI, S-NSSAI)
Steps 7 to 14 of Figure 4.2.9.2-1 of TS 23.502 [4]
15. AAA protocol message (EAP Successful/failure, GPSI, S-NSSAI)
16. AAA protocol message (EAP Successful/failure, GPSI, S-NSSAI)
17. Nnssaaf_NSSAA_Authenticate Resp (EAP Success/failure msg, GPSI, S-NSSAI)
17ch-a. Charging Data Request (Termination, S-NSSAI)
17ch-b Account, Rating, Control
17ch-c Close CDR
17ch-d. Charging Data Response
18. NAS MM Transport (EAP Successful/failure)

Figure 5.2.2.2.5-1: Network slice-specific authentication and authorization – NSSAAF - ECUR

Steps 1 to 4 per 3GPP TS 23.502 [4] Figure 4.2.9.2-1 Network Slice-Specific Authentication and Authorization procedure, AMF sends the EAP Identity Response to the NSSAAF.

4ch-a: NSSAAF sends Charging Data Request [Initial] to CHF with GPSI and S-NSSAI.

4ch-b: Account, Rating, control by the CHF be granted authorization for NSSAA.

4ch-c: The CHF opens a CDR.

4ch-d: CHF provides response to NSSAAF.

Steps 5 to 17 per 3GPP TS 23.502 [4] Figure 4.2.9.2-1 Network Slice-Specific Authentication and Authorization procedure.

17ch-a: NSSAAF procedure with AAA-S is completed: NSSAAF sends Charging Data Request [Terminationt] to CHF with EAP-Success/Failure, GPSI and S-NSSAI.

17ch-b: Account, Rating, control by the CHF for NSSAA.

17ch-c: The CHF closes the CDR.

17ch-d: CHF provides response to NSSAAF.

Step 18: per 3GPP TS 23.502 [4] Figure 4.2.9.2-1 Network Slice-Specific Authentication and Authorization procedure.

5.2.2.3 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization charging

5.2.2.3.1 General

The subclauses below describe "AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization" charging message flows based on figure 4.2.9.3-1 of 3GPP TS 23.502 [4].

5.2.2.3.2 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization - AMF - PEC

The following figure 5.2.2.3.2-1 describes a "AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization" charging in PEC scenario for AMF.

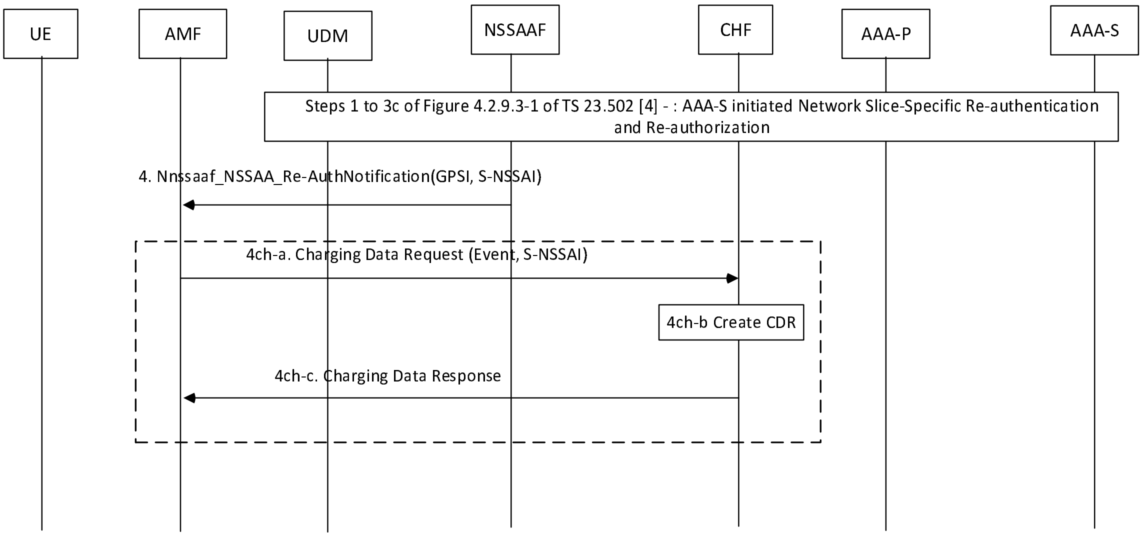
UE
AMF
UDM
NSSAAF
CHF
AAA-P
AAA-S
Steps 1 to 3c of Figure 4.2.9.3-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Re-authentication and Re-authorization
4. Nnssaaf_NSSAA_Re-AuthNotification(GPSI, S-NSSAI)
4ch-a. Charging Data Request (Event, S-NSSAI)
4ch-b Create CDR
4ch-c. Charging Data Response

Figure 5.2.2.3.2-1: AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure - AMF - PEC

Steps 1 to 4: per 3GPP TS 23.502 [4] Figure 4.2.9.3-1 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure.

4ch-a: AAA-S Network Slice-Specific Re-authentication and Re-authorization request received in AMF : AMF sends Charging Data Request [Event] to CHF with GPSI and S-NSSAI.

4ch-b: The CHF creates a CDR.

4ch-c: CHF provides response to AMF.

5.2.2.3.3 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization - NSSAAF - PEC

The following figure 5.2.2.3.3-1 describes a "AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization" charging in PEC scenario for NSSAAF.

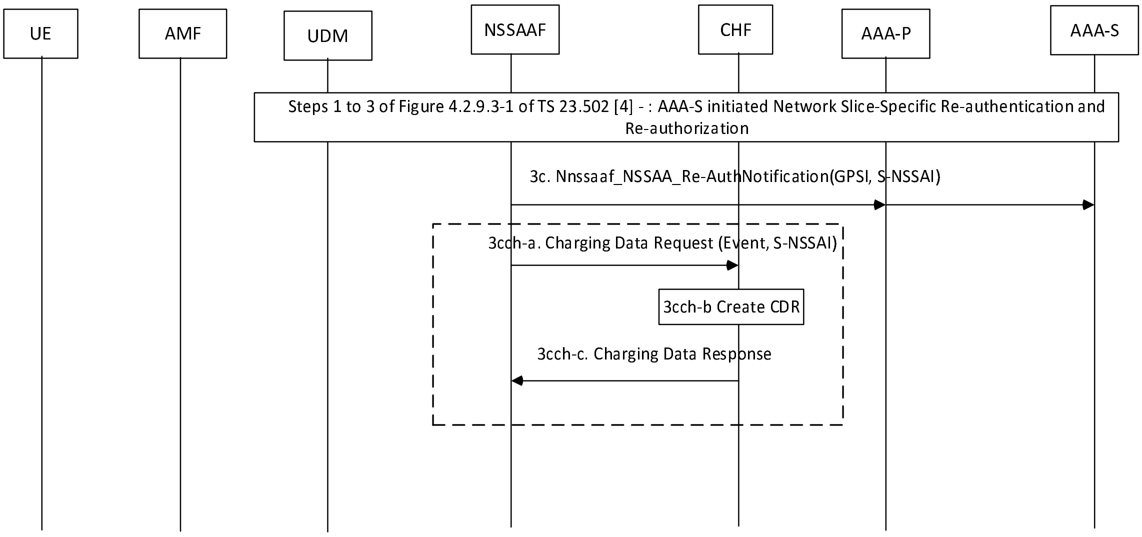
UE
AMF
UDM
NSSAAF
CHF
AAA-P
AAA-S
Steps 1 to 3 of Figure 4.2.9.3-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Re-authentication and Re-authorization
3c. Nnssaaf_NSSAA_Re-AuthNotification(GPSI, S-NSSAI)
3cch-a. Charging Data Request (Event, S-NSSAI)
3cch-b Create CDR
3cch-c. Charging Data Response

Figure 5.2.2.3.3-1: AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure - NSSAAF - PEC

Steps 1 to 3c: per 3GPP TS 23.502 [4] Figure 4.2.9.3-1 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure.

3cch-a: AAA-S Network Slice-Specific Re-authentication and Re-authorization completed in NSSAAF : NSSAAF sends Charging Data Request [Event] to CHF with GPSI and S-NSSAI.

3cch-b: The CHF creates a CDR.

3cch-c: CHF provides response to NSSAAF.

5.2.2.3.4 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization - NSSAAF - IEC

The following figure 5.2.2.3.4-1 describes a "AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization" charging in IEC scenario for NSSAAF.

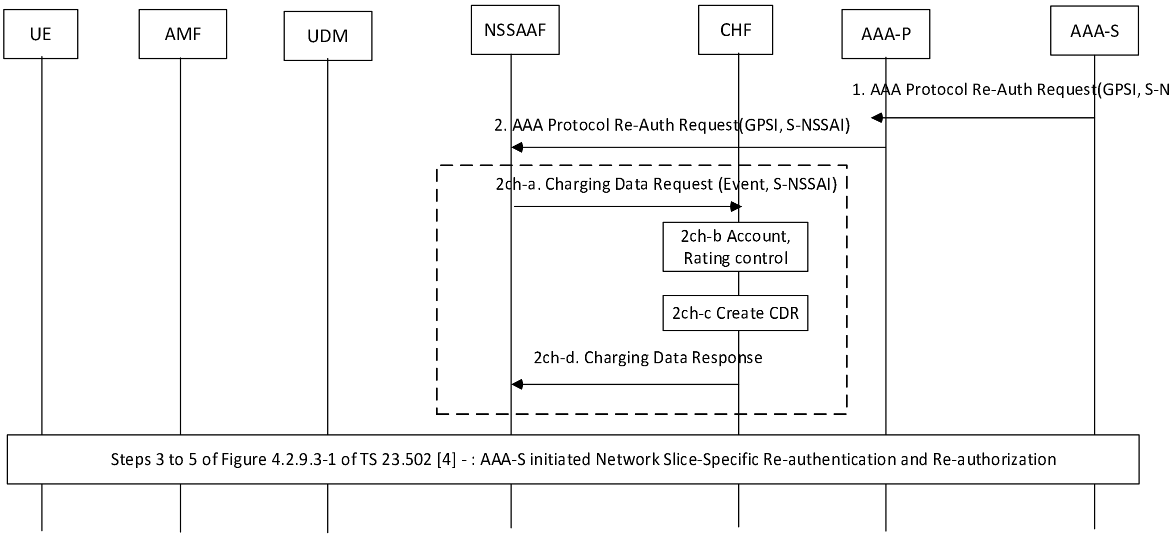
UE
AMF
UDM
NSSAAF
CHF
AAA-P
AAA-S
1. AAA Protocol Re-Auth Request(GPSI, S-N
2. AAA Protocol Re-Auth Request(GPSI, S-NSSAI)
2ch-a. Charging Data Request (Event, S-NSSAI)
2ch-b Account, Rating control
2ch-c Create CDR
2ch-d. Charging Data Response
Steps 3 to 5 of Figure 4.2.9.3-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Re-authentication and Re-authorization

Figure 5.2.2.3.4-1: AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure - NSSAAF - IEC

Steps 1 to 2: per 3GPP TS 23.502 [4] Figure 4.2.9.3-1 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure.

2ch-a: AAA-S Network Slice-Specific Re-authentication and Re-authorization request received in NSSAAF : NSSAAF sends Charging Data Request [Event] to CHF with GPSI and S-NSSAI.

2ch-b: Account, Rating, control by the CHF.

2ch-c: The CHF creates a CDR.

2ch-d: CHF provides response to NSSAAF.

Steps 3 to 5: per 3GPP TS 23.502 [4] Figure 4.2.9.3-1 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure.

5.2.2.3.5 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization - NSSAAF - ECUR

The following figure 5.2.2.3.5-1 describes a "AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization" charging in ECUR scenario for NSSAAF.

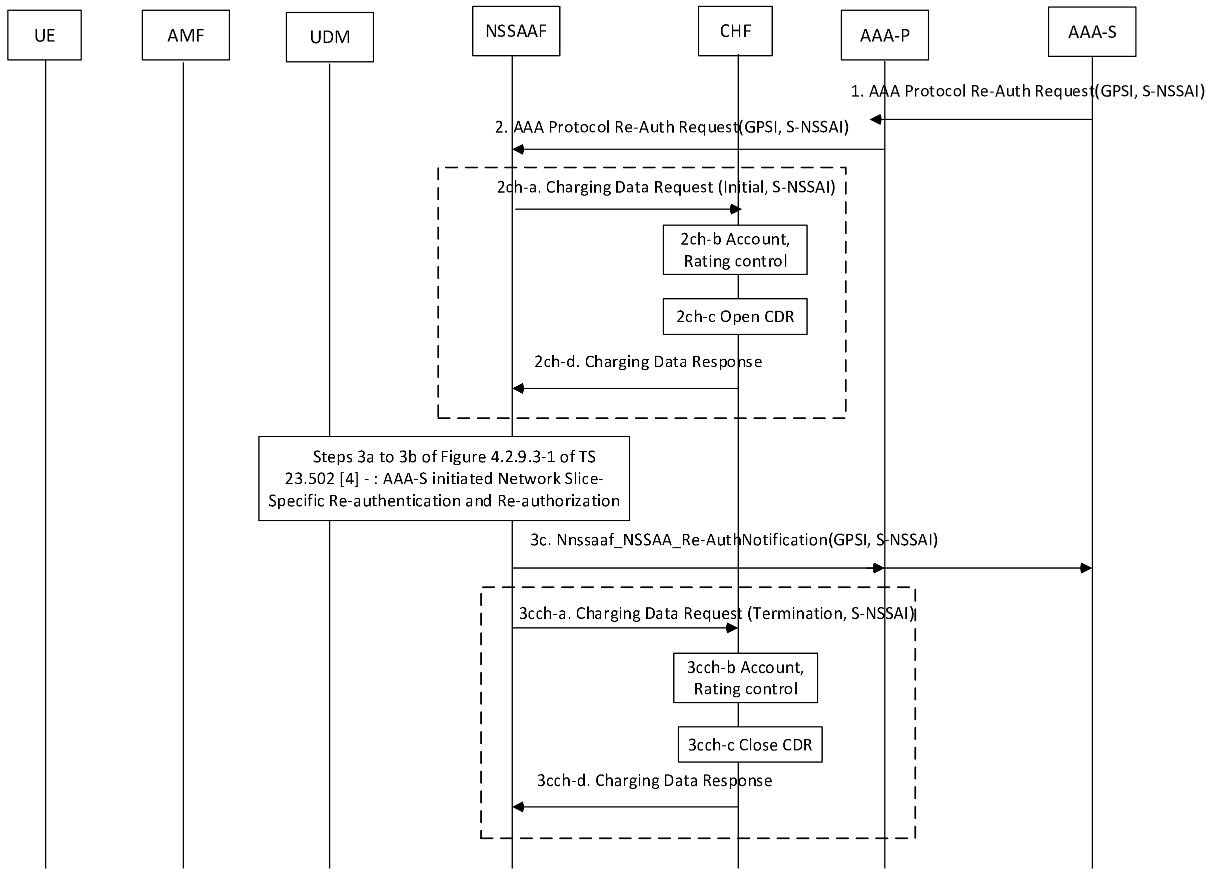
UE
AMF
UDM
NSSAAF
CHF
AAA-P
AAA-S
1. AAA Protocol Re-Auth Request(GPSI, S-NSSAI)
2. AAA Protocol Re-Auth Request(GPSI, S-NSSAI)
2ch-a. Charging Data Request (Initial, S-NSSAI)
2ch-b Account, Rating control
2ch-c Open CDR
2ch-d. Charging Data Response
Steps 3a to 3b of Figure 4.2.9.3-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Re-authentication and Re-authorization
3c. Nnssaaf_NSSAA_Re-AuthNotification(GPSI, S-NSSAI)
3cch-a. Charging Data Request (Termination, S-NSSAI)
3cch-b Account, Rating control
3cch-c Close CDR
3cch-d. Charging Data Response

Figure 5.2.2.3.5-1: AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure - NSSAAF - ECUR

Steps 1 to 2: per 3GPP TS 23.502 [4] Figure 4.2.9.3-1 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure.

2ch-a: AAA-S Network Slice-Specific Re-authentication and Re-authorization request received in NSSAAF : NSSAAF sends Charging Data Request [Initial] to CHF with GPSI and S-NSSAI.

2ch-b: Account, Rating, control by the CHF.

2ch-c: The CHF opens a CDR.

2ch-d: CHF provides response to NSSAAF.

3cch-a: AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure is completed: NSSAAF sends Charging Data Request [Termination] to CHF with GPSI and S-NSSAI.

3cch-b: Account, Rating, control by the CHF.

3cch-c: The CHF closes the CDR.

3cch-d: CHF provides response to NSSAAF.

5.2.2.4 AAA Server triggered Network Slice-Specific Authorization Revocation charging

5.2.2.4.1 General

The subclauses below describe "AAA Server triggered Network Slice-Specific Authorization Revocation" charging message flows based on figure 4.2.9.4-1 of 3GPP TS 23.502 [4].

5.2.2.4.2 AAA Server triggered Network Slice-Specific Authorization Revocation - AMF - PEC

The following figure 5.2.2.4.2-1 describes a "AAA Server triggered Network Slice-Specific Authorization Revocation" charging in PEC scenario for AMF.

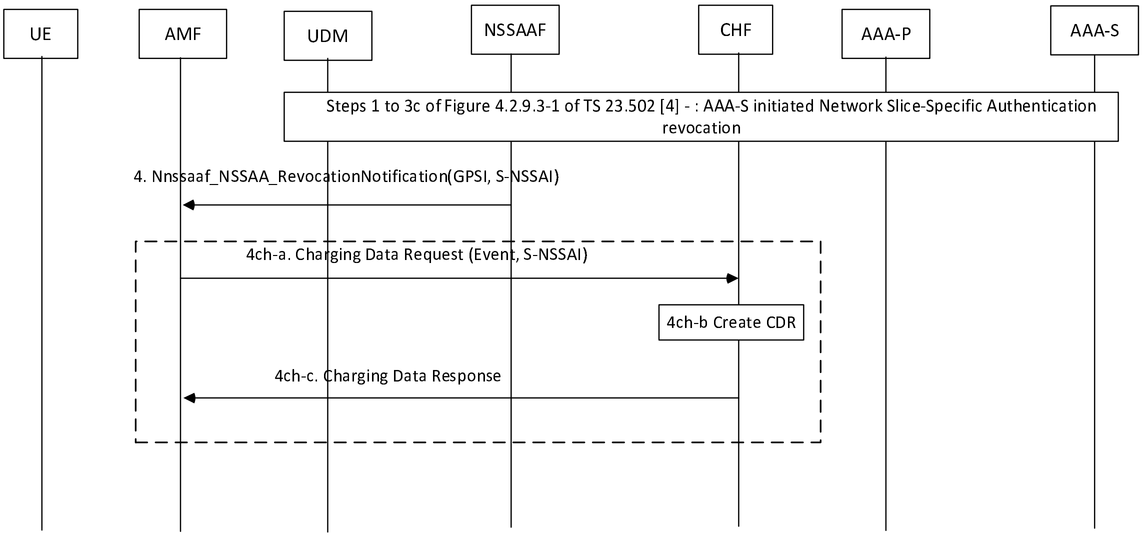
UE
AMF
UDM
NSSAAF
CHF
AAA-P
AAA-S
Steps 1 to 3c of Figure 4.2.9.3-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Authentication revocation
4. Nnssaaf_NSSAA_RevocationNotification(GPSI, S-NSSAI)
4ch-a. Charging Data Request (Event, S-NSSAI)
4ch-b Create CDR
4ch-c. Charging Data Response

Figure 5.2.2.4.2-1: AAA Server triggered Network Slice-Specific Authorization Revocation procedure - AMF - PEC

Steps 1 to 4: per 3GPP TS 23.502 [4] Figure 4.2.9.4-1 AAA Server triggered Network Slice-Specific Authorization Revocation procedure.

4ch-a: AAA-S Network Slice-Specific Authentication revocation Notification received in AMF : AMF sends Charging Data Request [Event] to CHF with GPSI and S-NSSAI.

4ch-b: The CHF creates a CDR.

4ch-c: CHF provides response to AMF.

5.2.2.4.3 AAA Server triggered Network Slice-Specific Authorization Revocation- NSSAAF - PEC

The following figure 5.2.2.4.3-1 describes a "AAA Server triggered Network Slice-Specific Authentication revocation" charging in PEC scenario for NSSAAF.

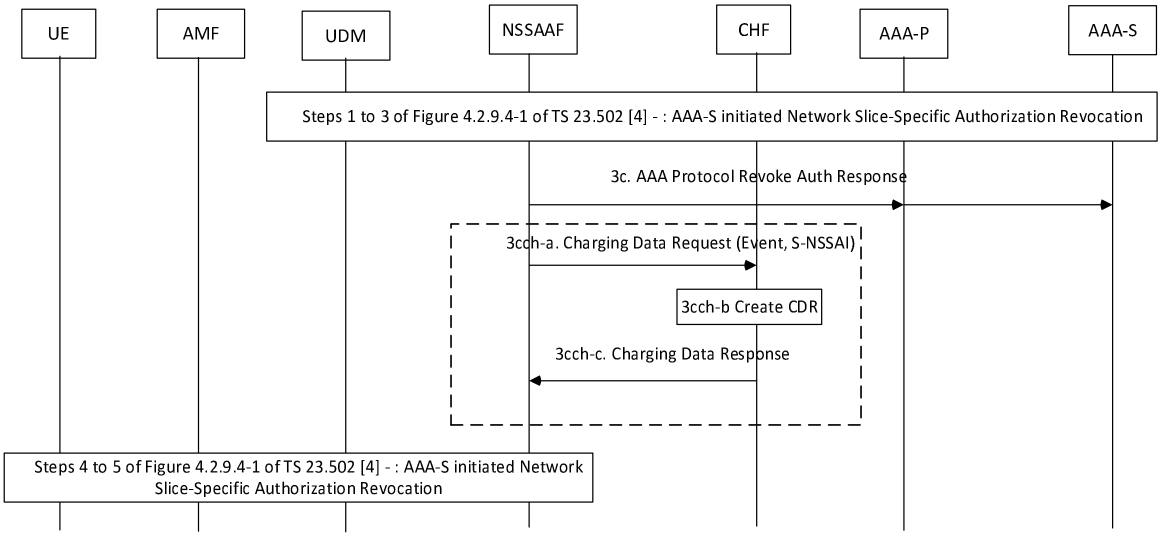
UE
AMF
UDM
NSSAAF
CHF
AAA-P
AAA-S
Steps 1 to 3 of Figure 4.2.9.4-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Authorization Revocation
3c. AAA Protocol Revoke Auth Response
3cch-a. Charging Data Request (Event, S-NSSAI)
3cch-b Create CDR
3cch-c. Charging Data Response
Steps 4 to 5 of Figure 4.2.9.4-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Authorization Revocation

Figure 5.2.2.4.3-1: AAA Server triggered Network Slice-Specific Authorization Revocation procedure - NSSAAF - PEC

Steps 1 to 3c: per 3GPP TS 23.502 [4] Figure 4.2.9.4-1 AAA Server triggered Network Slice-Specific Authorization Revocation procedure.

3cch-a: AAA-S Network Slice-Specific Authorization Revocation completed in NSSAAF : NSSAAF sends Charging Data Request [Event] to CHF with GPSI and S-NSSAI.

3cch-b: The CHF creates a CDR.

3cch-c: CHF provides response to NSSAAF.

5.2.2.4.4 AAA Server triggered Network Slice-Specific Authorization Revocation - NSSAAF - IEC

The following figure 5.2.2.4.4-1 describes a "AAA Server triggered Network Slice-Specific Authorization Revocation" charging in IEC scenario for NSSAAF.

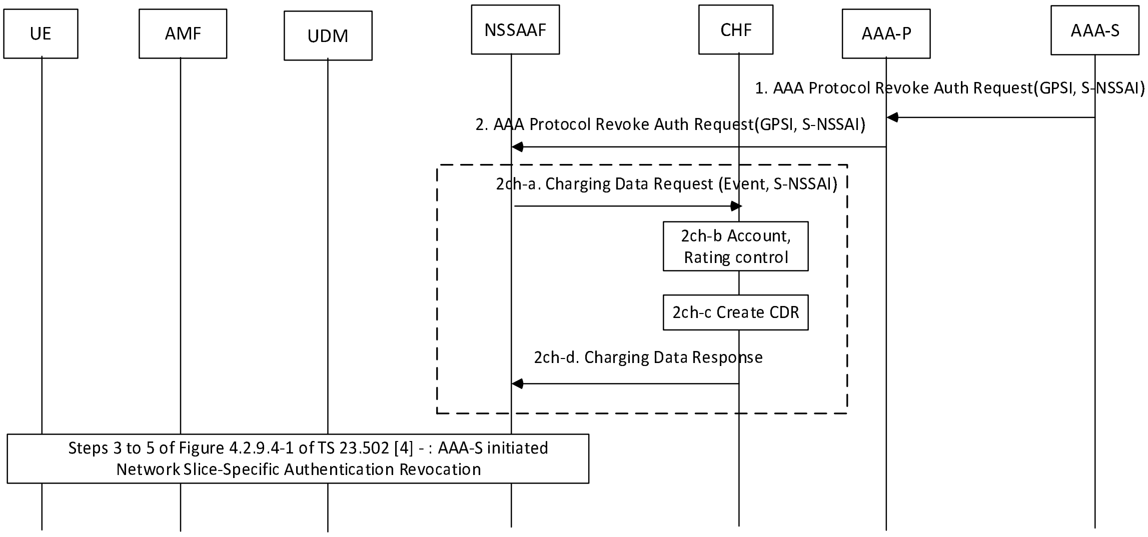
UE
AMF
UDM
NSSAAF
CHF
AAA-P
AAA-S
1. AAA Protocol Revoke Auth Request(GPSI, S-NSSAI)
2. AAA Protocol Revoke Auth Request(GPSI, S-NSSAI)
2ch-a. Charging Data Request (Event, S-NSSAI)
2ch-b Account, Rating control
2ch-c Create CDR
2ch-d. Charging Data Response
Steps 3 to 5 of Figure 4.2.9.4-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Authentication Revocation

Figure 5.2.2.4.4-1: AAA Server triggered Network Slice-Specific Authorization Revocation procedure - NSSAAF - IEC

Steps 1 to 2: per 3GPP TS 23.502 [4] Figure 4.2.9.4-1 AAA Server triggered Network Slice-Specific Authorization Revocation procedure.

2ch-a: AAA-S Network Slice-Specific Authorization Revocation request received in NSSAAF : NSSAAF sends Charging Data Request [Event] to CHF with GPSI and S-NSSAI.

2ch-b: Account, Rating, control by the CHF.

2ch-c: The CHF creates a CDR.

2ch-d: CHF provides response to NSSAAF.

Steps 3 to 5: per 3GPP TS 23.502 [4] Figure 4.2.9.4-1 AAA Server triggered Network Slice-Specific Authorization Revocation procedure.

5.2.2.4.5 AAA Server triggered Network Slice-Specific Authorization Revocation - NSSAAF - ECUR

The following figure 5.2.2.4.5-1 describes a "AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization" charging in ECUR scenario for NSSAAF.

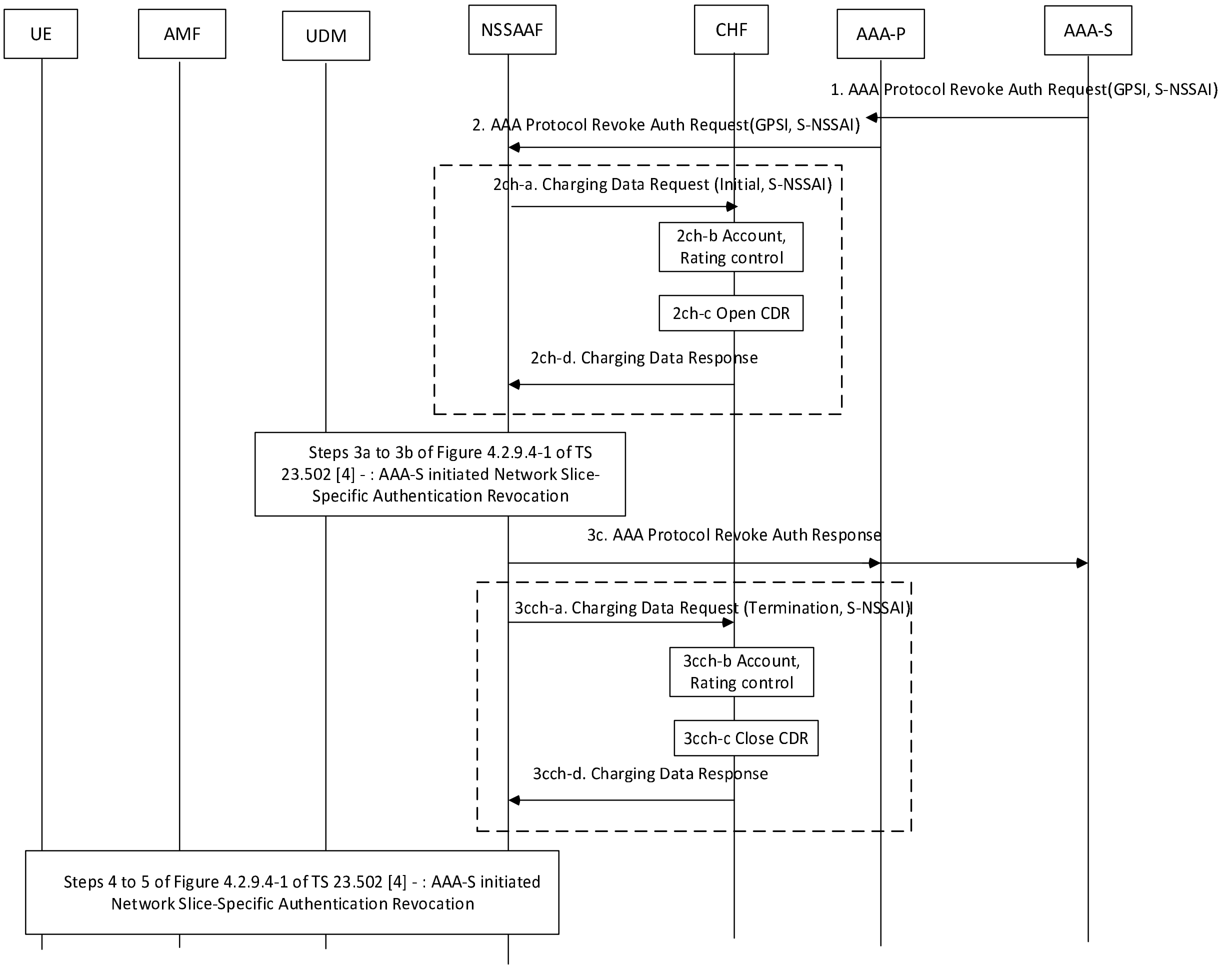
UE
AMF
UDM
NSSAAF
CHF
AAA-P
AAA-S
1. AAA Protocol Revoke Auth Request(GPSI, S-NSSAI)
2. AAA Protocol Revoke Auth Request(GPSI, S-NSSAI)
2ch-a. Charging Data Request (Initial, S-NSSAI)
2ch-b Account, Rating control
2ch-c Open CDR
2ch-d. Charging Data Response
Steps 3a to 3b of Figure 4.2.9.4-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Authentication Revocation
3c. AAA Protocol Revoke Auth Response
3cch-a. Charging Data Request (Termination, S-NSSAI)
3cch-b Account, Rating control
3cch-c Close CDR
3cch-d. Charging Data Response
Steps 4 to 5 of Figure 4.2.9.4-1 of TS 23.502 [4] - : AAA-S initiated Network Slice-Specific Authentication Revocation

Figure 5.2.2.4.5-1: AAA Server triggered Network Slice-Specific Authorization Revocation procedure - NSSAAF - ECUR

Steps 1 to 2: per 3GPP TS 23.502 [4] Figure 4.2.9.4-1 AAA Server triggered Network Slice-Specific Authorization Revocation procedure.

2ch-a: AAA-S Network Slice-Specific Authorization Revocation request received in NSSAAF : NSSAAF sends Charging Data Request [Initial] to CHF with GPSI and S-NSSAI.

2ch-b: Account, Rating, control by the CHF.

2ch-c: The CHF opens a CDR.

2ch-d: CHF provides response to NSSAAF.

3cch-a: AAA Server triggered Network Slice-Specific Authorization Revocation procedure is completed: NSSAAF sends Charging Data Request [Termination] to CHF with GPSI and S-NSSAI.

3cch-b: Account, Rating, control by the CHF.

3cch-c: The CHF closes the CDR.

3cch-d: CHF provides response to NSSAAF.

5.2.3 CDR generation

5.2.3.1 Introduction

The CHF CDRs for Network Slice-Specific Authentication and Authorization charging are generated by the CHF to collect charging information that they subsequently transfer to the Charging Gateway Function (CGF).

The following clauses describe in detail the conditions for generating the CHF CDR, which shall be supported by the CHF.

5.2.3.2 Triggers for CHF CDR

5.2.3.2.1 General

A Network Slice-Specific Authentication and Authorization charging CHF CDR is used to collect charging information related to Network Slice-Specific Authentication and Authorization chargeable events for PEC, IEC and ECUR scenarios.

5.2.3.2.2 Triggers for CHF CDR generation

A CHF CDR shall be generated by the CHF for each received Charging Data Request [Event].

5.2.3.2.3 Triggers for CHF CDR opening

A CHF CDR shall be opened when the CHF receives Charging Data Request [Initial].

5.2.3.2.4 Triggers for CHF CDR closure

The CHF CDR shall be closed when the CHF receives Charging Data Request [Termination].

5.2.4 Ga record transfer flows

Details of the Ga protocol application are specified in 3GPP TS 32.295 [9].

5.2.5 Bnssaa CDR file transfer

Details of the Bnssaa protocol application are specified in 3GPP TS 32.297 [10].

6 Definition of charging information

6.1 Data description for Network slice-specific authentication and authorization charging

6.1.1 Message contents

6.1.1.1 General

The Charging Data Request and Charging Data Response are specified in subclause 5.1.2.2.1 of 3GPP TS 32.290 [6].

Table 6.1.1.1-1 describes the use of these messages for Network slice-specific authentication and authorization charging.

Table 6.1.1.1-1: Network slice-specific authentication and authorization charging messages reference table

Message	Source	Destination
Charging Data Request	NSSAAF, AMF	CHF
Charging Data Response	CHF	NSSAAF, AMF

The following clauses describe the different fields used in the Charging Data messages and the category in the tables is used according to the charging data configuration defined in clause 5.4 of 3GPP TS 32.240 [2].

6.1.1.2 Charging Data Request message

Table 6.1.1.2-1 illustrates the basic structure of a Charging Data Request message from the NSSAAF and AMF, as used for network slice-specific authentication and authorization.

Table 6.1.1.2-1: Charging Data Request message contents

Information Element	Converged Charging Category	Description
Session Identifier	O_C	Described in 3GPP TS 32.290 [6]
Subscriber Identifier	O_M	This field contains the identification of the individual subscriber in the PLMN i.e. SUPI.
NF Consumer Identification	M	Described in 3GPP TS 32.290 [6] and holds the identifier of the NSACF
NF Functionality	M	Described in 3GPP TS 32.290 [6].
NF Name	O_C	Described in 3GPP TS 32.290 [6].
NF Address	O_C	Described in 3GPP TS 32.290 [6].
NF PLMN ID	O_C	Described in 3GPP TS 32.290 [6].
Charging Identifier	O_M	Described in 3GPP TS 32.290 [6].
Invocation Timestamp	M	Described in 3GPP TS 32.290 [6].
Invocation Sequence Number	M	Described in 3GPP TS 32.290 [6].
One-time Event	O_C	Described in 3GPP TS 32.290 [6].
One-time Event Type	O_C	Described in 3GPP TS 32.290 [6].
Supported Features	O_C	Described in 3GPP TS 32.290 [6].
Service Specification Information	O_C	Described in 3GPP TS 32.290 [6].
Multiple Unit Usage	O_M	Described in 3GPP TS 32.290 [6].
Rating Group	M	Described in 3GPP TS 32.290 [6].
Requested Unit	O_C	Described in 3GPP TS 32.290 [6].
NSSAA Charging Information	C	This field holds NSSAA specific information described in clause 6.2.1.2.

6.1.1.3 Charging data response message

Table 6.1.1.3-1 illustrates the basic structure of a Charging Data Response message from the CHF to the NSSAAF and AMF as used for network slice-specific authentication and authorization.

Table 6.1.1.3-1: Charging Data Response message contents

Information Element	Converged Charging Category	Description
Session Identifier	O_C	Described in 3GPP TS 32.290 [6].
Invocation Timestamp	M	Described in 3GPP TS 32.290 [6].
Invocation Result	O_C	Described in 3GPP TS 32.290 [6].
Invocation Sequence Number	O_M	Described in 3GPP TS 32.290 [6].
Session Failover	O_C	Described in 3GPP TS 32.290 [6].
Supported Features	O_C	Described in 3GPP TS 32.290 [6].
Multiple Unit Information	O_C	Described in 3GPP TS 32.290 [6].
Result Code	O_C	Described in 3GPP TS 32.290 [6].
Rating Group	O_M	Described in 3GPP TS 32.290 [6].
Granted Unit	O_C	Described in 3GPP TS 32.290 [6].
Validity Time	O_C	Described in 3GPP TS 32.290 [6].

6.1.2 Ga message contents

See clause 5.2.4.

6.1.3 CDR description on the B$_{nssaa}$ interface

6.1.3.1 General

This clause describes the CDR content and format generated for Network slice-specific authentication and authorization charging.

The following tables provide a brief description of each CDR parameter. The category in the tables is used according to the charging data configuration defined in clause 5.4 of 3GPP TS 32.240 [2]. Full definitions of the CDR parameters, sorted by the name in alphabetical order, are provided in 3GPP TS 32.298 [8].

6.1.3.2 Network slice-specific authentication and authorization charging CHF CDR data

If enabled, CHF CDRs for Network slice-specific authentication and authorization charging shall be produced for NSSAA chargeable events.

The fields of Network slice-specific authentication and authorization charging CHF CDR are specified in table 6.1.3.2-1.

Table 6.1.3.2-1: Network slice-specific authentication and authorization charging CHF record data

Field	Category	Description
Record Type	M	Described in 3GPP TS 32.298 [8]
Recording Network Function ID	O_M	Described in 3GPP TS 32.298 [8]
Charging Session Identifier	O_C	Described in 3GPP TS 32.298 [8]
Subscriber Identifier	O_M	Described in 3GPP TS 32.298 [8]
NF Consumer Information	M	This field holds the information of the entity that used the charging service (i.e. NSSAAF, AMF).
NF Functionality	M	This field holds the type of functionality the NF provides: i.e. NSACF
NF Name	O_C	This field holds the name of the NSSAAF or AMF.
NF Address	O_C	This field holds the IP Address of the used NSSAAF or AMF.
NF PLMN ID	Oc	This field holds the PLMN identifier (MCC MNC) of the NSSAAF or AMF.
Charging Identifier	O_M	Described in 3GPP TS 32.298 [8]
Record Opening Time	M	Described in 3GPP TS 32.298 [8]
Duration	M	Described in 3GPP TS 32.298 [8]
Record Sequence Number	C	Described in 3GPP TS 32.298 [8]
Cause for Record Closing	M	Described in 3GPP TS 32.298 [8]
Diagnostics	O_M	Described in 3GPP TS 32.298 [8]
Local Record Sequence Number	O_M	Described in 3GPP TS 32.298 [8]
Record Extensions	O_C	Described in 3GPP TS 32.298 [8]
NSSAA Charging Information	O_M	This field holds NSSAA specific information described in clause 6.2.1.2

6.2 Network slice-specific authentication and authorization charging specific parameters

6.2.1 Definition of Network slice-specific authentication and authorization charging information

6.2.1.1 General

The Charging Information parameter used for Network slice-specific authentication and authorization charging is provided in the following clauses.

6.2.1.2 Definition of Network slice-specific authentication and authorization charging information

Specific charging information used for Network slice-specific authentication and authorization charging is provided within the NSSAA Charging Information.

The detailed structure of the NSSAA Charging Information can be found in table 6.2.1.2-1.

Table 6.2.1.2-1: Structure of NSSAA Charging Information

Information Element	Category	Description
NSSAA message type	M	This field holds the message type of the NSSAA procedure
User identification	M	This field holds the user identification of the individual subscriber, i.e. Generic Public Subscription Identifier (GPSI).
S NSSAI	M	This field holds the Single Network Slice Selection Assistance Information identifying the network slice.
AAA P Address	O_C	This field holds the AAA-P Address when available.
AAA S Address	O_C	This field holds the AAA-S Address when available.
EAP ID Response	O_C	This field holds the EAP ID Response message from the UE.
EAP auth status	O_C	This field holds the result of EAP authentication procedure.
AMF Identifier	O_C	This field holds the AMF identifier of the AMF serving the UE

6.2.2 Detailed message format for converged charging

The following clause specifies per Operation Type the charging data that are sent by NSSAAF and AMF for Network slice-specific authentication and authorization converged charging.

The Operation Types are listed in the following order: I (Initial)/U (Update)/T (Termination)/E (Event). Therefore, when all Operation Types are possible it is marked as IUTE. If only some Operation Types are allowed for a node, only the appropriate letters are used (i.e. IUT or E) as indicated in the table heading. The omission of an Operation Type for a particular field is marked with "-" (i.e. IU-E). Also, when an entire field is not allowed in a node the entire cell is marked as "-".

Table 6.2.2-1 defines the basic structure of the supported fields in the *Charging Data Request* message for Network slice-specific authentication and authorization converged charging.

Table 6.2.2-1: Supported fields in Charging Data Request message

Information Element	NSSAA NF	NSSAAF	AMF
	Supported Operation Types	I/T/E	E
Session Identifier		T	-
Subscriber Identifier		ITE	E
NF Consumer Identification		ITE	E
Charging Identifier		ITE	E
Invocation Timestamp		ITE	E
Invocation Sequence Number		ITE	E
One-time Event		--E	E
One-time Event Type		--E	E
Supported Features		ITE	E
Service Specification Information		ITE	E
Multiple Unit Usage		ITE	-
Rating Group		I-E	E
Requested Unit		I-E	E
NSSAA Charging Information			
NSSAA message type		ITE	E
User identification		ITE	E
S NSSAI		ITE	E
AAA P Address		ITE	E
AAA S Address		ITE	E
EAP ID Response		ITE	E
EAP auth status		ITE	E
AMF Identifier		-	E

Table 6.2.2-2 defines the basic structure of the supported fields in the *Charging Data Response* message for Network slice-specific authentication and authorization converged charging.

Table 6.2.2-2: Supported fields in Charging Data Response message

Information Element	NSSAA NF	NSSAAF	AMF
	Supported Operation Types	I/T/E	E
Session Identifier		ITE	E
Invocation Timestamp		ITE	E
Invocation Result		ITE	E
Invocation Sequence Number		ITE	E
Session Failover		I--	-
Supported Features		I-E	E
Multiple Unit Information		I-E	E
Result Code		I-E	E
Rating Group		I-E	E
Granted Unit		I-E	E
Validity Time		I-E	E

6.2.3 Formal Network slice-specific authentication and authorization charging parameter description

6.2.3.1 Network slice-specific authentication and authorization CHF CDR parameters

The detailed definitions, abstract syntax and encoding of the Network slice-specific authentication and authorization CHF CDR parameters are specified in 3GPP TS 32.298 [8].

6.2.3.2 Network slice-specific authentication and authorization resources attributes

The detailed definitions of resources attributes used for Network slice-specific authentication and authorization charging are specified in 3GPP TS 32.291 [7].

6.3 Bindings for Network slice-specific authentication and authorization converged charging

This mapping between the Information Elements, resource attributes and CHF CDR parameters for Network slice-specific authentication and authorization converged charging is described in clause 7 of 3GPP TS 32.291 [7].

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2023-04	SA5#148e					Initial skeleton	0.0.0
2023-04	SA5#148e	S5-233220 S5-233222 S5-233223 S5-233656				Introduction of the Reference Introduction of the Terms Introduction of the Abbreviations Introduction of the Scope	0.1.0
2023-05	SA5#149	S5-234473 S5-234474				Introduce architecture Introduce charging principles	0.2.0
2023-06	SA5#150	S5-235766 S5-235767 S5-235768 S5-235783 S5-235784				Introduce charging scenarios principles Introduce applicable triggers Introduce PEC message flow Introduce IEC message flow Introduce ECUR message flow	0.3.0
2023-10	SA5#151	S5-236289 S5-236291 S5-236292 S5-236293 S5-236904 S5-236295 S5-236905 S5-236297				Introduce Reference Point for NSSAAF Addition of applicable triggers Introduction of AAA-S Re-authentication and Re-authorization flows Introduction of AAA-S triggered NS-Specific Autho. Revocation flows Introduce CDR generation Introduce Ga record and CDR file transfer Introduce definition of charging information Introduce NSSAA specific charging information	0.4.0
2023-11	SA5#152	S5-237450 S5-237451 S5-237528 S5-238003 S5-237453 S5-237454				Introduction of CHF selection Introduction of CDR description Refinement on charging information Introduction of Detailed message format for converged charging Introduction of Formal NS-specific auth charging parameter desc Introduction of Bindings for NS-specific auth and autho converged charging	0.5.0
2023-12	SA#102	SP-231520				Presented for information and approval`	1.0.0
2023-12	SA#102					Upgrade to change control version	18.0.0
2023-12	SA#102					Fix clause numbering	18.0.1
2024-06	SA#104	SP-240840	0002	1	F	Rel-18 CR 28.204 Correction on trigger for NSSAA message content	18.1.0
2024-07	SA#104					Fix indentation of some text in tables 6.2.2-1 and 6.2.2-2.	18.1.1

History

Document history		
V18.0.1	May 2024	Publication
V18.1.1	August 2024	Publication