Technical Specification of the SIP (Gm) interface between the User Equipment (UE) and the NGN platform of Deutsche Telekom

1 TR 114

Version: 3.0.0

Amendment 7
(Clarification on Authentication)

13. September 2016

Herausgeber / Publisher

Deutsche Telekom AG

Verantwortlich/ Responsible

Deutsche Telekom Netzproduktion GmbH

Fixed Mobile Engineering Deutschland

Abteilung FMED-321

64307 Darmstadt

Bestellangabe / Order Information

Kurztitel / Title: 1 TR 114

Ausgabe / Version: 3.0.0 Amendment 7 (September 2016)

Erweiterung für / Amendment for 1 TR 114, Ausgabe / Version 3.0.0 (June 2013)

Bezugsanschrift / Order address

Internet Download:

https://www.telekom.de/hilfe/geraete-zubehoer/telefone-und-anlagen/informationen-zu-telefonanlagen/schnittstellenbeschreibungen-fuer-hersteller?samChecked=true

1 Scope

This Amendment is an addition to 1 TR 114 V3.0.0

Markings general used within the TEXT:

Text modified due to Deutsche Telekom requirements that is added or deleted compared to 1 TR 114 is shown as cursive and underlined (*example for added text*) or cursive and stricken (~~*example for stricken text*~~).

2 Clarification on Authentication Procedure to 1 TR 114 and 1 TR 114 Annex B

2.1 References

These references are taken out of 1 TR 114 Annex B, thus the numbering is kept the same as in Annex B.

[21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

2.2 1 TR 114 clarifications

1 TR 114 States in section 7.2.1 Global modifications to 3GPP TS 24.229 Release 11 the following:

- *The challenge mechanism shall be supported.*
- *To avoid too many challenge cycles the nonce shall be included within each request during its validity.*

Replace these two statements in section 7.2.1 Global modifications to 3GPP TS 24.229 Release 11 with the following text:

- *The challenge mechanism shall be supported.*

Note: This requirement seen from UE point of view is needed that a received 401 or 407 is processed properly. I.e. using the correct nonce and procedures as defined in RFC 2617 [21] and this document for the next request sent by the UE. This shall apply for NASS bundled as well as for Digest authentication.

- *To avoid too many challenge cycles the nonce shall be included within each request during its validity.*

Note: This requirement seen from UE point of view is needed to include the stored credentials (nonce value) into the next request. This shall apply for NASS bundled as well as for Digest authentication.

- *The next-nonce mechanism as defined within RFC 2617 [21] shall be supported.*
- *The nonce received in 401 or 407 by the UE is valid for registration as well as for initial requests.*
- *The next- nonce received in a 200 OK is valid for next requests (including REGISTER) sent by the UE.*
- *The latest receives "next-nonce" shall be used for the Re-REGISTER.*

Section "7.3.4 Support of SIP Headers on the UNI (Gm) –Interface" describes within Table 7-4 the SIP header fields that must be supported by the UE.

Table -1: Supported headers

Item	Header	Sending (UE to P-CSCF)			Receiving (P-CSCF to UE)		
		Ref.	Profile status UNI (Gm)	Profile status UE	Ref.	Profile status UNI (Gm)	Profile status UE
8	Authentication-Info	[26] 20.6	o	m	[26] 20.6	o	m
9	Authorization	[26] 20.7	m	m	[26] 20.7	~~m~~c2	~~m~~c2
43	Proxy-Authenticate	[26] 20.27	n/a	n/a	[26] 20.27	m	m
44	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	n/a	c1
73	WWW-Authenticate	[26] 20.44	n/a	n/a	[26] 20.44	o	m
c1: If Received ignore c2: Applicable for authentication between UA							

Table 7-4 states that the Authentication-Info header used for providing the next-nonce value is mandatory.

In general the nonce generated by the network is valid for "Authorization" as well as for "Proxy-Authorization".

The SIP www-authenticate and the Authorization header field is used for registering and re-registering the UE at the IMS. This is independent of the method used for registration.

The SIP Authentication-Info header field is used for providing the next-nonce in a 200 OK (REGISTER or INVITE)

Proxy- Authorization is used within INVITE containing the valid nonce to avoid a challenge response (i.e. 407)

2.2 1 TR 114 Annex B clarifications

In "Section 5.1.1.5.4 SIP digest without TLS – general" the following paragraph describes the use of the next-nonce value received within a 200 OK response as part of the SIP Authentication-Info header field . Modify the text as follows.

5.1.1.5.4 SIP digest without TLS – general

...

On receiving the 200 (OK) response for the REGISTER request, if the "algorithm" Authentication-Info header field parameter is "MD5", the UE shall authenticate the S-CSCF using the "rspauth" Authentication-Info header field parameter as described in RFC 2617 [21]. If the nextnonce field is present in the Authentication-Info header field the UE ~~*should*~~ *shall* use it when constructing the Authorization (***Authorization header for REGISTER and Proxy-Authorization for INVITE***) header for its next request as specified in RFC 2617 [21].

The nexnonce shall be stored by the IAD as long as the nonce value is valid. i.e. a new nonce will be provided either by sending the nonce in a Authentication-Info with the "nextnonce" or via nonce value received within a challenge response (401 or 407) as described in RFC 2617 [21]

The procedure for the use of nonce, nonce counter and next-nonce described within this document is valid for NASS bundled and Digest authentication.

The latest received "next-nonce" within a 200 OK for a request shall be used for the Re-Register.

Modify Section 5.1.2A of 1 TR 114 Annex B as follows:

5.1.2A Generic procedures applicable to all methods excluding the REGISTER method

5.1.2A.1 UE-originating case

5.1.2A.1.1 General

....

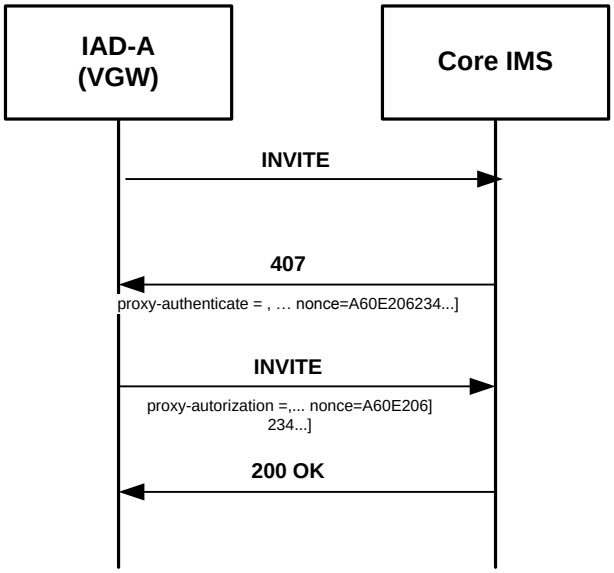
When SIP digest *or NASS bundled authentication is* in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;
- if the contained nonce value is associated to the realm used for the related REGISTER request authentication, store the contained nonce as a nonce value for proxy authentication *(next INVITE Requests) as well as for authentication (next REGISTER request)* associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for proxy authentication for this registration or registration flow;
- calculate the response as described in RFC 2617 [21] using the stored nonce value for proxy authentication *(which is the same as for authentication)* associated to the same registration or registration flow (if the multiple registration mechanism is used); and
- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

....

2.3 Examples

2.3.1. Challenge when INVITE does not contain Proxy-Authorization header



Initial Request INVITE w/o Authorization header

Challenge Request in SIP Response 407:

Proxy-Authenticate

Digest nonce="A60E206B33C999900000000DAA2F522"

,realm="tel.t-online.de",

algorithm=MD5,

qop="auth"

Answer in following INVITE:

Proxy-Authorization:

username="Alice@t-online.de",

realm="tel.t-online.de",

Digest nonce="A60E206B33C999900000000DAA2F522",

uri="sip:+Alice_E164@tel.t-online.de",

response="3d0ae894faee9999d0cfe7fcce5ee402",

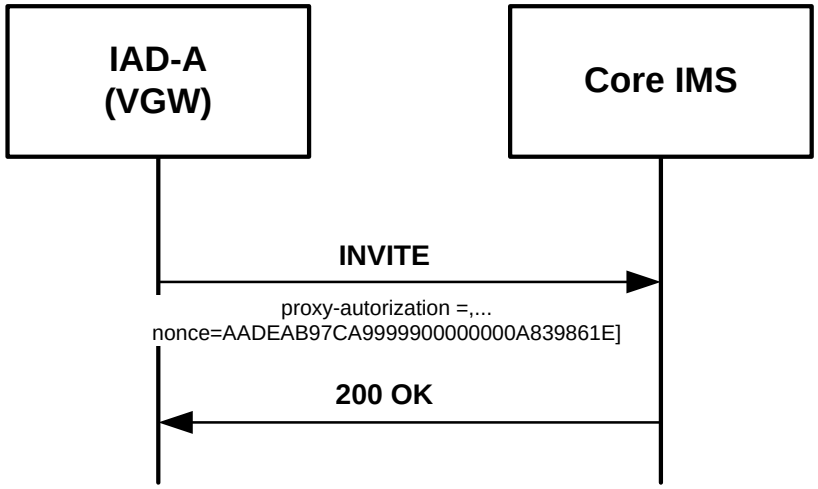
algorithm=MD5,

cnonce="E013376E7888856D",

qop=auth,

nc=00000001

2.3.2 Example with correct Proxy-Authorization header in INVITE



Exampe initial INVITE using nonce from Registration:

Proxy-Authorization:

Digest username="Alice@t-online.de",

realm="tel.t-online.de",

nonce="AADEAB97CA9999900000000A839861E",

uri="sip:Alice_E164@tel.t-online.de;

user=phone;transport=udp",

response="e7c5f54f744dd8f88b63e84052

Algorithm: MD5

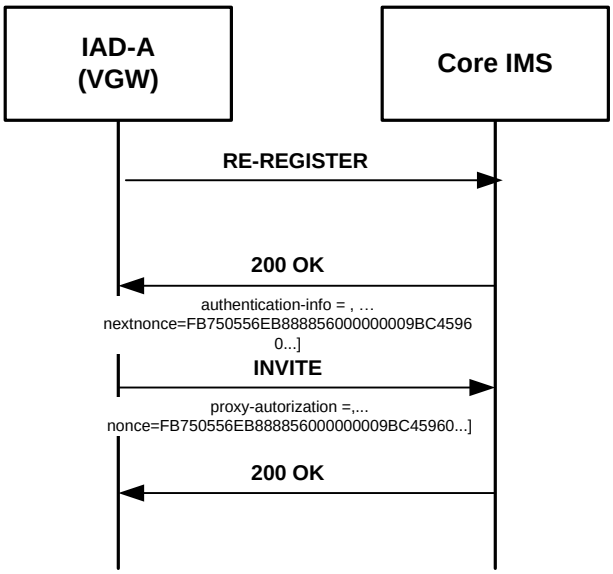
CNonce Value: "568a61bf"

QOP: auth

Nonce Count: 00001234

The nonce value was exchanged during registration procedure and stored within the IAD.

2.3.2 Example with correct Authentication-Info header in 200 OK for REGISTER



200OK for Re-Register

Authentication-Info:

nextnonce="FB750556EB888856000000009BC45960",

qop=auth,

rspauth="b385ad644ba1f25cc32e2dbbf3cc166c",

cnonce="568a61cc",

nc=00001234

Example initial INVITE using nonce from 200 OK (REGISTER):

Proxy-Authorization:

Digest username="Alice@t-online.de",

realm="tel.t-online.de",

nonce=" FB750556EB888856000000009BC45960",

uri="sip:Alice_E164@tel.t-online.de;

user=phone;transport=udp",

response="e7c5f54f744dd8f88b63e84052

Algorithm: MD5

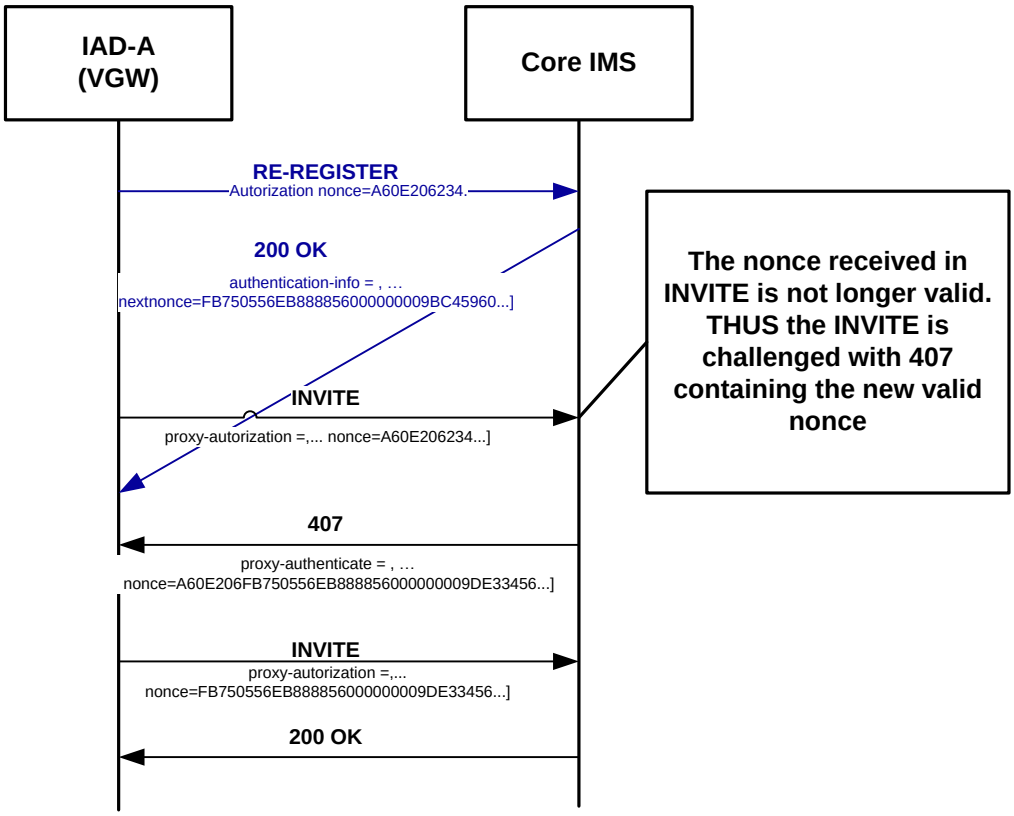
CNonce Value: "568a61bf"

QOP: auth

Nonce Count: 00001234

Note: Authentication-Info is currently not used for 200 OK answering an INVITE request.

2.3.3 Example with race condition Authentication-Info header in 200 OK for REGISTER crosses INVITE with "old nonce"



Version	Published	Remarks
3.0.0		-locating P-CSCF and correct prioritization of P-CSCF in case of registration including maintenance procedures. -Preconditions support "passive" better described -Early-Media Header and indication of early media described to avoid misinterpretation. And allow handling of calls initiated by mobile devices. - use of from-change. No default setting - deletion of Annex A - Update of Annex B - Deletion of TS 124.503 - UPDATE to 3GPP Release 11 documents -Correction of *# Procedures using PIN (ECT, OCB, Kick Out, Black List, White List, ACR, CB, ICB) - CLIR 3 included in D.2.0 - Documentation Update TIP/TIR and OIP/OIR -MWI voided - Documentation Update of " 8.6 Support of NAT traversal by the UE" -MIME Type UPDATE Table 7-5 -UPDATE Table 7-4 SIP Headers

Version	Published	Remarks
		- add references TR-069, TR-104 and TR-181 - add reference 3GPP TS 23.003 - C.2.8 allow implementations acting on "application/vnd.3gpp.cw+xml" All changes are backward compatible with the procedures described within 1 TR 114 Version 2.4.0
Amendment 7	13.09.2016	Clarification on Authentication procedures