**3GPP TSG-CT WG1 Meeting #125-eC1-205386**

**Electronic meeting, 20-28 August 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.229** | **CR** | **6433** | **rev** | **1** | **Current version:** | **16.6.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **x** | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Usage of RFC 5688. |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | IMSProtoc17 |  | ***Date:*** | 2020-08-27 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)* |
|  |  |
| ***Reason for change:*** | SA4 have defined usage of the sip.app-subtype media feature tag defined in RFC 5688, see the LS in C1-204650. 24.229 only specifies that a UE needs to include the media feature tags for streaming media types that are defined in RFC 3840. This makes it uncertain whether the media feature tag defined in RFC 5688 is in scope. Annex A in 24.229 already indicates support for RFC 5688. |
|  |  |
| ***Summary of change:*** | Indicate that the media feature tag in RFC 5688 is in scope in the cases where RFC 3840 is referenced in relation to streaming media types. |
|  |  |
| ***Consequences if not approved:*** | Unclear specifications in how RFC 5688 is used. |
|  |  |
| ***Clauses affected:*** | 5.1.1.2.1, 5.1.1.4.1, 5.1.3.1, 5.1.4.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* First Change \* \* \* \*

##### 5.1.1.2.1 General

The initial registration procedure consists of the UE sending an unprotected REGISTER request and, if challenged depending on the security mechanism supported for this UE, sending the integrity-protected REGISTER request or other appropriate response to the challenge. The UE can register a public user identity with any of its contact addresses at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

When registering any public user identity belonging to the UE, the UE shall either use an already active pair of security associations or a TLS session to protect the REGISTER requests, or register the public user identity via a new initial registration procedure.

When binding any one of its public user identities to an additional contact address via a new initial registration procedure, the UE shall follow the procedures described in RFC 5626 [92]. The set of security associations or a TLS session resulting from this initial registration procedure will have no impact on the existing set of security associations or TLS sessions that have been established as a result of previous initial registration procedures. However, if the UE registers any one of its public user identities with a new contact address via a new initial registration procedure and does not employ the procedures described in RFC 5626 [92], then the new set of security associations or TLS session shall replace any existing set of security association or TLS session.

If the UE detects that the existing security associations or TLS sessions associated with a given contact address are no longer active (e.g., after receiving no response to several protected messages), the UE shall:

- consider all previously registered public user identities bound to this security associations or TLS session that are only associated with this contact address as deregistered; and

- stop processing all associated ongoing dialogs and transactions that were using the security associations or TLS session associated with this contact address, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs).

The UE shall send the unprotected REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, or if the UE was pre-configured with the P-CSCF's IP address or domain name and was unable to obtain specific port information, the UE shall send the unprotected REGISTER request to the SIP default port values as specified in RFC 3261 [26].

NOTE 1: The UE will only send further registration and subsequent SIP messages towards the same port of the P-CSCF for security mechanisms that do not require to use negotiated ports for exchanging protected messages.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains:

1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

2) the public user identity to be registered;

b) a To header field set to the SIP URI that contains:

1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

2) the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE:

1) supports GRUU (see table A.4, item A.4/53);

2) supports multiple registrations;

3) has an IMEI available; or

4) has an MEID available;

 the UE shall include a "+sip.instance" header field parameter containing the instance ID. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

 If the UE supports multiple registrations it shall include a "reg-id" header field parameter as described in RFC 5626 [92].

 The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62].

 The UE shall include the media feature tags defined in RFC 3840 [62] and RFC 5688 [120] for all supported streaming media types.

 If the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Contact URI without a user portion and containing the "bnc" URI parameter.

 If the UE has no specific reason not to include a user part in the URI of the contact address (eg. some UE performing the functions of an external attached network), the UE should include a user part in the URI of the contact address such that the user part is globally unique and does not reveal any private information;

NOTE 3: A time-based UUID (Universal Unique Identifier) generated as per subclause 4.2 of RFC 4122 [154] is globally unique and does not reveal any private information.

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDP is used. For TCP, the response is received on the TCP connection on which the request was sent. For the UDP, the UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223 [143];

NOTE 4: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 5: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

1) if GRUU is supported, the option-tag "gruu"; and

2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7;

NOTE 6: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and

k) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

a) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, the UE may initiate that mechanism on a media level when it initiates new media in an existing session.

NOTE 7: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header field value and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

NOTE 8: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the To header field will contain the main URI of the UE.

b) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header field and bind it to the respective contact address of the UE and the associated set of security associations or TLS session;

NOTE 9: When using the respective contact address and associated set of security associations or TLS session, the UE can utilize additional URIs contained in the P-Associated-URI header field and bound it to the respective contact address of the UE and the associated set of security associations or TLS session, e.g. for application purposes.

c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header field;

d) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session over which the REGISTER request was sent;

NOTE 10: When multiple registration mechanism is not used, there will be only one list of service route values bound to a contact address. However, when multiple registration mechanism is used, there will be different list of service route values bound to each registration flow and the associated contact address.

NOTE 11: The UE will use the stored list of service route values to build a proper preloaded Route header field for new dialogs and standalone transactions (other than REGISTER method) when using either the respective contact address or the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session.

e) if the UE indicated support for GRUU in the Supported header field of the REGISTER request then:

- if the UE did not use the procedures specified in RFC 6140 [191] for registration, find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered; and

- if the UE used the procedures specified in RFC 6140 [191] for registration then find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter then store the value of the "pub-gruu" header field parameter for use for generating public GRUUs for registering UAs as specified in RFC 6140 [191]. If this contains a "temp-gruu-cookie" header field parameter then store the value of the "temp-gruu-cookie" header field parameter for use for generating temporary GRUUs for registering UAs as specified in RFC 6140 [191];

NOTE 12: When allocating public GRUUs to registering UAs the functionality within the UE that performs the role of registrar will add an "sg" SIP URI parameter that uniquenly identifies that UA to the public GRUU it received in the "pub-gruu" header field parameter. The procedures for generating a temporary GRUU using the "temp-gruu-cookie" header field parameter are specified in subclause 7.1.2.2 of RFC 6140 [191].

f) if the REGISTER request contained the "reg-id" and "+sip.instance" Contact header field parameter and the "outbound" option tag in a Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field:

- if no option-tag "outbound" is present, the UE shall conclude that the S-CSCF does not support the registration procedure as described in RFC 5626 [92], and the S-CSCF has followed the registration procedure as described in RFC 5627 [93] or RFC 3261 [26], i.e., if there is a previously registered contact address, the S-CSCF replaced the old contact address and associated information with the new contact address and associated information (see bullet e) above). Upon detecting that the S-CSCF does not support the registration procedure as defined in RFC 5626 [92], the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626 [92]; or

NOTE 13: Upon replaces the old contact address with the new contact address, the S-CSCF performs the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5. Hence, the UE will receive a NOTIFY request informing the UE about the deregistration of the old contact address.

- if an option-tag "outbound" is present, the UE may establish additional IMS flows for the same private identity, as defined in RFC 5626 [92];

g) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session;

NOTE 14: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

h) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in RFC 6223 [143];

i) if the 200 (OK) response includes a Feature-Caps header field, as specified in RFC 6809 [190], with "+g.3gpp.icsi-ref" header field parameter, then the UE may consider the values included in the "+g.3gpp.icsi-ref" header field parameter of the Feature-Caps header field of 200 (OK) response as supported by the IM subsystem for the established registration or registration flow (if the multiple registration mechanism is used);

NOTE 15: The UE and related applications can use the ICSI values received in the Feature-Caps header field of 200 (OK) response to improve the user experience.

j) if the 200 (OK) response includes one or more Feature-Caps header fields containing the capability indicators listed in subclause 7.9A.7 that indicate the media capabilities supported by the IMS-AGW then the UE may consider this information when providing media options to the user or determining whether an application communication capability will be successful (e.g. if "sip.video" is not indicated then the UE might not offer the user the option to attempt to add video to the session); and

NOTE 16: If media capability indication is not supported, no capability indicators listed in subclause 7.9A.7 are included and it can be assumed that all the media capabilities are supported.

k) if the 200 (OK) response includes a Feature-Caps header field, as specified in RFC 6809 [190], with a "+g.3gpp.verstat" header field parameter and if the UE supports calling number verification status determination, determine that the home network supports calling number verification using signature verification and attestation information, as defined in subclause 3.1.

On receiving a 305 (Use Proxy) response to the unprotected REGISTER request, unless otherwise specified in access specific annexes (as described in annex B, annex L or annex U), the UE shall:

a) ignore the contents of the Contact header field if it is included in the received message;

NOTE 17: The 305 response is not expected to contain a Contact header field.

b) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

c) initiate either a new P-CSCF discovery procedure as described in subclause 9.2.1, or select a new P-CSCF, if the UE was pre-configured with more than one P-CSCF's IP addresses or domain names;

d) select a P-CSCF address, which is different from the previously used address, from the address list; and

e) perform the procedures for initial registration as described in subclause 5.1.1.2.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the registration expiration interval value with an expiration timer of at least the value received in the Min-Expires header field of the 423 (Interval Too Brief) response.

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) or 600 (Busy Everywhere) response or 403 (Forbidden) response for an initial registration, the UE may attempt to perform initial registration again.

When the timer F expires at the UE, the UE:

a) shall mark the currently used P-CSCF address as unavailable for the last duration of the retry delay time computed by the algorithm defined in subclause 4.5 of RFC 5626 [92] plus 5 minutes;

b) if there is a locally stored P-CSCF address as specified in subclause 5.1.9 which is different than the currently used P-CSCF address and which is not marked as unavailable, may initiate an initial registration as specified in subclause 5.1.1.2 using that P-CSCF; and

c) if there is no locally stored P-CSCF address as specified in subclause 5.1.9 which is different than the currently used P-CSCF address and which is not marked as unavailable, may get a new set of P-CSCF-addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in annex B, annex L or annex U) and initiate an initial registration as specified in subclause 5.1.1.2.

NOTE 18: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

On receiving a 4xx, 5xx (except 503) or 6xx response to the REGISTER request, whereby the response contains a Retry-After header field, the UE shall not automatically attempt an initial registration via the same IP-CAN and the same P-CSCF for the amount of time indicated in the Retry-After header field. If the UE is power cycled, the UE can attempt an initial registration. If no initial registration occurs within the time period indicated by the Retry-After header field, the counter of unsuccessful initial registration attempts is reset.

On receiving a 503 response with a Retry-After header field to the REGISTER request and the Retry-After header field indicates time bigger than the value for timer F as specified in table 7.7.1, the UE:

a) shall mark the currently used P-CSCF address as unavailable for the time indicated by the Retry-After header field;

b) if there is a locally stored P-CSCF address as specified in subclause 5.1.9 which is different than the currently used P-CSCF address and which is not marked as unavailable, may initiate an initial registration as specified in subclause 5.1.1.2 using that P-CSCF; and

c) if there is no locally stored P-CSCF address as specified in subclause 5.1.9 which is different than the currently used P-CSCF address and which is not marked as unavailable, may get a new set of P-CSCF addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in annex B, annex L or annex U) and initiate an initial registration as specified in subclause 5.1.1.2.

NOTE 19: if the Retry-After header field indicates time smaller than the value for timer F as specified in table 7.7.1, the UE continues using the currently used P-CSCF address.

After a first unsuccessful initial registration attempt, if the Retry-After header field was not present and the initial registration was not performed as a consequence of a failed reregistration, the UE shall not wait more than 5 minutes before attempting a new registration.

After a maximum of 2 consecutive unsuccessful initial registration attempts, if the Retry-After header field was not present in failure responses of those unsuccessful initial registration attempts, the UE shall start to implement the mechanism defined in subclause 4.5 of RFC 5626 [92] for determination of the retry delay time before each new registration attempt. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in subclause 4.5 of RFC 5626 [92]. If no values of the parameters max-time and base-time (if all failed) have been provided to the UE by the network, the default values defined in subclause 4.5 of RFC 5626 [92] shall be used.

The values of max-time and base-time (if all failed) may be provided by the network to the UE using OMA-DM with the management objects specified in 3GPP TS 24.167 [8G]. Other mechanisms may be used as well and are outside the scope of the present specification.

For each 4xx, 5xx or 6xx response received without a Retry-After header field to the REGISTER request, the UE shall:

a) mark the currently used P-CSCF address as unavailable for the last duration of the retry delay time computed by the algorithm defined in subclause 4.5 of RFC 5626 [92] plus 5 minutes; and

b) initiate an initial registration as specified in subclause 5.1.1.2 after the amount of time of the last retry delay time computed by the algorithm defined in subclause 4.5 of RFC 5626 [92]; and

- if there is a locally stored P-CSCF address as specified in subclause 5.1.9 which is different than the currently used P-CSCF address and which is not marked as unavailable, may initiate the initial registration using that P-CSCF; and

- if there is no locally stored P-CSCF address as specified in subclause 5.1.9 which is different than the currently used P-CSCF address and which is not marked as unavailable, may get a new set of P-CSCF addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in annex B, annex L or annex U) and initiate the initial registration as specified in subclause 5.1.1.2.

\* \* \* Next Change \* \* \* \*

##### 5.1.1.4.1 General

The UE can perform the reregistration of a previously registered public user identity bound to any one of its contact addresses and the associated set of security associations or TLS sessions at any time after the initial registration has been completed.

The UE can perform the reregistration of a previously registered public user identity over any existing set of security associations or TLS session that is associated with the related contact address.

The UE can perform the reregistration of a previously registered public user identity via an initial registration as specified in subclause 5.1.1.2, when binding the previously registered public user identity to new contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used).

The UE can perform registration of additional public user identities at any time after the initial registration has been completed. The UE shall perform the registration of additional public user identities either:

- over the existing set of security associations or TLS sessions, if appropriate to the security mechanism in use, that is associated with the related contact address; or

- via an initial registration as specified in subclause 5.1.1.2.

The UE can fetch bindings as defined in RFC 3261 [26] at any time after the initial registration has been completed. The procedure for fetching bindings is the same as for a reregistration except that the REGISTER request does not contain a Contact header field.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister an already registered public user identity either 600 seconds before the expiration time if the previous registration was for greater than 1200 seconds, or when half of the time has expired if the previous registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 [62] and RFC 5688 [120] or when the UE needs to modify the ICSI values that the UE intends to use in a g.3gpp.icsi-ref media feature tag or IARI values that the UE intends to use in the g.3gpp.iari-ref media feature tag.

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated either with the contact address or with the registration flow and the associated contact address used to send the request, see 3GPP TS 33.203 [19], established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains:

1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

2) the public user identity to be registered;

b) a To header field set to the SIP URI that contains:

1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

2) the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE:

1) supports GRUU (see table A.4, item A.4/53);

2) supports multiple registrations;

3) has an IMEI available; or

4) has an MEID available.

 Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 1: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

 If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62].

 If the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Contact URI without a user portion and containing the "bnc" URI parameter.

 If a user part has previously been included in an initial REGISTER request, the UE shall use the user part which was previously used to create the binding being refreshed or removed;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in RFC 6223 [143];

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and:

1) if GRUU is supported, the option-tag "gruu"; and

2) if multiple registrations is supported, the option-tag "outbound";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7;

NOTE 3: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and

k) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value either to the contact address or to the registration flow and the associated contact address used in this registration;

NOTE 4: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the To header field will contain the main URI of the UE.

b) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

NOTE 5: The stored list of service route values will be used to build a proper preloaded Route header field for new dialogs and standalone transactions (other than REGISTER method) when using either the respective contact address or the registration flow and the associated contact address (if the multiple registration mechanism is used).

NOTE 6: If the list of Service-Route headers saved from a previous registration and bound either to this contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 7: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) if the UE indicated support for GRUU in the Supported header field of the REGISTER request then:

- if the UE did not use the procedures specified in RFC 6140 [191] for registration find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered; and

- if the UE used the procedures specified in RFC 6140 [191]for registration then find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter then store the value of the "pub-gruu" header field parameter for use for generating public GRUUs for registering UAs as specified in RFC 6140 [191]. If this contains a "temp-gruu-cookie" header field parameter then store the value of the "temp-gruu-cookie" header field parameter for use for generating temporary GRUUs for registering UAs as specified in RFC 6140 [191];

NOTE 8: When allocating public GRUUs to registering UAs the functionality within the UE that performs the role of registrar will add an "sg" SIP URI parameter that uniquenly identifies that UA to the public GRUU it received in the "pub-gruu" header field parameter. The procedures for generating a temporary GRUU using the "temp-gruu-cookie" header field parameter are specified in subclause 7.1.2.2 of RFC 6140 [191].

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field and labelled with the "mediasec" header field parameter specified in subclause 7.2A.7, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session;

NOTE 9: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in RFC 6223 [143], towards the P-CSCF;

f) if the 200 (OK) response contains the Authentication-Info header field including a nextnonce field, store the contained nonce as a nonce for authentication 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 authentication for this registration or registration flow (if the multiple registration mechanism is used);

NOTE 10: The related registration flow or registration is identified by the couple instance-id and reg-id if the multiple registration mechanism is used or by contact address if not.

g) if the 200 (OK) response includes a Feature-Caps header field, as specified in RFC 6809°[190], with "+g.3gpp.icsi-ref" header field parameter, then the UE may consider the values included in the "+g.3gpp.icsi-ref" header field parameter of the Feature-Caps header field of 200 (OK) response as supported for the established registration or registration flow (if the multiple registration mechanism is used) according to RFC 6809 [190]; and

NOTE 11: The UE and related applications can use the ICSI values received in the Feature-Caps header field to improve the user experience.

h) if the 200 (OK) response includes one or more Feature-Caps header fields containing the capability indicators listed in subclause 7.9A.7 that indicate the media capabilities supported by the IMS-AGW then the UE may consider this information when providing media options to the user or determining whether an application communication capability will be successful (e.g. if "sip.video" is not indicated then the UE might not offer the user the option to attempt to add video to the session).

NOTE 12: If media capability indication is not supported, no capability indicators listed in subclause 7.9A.7 are included and it can be assumed that all the media capabilities are supported.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the registration expiration interval value with an expiration timer of at least the value received in the Min-Expires header field of the 423 (Interval Too Brief) response.

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) response or 403 (Forbidden) response for a reregistration, the UE shall perform the procedures for initial registration as described in subclause 5.1.1.2.

On receiving a 305 (Use Proxy) response to the REGISTER request, unless otherwise specified in the access specific annexes (as described in annex B, annex L or annex U), the UE shall:

a) ignore the contents of the Contact header field if it is included in the received message;

NOTE 13: The 305 response is not expected to contain a Contact header field.

b) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

c) initiate either a new P-CSCF discovery procedure as described in subclause 9.2.1, or select a new P-CSCF, if the UE was pre-configured with more than one P-CSCF's IP addresses or domain names;

d) select a P-CSCF address, which is different from the previously used address, from the address list; and

e) perform the procedures for initial registration as described in subclause 5.1.1.2.

When the timer F expires at the UE:

1) the UE shall stop processing of all ongoing dialogs and transactions associated with that flow, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs); and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2:

a) the UE may select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1 or from its pre-configured list of P-CSCF's IP addresses or domain names;

b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in annex B, annex L or annex U);

c) the UE may perform the procedures for initial registration as described in subclause 5.1.1.2; and

d) the UE shall perform the procedures in RFC 5626 [92] to form a new flow to replace the failed one if it supports multiple registrations. If failed registration attempts occur in the process of creating a new flow, the UE shall implement the flow recovery procedures defined in subclause 4.5 of RFC 5626 [92] for determination of the retry delay time before each new registration attempt. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in subclause 4.5 of RFC 5626 [92]. If no values of the parameters max-time and base-time (if all failed) have been provided to the UE by the network, the default values defined in subclause 4.5 of RFC 5626 [92] shall be used.

NOTE 14: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

\* \* \* Next Change \* \* \* \*

#### 5.1.3.1 Initial INVITE request

Where multiple domains exist for initiating a call/session, before sending an initial INVITE request, the UE shall perform access domain selection in accordance with the appropriate specification for the IP-CAN in use, taking into account the media to be requested. Access domain selection allows the policy of the network operator to be taken into account before the initial INVITE request is sent. Access dependent aspects of access domain selection are defined in the access technology specific annexes for each access technology.

Upon generating an initial INVITE request, the UE shall include the Accept header field with "application/sdp", the MIME type associated with the 3GPP IM CN subsystem XML body (see subclause 7.6.1) and any other MIME type the UE is willing and capable to accept.

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

The preconditions mechanism should be supported by the originating UE.

If the precondition mechanism is disabled as specified in subclause 5.1.5A, the UE shall not use the precondition mechanism.

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

NOTE 1: The originating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

In order to allow the peer entity to reserve its required resources, if the precondition mechanism is enabled as specified in subclause 5.1.5A; the originating UE supporting the precondition mechanism should make use of the precondition mechanism, even if it does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header field; and

- indicate the support for the preconditions mechanism and specify it using the Supported header field.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall not indicate the requirement for the precondition mechanism by using the Require header field.

During the session initiation, if the originating UE indicated the support for the precondition mechanism in the initial INVITE request and:

a) the received response with an SDP body includes a Require header field with "precondition" option-tag, the originating UE shall include a Require header field with the "precondition" option-tag:

- in subsequent requests that include an SDP body, that the originating UE sends in the same dialog as the response is received from; and

- in responses with an SDP body to subsequent requests that include an SDP body and include "precondition" option-tag in Supported header field or Require header field received in-dialog; or

b) the received response with an SDP body does not include the "precondition" option-tag in the Require header field,

- in subsequent requests that include an SDP body, the originating UE shall not include a Require or Supported header field with "precondition" option-tag in the same dialog;

- in responses with an SDP body to subsequent requests with an SDP body but without "precondition" option-tag in the Require or Supported header field, the originating UE shall not include a Require or Supported header field with "precondition" option-tag in the same dialog; and

- in responses with an SDP body to subsequent requests with an SDP body and with "precondition" option-tag in the Require or Supported header field, the originating UE shall include a Require header field with "precondition" option-tag in the same dialog.

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

NOTE 3: In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation after a 200 (OK) response has been received for the initial INVITE request, in case the terminating UE does not support the PRACK request (as described in RFC 3262 [27]) and does not support the UPDATE request (as described in RFC 3311 [29]).

NOTE 4: The UE can receive a P-Early-Media header field authorizing an early-media flow while the required preconditions, if any, are not met and/or the flow direction is not enabled by the SDP direction parameter. According to RFC 5009 [109], an authorized early-media flow can be established only if the necessary conditions related to the SDP negotiation are met. These conditions can evolve during the session establishment.

NOTE 5: When the UE is confirming the successful resource reservation using an UPDATE request (or a PRACK request) and the UE receives a 180 (Ringing) response or a 200 (OK) response to the initial INVITE request before receiving a 200 (OK) response to the UPDATE request (or a 200 (OK) response to the PRACK request), the UE does not treat this as an error case and does not release the session.

NOTE 6: The UE procedures for rendering of the received early media and of the locally generated communication progress information are specified in 3GPP TS 24.628 [8ZF].

If the UE wishes to receive early media authorization indications, as described in RFC 5009 [109], the UE shall add the P-Early-Media header field with the "supported" parameter to the initial INVITE request.

A UE supporting the Session Timer extension as described in RFC 4028 [58] may support the extension being configured using Session\_Timer\_Support node specified in 3GPP TS 24.167 [8G].

If the UE supports the Session Timer extension, the UE shall include the option-tag "timer" in the Supported header field and should either insert a Session-Expires header field with the header field value set to the configured session timer interval value, or should not include the Session-Expires header field in the initial INVITE request. The header field value of the Session-Expires header field may be configured using local configuration or using the Session\_Timer\_Initial\_Interval node specified in 3GPP 24.167 [8G]. If the UE is configured with both the local configuration and the Session\_Timer\_Initial\_Interval node specified in 3GPP 24.167 [8G], then the local configuration shall take precedence.

If the UE inserts the Session-Expires header field in the initial INVITE request, the UE may also include the "refresher" parameter with the "refresher" parameter value set to "uac".

When a final answer is received for one of the early dialogs, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogs to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and

2) send a BYE request to this dialog in order to terminate it.

Upon receiving a 488 (Not Acceptable Here) response to an initial INVITE request, the originating UE should send a new INVITE request containing SDP according to the procedures defined in subclause 6.1.

NOTE 7: An example of where a new request would not be sent is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resulting SDP would describe a session that did not meet the user requirements.

Upon receiving a 421 (Extension Required) response to an initial INVITE request in which the precondition mechanism was not used, including the "precondition" option-tag in the Require header field, if the UE supports the precondition mechanism and the precondition mechanism is enabled as specified in subclause 5.1.5A, the originating UE shall:

- send a new INVITE request using the precondition mechanism; and

- send an UPDATE request as soon as the necessary resources are available and a 200 (OK) response for the first PRACK request has been received.

Upon receiving a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header field, then the originating UE shall not automatically reattempt the request via the same P-CSCF until after the period indicated by the Retry-After header field contents.

The UE may include a "cic" tel URI parameter in a tel URI, or in the userinfo part of a SIP URI with user=phone, in the Request-URI of an initial INVITE request if the UE wants to identify a user-dialed carrier, as described in RFC 4694 [112].

NOTE 8: The method whereby the UE determines when to include a "cic" tel-URI parameter and what value it should contain is outside the scope of this document (e.g. the UE could use a locally configured digit map to look for special prefix digits that indicate the user has dialled a carrier).

NOTE 9: The value of the "cic" tel-URI parameter reported by the UE is not dependent on UE location (e.g. the reported value is not affected by roaming scenarios).

In the event the UE receives a 380 (Alternative Service) response to an initial INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry of the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), the UE shall select a domain in accordance with the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B], and:

- if the CS domain is selected, the UE behavior is defined in subclause 7.1.2 of 3GPP TS 23.167 [4B] and, where appropriate, in the access technology specific annex; and

- if the IM CN subsystem is selected, the UE shall apply the procedures in subclause 5.1.6 with the exception of selecting a domain for the emergency call attempt.

NOTE 10: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

Upon receiving a 199 (Early Dialog Terminated) provisional response to an established early dialog the UE shall release resources specifically related to that early dialog.

The UE shall include the media feature tags defined in RFC 3840 [62] and RFC 5688 [120] for all supported streaming media types in the initial INVITE request.

If the UE sends a CANCEL request to cancel an initial INVITE request, the UE shall when applicable include in the CANCEL request a Reason header field with a protocol value set to "RELEASE\_CAUSE" and a "cause" header field parameter as specified in subclause 7.2A.18.11.2. The UE may also include the "text" header field parameter with reason-text as specified in subclause 7.2A.18.11.2.

Upon receiving a 500 (Server Internal Error) response to an initial INVITE request including a Reason header field with a protocol value set to "FAILURE\_CAUSE" and a cause header field parameter value set to "1" as specified in subclause 7.2A.18.12.2 and a Response-Source header field with a "fe" header field parameter set to "<urn:3gpp:fe:p-cscf.orig>", the UE can determine that the QoS or bearer resources in the originating IP-CAN is not available.

#### 5.1.4.1 Initial INVITE request

The preconditions mechanism should be supported by the terminating UE.

The handling of incoming initial INVITE requests at the terminating UE is mainly dependent on the following conditions:

- the specific service requirements for "integration of resource management and SIP" extension (hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by RFC 4032 [64], and with the request for such a mechanism known as a precondition);

- the UEs configuration for the case when the specific service does not require the precondition mechanism; and

- the precondition disabling policy specified in subclause 5.1.5A, if supported by the UE.

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

During the session initiation, if local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field or Require header field and the precondition mechanism is enabled as specified in subclause 5.1.5A, the terminating UE shall use the precondition mechanism and shall include a Require header field with the "precondition" option-tag:

- in responses to that INVITE request if those responses include an SDP body;

- in responses to subsequent requests received in-dialog that include an SDP body and include "precondition" option-tag in Supported header field or Require header field; and

- in subsequent requests that include an SDP body, that it sends towards the originating UE during the session initiation;

b) the received INVITE request includes the "precondition" option-tag in the Supported header field, and the precondition mechanism is disabled as specified in subclause 5.1.5A, the terminating UE shall not use the precondition mechanism:

c) the received INVITE request includes the "precondition" option-tag in the Require header field, and the precondition mechanism is disabled as specified in subclause 5.1.5A, the terminating UE shall reject the INVITE request with a 420 (Bad Extension) response; and

d) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not use the precondition mechanism.

During the session initiation, if local resource reservation is not required by the terminating UE and the terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field and:

i) the required resources at the originating UE are not reserved, and the precondition mechanism is enabled as specified in subclause 5.1.5A, the terminating UE shall use the precondition mechanism and shall include a Require header field with the "precondition" option-tag:

- in responses to that INVITE request if those responses include an SDP body;

- in responses with an SDP body to subsequent requests received in-dialog that include an SDP body and include "precondition" option-tag in Supported header field or Require header field; and

- in subsequent requests that include an SDP body, that it sends towards the originating UE during the session initiation;

ii) the required local resources at the originating UE and the terminating UE are available and the precondition mechanism is enabled as specified in subclause 5.1.5A, the terminating UE may use the precondition mechanism; and

iii) the precondition mechanism is disabled as specified in subclause 5.1.5A, the terminating UE shall not use the precondition mechanism;

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not use the precondition mechanism;

c) the received INVITE request includes the "precondition" option-tag in the Require header field and the precondition mechanism is enabled as specified in subclause 5.1.5A, the terminating UE shall use the precondition mechanism; and

d) the received INVITE request includes the "precondition" option-tag in the Require header field, and the precondition mechanism is disabled as specified in subclause 5.1.5A, the terminating UE shall reject the INVITE request with a 420 (Bad Extension) response.

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26].

NOTE 3: If the terminating UE does not support the precondition mechanism it will apply regular SIP session initiation procedures.

If the received INVITE request indicated support for reliable provisionable responses, but did not require their use and the terminating UE supports reliable provisional responses, and if:

a) the terminating UE requires a reliable alerting indication at the originating side;

b) the 18x response (other than 183 response) carries SDP or for other application related purposes that requires its reliable transport; or

c) the reliable 18x policy indicates (see subclause 5.1.4.2) the UE to do so;

the terminating UE shall send the 18x response (other than 183 response) reliably.

NOTE 4: If the terminating UE is configured by the home operator to send the 18x response (other than 183 response) reliably and the received INVITE request did not indicate support for reliable provisional responses, then the terminating UE sends the 18x response (other than 183 response) unreliably.

The terminating UE shall send the 18x responses (other than 183 response) unreliably if the reliable 18x policy (see subclause 5.1.4.2) indicates the UE to do so, unless the received INVITE request requires to use reliable provisional responses.

NOTE 5: Certain applications, services and operator policies might mandate the terminating UE to send a 199 (Early Dialog Terminated) provisional response (see RFC 6228 [142]) prior to sending a non-2xx final response to the INVITE request.

If the terminating UE uses the precondition mechanism, upon successful reservation of local resources:

- if the originating side requested confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE, the terminating UE shall confirm the successful resource reservation (see subclause 6.1.3) within an SIP UPDATE request; and

NOTE 6: Originating side requests confirmation for the result of the resource reservation at the terminating UE e.g. when an application server performs 3rd party call control. The request for confirmation for the result of the resource reservation at the terminating UE can be included e.g. in the SDP answer in the PRACK request.

- if the originating side did not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE, the terminating UE shall not confirm the successful resource reservation (see subclause 6.1.3) within an UPDATE request.

NOTE 7: The terminating UE can send an UPDATE request for reasons other than confirmation of the successful resource reservation.

If the terminating UE included an SDP offer or an SDP answer in a reliable provisional response to the INVITE request and both the terminating UE and the originating UE support UPDATE method, then in order to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE shall send an UPDATE request with a new SDP offer and delays sending of 200 (OK) response to the INVITE request till after reception of 200 (OK) response to the UPDATE request.

If the user does not accept a media stream accepted in the SDP answer and the terminating UE, the originating UE or both do not support the UPDATE method, then after reception of ACK request related to 200 (OK) response to the INVITE request, the UE shall modify the session.

The terminating UE shall include the media feature tags defined in RFC 3840 [62] and RFC 5688 [120] for all supported streaming media types in the SIP response other than the 100 (Trying) response to the SIP INVITE request.

If the received INVITE request was received over a registration for which the 200 (OK) contained a Feature-Caps header field including the "+sip.607" header field parameter the UE may send a 607 (Unwanted) response as specified in RFC 8197 [254].

NOTE 8: 607 (Unwanted) response is normally sent after user interaction.

If the terminating UE supports the Session Timer extension, as described in RFC 4028 [58], and if the received INVITE request includes the "timer" option tag in the Supported header field, then the terminating UE shall behave as described in RFC 4028 [58] with the following clarification:

- If the received INVITE request does not contain the Session-Expires header field, then the terminating UE shall include a Session-Expires header field with the header field value set to the greater of the configured session timer interval value or the value contained in the Min-SE header field (if present, in the received INVITE), and the "refresher" parameter set to the configured "refresher" parameter value in the 200 (OK) response to the INVITE request. The session timer interval value may be configured using local configuration or the Session\_Timer\_Initial\_Interval node specified in 3GPP 24.167 [8G]. If the UE is configured with both the local configuration and the Session\_Timer\_Initial\_Interval node, then the local configuration shall take precedence. The"refresher" parameter value may be configured using local configuration or using the Session\_Timer\_Initial\_MT\_Refresher node specified in 3GPP 24.167 [8G]. If the UE is configured with both the local configuration and the Session\_Timer\_Initial\_MT\_Refresher node, then the local configuration shall take precedence;

- If the received INVITE request includes the "timer" option tag in the Supported header field and contains the Session-Expires header field without "refresher" parameter, then the terminating UE shall include a Session-Expires header field with the "refresher" parameter set to the configured "refresher" parameter value in the 200 (OK) response to the INVITE request, and shall set the header field value of the Session-Expires header field of the 200 (OK) response to the INVITE request to the value received in the INVITE request. The "refresher" parameter value may be configured using local configuration or using the Session\_Timer\_Initial\_MT\_Refresher node specified in 3GPP 24.167 [8G]. If the UE is configured with both the local configuration and the Session\_Timer\_Initial\_MT\_Refresher node specified in 3GPP 24.167 [8G], then the local configuration shall take precedence; or

- If the received INVITE request contains the Session-Expires header field with "refresher" parameter, then the terminating UE shall include a Session-Expires header field with the "refresher" parameter set to the received "refresher" parameter value in the 200 (OK) response to the INVITE request, and shall set the header field value of the Session-Expires header field of the 200 (OK) response to the INVITE request to the value received in the INVITE request.

\* \* \* End of Changes \* \* \* \*