**3GPP TSG-CT WG1 Meeting #141eC1-23xxxx**

**Online 17– 21 April 2023 Revision of C1-232103**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **Current version:** | **1** |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | IMS DC capability negotiation | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | China Mobile, Huawei, HiSilicon, ZTE | | | | | | | | | |
| ***Source to TSG:*** | CT1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | NG\_RTC | | | | |  | ***Date:*** | | | 2023-03-20 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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 can be 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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | S2-2303216 (CR 1268 to TS 23.228) specifies how UE and IMS network negotiate the DC capability of each other. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is proposed to specify how UE negotiates the DC capability of IMS network. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The UE cannot be aware of whether or not the IMS network supports data channel capability. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.1.1.2.1; 5.4.1.2.2F; 7.9A.1X (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **N** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **N** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **N** | 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, for the data channel capability it shall use +sip.app-subtype="webrtc-datachannel" as specified in 3GPP TS 26.114 [9B].

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 a Feature-Caps header field, as specified in RFC 6809 [190] is received, a UE supporting the Feature-Caps header field shall consider the ICSI values received in 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) void;

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; and

l) if the 200 (OK) response includes a Feature-Caps header field, as specified in RFC 6809 [190], with a +sip.app-subtype="webrtc-datachannel" header field parameter and if UE supports data channel capability, determine that the home network supports the data channel capability as specified in 3GPP TS 26.114 [9B].

NOTE 16: If the home network doesn't support the data channel capability, the UE will not include data channel related media description in SDP offers.

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 from 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 from 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 from 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 from 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.

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

a) use the mechanism defined in subclause 4.5 of RFC 5626 [92] for determination of the retry delay time before each new registration attempt;

b) 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

c) 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 from 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 from 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.

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

NOTE 20: If the UE stops initiating initial registration, the UE can attempt to perform initial registration with the network again based on the local configuration and not wait till power-cycled. The local configuration is outside the scope of this specification.

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

##### 5.4.1.2.2F Successful registration

If a 200 (OK) response is to be sent for a REGISTER request, the S-CSCF shall, in addition to any contents identified elsewhere in subclause 5.4.1.2, include:

a) the list of received Path header fields;

b) a P-Associated-URI header field containing the list of the registered distinct public user identity and its associated set of implicitly registered distinct public user identities. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be a registered public user identity. The S-CSCF shall place the default public user identity as the first entry in the list of URIs present in the P-Associated-URI header field. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header field, as described in subclause 5.2.6.3. If the S-CSCF received a display name from the HSS for a public user identity, then the S-CSCF shall populate the P-Associated-URI header field entry for that public identity with the associated display name. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header field;

NOTE 1: The P-Associated-URI header field lists only the public user identity and its associated set of implicitly registered public user identities that have been registered, rather than the list of user's URIs that may be either registered or unregistered as specified in RFC 7315 [52]. If the registered public user identity which is not barred does not have any other associated public user identities or wildcarded public user identities, the P-Associated-URI header field lists only the registered public user identity itself. The P-Associated-URI header field does not list wildcarded public user identities.

c) a Service-Route header field containing:

A) the SIP URI identifying the S-CSCF containing an indication that subsequent requests routed via this service route (i.e. from the P-CSCF to the S-CSCF) was sent by the UE using either the contact address of the UE or the registration flow and the associated contact address (if the multiple registration mechanism is used) that has been registered and are treated as for the UE-originating case.

NOTE 2: This indication can e.g. be in a parameter in the URI, a character string in the user part of the URI or be a port number in the URI.

The S-CSCF shall use a different SIP URI for each registration. If the multiple registration mechanism is used, the S-CSCF shall also use a different SIP URI for each registration flow associated with the registration;

B) if network topology hiding is required a SIP URI identifying an IBCF as the topmost entry; and

NOTE 3: In accordance with the procedures described in RFC 3608 [38], an IBCF does not insert its own routable SIP URI to the Service-Route header field.

C) if

1) S-CSCF supports indicating the traffic leg associated with a URI as specified in RFC 7549 [225];

2) the UE is roaming;

3) the P-CSCF is not in the home network; and

4) required by local policy

then the S-CSCF may append an "iotl" SIP URI parameter with a value set to "visitedA-homeA" to the S-CSCF SIP URI in the Service-Route header field;

d) if the P-CSCF is in the same network as the S-CSCF a P-Charging-Function-Addresses header field containing the values received from the HSS. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request;

NOTE 4: The P-CSCF does not check the P-Charging-Function-Addresses header field, providing this header field to the visiting network could cause undefined charging behaviour.

e) a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the REGISTER request, a type 1 "term-ioi" header field parameter and the "icid-value" header field parameter. The S-CSCF shall set the type 1 "term-ioi" header field parameter to a value that identifies the sending network of the response, the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter and the "icid-value" header field parameter is set to the previously received value of "icid-value" header field parameter in the request;

f) a Contact header field listing all contact addresses for this public user identity, including all saved header field parameters and URI parameters (including all ICSI values and IARI values) received in the Contact header field of the REGISTER request,

g) GRUUs in the Contact header field. If the REGISTER request contained a Required or Supported header field containing the value "gruu" then for each contact address in the Contact header field that has a "+sip.instance" header field parameter:

i) add "pub-gruu" header field parameter containing the public GRUU representing (as specified in subclause 5.4.7A.2) the association between the public user identity from the To header field in the REGISTER request and the instance ID contained in the "+sip.instance" header field parameter;

ii) if the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then add a "temp-gruu" header field parameters. containing the most recently assigned temporary GRUU representing (as specified in subclause 5.4.7A) the association between the public user identity from the To header field in the REGISTER request and the instance ID contained in the "+sip.instance" header field parameter; and

iii) if the S-CSCF supports RFC 6140 [191] and the Contact URI in the Contact header field contains a "bnc" URI parameter, then add a "temp-gruu-cookie" header field parameter containing a value generated as specified in RFC 6140 [191];

h) if the received REGISTER request contained both a "reg-id" and "+sip.instance" header field parameters in the Contact header field, and the first URI within the Path header field contains the "ob" SIP URI parameter a Require header field with the "outbound" option-tag as described in RFC 5626 [92];

NOTE 5: There might be other contact addresses available, that this UE or other UEs have registered for the same public user identity.

i) void

j) optionally, a Feature-Caps header field including the ICSI values contained in the service profile of the served user except the ones that require explicit support indication of capabilities by intermediary entities and that have not been indicated as supported according to RFC 6809 [190] for the corresponding registration or registration flow (if multiple registration mechanism is used);

k) if the home network supports calling number verification using signature verification and attestation information, as defined in subclause 3.1,a Feature-Caps header field, as specified in RFC 6809 [190], including the "+g.3gpp.verstat" header field parameter;

NOTE 6: If the network has indicated support for the calling number verification using signature verification and attestation information to a UE during registration, the network needs to perform calling number verification for all calls delivered to the registered contact address.

l) if the home network supports the response code 607 (Unwanted) as specified in RFC 8197 [254], a Feature-Caps header field including the "+sip.607" header field parameter; and

m) if the home network supports the data channel capability as specified in 3GPP TS 26.114 [9B], and the UE has indicated support of the IMS data channel in the REGISTER request, a Feature-Caps header field, as specified in RFC 6809 [190], including the +sip.app-subtype="webrtc-datachannel" header field parameter.

and send the so created 200 (OK) response to the UE.

For all service profiles in the implicit registration set, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria of the service profile from the HSS for the REGISTER event; and,

NOTE 7: If this registration is a reregistration, the Filter Criteria already exists in the local data.

NOTE 8: If the same AS matches the Filter Criteria of several service profiles for the event of REGISTER request, then the AS will receive several third-party REGISTER requests. Each of these requests will include a public user identity from the corresponding service profile.

The S-CSCF shall consider the public user identity being registered to be bound either to the contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used), as specified in the Contact header field, for the duration indicated in the registration expiration interval value.

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

### 7.9A.1X Definition of feature-capability indicator +sip.app-subtype="webrtc-datachannel"

Editor's note: [NG\_RTC, CR#6587] this feature-capability indicator is to be registered with IANA when release 18 is completed.

Feature-capability indicator name: +sip.app-subtype="webrtc-datachannel"

Summary of the feature indicated by this feature-capability indicator:

This feature-capability indicator can be included in a Feature-Caps header field as specified in RFC 6809 [190] in a 200 (OK) response to the REGISTER request, with the same value as in the +sip.app-subtype="webrtc-datachannel" media feature tag in the Contact header of the REGISTER request, indicates that the home network supports data channel capability as specified in 3GPP TS 26.114 [9B].

Feature-capability indicator specification reference: 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature-capability indicator: Not applicable

The feature-capability indicator is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature-capability indicator is used to indicate the support of data channel capability.

Examples of typical use: Indicating the support of data channel capability in the home network.

Security Considerations: Security considerations for this feature-capability indicator are discussed in clause 9 of RFC 6809.

\* \* \* End of Change \* \* \* \*