Start of first changes

5.1.2 Subscription and notification

5.1.2.1 Notification about multiple registered public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the UE shall maintain the generated dialog (identified by the values of the Call-ID, To and From headers).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the registration-state event package the UE shall perform the following actions:

- if a registration state value "open", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;
- if a registration state value "closed", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered.

NOTE: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE, i.e. the UE does not know that they have been registered. The implicitly registered public user identities may also belong to different service profiles. The here-described procedures provide a mechanism to inform the UE about these automatically registered public user identities.

End of first changes

Start of second changes

5.4 Procedures at the S-CSCF

5.4.1 Registration and authentication

5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs of the IM CN subsystem with public user identities.

The S-CSCF shall support the use of the Path and P-Service-Route header. The S-CSCF must also support the Require and Supported headers. The Path header is only applicable to the REGISTER request and its 200 (OK) response. The P-Service-Route header is only applicable to the 200 (OK) response of REGISTER.

The network operator defines minimum and maximum times for each registration. These values are provided within the S-CSCF.

The procedures for notification concerning automatically registered public user identities of a user are described in subclause 5.4.2.1.2.

End of second changes

Start of third changes

5.4.1.2.2 User-initiated reregistration

Upon receipt of a REGISTER request for an already registered user, the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the From header of the REGISTER request;

2) check whether the P-CSCF included the Integrity-protection field of the Authorization header set to yes, indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps if the field is set to yes;

3) check if the user needs to be reauthenticated.

   The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for registration requests received without integrity protection by the P-CSCF. The information that a REGISTER request was received integrity protected at the P-CSCF may be used as part of the decision to challenge the user.

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph;

4) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall proceed with the procedures as described for the second REGISTER in subclause 5.4.1.2, beginning with step 7); and

5) remove the P-Access-Network-Info header and may act upon the contents accordingly.

5.4.1.2.3 Abnormal cases

The S-CSCF need not challenge an unprotected REGISTER request for a private user identity that already has a registration in process, but instead return a 500 (Server Internal Error) response. The response shall contain a Retry-After header with a value indicating a time the UE shall wait before resending the request.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by an initial registration or a UE initiated reauthentication, the S-CSCF shall either:

- start a network initiated re-authentication procedure as defined in subclause 5.4.1.6; or

- send a further challenge 401 (Unauthorized) to the UE.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by a network initiated reauthentication the S-CSCF shall either:

- attempt a further authentication challenge; or

- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid and with no RES or AUTS parameter, the S-CSCF shall:

- respond with the relevant 4xx response (e.g. 401 (Unauthorized) to initiate a further authentication attempt, or 403 (Forbidden) if the authentication attempt is to be abandoned).

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid but contains the AUTS parameter, the S-CSCF will fetch new authentication vectors from the HSS, including AUTS and RAND in the request to indicate a resynchronisation. On receipt of these vectors from the HSS, the S-CSCF shall:

- send a 401 Unauthorized to initiate a further authentication attempt, using these new vectors.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

5.4.1.3 Authentication and reauthentication

Authentication and reauthentication is performed by the registration procedures as described in subclause 5.4.1.2.

5.4.1.4 User-initiated deregistration

When S-CSCF receives a REGISTER request with the Expires header field containing the value zero, the S-CSCF shall:

- deregister the public user identity found in the To header field together with the implicitly registered public user identities;

- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

Based on operators' policy the S-CSCF can request from HSS to either be kept or cleared as the S-CSCF allocated to this subscriber. In both cases the state of the subscriber identity is stored as unregistered in the HSS and the S-CSCF. Based on HSS decision, the S-CSCF may either keep all or only a part of the user profile or removes it.

5.4.1.5 Network-initiated deregistration

When a network-initiated deregistration event occurs for a public user identity, and the UE has subscribed for the registration-state event, the S-CSCF shall generate a NOTIFY request in order to inform the UE of the network-initiated deregistration event for that public user identity. The S-CSCF shall set the event header to the name of the event package, which provides information about the registration state of the UE.

When a network-initiated deregistration event occurs for a public user identity, and the P-CSCF has subscribed for registration events for that public user identity, the S-CSCF shall generate a NOTIFY request in order to inform the P-CSCF of the network initiated deregistration event for that public user identity. The S-CSCF shall set the event header to the name of the event package, which provides information about the registration state of the UE.

If the network-initiated deregistration is for a set of public user identities associated with the subscriber, the NOTIFY shall send the registration state of all public user identities of the subscriber.

Editor's note: The possible values of the event header are: presence, registration-state, a new subpackage of presence.

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

The S-CSCF shall then deregister the public user identity together with the implicitly registered public user identities.

5.4.1.6 Network-initiated reauthentication

The S-CSCF may request a subscriber to reauthenticate at any time, based on a number of possible operator settable triggers as described in subclause 5.4.1.2.

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs (i.e. the dialog between S-CSCF and the UE and additionally between S-CSCF and P-CSCF) which have been established due to subscription to the registration-state event package of that user. The S-CSCF shall populate the content of the NOTIFY request and additionally shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "registration-state" value; and
- indicate a public user identity of the user for which the private user identity needs to be re-authenticated in the body of the NOTIFY request with registration state "re-authenticate".

Afterwards the S-CSCF shall:

- wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE: Network initiated re-authentication might be requested from the HSS or may occur due to internal processing within the S-CSCF.

In case S-CSCF receives no data it can authenticate the subscriber from, the S-CSCF may as an implementation option try to request the UE by other means to re-authenticate, e.g. by sending a REFER method in order to request a REGISTER request.

When generating the NOTIFY request, the S-CSCF shall shorten the validity of subscriber's registration timer to an operator defined value that will allow the user to be re-authenticated. If user fails to reauthenticate while its registration is still valid, the S-CSCF shall deregister the private user identity as described in subclause 5.4.1.5 and terminate the ongoing sessions of that user.

5.4.1.7 Notification of Application Servers about registration status

If the registration procedure described in subclauses 5.4.1.2, 5.4.1.4 or 5.4.1.5 (as appropriate) was successful, the S-CSCF shall send a third-party REGISTER request to each Application Server with the following information:

a) the Request-URI shall contain the AS's SIP URL;

b) the From header shall contain the S-CSCF's SIP URL;

c) the To header shall contain the public user identity as contained in the REGISTER request received form the UE;

d) the Contact header shall contain the S-CSCF's SIP URL;

e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header shall contain the same value that the S-CSCF returned in the 200 (OK) response for the REGISTER request received form the UE;

f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header shall contain the value zero;

g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body shall be included in the REGISTER request if there is Filter Criteria indicating the need to include HSS provided data for the REGISTER event (e.g. HSS may provide AS specific data to be included in the third-party REGISTER, such as IMSI to be delivered to IM SSF). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then it shall be included in the message body of the REGISTER request within the <service-info> XML element as described in subclause 7.6. For the messages including the 3GPP IMS XML body, set the value of the Content-Type header to include the MIME type specified in subclause 7.6;

h) for initial registration, the P-Charging-Vector header shall contain the same icid parameter that the S-CSCF received in the original REGISTER request from the UE;

i) for initial registration, a P-Charging-Function-Addresses header (see subclause 7.2.5) shall be populated with values received from the HSS if the message is forwarded within the S-CSCF home network.

5.4.2 Subscription and notification

5.4.2.1 Subscriptions to S-CSCF events

5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header with the registration-state event package, the S-CSCF shall generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the subscription was successful. Furthermore, the response shall include:

- an Expires header which either contains the same or a decreased value as the Expires in SUBSCRIBE request; and
- a Contact header which is an identifier generated within the S-CSCF that will help to correlate refreshes for the SUBSCRIBE.

Afterwards the S-CSCF shall perform the procedures for notification about registration state as described in subclause 5.4.2.1.2.

5.4.2.1.2 Notification about registration state

Notification of the registration state shall affect the non-barred public user identities. The barred public user identities shall never be sent in a NOTIFY message.

If the registration state of one or more public user identities changes, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the registration-state event package of that user. For each NOTIFY request, the S-CSCF shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "registration-state" value;
- indicate registration state "open" for all public user identities which are currently registered;
- indicate registration state "closed" for all public user identities which are currently deregistered; and
- indicate within the "<note>" information of those public user identities which will be automatically reregistered the "automatically by" information, followed by the specific public user identity which will cover the reregistration.

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<tuple name="sip:user1_public1@home1.net">
   <status><basic>open</basic><<<</status>
</tuple>

<tuple name="sip:user1_public2@home1.net">
   <status> <basic>open</basic> </status>
   <note>automatically by sip:user1_public1@home1.net</note>
</tuple>
```

Afterwards the S-CSCF shall send the generated NOTIFY request on the dialog and await a 2xx response.

5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

5.4.3.1 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a refresh request or a stand-alone transaction, the S-CSCF shall:

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Path header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,

- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

5.4.3.2 Requests initiated by the served user

When the S-CSCF receives from the served user an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

- determine whether the request contains a barred public user identity in the From or Remote-Party-ID header fields of the request or not. In case any of the said header fields contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps;

- remove its own SIP URL from the topmost Route header;

- if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [22]) to a globally routeable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or an appropriate SIP response shall be sent to the originator;

- check if P-Original-Dialog-ID header is present in the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The od-to-tag, od-from-tag and od-call-idparameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID header in the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request;

- check whether the initial request matches the initial filter criteria based on a public user identity in the P-Asserted-Identity header~~from the service profile associated with the received public user identity~~, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and

  - populate the P-Original-Dialog-ID header in the message with the original To tag, From tag and Call-ID headers received in the request. See subclause 7.2.7 for further information on the original dialog identifier;

- store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

- insert an ioi-originating parameter into the P-Charging-Vector header if the next hop is an AS, I-CSCF or outside of the current network. The ioi-originating parameter shall be set to a value that identifies the sending network. The ioi-terminating parameter shall not be included;

- insert a P-Charging-Function-Addresses header (see subclause 7.2.5) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

- in the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

- in the case where the network operator has policy to provide privacy on From headers, and such privacy is required for this dialog, change the From header to "Anonymous". Network policy may also require the removal of the display field;

- determine the destination address (e.g. DNS access) using the URL placed in the topmost Route header if present, otherwise based on the Request-URI;

- if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header;

- in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed;

- remove the P-Access-Network-Info header and act upon the contents accordingly; and

- route the request based on SIP routeing procedures.

When the S-CSCF receives any response to the above request, the S-CSCF may:

- apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header.

NOTE 1: This header would normally only be expected in 1xx or 2xx responses.

NOTE 2: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

When the S-CSCF receives a response to the initial request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog if needed.

When the S-CSCF receives from the served user a refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- remove its own URL from the topmost Route header;

- create a Record-Route header containing its own SIP URL and save the Contact header from the request in order to release the dialog when needed;

- remove the P-Access-Network-Info header and act upon the contents accordingly; and

- route the request based on the topmost Route header.

When the S-CSCF receives a response to the refresh request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog if needed.

When the S-CSCF receives from the served user a subsequent request other than refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- remove its own URL from the topmost Route header;

- remove the P-Access-Network-Info header and act upon the contents accordingly; and

- route the request based on the topmost Route header.

5.4.3.3 Requests terminated at the served user

When the S-CSCF receives, destined for a registered served user, an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

1) remove its own URL from the topmost Route header;

2) check if P-Original-Dialog-ID header is present in the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The od-to-tag, od-from-tag and od-call-id parameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. The S-CSCF shall determine the next hop using initial filter criteria. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-

Dialog-ID header in the message of the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request;

3) check whether the initial request matches the initial filter criteria based on the public user identity in the Request-URI~~from the service profile associated with the received public user identity~~, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

   a) insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and

   b) populate the P-Original-Dialog-ID header in the message with the original To tag, From tag and Call-ID headers received in the request. See subclause 5.4.3.4 for further information on the original dialog identifier;

4) insert a P-Charging-Function-Addresses header (see subclause 7.2.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

5) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;

6) store the value of the ioi-originating parameter received in the P-Charging-Vector header, if present. The ioi-originating parameter identifies the sending network of the request message. The ioi-originating parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;

7) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2;

8) build the Route header field with the values determined in the previous step;

9) determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2;

10) build a Request-URI with the contents of the saved Contact URL determined in the previous step;

11) insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;

12) in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed; and

13) optionally, apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header; and

NOTE: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

14) forward the request based on the topmost Route header.

When the S-CSCF receives, destined for an unregistered user, an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall:

1) execute the procedures described in the steps 1 and 2 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);

2) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14];

3) keep the user registration status as unregistered for the duration of the dialog. When the dialog expires, the S-CSCF shall inform appropriately the HSS according to the procedures described in 3GPP TS 29.228 [14];

4) execute the procedure described in step 3 and 4 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

In case that no AS needs to be contacted, then S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures; and

5) execute the procedures described in the steps 5, 6, 11, 12, 13 and 14 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

When the S-CSCF receives a response to the initial request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed. In the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URI; in the case where the network operator has policy to provide privacy on To headers, and such privacy is required for this dialog, change the To header to "Anonymous". Network policy may also require the removal of the display field.

When the S-CSCF receives, destined for a served user, a refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

1) remove its own URL from the topmost Route header;

2) create a Record-Route header containing its own SIP URL and save the Contact header from the refresh request in order to release the dialog when needed;

3) remove the P-Access-Network-Info header, if it is present, and may act upon its contents accordingly; and

4) forward the request based on the topmost Route header.

When the S-CSCF receives a response to the refresh request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed.

When the S-CSCF receives, destined for the served user, a subsequent request other than refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

1) remove its own URL from the topmost Route header; and

2) forward the request based on the topmost Route header.

When the S-CSCF receives a request destined for a barred public user identity, the S-CSCF shall return an appropriate unsuccessful SIP response. This response may be, e.g., a 404 (Not found) or 604 (Does not exist anywhere).

5.4.3.4 Original dialog identifier

The original dialog identifier is coded as the P-Original-Dialog-ID as described in subclause 7.2.7.

5.4.3.5 Abnormal cases

The S-CSCF shall, when contacting application servers based on the initial filter criteria, expect either a final response from the application server as the session terminates there, or the initial request message, that may be modified. In either case the message should be identified (using P-Original-Dialog-ID) as belonging to the original request forwarded by the S-CSCF.

If the S-CSCF receives a message including an P-Original-Dialog-ID that does not match any that it has forwarded to the application server it shall:

- respond to the application server with 481 Call Leg/Transaction Does Not Exist.

End of ~~second~~ third changes