3GPP TSG SA WG3 Security ó S3#36 **S3-041061**
November 23-26, 2004, Shenzhen, China

CR-Form-v7.1

PSEUDO CHANGE REQUEST

⌘ **33.878** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.0.3** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: | UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Detailed specification of registration and authentication procedures based on LS from CN1 (S3-041048)
Source:	⌘	Vodafone
Work item code:	⌘	Early IMS
Date:	⌘	23/11/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction 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.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	Some detail of the registration and authentication procedures is missing.
Summary of change:	⌘	Addition of detailed specification of registration and authentication procedures based on LS from CN1 (S3-041048).
Consequences if not approved:	⌘	Incomplete specifications.

Clauses affected:	⌘	2, 7.2.3, 7.2.4

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 23.981: " Interworking aspects and migration scenarios for IPv4 based IMS Implementations ".

[2] 3GPP TS 33.203: " Access security for IP-based services ".

[3] 3GPP TS 23.228: " IP Multimedia Subsystem (IMS); Stage 2 ".

[4] 3GPP TS 29.061: " Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) ".

[5] 3GPP TS 23.060: " General Packet Radio Service (GPRS); Service description; Stage 2 ".

[6] IETF RFC 3261: " Session Initiation Protocol ".

[7] 3GPP TS 24.229: " IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3 ".

[x] 3GPP TS 29.228: " IP Multimedia (IM) Subsystem Cx and Dx interface; signalling flows and message contents ".

**** next change ****

7.2 Detailed specification

7.2.1 Update of UEís IP address in HSS depending on PDP context state

During PDP context request towards the IMS, the GGSN shall send a RADIUS "ACCOUNTING-REQUEST START" message to a RADIUS server attached to the HSS. The message shall include the UEís IP address and MSISDN. The format of the message shall be compliant with 3GPP TS 29.061 [4]. On receipt of the message, the HSS shall use the MSISDN to find the subscriberís IMPI (derived from IMSI) and then store the IP address against the IMPI.

NOTE1: It is assumed here that the RADIUS server for handling the accounting request to receive the IP address from the GGSN is different to the RADIUS server that the GGSN may use for access control and IP address assignment. However, according to TS 23.060 [5] there is no limitation on whether RADIUS servers for Accounting and Access control have to be separate or combined.

NOTE2: It is also possible to utilize RADIUS to DIAMETER conversion in the interface between GGSN and HSS. This makes it possible to utilize the existing support for DIAMETER in the HSS. One possibility to implement the conversion is to re-use the AAA architecture of I-WLAN i.e. the 3GPP AAA Proxy or Server and its capability to perform RADIUS to DIAMETER conversion. It should be noted that the GGSN shall always uses RADIUS for this communication. Furthermore, it should be noted that DIAMETER is not mandatory to support in the HSS for communication with the GGSN.

GGSN shall not activate the PDP context if the accounting start message is not successfully handled by the HSS. In particular, it shall not be possible to have an active IMS PDP context if the corresponding IP address is not stored in the HSS.

In case of PDP context deletion, the GGSN sends an "ACCOUNTING-REQUEST STOP" message to the HSS after the idle timer in the GGSN expires. The HSS shall then start the 3GPP HSS-initiated de-registration procedure.

If the UE establishes a new PDP context and therefore gets a new IP address, the UE shall start the IMS initial registration procedure. Because the idle timer in the GGSN could be set with a large value, e.g. 1 hour, it is quite likely that the UE will send a PDP context creation request before the idle timer expires. Two cases are distinguished:

- If the PDP context creation request is processed by the same SGSN as the old PDP context, then the SGSN will assign the existing PDP context to the UE. Therefore the IP address of the UE is unchanged and the IMS registration is still valid.

- If the PDP context creation request is processed by a different SGSN compared to the old PDP context, e.g. in case of a routing area update, the SGSN will create a new PDP context for the UE. In this case the GGSN shall send an "ACCOUNTING-REQUEST START" to the HSS with the new IP address. Because this IP address is different to the IP address the UE registered with, the HSS shall start the 3GPP HSS-initiated de-registration procedure. Later, the idle timer for the old PDP context expires and the old PDP context will be deleted by the GGSN. The HSS will be informed about the event via the "ACCOUNTING-REQUEST STOP" message. The HSS checks the IP address indicated by the "ACCOUNTING-REQUEST STOP" message against the IP address stored in the HSS. If they are the same, a network-initiated de-registration procedure shall be started. In this case they are different, so the HSS shall then ignore the message.

7.2.2 Protection against IP address spoofing in GGSN

All GGSNs that offer connection to IMS shall implement measures to prevent source IP address spoofing. Specifically, a UE attached to the GGSN shall not be able to successfully transmit an IP packet with a source IP address that is different to the one assigned by the GGSN during PDP context activation. If IP address spoofing is detected the GGSN shall drop the packet and log the event in its security log against the subscriber information (IMSI/MSISDN).

7.2.3 ~~Source IP address checking in the P-CSCF and S-CSCF~~Impact on IMS registration and authentication procedures

A UE shall not be able to spoof its assigned IP address and successfully receive service from the IMS. The mechanisms in the following sub-clauses shall be supported to prevent IP address spoofing in the IMS domain. The changes to the IMS registration and authentication procedures are detailed in the following subclauses.

7.2.3.1 Procedures at the UE

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include an Authorization header field and not include a Security-Client header field. The From header, To header, Contact header, Expires header, Request URI, Supported header and a P-Asserted-Id header shall be set according subclause 5.1.1.2 of TS 24.229 [7].

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according subclause 5.1.1.2 of TS 24.229 [7].

NOTE 1: Early IMS security does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

NOTE 2: The UE shall not use the temporary public user identity used for registration in any subsequent SIP requests.

7.2.3.2~~1~~ Procedures at the P-CSCF ~~mechanisms~~

NOTE: As ~~mandated by section 18.2.1 of~~specified in RFC 3261 [6], when the P-CSCF receives a SIP request from an early IMS UE, the P-CSCF ~~will~~ checks the IP address in the ìsent-byî parameter of the top ~~ì~~Via~~î~~ header field. ~~Specifically, if the host portion of~~If the "sent-by" parameter contains a domain name, or if it contains an IP address that differs from the packet source IP address, the ~~server will~~P-CSCF adds a "received" parameter to that Via header field value. This parameter contains the source IP address from which the packet was received. ~~After this processing, the P-CSCF forwards the SIP message to the I-CSCF or S-CSCF.~~

7.2.4.2.1 Registration

When the P-CSCF receives a REGISTER request from the UE that does not contain an Authorization header and does not contain a Security-Client header, the P-CSCF shall handle the Path header, the Require header, the P-Charging-Vector header and the P-Visited-Network-ID header as described in subclause 5.2.12 of TS 24.229 [7]. Afterwards the P-CSCF shall determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) handle the Service-Route header, the public user identities, the P-Asserted-Identity header, the P-Charging-Function-Address header as described in subclause 5.2.2 of TS 24.229 [7] for the reception of a 200 (OK) response; and

2) forward the 200 (OK) response to the UE.

7.2.4.2.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

As the early IMS security solution does not offer IPsec, the P-CSCF shall implement the procedures as described in subclause 5.2.6 of TS 24.229 [7] with the following deviations.

For requests initiated by the UE, when the P-CSCF receives a 1xx or 2xx response, the P-CSCF shall not rewrite its own Record Route entry.

For requests terminated by the UE, when the P-CSCF receives a request, prior to forwarding the request, the P-CSCF shall not include a protected server port in the Record-Route header and in the Via header.

7.2.4.3 Procedures at the I-CSCF

NOTE: Topology hiding is not available with early IMS security because topology hiding alters the "via" header.

7.2.3.3~~2~~ Procedures at the S-CSCF ~~mechanisms~~

7.2.4.4.1 Registration

Upon receipt of an initial REGISTER request without an Authorization header, the S-CSCF shall:

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

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) if no IP address is stored for the UE, query the HSS, as described in clause <xx> with the public user ID as input and store the received IP address of the UE. Prior to contacting the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [x];

NOTE: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

4) ~~S-CSCF shall use the IMPI to retrieve the IP address stored during PDP context activation. For all requests, the S-CSCF first~~ checks whether a ìreceivedî parameter exists in the top ìviaî header field. If a ìreceivedî parameter exists, S-CSCF shall compare the IP address recorded in the ìreceivedî parameter against the UEís IP address stored during registration. If no ìreceivedî parameter exists in the top ìviaî header field, then S-CSCF shall compare IP address recorded in the ìsent-byî parameter against the stored UE IP address ~~stored during registration~~. In both cases, if the ~~HSS retriev~~stored IP address and the IP address recorded in the top ìviaî header do not match, the S-CSCF shall reject the registration with a 403 (Forbidden) response and skip the following steps.

5) handle the Cx Server Assignment procedure, the ICID, each non-barred registered public user identity, the Path header, the registration duration as described in subclause 5.4.1.2.2 of TS 24.229 [7]; and

6) send a 200 (OK) response to the UE as described in subclause 5.4.1.2.2 of TS 24.229 [7].

~~If the request sent is an initial REGISTER, then the S-CSCF shall always query the HSS to retrieve the IP address registered during PDP context activation. The IP address fetched during a initial SIP REGISTER shall be stored in the S-CSCF and used for checking subsequent non-REGISTER SIP requests and non-initial REGISTER requests. The S-CSCF shall implement procedures to recover the registration information (including IP address) from the HSS in case of a system failure.~~

~~The S-CSCF shall check the IP address for every SIP request, but it shall only contact the HSS to fetch the IP address during the initial SIP Register.~~

~~NOTE: The S-CSCF only needs to contact the HSS to fetch the IP address during the initial SIP REGISTER because any change in IP address at the GPRS level will trigger the UE to send an initial REGISTER. Furthermore, the GGSN always notifies the HSS when the IP address is deallocated and the HSS then immediately deregisters the user. This mechanism requires that the S-CSCF can distinguish between initial REGISTER requests and re-REGISTER requests. Contacting HSS for every SIP message would place too high a load on the HSS.~~

7.2.4.4.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

On the reception of any request other than an initial REGISTER request, the S-CSCF shall check whether a "received" parameter exists in the top "via"î header field. If a "received" parameter exists, S-CSCF shall compare the IP address received in the "received" parameter against the UEís IP address stored during registration. If no "received" parameter exists in the top "via"î header field, then S-CSCF shall compare IP address received in the "sent-by" parameter against the IP address stored during registration. If the stored IP address and the IP address received in the top "via" header field do not match, the S-CSCF shall reject the request with a 403 (Forbidden) response.

In case the stored IP address and the IP address receive in the top "via" header field do match, the S-CSCF shall proceed as described in 5.4.3 of TS 24.229 [7].

7.2.4 Interworking cases

It is expected that both fully 3GPP compliant UEs implementing the security mechanisms in TS 33.203 [2] (denoted ì fully compliantî in the following) and UEs implementing the early IMS security security solution specified in the present document (denoted ì early IMSî in the following) will access the same IMS. In addition, IMS networks will support only fully compliant UEs, early IMS UEs, or both. Both UEs and IMS networks must therefore be able to properly handle the different possible interworking cases.

Editorís note: The interworking solution described in this clause is agreed as a working assumption in SA3. An alternative approach based on explicit identification of early IMS support on UEs has been suggested, but a detailed proposal has not yet been developed. If compelling reasons are found to replace the working assumption with this alternative approach, then this will be done at SA3#36 (23-26 November 2004).

Since early IMS security does not require the security headers specified for fully compliant UEs, these headers shall not be used for early IMS. The Register message sent by an early IMS UE to the IMS network shall not contain the security headers specified by TS 33.203 (Authorization and Security-Client).

As a result, early IMS UEs shall not add an explicit indication for the security used to the IMS signaling. An IMS network supporting both early IMS and fully 3GPP compliant UEs shall use early IMS security for authenticating the UE during registrations that do not contain the security headers specified by TS 33.203 (Authorization and Security-Client).

Without sending an Authorization Header in the initial Register message, early IMS UEs only provide the IMS public identity, but not the IMS private identity to the network (this is only present in the Authorization header for fully compliant UEs). The IMS private identity shall therefore be derived from the subscriberís public identity in the HSS.

During the process of user registration, the Cx interface carries both the private user identity and the public user identity in Cx-MAR requests (sent by I-CSCF and S-CSCF). For early IMS, only the public user identity shall be sent to the HSS within these requests, and the private user identity shall be empty. This avoids changes to the message format to the Cx interface.

If the S-CSCF receives an indication that the UE is early IMS, then it shall be able to select the ì IP-basedî authentication scheme in the Cx-MAR request. The Cx interface shall support the error case that the S-CSCF selects the

ì Digest-AKAv1-MD5î authentication scheme based on UE indication, but the HSS detects that the subscriber has a SIM instead of a USIM or ISIM. In this case the HSS shall respond with an appropriate error command. The S-CSCF will then respond to the UE with a 403 Forbidden message. If the UE is capable of early IMS then, according to step 5, the UE will take this as an indication to attempt registration using early IMS.

For interworking between early IMS and fully compliant implementations during IMS registration, the following cases shall be supported:

1. Both UE and IMS network support early IMS only

   IMS registration shall take place as described by the present document.

2. UE supports early IMS only, IMS network supports both early IMS and fully compliant access security

   Early IMS security according to this annex shall be used for authenticating the UE for all registrations from UEs that do not provide the fully compliant security headers.~~The IMS network shall use early IMS security according to the present document for authenticating the UE for all registrations from UEs that do not provide the fully compliant security headers.~~

3. UE supports both, IMS network supports early IMS only

   If the UE already has knowledge about the IMS network capabilities (which could for example be preconfigured in the UE), the appropriate authentication method shall be chosen. The UE shall use f~~F~~ully compliant security ~~shall be used,~~ if the network supports this, otherwise the UE shall use early IMS security ~~shall be used~~.

   If the UE does not have such knowledge it shall start with the fully compliant Registration procedure. The early IMS P-CSCF shall answer with a 420 ì Bad Extensionî failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial Register message ~~(this header cannot be ignored by the P-CSCF)~~.

NOTE: The Proxy-Require header cannot be ignored by the P-CSCF.

   The UE shall, after receiving the error message, send an early IMS registration, i.e., shall send a new ~~Register~~ REGISTER ~~message~~ request without the fully compliant security headers. ~~The network shall respond with a 200 OK message according to the registration message flow as specified in clause 7.2.5.1.~~

4. UE and IMS network support both

   The UE shall start with the fully compliant IMS registration procedure. The network, with receiving the initial ~~Register~~ REGISTER message, receives indication that the UE is fully compliant and shall continue as specified by TS 33.203 [2].

5. UE and IMS network support both, UE contains a SIM

   The UE might start with the fully compliant IMS registration procedure. However, when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that the UE contains a SIM and return an error.

   The S-CSCF shall answer with a 401 (Unauthorized) with an Error-info: header containing the text "Early security required". The UE then retries using early IMS security.

~~5.~~6. UE supports early IMS only, IMS network supports fully compliant access security only

   The UE sends a ~~Register~~ REGISTER ~~message~~ request to the IMS network that does not contain the ~~necessary~~ security headers required by fully compliant IMS. The fully compliant P-CSCF will detect that the Security-Client header is missing and return a 4xx messages, as described in clause 5.2.2 of of TS 24.229 [7].~~In this case the IMS network will answer with an error message (403 Forbidden with ì Authentication Failedî reason phrase) indicating to the early IMS UE that the authentication method is incorrect. After receiving the error message, the early IMS UE shall stop the attempt to register with this network, since early IMS is not supported.~~

~~6.~~7. UE supports fully compliant access security only, IMS network supports early IMS only

The UE shall start with the fully compliant IMS registration procedure. The early IMS P-CSCF shall answer with a 420 ìBad Extensionî failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial Register message ~~(this header cannot be ignored by the P-CSCF)~~. After receiving the error message, the UE shall stop the attempt to register with this network, since the fully 3GPP compliant security according to TS 33.203 [2] is not supported.

7.2.5 Message flows

7.2.5.1 Successful registration

Figure 1 below describes the message flow for successful registration to the IMS that is specified by the early IMS security solution.

Note, that the ìreceivedî parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 7.2.3.1.

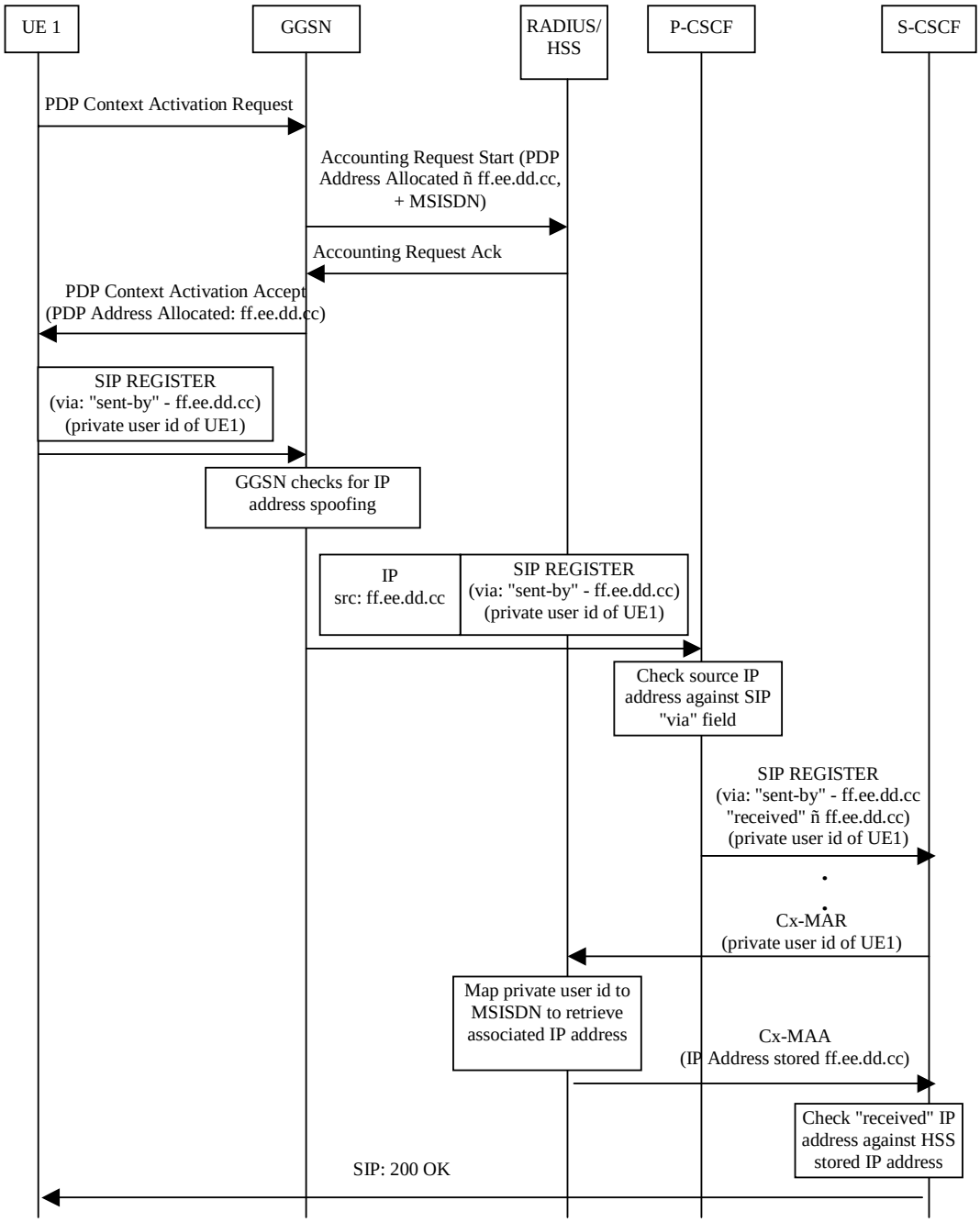

Figure 1: Message sequence for early IMS security showing a successful registration

7.2.5.2 Unsuccessful registration

Figure 2 below gives an example message flow for the unsuccessful attempt of an attacker trying to spoof the IMS identity of a valid IMS user.

Again, the ìreceivedî parameter is only present between P-CSCF to S-CSCF under the conditions given in clause 7.2.3.1.

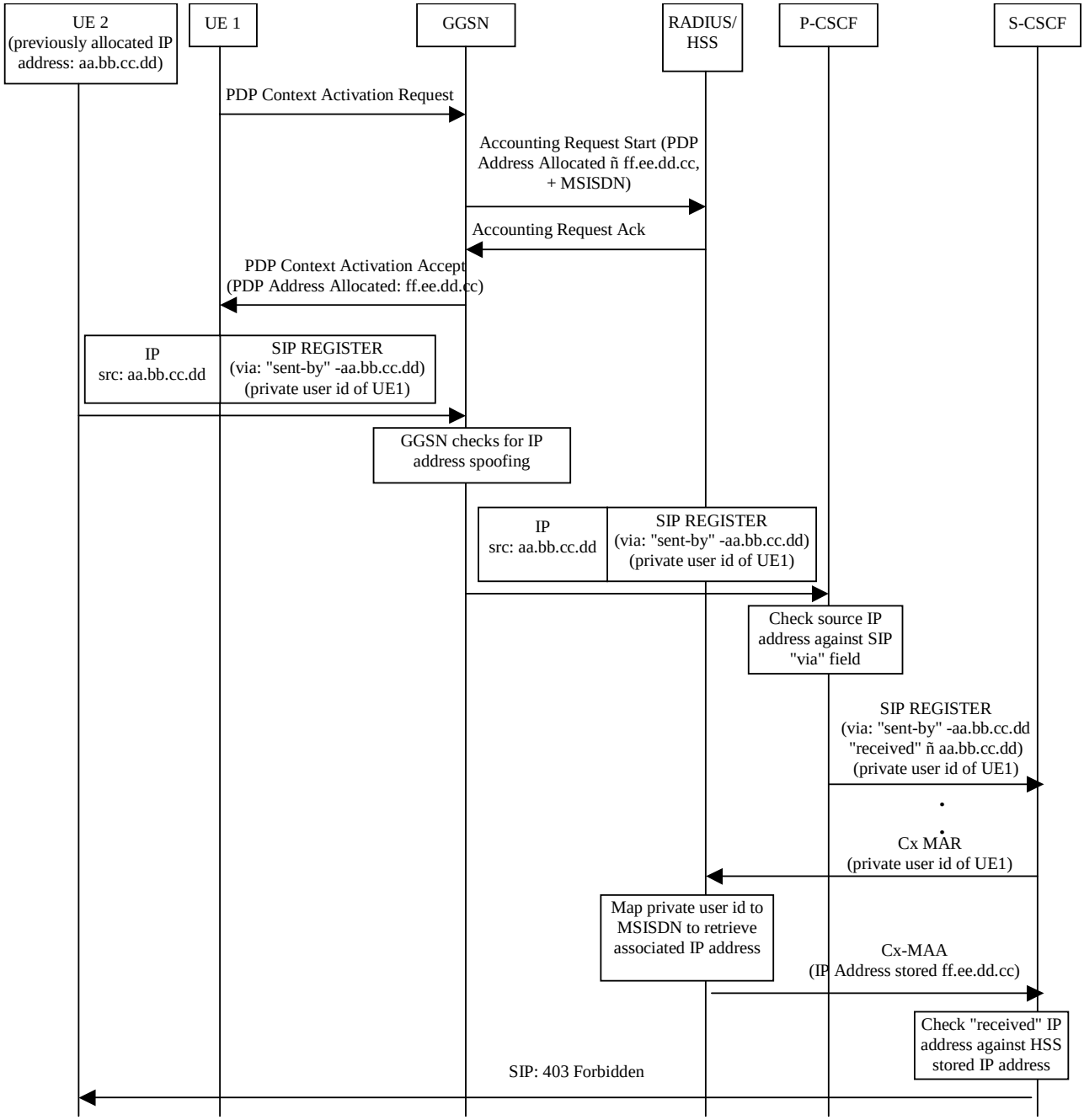

Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

7.2.5.3 Successful registration for a selected interworking case

Figure 3 below describes the message flow for successful registration to the IMS in the case that the UE supports both fully compliant and early IMS access security and the network supports early IMS only. This case is denoted as case 3 in clause 7.2.4.

Note, that the ìreceivedî parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 7.2.3.1.

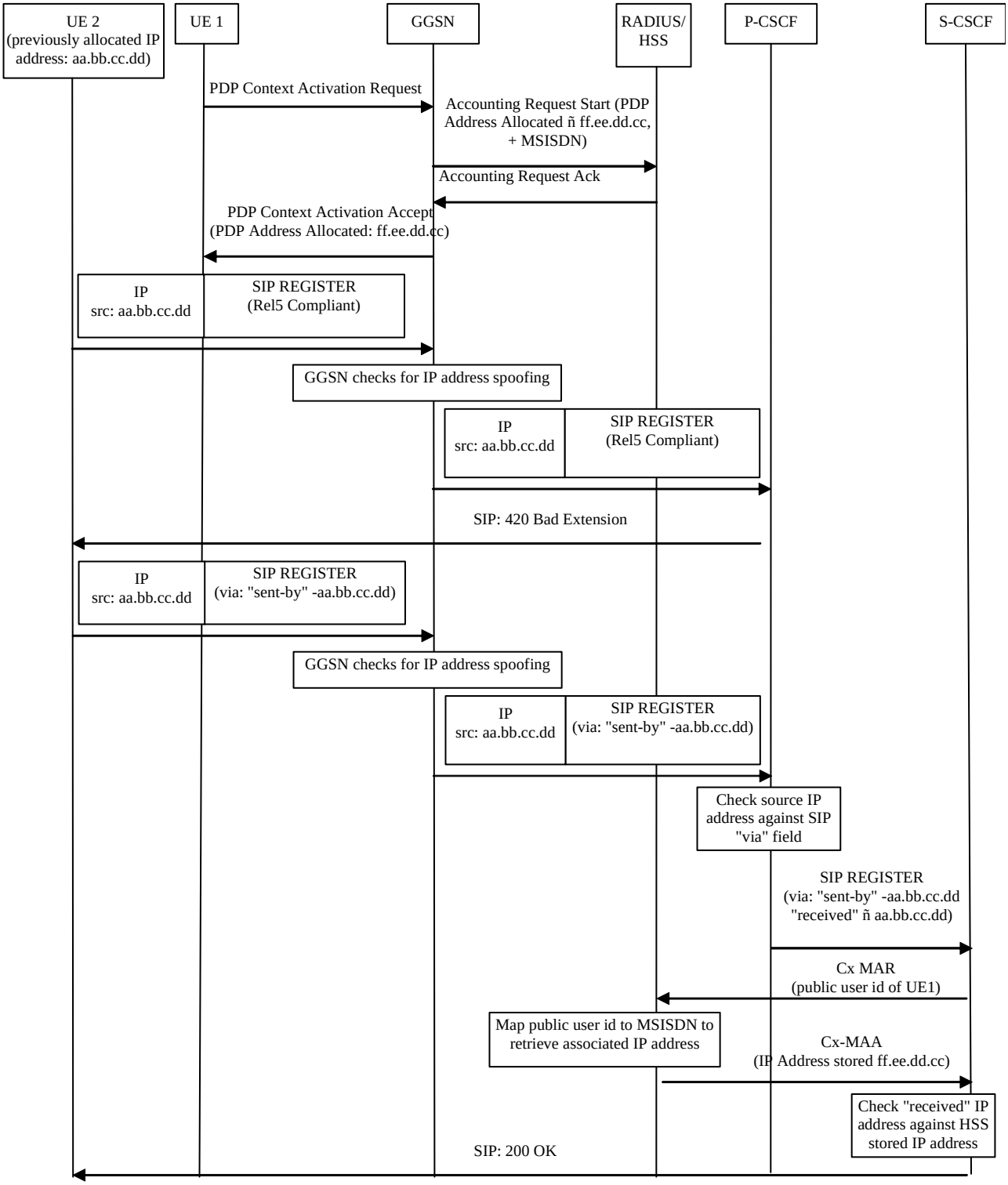

Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant and early IMS access security and network supports early IMS security only