3GPP TSG SA WG3 Security ó S3#36 **S3-041063**
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 **X**

Title:	⌘	Impact on Cx interface based on LS from CN4 (S3-041047)
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 Cx interface is missing.
Summary of change:	⌘	Addition of detailed specification of Cx interface based on LS from CN4 (S3-041047).
Consequences if not approved:	⌘	Incomplete specifications.

Clauses affected:	⌘	2, 7.2.3a (new clause)

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

Other comments:	⌘	Section 7.2.3a could become section 7.2.4 and subsequent sections could be renumbered accordingly.

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 ".

[y] IETF draft ì draft-ietf-aaa-diameter-nasreq-17.txtî .

[z] 3GPP TS 29.229: " Cx Interface based on Diameter ñ Protocol details ".

**** 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

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.

7.2.3.1 P-CSCF mechanisms

As mandated by section 18.2.1 of RFC 3261 [6] the P-CSCF will check the IP address in the ìsent-byî parameter of the top ìViaî header field. Specifically, if the host portion of 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 add 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.

7.2.3.2 S-CSCF mechanisms

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 IP address stored during registration. In both cases, if the HSS retrieved 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.

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.

7.2.3a Impact on Cx Interface

Early IMS Security mechanism affects the use of the protocol defined for the Cx interface. In particular, the User-Authorisation-Request and Multimedia-Auth-Request/Answer messages are impacted.

Because in Early IMS Security the Private User Identity of the subscriber is not made available to the IMS domain in SIP messages, it is necessary to derive a Private User Identity from the Temporary Public User Identity to use as the content of the User-Name AVP in certain Cx messages (most notable UAR and MAR).

7.2.3a.1 User registration status query

The UAR command, when implemented to support Early IMS Security follow the description in 6.1.1 of 3GPP TS 29.228 [x], with the following exception;-

- the Private User Identity (User-Name AVP) in the UAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present port number, URI parameters, and headers

7.2.3a.2 Authentication procedure

The MAR and MAA commands, when implemented to support Early IMS Security follow the description in 6.3 of 3GPP TS 29.228 [x] of this document, with the following exceptions;-

- the Private User Identity (User-Name AVP) in the MAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present: port number, URI parameters, and headers.

- In the MAR and MAA commands, the Authentication Scheme (Authentication-Scheme AVP described in section 7.9.2 of 3GPP TS 29.228 [x]) within the SIP-Auth-Data-Item grouped AVP shall contain ìEarly-IMS-Securityî.

- In the MAA command, the SIP-Auth-Data-Item grouped AVP shall contain the user IP address. If the address is IPv4 it shall be included within the Framed-IP-Address AVP as defined in draft-ietf-aaa-diameter-nasreq-17.txt [y]. If the address is IPv6 it shall be included within the Framed-IPv6-Prefix AVP and, if the Framed-IPv6-Prefix AVP alone is not unique for the user it shall also contain Framed-Interface-Id AVP.

  This results in SIP-Auth-Data-Item as depicted in table 6.3.4 of 3GPP TS 29.228 [x], being replaced when Early IMS Security is employed by a structure as shown in table 2.1;-

Table 2.1: Authentication Data content for Early IMS Security ñ response

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For Early IMS Security it will indicate ìEarly-IMS-Securityî

User IPv4 Address	Framed-IP-Address	C	If the IP Address of the User is an IPv4 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [y].
User IPv6 Prefix	Framed-IPv6-Prefix	C	If the IP Address of the User is an IPv6 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [y].
Framed Interface Id	Framed-Interface-Id	C	If the IP Address of the User is an IPv6 address and the Framed-IPv6-Address AVP alone is not unique for the user this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [y].

The ABNF description of the AVP as given in section 6.3.13 of 3GPP TS 29.229 [z] is replaced with that given below.

```
SIP-Auth-Data-Item :: = < AVP Header : TBD >
        [ SIP-Authentication-Scheme ]
        [ Framed-IP-Address ]
        [ Framed-IPv6-Prefix ]
        [ Framed-Interface-Id ]
        * [AVP]
```

- Step 5 of section 6.3.1 of this document shall apply with the following exception:
- HSS shall return only one SIP-Auth-Data-Item

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 ìIP-basedî authentication scheme in the Cx-MAR request. The Cx interface shall support the error case that the S-CSCF selects the ìDigest-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

   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. Fully compliant security shall be used, if the network supports this, otherwise 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 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).

   The UE shall, after receiving the error message, send an early IMS registration, i.e., shall send a new Register message 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 message, receives indication that the UE is fully compliant and shall continue as specified by TS 33.203.

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

   The UE sends a Register message to the IMS network that does not contain the necessary security headers required by fully compliant IMS. In this case the IMS network will answer with an error message (403 Forbidden with ìAuthentication 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. 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 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.

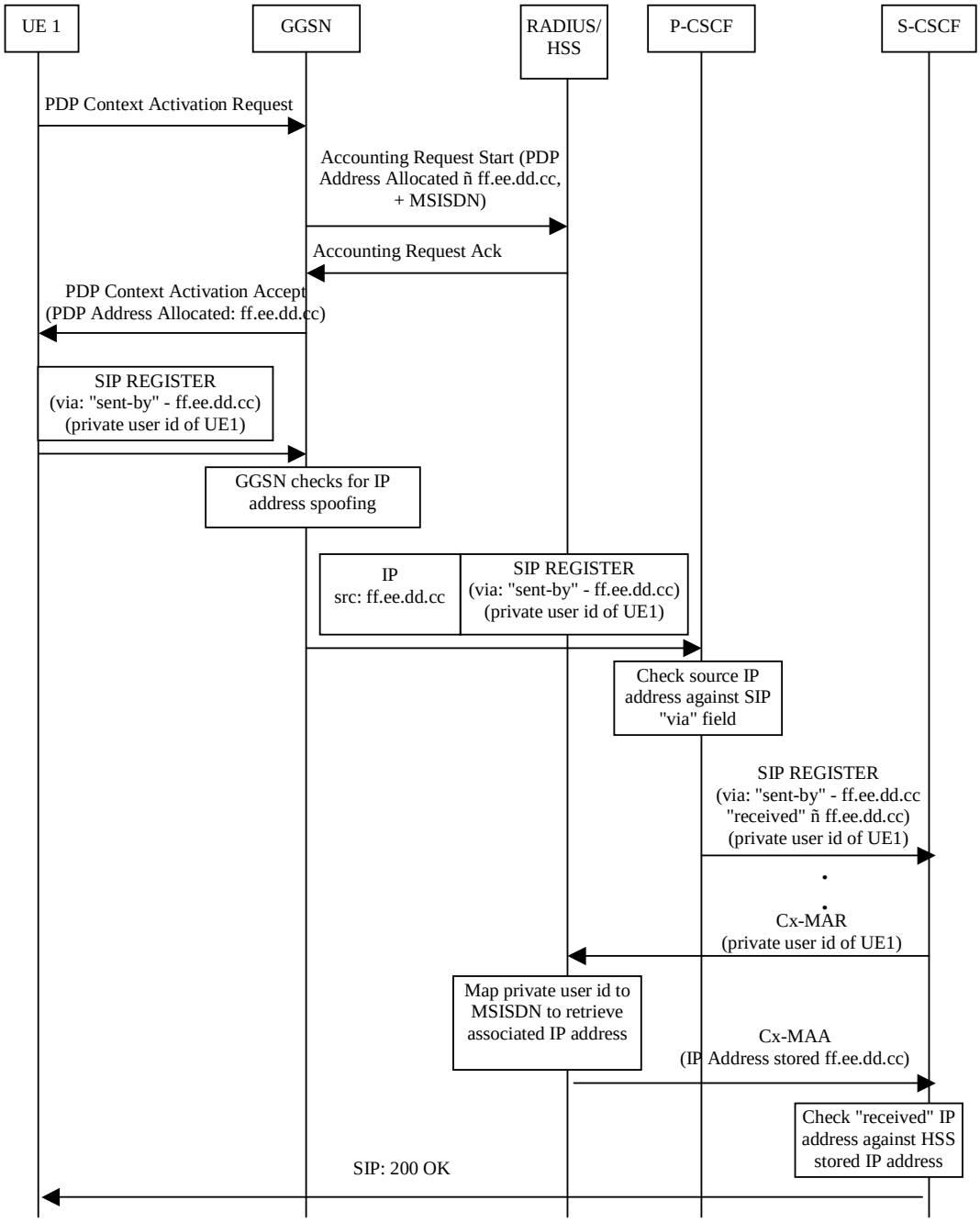

Figure 1: Message sequence for early IMS security showing a successful registration

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.

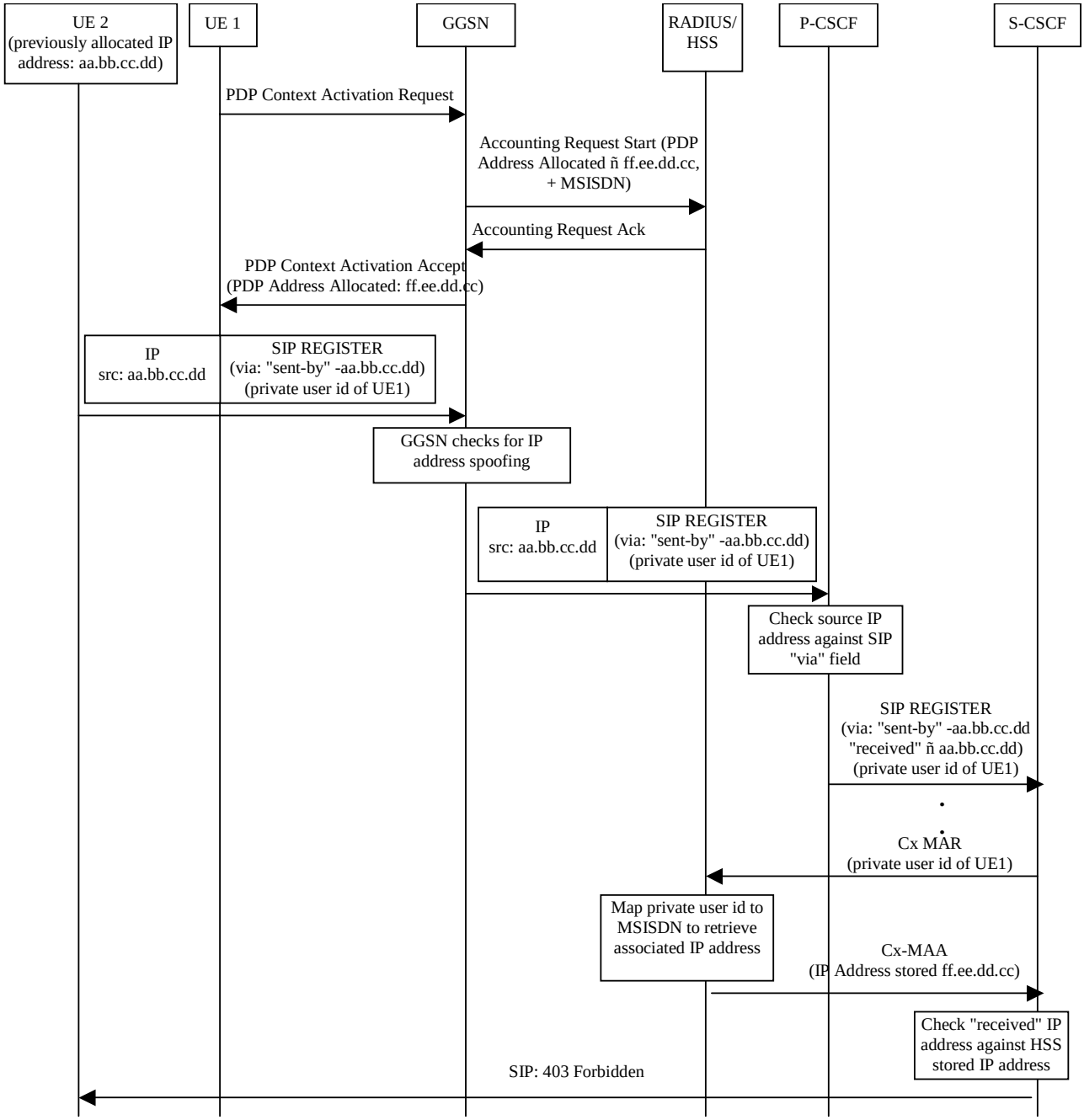

Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

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.

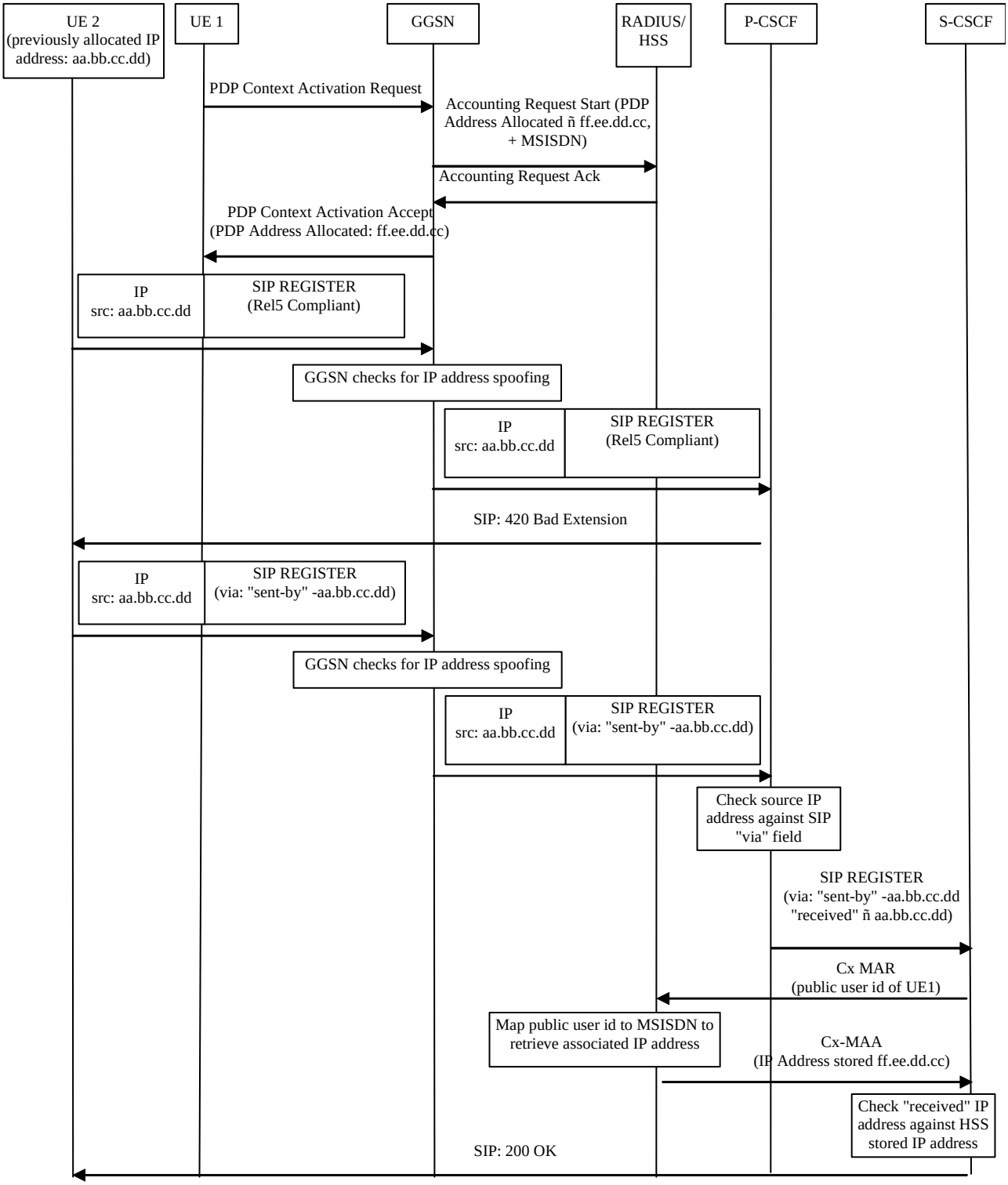

Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant and early IMS access security and network supports early IMS security only