3GPP TSG SA WG3 Security — S3#37 **S3-050087**
February 21-25, 2005, Sophia Antipolis, France

CR-Form-v7

PSEUDO-CHANGE REQUEST

⌘ **33.878** **Pseudo-CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **1.0.0** ⌘

*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:	⌘	Clarifications and corrections
Source:	⌘	Siemens
Work item code:	⌘	Early IMS
Date:	⌘	14/01/2005
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:

2	*(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)*

Reason for change:	⌘	Unclear text needs to be corrected.
Summary of change:	⌘	A note is added to clarify the registration of one public identity from several terminals. Clarifying text is added to show how compression is handled in the UE and the P-CSCF. Text on the handling of the Cx-SAR command in the S-CSCF is added. It is clarified that the Cx-UAR command is sent by the I-CSCF. Figure 1 is corrected. A few minor editorial changes are made.
Consequences if not approved:	⌘	Unclear specification

Clauses affected:	⌘	6

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

Other comments:	⌘	-

6 Specification

6.1 Overview

The early IMS security solution works by creating a secure binding in the HSS between the public/private user identity (SIP-level identity) and the IP address currently allocated to the user at the GPRS level (bearer/network level identity). Therefore, IMS level signaling, and especially the IMS identities claimed by a user, can be connected securely to the PS domain bearer level security context.

The GGSN, terminates each user's PDP context and has assurance that the IMSI used within this PDP context is authenticated. The GGSN shall provide the user's IP address, IMSI and MSISDN to a RADIUS server in the HSS over the Gi interface when a PDP context is activated towards the IMS system. The HSS has a binding between the IMSI and/or MSISDN and the IMPI and IMPU(s), and is therefore able to store the currently assigned IP address from the GGSN against the user's IMPI and/or IMPU(s). The precise way of the handling of these identities in the HSS is outside the scope of standardization. The GGSN informs the HSS when the PDP context is deactivated/modified so that the stored IP address can be updated in the HSS. When the S-CSCF receives a SIP registration request or any subsequent requests for a given IMPU, it checks that the IP address in the SIP header (verified by the network) matches the IP address that was stored against that subscriber's IMPU in the HSS.

The mechanism assumes that the GGSN does not allow a UE to successfully transmit an IP packet with a source IP address that is different to the one assigned during PDP context activation. In other words, the GGSN must prevent "source IP spoofing". The mechanism also assumes that the P-CSCF checks that the source IP address in the SIP header is the same as the source IP address in the IP header received from the UE (the assumption here, as well as for the full security solution, is that no NAT is present between the GGSN and the P-CSCF).

The mechanism prevents an attacker from using his own IP address in the IP header but spoofing someone else's IMS identity or IP address in the SIP header, so that he pays for GPRS level charges, but not for IMS level charges. The mechanism also prevents an attacker spoofing the address in the IP header so that he does not pay for GPRS charges. It therefore counters the threat scenarios given in clause 5 above.

The mechanism assumes that only one contact IP address is associated with one IMPI. Furthermore, the mechanism supports the case that there may be several IMPUs associated with one IMPI, but one IMPU is associated with only one IMPI.

In early IMS the IMS user authentication is performed by linking the IMS registration (based on an IMPI) to a PDP context (based on an authenticated IMSI). The mechanism here assumes that there is a one-to-one relationship between the IMSI for bearer access and the IMPI for IMS access.

For the purposes of this present document, an APN, which is used for IMS services, is called an IMS APN. An IMS APN may be also used for non-IMS services. The mechanism described in this present document further adds the~~a restriction~~ requirement on the UE that it allows ~~there is~~ only one APN for accessing IMS for a PLMN and that all active PDP contexts, for a single UE, associated with that IMS APN use the same IP address at any given time.

In the following we use the terms P-CSCF and S-CSCF in a general sense to refer to components of an early IMS system. We note however that early IMS solutions may not have the same functionality split between SIP entities as defined in TS 23.228 [3]. Therefore, the requirements imposed on the SIP/IP core are specified in such a way that they are independent of the functionality split between SIP entities as far as possible. While the exact functionality split of the SIP/IP core may be left open, it is important that any changes to the Cx interface towards the HSS and changes to the interface towards the UE are standardised for vendor interoperability reasons.

6.2 Detailed specification

6.2.1 GGSN-HSS interaction

When receiving an Activate PDP Context Request message, based on operator policy, a GGSN supporting early IMS security shall send a RADIUS "Accounting-Request START" message to a AAA server attached to the HSS. The

message shall include the mandatory fields defined in clause 16.4.3 of TS 29.061 [4] and the UE's IP address, MSISDN and IMSI. On receipt of the message, the HSS shall use the IMSI and/or the MSISDN to find the subscriber's IMPI (derived from IMSI) and then store the IP address against a suitable identity, e.g. the IMPI.

NOTE 1: It is assumed here that the RADIUS server attached to the HSS 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.

NOTE 2: 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 accept the activation of the PDP context if the accounting start request is not successfully handled by the HSS (e.g. a positive Create PDP Context Response should not be sent by the GGSN until the "Accounting-Request START" message is received or a negative Create PDP Context Response is sent after some RADIUS response timeout occurs). In particular, it shall not be possible to have an active PDP context associated with the IMS APN if the corresponding IP address is not stored in the HSS.

When the UE establishes ~~its first~~a PDP context for an IMS APN which is not a secondary PDP context, a new IP address is obtained, and the GGSN shall send an "Accounting-Request START" to the HSS with the assigned IP address. Depending on the status of the HSS the following steps have to be executed:

1) If an IP address is stored in the HSS and this IP address is different from the IP address ~~already stored in the HSS (i.e. the "old" IP address)~~received from the GGSN, the HSS shall (i) start the 3GPP IMS HSS-initiated de-registration procedure, if the UE is IMS registered, using a Cx-RTR/Cx-RTA exchange, and (ii) delete the old IP address.

2) The HSS stores the new IP address and confirms the "Accounting-Request START" to the GGSN. In case step 1 was executed, confirmation is sent either when ~~either~~ the de-registration procedure is successfully completed or after a suitable time-out.

3) The UE starts the IMS initial registration procedure.

4) In case step 1 was executed, ~~T~~the HSS shall abandon the de-registration procedure when a new successful authentication for this user is signalled by the S-CSCF in a Cx-SAR message.

When all the PDP contexts are de-activated at the IMS APN of the GGSN, the GGSN sends an "Accounting-Request STOP" request to the HSS. 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, an HSS-initiated de-registration procedure shall be started, if the UE is registered, using a Cx-RTR/Cx-RTA exchange. In the case they are different, the HSS shall ignore the message.

6.2.2 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. It shall be possible for the GGSN to log the event in its security log against the subscriber information (IMSI/MSISDN), e.g. based on operator configuration.

6.2.3 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 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 clauses.

6.2.3.1 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 header fields or header field values as required by RFC3329~~a Security-Client header field~~. The From header, To header, Contact header, Expires header, Request URI, and Supported header ~~and a P-Asserted-Id header~~ shall be set according clause 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 clause 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.

The UE shall support SIP compression as specified in 3GPP TS 24.229 [7] with the following deviation. When the UE will create the compartment is implementation specific, but the compartment shall not be created before the REGISTER request is sent.

6.2.3.2 Procedures at the P-CSCF

NOTE: As specified in RFC 3261 [6], when the P-CSCF receives a SIP request from an early IMS UE, the P-CSCF checks the IP address in the "sent-by" parameter of the Via header field provided by the UE. 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 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.

6.2.3.2.1 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 clause 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-Associated-URI ~~Asserted-Identity~~ header, the P-Charging-Function-Address header as described in clause 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.

The P-CSCF shall support SIP compression as specified in 3GPP TS 24.229 [7] with the following deviation. When the P-CSCF will create the compartment is implementation specific, but the compartment shall not be created before the REGISTER request is sent.

6.2.3.2.2 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 clause 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 use a protected server port number to rewrite its own Record Route entry. Instead, it shall use the number of an unprotected port where it awaits subsequent requests from the UE.

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. Instead, it shall include the

number of an unprotected port where it expects subsequent requests from the UE, and the number of an unprotected port where it expects responses to the current request, respectively.

6.2.3.3 Procedures at the I-CSCF

If the I-CSCF receives an initial REGISTER request with no Authorization header included, the I-CSCF shall not reject the message. Instead, it shall behave as described in section 6.2.5.1.

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

6.2.3.4 Procedures at the S-CSCF

6.2.3.4.1 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 6.2.5 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 TS 29.228 [10]~~;

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) check whether a "received" parameter exists in the Via header field provided by the UE. If a "received" parameter exists, S-CSCF shall compare the IP address recorded in the “received” parameter against the UE's IP address stored during registration. If no "received" parameter exists in the Via header field provided by the UE, then S-CSCF shall compare IP address recorded in the "sent-by" parameter against the stored UE IP address. In both cases, if stored IP address and the IP address recorded in the Via header provided by the UE do not match, the S-CSCF shall query the HSS, as described in clause 6.2.5 with the public user ID as input and store the received IP address of the UE. If the stored IP address and the IP address recorded in the Via header provided by the UE still 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 clause 5.4.1.2.2 of TS 24.229 [7]; and send a 200 (OK) response to the UE as described in clause 5.4.1.2.2 of TS 24.229 [7].

6.2.3.4.2 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 Via header field provided by the UE. If a "received" parameter exists, S-CSCF shall compare the IP address received in the "received" parameter against the UE's IP address stored during registration. If no "received" parameter exists in the Via header field provided by the UE, 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 Via header field provided by the UE 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 received in the Via header field provided by the UE do match, the S-CSCF shall proceed as described in clause 5.4.3 of TS 24.229 [7].

6.2.4 Identities and subscriptions

When early IMS security is supported, the HSS shall include for each subscription an IMPI and IMPU derived from the IMSI of the subscription according to the rules in TS 23.003 [8]. If the network supports both early IMS security and fully compliant IMS security, the IMSI-derived IMPI and IMPU shall be stored in addition to other IMPIs and IMPUs that may have been allocated to the subscription.

If a UE attempts a registration using early IMS security, the REGISTER shall include an IMPU that is derived from the IMSI that is used for bearer network access according to the rules in TS 23.003 [8]. The UE shall apply this rule even if a UICC containing an ISIM is present in the UE.

In the case that a UE is registering using early IMS security with an IMSI-derived IMPU, implicit registration shall be used as a mandatory function to register the subscriber's public user identity(s) using the rules defined in clause 5.2.1a.1 of TS 23.228 [3]. By applying these rules the IMSI-derived IMPU shall be barred in the HSS for all procedures other than SIP registration.

"NOTE: Early IMS security derives the public user identity used in the REGISTER request from the IMSI. Consequently, the same public user identity cannot be simultaneously registered from multiple terminals, using only early IMS registration procedures. However, simultaneous registration of a public user identity from one terminal using early IMS security, and from other terminals using fully compliant IMS security is not precluded.

6.2.5 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/Answer (Cx-UAR/UAA), the ~~and~~ Multimedia-Auth-Request/Answer (Cx-MAR/MAA) and the Server-Assignment-Request/Answer (Cx-SAR/SAA) 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).

6.2.5.1 User registration status query

The UAR command, when implemented to support Early IMS Security follow the description in clause 6.1.1 of TS 29.228 [10], 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.

6.2.5.2 S-CSCF registration/deregistration notification

The SAR command, when implemented to support Early IMS Security follows the description in clause 6.1.2 of TS 29.228 [10], with the following exception:

- the Private User Identity (User-Name AVP) in the SAR 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.

6.2.5.~~2~~3 Authentication procedure

The MAR and MAA commands, when implemented to support Early IMS Security follow the description in clause 6.3 of TS 29.228 [10], 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 clause 7.9.2 of TS 29.228 [10]) within the SIP-Auth-Data-Item grouped AVP shall contain "Early-IMS-Security".

- 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 [11]. 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 TS 29.228 [10], being replaced when Early IMS Security is employed by a structure as shown in table 2.

Table 2: Authentication Data content for Early IMS Security

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 "Early-IMS-Security"
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 [11].
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 [11].
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 [11].

The ABNF description of the AVP as given in clause 6.3.13 of TS 29.229 [12] 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 clause 6.3.1 of TS 29.229 [12] shall apply with the following exception:
  - HSS shall return only one SIP-Auth-Data-Item

6.2.6 Interworking cases

For the purposes of the interworking considerations in this clause, it is assumed that the IMS entities P-CSCF, I-CSCF, S-CSCF and HSS reside in the home network and all support the same variants of IMS, i.e. all support either only early IMS, or only fully compliant IMS, or both.

NOTE: It is compatible with the considerations in this document that the UE uses different APNs to indicate the IMS variant currently used by the UE, in case the P-CSCF functionality is split over several physical entities.

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

Since early IMS security does not require the security headers specified for fully compliant IMS UEs, these headers shall not be used for early IMS. The REGISTER request 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 IMS 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 request, early IMS UEs only provide the IMS public identity (IMPU), but not the IMS private identity (IMPI) to the network (this is only present in the Authorization header for fully compliant IMS UEs).

During the process of user registration for early IMS, the Cx interface carries ~~only~~ the public user identity in Cx-~~M~~UAR requests (sent by I-CSCF) and Cx-MAR as well as Cx-SAR requests (sent by S-CSCF ~~HSS~~). The private user identity within these requests shall be generated according to section 6.2.5.1~~contain the IMPU as received by the UE~~. This avoids changes to the message format on the Cx interface.

If the S-CSCF receives an indication that the UE is early IMS, then it shall be able to select the "Early-IMS-Security" authentication scheme in the Cx-MAR request. The Cx interface shall support the error case that the S-CSCF selects the "Digest-AKAv1-MD5" 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) response. 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 IMS 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 IMS 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 IMS 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 fully compliant IMS security, if the network supports this, otherwise the UE shall use early IMS security.

   If the UE does not have such knowledge it shall start with the fully compliant IMS Registration procedure. The early IMS P-CSCF shall answer with a 420 (Bad Extension) failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial REGISTER request.

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

The UE shall, after receiving the error response, send an early IMS registration, i.e., shall send a new REGISTER request without the fully compliant IMS security headers.

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 request, receives indication that the IMS UE is fully compliant and shall continue as specified by TS 33.203 [2].

5. Mobile equipment 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~~a Warning: header containing a warn-code 399 and the warning text "Early security required". The UE then retries using early IMS security.

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

   The UE sends a REGISTER request to the IMS network that does not contain the 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 responses, as described in clause 5.2.2 of TS 24.229 [7].

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

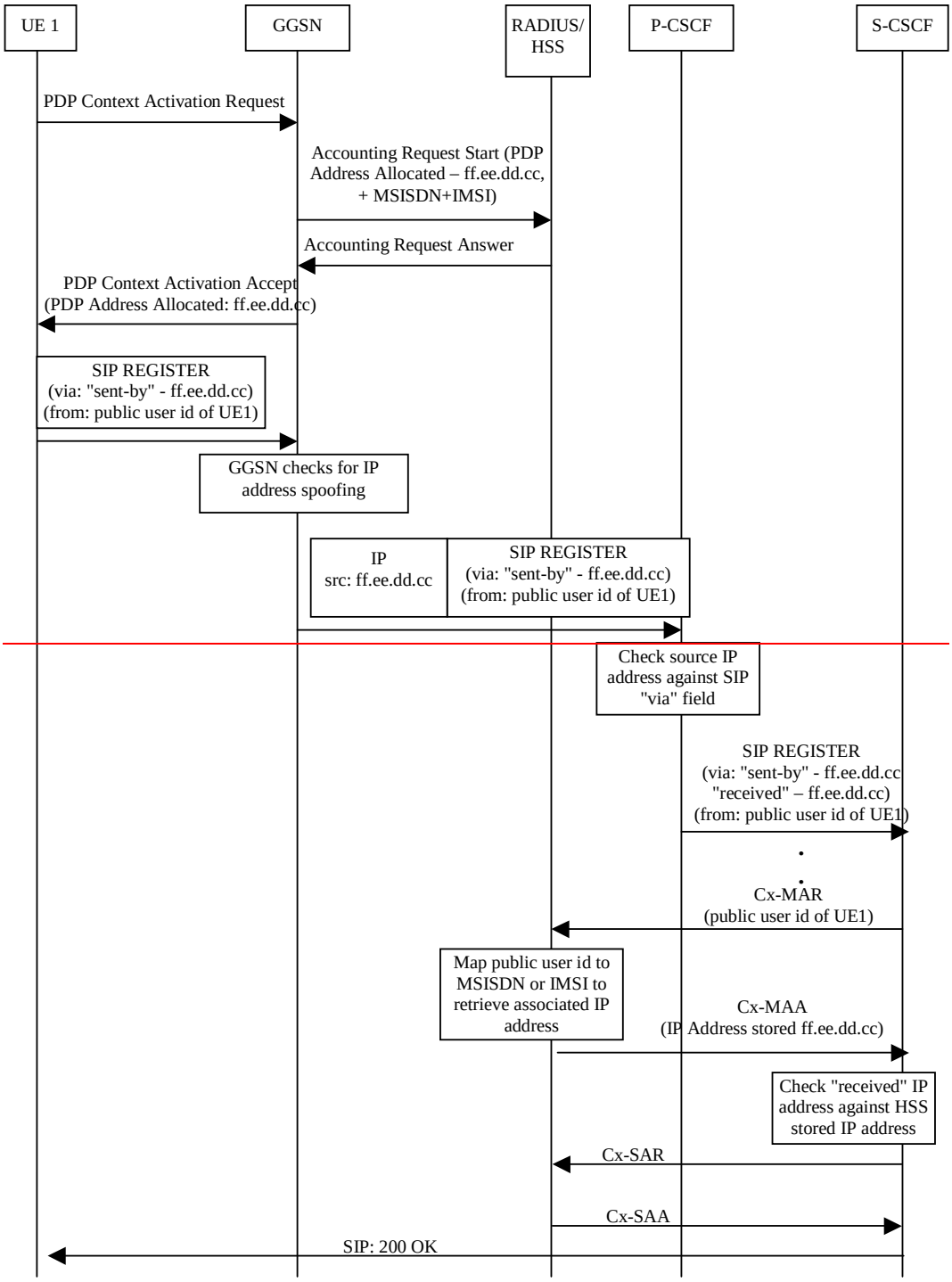
   The UE shall start with the fully compliant IMS registration procedure. The early IMS P-CSCF shall answer with a 420 (Bad Extension) failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial REGISTER request. After receiving the error response, the UE shall stop the attempt to register with this network, since the fully compliant IMS security according to TS 33.203 [2] is not supported.

6.2.7 Message flows

6.2.7.1 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: The "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 6.2.3.2.


UE 1
GGSN
RADIUS/ HSS
P-CSCF
S-CSCF
PDP Context Activation Request
Accounting Request Start (PDP Address Allocated – ff.ee.dd.cc, + MSISDN+IMSI)
Accounting Request Answer
PDP Context Activation Accept (PDP Address Allocated: ff.ee.dd.cc)
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc) (from: public user id of UE1)
GGSN checks for IP address spoofing
IP src: ff.ee.dd.cc
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc) (from: public user id of UE1)
Check source IP address against SIP "via" field
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc "received" – ff.ee.dd.cc) (from: public user id of UE1)
Cx-MAR (public user id of UE1)
Map public user id to MSISDN or IMSI to retrieve associated IP address
Cx-MAA (IP Address stored ff.ee.dd.cc)
Check "received" IP address against HSS stored IP address
Cx-SAR
Cx-SAA
SIP: 200 OK

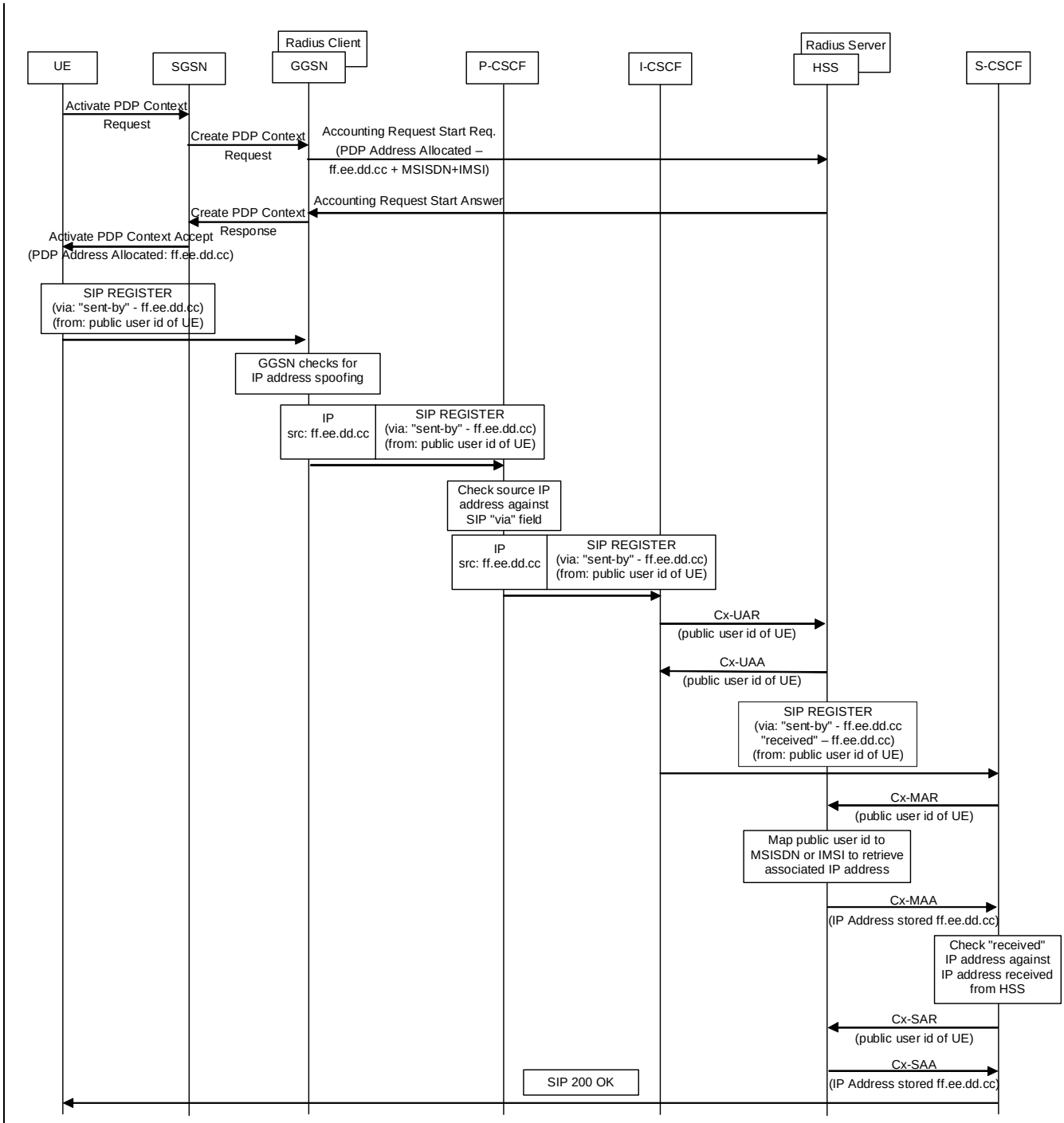


Figure 1: Message sequence for early IMS security showing a successful registration

6.2.7.2 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 "received" parameter is only present between P-CSCF to S-CSCF under the conditions given in clause 6.2.3.2.

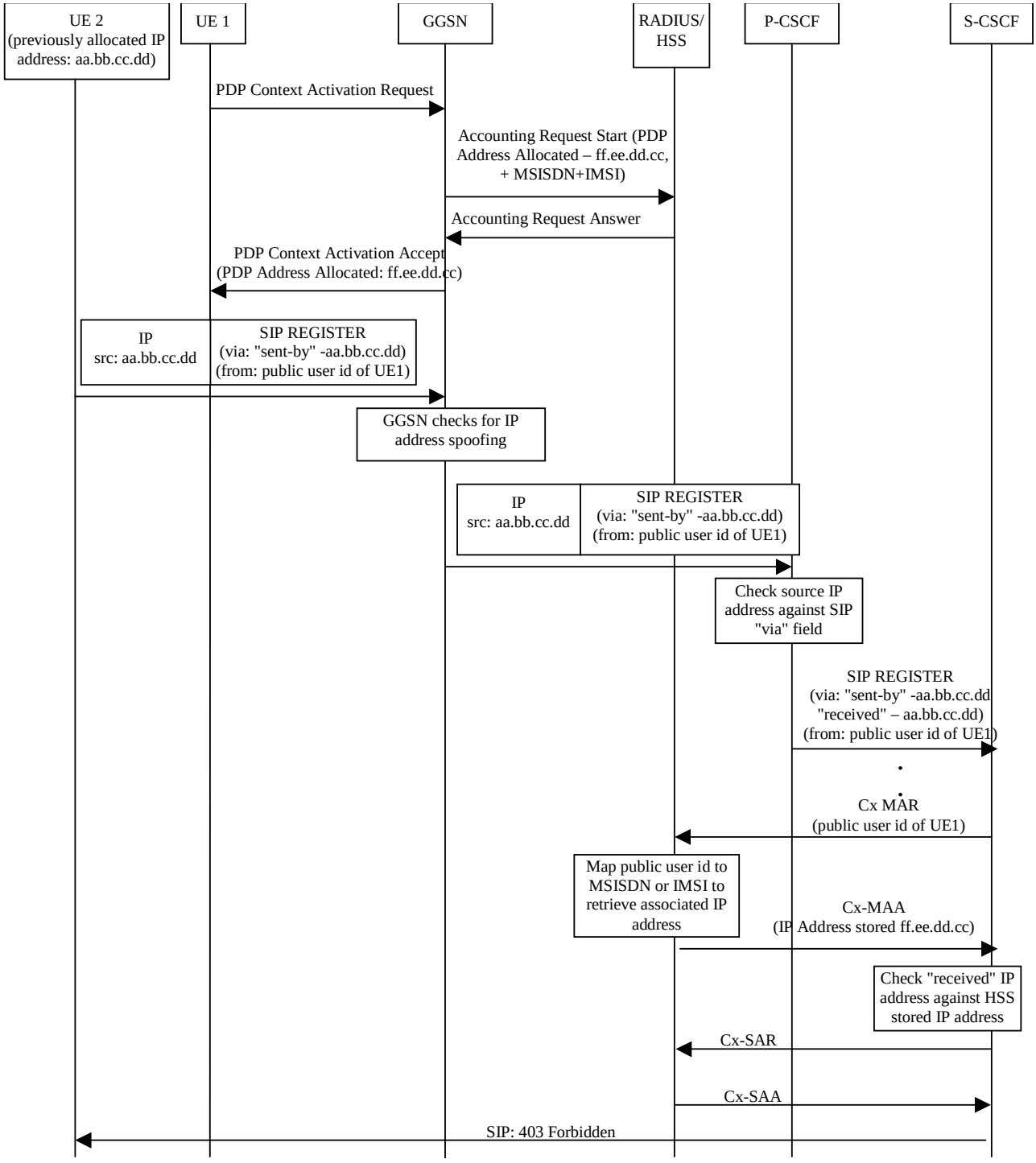


Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

6.2.7.3 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 IMS and early IMS access security and the network supports early IMS only. This case is denoted as case 3 in clause 6.2.6.

NOTE: The "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 6.2.3.2.

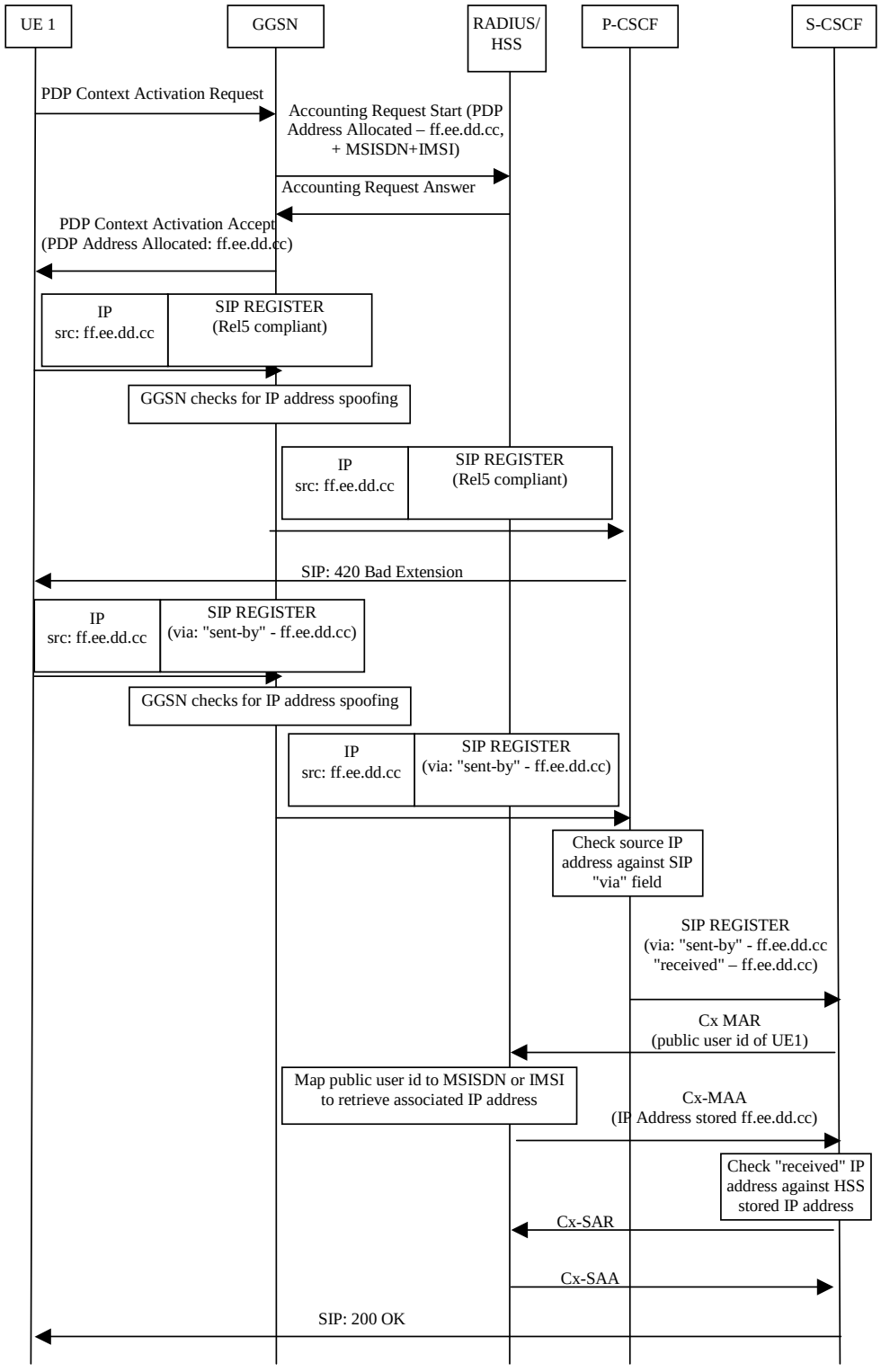


Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant IMS and early IMS access security and network supports early IMS security only