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: ⌘	Clarifications and corrections to Early IMS Security TR	
Source: ⌘	Ericsson	
Work item code:⌘	Early IMS	*Date:* ⌘ 22/11/2004

Category: ⌘ **F**	*Release:* ⌘ Rel-6

Use <u>one</u> 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 <u>one</u> 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: ⌘	The use of the terminology "top via header" is ambigous, as it is not clear which via header is referred to. Corrections are needed to the figures describing the message flows, to align the figures with the body text .
Summary of change:⌘	Updating wording in 7.2.3.2 to clearly indicate that the via header provided by the UE should be checked for the "received" parameter. Correcting figures 1, 2 and 3 in 7.2.5 to align the figures with the text.
Consequences if not approved: ⌘	Ambigous Technical Report

Clauses affected: ⌘	7.2.3.2, 7.2.5.1, 7.2.5.2, 7.2.5.3

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

Other comments: ⌘	

***** Begin of Changes *****

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 "received" parameter exists in the ~~top~~ "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 ~~top~~ "via" header field provided by the UE, then S-CSCF shall compare IP address recorded in the "sent-by" 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~~ "via" header provided by the UE 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.
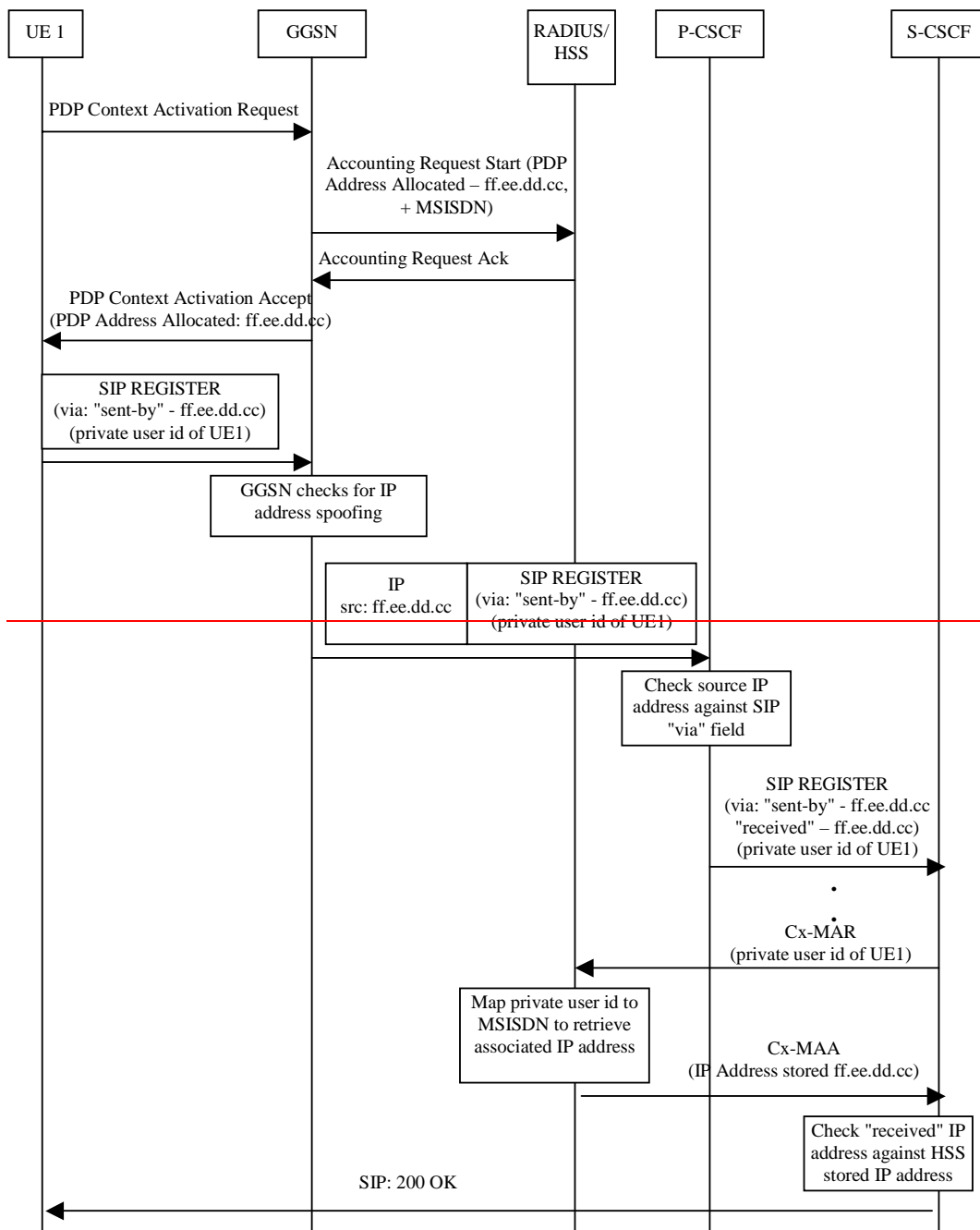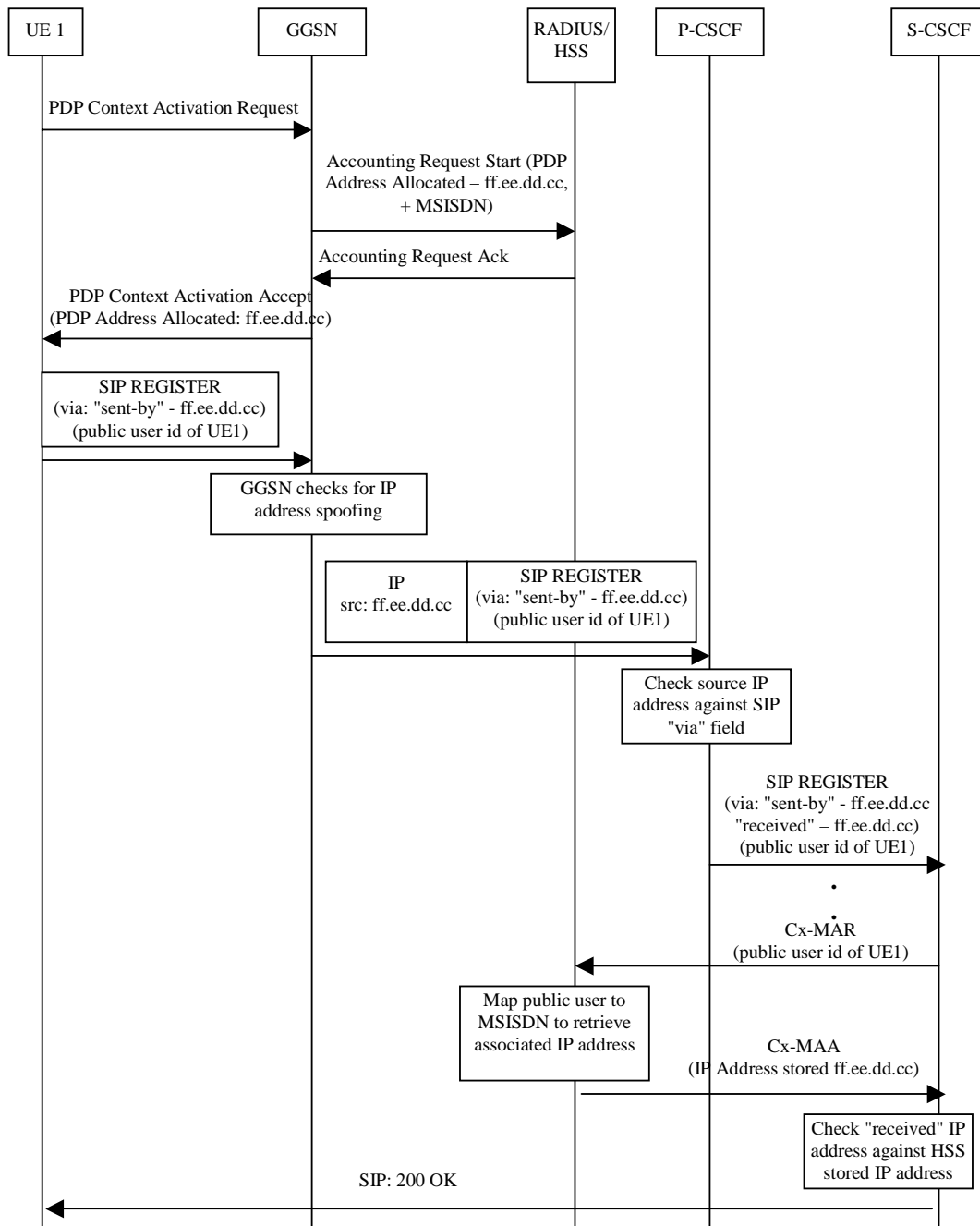
***** Next Change *****

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 "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 7.2.3.1.

```
    UE 1              GGSN           RADIUS/         P-CSCF          S-CSCF
                                      HSS

     │   PDP Context Activation Request  │               │               │
     ├──────────────────────►│           │               │               │
     │                       │           │               │               │
     │                       │ Accounting Request Start (PDP │           │
     │                       │ Address Allocated – ff.ee.dd.cc, │        │
     │                       │      + MSISDN)    │           │           │
     │                       ├──────────►│       │           │           │
     │                       │           │       │           │           │
     │                       │ Accounting Request Ack │      │           │
     │                       │◄──────────┤       │           │           │
     │  PDP Context Activation Accept    │       │           │           │
     │ (PDP Address Allocated: ff.ee.dd.cc) │    │           │           │
     │◄──────────────────────┤           │       │           │           │
     │                       │           │       │           │           │
  ┌──┴──────────────────┐    │           │       │           │           │
  │   SIP REGISTER       │    │           │       │           │           │
  │ (via: "sent-by" - ff.ee.dd.cc) │     │       │           │           │
  │ (private user id of UE1) │           │       │           │           │
  └──┬──────────────────┘    │           │       │           │           │
     ├──────────────────────►│           │       │           │           │
     │                 ┌─────┴────────┐  │       │           │           │
     │                 │ GGSN checks for IP │    │           │           │
     │                 │ address spoofing   │    │           │           │
     │                 └─────┬────────┘  │       │           │           │
     │          ┌───────────┬┴──────────────────┐│           │           │
     │          │    IP     │  SIP REGISTER      ││           │           │
     │          │ src: ff.ee.dd.cc │ (via: "sent-by" - ff.ee.dd.cc) │    │
─────┼──────────┤           │ (private 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) │
     │                       │           │       │           │ (private user id of UE1) │
     │                       │           │       │           ├──────────►│
     │                       │           │       │           │    .      │
     │                       │           │       │           │    .      │
     │                       │           │       │    Cx-MAR │    .      │
     │                       │           │       │  (private user id of UE1) │
     │                       │           │       │◄──────────┼───────────┤
     │                       │           │  ┌────┴───────┐   │           │
     │                       │           │  │ Map private user id to │   │
     │                       │           │  │ MSISDN to retrieve │       │
     │                       │           │  │ associated IP address │    │
     │                       │           │  └────┬───────┘   │    Cx-MAA │
     │                       │           │       │  (IP Address stored ff.ee.dd.cc) │
     │                       │           │       ├──────────┼───────────►│
     │                       │           │       │           │  ┌────────┴───┐
     │                       │           │       │           │  │ Check "received" IP │
     │                       │           │       │           │  │ address against HSS │
     │                       │  SIP: 200 OK │     │           │  │ stored IP address │
     │◄──────────────────────┼───────────┼───────┼───────────┼──└────────┬───┘
     │                       │           │       │           │           │
```

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

***** Next Change *****

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 "received" parameter is only present between P-CSCF to S-CSCF under the conditions given in clause 7.2.3.1.
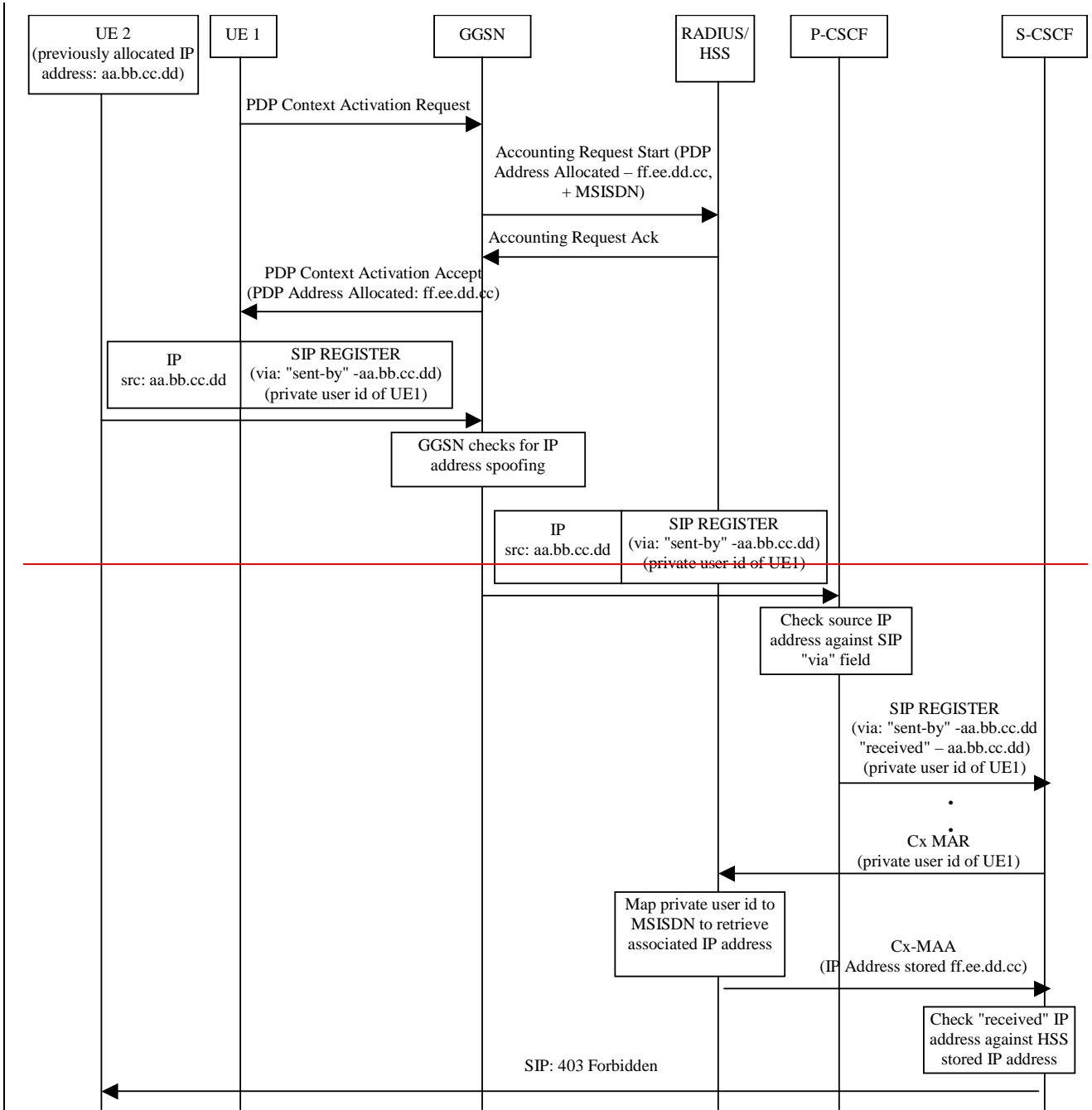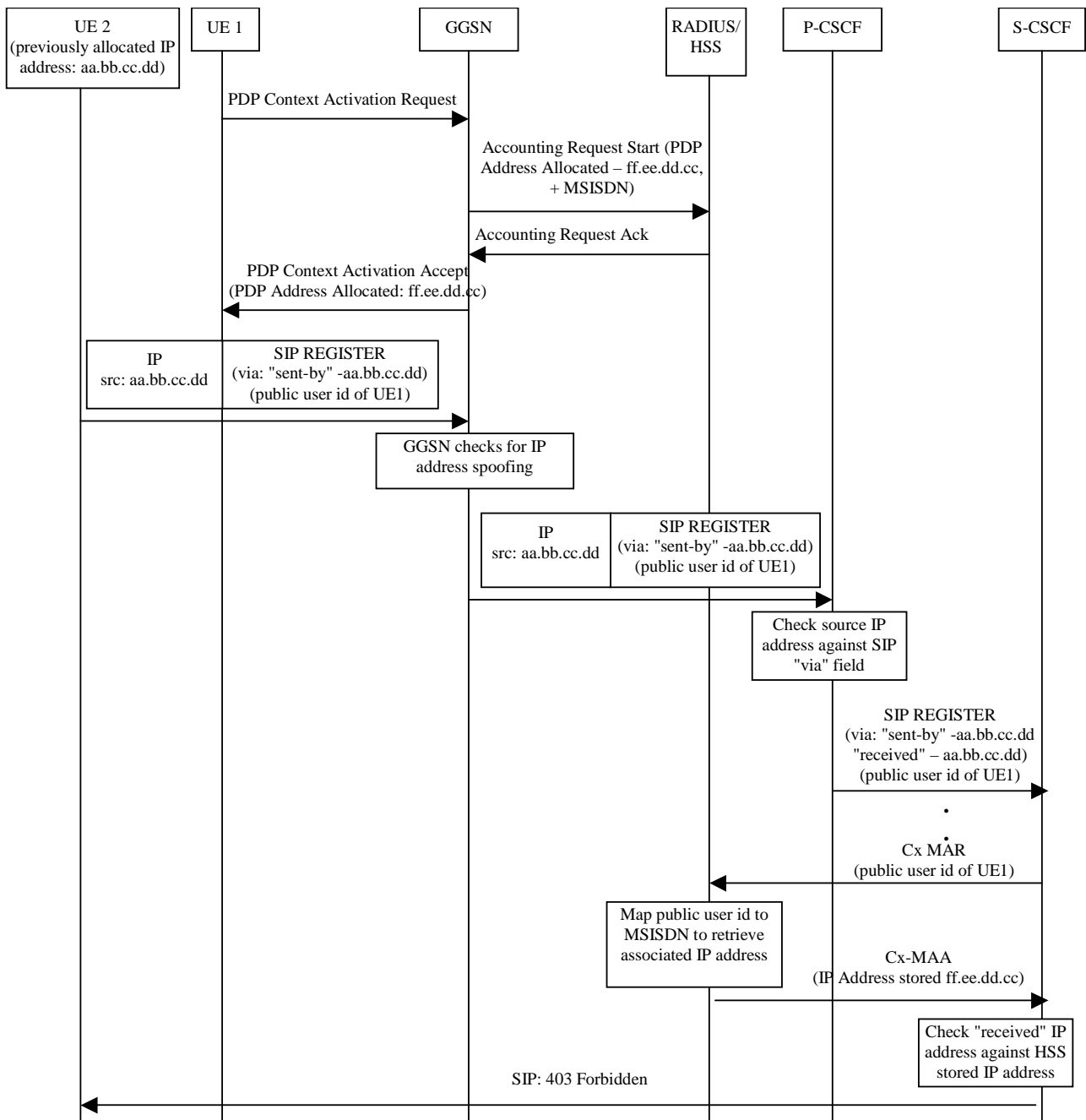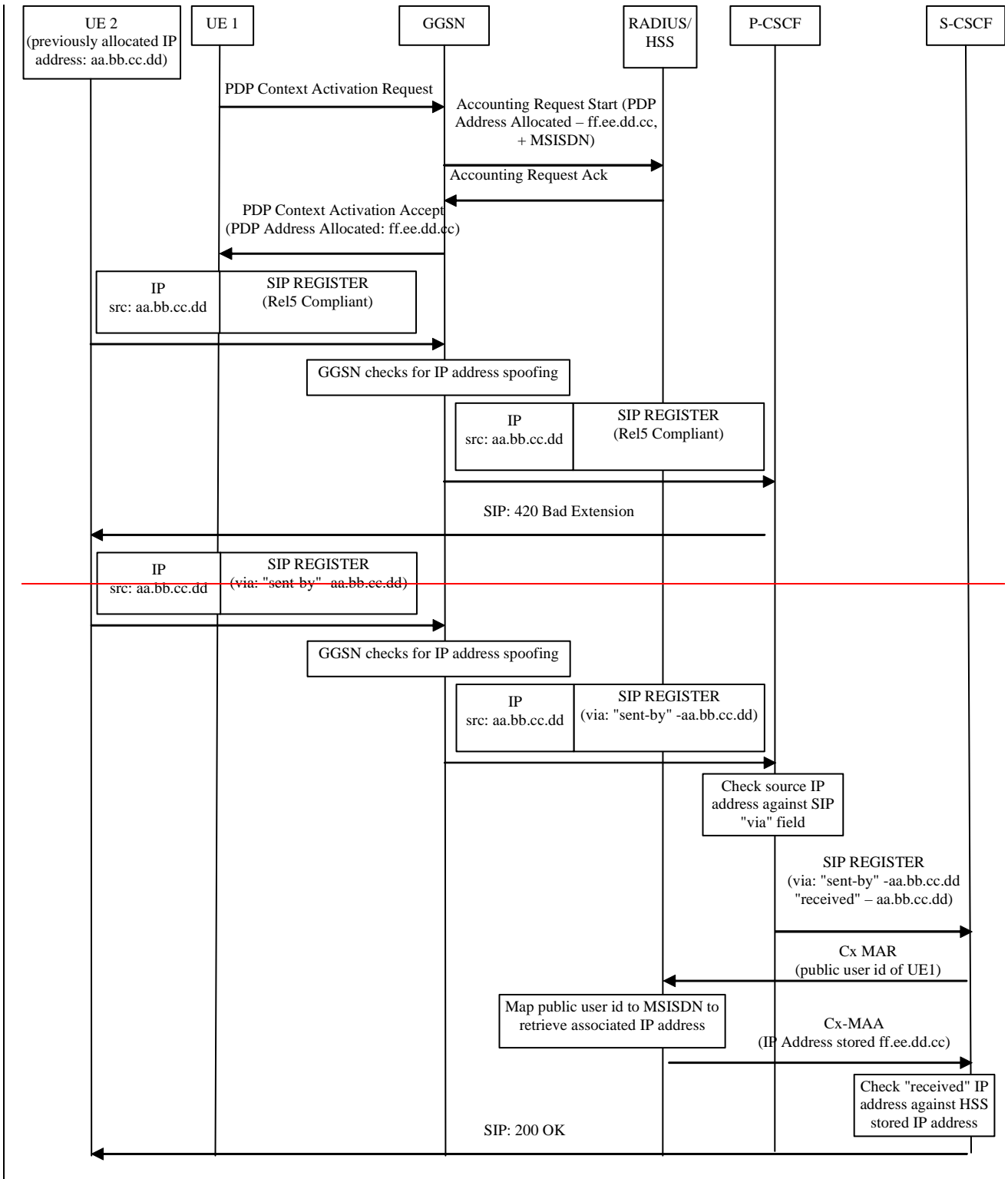
Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

***** Next Change *****

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 "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 7.2.3.1.

UE 2
(previously allocated IP address: aa.bb.cc.dd)

UE 1

GGSN

RADIUS/ HSS

P-CSCF

S-CSCF

PDP Context Activation Request

Accounting Request Start (PDP Address Allocated – ff.ee.dd.cc, + MSISDN)

Accounting Request Ack

PDP Context Activation Accept
(PDP Address Allocated: ff.ee.dd.cc)

IP
src: aa.bb.cc.dd

SIP REGISTER
(Rel5 Compliant)

GGSN checks for IP address spoofing

IP
src: aa.bb.cc.dd

SIP REGISTER
(Rel5 Compliant)

SIP: 420 Bad Extension

IP
src: aa.bb.cc.dd

SIP REGISTER
(via: "sent-by" aa.bb.cc.dd)

GGSN checks for IP address spoofing

IP
src: aa.bb.cc.dd

SIP REGISTER
(via: "sent-by" -aa.bb.cc.dd)

Check source IP address against SIP "via" field

SIP REGISTER
(via: "sent-by" -aa.bb.cc.dd
"received" – aa.bb.cc.dd)

Cx MAR
(public user id of UE1)

Map public user id to MSISDN to retrieve associated IP address

Cx-MAA
(IP Address stored ff.ee.dd.cc)

Check "received" IP address against HSS stored IP address
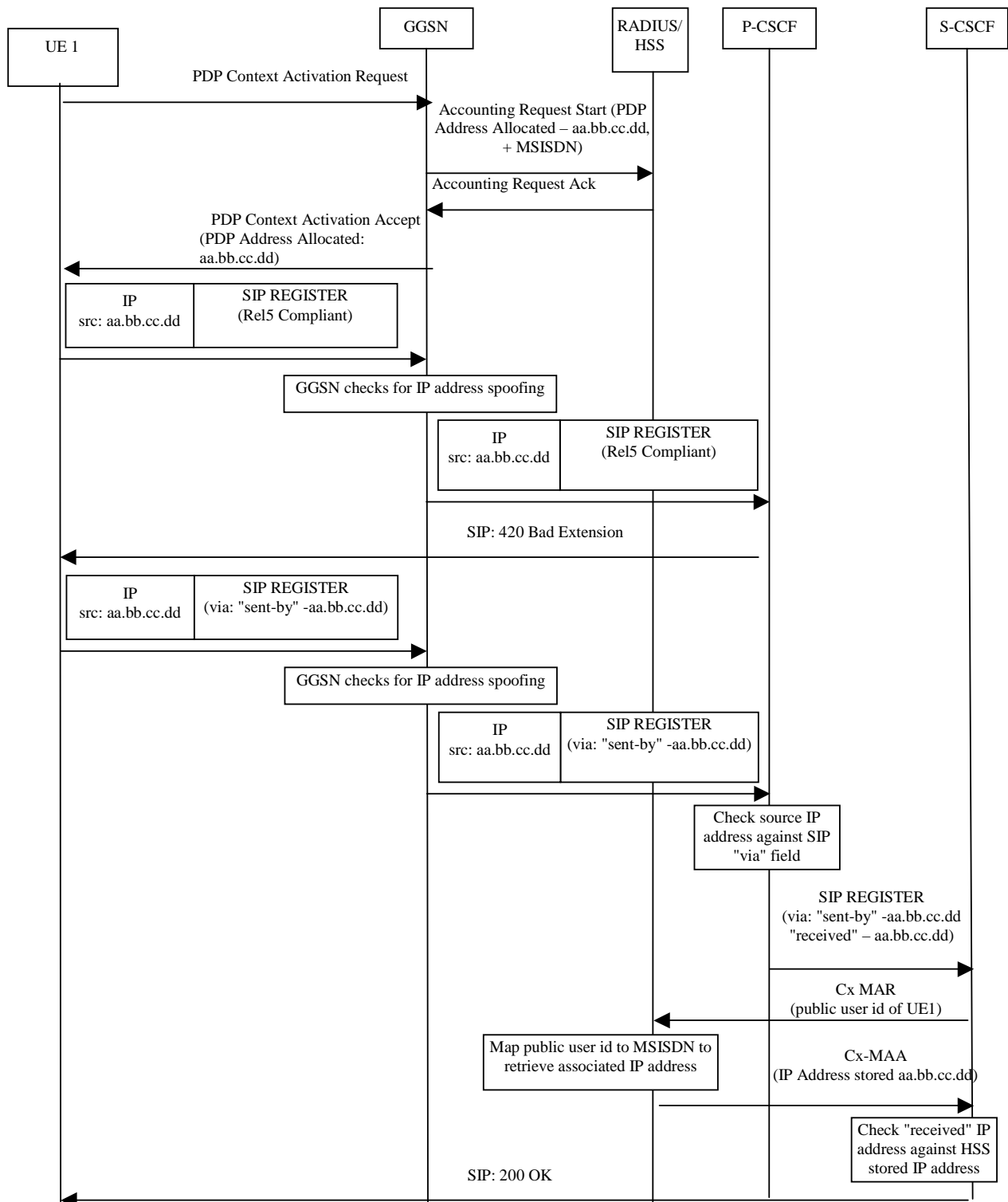
SIP: 200 OK

CR page 7

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

***** End of Changes *****