3GPP TSG-SA WG3 SECURITY Meeting #36
Shenzhen, China, 23-26 November 2004

Tdoc ⌘ S3-040939

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:	⌘	Correction of figures
Source:	⌘	Huawei
Work item code:	⌘	Early IMS
Date:	⌘	5/11/2004
Category:	⌘	
Release:	⌘	

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:	⌘	In the figures of registration, there is not notification of registration status to the HSS after the authentication, then HSS don't know the result of authentication. it can not record the UE as registered when successful authentication, or delete the pending flag when unsuccessful authentication.
Summary of change:	⌘	Adding registration status notification to HSS in registration procedure
Consequences if not approved:	⌘	The registration procedure is incomplete

Clauses affected:	⌘	7.2.5.1, 7.2.5.2, 7.2.5.3

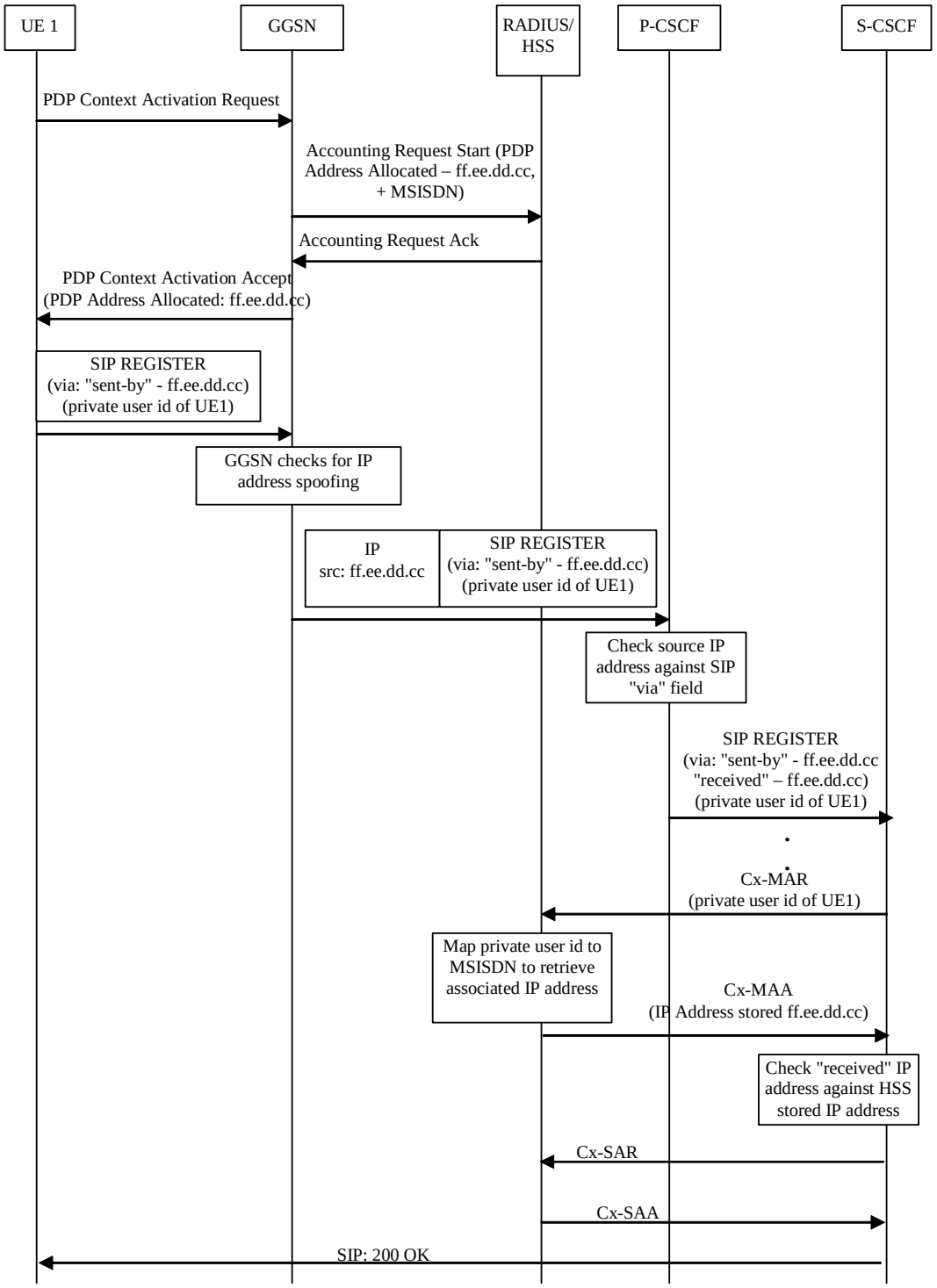
Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

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/ 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)
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc) (private 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) (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 stored IP address
Cx-SAR
Cx-SAA
SIP: 200 OK

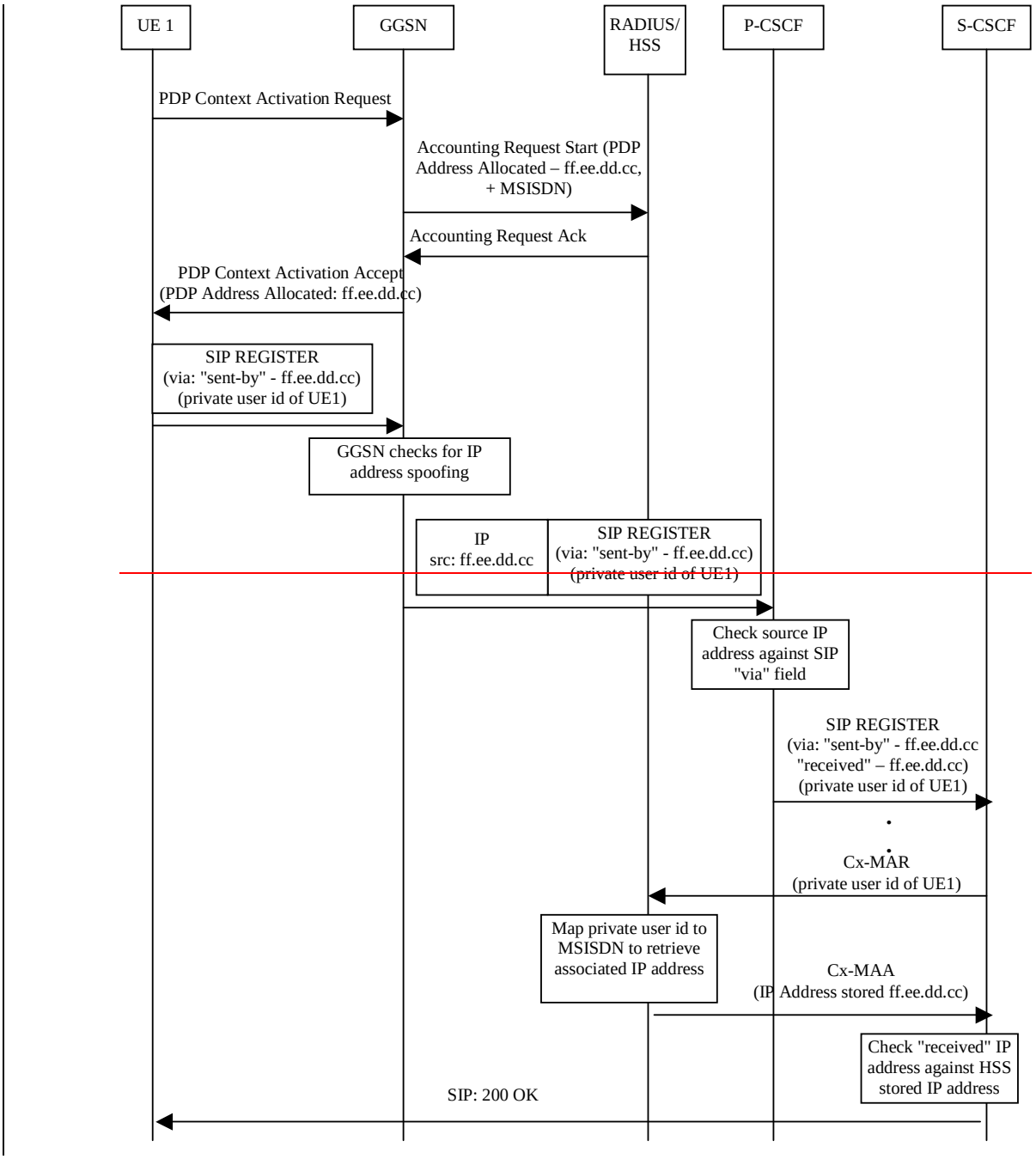
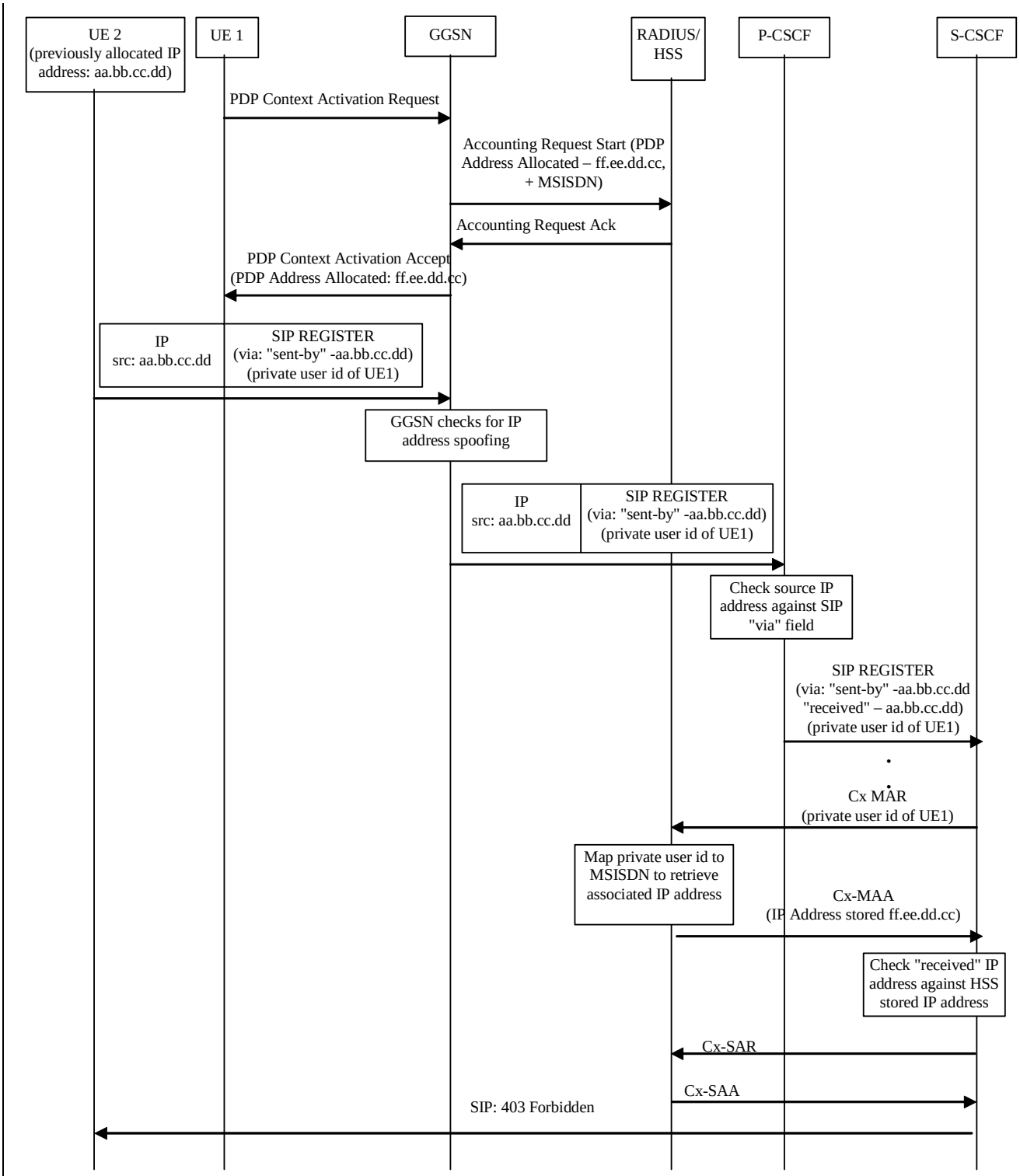


Figure 1: Message sequence for early IMS security showing a successful registration

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 “received” parameter is only present between 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 (via: "sent-by" -aa.bb.cc.dd) (private user id of UE1)
GGSN checks for IP address spoofing
IP src: aa.bb.cc.dd
SIP REGISTER (via: "sent-by" -aa.bb.cc.dd) (private user id of UE1)
Check source IP address against SIP "via" field
SIP REGISTER (via: "sent-by" -aa.bb.cc.dd "received" – aa.bb.cc.dd) (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 stored IP address
Cx-SAR
Cx-SAA
SIP: 403 Forbidden

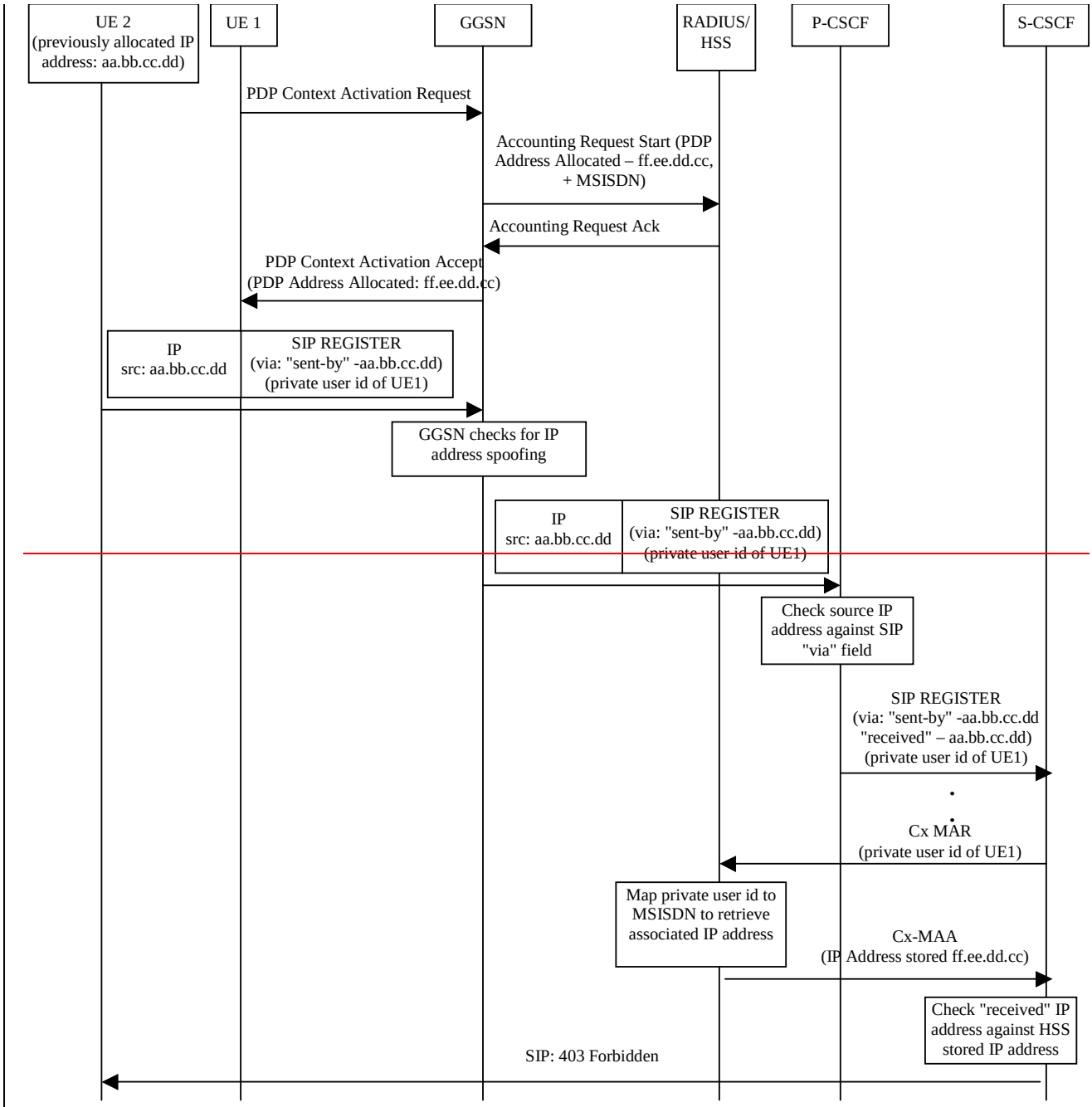
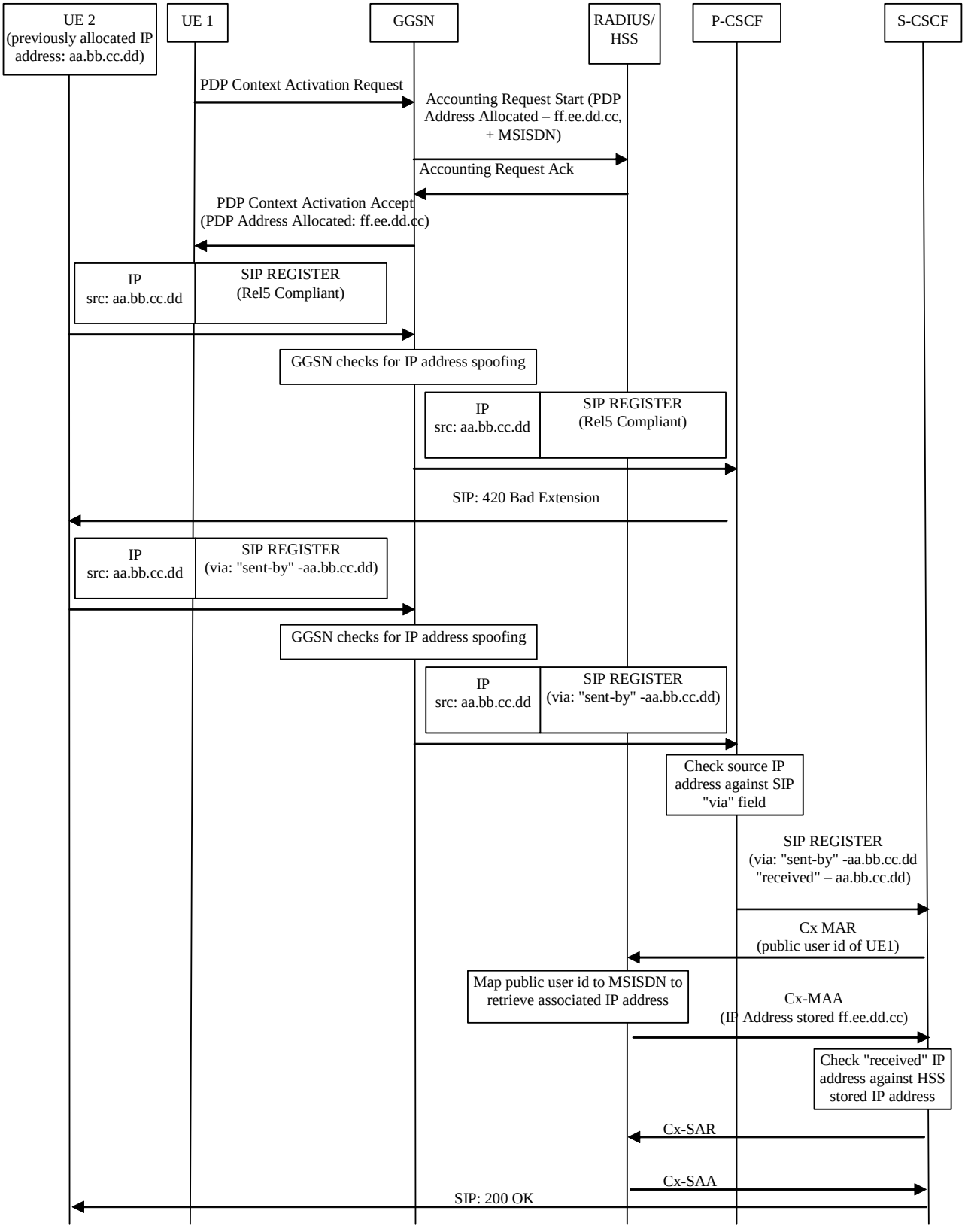


Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

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 “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
Cx-SAR
Cx-SAA
SIP: 200 OK

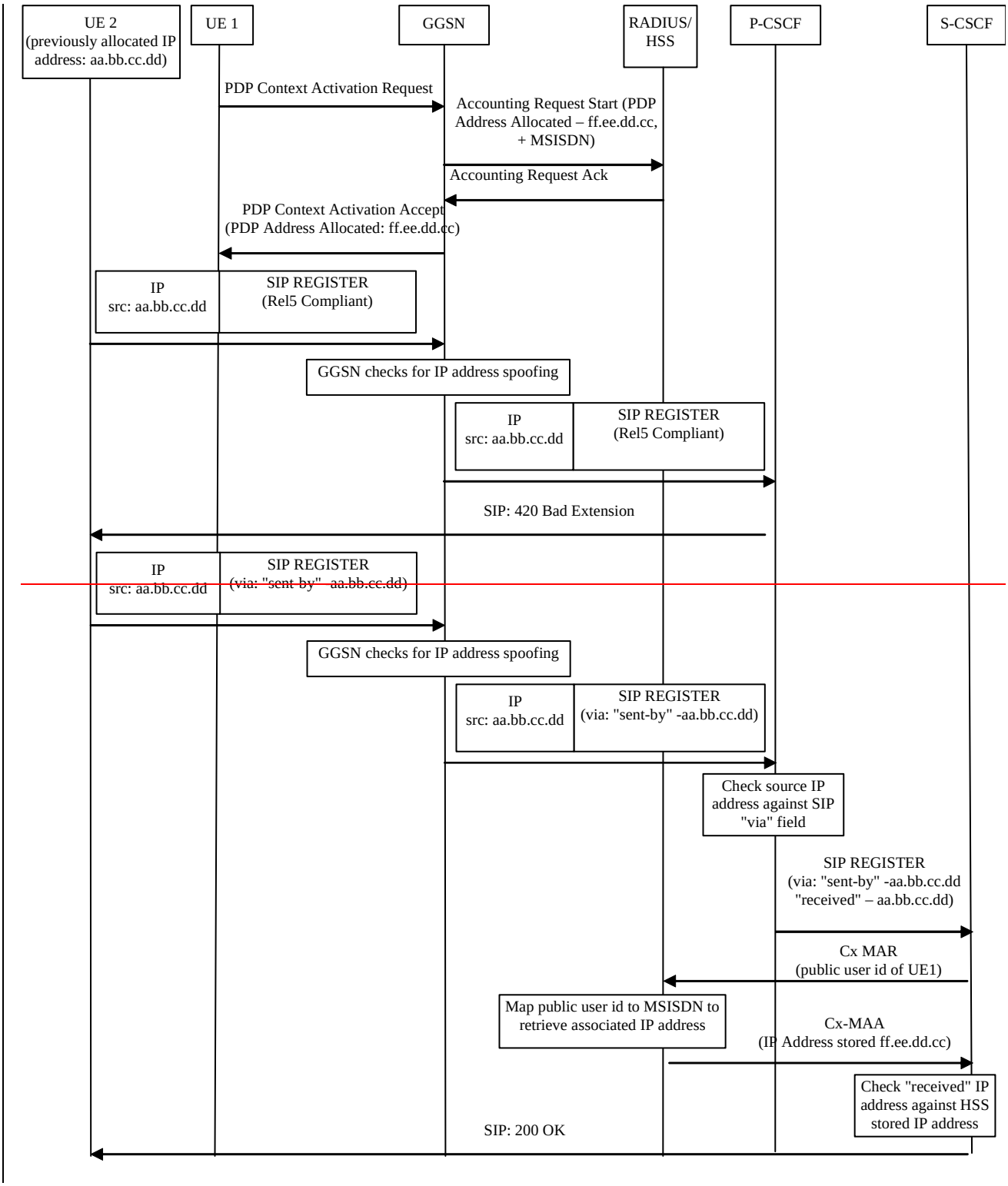


Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant and early IMS access security and network supports early IMS security only