

## PSEUDO CHANGE REQUEST

⌘ **TR 33.878 CR CRNum** ⌘ rev **-** ⌘ Current version: **0.0.2** ⌘

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

<b>Title:</b>	<span>⌘</span> Editorial changes, cleanup of editorís notes, clarifications		
<b>Source:</b>	<span>⌘</span> Vodafone		
<b>Work item code:</b>	<span>⌘</span> Early IMS Solution	<b>Date:</b>	<span>⌘</span> 07/10/2004
<b>Category:</b>	<span>⌘</span>	<b>Release:</b>	<span>⌘</span> Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<b>F</b> (correction)		<b>2</b> (GSM Phase 2)
	<b>A</b> (corresponds to a correction in an earlier release)		<b>R96</b> (Release 1996)
	<b>B</b> (addition of feature),		<b>R97</b> (Release 1997)
	<b>C</b> (functional modification of feature)		<b>R98</b> (Release 1998)
	<b>D</b> (editorial modification)		<b>R99</b> (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<b>Rel-4</b> (Release 4)
			<b>Rel-5</b> (Release 5)
			<b>Rel-6</b> (Release 6)

<b>Reason for change:</b>	<span>⌘</span> Reasons for change are listed in the summary of change.
<b>Summary of change:</b>	<ul style="list-style-type: none"> <li><span>⌘</span> • Clarification that the mechanism is not restricted to SIM-based GPRS access, but also supports USIM-based PS domain access.             <ul style="list-style-type: none"> <li>o Reason: need to make it clear that the mechanism is independent of whether SIM or USIM is used for PS domain access</li> </ul> </li> <li><span>⌘</span> • Delete editorís note about applicability to other access networks.             <ul style="list-style-type: none"> <li>o Reason: too late to include support for other access networks within Rel-6 timescales</li> </ul> </li> <li><span>⌘</span> • Delete editorís note that suggests IMPI-IMPU mappings other than one-to-one mappings may be possible.             <ul style="list-style-type: none"> <li>o Reason: too late to include support for other mappings within Rel-6 timescales</li> </ul> </li> <li><span>⌘</span> • Delete editorís note that suggests IMPI-IMPU mappings other than one-to-one mappings may be possible.             <ul style="list-style-type: none"> <li>o Reason: too late to include support for other mappings within Rel-6 timescales</li> </ul> </li> <li><span>⌘</span> • Clarification about which interfaces need to be modified             <ul style="list-style-type: none"> <li>o Reason: need to make it clear which stage 3 specifications are impacted.</li> </ul> </li> <li><span>⌘</span> • Delete editorís note that describes an alternative approach where IP address is checked in HSS rather than in S-CSCF.             <ul style="list-style-type: none"> <li>o Reason: no contributions supporting this alternative have been received.</li> </ul> </li> <li><span>⌘</span> • Delete editorís note that indicates that the exact specification of message contents is for further study.             <ul style="list-style-type: none"> <li>o Reason: detail of message contents can be left to CN stage 3 specifications.</li> </ul> </li> </ul>

- Add clarification text to Annex A.
  - Reason: SA approved work item specifies that a single solution should be standardised.
- Various editorial modifications.
  - Reason: improve clarity and readability of specification

**Consequences if not approved:** ☒ Not applicable

**Clauses affected:** ☒ Various

<b>Other specs affected:</b>	☒	<b>Y</b>	<b>N</b>	Other core specifications ☒	
		<b>Y</b>			
		<b>N</b>			Test specifications
		<b>N</b>			O&M Specifications

**Other comments:** ☒ When the new version of the TR is produced it is also proposed to include the specification number, TR 33.878.

---

## 4 Background and motivation

3GPP IMS provides an IP-based session control capability based on the SIP protocol. IMS can be used to enable services such as push to talk, instant messaging, presence and conferencing. It is understood that early implementations of these services will exist that are not fully compliant with 3GPP IMS. For example, it has been recognized that although 3GPP IMS uses exclusively IPv6, as specified in clause 5.1 of TS 23.221, there will exist IMS implementations based on IPv4 [1].

Non-compliance with IPv6 is not the only difference between early IMS implementations and 3GPP compliant implementations. In particular, it is expected that there will be a need to deploy some IMS-based services before products are available which fully support the 3GPP IMS security features defined in TS 33.203 [2]. Non-compliance with TS 33.203 security features is expected to be a problem mainly at the terminal side, because of the potential lack of support of the USIM/ISIM interface (especially in 2G-only devices) and because of the potential inability to support IPsec on some terminal platforms.

Although full support of TS 33.203 security features is preferred from a security perspective, it must be acknowledged that early IMS implementations will exist which do not support these features. Therefore, there is a need to ensure that simple, yet adequately secure, mechanisms are in place to protect against the most significant security threats that will exist in early IMS implementations. Furthermore, to maximise interoperability, it is important that these mechanisms are adequately standardised.

---

## 5 Requirements on interim solution

**Low impact on existing entities:** Any early IMS security mechanisms should be such that impacts on existing entities, especially on the UE, are minimised and would be quick to implement. It is especially important to minimise impact on the UE to maximise interoperability with early IMS terminals. The mechanisms should be quick to implement so that the window of opportunity for the interim solution is not missed.

**Adequate level of security:** Although it is recognised that the interim solution will be simpler than the full 3GPP IMS security solution, it should still provide an adequate level of security to protect against the most significant security threats that will exist in early IMS implementations. As a guide, the strength of subscriber authentication should be comparable to the level of authentication provided for existing chargeable services in mobile networks.

**Smooth and cost effective migration path to 3GPP solution:** Clearly, any security mechanisms developed for early IMS systems will provide a lower level of protection compared with that offered by the full set of 3GPP IMS security features. The security mechanisms developed for early IMS systems should therefore be considered as an interim solution and migration to the full set of 3GPP IMS security features should take place as soon as suitable products become available at an acceptable cost. In particular, the interim solution should not be used as a long-term replacement for full 3GPP IMS security. It is important that the interim solution allows a smooth and cost-effective migration path to the full 3GPP solution.

**Co-existence with 3GPP solution:** It is clear that terminals supporting the interim solution will need to be supported even after 3GPP compliant terminals are deployed. The interim solution should therefore be able to co-exist with the full 3GPP solution. In particular, it shall be possible for the SIP/IP core to differentiate between a subscription using interim security mechanisms and a subscription using the full 3GPP solution.

**Protection against bidding down:** It should not be possible for an attacker to force the use of the interim solution when both the terminal and the network support the full 3GPP solution.

**No restrictions on the type of charging model:** Compared with full 3GPP IMS security solution, the interim solution should not impose any restrictions on the type of charging model that can be adopted.

**Standardisation of a single interim solution:** Interfaces that are impacted by the interim solution should be adequately standardised to ensure interoperability between vendors. To avoid unnecessary complexity, a single interim solution should be standardised.

**Support access over 3GPP PS domain:** Currently the main requirement is to support secure access over the 3GPP PS domain (including GSM/GPRS and UMTS access). Access based on WLAN scenario 2, or other alternative access networks, is a lower priority.

~~Editor's note: The solution described in this TR is primarily focused on secure access over 3GPP PS domain. Applicability of the solution to other access networks is ffs.~~

**Low impact on provisioning:** The impact on provisioning should be low compared with the full 3GPP solution.

---

## 6 Threat scenarios

To understand what controls are needed to address the security requirements, it is useful to describe some of the threat scenarios.

NOTE: There are many other threats, which are outside the scope of this TR.

### 6.1 Impersonation on IMS level using the user identity of an innocent user

The scenario proceeds as follows:

- Attacker A attaches to GPRS, GGSN allocates IP address, IPgprs-a
- Attacker A registers in the IMS using his IMS identity, IDims-a
- Attacker A sends SIP invite using his own source IP address (IPgprs-a) but with the IMS identity of B (IDims-b).

If the binding between the IP address on the bearer level, and the public and private user identities is not checked then the attacker will succeed, i.e. A pays for IP connectivity but IMS service is fraudulently charged to B. The fraud situation is made worse if IP flow based charging is used to "zero rate" the IP connectivity.

The major problem is however that without this binding multiple users within a group of friends could sequentially (or possibly simultaneously) share B's private/public user identities, and thus all get (say) the push-to-talk service by just one of the group paying a monthly subscription. Without protection against this attack, operators could be restricted to IP connectivity based tariffs and, in particular, would be unable to offer bundled tariffs. This is unlikely to provide sufficiently flexibility in today's market place.

### 6.2 IP spoofing

The scenario proceeds as follows:

- User B attaches to GPRS, GGSN allocates IP address, IPgprs-b
- User B registers in the IMS using his IMS identity, IDims-b
- Attacker A sends SIP messages using his own IMS identity (IDims-a) but with the source IP address of B (IPgprs-b)

If the binding between the IP address that the GGSN allocated the mobile in the PDP context activation and the source IP address in subsequent packets is not checked then the attacker will succeed, i.e. A pays for IMS service but IP connectivity is fraudulently charged to B. Note that this attack only makes sense for IMS services with outgoing traffic only because the attacker will not receive any incoming packets addressed to the IMS identity that he is impersonating.

### 6.3 Combined threat scenario

The scenario proceeds as follows:

- User B attaches to GPRS, GGSN allocates IP address, IPgprs-b
- User B registers in the IMS using his IMS identity, IDims-b
- Attacker A sends SIP messages using IMS identity (IDims-b) and source IP address (IPgprs-b)

If the bindings mentioned in the scenarios in section 6.2 and 6.3 are not checked then the attacker will succeed, i.e. A fraudulently charges both IP connectivity and the IMS service to B. Note this attack only makes sense for IMS services with outgoing traffic only because the attacker will not receive any incoming packets addressed to the IMS identity that he is impersonating.

---

## 7 Specification of interim IMS security

### 7.1 Overview

The interim 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 [SIM-based GPRS-PS domain bearer level](#) security context.

The GGSN, terminating each user's authenticated PDP context, provides the user's IP address / MSISDN pair to the HSS when a PDP context is activated towards the IMS system. The HSS has a binding between the MSISDN and the IMPI, and is therefore able to store the currently assigned IP address from the GGSN against the user's IMPI. 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 IMPI, 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 IMPI in the HSS.

The mechanism assumes that the GGSN does not allow a mobile 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 mobile (the assumption here, as well as for [the full 3GPP-compliant IMS systems 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 section 6 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.

~~Editor's Note: It is for further study whether the mechanism shall be extended to support the case that one IMPU may be associated with several IMPIs, or whether the mechanism shall be restricted to only support the case that there is a one-to-one mapping between IMPI and IMPU.~~

In early IMS the IMS user authentication is performed by linking the IMS registration (based on an IMPI) to an authenticated PDP context (based on an 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.

~~Editor's Note: It is for further study whether the mechanism shall be extended to support one-to-many or many-to-many relationships between the IMSI for bearer access and the IMPI for IMS access.~~

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. ~~Note however that w~~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 mobile](#) are standardised for vendor interoperability reasons.

## 7.2 Detailed specification

### 7.2.1 Update of mobile's 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 UE's 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 subscriber's IMPI (derived from IMSI) and then store the IP address against the IMPI.

NOTE: 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.

**Editor's note:** An alternative approach would be 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 such that the HSS will not specifically need to support RADIUS (existing DIAMETER functionality of HSS can be re-used). This is ffs.

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 following mechanisms in the following sub-sections shall be supported ~~are required~~ 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 `sent-by` parameter of the top `Via` 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 `received` parameter exists in the top `via` header field. 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, 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 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.

~~Editor's Note: — It is for further study whether an alternative approach where the IP address is checked in the HSS rather than in the S-CSCF should be adopted. With this alternative the HSS would provide the IP address to the HSS during each initial REGISTER and accept the REGISTER only if the HSS returns a positive result. For subsequent non-initial REGISTER requests, the S-CSCF would then check the received IP address against the IP address stored during the initial REGISTER.~~

## 7.2.4 Identification of terminals supporting the interim solution

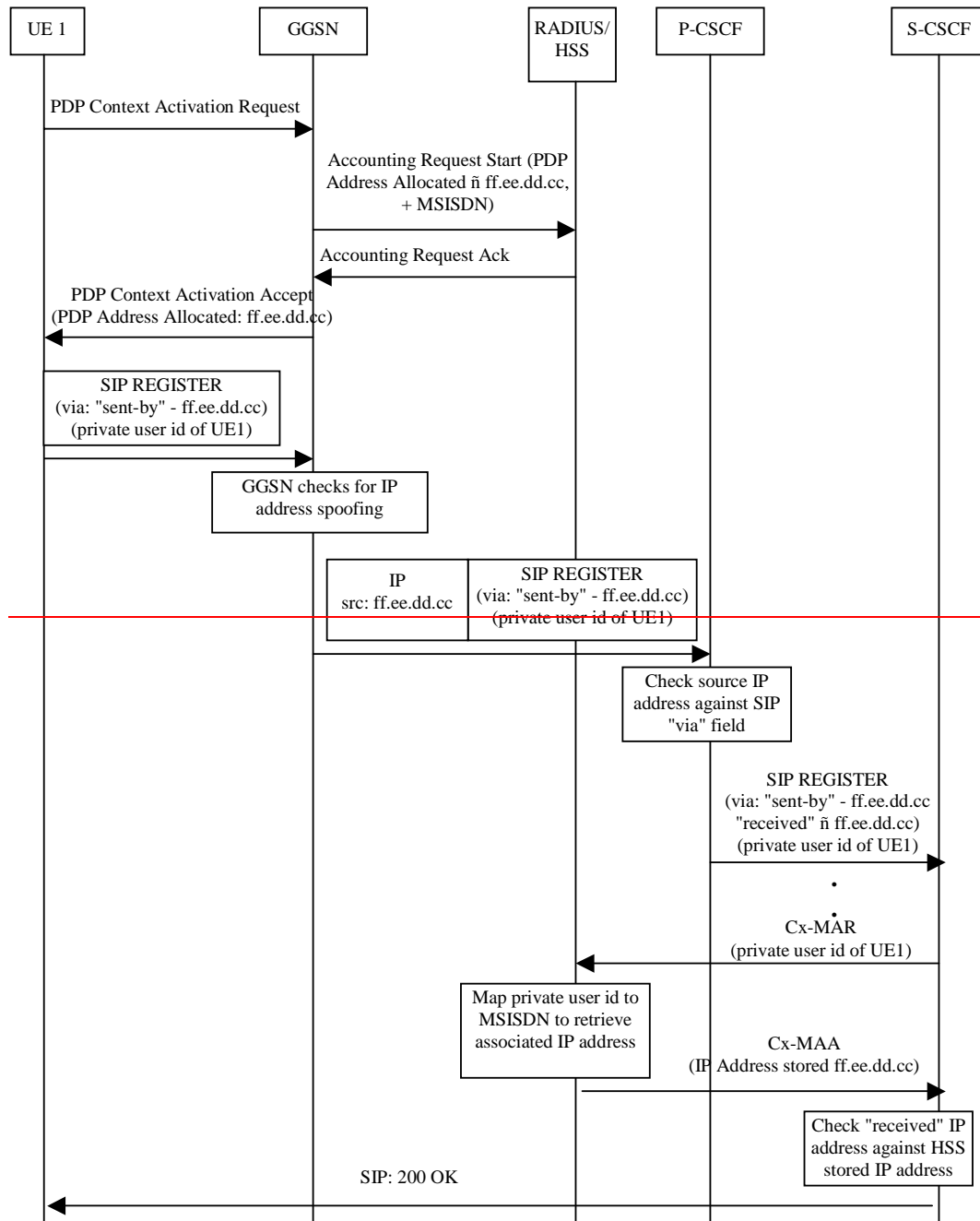
At some stage, it is expected that both fully 3GPP compliant terminals and terminals implementing the interim security solution will access the same IMS. Therefore, some indication shall be given that a terminal supports the interim solution rather than the full 3GPP solution.

~~Editor's note: The exact format, and means to carry this information, is for further study.~~

## 7.2.5 ~~7.2.5~~ Message flows

### 7.2.5.1 Successful registration

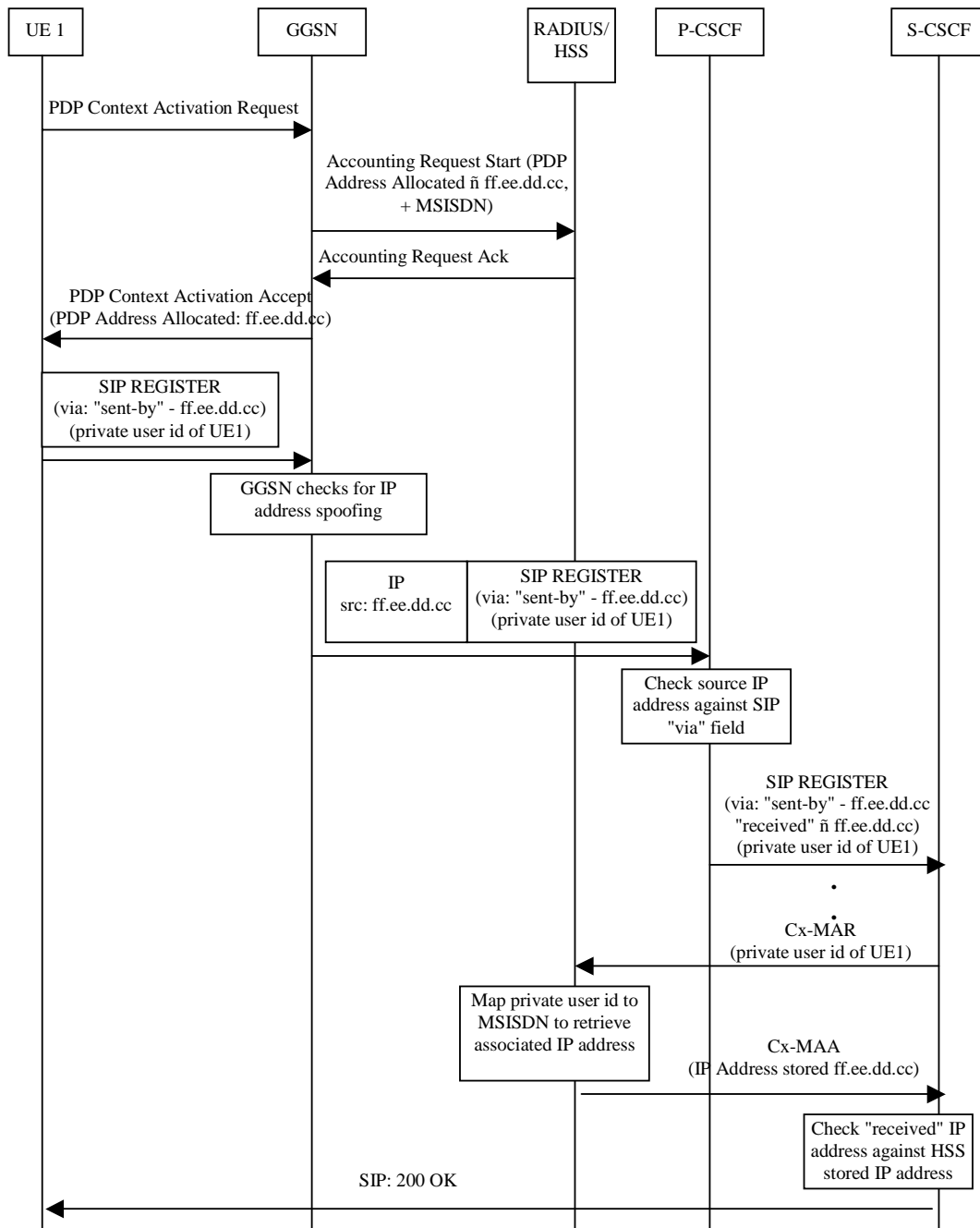
~~Editor's Note: The exact specification of message contents is for further study. Changes to the Cx interface MAR/MAA commands would need to be specified in the appropriate CN4 specifications.~~



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

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





**Figure 1: Message Sequence for Interim Security Solution (successful registration)**

## 7.2.5.1 Unsuccessful registration

Figure 2

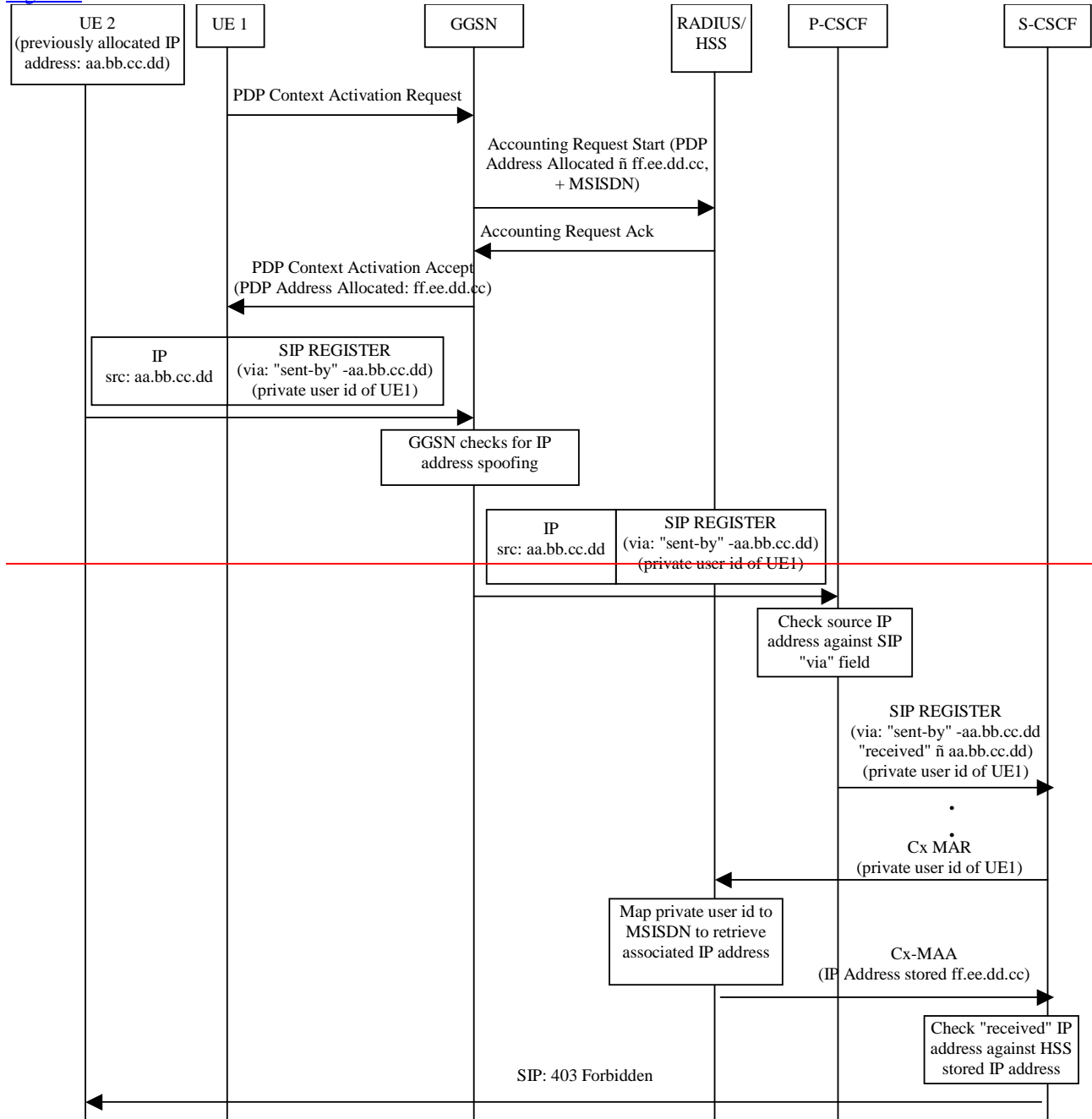


Figure 2 below gives an example message flow for the unsuccessful attempt of an attacker trying to spoof the IMS identity of a valid IMS user.

Again, the "received" parameter is only present between P-CSCF to S-CSCF under the conditions given in section 7.2.3.1.

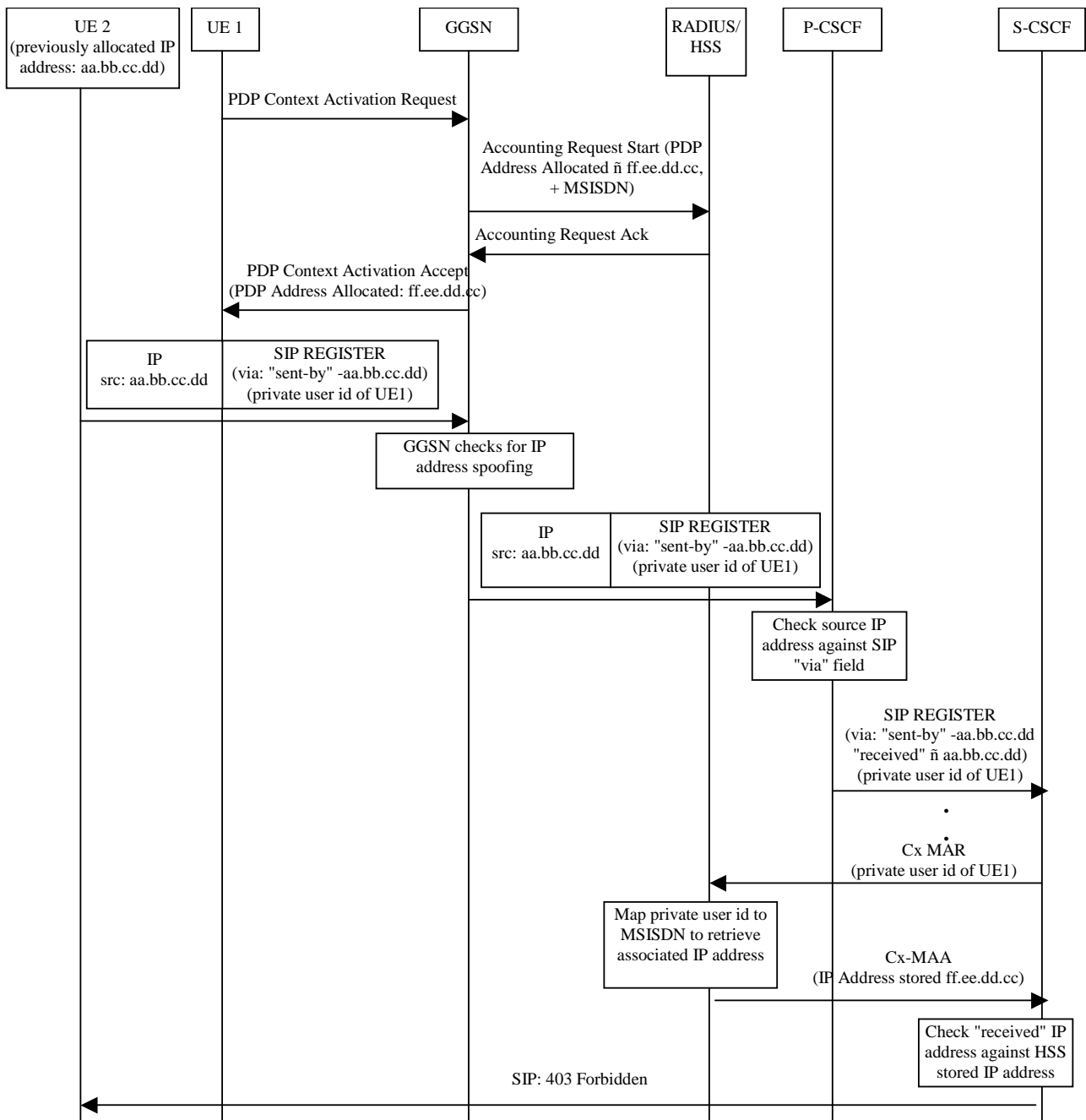


Figure 2: Message Sequence for Interim Security Solution showing an unsuccessful identity theft

## Annex A: Comparison with alternative approaches

An alternative approach is/would have been to use password-based authentication for early IMS implementations. For example, HTTP Digest could have been used for authenticating the IMS subscriber. This method would have required a subscriber-specific password to be provisioned on the IMS terminal. This alternative was not selected by 3GPP due to ~~Compared with the approach specified in section 7, password-based authentication has~~ the following disadvantages:

- It imposes restrictions on the type of charging schemes that can be adopted. In particular, if a subscriber could find out his or her own password from an insecure implementation on the terminal, then he or she could share the IMS subscription with friends. This could impact revenue for the operator if bundled or partly subscription based tariffs are used rather than purely usage based tariffs. For example, a subscriber could take out a subscription for 100 instant messages and then share this with his or her friends. Although contractual obligations could be

imposed on customers to prohibit this behaviour, in practice this would be difficult to enforce. If charging were purely usage based then there would be no incentive for the subscriber to do this (and no impact on operator revenue). The solution specified in section 7 is flexible in allowing a range of different charging models including bundled or partly subscription based tariffs.

- It provides a weak form of subscriber authentication compared with the levels of authentication used for other services offered over 3GPP networks, where authentication is typically based directly or indirectly on the (U)SIM. This has implications on the reliability of charging, and on the level of assurance that can be given to the customer that their communications cannot be masqueraded. In the solution specified in section 7, authentication of the IMS subscriber is indirectly based on (U)SIM authentication at the GPRS level. The level of security is similar to that currently used for certain WAP services, where the user's MSISDN is provided by the GGSN to the WAP gateway. Security does not rely on the terminal securely storing any long-term secret information (e.g. passwords).
- Provisioning is more complex since subscriber-specific information (i.e. passwords) must be installed in each mobile.

---

Annex **A****B**:  
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
29/6/04					First version based on input from S3-040264 and S3-040265.		0.0.1
8/7/04					Incorporates comments received at SA3#34.	0.0.1	0.0.2