3GPP TSG SA WG3 Security — S3#36 **S3-041000**
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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Completion of introductory sections and other editorial changes		
Source:	⌘	Vodafone		
Work item code:	⌘	Early IMS	***Date:*** ⌘	16/11/2004
Category:	⌘	**F** *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.	***Release:*** ⌘	Rel-6 *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:	⌘	
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘					
		Y	**N**			
Other specs affected:	⌘		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.

Introduction

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 fully 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 UE 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 UE platforms.

Although full support of TS 33.203 security features is preferred from a security perspective, it is 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.

~~*This clause is optional. If it exists, it is always the second unnumbered clause.*~~

1 Scope

~~*This clause shall start on a new page. No text block identified. Should start:*~~

The present document specifies an interim security solution for early IMS implementations that are not fully compliant with the IMS security architecture specified in 3GPP TS 33.203 [2]. ~~…~~

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 21.905: " Vocabulary for 3GPP Specifications ".

3 Definitions, symbols and abbreviations

~~*Delete from the above heading those words which are not applicable.*~~

~~*Subclause numbering depends on applicability and should be renumbered accordingly.*~~

3.1 Definitions

For the purposes of the present document, the ~~[following]~~ terms and definitions ~~[~~given in TS 21.905 [x] ~~…~~ and the following~~]~~ apply.

~~*Definition format*~~

*<**defined term**>: <definition>.*

ExampleEarly IMS: text used to clarify abstract rules by applying them literallya UE or network element implementing the early IMS security solution specified in the present document.

Fully compliant IMS: a UE or network element implementing the IMS security solution specified in TS 33.203 [2]..

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format

Cx	Reference Point between a CSCF and an HSS.
<symbol>	<Explanation>

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

Abbreviation format

<ACRONYM>	<Explanation>
AAA	Authentication Authorisation Accounting
APN	Access Point Name
CSCF	Call/Session Control Function
GGSN	Gateway GPRS Support Node
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
IMPI	IM Private Identity
IMPU	IM Public Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	IP Security protocol
ISIM	IMS Subscriber Identity Module
NAT	Network Address Translation
P-CSCF	Proxy-CSCF
PDP	Packet Data Protocol
S-CSCF	Serving-CSCF
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
UE	User Equipment

4 Background

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 fully 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 UE 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 UE platforms.

Although full support of TS 33.203 security features is preferred from a security perspective, it is 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.

54 Requirements

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 UEs. The mechanisms should be quick to implement so that the window of opportunity for the early IMS security solution is not missed.

Adequate level of security: Although it is recognised that the early IMS security solution will be simpler than the fully compliant 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 fully compliant 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 fully compliant 3GPP IMS security featuressolution. The security mechanisms developed for early IMS systems should therefore be considered as an interim solution and migration to the fully compliant IMS security solutionfull set of 3GPP IMS security features should take place as soon as suitable products become available at an acceptable cost. In particular, the early IMS security solution should not be used as a long-term replacement for the fully compliant IMS security solutionfull 3GPP IMS security. It is important that the early IMS security solution allows a smooth and cost-effective migration path to the fully compliant IMS security full 3GPP solution.

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

Protection against bidding down: It should not be possible for an attacker to force the use of the early IMS security solution when both the UE and the network support the fully compliant IMS security 3GPP solution.

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

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

Support access over 3GPP PS domain: It is a requirement is to support secure access over the 3GPP PS domain (including GSM/GPRS and UMTS access).

Low impact on provisioning: The impact on provisioning should be low compared with the fully compliant IMS security 3GPP solution.

65 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.

65.1 Impersonation on IMS level using the identity of an innocent user

The scenario proceeds as follows:

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

65.2 IP spoofing

The scenario proceeds as follows:

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

If the binding between the IP address that the GGSN allocated the UE 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.

65.3 Combined threat scenario

The scenario proceeds as follows:

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

If the bindings mentioned in the scenarios in clause 56.2 and 56.3 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.

76 Specification

76.1 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, 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 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 ~~6~~ 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 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.

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.

~~7~~6.2 Detailed specification

~~7~~6.2.1 Update of UE'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.

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~~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 and log the event in its security log against the subscriber information (IMSI/MSISDN).

~~7~~6.2.3 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~~6.2.3.1 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~~6.2.3.2 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.

76.2.4 Interworking cases

It is expected that both fully 3GPP 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 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.

Editor's 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 IMS 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 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 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 IMS UEs). The IMS private identity shall therefore be derived from the subscriber's 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 "IP-based" 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 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 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

   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 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. Fully compliant IMS 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 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 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 IMS security headers. The network shall respond with a 200 OK message according to the registration message flow as specified in clause 67.2.5.1.

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 IMS UE is fully compliant and shall continue as specified by TS 33.203.

5. UE supports early IMS only, IMS network supports fully compliant IMS 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 "Authentication Failed" 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 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 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 IMS security according to TS 33.203 is not supported.

7.2.5 7.2.5 Message flows

7.2.5.16.2.5.1 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 76.2.3.1.

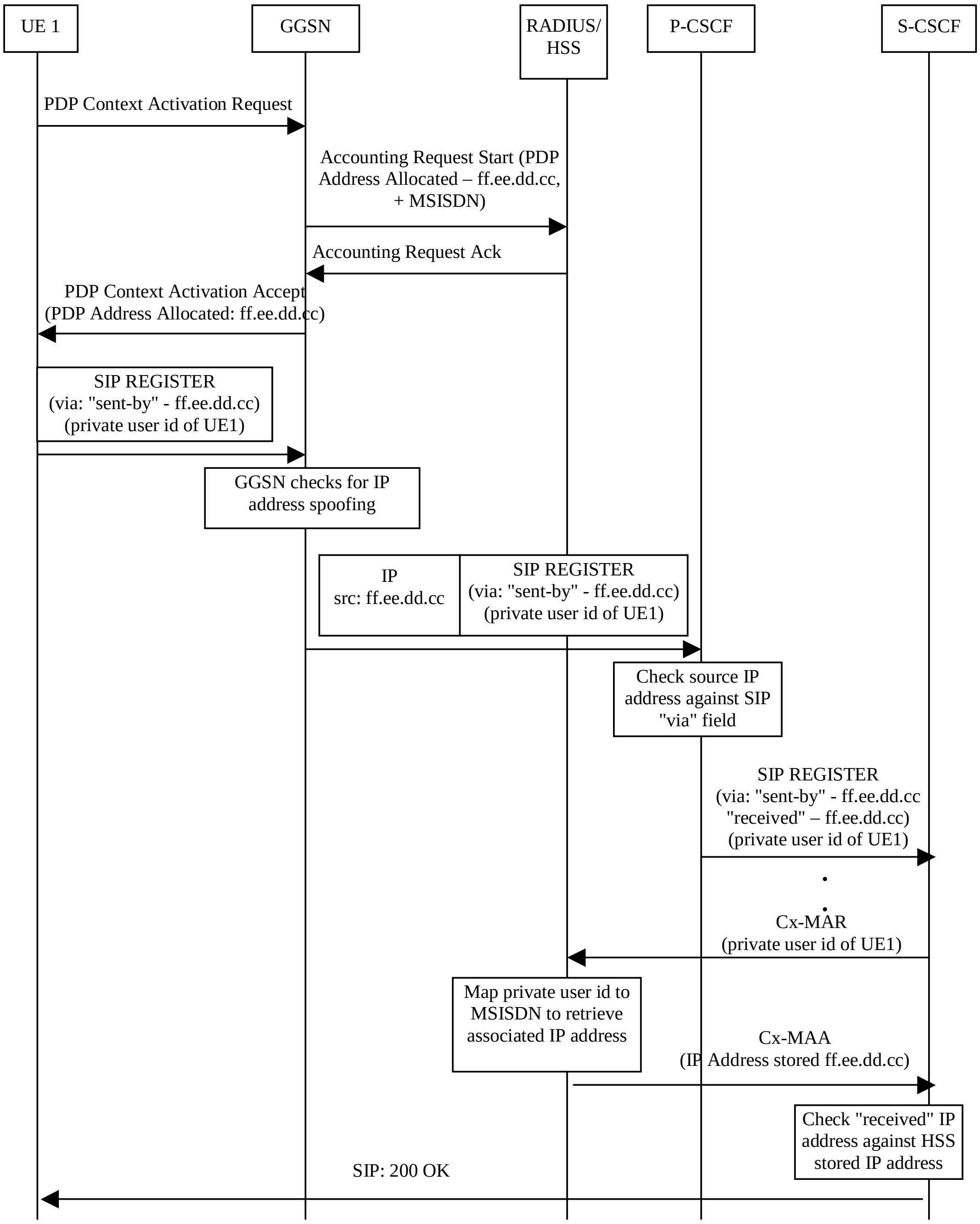

Figure 1: Message sequence for early IMS security showing a successful registration

~~7~~6.2.5.2 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~~6.2.3.1.

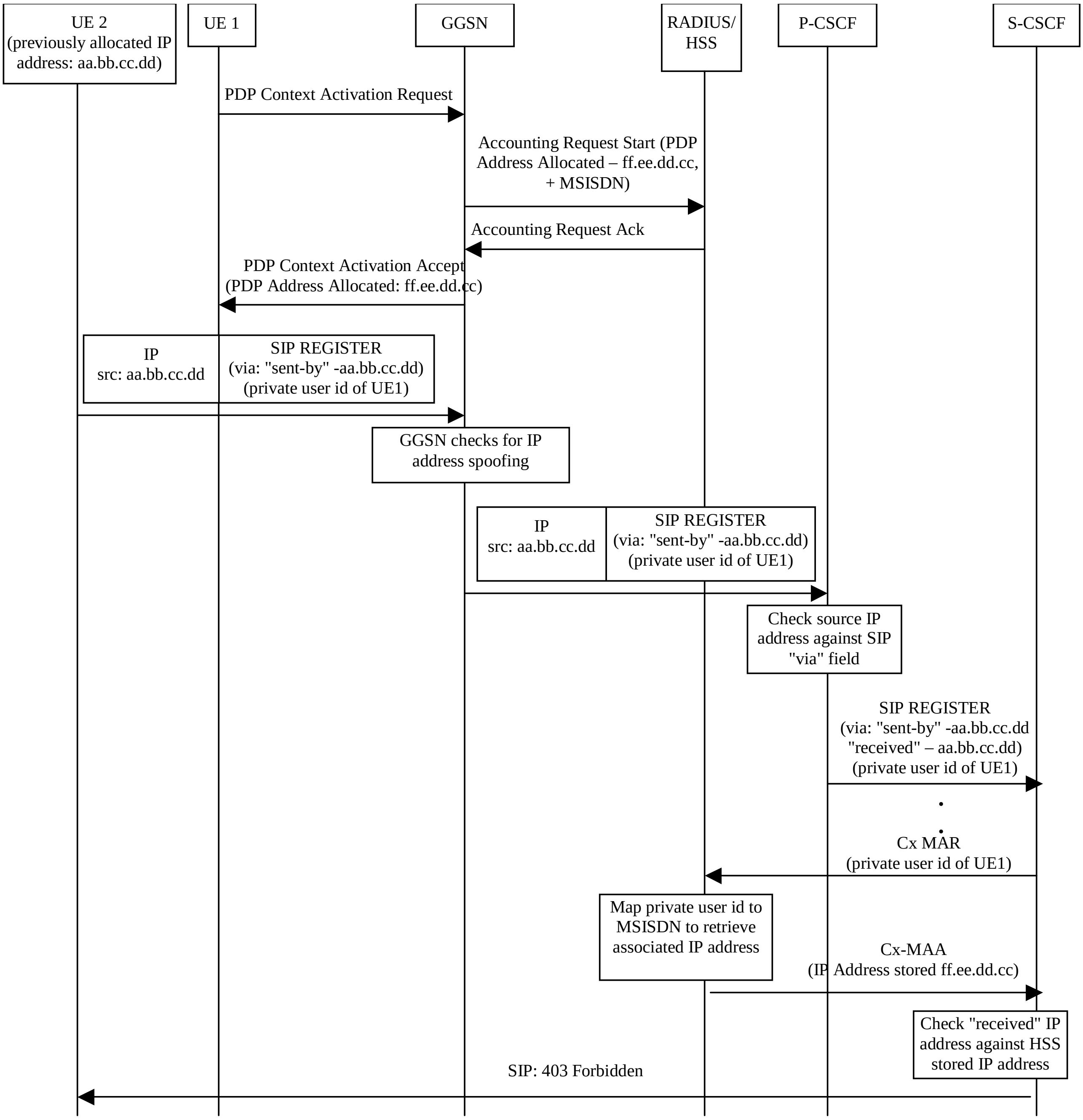

Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

~~7~~6.2.5.3 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 IMS and early IMS access security and the network supports early IMS only. This case is denoted as case 3 in clause ~~7~~6.2.4.

Note, that the "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause ~~7~~6.2.3.1.

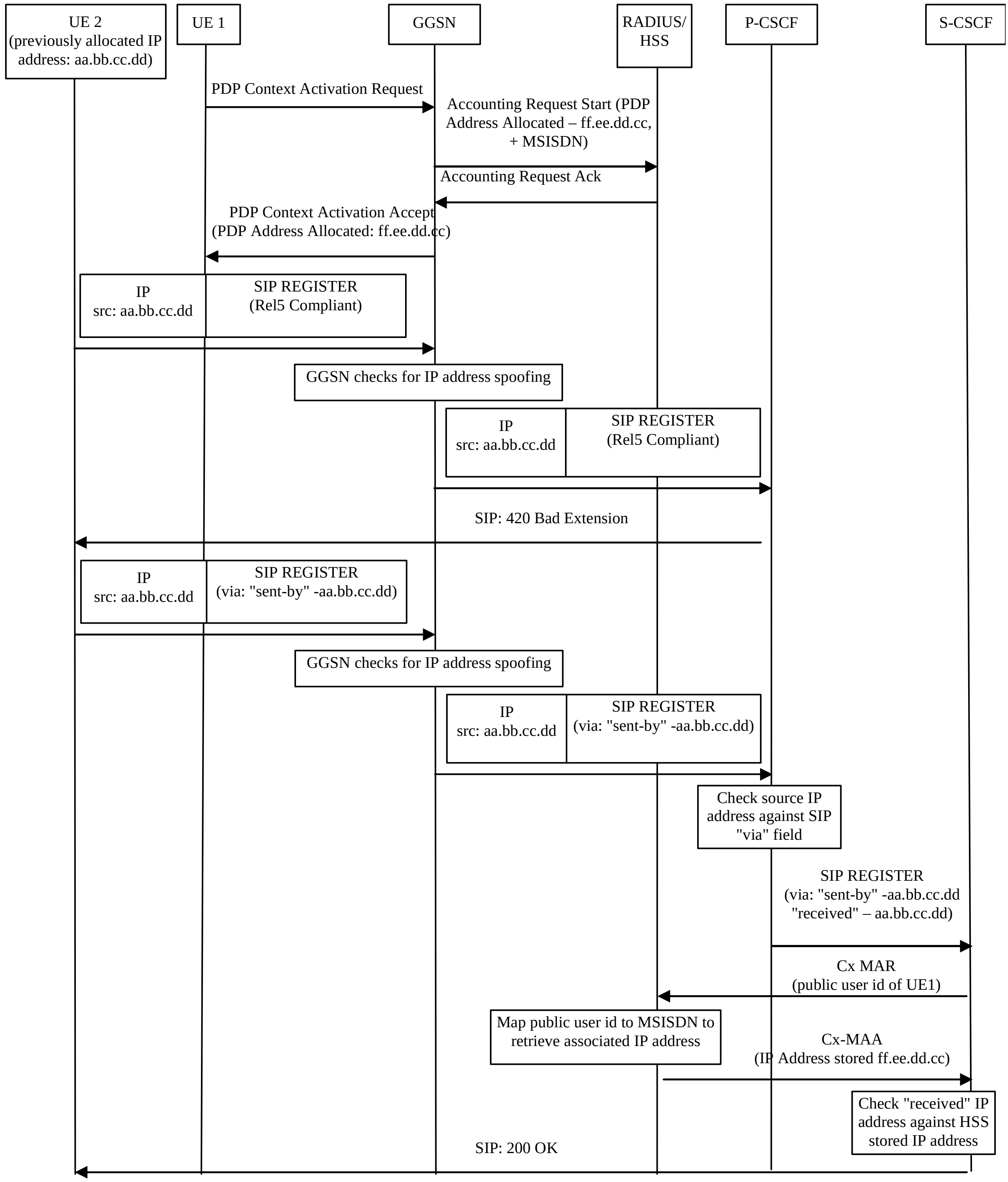

Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant IMS and early IMS access security and network supports early IMS security only

Annex A: Comparison with an alternative approach – HTTP Digest

An alternative approach would have been to use password-based authentication for early IMS implementations. For example, HTTP Digest (IETF RFC 2617) could have been used for authenticating the IMS subscriber. The HTTP Digest method is a widely supported authentication mechanism. It is not dependent of the GPRS network and it does not require new functional elements or interfaces in IMS network. However, this method would have required a subscriber-specific password to be provisioned on the IMS UE. This alternative is not adopted for use in early IMS systems.

The HTTP Digest method has the following advantages and disadvantages:

Advantages:

- Fully standardized and supported by RFC 3261 [6] compliant implementations and therefore by 3GPP TS 24.229 [7] compliant implementations (SIP protocol mandates support of HTTP Digest).

Editor's note: The following bullet point is still under study for inclusion in this section.

- HTTP Digest enables access via multiple technologies (e.g. WLAN). Note that this is not considered an advantage in the context of early IMS systems since it is specified in clause 4~~5~~ that it is only a requirement to support secure access over the 3GPP PS domain (including GSM/GPRS and UMTS access).

- HTTP Digest can support partial message integrity protection for those parts of the message used in the calculation of the WWW-Authenticate and Authorization header field response directive values (when qop=auth-int).

- HTTP Digest implementations can employ methods to protect against replay attacks (e.g. using server created nonce values based on user ID, time-stamp, private server key, or using one-time nonce values).

Disadvantages:

- HTTP Digest may impose restrictions on the type of charging schemes that can be adopted by an operator. In particular, if a subscriber could find out his or her own password from an insecure implementation on the UE, 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 without employing special protection mechanisms, e.g. disallow multiple binding to a single IP address. If charging were purely usage based then there would be no incentive for the subscriber to do this, therefore using HTTP Digest may not impact on operator's revenue. The solution specified in clause 6~~7~~ is flexible in allowing a range of different charging models including bundled or partly subscription based tariffs.

- HTTP Digest provides a weaker form of subscriber authentication when 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. Subscription authentication depends, among other things, on the strength of the password used as well as on the password provisioning methods, such as bootstrapping passwords into the IMS capable UE. A weak subscriber authentication, vulnerable to dictionary attacks, 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 clause 6~~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 UE securely storing any long-term secret information (e.g. passwords).

- HTTP Digest provisioning is more complex since subscriber-specific information (i.e. passwords) must be installed or bootstrapped into each IMS UE.

Annex 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
8/10/04					Incorporates changes agreed at SA3#35.	0.0.2	0.0.3