3GPP TSG SA WG3 Security **S3-040867**

5 - 8 October 2004

St Paul's Bay, Malta, October 5-8, 2004

Title:	LS on Revisiting forwards compatibility towards TLS based access security
Release:	Rel-6
Source:	SA3
To:	SA2, SA1
Cc:	CN1, CN4

Contact Person:

Name:	Bengt Sahlin
Tel. Number:	+358 40 7784580
E-mail Address:	bengt.sahlin@ericsson.com

Attachments: S3-040762 (Updated discussion paper on the problem statement)
S3-040868 (Proposed CR)

---

1. Overall Description:

SA3 has continued discussions on potential future backwards compatibility problem related to the way IMPI, IMPU and Home Network Domain Name are specified in ISIM related specifications. An updated CR has been provided in S3-040868 that proposes that the naming restrictions are relaxed: it is not necessary that these naming rules are visible to the end-user, and consequently there will be no new requirements related to IMPUs, while IMPI and Home Network Domain Name are still affected. SA3 needs to further study if the naming requirements resolves the potential future backwards compatibility problem for the roaming case.

SA3 would like to ask if the naming requirements are acceptable from SA1 and SA2 point of view.

2. Actions:

To SA1 and SA2

ACTION: SA3 kindly asks SA1 and SA2 if the naming requirements are acceptable from SA1 and SA2 point of view.

To SA2

ACTION: SA3 kindly asks SA2 to take note of the above decision.

3. Date of Next TSG-SA3 Meetings:

SA3#36	23 - 26 November 2004	Shenzhen, China

3GPP TSG SA WG3 Security **S3-040762**

5 - 8 October 2004

St Paul's Bay, Malta, October 5-8, 2004

Agenda Item: IMS

Source: Ericsson

Title: Revisiting forwards compatibility towards TLS based access security

Document for: Discussion/Decision

1. Discussion

SA3#34 adopted new naming requirements to 33.203 R6 related to potential future use of TLS in IMS access security. The requirements were adopted in order to avoid a future backwards compatibility problem if 3GPP decides to use TLS for access security some day in the future. In one TLS deployment model, it will be practically impossible for UE to figure out if the visited network should be trusted and if it belongs to the same trust domain with the home network. See more technical details in Appendix A.

SA3#34 sent LS to CN1, CN4 and SA2. In these groups, the LS caused worries on end-user experience, especially because it set naming restrictions to public user identities (IMPUs). The general feeling was that the naming restrictions should not be visible to the end-user.

The CR was also discussed in SA Plenary. Similar concerns were repeated, and the CR was rejected.

Ericsson agrees on the concerns related to IMPU naming, and would like to propose an updated version of the CR in which the naming restrictions are limited to those naming schemes which are not visible to the user, i.e. home network names and IMPIs. In fact, from security point of view, there is no need to have naming restrictions on IMPUs. The username that is authenticated in IMS access security is IMPI, and IMPUs are not directly involved.

New versions of the CR and the LS are attached to this document.

Appendix A: Technical analysis presented in TD S3-040531

2. Background

There are no current plans in SA3 to use TLS for IMS access security. However, there are some reasons why this may become interesting option in the future:

- TLS is the only mandatory access security mechanism that all SIP servers support. Consequently, it is very likely that there will be SIP terminals that support TLS but not IPsec. 3GPP may want to exploit this terminal base in the future.
- IMS UE must have TLS in Release 6 for Presence. Using the same security solution with IMS related applications would make sense from UE perspective.
- One reason why TLS was not accepted as IMS access security solution in R5 was that TLS couldn't be used with UDP. However, there have been proposals for creating a TLS variant that could do this, i.e. WTLS in former WAP forum, and recent work in IETF on DTLS (Rescorla & Modadugu 2004).

Figure 1 demonstrates the general differences between the IPsec and TLS based access security solutions. The IPsec based solution handles the security agreement and (UDP related) re-transmission at SIP layer while the TLS based solution would do these at TLS and transport layer. On the other hand, the message protection itself is located either over IP (IPsec) or transport (TLS).

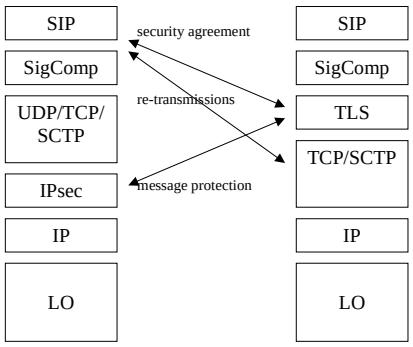


Figure 1: Change of responsibilities in protocols stack

3. Forwards compatibility requirements

Even though this document does not propose that TLS should be used in IMS for access security, it is still important to keep this option open for future. TLS could be applied in several formats for IMS in the similar way that SA3 has already discussed with HTTPS context. This section analyzes forwards compatibility requirements with three main deployment models, i.e. shared key based UE authentication with certificate-based P-CSCF authentication, certificate based mutual authentication, and shared key based mutual authentication.

3.1 Shared key based UE authentication with certificate based P-CSCF authentication

In this case, TLS would be used in the mode where the server side was authenticated using TLS server certificate, and the client using HTTP Digest AKA. TLS connection would be set up using SIP REGISTER message, and then left open for further SIP messages (cf. registration procedure in RFC 3261). Note that using a UAC initiated TLS connection to receive SIP requests to UAS is possible in this model, however, it may require some specific features from SIP/TLS implementation. Note also that TLS session cannot be resumed from P-CSCF side; only UE is able to resume TLS sessions.

There are two general recommendations specified in RFC 3261 related to server side naming of SIP registrars (see section "26.3.2.1 Registration" in Security Considerations). Firstly, UAs should not trust on the registrar (or first-hop proxy such as P-CSCF) unless the domain name in TLS server certificate match the name of the home domain of the UA (or chain back to a trusted root certificate which belongs to the UA's home domain). Secondly, the realm parameter in the HTTP Digest authentication header should also match the TLS server certificate. If these two conditions are not met, the UA is not able to verify if the registrar/first-hop proxy is authorized to act in that role (i.e. potential man-in-the-middle attack). Also in IMS, the registration procedure should be done using a TLS server certificate that somehow chain back to the home domain of the UE. That is, the site TLS certificate should identify a host within the domain of the UE. Furthermore, the realm parameter in the WWW-Authenticate header should somehow correspond with the site certificate received from P-CSCF.

All entities that support TLS must also have a mechanism for validating certificates during TLS negotiation. In practice, this means that all these entities must belong to some PKI, and possess one or more trusted root certificate/public key. TLS uses the so-called “certificate list” to communicate PKI trust models, i.e. the certificate hierarchy must be a chain. The senders certificate is always first in the list, and each following certificate must directly certify the one preceding it. The certificate lists are always static: it is not possible to offer different lists for different clients.

One possible solution to the problem would be to defined IMS as one big trust domain. For example, IMS trust domain could be “ims.com”, and consequently all P-CSCFs, both in visited and home networks, should possess a certificate with this one name. Also, S-CSCF should use an operator specific identifier of IMS trust domain in the realm parameter, e.g. “operator1.ims.com” or “operator1@ims.com”. IMS specifications already include similar name space that could be re-used. The name space is specified in 23.003, section 13 for the case when USIM is used to access IMS. All home networks domain names and private/public user identities that are derived from the IMSI begins with a static string “ims.”, and end with a string “3gppnetwork.com”.

3.2 Certificate based mutual authentication

In certificate based mutual authentication, both UE and P-CSCF would have TLS certificates. Theoretically speaking, there are two ways to apply certificates for mutual authentication:

- If UE has only TLS client certificate, the deployment model is similar to what was described in section 3.1. More specifically, the TLS session should be left open after successful authentication.
- If UE has also TLS server certificate, the TLS session could be turned off after registration because also P-CSCF would be able to initiate TLS handshake (taking the TLS client role).

The use of mutual authentication between UE and P-CSCF does not remove the need for end-to-end authentication between UE and S-CSCF. Consequently, this deployment model includes all the same naming issues than what was described in section 3.1 (assuming that UE needs to avoid man-in-the-middle attacks related to registration procedure).

3.3 Shared key based mutual authentication

The use of shared-key TLS in IMS does not have the naming problems described in section 3.1. However, shared-key TLS should only be seen as an optimization, and consequently at least one certificate based TLS solution should also be supported.

4. References

Rescorla & Modadugu (2004) Datagram Transport Layer Security, IETF, work in progress, draft-rescorla-dtls-00.txt.

RFC 3261 SIP: Session Initiation Protocol, IETF, June 2002.

23.003, Numbering, addressing and identification, 3GPP, Technical Specification, V6.3.0, Release 6.

CR-Form-v7

CHANGE REQUEST

⌘ 33.203 CR 074 ⌘rev - ⌘ Current version: 6.4.0 ⌘

*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 [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	Forwards compatibility to TLS based access security
Source:	⌘	Ericsson
Work item code:	⌘	IMS-ASEC
Date:	⌘	5 October 2004
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:	⌘	Current IMS specification is not forward compatible to one potential deployment mode of TLS based access security.
Summary of change:	⌘	Adds one potential solution.
Consequences if not approved:	⌘	One potential TLS deployment mode cannot be used when UE is roaming in visited network.

Clauses affected:	⌘	8.1			
Other specs affected:	⌘	Y: Other core specifications N: Test specifications N: O&M Specifications	⌘	23.003	
Other comments:	⌘				

***** Begin of Change ****

8.1 Requirements on the ISIM application

This clause identifies requirements on the ISIM application to support IMS access security. It does not identify any data or functions that may be required on the ISIM application for non-security purposes.

The ISIM shall include:

- The IMPI;
- At least one IMPU;
- Home Network Domain Name;
- Support for sequence number checking in the context of the IMS Domain;
- The same framework for algorithms as specified for the USIM applies for the ISIM;
- An authentication Key.

Domain and realm names used in IMPI, and Home Network Domain Name shall contain IMS Trust Domain Name.

NOTE: The exact content and format of IMS Trust Domain Name is out of the scope of this specification. It could be, for example, “ims.com” or “3gppnetwork.com”.

NOTE: This requirement guarantees that TLS can be used for IMS access security between UE and P-CSCF in the future.

The ISIM shall deliver the CK to the UE although it is not required that SIP signalling is confidentiality protected.

At UE power off the existing SAs in the MT shall be deleted. The session keys and related information in the SA shall never be stored on the ISIM.

***** End of Change ****

3GPP TSG SA WG3 Security **S3-040762**

5 - 8 October 2004

St Paul's Bay, Malta, October 5-8, 2004

Title:	LS on Revisiting forwards compatibility towards TLS based access security
Release:	Rel-6
Source:	SA3
To:	CN1, CN4, SA2
Cc:	-

Contact Person:

Name:	Bengt Sahlin
Tel. Number:	+358 40 7784580
E-mail Address:	bengt.sahlin@ericsson.com

Attachments: S3-040xxx (Updated discussion paper on the problem statement)
S3-040xxy (Proposed CR)

---

1. Overall Description:

SA3 has continued discussions on potential future backwards compatibility problem related to the way IMPI, IMPU and Home Network Domain Name are specified in ISIM related specifications. SA3 has re-evaluated its earlier decision on introducing naming restrictions, and decided to loose the proposed requirement. It is still believed that IMS access security architecture should be based on naming scheme in which the domain and realm names are defined in that way that IMS is seen as one big trust domain. Otherwise, one deployment mode of using TLS for IMS access security is not possible in the future (see more details in the attached documents). However, it is not necessary that these naming rules are visible to the end-user, and consequently there will be no new requirements related to IMPUs. IMPI and Home Network Domain Name are still affected.

2. Actions:

To CN1 and CN4

ACTION: SA3 kindly asks CN1 and CN4 to take note of the above decision, and update related IMS specifications accordingly.

To SA2

ACTION: SA3 kindly asks SA2 to take note of the above decision.

3. Date of Next TSG-SA3 Meetings:

SA3#36	23 - 26 November 2004	Shenzhen, China

3GPP TSG SA WG3 Security#35 **S3-040868**
5-8 October, 2004
St Paulís Bay. Malta

Agenda Item: **6.1.2**

Source: **Vodafone**

Title: **New version of TR 33.878**

Document for: **Information**

A new version of the draft TR on early IMS security has been produced. This version incorporates changes agreed during SA3#33. A revision-marked and a clean version are attached.

The following documents have been used as the basis for the changes: S3-040733, S3-040738, S3-040739, S3-040779, S3-040820 and S3-040846. The deviations from the proposed changes in the above listed documents are summarized below:

1. Global changes
    a. Interim (security) solution → early IMS (security) solution
    b. Terminal/mobile → UE
    c. Use terms ìearly IMSî and ìfully compliantî consistently
    d. Various editorial changes
2. Added TR number.
3. Updated version, date, document history and table of contents.
4. Some modifications to PS domain access requirement in clause 5 based on decision to delete editorís note.
5. Promoted editorís note to NOTE in clause 7.2.1 as per S3-040738 and included new text about RADIUS and DIAMETER support as agreed.
6. Added a new editorís note in clause 7.2.4 as agreed to indicate that an alternative approach based on an explicit indication from the UE has been considered.
7. Fifth paragraph after editorís note in clause 7.2.4 integrates the proposal in S3-040733 with some modifications to the proposed text.
8. Introductory text added to clause 7.2.5.3 to describe message sequence referred to in S3-040779.
9. In Annex A the changes from S3-040739, S3-040820 and S3-040846 are merged with the following modifications:
    a. A new sentence is added to the first paragraph: ìThis alternative is not adopted for use in early IMS systems.î
    b. The sentence before the list of advantages and disadvantages is replaced as follows: ìThe HTTP Digest method has the following advantages and disadvantagesî.
    c. In the second advantage, the statement that the solution in clause 5 only supports GPRS access is deleted and a new sentence is added as agreed: ìNote that this is not considered an advantage in the context of early IMS systems since it is specified in clause 5 that it is only a requirement to support secure access over the 3GPP PS domain (including GSM/GPRS and UMTS access).î

3GPP TR 33.878 V0.0.3 (2004-10)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects of Early IMS (Release 6)

Keywords

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword....4
Introduction....4
1 Scope....5
2 References....5
3 Definitions, symbols and abbreviations....5
3.1 Definitions....5
3.2 Symbols....6
3.3 Abbreviations....6
4 Background....6
5 Requirements....6
6 Threat scenarios....7
6.1 Impersonation on IMS level using the identity of an innocent user....7
6.2 IP spoofing....7
6.3 Combined threat scenario....8
7 Specification....8
7.1 Overview....8
7.2 Detailed specification....9
7.2.1 Update of UEís IP address in HSS depending on PDP context state....9
7.2.2 Protection against IP address spoofing in GGSN....9
7.2.3 Source IP address checking in the P-CSCF and S-CSCF....9
7.2.3.1 P-CSCF mechanisms....9
7.2.3.2 S-CSCF mechanisms....10
7.2.4 Interworking cases....10
7.2.5 Message flows....11
7.2.5.1 Successful registration....11
7.2.5.2 Unsuccessful registration....12
7.2.5.3 Successful registration for a selected interworking case....13
Annex A: Comparison with an alternative approach ñ HTTP Digest....14
Annex B: Change history....16

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

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 Ö

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 ".

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 ... and the following] apply.

Definition format

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

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

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

Symbol format

<symbol> <Explanation>

3.3 Abbreviations

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

Abbreviation format

<ACRONYM> <Explanation>

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 ì earlyî 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.

5 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 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 early IMS security solution should not be used as a long-term replacement for full 3GPP IMS security. It is important that the early IMS security solution allows a smooth and cost-effective migration path to the full 3GPP solution.

Co-existence with 3GPP solution: It is clear that UEs supporting the early IMS security solution will need to be supported even after 3GPP compliant UEs are deployed. The early IMS security 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 early IMS 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 early IMS security solution when both the UE and the network support the full 3GPP solution.

No restrictions on the type of charging model: Compared with full 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 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 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 ëzero rateí the IP connectivity.

The major problem is however that without this binding multiple users within a group ìof friendsî could sequentially (or possibly simultaneously) share Bís 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 todayís market place.

6.2 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.

6.3 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 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

7.1 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 userís authenticated PDP context, provides the userís 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 userís 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 subscriberís 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 ìsource IP Spoofingî. 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 elseís 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 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.

7.2 Detailed specification

7.2.1 Update of UEís 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 UEís 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 subscriberís 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.

7.2.2 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 mechanisms in the following sub-clauses shall be supported 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 ìsent-byî parameter of the topìViaî 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 ìreceivedî parameter exists in the top ìviaî header field. If a ìreceivedî parameter exists, S-CSCF shall compare the IP address recorded in the ìreceivedî parameter against the UEís IP address stored during registration. If no ìreceivedî parameter exists in the top ìviaî header field, then S-CSCF shall compare IP address recorded in the ìsent-byî 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 ìviaî 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.

7.2.4 Interworking cases

It is expected that both fully 3GPP compliant UEs implementing the security mechanisms in TS 33.203 [2] (denoted ìfully compliantî in the following) and UEs implementing the early IMS security security solution specified in the present document (denoted ìearly IMSî in the following) will access the same IMS. In addition, IMS networks will support only fully compliant UEs, early IMS UEs, or both. Both UEs and IMS networks must therefore be able to properly handle the different possible interworking cases.

Editorís 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 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 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 UEs). The IMS private identity shall therefore be derived from the subscriberís 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 ìIP-basedî authentication scheme in the Cx-MAR request. The Cx interface shall support the error case that the S-CSCF selects the ìDigest-AKAv1-MD5î 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 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 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 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 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 Registration procedure. The early IMS P-CSCF shall answer with a 420 ìBad Extensionî 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 security headers. The network shall respond with a 200 OK message according to the registration message flow as specified in clause 7.2.5.1.

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

5. UE supports early IMS only, IMS network supports fully compliant 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 ìAuthentication Failedî 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 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 ìBad Extensionî 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 security according to TS 33.203 is not supported.

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

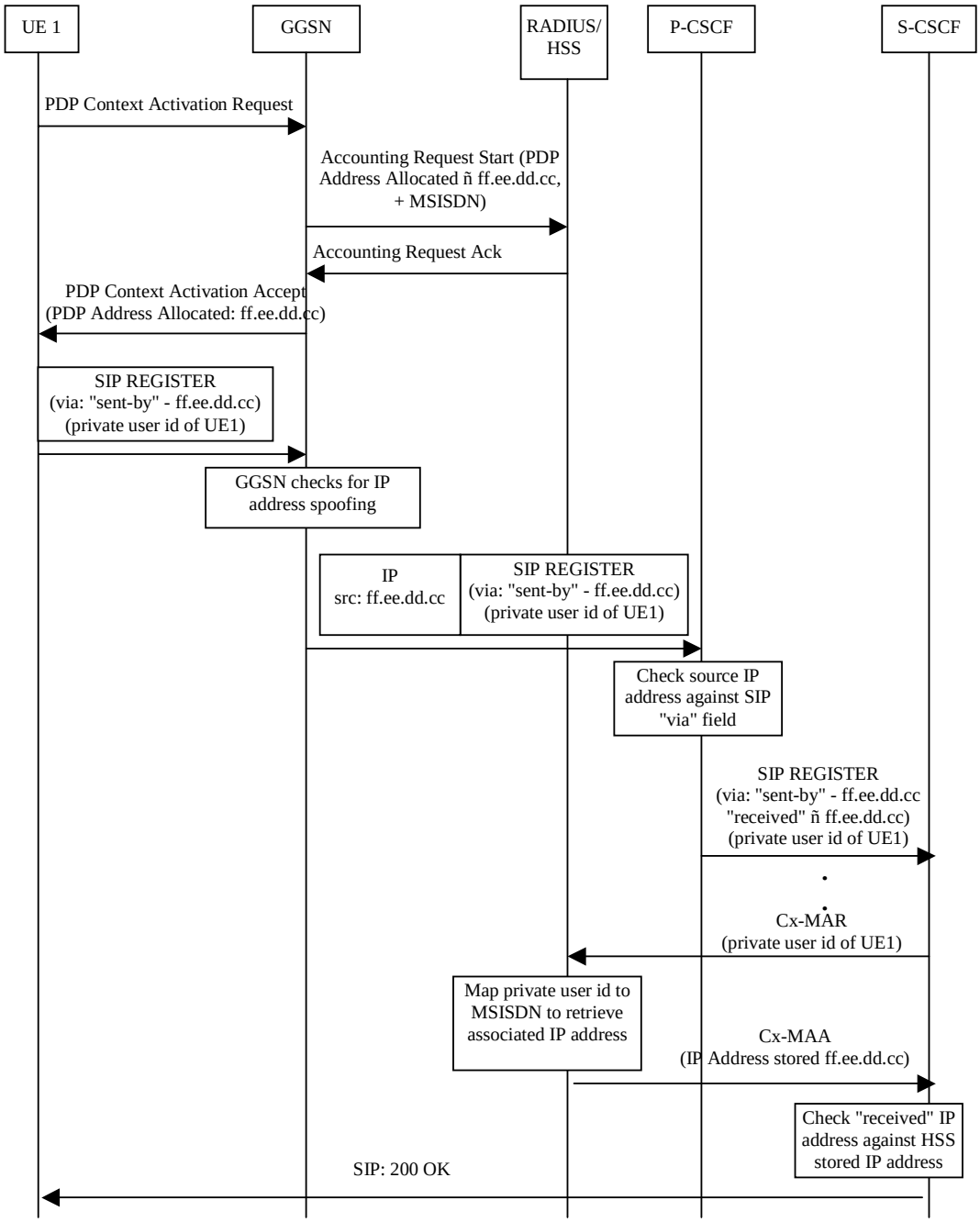


Figure 1: Message sequence for early IMS security showing a successful registration

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 ìreceivedî parameter is only present between P-CSCF to S-CSCF under the conditions given in clause 7.2.3.1.

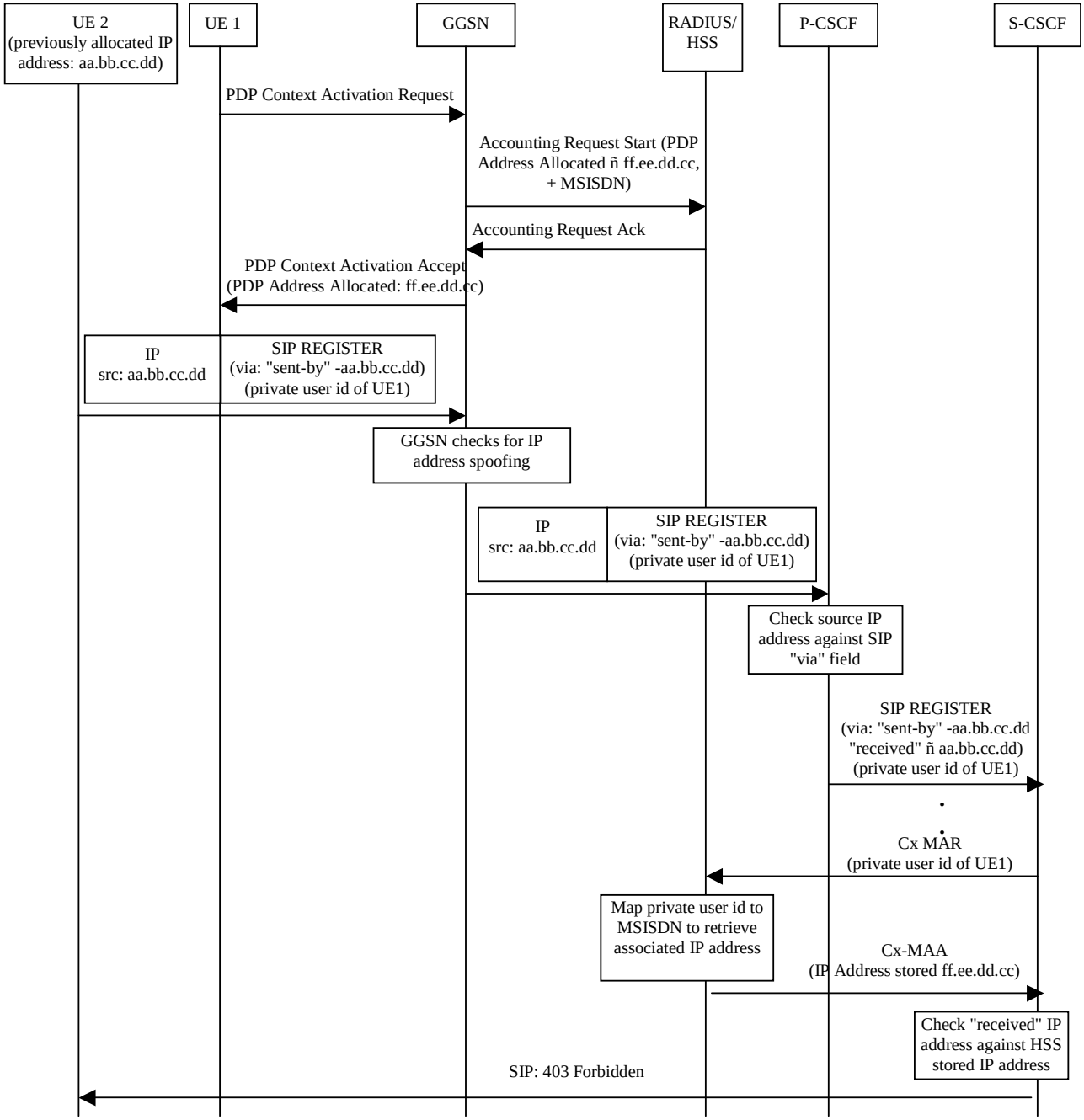


Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

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

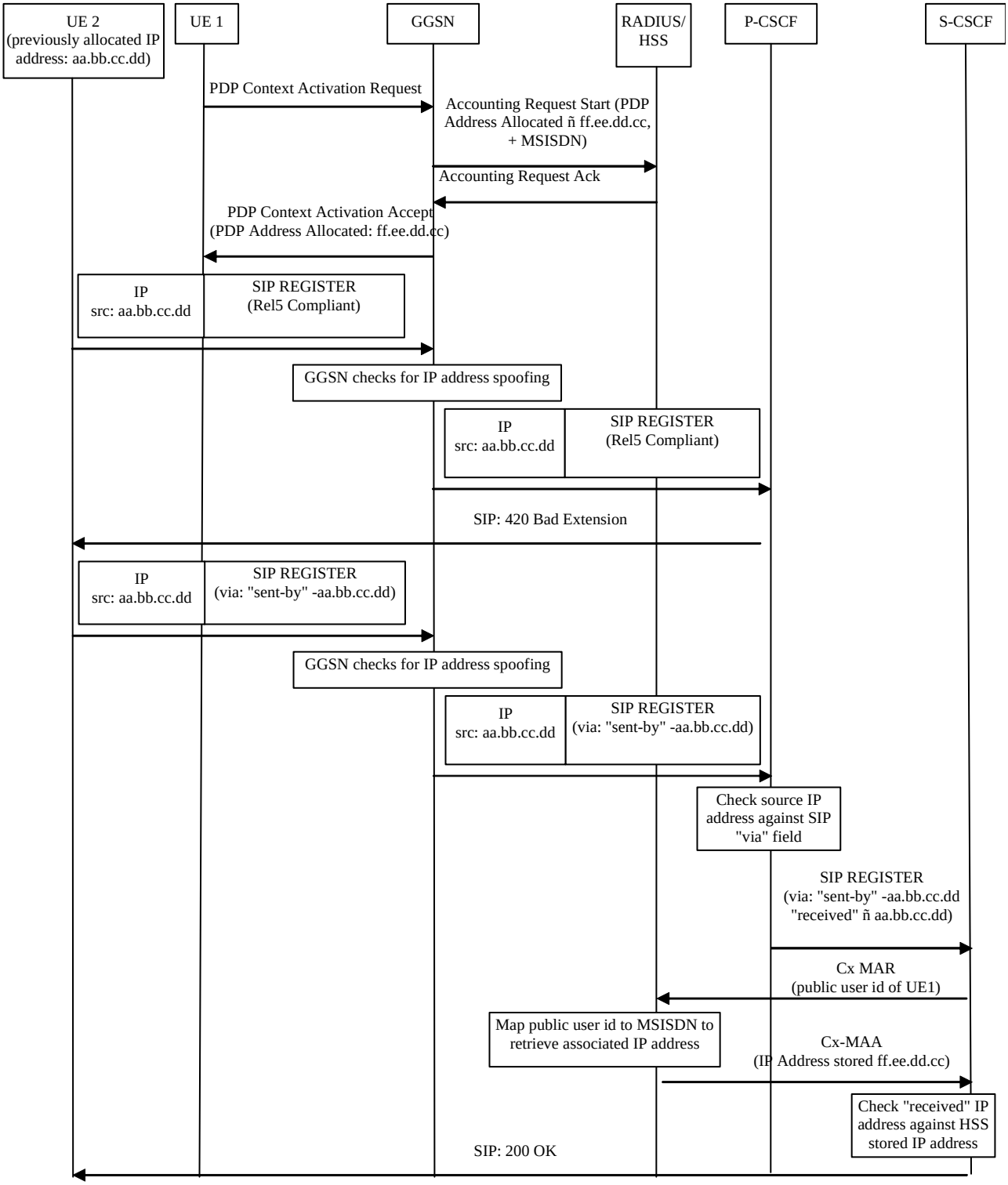


Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant and early IMS access security and network supports early IMS security only

Annex A:
Comparison with an alternative approach ñ 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).
- 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 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 operatorís revenue. The solution specified in clause 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 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 userís 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

3GPP TR 33.~~cde~~ 878 V0.0.~~2~~ 3 (2004-~~07~~10)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects of Early IMS (Release 6)

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Keywords

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword....5
Introduction....5
1 Scope....6
2 References....6
3 Definitions, symbols and abbreviations....6
3.1 Definitions....6
3.2 Symbols....7
3.3 Abbreviations....7
4 Background....7
5 Requirements....7
6 Threat scenarios....8
6.1 Impersonation on IMS level using the identity of an innocent user....8
6.2 IP spoofing....8
6.3 Combined threat scenario....9
7 Specification....9
7.1 Overview....9
7.2 Detailed specification....10
7.2.1 Update of UEís IP address in HSS depending on PDP context state....10
7.2.2 Protection against IP address spoofing in GGSN....11
7.2.3 Source IP address checking in the P-CSCF and S-CSCF....11
7.2.3.1 P-CSCF mechanisms....11
7.2.3.2 S-CSCF mechanisms....11
7.2.4 Interworking cases....11
7.2.5 Message flows....14
7.2.5.1 Successful registration....14
7.2.5.2 Unsuccessful registration....15
7.2.5.3 Successful registration for a selected interworking case....17
Annex A: Comparison with an alternative approach ñ HTTP Digest....18
Annex B: Change history....20
~~Foreword....4~~
~~Introduction....4~~
~~1 Scope....5~~
~~2 References....5~~
~~3 Definitions, symbols and abbreviations....5~~
~~3.1 Definitions....5~~
~~3.2 Symbols....6~~
~~3.3 Abbreviations....6~~
~~4 Background and motivation....6~~
~~5 Requirements on interim solution....6~~
~~6 Threat scenarios....7~~
~~6.1 Impersonation on IMS level using the user identity of an innocent user....7~~
~~6.2 IP spoofing....7~~
~~6.3 Combined threat scenario....8~~
~~7 Specification of interim IMS security solution....8~~
~~7.1 Overview....8~~

7.2 Detailed specification 9
7.2.1 Update of mobileís IP address in HSS depending on PDP context state 9
7.2.2 Protection against IP address spoofing in GGSN 10
7.2.3 Source IP address checking in the P-CSCF and S-CSCF 10
7.2.3.1 P-CSCF mechanisms 10
7.2.3.2 S-CSCF mechanisms 10
7.2.4 Identification of terminals supporting the interim solution 10
7.2.5 Message flows 11

Annex A: Comparison with alternative approaches 16

Annex B: Change history 18

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

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 Ö

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 ".

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 ... and the following] apply.

Definition format

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

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

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

Symbol format

<symbol> <Explanation>

3.3 Abbreviations

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

Abbreviation format

<ACRONYM> <Explanation>

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 ìearlyî 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 ~~terminal~~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 ~~terminal~~UE platforms.

Although full support of TS 33.203 security features is preferred from a security perspective, it ~~must~~ is~~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 ~~terminal~~UEs. The mechanisms should be quick to implement so that the window of opportunity for the ~~interim~~early IMS security solution is not missed.

Adequate level of security: Although it is recognised that the ~~interim~~early IMS security 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~~early IMS security solution should not be used as a long-term replacement for full 3GPP IMS security. It is important that the ~~interim~~early IMS security solution allows a smooth and cost-effective migration path to the full 3GPP solution.

Co-existence with 3GPP solution: It is clear that ~~terminal~~UEs supporting the ~~interim~~early IMS security solution will need to be supported even after 3GPP compliant ~~terminal~~UEs are deployed. The ~~interim~~early IMS security 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~~early IMS 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~~early IMS security solution when both the ~~terminal~~UE 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~~early IMS security solution should not impose any restrictions on the type of charging model that can be adopted.

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

Support access over 3GPP PS domain: ~~Currently the main~~ It is a 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.~~

~~Editorís 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, $IP_{~~gprs-a~~A}$
- Attacker A registers in the IMS using his IMS identity, $ID_{~~ims-a~~A}$
- Attacker A sends SIP invite using his own source IP address ($IP_{~~gprs-a~~A}$) but with the IMS identity of B (ID_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 ëzero rateí the IP connectivity.

The major problem is however that without this binding multiple users within a group ì of friendsî could sequentially (or possibly simultaneously) share Bís 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 todayís market place.

6.2 IP spoofing

The scenario proceeds as follows:

- User B attaches to GPRS, GGSN allocates IP address, IP_B~~IPgprs-b~~
- User B registers in the IMS using his IMS identity, ID_B~~IDims-b~~

- Attacker A sends SIP messages using his own IMS identity (ID_A ~~IDims a~~) but with the source IP address of B (IP_B ~~IPgprs b~~)

If the binding between the IP address that the GGSN allocated the ~~mobile~~ 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.

6.3 Combined threat scenario

The scenario proceeds as follows:

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

If the bindings mentioned in the scenarios in ~~section~~ clause 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~~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 ~~SIM based GPRS~~ security context.

The GGSN, terminating each userís authenticated PDP context, provides the userís 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 userís 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 subscriberís IMPI in the HSS.

The mechanism assumes that the GGSN does not allow a ~~mobile~~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 ìsource IP Spoofingî. 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~~UE (the assumption here, as well as for ~~3GPP compliant IMS systems~~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 elseís 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~~clause 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.

~~Editorís 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.

~~Editorís 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~~w~~hile 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.

7.2 Detailed specification

7.2.1 Update of ~~mobile~~UEís 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 UEís 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 subscriberís 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.

~~Editorís 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-clauses 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 ìsent-byî parameter of the top ìViaî 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 ìreceivedî parameter exists in the top ìviaî header field. If a ìreceivedî parameter exists, S-CSCF shall compare the IP address recorded in the ìreceivedî parameter against the UEís IP address stored during registration. If no ìreceivedî parameter exists in the top ìviaî header field, then S-CSCF shall compare IP address recorded in the ìsent-byî 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 ìviaî 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.

~~Editorís 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~~Interworking cases

~~At some stage, i~~It is expected that both fully 3GPP compliant ~~terminal~~UEs implementing the security mechanisms in TS 33.203 [2] (denoted ìfully compliantî in the following) and ~~terminal~~UEs implementing the early IMS ~~interim~~ security security solution specified in the present document (denoted ìearly IMSî in the following) will access the same IMS. In addition, IMS networks will support only fully compliant UEs, early IMS UEs, or both. Both UEs and IMS networks

must therefore be able to properly handle the different possible interworking cases.~~Therefore, some indication shall be given that a terminal supports the interim solution rather than the full 3GPP solution.~~

Editorís note: ~~The exact format, and means to carry this information, is for further study.~~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 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 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 UEs). The IMS private identity shall therefore be derived from the subscriberís 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 ì IP-basedî authentication scheme in the Cx-MAR request. The Cx interface shall support the error case that the S-CSCF selects the ì Digest-AKAv1-MD5î 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 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 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 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 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 Registration procedure. The early IMS P-CSCF shall answer with a 420 ì Bad Extensionî 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 security headers. The network shall respond with a 200 OK message according to the registration message flow as specified in clause 7.2.5.1.

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

5. UE supports early IMS only, IMS network supports fully compliant 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 ì Authentication Failedî 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.

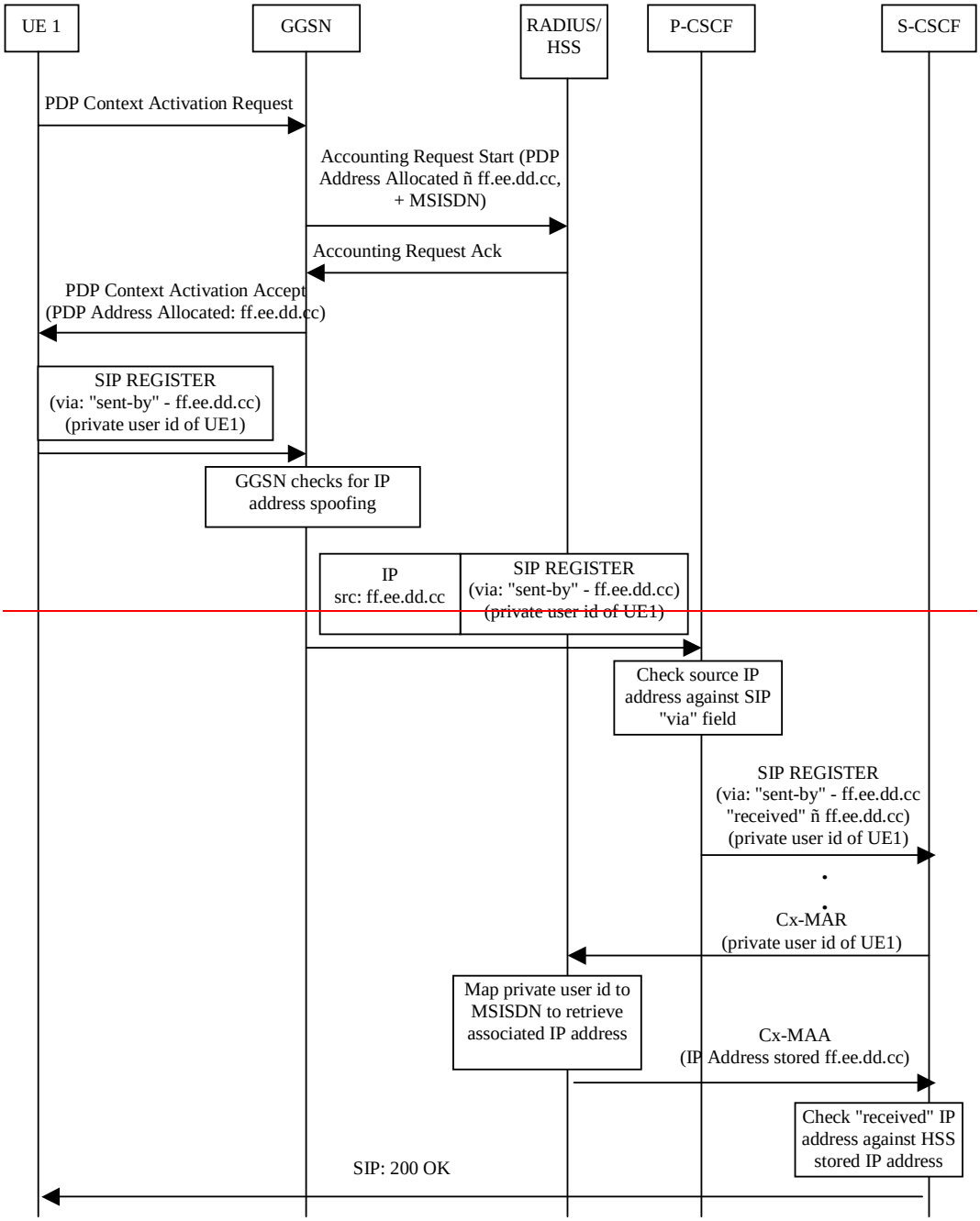
6. UE supports fully compliant access security only, IMS network supports early IMS only

The UE shall start with the fully compliant IMS registration procedure. The early IMS P-CSCF shall answer with a 420 ì Bad Extensionî 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 security according to TS 33.203 is not supported.

7.2.5 Message flows

7.2.5.1 Successful registration

~~Editorís 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~~early IMS security solution.

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

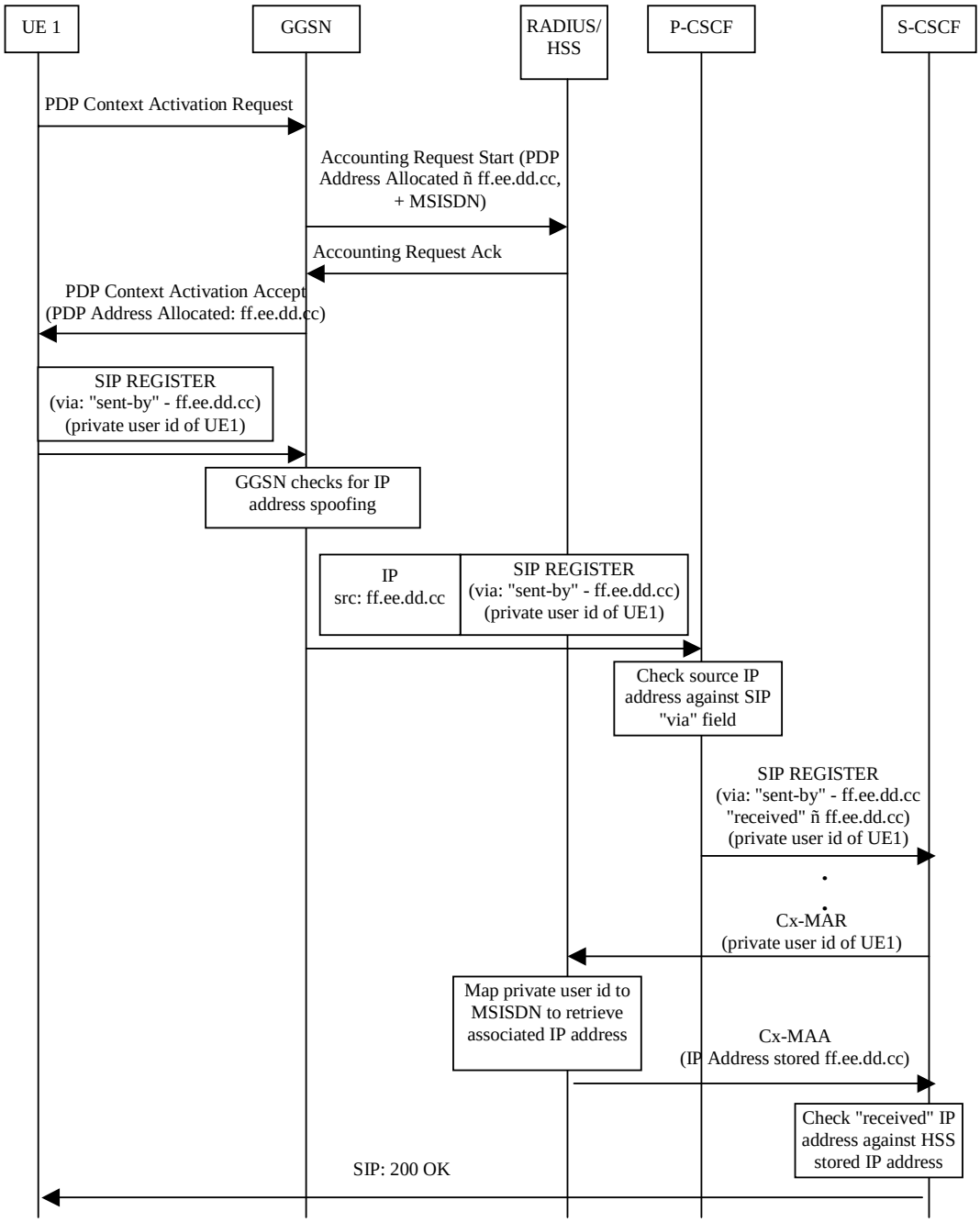
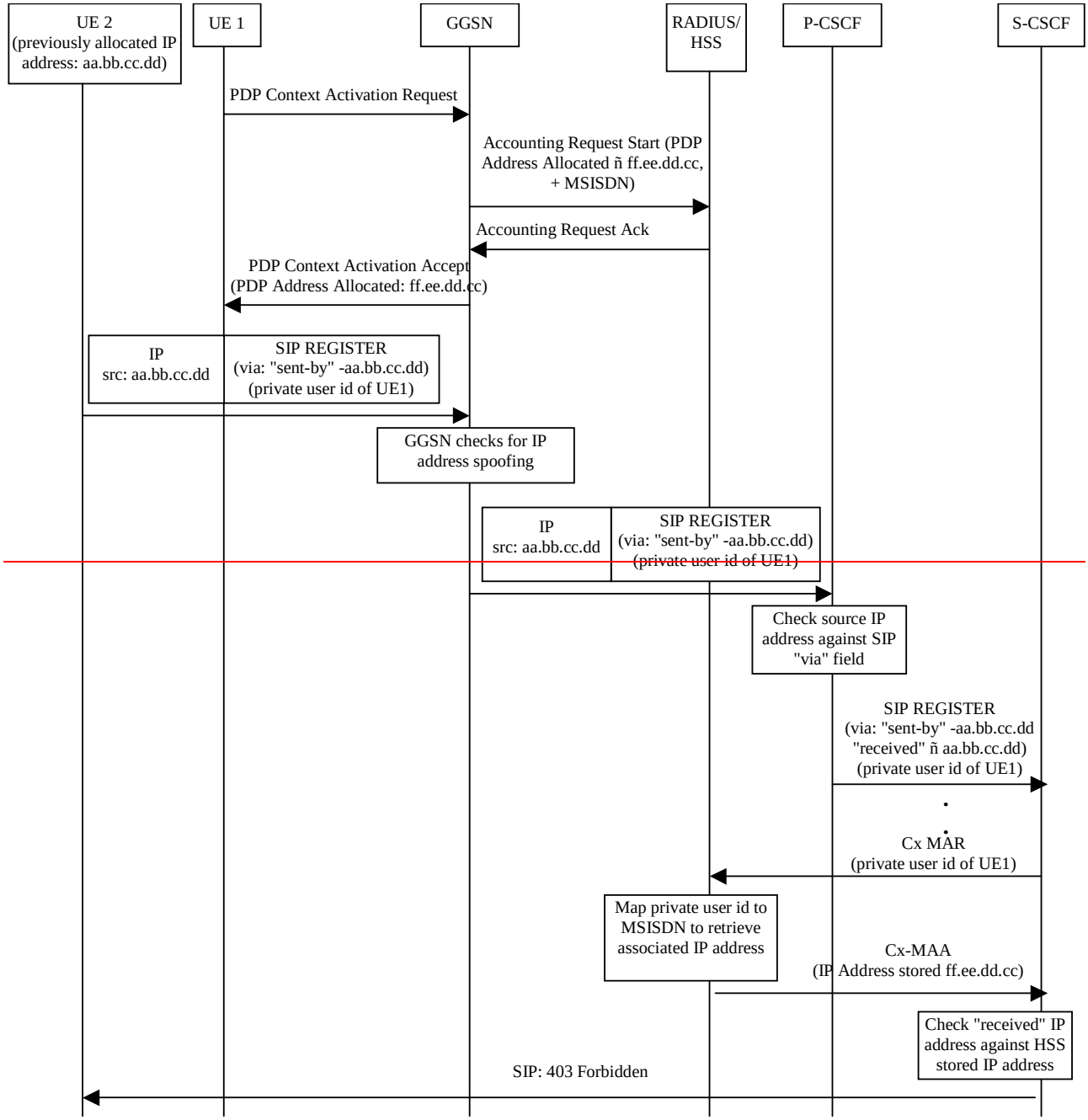


Figure 1: Message ~~S~~sequence for ~~Interim~~early IMS sSecurity ~~Solution (~~showing a successful registration~~)~~

7.2.5.2 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 ìreceivedî parameter is only present between P-CSCF to S-CSCF under the conditions given in ~~section~~clause 7.2.3.1.

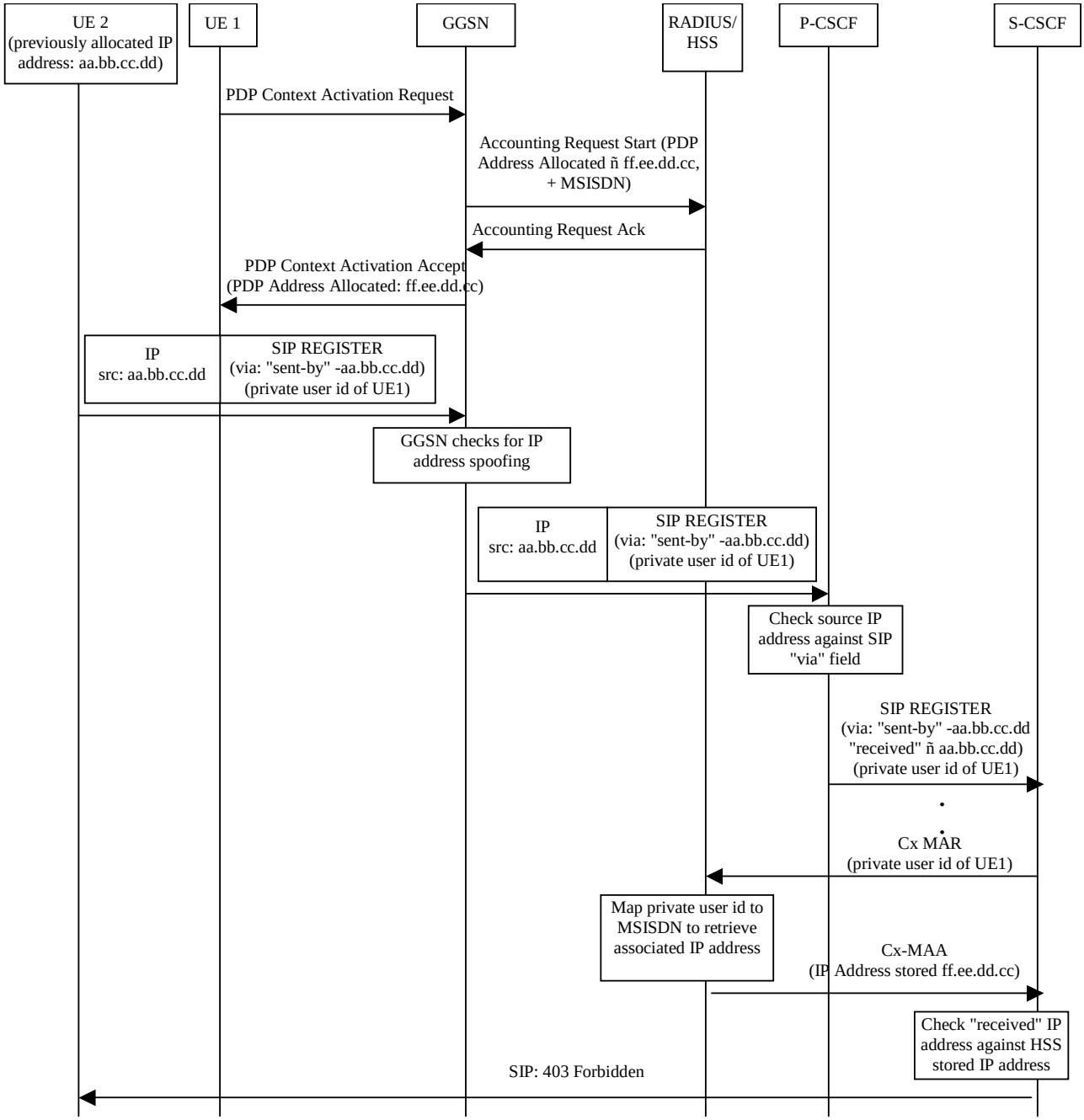


Figure 2: Message ~~S~~sequence for ~~Interim~~early IMS ~~S~~security ~~Solution~~ showing an unsuccessful identity theft

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

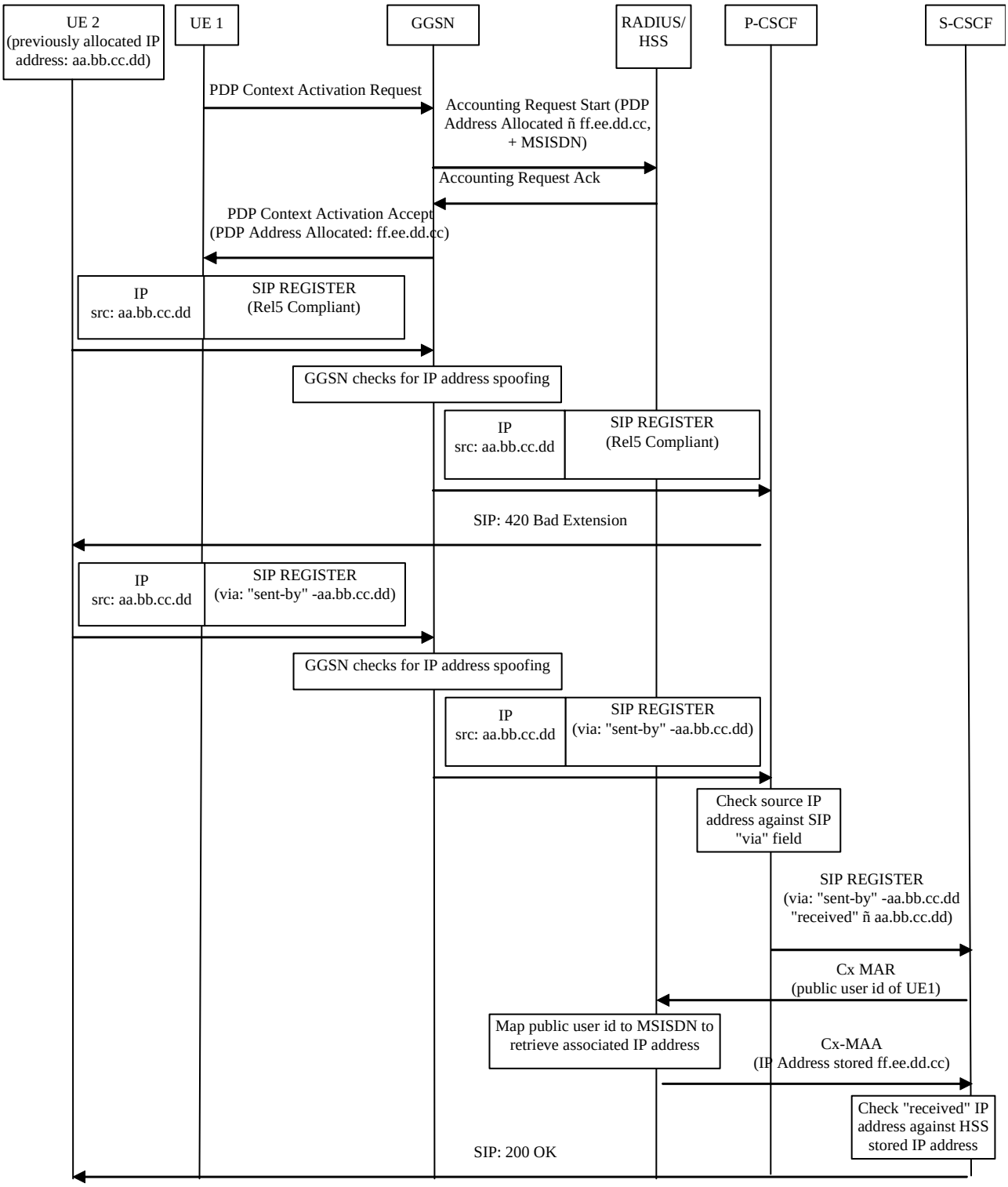


Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant and early IMS access security and network supports early IMS security only

Annex A:
Comparison with an alternative approach~~es~~ ñ HTTP Digest

An alternative approach would have been ~~is~~ 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, t~~T~~his method would have required a subscriber-specific password to be provisioned on the IMS ~~terminal~~UE. This alternative is not adopted for use in early IMS systems.

The HTTP Digest method has~~Compared with the approach specified in section 7, password based authentication 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).
- 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 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 ~~It~~ impose~~s~~ 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 ~~terminal~~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 ~~(and~~ not impact on operatorís revenue~~)~~. The solution specified in ~~section~~clause 7 is flexible in allowing a range of different charging models including bundled or partly subscription based tariffs.
- ~~It~~ 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, ~~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~~clause 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 userís MSISDN is provided by the GGSN to the WAP gateway. Security does not rely on the ~~terminal~~UE securely storing any long-term secret information (e.g. passwords).
- HTTP Digest p~~P~~rovisioning is more complex since subscriber-specific information (i.e. passwords) must be installed or bootstrapped into each ~~mobile~~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