3GPP TSG SA WG3 Security#36 **S3-041091**
Shenzhen, China, 23-26 November 2004.

Agenda Item: **6.1.2**

Source: **Vodafone**

Title: **New version of TR 33.878**

Document for: **Approval**

A new version of TR 33.878 “Security aspects of early IMS” has been produced. A revision-marked and a clean version are attached.

The proposed changes indicated in the following documents were agreed at SA3#36 and have been incorporated into the attached version of TR:

S3-040921, S3-040974, S3-040998, S3-040999, S3-041000, S3-041006, S3-041007, S3-041031, S3-040939, S3-041052, S3-041062, S3-041063, S3-041069, S3-041074.

In addition, the following changes have been incorporated as agreed:

1. The change in S3-040974 was modified so that all instances of “top via header” as changed as indicated.
2. The change in S3-041007 was modified to indicate that the condition is best fulfilled if all IMS network entities reside in the home network. The change in S3-041007 was also modified to include a note to indicate that different APNs may be used to indicate the IMS security variant currently used by the UE, in the case that separate P-CSCFs supporting different IMS security variants are supported in the network (based on rule 1 in S3-040973).
3. The change in S3-041031 was modified so that the word “assumes” is replaced with “adds a restriction”.
4. IMSI is added to the message from the GGSN to the HSS in the figure in section 6.2.7.3.

Some editorial changes were also made:

1. Updated version, date, document history and table of contents.
2. Various editorial changes and improvements throughout the TR.

3GPP TR 33.878 V0.0.4 (2004-11)

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

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

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 subclause 5.1 of 3GPP 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 3GPP 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.

1 Scope

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".

[8] 3GPP TS 23.003: "Numbering, addressing and identification".

[9] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

[10] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interface; signalling flows and message contents".

[11] draft-ietf-aaa-diameter-nasreq-17.txt (July 2004), "Diameter Network Access Server Application", work in progress.

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[12] 3GPP TS 29.229: "Cx Interface based on Diameter – Protocol details".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 21.905[9] and the following apply.

Early IMS: a 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:

Cx	Reference Point between a CSCF and an HSS.
Gi	Reference point between GPRS and an external packet data network

3.3 Abbreviations

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

AAA	Authentication Authorisation Accounting
ABNF	Augmented Backus-Naur Form
APN	Access Point Name
AVP	Attribute-Value Pair
CSCF	Call/Session Control Function
GGSN	Gateway GPRS Support Node
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
ICID	IM CN subsystem Charging Identifier
IM	IP Multimedia
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
RFC	Request For Comments
S-CSCF	Serving-CSCF
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLF	Server Locator Function
UE	User Equipment
URI	Uniform Resource Identifier

4 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 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 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 fully compliant IMS security solution. The security mechanisms developed for early IMS systems should therefore be considered as an interim solution and migration to the fully compliant IMS security solution 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 solution. It is important that the early IMS security solution allows a smooth and cost-effective migration path to the fully compliant IMS security solution.

Co-existence with fully compliant solution: It is clear that UEs supporting the early IMS security solution will need to be supported even after fully compliant IMS UEs are deployed. The early IMS security solution should therefore be able to co-exist with the fully compliant IMS security 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 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 solution.

No restrictions on the type of charging model: Compared with fully compliant 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 solution.

5 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.

5.1 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.

5.2 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.

5.3 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 subclauses 5.1 and 5.2 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.

6 Specification

6.1 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, terminates each user's PDP context and has assurance that the IMSI used within this PDP context is authenticated. The GGSN shall provide the user's IP address, IMSI and MSISDN to a RADIUS server in the HSS over the Gi interface when a PDP context is activated towards the IMS system. The HSS has a binding between the IMSI and/or MSISDN and the IMPI and IMPU(s), and is therefore able to store the currently assigned IP address from the GGSN against the user's IMPI and/or IMPU(s). The precise way of the handling of these identities in the HSS is outside the scope of standardization. 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 IMPU, 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 IMPU 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 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 a PDP context (based on an authenticated 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.

For the purposes of this present document, an APN, which is used for IMS services, is called an IMS APN. An IMS APN may be also used for non-IMS services. The mechanism described in this present document further adds a restriction that there is only one APN for accessing IMS for a PLMN and that all active PDP contexts, for a single UE, associated with that IMS APN use the same IP address at any given time.

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.

6.2 Detailed specification

6.2.1 GGSN-HSS interaction

When receiving an Activate PDP Context Request message, based on operator policy, a GGSN supporting early IMS security shall send a RADIUS "Accounting-Request START" message to a AAA server attached to the HSS. The message shall include the mandatory fields defined in subclause 16.4.3 of 3GPP TS 29.061 [4] and the UE's IP address, MSISDN and IMSI. On receipt of the message, the HSS shall use the IMSI and/or the MSISDN to find the subscriber's IMPI (derived from IMSI) and then store the IP address against a suitable identity, e.g. the IMPI.

NOTE 1: It is assumed here that the RADIUS server attached to the HSS 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.

NOTE 2: 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 accept the activation of the PDP context if the accounting start request is not successfully handled by the HSS (e.g. a positive Create PDP Context Response should not be sent by the GGSN until the "Accounting-Request START" message is received or a negative Create PDP Context Response is sent after some RADIUS response timeout occurs). In particular, it shall not be possible to have an active PDP context associated with the IMS APN if the corresponding IP address is not stored in the HSS.

When the UE establishes its first PDP context for an IMS APN a new IP address is obtained, and the GGSN shall send an "Accounting-Request START" to the HSS with the assigned IP address. If this IP address is different from the IP address already stored in the HSS (i.e. the "old" IP address), the HSS shall start the 3GPP IMS HSS-initiated de-registration procedure, if the UE is IMS registered, using a Cx-RTR/Cx-RTA exchange, and delete the old IP address. The HSS stores the new IP address and confirms the "Accounting-Request START" to the GGSN when either the de-registration procedure is successfully completed or after a suitable time-out. The UE starts the IMS initial registration procedure. The HSS shall abandon the de-registration procedure when a new successful authentication for this user is signalled by the S-CSCF in a Cx-SAR message.

When all the PDP contexts are de-activated at the IMS APN of the GGSN, the GGSN sends an "Accounting-Request STOP" request to the HSS. 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, an HSS-initiated de-registration procedure shall be started, if the UE is registered, using a Cx-RTR/Cx-RTA exchange. In the case they are different, the HSS shall ignore the message.

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. It shall be possible for the GGSN to log the event in its security log against the subscriber information (IMSI/MSISDN), e.g. based on operator configuration.

6.2.3 Impact on IMS registration and authentication procedures

A UE shall not be able to spoof its assigned IP address and successfully receive service from the IMS. The mechanisms in the following subclauses shall be supported to prevent IP address spoofing in the IMS domain. The changes to the IMS registration and authentication procedures are detailed in the following subclauses.

6.2.3.1 Procedures at the UE

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include an Authorization header field and not include a Security-Client header field. The From header, To header, Contact header, Expires header, Request URI, Supported header and a P-Asserted-Id header shall be set according subclause 5.1.1.2 of 3GPP TS 24.229 [7].

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according subclause 5.1.1.2 of 3GPP TS 24.229 [7].

NOTE 1: Early IMS security does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

NOTE 2: The UE shall not use the temporary public user identity used for registration in any subsequent SIP requests.

6.2.3.2 Procedures at the P-CSCF

NOTE: As specified in RFC 3261 [6], when the P-CSCF receives a SIP request from an early IMS UE, the P-CSCF checks the IP address in the "sent-by" parameter of the Via header field provided by the UE. If the "sent-by" parameter contains a domain name, or if it contains an IP address that differs from the packet source IP address, the P-CSCF adds a "received" parameter to that Via header field value. This parameter contains the source IP address from which the packet was received.

6.2.3.2.1 Registration

When the P-CSCF receives a REGISTER request from the UE that does not contain an Authorization header and does not contain a Security-Client header, the P-CSCF shall handle the Path header, the Require header, the P-Charging-Vector header and the P-Visited-Network-ID header as described in subclause 5.2.12 of 3GPP TS 24.229 [7]. Afterwards the P-CSCF shall determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) handle the Service-Route header, the public user identities, the P-Asserted-Identity header, the P-Charging-Function-Address header as described in subclause 5.2.2 of 3GPP TS 24.229 [7] for the reception of a 200 (OK) response; and

2) forward the 200 (OK) response to the UE.

6.2.3.2.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

As the early IMS security solution does not offer IPsec, the P-CSCF shall implement the procedures as described in subclause 5.2.6 of 3GPP TS 24.229 [7] with the following deviations.

For requests initiated by the UE, when the P-CSCF receives a 1xx or 2xx response, the P-CSCF shall not rewrite its own Record Route entry.

For requests terminated by the UE, when the P-CSCF receives a request, prior to forwarding the request, the P-CSCF shall not include a protected server port in the Record-Route header and in the Via header.

6.2.3.3 Procedures at the I-CSCF

NOTE: Topology hiding is not available with early IMS security because topology hiding alters the Via header.

6.2.3.4 Procedures at the S-CSCF

6.2.3.4.1 Registration

Upon receipt of an initial REGISTER request without an Authorization header, the S-CSCF shall:

1) identify the user by the public user identity as received in the To header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) if no IP address is stored for the UE, query the HSS, as described in subclause 6.2.5 with the public user ID as input and store the received IP address of the UE. Prior to contacting the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [10];

NOTE: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

4) check whether a "received" parameter exists in the Via header field provided by the UE. If a "received" parameter exists, S-CSCF shall compare the IP address recorded in the “received” parameter against the UE's IP address stored during registration. If no "received" parameter exists in the Via header field provided by the UE, then S-CSCF shall compare IP address recorded in the "sent-by" parameter against the stored UE IP address. In both cases, if stored IP address and the IP address recorded in the Via header provided by the UE do not match, the S-CSCF shall query the HSS, as described in subclause 6.2.5 with the public user ID as input and store the received IP address of the UE. If the stored IP address and the IP address recorded in the Via header provided by the UE still do not match the S-CSCF shall reject the registration with a 403 (Forbidden) response and skip the following steps.

5) handle the Cx Server Assignment procedure, the ICID, each non-barred registered public user identity, the Path header, the registration duration as described in subclause 5.4.1.2.2 of 3GPP TS 24.229 [7]; and

6) send a 200 (OK) response to the UE as described in subclause 5.4.1.2.2 of 3GPP TS 24.229 [7].

6.2.3.4.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

On the reception of any request other than an initial REGISTER request, the S-CSCF shall check whether a "received" parameter exists in the Via header field provided by the UE. If a "received" parameter exists, S-CSCF shall compare the IP address received in the "received" parameter against the UE's IP address stored during registration. If no "received" parameter exists in the Via header field provided by the UE, then S-CSCF shall compare IP address received in the "sent-by" parameter against the IP address stored during registration. If the stored IP address and the IP address received in the Via header field provided by the UE do not match, the S-CSCF shall reject the request with a 403 (Forbidden) response.

In case the stored IP address and the IP address receive in the Via header field provided by the UE do match, the S-CSCF shall proceed as described in 5.4.3 of 3GPP TS 24.229 [7].

6.2.4 Identities and subscriptions

When early IMS security is supported, the HSS shall include for each subscription an IMPI and IMPU derived from the IMSI of the subscription according to the rules in 3GPP TS 23.003 [8]. If the network supports both early IMS security and fully compliant IMS security, the IMSI-derived IMPI and IMPU shall be stored in addition to other IMPIs and IMPUs that may have been allocated to the subscription.

If a UE attempts a registration using early IMS security, the REGISTER shall include an IMPU that is derived from the IMSI that is used for bearer network access according to the rules in 3GPP TS 23.003 [8]. The UE shall apply this rule even if a UICC containing an ISIM is present in the UE.

In the case that a UE is registering using early IMS security with an IMSI-derived IMPU, implicit registration shall be used as a mandatory function to register the subscriber's public user identity(s) using the rules defined in subclause 5.2.1a.1 of 3GPP TS 23.228 [3]. By applying these rules the IMSI-derived IMPU shall be barred in the HSS for all procedures other than SIP registration.

6.2.5 Impact on Cx Interface

Early IMS Security mechanism affects the use of the protocol defined for the Cx interface. In particular, the User-Authorisation-Request and Multimedia-Auth-Request/Answer messages are impacted.

Because in Early IMS Security the Private User Identity of the subscriber is not made available to the IMS domain in SIP messages, it is necessary to derive a Private User Identity from the Temporary Public User Identity to use as the content of the User-Name AVP in certain Cx messages (most notable UAR and MAR).

6.2.5.1 User registration status query

The UAR command, when implemented to support Early IMS Security follow the description in 6.1.1 of 3GPP TS 29.228 [10], with the following exception;-

- the Private User Identity (User-Name AVP) in the UAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present port number, URI parameters, and headers

6.2.5.2 Authentication procedure

The MAR and MAA commands, when implemented to support Early IMS Security follow the description in 6.3 of 3GPP TS 29.228 [10] of this document, with the following exceptions;-

- the Private User Identity (User-Name AVP) in the MAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present: port number, URI parameters, and headers.
- In the MAR and MAA commands, the Authentication Scheme (Authentication-Scheme AVP described in subclause 7.9.2 of 3GPP TS 29.228 [10]) within the SIP-Auth-Data-Item grouped AVP shall contain "Early-IMS-Security".
- In the MAA command, the SIP-Auth-Data-Item grouped AVP shall contain the user IP address. If the address is IPv4 it shall be included within the Framed-IP-Address AVP as defined in draft-ietf-aaa-diameter-nasreq-

17.txt [11]. If the address is IPv6 it shall be included within the Framed-IPv6-Prefix AVP and, if the Framed-IPv6-Prefix AVP alone is not unique for the user it shall also contain Framed-Interface-Id AVP.

This results in SIP-Auth-Data-Item as depicted in table 6.3.4 of 3GPP TS 29.228 [10], being replaced when Early IMS Security is employed by a structure as shown in Table 2.

Table 2: Authentication Data content for Early IMS Security

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For Early IMS Security it will indicate "Early-IMS-Security"
User IPv4 Address	Framed-IP-Address	C	If the IP Address of the User is an IPv4 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11].
User IPv6 Prefix	Framed-IPv6-Prefix	C	If the IP Address of the User is an IPv6 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11].
Framed Interface Id	Framed-Interface-Id	C	If the IP Address of the User is an IPv6 address and the Framed-IPv6-Address AVP alone is not unique for the user this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11].

The ABNF description of the AVP as given in subclause 6.3.13 of 3GPP TS 29.229 [12] is replaced with that given below.

```
SIP-Auth-Data-Item :: = < AVP Header : TBD >

     [ SIP-Authentication-Scheme ]

     [ Framed-IP-Address ]

     [ Framed-IPv6-Prefix ]

     [ Framed-Interface-Id ]

     * [AVP]
```

- Step 5 of subclause 6.3.1 of 3GPP TS 29.229 [12] shall apply with the following exception:
  - HSS shall return only one SIP-Auth-Data-Item

6.2.6 Interworking cases

For the purposes of the interworking considerations in this subclause, it is assumed that the IMS entities P-CSCF, I-CSCF, S-CSCF and HSS reside in the home network and all support the same variants of IMS, i.e. all support either only early IMS, or only fully compliant IMS, or both.

NOTE: It is compatible with the considerations in this document that the UE uses different APNs to indicate the IMS variant currently used by the UE, in case the P-CSCF functionality is split over several physical entities.

It is expected that both fully 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 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.

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 request 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 request, early IMS UEs only provide the IMS public identity (IMPU), but not the IMS private identity (IMPI) to the network (this is only present in the Authorization header for fully compliant IMS UEs).

During the process of user registration for early IMS, the Cx interface carries only the public user identity in Cx-MAR requests (sent by I-CSCF and S-CSCF HSS). The private user identity within these requests shall contain the IMPU as received by the UE. This avoids changes to the message format on the Cx interface.

If the S-CSCF receives an indication that the UE is early IMS, then it shall be able to select the "Early-IMS-Security" 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) response. 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

   Early IMS security according to this annex shall be used 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. The UE shall use fully compliant IMS security, if the network supports this, otherwise the UE shall use early IMS security.

   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 request.

NOTE: The Proxy-Require header cannot be ignored by the P-CSCF.

   The UE shall, after receiving the error response, send an early IMS registration, i.e., shall send a new REGISTER request without the fully compliant IMS security headers.

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 request, receives indication that the IMS UE is fully compliant and shall continue as specified by TS 33.203 [2].

5. Mobile equipment and IMS network support both, UE contains a SIM

   The UE might start with the fully compliant IMS registration procedure. However, when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that the UE contains a SIM and return an error.

The S-CSCF shall answer with a 401 (Unauthorized) with an Error-info: header containing the text "Early security required". The UE then retries using early IMS security.

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

   The UE sends a REGISTER request to the IMS network that does not contain the security headers required by fully compliant IMS. The fully compliant P-CSCF will detect that the Security-Client header is missing and return a 4xx responses, as described in subclause 5.2.2 of 3GPP TS 24.229 [7].

7. 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 request. After receiving the error response, the UE shall stop the attempt to register with this network, since the fully compliant IMS security according to TS 33.203 [2] is not supported.

6.2.7 Message flows

6.2.7.1 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 subclause 6.2.3.2.

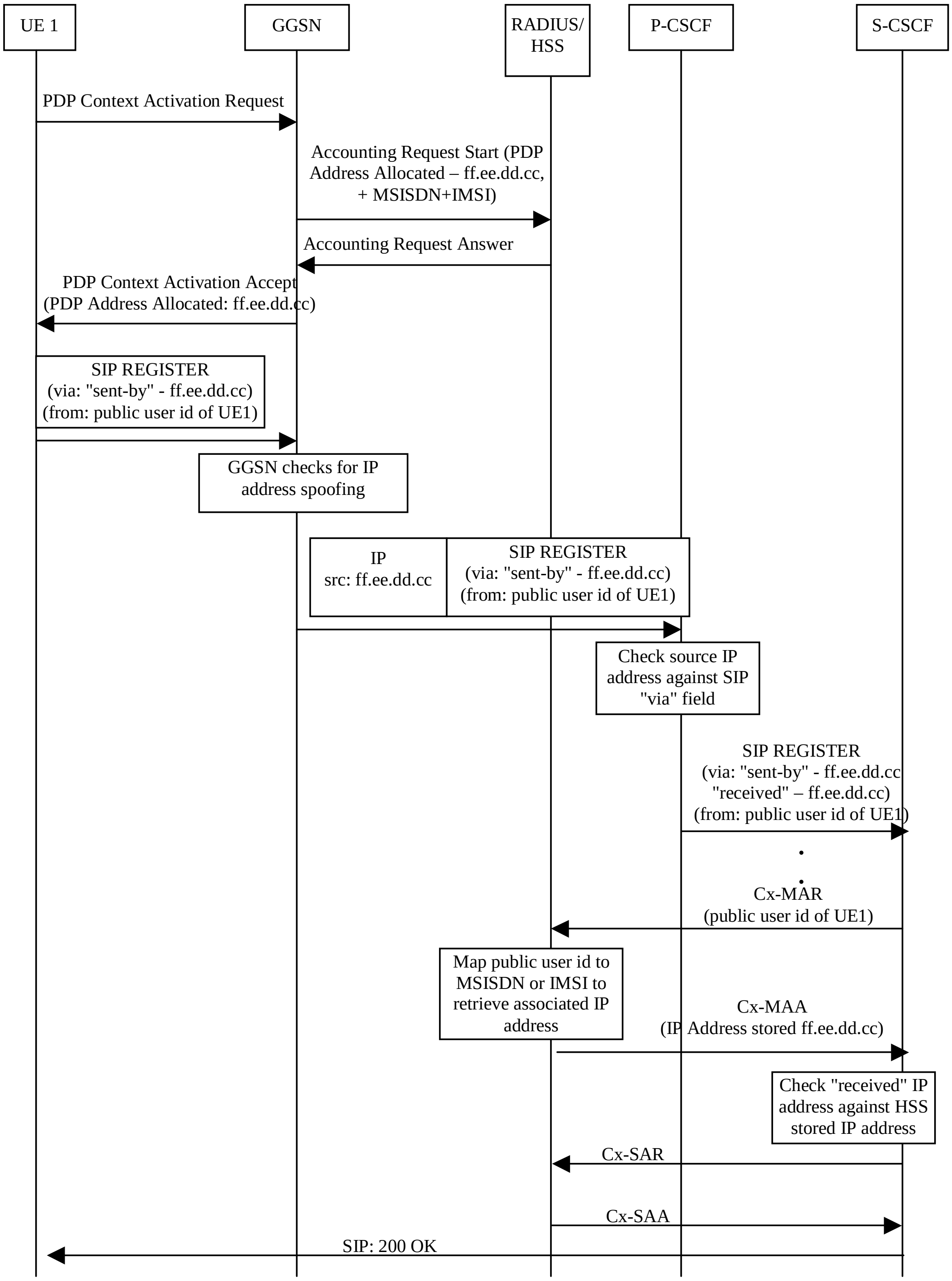


Figure 1: Message sequence for early IMS security showing a successful registration

6.2.7.2 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 subclause 6.2.3.2.

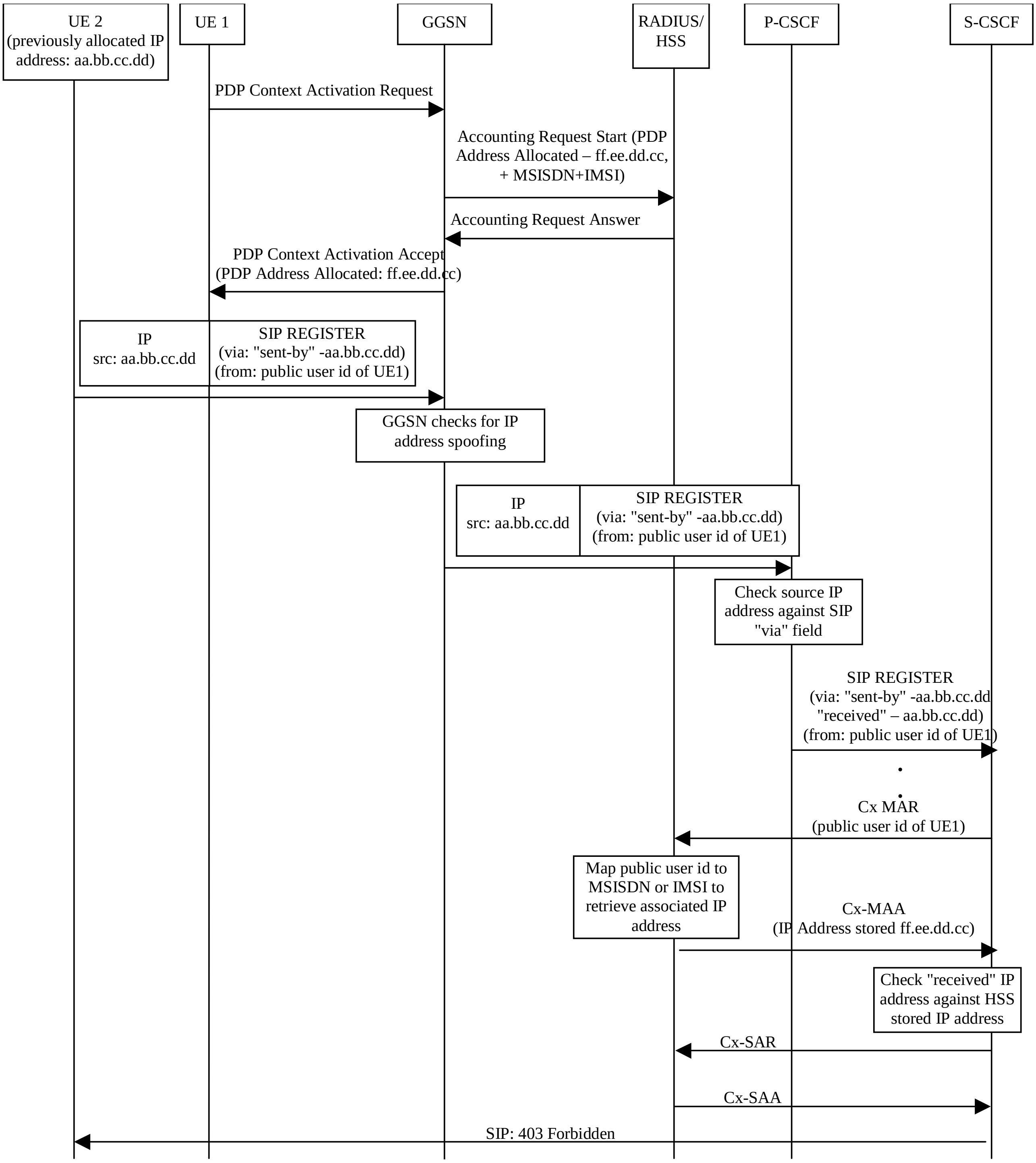


Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

6.2.7.3 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 subclause 6.2.6.

Note, that the "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in subclause 6.2.3.2.

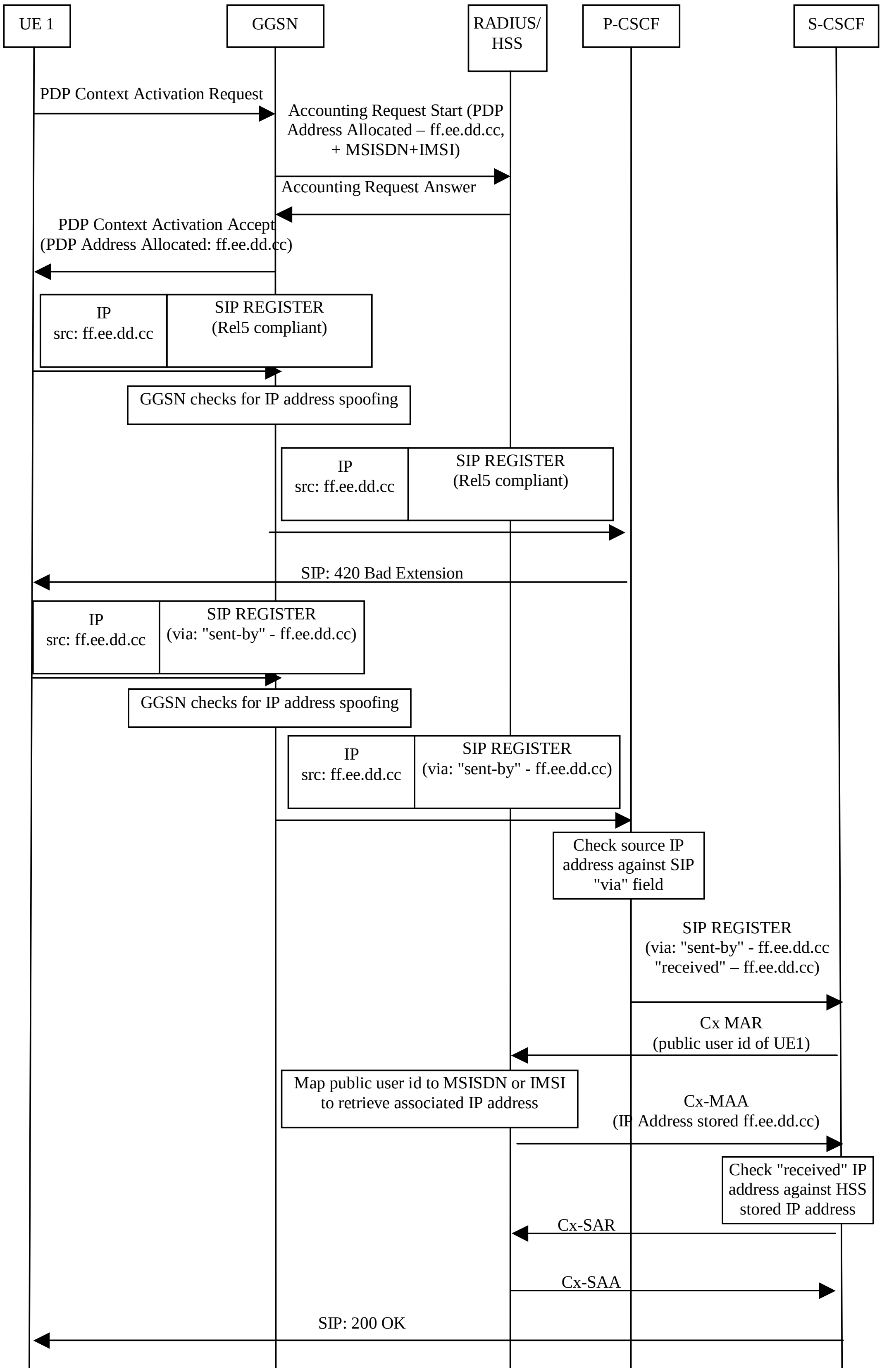


Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant IMS and early IMS access security and network supports early IMS security only

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).
- 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 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, 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
25/11/04					Incorporates changes agreed at SA3#36.	0.0.3	0.0.4

3GPP TR 33.878 V0.0.4~~3~~ (2004-11~~0~~)

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

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

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 subclause 5.1 of 3GPP 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 3GPP 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".

[8] 3GPP TS 23.003: "Numbering, addressing and identification".

[9] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

[10] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx interface; signalling flows and message contents".

[11] draft-ietf-aaa-diameter-nasreq-17.txt (July 2004), "Diameter Network Access Server Application", work in progress.

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[12] 3GPP TS 29.229: "Cx Interface based on Diameter – Protocol details".

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 3GPP TS 21.905[9]... and the following] apply.

Definition format

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

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

Early IMS: a 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

<symbol>	<Explanation>
Cx	Reference Point between a CSCF and an HSS.
Gi	Reference point between GPRS and an external packet data network

3.3 Abbreviations

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

Abbreviation format

<ACRONYM>	<Explanation>
AAA	Authentication Authorisation Accounting
ABNF	Augmented Backus-Naur Form
APN	Access Point Name
AVP	Attribute-Value Pair
CSCF	Call/Session Control Function
GGSN	Gateway GPRS Support Node
HSS	Home Subscriber Server
I-CSCF	Interrogating CSCF
ICID	IM CN subsystem Charging Identifier
IM	IP Multimedia
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
RFC	Request For Comments
S-CSCF	Serving-CSCF
SGSN	Serving GPRS Support Node

SIP	Session Initiation Protocol
SLF	Server Locator Function
UE	User Equipment
URI	Uniform Resource Identifier

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.

45 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 3GPPfully compliant 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 fully compliant 3GPP solution: Clearly, any security mechanisms developed for early IMS systems will provide a lower level of protection compared with that offered by the fully compliantfull set of 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 compliantfull set of 3GPP IMS security features solution 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 3GPPthe fully compliant IMS security solution. It is important that the early IMS security solution allows a smooth and cost-effective migration path to the fully compliant IMS securityfull 3GPP solution.

Co-existence with fully compliant3GPP 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 fully compliant IMS securityfull 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 securityfull 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 fully compliant IMS securityfull 3GPP solution.

No restrictions on the type of charging model: Compared with fully compliant ~~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 fully compliant IMS security~~full 3GPP~~ solution.

5~~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.

5~~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 '~~‘~~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.

5~~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.

5~~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 subclauses ~~6~~5.1~~2~~ and ~~6~~5.2~~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.

6~~7~~ Specification

6~~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~~ terminates each user'~~’~~s ~~authenticated~~ PDP context and has assurance that the IMSI used within this PDP context is authenticated~~,~~. The GGSN shall provide~~s~~ the user'~~’~~s IP address, IMSI and ~~/~~ MSISDN ~~pair~~ to a RADIUS server in the HSS over the Gi interface when a PDP context is activated towards the IMS system. The HSS has a binding between the IMSI and/or MSISDN and the IMPI and IMPU(s), and is therefore able to store the currently assigned IP address from the GGSN against the user'~~’~~s IMPI and/or IMPU(s). The precise way of the handling of these identities in the HSS is outside the scope of standardization. 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 IMPU~~I~~, 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~~ IMPU 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 ~~S~~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 a~~n~~ ~~authenticated~~ PDP context (based on an authenticated 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.

For the purposes of this present document, an APN, which is used for IMS services, is called an IMS APN. An IMS APN may be also used for non-IMS services. The mechanism described in this present document further adds a restriction that there is only one APN for accessing IMS for a PLMN and that all active PDP contexts, for a single UE, associated with that IMS APN use the same IP address at any given time.

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.

67.2 Detailed specification

67.2.1 Update of UE's IP address in HSS depending on PDP context stateGGSN-HSS interaction

When receiving an Activate PDP Context Request message, based on operator policy, a GGSN supporting early IMS security shall send a RADIUS "Accounting-Request START" message to a AAA server attached to the HSS. The message shall include the mandatory fields defined in subclause 16.4.3 of 3GPP TS 29.061 [4] and the UE's IP address, MSISDN and IMSI. 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 IMSI and/or the MSISDN to find the subscriber''s IMPI (derived from IMSI) and then store the IP address against the IMPIa suitable identity, e.g. the IMPI.

NOTE 1: It is assumed here that the RADIUS server for handling the accounting request to receive the IP address from the GGSN attached to the HSS 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.

NOTE 2: 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 accept the activatione of the PDP context if the accounting start message request is not successfully handled by the HSS (e.g. a positive Create PDP Context Response should not be sent by the GGSN until the "Accounting-Request START" message is received or a negative Create PDP Context Response is sent after some RADIUS response timeout occurs). In particular, it shall not be possible to have an active IMS PDP context associated with the IMS APN 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 When the UE establishes a newits first PDP context and therefore gets for an IMS APN a new IP address is obtained, and the GGSN shall send an "Accounting-Request START" to the HSS with the assigned IP address. If this IP address is different from the IP address already stored in the HSS (i.e. the "old" IP address), the HSS shall start the 3GPP IMS HSS-initiated de-registration procedure, if the UE is IMS registered, using a Cx-RTR/Cx-RTA exchange, and delete the old IP address. The HSS stores the new IP address and confirms the "Accounting-Request START" to the GGSN when either the de-registration procedure is successfully completed or after a suitable time-out. tThe UE shall starts the IMS initial registration procedure. The HSS shall abandon the de-registration procedure when a new successful authentication for this user is signalled by the S-CSCF in a Cx-SAR message.

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. When all the PDP contexts are de-activated at the IMS APN of the GGSN, the GGSN sends an "Accounting-Request STOP" request to the HSS. The HSS checks the IP address indicated by the "Accounting-RequestACCOUNTING-REQUEST STOP" message against the IP address stored in the HSS. If they are the same, an networkHSS-initiated de-registration procedure shall be started, if the UE is registered, using a Cx-RTR/Cx-RTA exchange. In theis case they are different, so the HSS shall then ignore the message.

6~~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. It shall be possible for the GGSN to ~~and~~ log the event in its security log against the subscriber information (IMSI/MSISDN), e.g. based on operator configuration.

6~~7~~.2.3 ~~Source IP address checking in the P-CSCF and S-CSCF~~Impact on IMS registration and authentication procedures

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. The changes to the IMS registration and authentication procedures are detailed in the following subclauses.

6.2.3.1 Procedures at the UE

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include an Authorization header field and not include a Security-Client header field. The From header, To header, Contact header, Expires header, Request URI, Supported header and a P-Asserted-Id header shall be set according subclause 5.1.1.2 of 3GPP TS 24.229 [7].

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according subclause 5.1.1.2 of 3GPP TS 24.229 [7].

NOTE 1: Early IMS security does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

NOTE 2: The UE shall not use the temporary public user identity used for registration in any subsequent SIP requests.

6~~7~~.2.3.2~~1~~ Procedures at the P-CSCF ~~mechanisms~~

NOTE: As ~~mandated by section 18.2.1 of~~specified in RFC 3261 [6], when the P-CSCF receives a SIP request from an early IMS UE, the P-CSCF~~will~~ checks the IP address in the "~~“~~sent-by"~~”~~ parameter of the ~~top~~ ~~“~~Via~~”~~ header field provided by the UE. ~~Specifically, if the host portion o~~If 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~~P-CSCF adds 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.~~

6.2.3.2.1 Registration

When the P-CSCF receives a REGISTER request from the UE that does not contain an Authorization header and does not contain a Security-Client header, the P-CSCF shall handle the Path header, the Require header, the P-Charging-Vector header and the P-Visited-Network-ID header as described in subclause 5.2.12 of 3GPP TS 24.229 [7]. Afterwards the P-CSCF shall determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) handle the Service-Route header, the public user identities, the P-Asserted-Identity header, the P-Charging-Function-Address header as described in subclause 5.2.2 of 3GPP TS 24.229 [7] for the reception of a 200 (OK) response; and

2) forward the 200 (OK) response to the UE.

6.2.3.2.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

As the early IMS security solution does not offer IPsec, the P-CSCF shall implement the procedures as described in subclause 5.2.6 of 3GPP TS 24.229 [7] with the following deviations.

For requests initiated by the UE, when the P-CSCF receives a 1xx or 2xx response, the P-CSCF shall not rewrite its own Record Route entry.

For requests terminated by the UE, when the P-CSCF receives a request, prior to forwarding the request, the P-CSCF shall not include a protected server port in the Record-Route header and in the Via header.

6.2.3.3 Procedures at the I-CSCF

NOTE: Topology hiding is not available with early IMS security because topology hiding alters the Via header.

67.2.3.24 Procedures at the S-CSCF mechanisms

6.2.3.4.1 Registration

Upon receipt of an initial REGISTER request without an Authorization header, the S-CSCF shall:

1) identify the user by the public user identity as received in the To header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) if no IP address is stored for the UE, query the HSS, as described in subclause 6.2.5 with the public user ID as input and store the received IP address of the UE. Prior to contacting the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [10];

NOTE: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

4) 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 “Vvia” header field provided by the UE. If a "“received"” parameter exists, S-CSCF shall compare the IP address recorded in the “received” parameter against the UE'’s IP address stored during registration. If no "“received"” parameter exists in the top “Vvia” header field provided by the UE, then S-CSCF shall compare IP address recorded in the "“sent-by"” parameter against the stored UE IP address stored during registration. In both cases, if the HSS retrievedstored IP address and the IP address recorded in the top “vVia” header provided by the UE do not match, the S-CSCF shall query the HSS, as described in subclause 6.2.5 with the public user ID as input and store the received IP address of the UE. If the stored IP address and the IP address recorded in the Via header provided by the UE still do not match the S-CSCF shall reject the registration with a 403 (Forbidden) response and skip the following steps.

5) handle the Cx Server Assignment procedure, the ICID, each non-barred registered public user identity, the Path header, the registration duration as described in subclause 5.4.1.2.2 of 3GPP TS 24.229 [7]; and

6) send a 200 (OK) response to the UE as described in subclause 5.4.1.2.2 of 3GPP TS 24.229 [7].

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.

6.2.3.4.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

On the reception of any request other than an initial REGISTER request, the S-CSCF shall check whether a "received" parameter exists in the Via header field provided by the UE. If a "received" parameter exists, S-CSCF shall compare the IP address received in the "received" parameter against the UE's IP address stored during registration. If no "received" parameter exists in the Via header field provided by the UE, then S-CSCF shall compare IP address received in the "sent-by" parameter against the IP address stored during registration. If the stored IP address and the IP address received in the Via header field provided by the UE do not match, the S-CSCF shall reject the request with a 403 (Forbidden) response.

In case the stored IP address and the IP address receive in the Via header field provided by the UE do match, the S-CSCF shall proceed as described in 5.4.3 of 3GPP TS 24.229 [7].

6.2.4 Identities and subscriptions

When early IMS security is supported, the HSS shall include for each subscription an IMPI and IMPU derived from the IMSI of the subscription according to the rules in 3GPP TS 23.003 [8]. If the network supports both early IMS security and fully compliant IMS security, the IMSI-derived IMPI and IMPU shall be stored in addition to other IMPIs and IMPUs that may have been allocated to the subscription.

If a UE attempts a registration using early IMS security, the REGISTER shall include an IMPU that is derived from the IMSI that is used for bearer network access according to the rules in 3GPP TS 23.003 [8]. The UE shall apply this rule even if a UICC containing an ISIM is present in the UE.

In the case that a UE is registering using early IMS security with an IMSI-derived IMPU, implicit registration shall be used as a mandatory function to register the subscriber's public user identity(s) using the rules defined in subclause 5.2.1a.1 of 3GPP TS 23.228 [3]. By applying these rules the IMSI-derived IMPU shall be barred in the HSS for all procedures other than SIP registration.

6.2.5 Impact on Cx Interface

Early IMS Security mechanism affects the use of the protocol defined for the Cx interface. In particular, the User-Authorisation-Request and Multimedia-Auth-Request/Answer messages are impacted.

Because in Early IMS Security the Private User Identity of the subscriber is not made available to the IMS domain in SIP messages, it is necessary to derive a Private User Identity from the Temporary Public User Identity to use as the content of the User-Name AVP in certain Cx messages (most notable UAR and MAR).

6.2.5.1 User registration status query

The UAR command, when implemented to support Early IMS Security follow the description in 6.1.1 of 3GPP TS 29.228 [10], with the following exception;-

- the Private User Identity (User-Name AVP) in the UAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present port number, URI parameters, and headers

6.2.5.2 Authentication procedure

The MAR and MAA commands, when implemented to support Early IMS Security follow the description in 6.3 of 3GPP TS 29.228 [10] of this document, with the following exceptions;-

- the Private User Identity (User-Name AVP) in the MAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present: port number, URI parameters, and headers.

- In the MAR and MAA commands, the Authentication Scheme (Authentication-Scheme AVP described in subclause 7.9.2 of 3GPP TS 29.228 [10]) within the SIP-Auth-Data-Item grouped AVP shall contain "Early-IMS-Security".

- In the MAA command, the SIP-Auth-Data-Item grouped AVP shall contain the user IP address. If the address is IPv4 it shall be included within the Framed-IP-Address AVP as defined in draft-ietf-aaa-diameter-nasreq-17.txt [11]. If the address is IPv6 it shall be included within the Framed-IPv6-Prefix AVP and, if the Framed-IPv6-Prefix AVP alone is not unique for the user it shall also contain Framed-Interface-Id AVP.

  This results in SIP-Auth-Data-Item as depicted in table 6.3.4 of 3GPP TS 29.228 [10], being replaced when Early IMS Security is employed by a structure as shown in Table 2.

Table 2: Authentication Data content for Early IMS Security

Information element name	**Mapping to Diameter AVP**	**Cat.**	**Description**
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For Early IMS Security it will indicate "Early-IMS-Security"
User IPv4 Address	Framed-IP-Address	C	If the IP Address of the User is an IPv4 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11].
User IPv6 Prefix	Framed-IPv6-Prefix	C	If the IP Address of the User is an IPv6 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11].
Framed Interface Id	Framed-Interface-Id	C	If the IP Address of the User is an IPv6 address and the Framed-IPv6-Address AVP alone is not unique for the user this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11].

The ABNF description of the AVP as given in subclause 6.3.13 of 3GPP TS 29.229 [12] is replaced with that given below.

```
SIP-Auth-Data-Item :: = < AVP Header : TBD >
        [ SIP-Authentication-Scheme ]
        [ Framed-IP-Address ]
        [ Framed-IPv6-Prefix ]
        [ Framed-Interface-Id ]
        * [AVP]
```

- Step 5 of subclause 6.3.1 of 3GPP TS 29.229 [12] shall apply with the following exception:
  - HSS shall return only one SIP-Auth-Data-Item

~~7~~6.2.6~~4~~ ~~—~~Interworking cases

For the purposes of the interworking considerations in this subclause, it is assumed that the IMS entities P-CSCF, I-CSCF, S-CSCF and HSS reside in the home network and all support the same variants of IMS, i.e. all support either only early IMS, or only fully compliant IMS, or both.

NOTE: It is compatible with the considerations in this document that the UE uses different APNs to indicate the IMS variant currently used by the UE, in case the P-CSCF functionality is split over several physical entities.

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~~REGISTER ~~message~~ request 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~~REGISTER ~~message~~request, early IMS UEs only provide the IMS public identity (IMPU), but not the IMS private identity (IMPI) 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 for early IMS, the Cx interface carries ~~both the private user identity and~~only the public user identity in Cx-MAR requests (sent by I-CSCF and S-CSCF HSS). ~~For early IMS, only the public user identity shall be sent to the HSS within these requests, and t~~The private user identity within these requests shall contain the IMPU as received by the UE~~shall be empty~~. This avoids changes to the message format ~~to~~ on the Cx interface.

If the S-CSCF receives an indication that the UE is early IMS, then it shall be able to select the "~~"~~Early-IMS-Security~~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~~response. 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

   Early IMS security according to this annex shall be used for authenticating the UE for all registrations from UEs that do not provide the fully compliant IMS security headers.~~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. The UE shall use fFully compliant IMS security shall be used, if the network supports this, otherwise the UE shall use 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 RegisterREGISTER messagerequest (this header cannot be ignored by the P-CSCF).

NOTE: The Proxy-Require header cannot be ignored by the P-CSCF.

The UE shall, after receiving the error messageresponse, send an early IMS registration, i.e., shall send a new REGISTERegister requestmessage 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 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 Register messagerequest, receives indication that the IMS UE is fully compliant and shall continue as specified by TS 33.203 [2].

5. Mobile equipment and IMS network support both, UE contains a SIM

The UE might start with the fully compliant IMS registration procedure. However, when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that the UE contains a SIM and return an error.

The S-CSCF shall answer with a 401 (Unauthorized) with an Error-info: header containing the text "Early security required". The UE then retries using early IMS security.

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

The UE sends a REGISTERRegister requestmessage to the IMS network that does not contain the necessary security headers required by fully compliant IMS. The fully compliant P-CSCF will detect that the Security-Client header is missing and return a 4xx responses, as described in subclause 5.2.2 of 3GPP TS 24.229 [7].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.

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

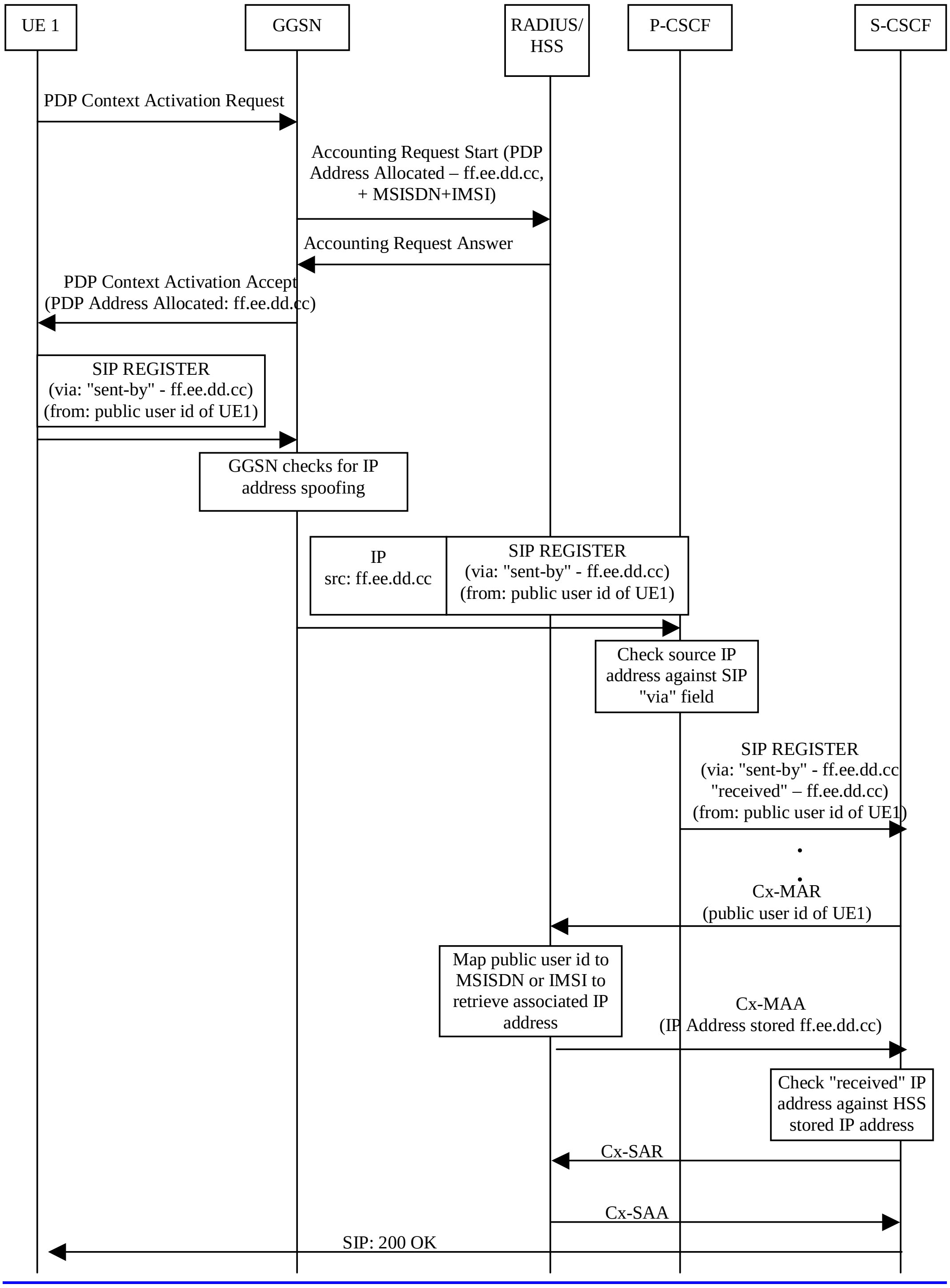
The UE shall start with the fully compliant IMS registration procedure. The early IMS P-CSCF shall answer with a 420 "(Bad Extension") failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial RegisterREGISTER messagerequest (this header cannot be ignored by the P-CSCF). After receiving the error messageresponse, the UE shall stop the attempt to register with this network, since the fully 3GPP compliant IMS security according to TS 33.203 [2] is not supported.

67.2.75 Message flows

7.2.5.16.2.7.1 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 clausesubclause 76.2.3.21.


UE 1
GGSN
RADIUS/ HSS
P-CSCF
S-CSCF
PDP Context Activation Request
Accounting Request Start (PDP Address Allocated – ff.ee.dd.cc, + MSISDN+IMSI)
Accounting Request Answer
PDP Context Activation Accept (PDP Address Allocated: ff.ee.dd.cc)
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc) (from: public user id of UE1)
GGSN checks for IP address spoofing
IP src: ff.ee.dd.cc
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc) (from: public user id of UE1)
Check source IP address against SIP "via" field
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc "received" – ff.ee.dd.cc) (from: public user id of UE1)
Cx-MAR (public user id of UE1)
Map public user id to MSISDN or IMSI to retrieve associated IP address
Cx-MAA (IP Address stored ff.ee.dd.cc)
Check "received" IP address against HSS stored IP address
Cx-SAR
Cx-SAA
SIP: 200 OK

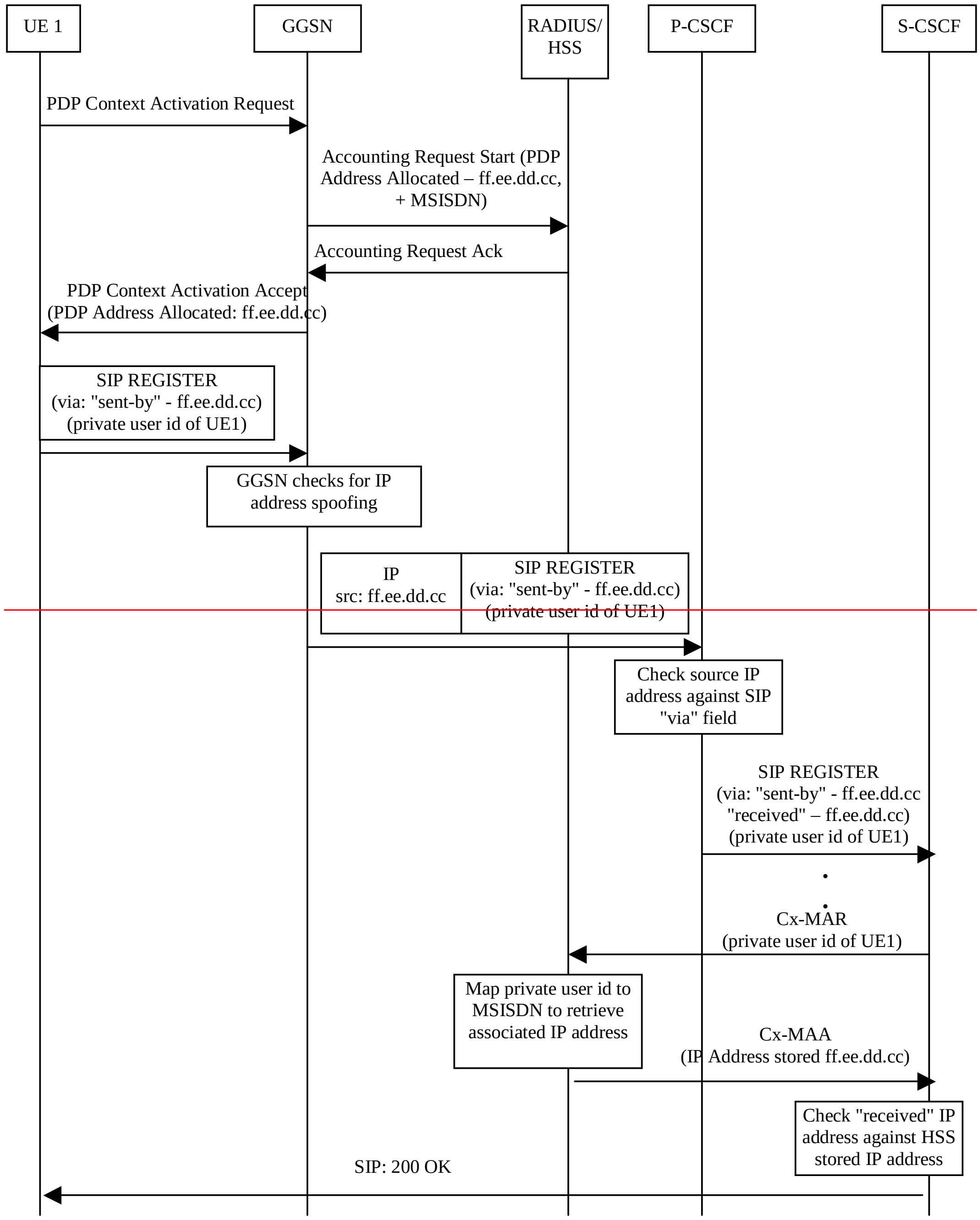
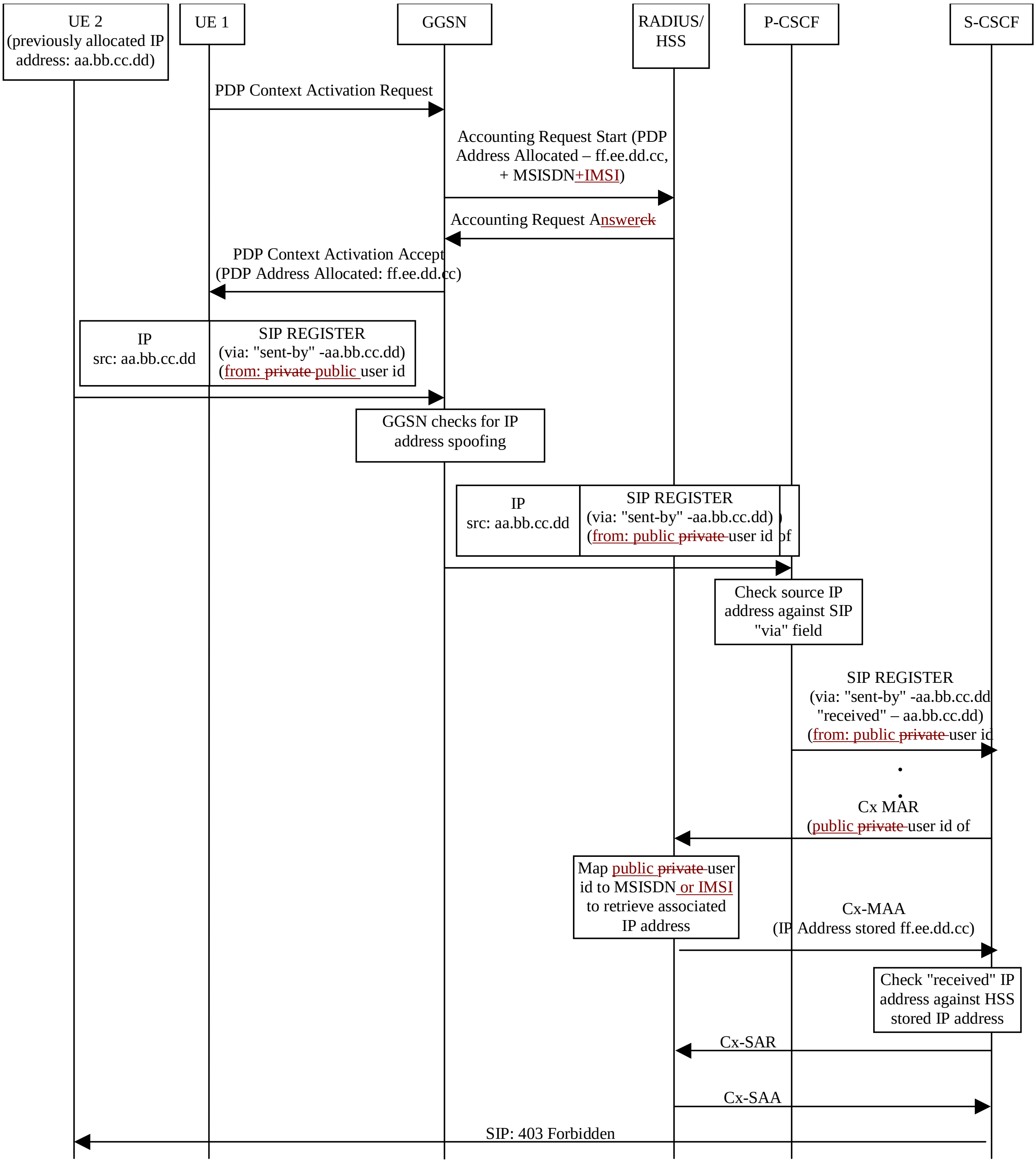


Figure 1: Message sequence for early IMS security showing a successful registration

67.2.75.2 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 clausesubclause 67.2.3.21.


UE 2
(previously allocated IP address: aa.bb.cc.dd)
UE 1
GGSN
RADIUS/ HSS
P-CSCF
S-CSCF
PDP Context Activation Request
Accounting Request Start (PDP Address Allocated – ff.ee.dd.cc, + MSISDN+IMSI)
Accounting Request Answerck
PDP Context Activation Accept (PDP Address Allocated: ff.ee.dd.cc)
IP src: aa.bb.cc.dd
SIP REGISTER (via: "sent-by" -aa.bb.cc.dd) (from: private public user id
GGSN checks for IP address spoofing
IP src: aa.bb.cc.dd
SIP REGISTER (via: "sent-by" -aa.bb.cc.dd) (from: public private user id of
Check source IP address against SIP "via" field
SIP REGISTER (via: "sent-by" -aa.bb.cc.dd "received" – aa.bb.cc.dd) (from: public private user id
Cx MAR (public private user id of
Map public private user id to MSISDN or IMSI to retrieve associated IP address
Cx-MAA (IP Address stored ff.ee.dd.cc)
Check "received" IP address against HSS stored IP address
Cx-SAR
Cx-SAA
SIP: 403 Forbidden

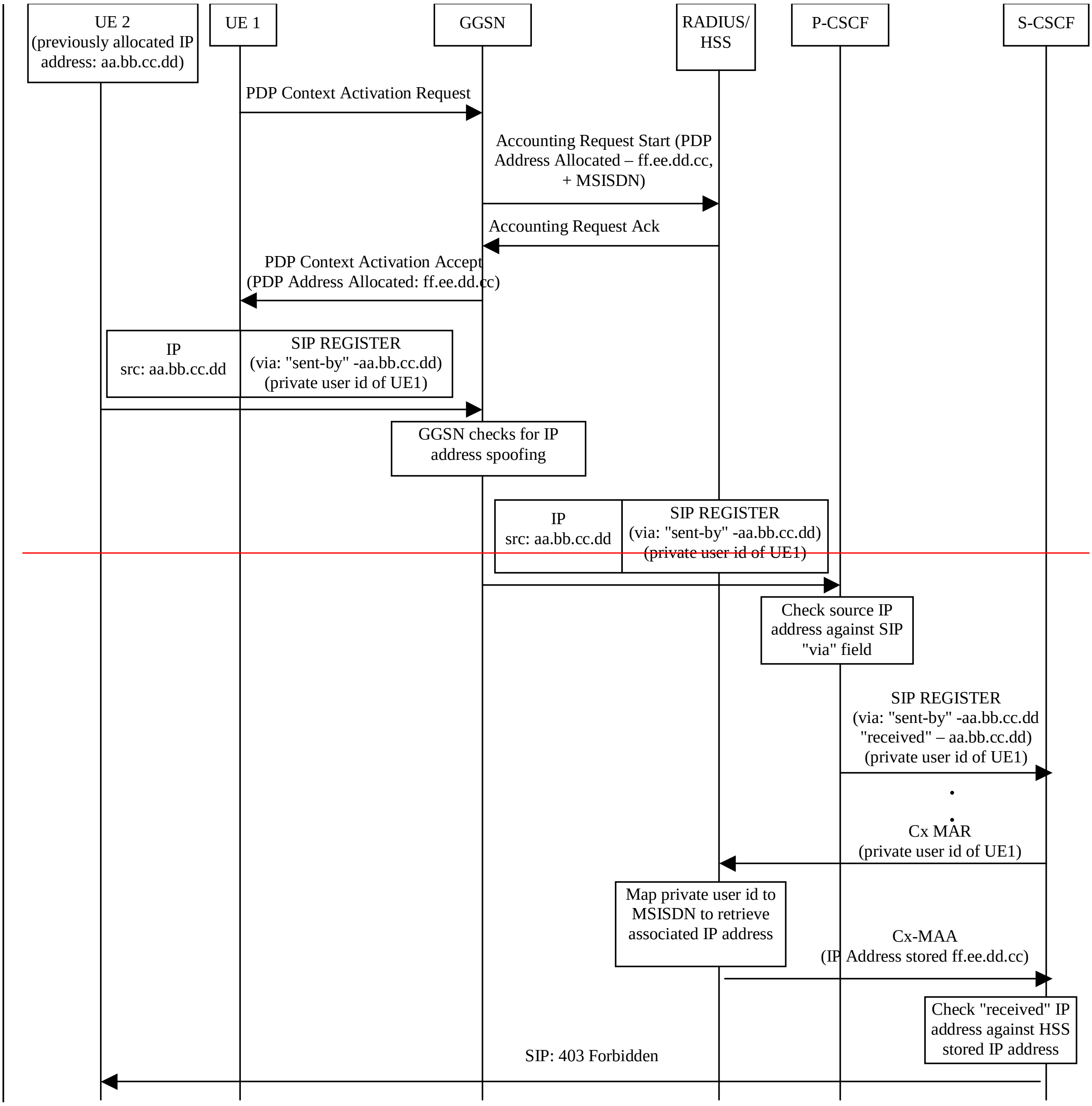
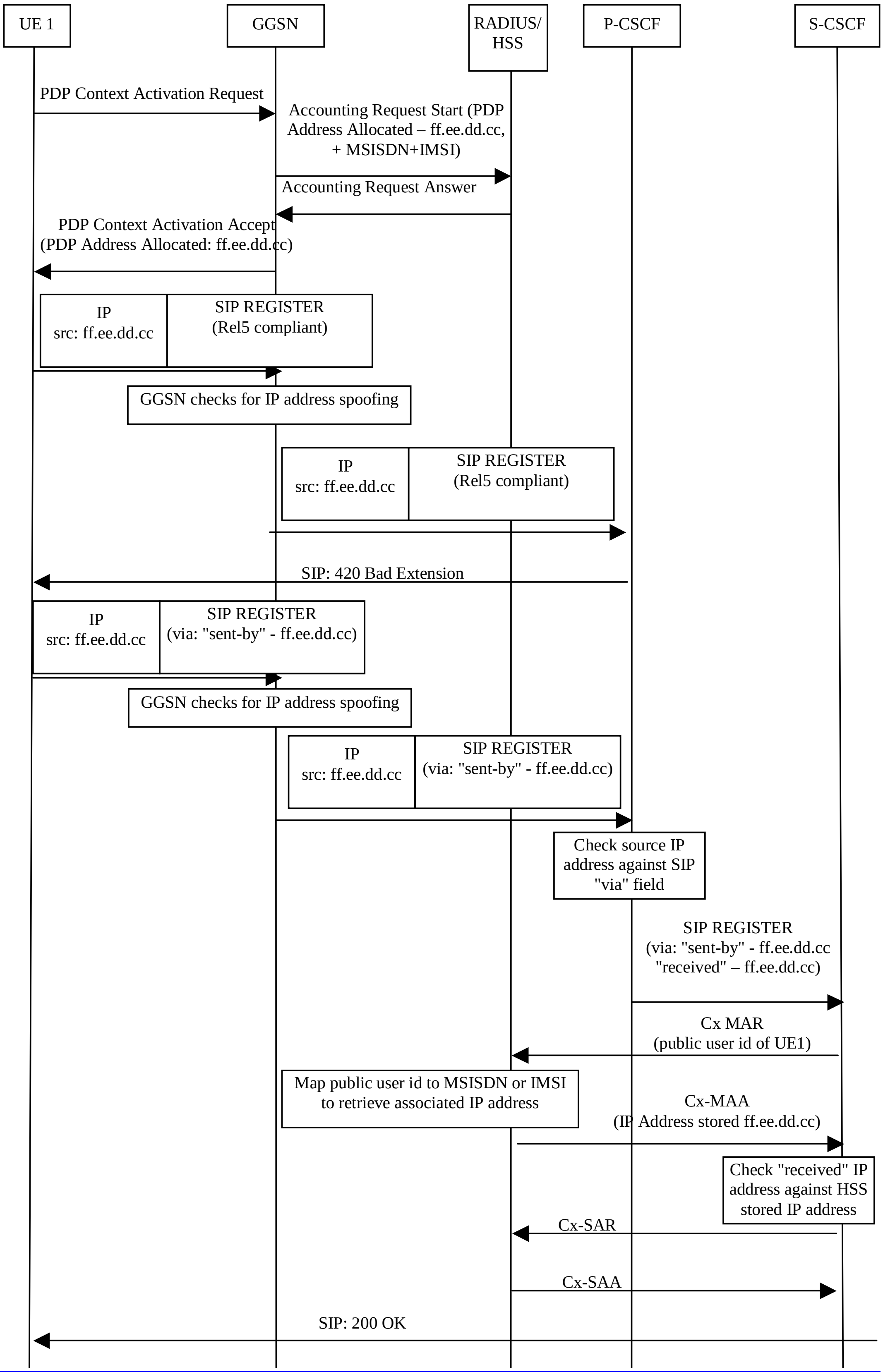


Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

6~~7~~.2.7~~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~~subclause 6~~7~~.2.6~~4~~.

Note, that the "~~“~~received"~~”~~ parameter is only sent from P-CSCF to S-CSCF under the conditions given in ~~clause~~subclause 6~~7~~.2.3.2~~1~~.


UE 1
GGSN
RADIUS/ HSS
P-CSCF
S-CSCF
PDP Context Activation Request
Accounting Request Start (PDP Address Allocated – ff.ee.dd.cc, + MSISDN+IMSI)
Accounting Request Answer
PDP Context Activation Accept (PDP Address Allocated: ff.ee.dd.cc)
IP src: ff.ee.dd.cc
SIP REGISTER (Rel5 compliant)
GGSN checks for IP address spoofing
IP src: ff.ee.dd.cc
SIP REGISTER (Rel5 compliant)
SIP: 420 Bad Extension
IP src: ff.ee.dd.cc
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc)
GGSN checks for IP address spoofing
IP src: ff.ee.dd.cc
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc)
Check source IP address against SIP "via" field
SIP REGISTER (via: "sent-by" - ff.ee.dd.cc "received" – ff.ee.dd.cc)
Cx MAR (public user id of UE1)
Map public user id to MSISDN or IMSI to retrieve associated IP address
Cx-MAA (IP Address stored ff.ee.dd.cc)
Check "received" IP address against HSS stored IP address
Cx-SAR
Cx-SAA
SIP: 200 OK

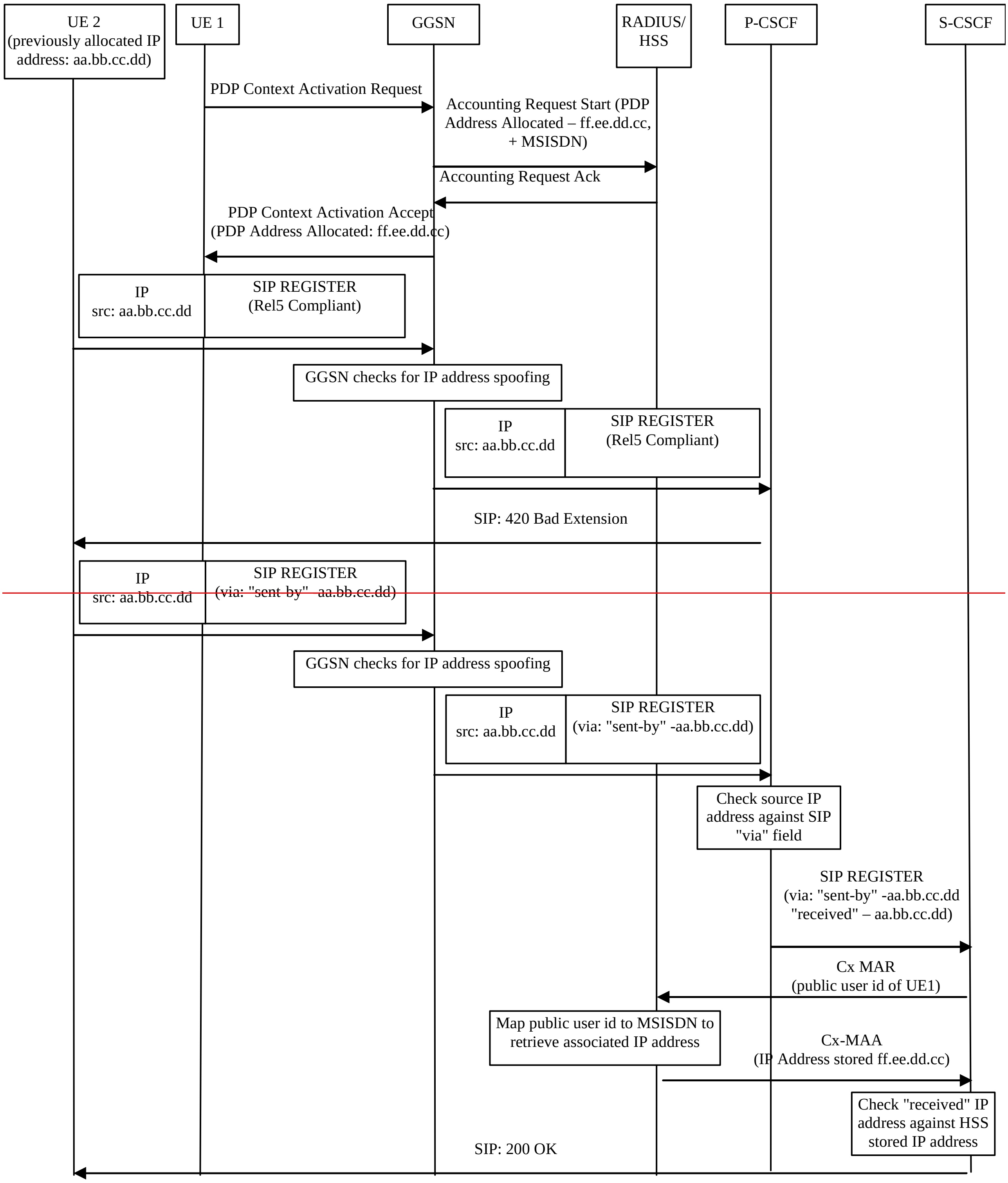


Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant IMS and early IMS access security and network supports early IMS security only

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 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
25/11/04					Incorporates changes agreed at SA3#36.	0.0.3	0.0.4