# ETSI TR 133 978 V6.6.0 (2006-12)

*Technical Report*

**Universal Mobile Telecommunications System (UMTS);**
**Security aspects of early IP Multimedia Subsystem (IMS)**
**(3GPP TR 33.978 version 6.6.0 Release 6)**

Reference

RTR/TSGS-0333978v660

Keywords

UMTS

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

***Important notice***

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

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

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

# 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 clause 5.1 of TS 23.221 [13], there will exist IMS implementations based on IPv4 (TR 23.981 [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.

# 1 Scope

The present document documents an interim security solution for early IMS implementations that are not fully compliant with the IMS security architecture specified in TS 33.203 [2]. For security reasons, the provisions in this TR only apply to IMS procedures used over the 3GPP PS domain.

# 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: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Interworking aspects and migration scenarios for IPv4 based IMS Implementations".

[2] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services".

[3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage ".

[4] 3GPP TS 29.061: "3rd Generation Partnership Project; Technical Specification Group Core Network; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[5] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[6] IETF RFC 3261: "Session Initiation Protocol".

[7] 3GPP TS 24.229: "3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[8] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[9] 3GPP TS 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[10] 3GPP TS 29.228: "3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[11] IETF RFC 4005 "Diameter Network Access Server Application",.

[12] 3GPP TS 29.229: "3rd Generation Partnership Project; Technical Specification Group Core Network; Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[13] 3GPP TS 23.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architectural requirements".

[14] 3GPP TS 33.141: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Presence service; security ".

[15] 3GPP TS 29.328 "3rd Generation Partnership Project; Technical Specification Group Core Network;IP Multimedia (IM) Subsystem Sh interface; signalling flows and message contents"

[16] 3GPP TS 29.329 "3rd Generation Partnership Project; Technical Specification Group Core Network;IP Multimedia (IM) Subsystem Sh interface; Protocol details "

[17] 3GPP TS 24.109 "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details "

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 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.

**A single early IMS security solution:** Interfaces that are impacted by the early IMS security solution should be adequately documented to ensure interoperability between vendors.

**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 clause 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

### 6.1.1 Security mechanism

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.

When using IPv6, stateless autoconfiguration is the only IP address allocation method mandatorily supported by the terminal in GPRS. With this method, a primary PDP context is bound only to the 64-bit prefix of the 128-bit IPv6 address, not the full address. This needs to be taken into account in Early IMS procedures.

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 (or the prefix in the case of IPv6 stateless autoconfiguration), 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 (or the prefix in the case of IPv6 stateless autoconfiguration) 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 (or the prefix in the case of IPv6 stateless autoconfiguration) 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 (or the prefix in the case of IPv6 stateless autoconfiguration) in the SIP header (verified by the network) matches the IP address (or the prefix in the case of IPv6 stateless autoconfiguration) 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 (or the prefix in the case of IPv6 stateless autoconfiguration) 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 early IMS security solution may also be re-used to protect HTTP traffic in order to provide user access to various potential self-customization services, e.g. to Presence Server.

### 6.1.2 Restrictions imposed by early IMS security

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 security 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 the requirement on the UE that it allows 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.

The early IMS security mechanism relies on the Via header remaining unchanged between the UE and the S-CSCF for requests and responses sent in the direction from the UE to the S-CSCF.

Due to the fact that the Authorisation header is not included in REGISTER requests in early IMS security, the I-CSCF is unable to use the presence or absence of the "integrity-protected" parameter to distinguish initial and non-initial REGISTER messages. Therefore the S-CSCF reselection procedure described in clause 5.3.1.3 of TS 24.229 [7] cannot be used.

Early IMS security requires the GGSN to be in the home network.

The interim solution works with UEs that contain a SIM or a USIM, whereas full IMS security requires a USIM or ISIM. The interim solution does not authenticate at the IMS level. Instead, it relies on bearer level security at the GPRS or UMTS PS level. Because there is no key agreement, IPsec security associations are not set up between UE and P-CSCF, as they are in the full IMS security solution.

The solution works by binding the IMS level transactions to the GPRS or UMTS PS domain security association established at a GPRS or UMTS PS domain level. In doing so, it creates a dependency between SIP and the PS bearer, which does not exist with the full IMS security solution. This means that the interim solution does not provide as high a degree of access network independency as the full solution. In particular, the solution does not currently support scenarios where IMS services are offered over WLAN. If support for WLAN access is required then the full solution must be used or the interim solution must be extended to cover WLAN access.

Early IMS security derives the public user identity used in the REGISTER request from the IMSI. Consequently, the same public user identity cannot be simultaneously registered from multiple terminals, using only early IMS security registration procedures. However, simultaneous registration of a public user identity from one terminal using early IMS security, and from other terminals using fully compliant IMS security is not precluded.

Unlike in full IMS security, the private user identity is not included in the REGISTER requests when early IMS security is used for registration, re-registration and mobile-initiated de-registration procedures. Subsequently, all REGISTER requests from the UE shall use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. Otherwise, the I-CSCF would be unable to derive the private user identity that is needed to query the HSS in certain Cx messages.

NOTE: The early IMS mechanism for security is completely independent of early IMS implementations based on IPv4. For example, an IPv4 based implementation may use the full IMS security solution in TS 33.203 [2].

### 6.1.3 Early IMS security and logical entities

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 clause 16.4.3 of TS 29.061 [4] and the UE's IP address (or the prefix in the case of IPv6 stateless autoconfiguration), 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 (or the prefix in the case of IPv6 stateless autoconfiguration) 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 (or the prefix in the case of IPv6 stateless autoconfiguration) is not stored in the HSS.

When the UE establishes a PDP context for an IMS APN, which is not a secondary PDP context, a new IP address (or the prefix in the case of IPv6 stateless autoconfiguration) is obtained, and the GGSN shall send an "Accounting-Request START" to the HSS with the assigned IP address (or the prefix in the case of IPv6 stateless autoconfiguration). Depending on the status of the HSS the following steps have to be executed:

1) If an IP address (or prefix) is stored in the HSS and this IP address (or prefix) is different from the IP address (or prefix) received from the GGSN, the HSS shall (i) start the 3GPP IMS HSS-initiated de-registration procedure, if the UE is IMS registered, using a Cx-RTR/Cx-RTA exchange, and (ii) delete the old IP address (or prefix).

2) The HSS stores the new IP address (or prefix) and confirms the "Accounting-Request START" to the GGSN. In case step 1 was executed, confirmation is sent either when the de-registration procedure is successfully completed or after a suitable time-out.

3) The UE starts the IMS initial registration procedure.

4) In case step 1 was executed, 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 (or prefix) indicated by the "Accounting-Request STOP" message against the IP address (or prefix) stored in the HSS. If they are the same, the HSS shall delete the IP address (or prefix) and 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 (or the prefix in the case of IPv6 stateless autoconfiguration) 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 (or prefix) and successfully receive service from the IMS. The mechanisms in the following 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 clauses.

#### 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 header fields or header field values as required by RFC3329. The From header, To header, Contact header, Expires header, Request URI and Supported header shall be set according clause 5.1.1.2 of 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 clause 5.1.1.2 of TS 24.229 [7].

The UE shall support SIP compression as described in TS 24.229 [7] subclause 8.1.1 with the exception that no security association exists between the UE and the P-CSCF. Therefore, when the UE creates the compartment is implementation specific.

The UE shall use the temporary public user identity (IMSI-derived IMPU, cf. section 6.1.2) only in registration messages (i.e. initial registration, re-registration or de-registration), but not in any other type of SIP requests.

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.

#### 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 clause 5.2.12 of 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-Associated-URI header, the P-Charging-Function-Address header as described in clause 5.2.2 of TS 24.229 [7] for the reception of a 200 (OK) response; and

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

The P-CSCF shall support SIP compression as described in TS 24.229[7] subclause 8.2.1 with the exception that no security association exists between the UE and the P-CSCF. Therefore, when the P-CSCF creates the compartment is implementation specific.

#### 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 clause 5.2.6 of 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 use a protected server port number to rewrite its own Record Route entry. Instead, it shall use the number of an unprotected port where it awaits subsequent requests from the UE.

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. Instead, it shall include the number of an unprotected port where it expects subsequent requests from the UE, and the number of an unprotected port where it expects responses to the current request, respectively.

### 6.2.3.3 Procedures at the I-CSCF

If the I-CSCF receives an initial REGISTER request with no Authorization header included, the I-CSCF shall not reject the message. Instead, it shall behave as described in section 6.2.5.1.

Early IMS security requires that the I-CSCF between a P-CSCF and S-CSCF does not alter the Via header for requests and responses sent in the direction from the UE to the S-CSCF. An I-CSCF between an S-CSCF and another S-CSCF is unaffected by early IMS security.

The S-CSCF reselection procedure described in clause 5.3.1.3 of TS 24.229 [7] shall not be applied.

### 6.2.3.4 Procedures at the S-CSCF

#### 6.2.3.4.1 Registration

Upon receipt of a 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 (or prefix) is stored for the UE, query the HSS, as described in clause 6.2.5 with the public user ID as input and store the received IP address (or prefix) of the UE; if the S-CSCF receives a prefix from the HSS, it will check only against prefixes in the sequel, otherwise against the full IP address.

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. In case of IPv6 stateless autoconfiguration, S-CSCF shall compare the prefix of the IP address recorded in the "received" parameter against the UE's IP address prefix 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 case of IPv6 stateless autoconfiguration, S-CSCF shall compare the prefix of the IP address recorded in the "sent-by" parameter against the UE's IP address prefix stored during registration. In any case, if stored IP address (or prefix) and the (prefix of 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 clause 6.2.5 with the public user ID as input and store the received IP address (or prefix) of the UE. If the stored IP address (or prefix) and the (prefix of 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 clause 5.4.1.2.2 of TS 24.229 [7]; and send a 200 (OK) response to the UE as described in clause 5.4.1.2.2 of TS 24.229 [7].

When a user de-registers, or is de-registered by the HSS (cf. section 6.2.1), the S-CSCF shall delete the IP address stored for the UE.

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

On the reception of any request other than a 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 (prefix of the) IP address received in the "received" parameter against the UE's IP address (or prefix) stored during registration. If no "received" parameter exists in the Via header field provided by the UE, then S-CSCF shall compare the (prefix of the) IP address received in the "sent-by" parameter against the IP address (or prefix) stored during registration. If the stored IP address (or prefix) and the (prefix of 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 (or prefix) and the (prefix of the) IP address received in the Via header field provided by the UE do match, the S-CSCF shall proceed as described in clause 5.4.3 of 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 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 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 clause 5.2.1a.1 of TS 23.228 [3]. By applying these rules the IMSI-derived IMPU shall be barred for all procedures other than SIP registration.

When early IMS security is used for registering an UE, the IMSI-derived IMPU shall be used for all registration procedures initiated by the UE (i.e., initial registration, re-registration and mobile-initiated de-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/Answer (Cx-UAR/UAA), the Multimedia-Auth-Request/Answer (Cx-MAR/MAA) and the Server-Assignment-Request/Answer (Cx-SAR/SAA) 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 clause 6.1.1 of 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 S-CSCF registration/deregistration notification

The SAR command, when implemented to support early IMS Security follows the description in clause 6.1.2 of TS 29.228 [10], with the following exception:

- the Private User Identity (User-Name AVP) in the SAR 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.

### 6.2.5.3 Authentication procedure

The MAR and MAA commands, when implemented to support Early IMS Security follow the description in clause 6.3 of TS 29.228 [10], 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 clause 7.9.2 of 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 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<br>(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.<br>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.<br>For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11]. |
| Framed Interface Id | Framed-Interface-Id | C | If and only if the IP Address of the User is an IPv6 address and the Framed-IPv6-Prefix AVP alone is not unique for the user this AVP shall be included.<br>For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11]. |

The ABNF description of the AVP as given in clause 6.3.13 of 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 clause 6.3.1 of TS 29.228 [10] 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 clause, 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 security, or only fully compliant IMS security, or both.

NOTE 1: 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 security" in the following) and UEs implementing the early IMS security solution specified in the present document (denoted "early IMS security" 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 security. The REGISTER request sent by an early IMS UE security to the IMS network shall not contain the security headers specified by TS 33.203 [2] (Authorization and Security-Client).

As a result, early IMS security UEs shall not add an explicit indication for the security used to the IMS signaling. An IMS network supporting both early IMS security and fully 3GPP compliant IMS security 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 security UEs).

During the process of user registration for early IMS security, the Cx interface carries the public user identity in Cx-UAR requests (sent by I-CSCF) and Cx-MAR as well as Cx-SAR requests (sent by S-CSCF). The private user identity within these requests shall be generated according to section 6.2.5.1. This avoids changes to the message format on the Cx interface.

If the S-CSCF receives an indication that the UE is an early IMS UE, then it shall be able to select the "Early-IMS-Security" authentication scheme in the Cx-MAR request.

For interworking between early IMS security and fully compliant IMS security implementations during IMS registration, an ME that implements the full IMS security solution from TS 33.203 [2] (or both Early IMS and full IMS security) shall not attempt to register using the full IMS security solution if neither a USIM nor a ISIM is present. The following cases shall be supported:

1. Both ME and IMS network support early IMS security only.

   IMS registration shall take place as described by the present document. This applies regardless of whether SIM or USIM/ISIM is in use.

2. ME supports early IMS security only, IMS network supports both early IMS security and fully compliant IMS security.

   IMS registration shall take place as described by the present document. This applies regardless of whether SIM or USIM/ISIM is in use.

3. ME supports both, IMS network supports early IMS security only.

   The ME shall check the smartcard application in use.

   If a SIM is in use, then it shall start with an Early IMS security procedure, else it shall start with the fully compliant IMS Registration procedure.

   In the second case, 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 2: 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.

NOTE 3: If the UE already has knowledge about the IMS network capabilities (which could for example be preconfigured in the UE), the appropriate authentication method can be chosen. The UE can use fully compliant IMS security, if the network supports this, otherwise the UE can use early IMS security.

4. ME and IMS network support both.

   The ME shall check the smartcard application in use.

   If a USIM/ISIM application is in use, then the ME shall start with the fully compliant IMS security 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].

   If a SIM is in use, then the ME shall start with the Early IMS security registration procedure. If the ME starts with the fully compliant IMS security registration procedure when a SIM is in use, this is an error case to be handled as follows: when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that a SIM is in use and returns an error. The S-CSCF shall answer with a 403 (Forbidden). After receiving the 403 response, the UE shall stop the attempt to register with this network.

5. ME supports early IMS security only, IMS network supports fully compliant IMS security only.

   The UE sends a REGISTER request to the IMS network that does not contain the security headers required by fully compliant IMS security. The fully compliant IMS security P-CSCF will detect that the Security-Client header is missing and return a 4xx response, as described in clause 5.2.2 of TS 24.229 [7]. This applies regardless of whether SIM or USIM/ISIM is in use.

6. ME supports fully compliant IMS security only, IMS network supports early IMS security only.

   A ME supporting Full IMS security only is not aware of Early IMS security, so its behaviour is expected to be compliant with TS 33.203 [2]. Based on this, if a SIM is in use, the ME should not attempt to register using the full IMS security solution. Whatever attempt would fail anyway, as Full IMS security requires ISIM/USIM.

If a USIM/ISIM application is in use, then the ME shall start with the fully compliant IMS security 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.

7. ME supports fully compliant IMS access security only, IMS network supports both.

   A ME supporting Full IMS security only is not aware of Early IMS security, so its behaviour is expected to be compliant with TS 33.203 [2]. Based on this, if a SIM is in use, the ME should not attempt to register using the full IMS security solution. Whatever attempt would fail anyway, as Full IMS security requires ISIM/USIM.

   If a USIM/ISIM application is in use, then the ME 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].

8. ME supports both, IMS network supports fully compliant IMS access security only.

   The ME shall check the smartcard application in use.

   If a USIM/ISIM application is in use, then the ME 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].

   If a SIM is in use, then the ME shall start with the Early IMS security registration procedure (in this case the IMS authentication procedure will fail). In this context, if the ME starts with the fully compliant IMS security registration procedure, this is an error case: when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that the a SIM is in use and return an error. The S-CSCF shall answer with a 403 (Forbidden). After receiving the 403 response, the UE shall stop the attempt to register with this network.

9. Both ME and IMS network support fully compliant IMS access security only.

   A ME supporting Full IMS security only is not aware of Early IMS security, so its behaviour is expected to be compliant with TS 33.203 [2]. Based on this, if a SIM is in use, the UE should not attempt to register using the full IMS security solution. If the UE starts with the fully compliant IMS security registration procedure when a SIM is in use, this is an error case to be handled as follows: the HSS will discover that a SIM is in use and return an error to the S-CSCF. The S-CSCF shall answer with a 403 (Forbidden). After receiving the 403 response, the UE shall stop the attempt to register with this network.

   If the USIM/ISIM application is in use, IMS registration shall take place as described by TS 33.203 [2].

## 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: The "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 6.2.3.2.

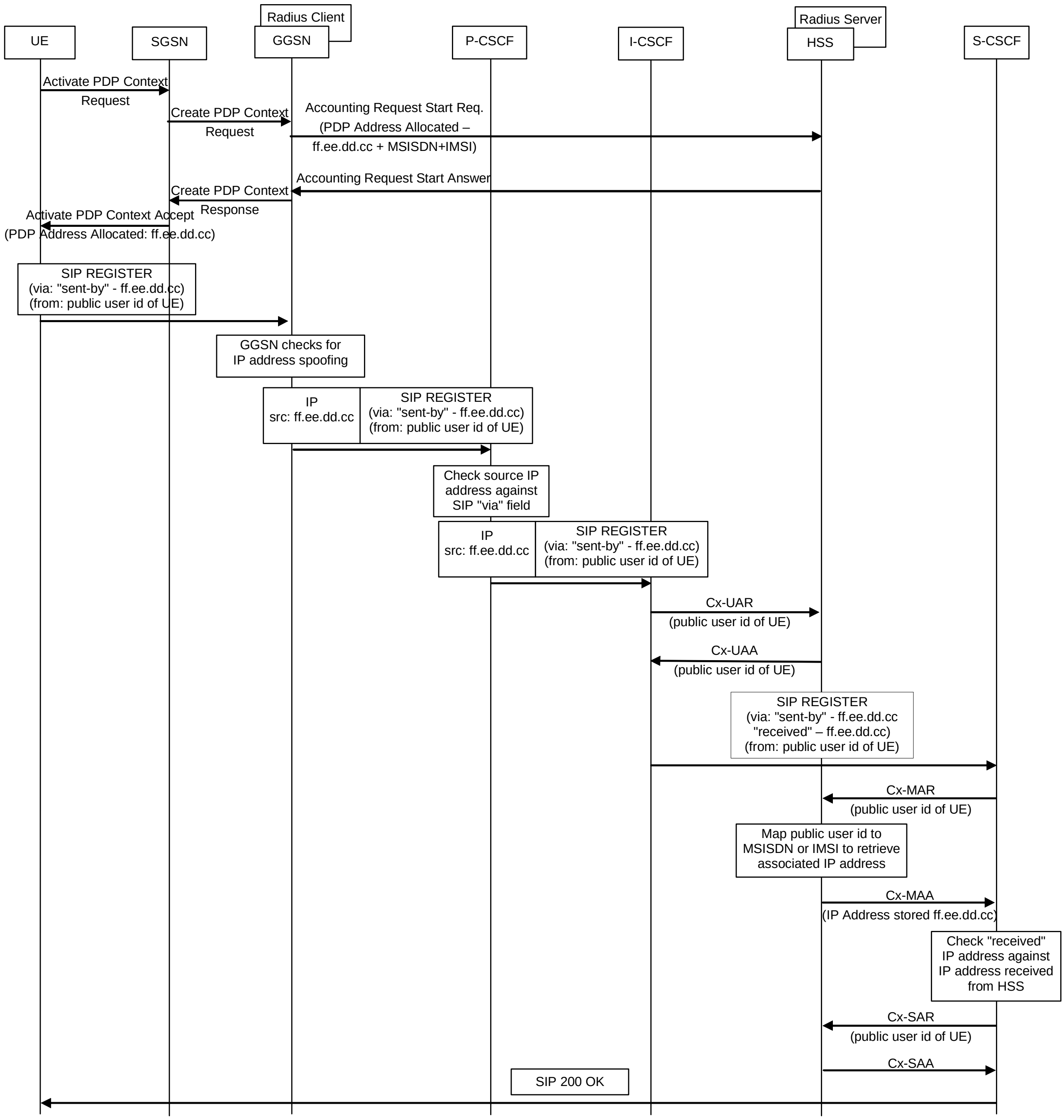


**Figure 1: Message sequence for early IMS security showing a successful registration**

### 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 clause 6.2.3.2.

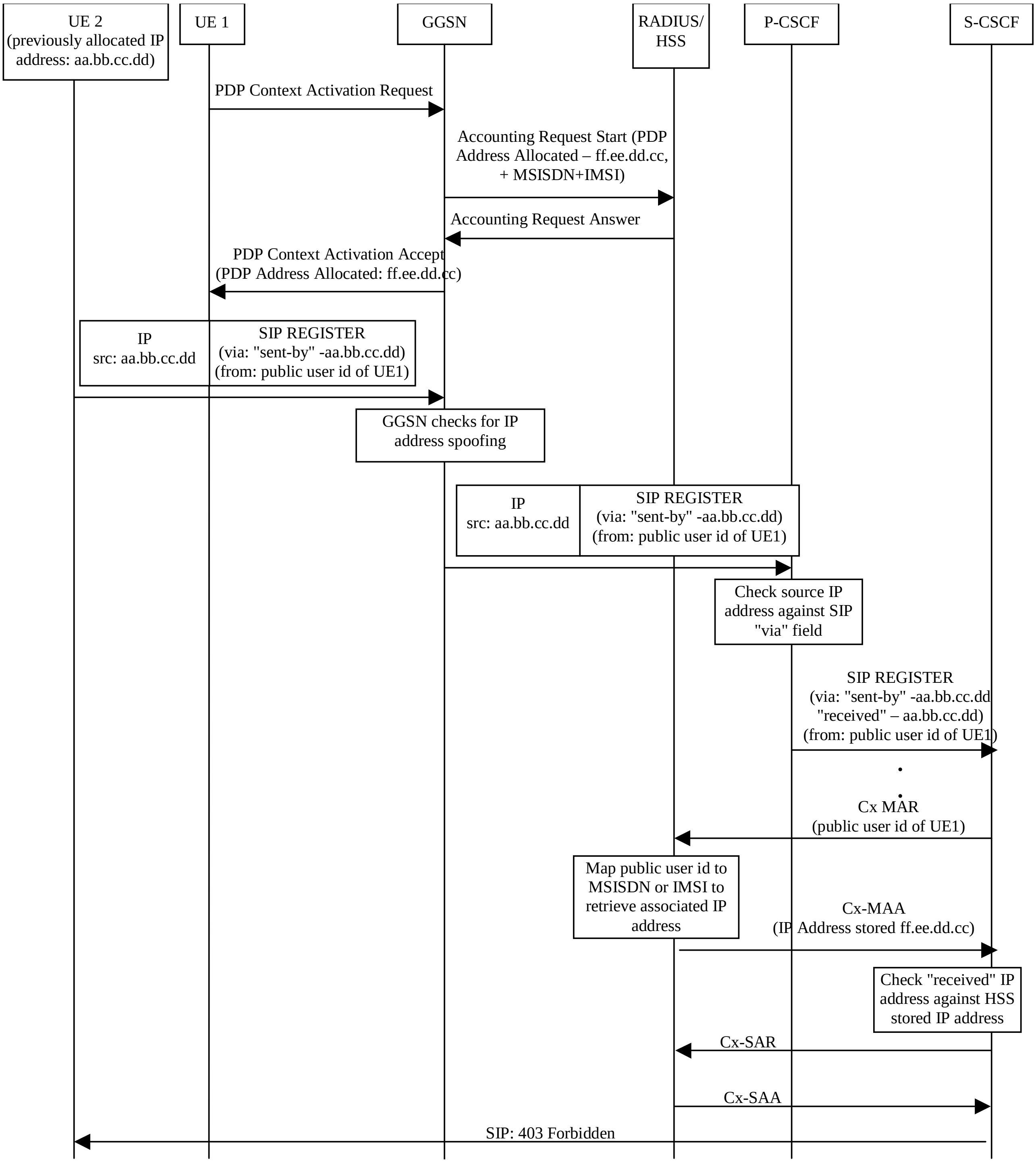


**Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft**

### 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 security only. This case is denoted as case 3 in clause 6.2.6.

NOTE: The "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 6.2.3.2.

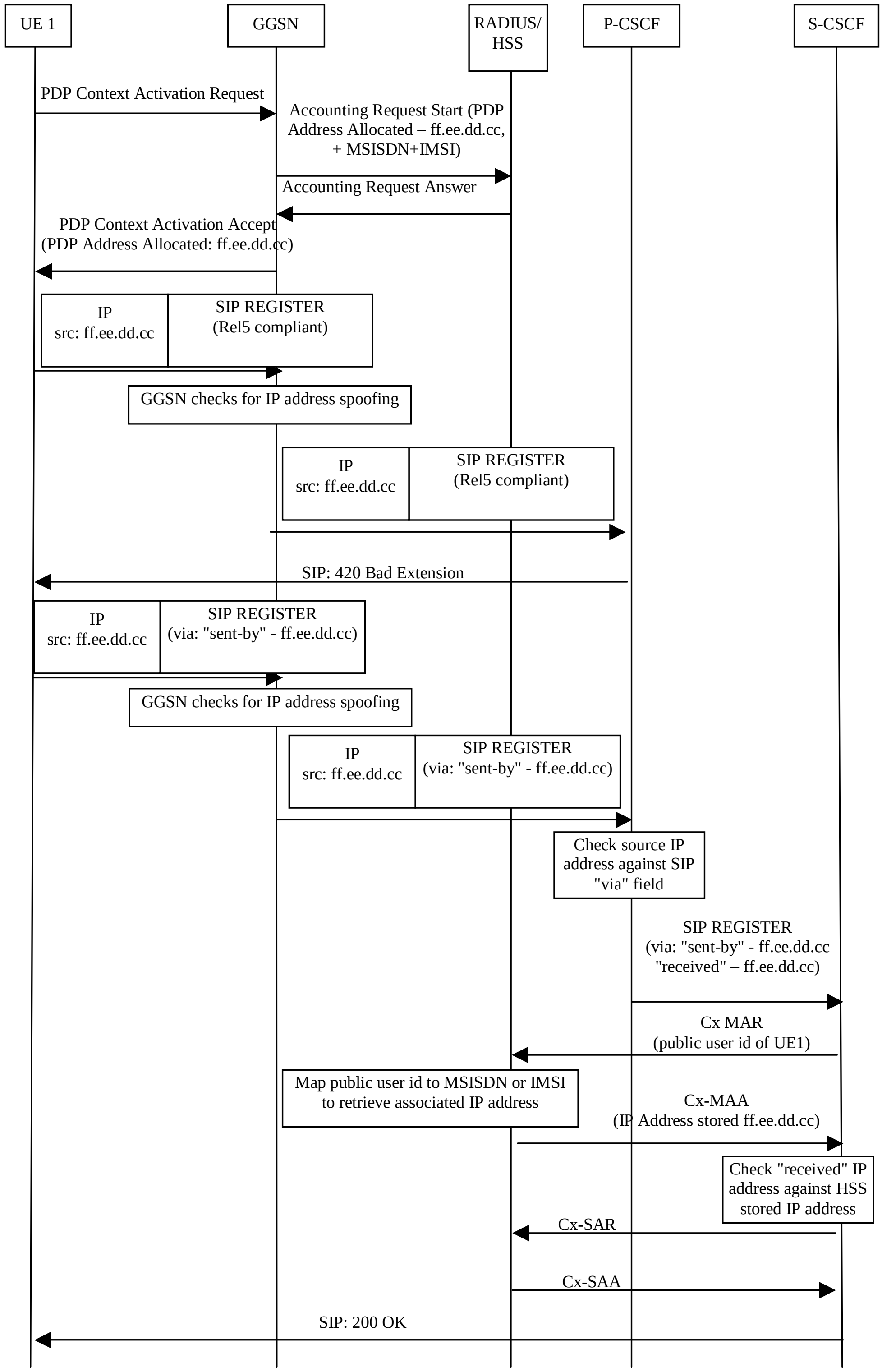


**Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant IMS and early IMS access security and network supports early IMS security only**

## 6.3 Security mechanism for HTTP services

The early IMS security solution may be re-used to protect HTTP services based on the secure IP address binding information stored in the HSS as an alternative to the mechanism specified in TS 33.141 [14]. To achieve this, the Sh interface shall be re-used by the Application Server (AS) to fetch secure IP address binding information from the HSS.

This approach requires the HTTP services to use the same APN as the early IMS service, and that all active PDP contexts, for a single UE, associated with that APN use the same IP address (or the prefix in the case of IPv6 stateless autoconfiguration) at any given time. This approach also requires the GGSN to be in the home network. The mechanism assumes that the GGSN does not allow a UE to successfully transmit an IP packet with a source IP address (or prefix) that is different to the one assigned during PDP context activation.

Since the security of this approach relies on the security of the PS bearer, a dependency is created between the HTTP service and the PS bearer, which does not exist with the mechanism specified in TS 33.141 [14]. This means that the solution described in this section does not provide as high a degree of access network independency as the solution in TS 33.141 [14]. In particular, the solution does not currently support scenarios where HTTP services are offered over WLAN.

The following steps describe the procedure:

1) UE sends the HTTP GET request to the AS. The "X-3GPP-Intended-Identity" header, as defined in TS 24.109 [17], shall be used by the UE to indicate the user identity. The user is identified by the IMPU that is derived from the IMSI of the subscription according to the rules in TS 23.003 [8].

2) AS decides to authenticate the UE based on the secure IP address binding information from the HSS. This decision might be based on the fact that GBA is not available. The AS checks whether secure IP address binding information is available at the AS; if yes, it proceeds with step 7, if not then it proceeds with step 3.

3) AS queries HSS using User-Data-Request (UDR) over the Sh interface, and the IMPU is used for User-Identity.

4) HSS responses with User-Data-Answer (UDA) including the secure binding information. If a securely bound IP address is not available in the HSS, then any incoming HTTP requests at the AS shall be rejected.

5) AS stores the secure binding information.

6) AS uses the subscriber/notify feature on the Sh interface to ensure that it is informed about any changes in the secure IP address binding information in the HSS. If the AS is notified by the HSS about such a change it updates the secure IP address binding information stored in the AS accordingly.

7) The AS shall check that the IP address (or prefix) from the UE in HTTP requests matches the IP address (or prefix) provided by the HSS, otherwise the HTTP request shall be rejected.

The mechanism does not preclude that the HTTP service may run inside a server-authenticated TLS tunnel established between the UE and the AS. However, support of TLS in the UE and in the AS is not mandated in this document.

The UDR and UDA commands, when implemented to support Early IMS Security, follow the description in clause 6.1.1 of TS 29.328 [15], with the following exceptions:

- The User Identity in the UDR command shall be the IMS Public User Identity of the user for whom the data is required.

- In the UDR commands, the Data Reference AVP described in clause 7.6 of TS 29.328[15] shall contain "IP address secure binding information", see Table 4.

The necessary UDR contents, when Early IMS Security is employed, are shown in Table 3.

**Table 3: UDR content for Early IMS Security**

| Information element name | Mapping to Diameter AVP | Cat. | Description |
|---|---|---|---|
| User Identity (See 7.1) | User-Identity | M | IMS Public User Identity of the user for whom the data is required.<br>See section 7.1 for the content of this AVP. |
| Requested data (See 7.3) | Data-Reference | M | This information element indicates the reference to the requested information. The set of valid reference values are defined in section 6.3 of 3GPP TS 29.329 [16].<br><br>When Early IMS Security data is required, the Data Reference Tag value shall be xx. |
| Application Server Identity (See 7.9) | Origin-Host | M | IE that identifies the AS originator of the request and that is used to check the AS permission list. |

NOTE 1: The section references in Table 3 refer to sections in 3GPP TS 29.328 [15], except where otherwise indicated.

Data Ref : xx is reserved in Section 6.3.4 of 3GPP TS 29.329 [16] for Early IMS security. The usage of Data Reference Tag xx is as shown in Table 4.

**Table 4: Data accessible via Sh interface for Early IMS Security (Data Ref: xx)**

| Data Ref. | XML tag | Defined in | Access key | Operations |
|---|---|---|---|---|
| 0 | RepositoryData | 7.6.1 | IMS Public User Identity + Data-Reference + Service-Indication | Sh-Pull, Sh-Update, Sh-Subs-Notif |
| 10 | IMSPublicIdentity | 7.6.2 | IMS Public User Identity or MSISDN + Data-Reference + Identity-Set | Sh-Pull |
| 11 | IMSUserState | 7.6.3 | IMS Public User Identity + Data-Reference | Sh-Pull, Sh-Subs-Notif |
| 12 | S-CSCFName | 7.6.4 | | Sh-Pull, Sh-Subs-Notif |
| 13 | InitialFilterCriteria | 7.6.5 | IMS Public User Identity + Data-Reference + Server-Name | Sh-Pull, Sh-Subs-Notif |
| 14 | LocationInformation | 7.6.6 | MSISDN + Data-Reference+ Requested-Domain | Sh-Pull |
| 15 | UserState | 7.6.7 | | |
| 16 | Charging information | 7.6.8 | IMS Public User Identity or MSISDN + Data-Reference | Sh-Pull |
| 17 | MSISDN | 7.6.9 | | Sh-Pull |
| xx | IP address secure binding information (note that this data is not transported in XML) | | IMS Public User Identity + Data-Reference | Sh-Pull, Sh-Subs-Notif |

NOTE 2: The section references in Table 4 refer to sections in 3GPP TS 29.328 [15].

When the AS uses the User-Data-Request (UDR) message and the Data-Reference with Data Ref:xx for the Early IMS Security data, the message format is described in clause 6.1.1 of TS 29.329 [16]. The User-Data-Answer (UDA) message as described in table 6.1.1.2, section 6.1.1 of 3GPP TS 29.328 [15] is modified as shown in Table 5.

**Table 5: UDA message content for Early IMS Security applied to Ut interface**

| Information element name | Mapping to Diameter AVP | Cat. | Description |
|---|---|---|---|
| Result<br>(See 7.5) | Result-Code / Experimental_ Result | M | Result of the request.<br><br>Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.<br><br>Experimental-Result AVP shall be used for Sh errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. |
| Data<br>(See 7.6) | User-Data | C | Requested data. This element shall be present if the requested data exists in the HSS and the AS has permissions to read it.<br><br>This element shall not be present if the Data Reference tag value in the request message is xx. |
| User IPv4 Address | Framed-IP-Address | C | If the Data Reference tag value in the request is xx and the IP Address of the User is an IPv4 address, this AVP shall be included.<br>For a description of the AVP see [11]. |
| User IPv6 Prefix | Framed-IPv6-Prefix | C | If the Data Reference tag value in the request is xx and the IP Address of the User is an IPv6 address, this AVP shall be included.<br>For a description of the AVP see [11]. |
| Framed Interface Id | Framed-Interface-Id | C | If the Data Reference tag value in the request is xx and the IP Address of the User is an IPv6 address and the Framed-IPv6-Prefix AVP alone is not unique for the user this AVP shall be included.<br>For a description of the AVP see [11]. |

NOTE 3: The references in Table 5 refer to section and document references in 3GPP TS 29.328 [15].

The corresponding ABNF in section 6.1.2 of 3GPP TS 29.329 [16] is replaced by that below.

```
< User-Data-Answer > ::=    < Diameter Header: 306, PXY, 16777217 >
                              < Session-Id >
                              { Vendor-Specific-Application-Id }
                              [ Result-Code ]
                              [ Experimental-Result ]
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              *[ Supported-Features ]
                              [ User-Data ]
                              [ Framed-IP-Address ]
                              [ Framed-IPv6-Prefix ]
                              [ Framed-Interface-Id ]
                              *[ AVP ]
                              *[ Failed-AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

Sh interface is an intra-operator interface, so the AS that uses the security mechanism described in this section should be in the home network.

The Subscribe-Notifications-Request (SNR) and Subscribe-Notifications-Answer (SNA) commands, when implemented to support Early IMS Security, follow the description in clause 6.1.3 of TS 29.328 [15], with the following exceptions:

- In the SNR commands, the Data Reference AVP described in clause 7.6 of TS 29.328[15] shall contain "IP address secure binding information", see Table 4.

The Push-Notification-Request (PNR) and Push-Notification-Answer (PNA) commands, when implemented to support Early IMS Security, follow the description in clause 6.1.4 of TS 29.328 [15], with the following exceptions:

- when the PNR command is sent to update the IP address of the subscriber, the contents of the command shown in Table 6 shall replace those described in Table 6.1.4.1 of 3GPP TS 29.328 [15].

**Table 6: PNR message content for Early IMS Security applied to Ut interface**

| Information element name | Mapping to Diameter AVP | Cat. | Description |
|---|---|---|---|
| User Identity (See 7.1) | User-Identity | M | IMS Public User Identity or Public Service Identity for which data has changed.<br>See section 7.1 for the content of this AVP. |
| User IPv4 Address | Framed-IP-Address | C | If the Sh-Notify is being sent to update the IP address of the subscriber for Early IMS Security on the Ut interface and the IP Address of the User is an IPv4 address, then this AVP shall be included. If the Sh-Notify is being sent to delete the IPv4 address of the subscriber for Early IMS Security on the Ut interface, then this AVP shall contain no contents.<br>For a description of the AVP see [11]. |
| User IPv6 Prefix | Framed-IPv6-Prefix | C | If the Sh-Notify is being sent to update the IP address of the subscriber for Early IMS Security on the Ut interface and the IP Address of the User is an IPv6 address, then this AVP shall be included If the Sh-Notify is being sent to delete the IPv6 address of the subscriber for Early IMS Security on the Ut interface, then this AVP shall contain no contents.<br>For a description of the AVP see [11]. |
| Framed Interface Id | Framed-Interface-Id | C | If the Sh-Notify is being sent to update the IP address of the subscriber for Early IMS Security on the Ut interface and the IP Address of the User is an IPv6 address and the Framed-IPv6-Prefix AVP alone is not unique for the user, then this AVP shall be included. If the Sh-Notify is being sent to delete the IPv6 address, then this AVP shall contain no contents.<br>For a description of the AVP see [11]. |

NOTE 4: The references in Table 6 refer to section and document references in 3GPP TS 29.328 [15].

The corresponding ABNF in clause 6.1.7 of 3GPP TS 29.329 [16] is replaced by that below.

```
< Push-Notification-Request > ::=   < Diameter Header:  309, REQ, PXY, 16777217 >
                                  < Session-Id >
                                  { Vendor-Specific-Application-Id }
                                  { Auth-Session-State }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  { Destination-Host }
                                  { Destination-Realm }
                                  { User-Identity }
                                  [ Framed-IP-Address ]
                                  [ Framed-IPv6-Prefix ]
                                  [ Framed-Interface-Id ]
                                  *[ AVP ]
                                  *[ Failed-AVP ]
                                  *[ Proxy-Info ]
                                  *[ Route-Record ]
```

# 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 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** | **Cat** | **Subject/Comment** | **Old** | **New** | **WI** |
| 2004-12 | SP_26 | SP-040866 | - | - | | Presentation to TSG SA for Approval (not approved by SA#26) | - | 1.0.0 | |
| 2005-03 | SP-27 | SP-050136 | - | - | | Presentation to TSG SA for Approval | | 2.0.0 | |
| 2005-03 | - | - | - | - | | Creation of Version 6.0.0 after TSG SA Approval | 1.0.0 | 6.0.0 | |
| 2005-04 | - | - | - | - | | Version 6.0.0 was created by MCC from the worng draft version of the TR. New version 6.0.1 created by MCC from version 2.0.0 (SP-050136) | 2.0.0 | 6.0.1 | |
| 2005-06 | SP-28 | SP-050267 | 0001 | - | F | Correction of use of 401 Unauthorized and 399 Warning headers | 6.0.1 | 6.1.0 | SEC-IMS |
| 2005-09 | SP-29 | SP-050617 | 0002 | 1 | F | Checking for USIM or ISIM before starting a fully compliant IMS registration | 6.1.0 | 6.2.0 | SEC-IMS |
| 2005-09 | SP-29 | SP-050617 | 0003 | - | F | Remove THIG function description | 6.1.0 | 6.2.0 | SEC-IMS |
| 2005-09 | SP-29 | SP-050617 | 0004 | - | F | Correction of figure 1 | 6.1.0 | 6.2.0 | SEC-IMS |
| 2005-09 | SP-29 | SP-050617 | 0005 | - | F | Correction of handling of IP addresses by the S-CSCF at de-registration | 6.1.0 | 6.2.0 | SEC-IMS |
| 2005-09 | SP-29 | SP-050617 | 0006 | - | F | Clarify the use of IMSI-derved IMPU in registration procedures | 6.1.0 | 6.2.0 | SEC-IMS |
| 2005-09 | SP-29 | SP-050617 | 0008 | - | F | S-CSCF reselection | 6.1.0 | 6.2.0 | SEC-IMS |
| 2005-09 | SP-29 | SP-050617 | 0009 | - | B | Ut interface protection | 6.1.0 | 6.2.0 | SEC-IMS |
| 2005-12 | SP-30 | SP-050769 | 0010 | - | F | Correction of CR implementation | 6.2.0 | 6.3.0 | SEC-IMS |
| 2005-12 | SP-30 | SP-050769 | 0011 | - | F | Use of IMPU in HTTP header for HTTP security mechanism | 6.2.0 | 6.3.0 | SEC-IMS |
| 2005-12 | SP-30 | SP-050769 | 0012 | - | F | Correction of Sh Secure IP Address Binding Information Notification Inconsistency | 6.2.0 | 6.3.0 | SEC-IMS |
| 2006-03 | SP-31 | SP-060055 | 0013 | - | F | Missing User-Identity AVP in PNR | 6.3.0 | 6.4.0 | SEC-IMS |
| 2006-09 | SP-33 | SP-060494 | 0014 | - | F | Correction of statement on use of temporary public user identities | 6.4.0 | 6.5.0 | SEC-IMS |
| 2006-09 | SP-33 | SP-060494 | 0015 | - | F | Correction of text on check of IP addresses | 6.4.0 | 6.5.0 | SEC-IMS |
| 2006-09 | SP-33 | SP-060646 | 0016 | 1 | F | Proposed changes to the Interworking cases section | 6.4.0 | 6.5.0 | SEC-IMS |
| 2006-12 | SP-34 | SP-060802 | 0017 | - | F | Correction of a reference | 6.5.0 | 6.6.0 | SEC-IMS |
| 2006-12 | SP-34 | SP-060802 | 0018 | 1 | F | Early-IMS impersonation threat | 6.5.0 | 6.6.0 | SEC-IMS |
| 2006-12 | SP-34 | SP-060802 | 0019 | - | F | Correction of text on check of IP addresses | 6.5.0 | 6.6.0 | SEC-IMS |

# History

| Document history | | |
|---|---|---|
| V6.0.0 | March 2005 | Publication (Withdrawn) |
| V6.0.1 | April 2005 | Publication |
| V6.1.0 | June 2005 | Publication |
| V6.2.0 | September 2005 | Publication |
| V6.3.0 | December 2005 | Publication |
| V6.4.0 | March 2006 | Publication |
| V6.5.0 | September 2006 | Publication |
| V6.6.0 | December 2006 | Publication |