3GPP TSG SA WG3 Security — SA3#35 S3-040779

St. Paul’s Bay, Malta, 5 – 8 October, 2004

Source:	**Siemens**
Title:	**Early-start IMS identification**
Document for:	**Discussion and decision**
Agenda Item:	**IMS**

1 Introduction

For the 3GPP IMS, SA3 is defining the security for Early-IMS. The motivation for this is that “early” implementations of the IMS services will exist that are not fully compliant with 3GPP IMS as defined for 3GPP Release 5. IMS services will be deployed before products are available which fully support the 3GPP IMS security features defined in TS 33.203 [2].

The approach is intended to provide an interim security solution before full IMS Release 5 security support is available. However, at the time when IMS Release 5 compliant systems begin to be deployed, this will lead to a situation where both early-IMS systems and Release 5 systems request IMS services, and register to the same IMS network.

This contribution discusses issues of this co-existence of the early-start IMS security, and IMS security as specified in TS 33.203 for Release 5, and proposes how to handle the relevant inter-working cases. The contribution therefore provides a proposed solution for section 7.2.4 of S3-040685 on “Identification of terminals supporting the interim solution”. In the annex, a text is proposed for this section.

2 Discussion

The motivation for this contribution is the expectation that, with early-start IMS terminals deployed and beginning deployment of IMS Release 5 security, both methods need to co-exist in practice for a certain while.

This creates the necessity for proper inter-working between the different authentication methods for terminals accessing the IMS. For example, a requirement already stated in the current early-IMS specification [S3-040685] is that the IMS core shall be able to differentiate between a subscription using interim security mechanisms and a subscription using the full 3GPP Release 5 solution. Section 7.2.4 of S3-040685 on “Identification of terminals supporting the interim solution” requires some indication (not necessarily given by the terminal) for Early-IMS support.

2.1 Overview of interworking issues

One issue that directly arises depends on the role of the P-CSCF for accepting or rejecting IMS signaling messages. TS33.203 states in section 7.1:

“The P-CSCF is allowed to receive only REGISTER messages and error messages on unprotected ports. All other messages not arriving on a protected port shall be either discarded or rejected by the P-CSCF”

With early-IMS clients accessing an IMS network that already supports IMS Rel5, this conflicts with a Rel5 P-CSCF policy of dropping all but REGISTER and error messages. The early-IMS proposal expects the P-CSCF to forward all messages sent by early-IMS terminals to the S-CSCF without checking the validity of such messages itself (the IP address check for early-IMS clients happens in the S-CSCF), see section 7.2.3.1 of [S3-040685].

The proposed approach is therefore to logically distinguish a Rel5 P-CSCF and an Early-IMS P-CSCF. The resulting requirement to the Early-IMS in this case is to allow entities implementing both a Rel5 P-CSCF and an Early-IMS P-CSCF to choose the correct function for each subscriber.

For inter-working in a scenario with support for both Early-IMS and IMS Rel5 access security, the following cases are relevant:

1. UE and IMS network supporting Early-IMS only
2. UE supporting Early-IMS only, IMS network supporting both
3. UE supporting both, IMS network supporting Early-IMS only
4. UE and IMS network supporting both

In case 1, both entities involved only support Early-IMS; no inter-working considerations are required.

Case 2 requires the P-CSCF/S-CSCF to discover that the UE only supports Early-IMS authentication, whereas in case 3 the UE must be able to detect that the IMS network only supports Early-IMS. These cases need to be addressed by the Early-IMS specification.

In case 4, the UE and P-CSCF shall use access security as specified for IMS Rel5. In this case, downgrading attacks may become possible. These are, however, hard to counter in the given inter-working scenario as long as Early-IMS is supported, unless a certain subscriber is only allowed to use Release 5 security, and the HSS can inform the S-CSCF accordingly (see next paragraph). The overall security level achieved is at least the security level offered by Early-IMS.

Information may additionally be made available to the IMS core entities from the subscriber profile stored in the HSS (as policy information about the allowed methods for secure IMS access for a specific subscriber). This case is not considered in this contribution. A mechanism providing distribution of such information may increase the complexity and impact of the Early-IMS solution. If it is, however, seen as a requirement, the fact should be considered that storing information about allowed authentication methods in the HSS cannot reflect the capabilities of the terminal actually used by the subscriber.

2.2 Discussion of possible solutions

The above cases 2 and 3 are discussed in the following (beginning with case 2) with focusing on the signaling between UE and IMS network.

In [S3-040685], section 7.2.4, it is required that some indication shall be given about the UE supporting early-IMS security. Such indication could be provided explicitly by the terminal (e.g. by a dedicated field in the Register header), or could be given implicitly (e.g. by missing IMS Rel5 headers like Security-Client).

For the 3GPP Release 5 initial register message, the following headers related to Rel5 authentication are expected by the IMS core (as specified in TS24.228, section 6.2):

```
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce="", uri="sip:registrar.home1.net", response=""
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi=12345678; port1=1357
Require: sec-agree
Proxy-Require: sec-agree
```

Without changes to the Release 5 client specification, an IMS client supporting the early-IMS security would be required to send the above headers (without implementing the underlying security mechanisms). However, since early-start clients do not run the security mechanism agreement according to TS33.203, it is proposed that an early-start (-only) client shall not send the Security-Client, Require and Proxy-Require headers.

The discussion of the Authorization header is more difficult, since in IMS Release 5 it indicates not only Digest-AKA support, but provides the IMS private identity (IMPI) to the IMS network. This information is required in the initial Register message of IMS Rel5 by the home network (I-CSCF, S-CSCF) for S-CSCF selection.

Considering the fact that in early-IMS implementations from a security perspective there is no need to send an Authorization header in the initial Register message (as no http digest is used), an option is to drop this header for early-IMS. The IMS network (P-CSCF) would recognize Rel5 registrations by the presence of the Rel5 security headers, and would treat all other registrations as Early-IMS.

Issues to be considered for this solution are:

- The missing IMPI in the initial Register. It is expected that this could be easily solved by requiring the HSS to resolve the missing IMPI from the IMPU that is always present in case of Early-IMS users.
  The I-CSCF can only provide the IMPU as user identity to the HSS during S-CSCF selection following the receipt of a Register message (the Cx interface of Rel5 mandates both the public user identity and the user-name parameter (carrying the IMPI) for Cx-MAR requests). In case of an empty IMPI field in the Cx-MAR, however, the HSS is expected to be able to resolve the received IMPU to the correct IMPI of the subscription.

- It would not be possible for the P-CSCF to distinguish between early-IMS clients and other (than Rel5 or Early-IMS) clients that e.g. use standard Internet SIP, since no explicit indication is given by Early-IMS clients. This, however, is not considered problematic, as on the one hand Early-IMS is only specified for GPRS access and does not consider inter-working with Internet-SIP clients, and on the other hand clients without a proper subscription would not be able to pass the S-CSCF IP address check anyway (i.e., this case can already be handled by standard Early-IMS means).

Another alternative for indicating early-IMS support to the IMS network would be some dedicated indication of Early-IMS in the initial Register message. However, the Security-Client header is not considered a good option, since a verification of this header in the second Register would not be possible with Early-IMS, and changes to RFC3329 (Security mechanism agreement) would possibly be required for such a solution.

Furthermore, it would be possible to use the Digest Authorization header. This header is already used in IMS Rel5 in the initial Register and in the PoC specifications. It could be used to additionally indicate Early-IMS support from the UE to the IMS network. However, in the case of Early-IMS this may conflict with the http digest specification as profiled by SIP (RFC3261), as some additional field would be necessary to carry the required information.

Summarizing the above discussions, it is proposed to use the first option for Early-IMS (implicit Early-IMS indication by missing Authorization, Security-Client, Require and Proxy-Require headers). The main reason for this proposal is the simplicity of the solution (e.g., no new requirements to the UE implementation by Early-IMS), since no clear need for an explicit indication for Early-IMS can be seen.

It is furthermore proposed to resolve the missing IMPI by requiring the HSS to derive this information from the IMPU.

The above proposal addresses case 2 of section 1. In addition, the following procedure is expected to cover the inter-working case 3:

- If the terminal already has knowledge about the IMS network capabilities (which could for example be preconfigured in the terminal), the appropriate authentication method shall be chosen (IMS Rel5, if the network supports this, Early-IMS if not) in advance. However, no need for standardization work is seen here.

- If not, the terminal starts with sending the standard IMS Rel5 Register message (including all security-related headers). If the network only supports Early-IMS, the P-CSCF must answer with a 420 “Bad Extension” failure, since it does not recognize the Rel5 Security headers and the Require/Proxy-Require header is present. This header cannot be ignored if it contains a tag.
  The terminal shall, after receiving the error message, fall back to Early-IMS registration for the access security part, i.e., shall send a new Register message without the IMS Rel5 security headers discussed above. The network shall respond with a 200OK message according to the registration message flow already given in [S3-040685].

In addition, the cases where UE and IMS network cannot interwork need to be specified correctly:

- UE supports Early-IMS only, IMS network supports Rel5 only
  As response to the initial Register, the IMS network will answer with an appropriate error message (403

Forbidden with “Authentication Failed” reason phrase). In this case the terminal must not retry registration with the same P-CSCF, as the IMS network does not support Early-IMS operation.
Considering this case, the Early-IMS should not use the same error messages as Rel5 compliant systems. Otherwise, it could happen that an Early-IMS terminal receives an error message from a Rel5 IMS network, but interprets it as an authentication mismatch during Early-IMS registration.
To handle this case, it is proposed to use a 403 Forbidden with a new reason phrase exclusively used by Early-IMS systems, e.g. “Early-IMS auth failed” instead of “Authentication Failed” that is used by Rel5 compliant systems.

- UE supports Rel5 only, IMS network supports Early-IMS only
  This case is already covered by the above considerations. The P-CSCF answers with a 420 “Bad Extension” failure, since it does not recognize the Rel5 Security headers and the Require/Proxy-Require header is present.

3 Conclusion

This contribution discusses the interworking cases to be solved for the Early-IMS security when deployed in parallel with the full IMS Rel5 security. The focus is on the required means for indicating and identifying which security mechanism is supported by the UE or the network.

As the result of this discussion, it is proposed to not include any of the IMS Rel5 security headers (Authorization, Security-Client) when an Early-IMS UE accesses an IMS network. A network that supports both IMS Rel5 and Early-IMS access security will recognize an Early-IMS client by the missing security headers.

The proposal is expected to allow interworking of Early-IMS implementations with IMS Rel5 implementation without impacting the already specified Rel5 interfaces. It, however, leads to the fact that the IMS private identity is not sent with the initial Register message by the UE. To handle this case, it is proposed to resolve the missing private identity by requiring the HSS to derive this information from the IMS public identity.

In addition, procedures are presented for interworking, especially for the case of a UE without knowledge about the IMS network capabilities it is trying to access) supporting both IMS Rel5 and Early-IMS.

SA3 is kindly requested to consider and include the above mechanisms in the SA3 Early-IMS TR. The annex below provides appropriate text that is proposed to be taken as input to section 7.2.4 of the current Early-IMS TR (S3-040685).

In addition, the proposals made in this contribution require minor changes to the message flows currently specified in the Early-IMS TR (remove the IMS private identity from the registration flow; introduce a dedicated Early-IMS reason phrase for 403 Forbidden responses). One additional flow is already provided in this contribution. In case the contribution is approved, Siemens is willing to update the other message flows as well.

4 Annex

This annex provides text that is proposed to be added to section 7.2.4 of the current Early-IMS TR (S3-040685).

7.2.4 Identification of terminals supporting the interim solution

At some stage, it is expected that both fully 3GPP compliant terminals (denoted Rel5 compliant in the following) as specified by TS 33.203 for 3GPP Release 5 and terminals implementing the Early-IMS security solution specified by this document will access the same IMS. In addition, IMS networks will support only Rel5 compliant terminals, Early-IMS terminals, or both.
Both terminals and IMS network must therefore be able to properly handle the different possible interworking cases.

Since Early-IMS security does not require the security-headers specified for Rel5 compliant terminals, these headers shall not be used for Early-IMS. The Register message sent by an Early-IMS terminal to the IMS network shall not contain the security headers specified by TS33.203 (Authorization and Security-Client).

As a result, Early-IMS terminals 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 terminals shall use Early-IMS security for authenticating the terminal during registrations that do not contain the security headers specified by TS 33.203 (Authorization and Security-Client).

Without sending an Authorization Header in the initial Register message, Early-IMS terminals only provide the IMS public identity, but not the IMS private identity to the network (this is only present in the Authorization header for Rel5 compliant terminals). The IMS private identity shall therefore be derived from the subscriber's public identity in the HSS.

During the process of user registration, the Cx interface carries both the private user identity and the public user identity in Cx-MAR requests (sent by I-CSCF and S-CSCF). For Early-IMS, only the public user identity shall be sent to the HSS within these requests, and the private user identity shall be empty. This avoids changes to the Release 5 message format to the Cx interface.

For interworking between Early-IMS and Rel5 compliant implementations during IMS registration, the following cases shall be supported:

1. Both terminal and IMS network support Early-IMS only

   IMS registration shall take place as described by this specification.

2. Terminal supports Early-IMS only, IMS network supports both Early-IMS and Rel5 compliant access security according to TS33.203

   The IMS network shall use Early-IMS security according to this specification for authenticating the terminal for all registrations from terminals that do not provide the Rel5 compliant security headers.

3. Terminal supports both, IMS network supports Early-IMS only

   If the terminal already has knowledge about the IMS network capabilities (which could for example be preconfigured in the terminal), the appropriate authentication method shall be chosen. Rel5 compliant security shall be used, if the network supports this, otherwise Early-IMS security.

   If the terminal does not have such knowledge it shall start with the Rel5 compliant 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 terminal in the initial Register message (this header cannot be ignored by the P-CSCF).

The terminal shall, after receiving the error message, send an Early-IMS registration, i.e., shall send a new Register message without the Rel5 compliant security headers. The network shall respond with a 200 OK message according to the registration message flow as specified in section [tbd.].

4. Terminal and IMS network support both

   The terminal shall start with the Rel5 compliant IMS registration procedure. The network, with receiving the initial Register message, receives indication that the terminal is Rel5 compliant and shall continue as specified by TS 33.203.

5. Terminal supports Early-IMS only, IMS network supports Rel5 compliant access security only

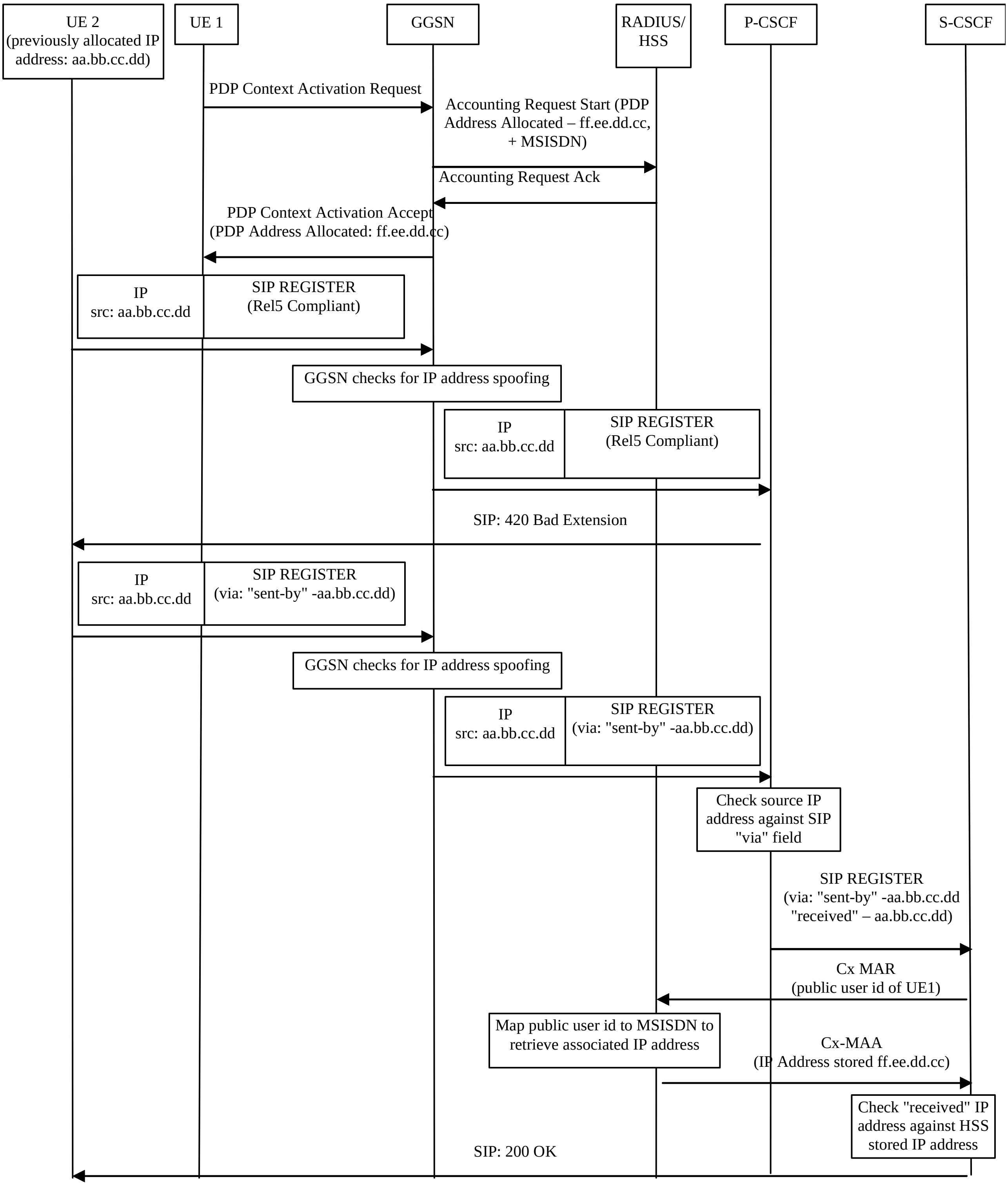
   The terminal sends a Register message to the IMS network that does not contain the necessary security headers required by Rel5 compliant IMS. In this case the IMS network will answer with an error message (403 Forbidden with “Authentication Failed” reason phrase) indicating to the early-IMS terminal that the authentication method is incorrect. After receiving the error message, the Early-IMS terminal shall stop the attempt to register with this network, since Early-IMS is not supported.

6. Terminal supports Rel5 compliant access security only, IMS network supports Early-IMS only

   The terminal shall start with the Rel5 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 terminal in the initial Register message (this header cannot be ignored by the P-CSCF). After receiving the error message, the terminal shall stop the attempt to register with this network, since the fully 3GPP compliant security according to TS33.203 is not supported.

7.2.5 Message flows

[the following figure is proposed to be added to section 7.2.5 of the current Early-IMS TR]



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)
Accounting Request Ack
PDP Context Activation Accept (PDP Address Allocated: ff.ee.dd.cc)
IP src: aa.bb.cc.dd
SIP REGISTER (Rel5 Compliant)
GGSN checks for IP address spoofing
IP src: aa.bb.cc.dd
SIP REGISTER (Rel5 Compliant)
SIP: 420 Bad Extension
IP src: aa.bb.cc.dd
SIP REGISTER (via: "sent-by" -aa.bb.cc.dd)
GGSN checks for IP address spoofing
IP src: aa.bb.cc.dd
SIP REGISTER (via: "sent-by" -aa.bb.cc.dd)
Check source IP address against SIP "via" field
SIP REGISTER (via: "sent-by" -aa.bb.cc.dd "received" – aa.bb.cc.dd)
Cx MAR (public user id of UE1)
Map public user id to MSISDN to retrieve associated IP address
Cx-MAA (IP Address stored ff.ee.dd.cc)
Check "received" IP address against HSS stored IP address
SIP: 200 OK

Figure 1: Message Sequence for Early-IMS in case a terminal supporting both Rel5 compliant and Early-IMS access security successfully registers with an Early-IMS only IMS network.