3GPP TSG SA WG3 Security#33 **S3-040265**
10 – 14 May, 2004
Beijing, China

Agenda Item: **6.1**

Source: **Vodafone**

Title: **Interim security solution for early IMS implementations**

Document for: **Discussion and Decision**

Abstract

As detailed in a recent LS from SA2 to SA3 [S2-041674] and in a companion contribution to this SA3 meeting [S3-040264], early IMS systems are not expected to offer the full set of 3GPP Release 5 and 6 features. This will hold for security features as well, creating the need for interim security solutions. These interim solutions need to meet certain security requirements. In [S2-041674], SA2 identifies a need for a standardized interim security solution and identifies the requirement for a minimized impact especially on the UE.

This contribution proposes an interim security solution to be standardized by SA3 that minimizes the impact on IMS terminals, and requires only a limited set of changes to the IMS core. The solution avoids key/password distribution issues during provisioning, and does not restrict the type of charging models that can be applied by the IMS operators.

1 Current situation

Currently, early IMS systems are not expected to provide the full set of 3GPP Release 5 security features. A motivation for this is given in a contribution to SA2#39 [S2-041399] as well as in a companion contribution to SA3#33 [S3-040264]. In section 3 of [S2-041399], a number of threat scenarios are given to further clarify the security requirements that apply to an interim security solution for the IMS. These threat scenarios are reproduced in section 2 of this document.

Based on the discussion at the SA2#39 meeting in April 2004, a liaison has been sent from SA2 to SA3 in [S2-041674], which states that SA2 sees a need for developing an interim IMS security solution and requests action from SA3.

In the following section, a proposal for a solution to the required interim IMS security is given.

2 Threat scenarios

To understand what controls are needed to address the security requirements, it is useful to describe some of the threat scenarios that we are trying to address. The threats include: Impersonation on IMS level using an IMS public user identity of an IMS user, IP address spoofing, and the two combined.

Threat scenario 1: Impersonation on IMS level using the public user identity of an innocent user

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

If the binding between the IP address on the bearer level, and the public and private user identities is not checked then the attacker will succeed, i.e. A pays for IP connectivity but IMS service is fraudulently charged to B. The fraud situation is made worse if IP flow based charging is used to ‘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.

Threat scenario 2: IP spoofing

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

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

Threat scenario 3: Combined threat scenario

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

If the bindings mentioned in scenarios (1) and (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.

There are of course many other threats, but which are outside the scope of this discussion paper.

3 Proposed interim IMS security solution

3.1 Solution overview

The proposed interim 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 SIM-based GPRS security context.

The GGSN, terminating each user's authenticated PDP context, provides the user's IP address / MSISDN pair to the HSS when a PDP context is activated towards the IMS system. The HSS has a binding between the MSISDN and the private user identity, and is therefore able to store the currently assigned IP address from the GGSN against the user's IMS private user identity. The GGSN informs the HSS when the PDP context is deactivated/modified so that the stored IP address can be updated in the HSS. When the S-CSCF receives a SIP registration request or any subsequent requests for a given IMS identity, it checks that the IP address in the SIP header (verified by the network) matches the IP address that was stored against that subscriber's private user identity in the HSS.

The mechanism assumes that the GGSN does not allow a mobile to successfully transmit an IP packet with a source IP address that is different to the one assigned during PDP context activation. In other words, the GGSN must prevent "source IP Spoofing". The mechanism also assumes that the P-CSCF checks that the source IP address in the SIP header is the same as the source IP address in the IP header received from the mobile (the assumption here, as well as for Release 5 compliant IMS systems, 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 section 2 above.

In this contribute we use the terms P-CSCF and S-CSCF is 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 Rel-5. If this solution is adopted then the requirements it imposes on the SIP/IP core should be specified without reference to specific x-CSCF. Note however that while the exact functionality split of the SIP/IP core may be left open, it is important that any changes to Cx interface towards the HSS is standardised for vendor interoperability problems.

3.2 Solution description

3.2.1 Update of mobile's IP address in HSS depending on PDP context state

During PDP context request towards the IMS, the GGSN shall send a RADIUS "ACCOUNTING-REQUEST START" message to a RADIUS server attached to the HSS[1,2]. The message shall include the UE's IP address and MSISDN. The format of the message shall be compliant with 3GPP TS 29.061 [29.061]. On receipt of the message, the HSS shall use the MSISDN to find the subscriber's IMS identity (derived from IMSI) and then store the IP address against the IMS identity.

GGSN shall not activate the PDP context if the accounting start message is not successfully handled by the HSS. In particular, it shall not be possible to have an active IMS PDP context if the corresponding IP address is not stored in the HSS.

In case of PDP context deletion, the GGSN sends an "ACCOUNTING-REQUEST STOP" message to the HSS after the idle timer in the GGSN expires. The HSS shall then start the 3GPP HSS-initiated de-registration procedure.

If the UE establishes a new PDP context and therefore gets a new IP address, the UE shall start the IMS initial registration procedure. Because the idle timer in the GGSN could be set with a large value, e.g. 1 hour, it is quite likely that the UE will send a PDP context creation request before the idle timer expires. Two cases are distinguished:

- If the PDP context creation request is processed by the same SGSN as the old PDP context, then the SGSN will assign the existing PDP context to the UE. Therefore the IP address of the UE is unchanged and the IMS registration is still valid.
- If the PDP context creation request is processed by a different SGSN compared to the old PDP context, e.g. in case of a routing area update, the SGSN will create a new PDP context for the UE. In this case the GGSN shall send an "ACCOUNTING-REQUEST START" to the HSS with the new IP address. Because this IP address is different to the IP address the UE registered with, the HSS shall start the 3GPP HSS-initiated de-registration procedure. Later, the idle timer for the old PDP context expires and the old PDP context will be deleted by the GGSN. The HSS will be informed about the event via the "ACCOUNTING-REQUEST STOP" message. The HSS checks the IP address indicated by the "ACCOUNTING-REQUEST STOP" message against the IP address stored in the HSS. If they are the same, a network-initiated de-registration procedure shall be started. In this case they are different, so the HSS shall then ignore the message.

3.2.2 Protection against IP address spoofing in GGSN

All GGSNs that offer connection to IMS shall implement measures to prevent source IP address spoofing. Specifically, a UE attached to the GGSN shall not be able to successfully transmit an IP packet with a source IP address that is different to the one assigned by the GGSN during PDP context activation. If IP address spoofing is detected the GGSN shall drop the packet and log the event in its security log against the subscriber information (IMSI/MSISDN).

3.2.3 Source IP address checking in the P-CSCF and S-CSCF

A UE shall not be able to spoof its assigned IP address and successfully receive service from the IMS. The following mechanisms are required to prevent IP address spoofing in the IMS domain.

---

1 An alternative approach would be to re-use the AAA architecture of I-WLAN i.e. the 3GPP AAA Proxy or Server and its capability to perform RADIUS to DIAMETER conversion such that the HSS will not specifically need to support RADIUS (existing DIAMETER functionality of HSS can be re-used).

2 It is assumed here that the RADIUS server for handling the accounting request to receive the IP address from the GGSN is different to the RADIUS server that the GGSN may use for access control and IP address assignment. Howeer, according to TS 23.060 there is no limitation on whether RADIUS servers for Accouting and Access control have to be separate or combined.

3.2.3.1 P-CSCF mechanisms

As mandated by section 18.2.1 of RFC 3261 the P-CSCF will check the IP address in the “sent-by” parameter of the top “Via” header field. Specifically, if the host portion of the "sent-by" parameter contains a domain name, or if it contains an IP address that differs from the packet source IP address, the server will add a "received" parameter to that Via header field value. This parameter contains the source IP address from which the packet was received. After this processing, the P-CSCF forwards the SIP message to the I-CSCF or S-CSCF.

3.2.3.2 S-CSCF mechanisms

S-CSCF shall use the IMS public user identity to retrieve the IP address stored during PDP context activation. For all requests, the S-CSCF first checks whether a “received” parameter exists in the top “via” header field. If a “received” parameter exists, S-CSCF shall compare the IP address recorded in the “received” parameter against the UE’s IP address stored during registration. If no “received” parameter exists in the top “via” header field, then S-CSCF shall compare IP address recorded in the “sent-by” parameter against the IP address stored during registration. In both cases, if the HSS retrieved IP address and the IP address recorded in the top “via” header do not match, the S-CSCF shall reject the registration with a 403 Forbidden response.

It should be noted that if the request sent is a REGISTER, then the S-CSCF shall always query the HSS to retrieve the IP address registered during PDP context activation. The IP address fetched during a SIP REGISTER shall be stored in the S-CSCF and used for checking subsequent non-REGISTER SIP requests. The S-CSCF shall implement procedures to recover the registration information (including IP address) from the HSS stored in case of a system failure.

Note that the S-CSCF should check the IP address for every SIP request, but it only needs to contact the HSS to fetch the IP address during a SIP Register. This is because any change in IP address at GPRS level will trigger the HSS to initiate a re-registration at the SIP level. Contacting HSS for every SIP message would place too high a load on the HSS.

3.2.4 Identification of terminals supporting the interim solution

At some stage, it is expected that both fully 3GPP compliant terminals and terminals implementing the interim security solution will access the same IMS. Therefore, some indication needs to be given that a terminal supports the interim solution rather than the full 3GPP solution. The exact format, and means to carry this information, is for further study.

3.2.5 Message flows

Figure 1 below describes the message flow for successful registration to the IMS that is specified by the interim security solution.

Note, that the “received” parameter is only sent from P-CSCF to S-CSCF under the conditions given in section 3.2.3.1.

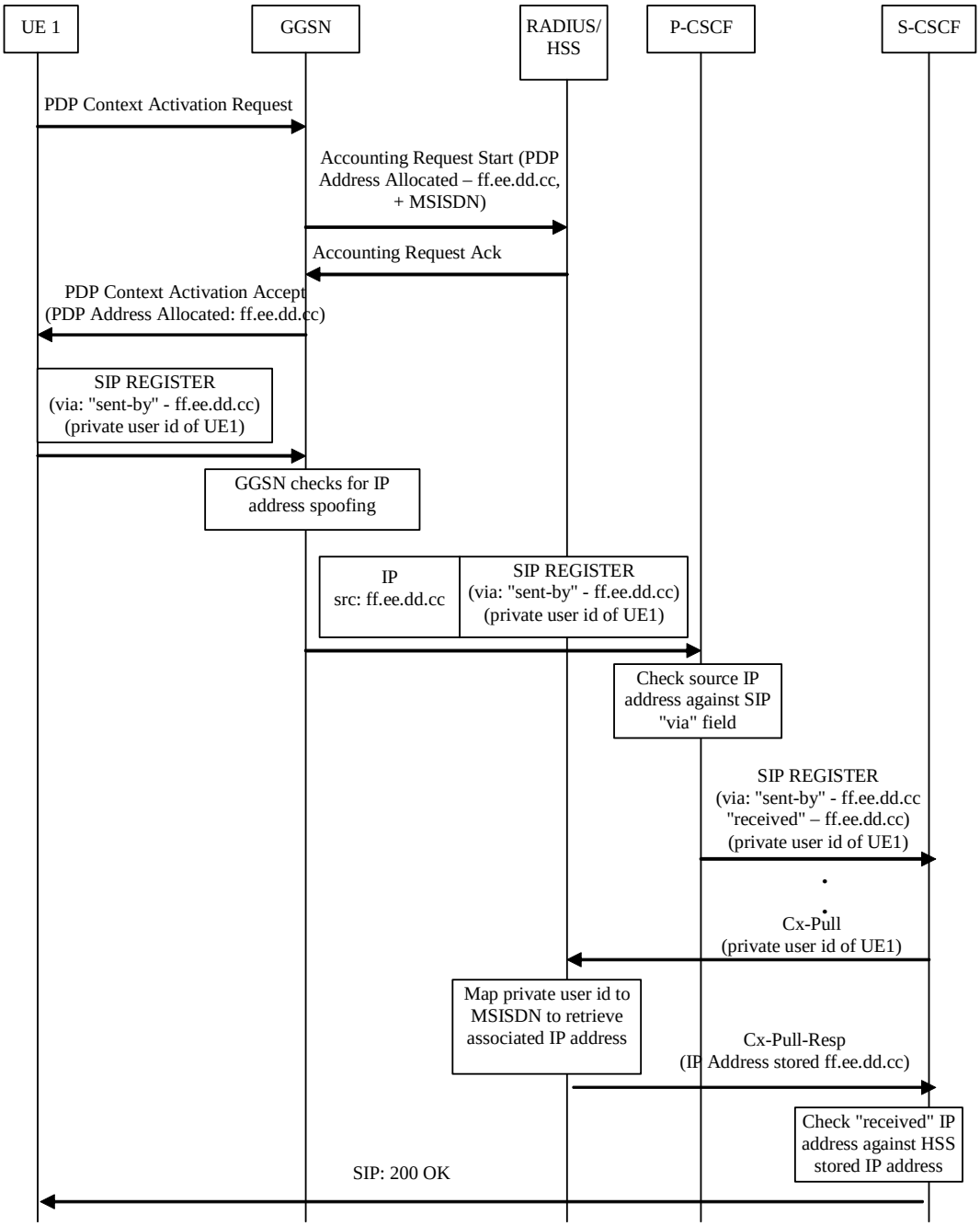

Figure 1: Possible Message Sequence for Interim Security Solution (successful registration)

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 section 3.2.3.1.

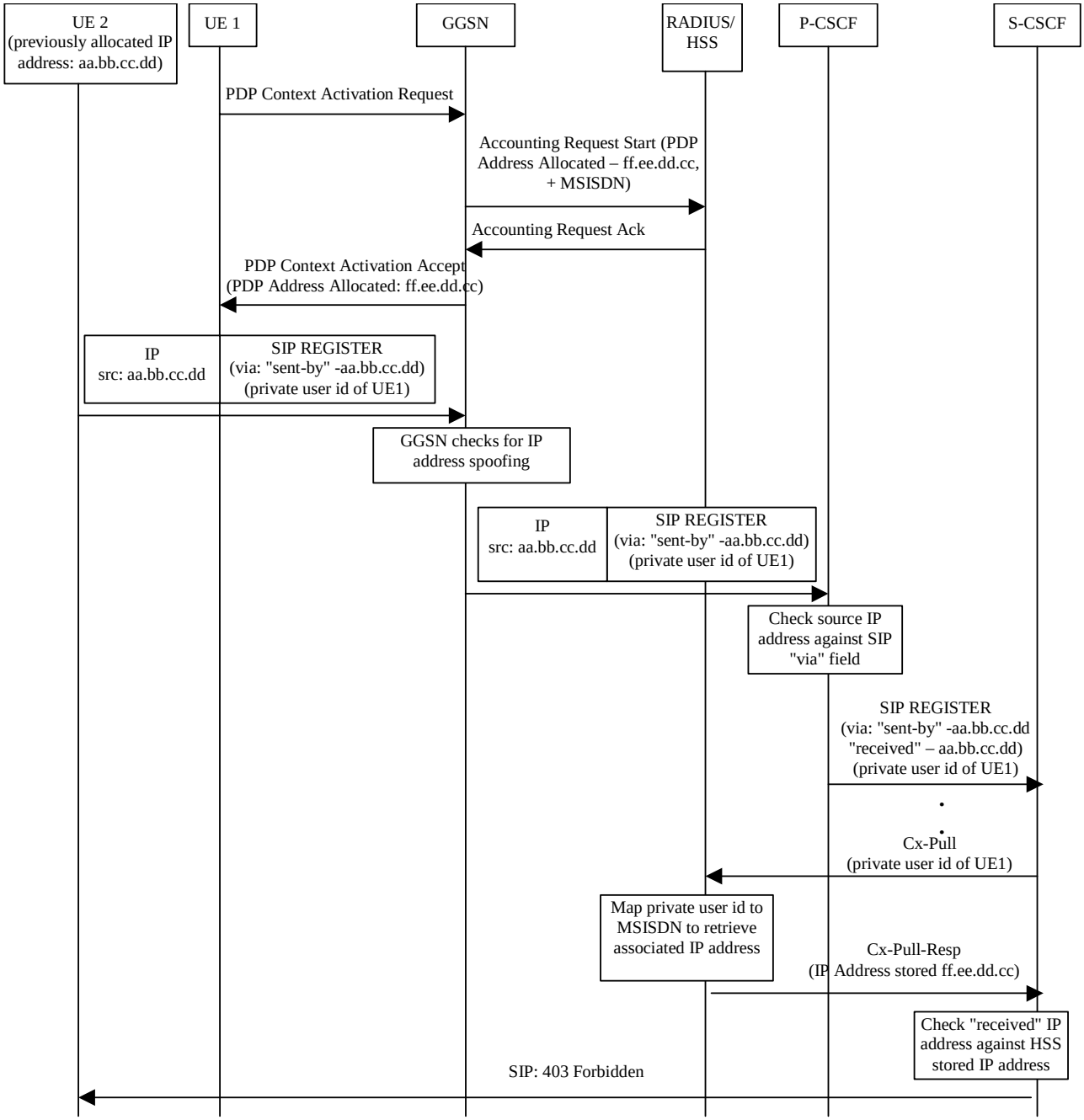

Figure 2: Possible Message Sequence for Interim Security Solution showing (unsuccessful) identity theft

4 Comparison with alternative approaches

An alternative approach is to use password-based authentication for early IMS implementations. For example, HTTP Digest could be used for authenticating the IMS subscriber. This method would require a subscriber-specific password to be provisioned on the IMS terminal. Compared with the approach proposed in section 2, password-based authentication has the following disadvantages:

- It imposes restrictions on the type of charging schemes that can be adopted. In particular, if a subscriber could find out his or her own password from an insecure implementation on the terminal, 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. If charging were purely usage based then there would be no incentive for the subscriber to do this (and no impact on operator revenue). The solution proposed in section 2 is flexible in allowing a range of different charging models including bundled or partly subscription based tariffs.

- It provides a weak form of subscriber authentication 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. This has implications on the reliability of charging, and on the level of assurance that can be given to the customer that their communications cannot be masqueraded. In the solution proposed in section 2, 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 terminal securely storing any long-term secret information (e.g. passwords).

- Provisioning is more complex since subscriber-specific information (i.e. passwords) must be installed in each mobile.

5 Conclusion and way forward

The interim IMS security solution proposed in section 2 of this contribution provides a common mechanism for authenticating IMS users based on the already deployed GPRS security infrastructure. The solution covers IMS signalling between the IMS user, and the S-CSCF in the home network. It has a limited impact on the current IMS core, and minimizes the impact on the user equipment. Current 2G-GPRS terminals and SIM cards are supported, as well as 3G terminals and USIM cards.

The proposed solution is intended for, and limited to, IMS access through GPRS. Secure access to http-based services, e.g. the security for the Ut reference point, was not addressed, as the focus of this contribution was the security of SIP messages in IMS. We would like to make only two remarks here:

- the use of passwords for http digest to secure the Ut reference point seems less critical, as it does not show the same potential for fraud and impact on charging models;

- it is possible to extend the approach presented here in a natural way to provide automated password distribution for http digest.

SA3 is kindly requested to consider the proposed solution given in section 3 of this contribution as the technical basis for the interim IMS security solution.

References

[S2-041399] 3GPP SA2 Tdoc S2-041399, "Discussion on interim security for IMS", SA2 meeting #39, Shenzhen, China, 19-23 April 2004.

[S2-041674] 3GPP SA2 Tdoc S2-041674, Liaison from SA2 to SA3: "LS on non-compliance to IMS security", SA2 meeting #39, Shenzhen, China, 19-23 April 2004.

[S3-040264] 3GPP SA3 Tdoc S3-040264, “Security for early IMS implementations”, SA3 meeting #33, Beijing, China, 10-14 May 2004.

[29.061] 3GPP TS 29.061, Interworking between Public Land Mobile Network (PLMN) supporting packet data services and Packet Data Networks (PDN).