3GPP TSG SA WG3 Security — S3#32 **S3-040153**
09 - 13 February 2004
Edinburgh, Scotland, UK

Title:	Sending IMSI across Gn/Gp interfaces and security implications
Reply to:	-
Source:	**SA3**
To:	**CN4**
Cc:	**-**

Contact Person:
Name: Krister Boman
Tel. Number: +46317474055
E-mail Address: krister.boman@ericsson.com

Attachments: S3-040082

1 Overall Description

In TDOC S3-040082 it has been analysed based on a discussion in CN4 if there are any security issues related to sending the IMSI across Gn/Gp interfaces. SA3 agrees with the conclusion given in TDOC S3-040082 and recommends CN4 to implement any solution of their choice that requires sending the IMSI across the Gn/Gp interfaces from a security point of view.

2 Actions

CN4 to consider the above conclusions in their future work.

Date of Next SA3 Meetings:

TSG SA WG3#33	11 – 14 May 2004	Beijing, China, Samsung
TSG SA WG3#34	06 – 09 July 2004	TBD, North American Friends'

3GPP TSG SA WG3 Security — S3#32 **S3-040082**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item: TBD

Source: Ericsson, Vodafone

Title: Sending IMSI over Gn/Gp

Document for: Discussion/Decision

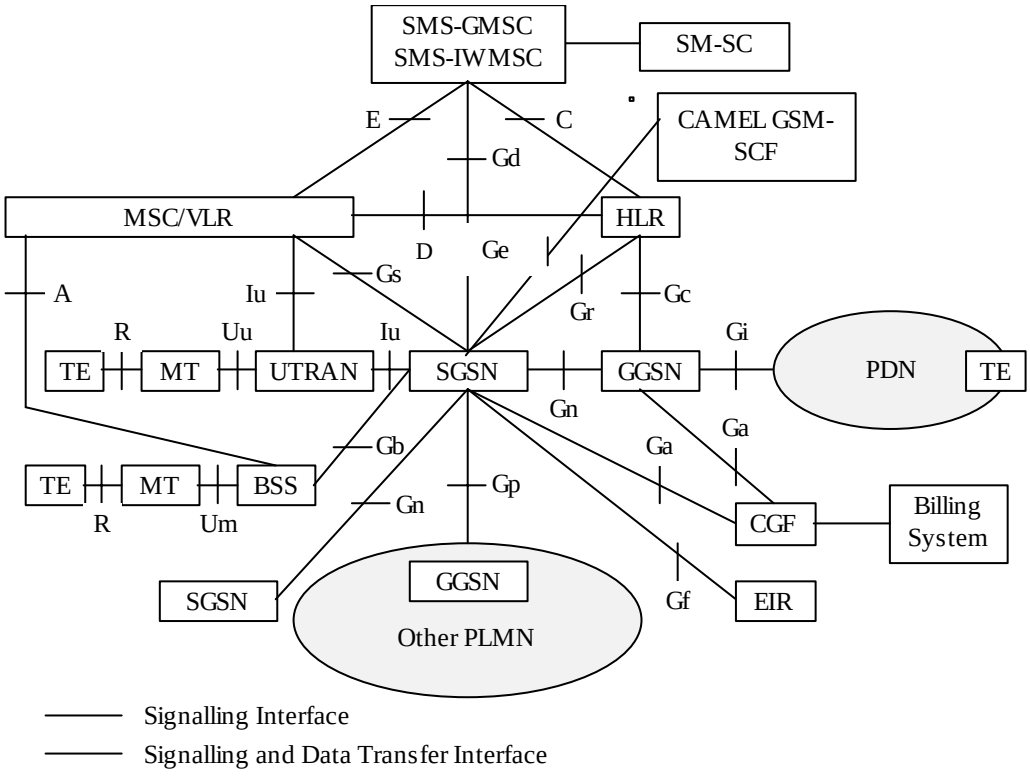
1. Summary

At the CN4#20 meeting a contribution on Introducing IMSI in Delete PDP Context Request message [N4-030854, N4-030855 and N4-030856] was discussed. It was premature to take a decision in CN4 due to concerns raised that IMSI should not be sent open across the Gn/Gp interfaces. This document analyses the security issues related to this and concludes that CN4 can send the IMSI in GTP messages between GSNs.

It is proposed that SA3 sends an LS to CN4 to inform them on this conclusion.

2. Introduction

The GPRS Tunnelling Protocol (GTP) is the protocol used between GPRS Support Nodes (GSNs) in the UMTS/GPRS backbone network. It includes both the GTP control plane (GTP-C) and data transfer (GTP-U) procedures. GTP is defined for the Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs.



According to 23.060, sub clause 9.2.4.1, if the SGSN receives a Deactivate PDP Context Request message for a PDP context that is currently being activated, the SGSN shall stop the PDP Context Activation procedure without responding to the MS, and continue with the PDP Context Deactivation initiated by MS procedure.

In GTP97 (GTP v0) the SGSN will send a Delete PDP Context Request message to the GGSN, with the TID (IMSI and NSAPI) in the GTP header. This will make the GGSN stop the activation handling and no hanging PDP contexts are created.

However, as from GTP99 (GTP v1) TID is not used. Instead there is one TEID for each direction, and the TEID is negotiated between SGSN and GGSN. In this case the SGSN must await the Create PDP Context Response message before it is able to send a Delete PDP Context Request message to the GGSN. If the Create PDP Context Response message, for some reason, never arrives, the corresponding PDP Context is hanging in GGSN.

At CN4#20 Ericsson suggested that by introducing the IMSI to the Delete PDP Context Request message, the GGSN would be able to identify (using IMSI and NSAPI) which PDP Context that is to be removed. However, the meeting's opinion was that one shall avoid sending the IMSI across the Gn/Gp interface because the Gn/Gp interface is insecure.

Ericsson and Vodafone understands that CN4 has the responsibility to decide upon what need to be transported across the Gn/Gp interfaces but in order to take the correct decisions CN4 would need a good understanding on the security issues related to sending IMSI across Gn/Gp interfaces.

3. Conclusions

According to the GSM Association's document PRD IR.34 on "Inter-PLMN Backbone Guidelines" (a common interworking document which operators who have roaming agreements adhere to), GPRS intra- and inter-PLMN backbone networks shall for security reasons remain invisible and inaccessible to the public Internet. What is more, using IPSec as an encryption and tunnelling method on the Inter-PLMN backbone is recommended.

In 3GPP, TS 33.210 put mandatory requirements on how GTP shall be protected when TS 33.210 is implemented. TS 33.210 mentions many sensitive messages and some of them already include IMSI as well as other sensitive data so adding IMSI in an additional message should not be an issue.

Furthermore, the precedence for this is already set since a Release 5 IMS terminal using USIM (i.e. ISIM not present) will include IMSI as part of the private IMS identity, which is transported on the Gn/Gp user plane. SA3 accepted this mechanism after considering IMSI privacy issues. There are some differences in this case (sending the clear IMSI in the control plane rather than the user plane) but this is not significant from a security perspective.

Ericsson and Vodafone propose that an LS is sent to CN4 to inform them of the above conclusion, and attach this document.

4. Excerpts from the standards that are of particular relevance to this discussion

PRD IR.34, 4.1 IP Addressing

> Public addressing shall be applied in all GPRS backbone networks. Using public addressing means that each operator has a unique address space that is officially reserved form Internet addressing authority. However, public addressing does not mean that these addresses should be visible to Internet. For security reasons, GPRS intra- and inter-PLMN backbone networks shall remain invisible and inaccessible to the public Internet. Generally Internet routers shouldn't know how to route to the IP addresses advertised to the inter-PLMN networks. In other words Inter-PLMN service provider and PLMN operator networks shall be totally separated from public Internet.

…

4.2.1 IPSec

GPRS operators may use IPSec [8, 9, 10] as an encryption and tunnelling method on the Inter-PLMN backbone, especially if the Inter-PLMN backbone medium itself does not guarantee security and data integrity.

Inter-PLMN backbone, if implemented on unsecured public networks, should support the use of IPSec, including Public Key Infrastructure (PKI) implementations such as Internet Key Exchange (IKE) [11].

TS 33.210, 5.6.1 ”Network domain security architecture outline”

The NDS/IP key management and distribution architecture is based on the IPsec IKE (RFC-2401 [12], RFC-2407 [18], RFC-2408 [19] and RFC-2409 [20]) protocol. As described in the previous section a number of options available in the full IETF IPsec protocol suite have been considered to be unnecessary for NDS/IP. Furthermore, some features that are optional in IETF IPsec have been mandated for NDS/IP and lastly a few required features in IETF IPsec have been deprecated for use within NDS/IP scope. Sections 5.3 and 5.4 give an overview over the profiling of IPsec and IKE in NDS/IP.

The compound effect of the design choices in how IPsec is utilized within the NDS/IP scope is that the NDS/IP key management and distribution architecture is quite simple and straightforward.

The basic idea to the NDS/IP architecture is to provide hop-by-hop security. This is in accordance with the *chained-tunnels* or *hub-and-spoke* models of operation. The use of hop-by-hop security also makes it easy to operate separate security policies internally and towards other external security domains.

In NDS/IP only the Security Gateways (SEGs) shall engage in direct communication with entities in other security domains for NDS/IP traffic. The SEGs will then establish and maintain IPsec secured ESP Security Association in tunnel mode between security domains. SEGs will normally maintain at least one IPsec tunnel available at all times to a particular peer SEG. The SEG will maintain logically separate SAD and SPD databases for each interface.

The NEs may be able to establish and maintain ESP Security Associations as needed towards a SEG or other NEs within the same security domain. All NDS/IP traffic from a NE in one security domain towards a NE in a different security domain will be routed via a SEG and will be afforded hop-by-hop security protection towards the final destination.

Operators may decide to establish only one ESP Security Association between two communicating security domains. This would make for coarse-grained security granularity. The benefits to this is that it gives a certain amount of protection against traffic flow analysis while the drawback is that one will not be able to differentiate the security protection given between the communicating entities. This does not preclude negotiation of finer grained security granularity at the discretion of the communicating entities.

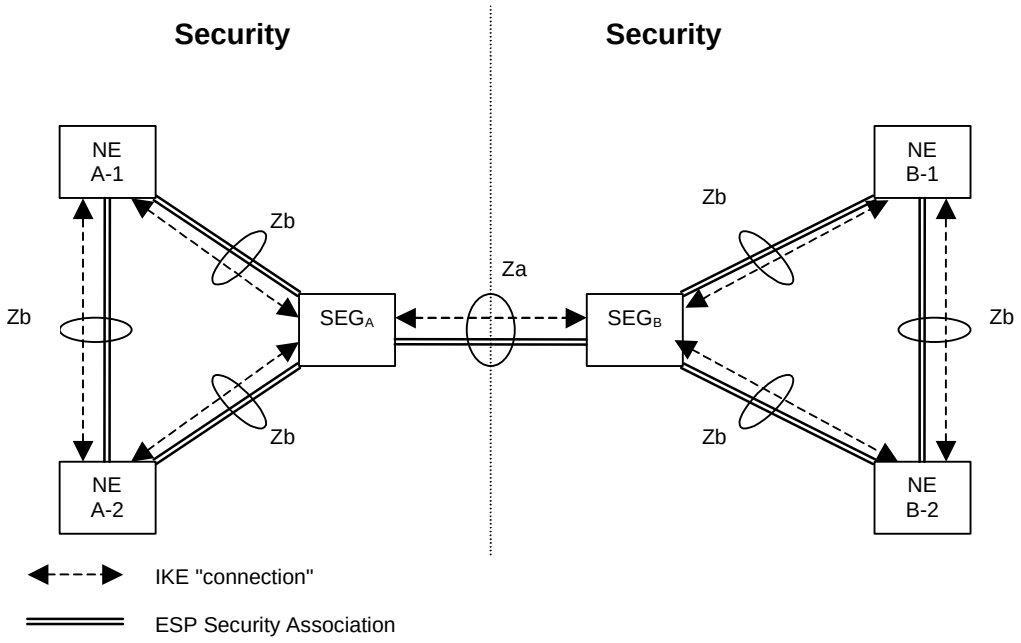


Figure 1: NDS architecture for IP-based protocols

TS 33.21, Annex B (normative): Security protection for GTP

This section details how NDS/IP shall be used when GTP is to be security protected.

B.1 The need for security protection

The GPRS Tunnelling Protocol (GTP) is defined in 3GPP TS 29.060 [6]. The GTP protocol includes both the GTP control plane signalling (GTP-C) and user plane data transfer (GTP-U) procedures. GTP is defined for Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs.

GTP-C is used for traffic that that is sensitive in various ways including traffic that is:

- critical with respect to both the internal integrity and consistency of the network;
- essential in order to provide the user with the required services;
- crucial in order to protect the user data in the access network and that might compromise the security of the user data should it be revealed.

Amongst the data that clearly can be considered sensitive are the mobility management messages, the authentication data and MM context data. Therefore, it is necessary to apply security protection to GTP signalling messages (GTP-C).

Network domain security is not intended to cover protection of user plane data and hence GTP-U is not protected by NDS/IP mechanisms.

Table 1 presents a list of GTP interfaces that shall be considered by NDS/IP.

Table 1: GTP Interfaces that are affected by NDS/IP

Interface	Description	Affected protocol
Gn	Interface between GSNs within the same network	GTP
Gp	Interface between GSNs in different PLMNs.	GTP