INTERNET-DRAFT
Working Group
July 30,2000
expires 30 January 2001

Charles Perkins
Nokia Research
Hossam Afifi
INT Evry

Internet General Packet Radio Service (IGPRS); Service description

draft-afifi-igprs-00.txt

Status of this Memo

This document is an individual contribution for consideration by the IPNG Working Group of the Internet Engineering Task Force. Comments should be submitted to the mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at:

http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at:

http://www.ietf.org/shadow.html.

Abstract

We propose an architecture (IGPRS) for the integration of the IPv6 protocol in the GPRS infrastructure. The data and signalling protocol suite will be based on mobile IPv6 protocol (instead of the GTP protocol). This new infrastructure will take advantage of the available internet protocols for routing and security. Since it is targetted to co-exist with the GPRS, it is a partial translation of MAP specifications to Internet protocols. This document uses some of the GPRS Service document and some of its terminology.

The IGPRS interface will be complementary to GPRS protocols and can co-exist with them. It represents hence a smooth migration to an all IP network. A GPRS terminal that has IGPRS functionality will be able to directly use the internet infrastructure for data and signalling transmission.
A GPRS Base Station that has this additional functionality will be able to translate all the traffic coming from an enhanced GPRS terminal

to a conventional IPv6 protocol suite. IPv4 can be used by mobile applications but the underlying infrastructure will be only based on IPv6. Transition mechanisms should hence be used when IPv4 is required.

Since a large legacy of management protocols is available and necessary in the GPRS/GSM+2 infrastructure and since the GPRS data protocols are designed to co-exist with the GSM, we propose an architecture that supports mobile Ipv6 as the data protocol and diameter as the main signalling protocol (AAA). In the boundaries we propose to interface the internet protocols with the conventional GPRS entities (e.g. HLRs, MSC/VLRs) in order to keep the necessary user management consistency.
The resulting architecture is then composed of enhanced Ipv6 GPRS terminals, enhanced GPRS Base stations and enhanced HLR/VLR functionalities capable of dealing with Internet protocols.

Table of Contents

---

1 . Introduction and scope

This document gives the service description of the Internet Based GPRS system (IGPRS) that represents an evolution of the current GPRS service as defined in the document [GPRS]. It is hence mainly

compliant with the current GPRS service description principles. It gives the procedures and functionalities that have to be implemented in the terminals and in the network in order to operate an IPv4/IPv6 based mobile public data network. This system is designed to run in presence of the conventional GPRS and GSM systems.

The base protocol in this architecture is IPv6 and does not at all preclude IPv4 in the mobile node. However, all mobility and signalling procedures are achieved using the v6 version only. IGPRS fully relies on the normal layer 2 GPRS protocols and eventually data compression. The following sections give the detailed operation of the IGPRS system. The rest of this document is organized as follows. Section 2 gives some definitions and abbreviations that will be frequently used in the subsequent sections. Section 3 defines the protocol main entities and states describing a mobile node and their relation to Mobile IPv6 states. In Section 4 we describe the packet formats. Section 5 gives the procedures and transitions between the protocol functions. Section 6 gives the security functions necessary for user authentication.

2 . Abbreviations and terminology

DNS Domain Name Service

IGSS Internet GPRS Support Server, it must be a v6 Home Agent.

IMSI International Mobile Subscriber Identity

NAI Network Access Identifier

MIPv6 Mobile IP v6

MN Mobile Node

PCB Protocol Control Block. Information associated with a node.

PLMN Public Land Mobile Network

RA Routing Area, A space of administration for a single Home Agent.

RAC Routing Area Code; IPv6 Prefix code

RAI Routing Area Identity; The canonical Name of the router responsible of the RAC

RLC Radio Link Control

TLLI Temporary Logical Link Identity

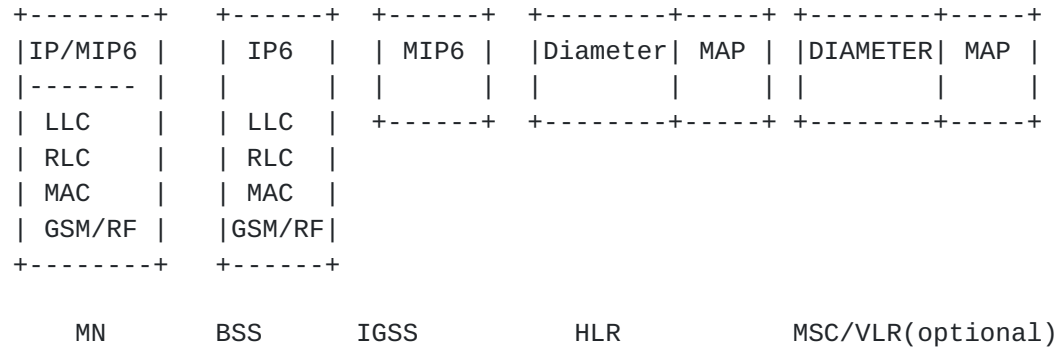
TMSI Temporary Mobile Subscriber Identity Regional Registration Identity

The GPRS architecture is mainly composed of a mobile node (MS), a base station (BSS), a home agent (SGSN) and databases (HLR). Most of entities in the IGPRS protocol suite are the same as defined in the GPRS infrastructure except for: IGSS, that replaces the SGSN. It is a Home Agent running Ipv6 with additional Diameter, DNS, routing and security functionalities. It can co-exist with an SGSN node. BSS, is the same as in the GPRS network except that it implements IPv4/IPv6 routing functionalities. A BSS may represent a group of layer 2 bridging equipments. It may be capable of header compression/decompression facilities and could be based on a connection oriented layer 2 protocol.

The main architecture of this document is based on the integration of the Home Agent entity in the SGSN. A second alternative is possible with the home agent being embedded in the GGSN. We do not consider this architecture in this document and we leave it for further study.

3 . Protocol Overview

In this section we present the main entities implied in IGPRS.



3 . 1 . Protocol Entities

IPv6 is implemented on the physical layer and layer 2 of the GPRS protocol. We identify the Mobile node MN, BSS, IGSS, HLR interface and MSC/VLR interface as the entities representing IGPRS. The MN has some interactions with the BSS and others with the IGSS. The BSS is responsible of informing the MN of its location area (the subnetwork in IPv6) and of its Home Agent identity. The IGSS initiates security functions and updates the HLR with any necessary mobility management procedure. The optional dialogue between the IGSS and MSC/VLR is for further study. Mobile IPv6 is only seen between the MN and the IGSS. The rest of the entities are not part of the mobility process. We describe in the following section the interaction of the IPv6 layer with layer 2 states. Some procedures in the IGPRS proposal are timer based and others location based. The first procedures are necessary to save the air interface resources and to rapidely detect any MN disappear. The second set of procedures correspond to mobility management at the network level.

The Mobile Node (MN)

The v6 Mobility Management (MM) activities related to a IGPRS subscriber are characterized by one of three different states. Each state describes a certain level of functionality and information allocated. It is to be noted that the MN will keep a link local address whenever it has to establish any pre-authentication procedure. Once it has to send user data it should obtain a valid address. This will be explained later. The IPv6 layer will be able to detect at each time the current state of the entity along with the related state variables and to achieve the necessary procedures.

IDLE (IGPRS) State

In GPRS IDLE state, the subscriber is not attached to the IGPRS mobility management. The MN and IGSS context hold no valid routing information for the subscriber. The subscriber-related mobility management procedures are not performed. The MN does not have a home agent (IGSS) neither. Since the MN listens to multicast layer1 physical information it can perform locally PLMN selection and IGPRS cell selection and re-selection processes. Data transmission to and from the mobile node as well as the paging of the subscriber are not possible. The GPRS MN is seen as not reachable in this case. From an IP/IPv6 point of view the node does not have any valid address (except a link local), valid default router or valid home agent information (routing area). In order to establish contexts in the MN and the IGSS, the MN shall perform the IGPRS Attach procedure explained in the Procedures section.

STANDBY State

In STANDBY state, the subscriber is attached to IGPRS mobility management. The MN and IGSS have established contexts for the subscriber's IMSI/NAI. Pages for data or signalling information may be received. User IPv6 reception and transmission are not possible in this state. The MN performs IGPRS Home Agent selection and IGPRS cell selection and re-selection locally. The MN listens on the broadcast channel to learn about the router advertisement and hence to know its prefix and whether it is still in the same routing area (HA) or not. The MN executes mobility management procedures to inform the IGSS when it has entered a new HA zone. This includes MIP procedures. The MN does not inform the IGSS on a change of cell in the same HA zone. Therefore, the location information in the IGSS context contains only the identification of the MN but not its cell location. The MN may initiate activation or deactivation of contexts while in STANDBY state. A context shall be activated before data can be transmitted or received for this PCB context. The IGSS may have to send data or signalling information to an MN in STANDBY state.

Paging in the STANDBY state is accomplished by Neighbour Sollicitation messages sent from the IGSS or BSS. The suffix is simply set to the IMSI identifier. It should be noted that no DAD is to be done on a IGPRS network. Paging may not be an efficient way to reach the MN but the procedure should be implemented to solve at minimum, emergency situations. An alternative to paging is to wait until the node subscribes with a new IGSS or updates the old one through the periodic routing updates as described in the following sections.

The MN or the network may initiate the IGPRS Detach procedure to move to the IDLE state. After expiry of the mobile reachable timer the IGSS may perform an implicit detach in order to return in the IGSS to IDLE state.

READY State

In READY state, the IGSS updates the MN context with its subnetwork (prefix). The MN performs mobility management procedures to provide the network with the actual selected cell (prefix). IGPRS cell selection and re-selection is done locally by the MN, or may optionally be controlled by the network. The MN Prefix is sent periodically to the IGSS via the BSS (the procedure can be achieved with hob-by-hop Options or ICMPv6 messages). When a mobile node makes a handover to a new cell, the default router may or may not change according to the network topology. Two cells may be in the same routing area. However it is good to know the cell identity (that would correspond to some layer two details) for a better interaction with the fixed network. The mobile node learns this information from the radio layer and forwards it to the BSS and IGSS

(through an ICMPv6 or Destination Option). The MN may send and receive Internet PDUs in this state. The network initiates no IGPRS pages for an MN in READY state The IGSS transfers downlink data to the BSS responsible for the subscriber's actual IGPRS cell. Regardless if a radio resource is allocated to the subscriber or not, the MN remains in the READY state even when there is no data being communicated. The READY state is supervised by a timer. An MN context moves from READY state to STANDBY state when the READY timer expires. In order to move from READY state to IDLE state, the MN initiates the IGPRS Detach procedure. This means that the IPv6 global address is no more valid.

Mobility management in the IGSS side

This section describes the additional states that have to be maintained relating IPv6 to the lower layer. The states are mainly related to timers. Some states are kept in both the MN and IGSS.

READY Timer Function

The READY timer function maintains the READY timer in the MN and IGSS. The READY timer controls the time an MN remains in READY state in the MN and the IGSS. The READY timer shall be reset and begin running in the MN when a packet is transmitted, and in the IGSS when it is correctly received. When the READY timer expires, the MN and IGSS contexts shall return to STANDBY state. The length of the READY timer shall be the same in the MN and IGSS. The initial length of the READY timer shall be defined by a default value. The IGSS, and only the IGSS, may change the length of the READY timer by transmitting a new value in the Attach Accept, Routing Area Update Accept. If the READY timer length is set to zero, the MN shall immediately be forced into STANDBY state.

Periodic RA Update Timer Function

Routing Area Update functionality is directly coupled with the MIPv6 management. The Periodic RA Update Timer function monitors the periodic RA update procedure in the MN. The periodic RA update timer is unique within an RA. Upon expiry of the periodic RA update timer, the MN shall start a periodic routing area update procedure.

Mobile Reachable Timer Function

The Mobile Reachable Timer function monitors the periodic RA update procedure in the IGSS. The mobile reachable timer shall be slightly longer than the periodic RA update timer used by an MN. The mobile reachable timer is stopped when the READY state is entered. The

mobile reachable timer is reset and started when the state returns to STANDBY. If the mobile reachable timer expires, the IGSS shall stop sending IGPRS paging messages to the MN, but other features may happen immediately.

4 . Messages Formats

This section describes the necessary packet and headers format for IGPRS infrastructure.
We identify messages from the MN to the IGSS. From the IGSS to the HLR and vice-versa.

Inter IGSS Diameter Extensions:

IGSS to HLR Diameter Messages:

IPv6 Hop-by-Hop IGSS option:
IPv6 Router Sollicitations Authentication Header and options:

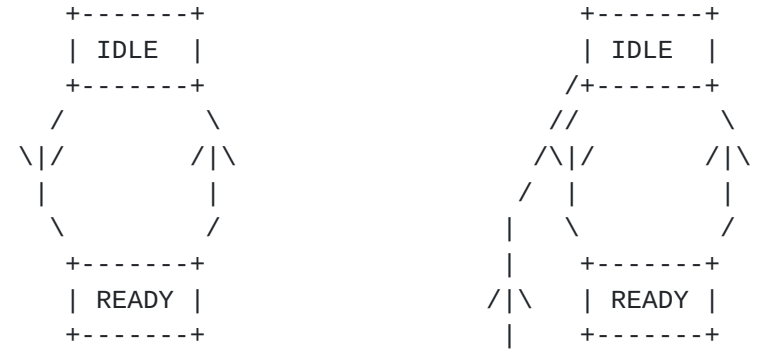
5 . IGPRS Procedures and Functions

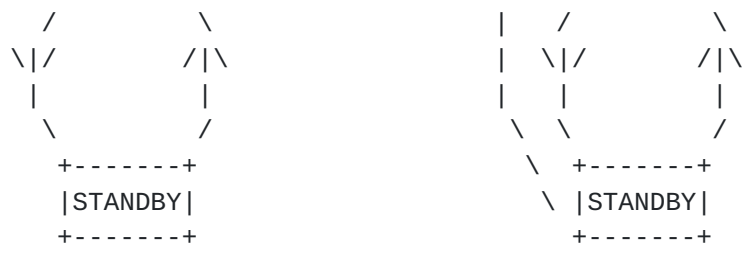
In this section we describe the actions that entities have to take to implement the mobility management for IGPRS. We start by describing the functions activated in IPv6 due to the state transitions occuring in both MN and IGSS. We also explain the procedures that are used to accomplish the routing update (change of HA and of default router).

5 . 1 . State transition in the MN and IGSS

This section gives details on the changes that will happen when a MN goes from one state to the other. These state information are obtained from the lower layers.

The movement from one state to the next is dependent on the current state (IDLE, STANDBY, or READY) and the event occurred (e.g., IGPRS attach). We describe the IPv6 necessary actions when such a transition happens.





MM states diagrams for MN and IGSS

Moving from IDLE to READY:

- IGPRS Attach: The MN requests access and a logical link to an IGSS is initiated.

Moving from STANDBY to IDLE:

- Implicit Detach: The MN and the IGSS shall return to IDLE.

- Cancel Location: The IGSS receives a MAP Cancel Location message from the HLR (through the Diameter extensions).

Moving from STANDBY to READY:

- PDU transmission: The MN sends a packet to the IGSS, possibly in response to a page.

- PDU reception: The IGSS receives an IPv6 from the MN.

Moving from READY to STANDBY:

- READY timer expiry: The MN and the IGSS return to STANDBY state.

- Force to STANDBY: The IGSS indicates an immediate return to STANDBY state before the READY timer expires.

- Abnormal RLC condition: The IGSS returns to STANDBY state in case of

delivery problems on the radio interface or in case of irrecoverable disruption of a radio transmission.

Moving from READY to IDLE:

- IGPRS Detach: The MN or the network requests to return to IDLE state. The IGSS may delete the MN from its entries.

- Cancel Location: The IGSS receives a MAP Cancel Location message from the HLR.

Attach Function

A IGPRS attach is made to the IGSS. A IGPRS-attached MN makes NAI/IMSI attach via the IGSS. In the attach procedure, the MN shall provide its identity and an indication of which type of attach that is to be executed. The regional Registration should be used as much as possible to prevent too many authentication exchanges with the home IGSS. A Temporary identification should be used (P-TMSI) After having executed the IGPRS attach, the MN is in READY state and the IGSS also.

The detailed procedure of an attach function is described here-after:

The MN initiates the attach procedure by sending an ICMPv6 router sollicitation message. The BSS, using the DIAMETER Protocol Direct Reboot Indication (IMSI or P-TMSI and old RAI, old P-TMSI Signature) sends a message to the IGSS. On the point to point wireless link the MN sends its IMSI for authentication. NAI/IMSI shall be included if the MN does not have a valid P-TMSI available. If the MN has a valid P-TMSI, then P-TMSI and the old RAI (Prefix) associated with P-TMSI shall be included in the ICMPv6 packet. If the MN identifies itself with P-TMSI and the IGSS has changed since detach, the new IGSS sends an Identification Request (P-TMSI, old RAI, old P-TMSI Signature) diameter message to the old IGSS to request the IMSI. The old IGSS responds with Identification Response (NAI/IMSI, Authentication Triplets). If the MN is not known in the old IGSS, the old IGSS responds with an appropriate error cause. The old IGSS also validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old IGSS. If the MN is unknown in both the old and new IGSS, the IGSS sends a DIAMETER Home-Agent-MIP-Request (Identity Type = IMSI) to the BSS. The MN responds and the BSS forwards with Identity Response (NAI/IMSI).

If the IGSS address has changed since the IGPRS detach, or if it is the very first attach, then the IGSS informs the HLR: The IGSS sends an Update Location (IGSS IPv6 Address, NAI/IMSI) to the HLR through Diameter extensions. The HLR sends Cancel Location (IMSI, Cancellation Type) to the old IGSS with Cancellation Type set to Update Procedure. The old IGSS acknowledges with Cancel Location Ack (IMSI). If there are any ongoing procedures for that MN, the old IGSS shall wait until these procedures are finished before removing the contexts. The HLR sends Insert Subscriber Data (IMSI, IGPRS subscription data) to the new IGSS. The new IGSS validates the MN presence in the (new) RA. If due to regional subscription restrictions the MN is not allowed to attach in the RA, the IGSS rejects the Attach Request with an appropriate cause, and may return

an Insert Subscriber Data Ack (IMSI, <IGSS Area Restricted>) message to the HLR. If subscription checking fails for other reasons, the IGSS

rejects the Attach Request with an appropriate cause and returns an Insert Subscriber Data Ack (IMSI, Cause) message to the HLR. If all checks are successful then the IGSS constructs a context for the MN and returns an Insert Subscriber Data Ack (IMSI) message to the HLR. The HLR acknowledges the Update Location message by sending an Update Location Ack to the SGSN after the cancelling of old context and insertion of new context are finished. If the Update Location is rejected by the HLR, the IGSS rejects the Attach Request from the MS with an appropriate cause. If the Attach Request cannot be accepted, the IGSS returns an Attach Reject (IMSI, Cause) message to the MN.

Detach Function

The Detach function allows an MN to inform the network that it wants to make a IGPRS and/or NAI/IMSI detach, and it allows the network to inform an MN that it has been IGPRS-detached or IMSI-detached by the network. The only proposed detach procedure is: - IGPRS detach;

The MN is detached from IGPRS either explicitly or implicitly: - Explicit detach: The network or the MN explicitly requests detach. - Implicit detach: The network detaches the MN, without notifying the MN, a configuration-dependent time after the mobile reachable timer expired, or after an irrecoverable radio error causes disconnection of the logical link. In the explicit detach case, a Detach Request (Cause) is sent by the IGSS to the MN, or by the MN to the IGSS.

5 . 2 Mobility Management procedures

Cell Update Procedure

A cell update takes place when the MN enters a new cell inside the current RA and the MN is in READY state. If the RA has changed, a routing area update is executed instead of a cell update. The MN performs the cell update procedure by sending an uplink packet of any type containing the MN identity to the IGSS with a Hop-by-Hop option. In the direction towards the IGSS, the BSS shall add the Cell Global Identity including RAC to all packets. A cell update is any correctly received and valid IPv6 PDU. The IGSS records this change of cell so that further traffic directed towards the MN is conveyed over the new cell.

Routing Area Update Procedure

A routing area update takes place when a IGPRS-attached MN detects that it has entered a new RA i.e a different Home Agent domain, when the periodic RA update timer has expired, or when a suspended MN is not resumed by the BSS. The IGSS detects that it is the same sub-network. In this case, the IGSS has the necessary information about the MN and there is no need to inform HLR about the new MN location. A periodic RA update is always an intra IGSS routing area update.

Intra IGSS Routing Area Update

The Intra IGSS Routing Area Update procedure consists in a change of the default router for the MN while keeping the same HA. The MN sends a Routing Area Update Request (it is done via a v6 binding update) (old RAI, old P-TMSI Signature, Update Type) to the IGSS. Update Type shall indicate RA update or periodic RA update. The BSS shall add the Cell Identity as a Hop-by-hop option. The IGSS validates

the MN presence in the new RA (sub-network). If due to regional subscription restrictions the MN is not allowed to be attached in the RA, or if subscription checking fails, then the IGSS rejects the routing area update. If all checks are successful then the IGSS updates the MN record. A new P-TMSI may be allocated. A confirmation is sent back to the mobile node (P-TMSI, P-TMSI Signature). If P-TMSI was reallocated, the MN acknowledges the new P-TMSI by returning a routing Area Update Complete AVP to the IGSS. If the routing area update procedure fails a maximum allowable number of times, or if the IGSS returns a routing Area Update Reject (Cause) AVP, the MN shall enter IDLE state.

Inter IGSS Routing Area Update

The Inter IGSS Routing Area Update procedure is explained in the following list. It consists in a change in the HA for the mobile node. The MN sends a Routing Area Update Request (binding update with the old HA address, old P-TMSI Signature, Update Type) to the new IGSS. Update Type shall indicate RA update or periodic RA update. The BSS shall add the Cell Global Identity in the Hop-by-hop option. The new IGSS sends Diameter AVP containing IGSS Context Request (old RAI, TLLI, old P-TMSI Signature, New IGSS Address) to the old IGSS for this MN. The old IGSS validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old IGSS. This should initiate the security functions in the new IGSS. If the security functions authenticate the MN correctly, the new IGSS shall send an IGSS Context Request (old RAI, TLLI, MN Validated, New IGSS Address) Diameter message to the old IGSS. MN Validated indicates that the new SGSN has authenticated the MN. These procedures are described in

the context of the Diameter extensions in details. If the old P-TMSI Signature was valid or if the new IGSS indicates that it has authenticated the MN, the old IGSS stops assigning forwarding the traffic downlink, and responds with IGSS Context Response. If the MN is not known in the old IGSS, the old IGSS responds with an appropriate error cause. Contrary to the original GPRS mechanism where the SGSN adds a new entity in the chain, the IGSS which is a home agent cannot be changed while active contexts are present. In the absence of active contexts the inter IGSS procedure can be applied. A timer is triggered in the old IGSS.

The new IGSS sends an IGSS Context Acknowledge message in the appropriate Diameter format to the old IGSS. This informs the old IGSS that the new IGSS is ready to receive data packets belonging to MN and the necessary DNS procedure are executed to change the MN prefix to the one belonging to the new IGSS. The old IGSS marks in its context that the information in the HLR is invalid.
If the security functions do not authenticate the MN correctly, then the routing area update shall be rejected, and the new IGSS shall send a reject indication to the old IGSS. The old IGSS shall continue as if the IGSS Context Request was never received. The new IGSS updates the MN entry (new IGSS Address HA) The new IGSS informs the HLR of the change by sending Update Location (IGSS v6 address, IMSI) to the HLR. The HLR sends Cancel Location (IMSI, Cancellation Type) to the old IGSS with Cancellation Type set to Update Procedure (This is done with the Diameter protocol). Then the old IGSS removes the contexts. Otherwise, the contexts are removed only when the timer expires. This allows the old IGSS to ensure that the contexts are kept in the old SGSN in case the MN initiates another inter IGSS routing area update before completing the ongoing routing area update to the new IGSS. The old IGSS acknowledges with Cancel Location

Ack (IMSI) The HLR sends Insert Subscriber Data (IMSI, IGPRS subscription data) to the new IGSS. The new IGSS validates the MN presence in the (new) RA. If due to regional subscription restrictions the MN is not allowed to be attached in the RA, the IGSS rejects the Routing Area Update Request with an appropriate cause, and may return an Insert Subscriber Data Ack message to the HLR. If all checks are successful then the IGSS constructs a context for the MN and returns an Insert Subscriber Data Ack (IMSI) message to the HLR. The HLR acknowledges the Update Location by sending Update Location Ack (IMSI) to the new IGSS. The new IGSS validates the MN presence in the new RA. If due to roaming restrictions the MN is not allowed to be attached in the IGSS, or if subscription checking fails, then the new IGSS rejects the routing area update with an appropriate cause. If all checks are successful then the new IGSS constructs contexts for the MN. The new IGSS responds to the MN

with Routing Area Update Accept (P-TMSI, P-TMSI Signature). The MN acknowledges the new P-TMSI by returning a Routing Area Update Complete message to the IGSS. In the case of a rejected routing area update operation, due to regional subscription or roaming restrictions, the new IGSS shall not construct a context. A reject shall be returned to the MN with an appropriate cause. The MN shall not re-attempt a routing area update to that RA. The RAI value shall be deleted when the MN is powered-up.

6 . Security Considerations

The Security function:

- Guards against unauthorised IGPRS service usage (authentication and service request validation).

- Provides user identity confidentiality (temporary identification-Regional Registration, and ciphering).

- Provides user data confidentiality (ciphering).

Authentication of Subscriber

Authentication procedures already defined in GSM and in the Diameter strong authentication shall be used, with the distinction that the procedures are executed from the IGSS. The IGSS may act according to Diameter specifications as a proxy in a chain. The IGPRS Authentication procedure performs subscriber authentication, or selection of the ciphering algorithm and the synchronization of the start of ciphering, or both. Authentication triplets are stored in the IGSS. The Authentication procedure is explained in the following list. If the IGSS does not have previously stored authentication triplets, a Send Authentication Info (IMSI) message is sent to the HLR through the Diameter protocol proxying procedures. The HLR responds with a Send Authentication Info Ack (Authentication Triplets) message. Each Authentication Triplet includes RAND, SRES, and Kc. The IGSS sends an Authentication and Ciphering Request (RAND, CKSN, Ciphering Algorithm) message to the MN. The MN responds with an Authentication and Ciphering Response message through Diameter extensions. The MN starts ciphering after sending the Authentication and Ciphering Response message. The IGSS starts ciphering when a valid Authentication and Ciphering Response is received from the MN. In the routing area update case, if ciphering was used before the routing area update, and if the Authentication procedure is omitted, then the IGSS shall resume ciphering with the same

algorithm when a ciphered Routing Area Update Accept Diameter

message is sent, and the MN shall resume ciphering when a ciphered Routing Area Update Accept Diameter message is received. User Identity Confidentiality A Temporary Logical Link Identity (TLLI) identifies a IGPRS user. The relationship between TLLI and IMSI is known only in the MN and in the IGSS. TLLI is derived from the P-TMSI allocated by the IGSS or built by the MN. The IGSS may reallocate the P-TMSI at any time when the MN is in READY state. The reallocation procedure can be performed by the P-TMSI Reallocation procedure, or it can be included in the Attach or Routing Area Update Diameter procedures.

P-TMSI Signature

P-TMSI Signature is optionally sent by the IGSS to the MN in Attach Accept and Routing Area Update Accept Diameter messages. If the P-TMSI Signature has been sent by the IGSS to the MN since the current P-TMSI was allocated, then the MN shall include the P-TMSI Signature in the next Routing Area Update Request and Attach Request for identification checking purposes. In the Attach and Routing Area Update procedures, the IGSS shall compare the P-TMSI Signature sent by the MN with the signature stored in the IGSS. If the values do not match, the IGSS should use the security functions to authenticate the MN. If the values match or if the P-TMSI Signature is missing, the IGSS may use the security functions to authenticate the MN. The P-TMSI Signature parameter has only local significance in the IGSS that allocated the signature. If ciphering is supported by the network, the IGSS shall send the P-TMSI Signature ciphered to the MS. Routing Area Update Request and Attach Request, into which the MN includes the P-TMSI Signature, are not ciphered.

IMEI

This is the identification of the terminal. It can be required by a given operator. It is hence taken into consideration in the security functions.

7 . Security Functions

P-TMSI Reallocation Procedure

This is the procedure by which the MN will obtain a temporary key in the authentication domain of the new IGSS. Diameter messages will help the exchange of keys between the original and the new IGSS. At the end of the procedure the MN should receive a valid P-TMSI using the IKE protocol.

Identity Check Procedure

The Identity Check procedure is explained in the following list.

1) The IGSS sends Identity Request (Identity Type) to the MN. The MN

responds with Identity Response (Mobile Identity).

2) If the IGSS decides to check the IMEI, it sends Check IMEI (IMEI) Diameter message to the BSS that translates it and forwards it to the MN.

0n) References

[CHAP] CHAP, PPP Challenge Handshake Authentication Protocol. rfc-1994.

[GPRS] Draft ETSI EN 301 344 V6.6.0 (2000-02) European Standard (Telecommunications series) Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2 (GSM 03.60 version 6.6.0 Release 1997)

[ADDRCONF] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

Authors may be reached at
charliep@iprg.nokia.com
hossam.afifi@int-evry.fr