The IMS and its technology (Part II)

From Gunnar Heine

Translation of an article of German Funkschau magazine of April

This article presents the following part of the article in the previous edition of Funkschau. The technic of the IP-Multimedia Subsystem, which is on the radar screen of manufacturers and telecommunication operators, was presented since quite some time.
To make a long story short, the IMS forms a “basis to provide IP-based communication services”. In the first part, the important problems of IMS were described for a spacious use. Target of this article is to outline the possible methods of resolution. Here it is necessary to outline that the introduced approaches, point of view and experience of the author or the company INACON GmbH were neither influenced by standardising boards nor by manufactures interests. Additionally it is important to ensure that the demonstrated methods of resolution do not present an “off-the-shelf” solution but they give room for discussions.

Resolution approach for problem 1: Incoming calls: Incoming calls are usually regular telephone calls that are coming from the public network for a user of IMS. As mentioned in the last edition, the problem is that the incoming calls cannot be forwarded to the user. The proposed solution between different IMS-types must be distinguished:

IMS of type 1: Here we deal with the IMS-Implementation of a Mobile Communication Network which provide their customers IMS-services, sometimes partially for short-term but completely for long-term. The delay sensitive element is provided by the acceptance of the customer for new end products which shall only allow VoIP telephony for longer-term. The caller of IMS type 1 dials the well-known E.213 phone number Both in common do not have Gateway-MSC’s. Instead, MGCFs are used here. However the – relatively easy - routing-decision by using a code (see above: 171) is not applicable.

There is need to analyse complete called number.

The telephone switches (exchange) ahead of the IAM-message with bullet 1b (figure 1) decides to direct this call to the MGCF.

Figure 1 should be understood as “either …., or ….”. Implicated figure 1 presents a fascinating combination of land-line and mobile network-provider, that calls its clients on the mobile phone, even if the land-line number was called and vice versa. The technical implementation (not the political one (-;) is incidentally one of the easier tests for the IMS. This is called “Forking” and here, a user is called on 3 sets, whereas the registration of VoIP-telephone and of UMTS-mobile-set was affected via the same P-CSCF. So, even two SIP:INVITE-messages (bullet 9) are placed to the upper P-CSCF. Back to the first question: How does the call come to the IMS-user? At the moment we are at the Gateway-MSC (bullet 1a) or at the MGCF (bullet 1b). Following are the proposals to minimise the necessary changes: Like as demonstrated in bullet 2a, the GMSC has to search at the HSS for routing-information, at first. This is nothing new for the GMSC. The well-known MAP-procedure sendRoutingInfo (really has to be written this way) executes the task via C-interface, already since the implementation of GSM. But in case of the mobile network provider, here is the first modification: If the called

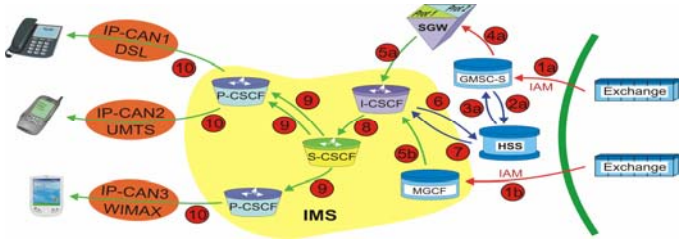

Figure: Possible handling of incoming calls in the IMS

participant is attainable only via IMS or primary is to be called by the IMS, the HSS does not give a VLR-entry, which would be the case with GSM-, or UMTS-registered members. Here the HSS cannot search for the provision of

so-called MSRN which makes possible the transmission to the GSM- /UMTS-network of the call to the "serving" VLR, in general.

This is not a big problem. There have always been GSM and UMTS not registered (disconnected) users and for these the call is being forwarded to the mailbox optionally. According to this, among other things there is one data set entry for the responsible mailbox with respect to each user-profile in the HSS. The necessary modification is to make a new data set entry for the responsible I-CSCF in the HSS additionally to the mailbox-entry. This can be done statically, this means, the I-CSCF or their address (as "Host Name Address") is preset or the load is shared amongst different I-CSCFs. Bullet 3 shows how the MAP: sendRoutingInfo answers and hands over the identification of the I-CSSF to the GMSC.

The next modification is demonstrated by the marked message in bullet 4 a. The GMSC transfers the IAM-message together with the address of the I.CSCF to a most-likely intern SGW which transforms the E.213 number of the participant to the so-called TEL-URI. According to our example, mentioned above: +49-171-540-7090 becomes "phone: +49-171-540-7090".

The SGW transfers the ISUP: IAM-massage with help of this information into a SIP: INVITE-message, which is shown in *bullet 5a*. Here we have to pay our attention to the b-variant, below in figure 1. The MGCF of the land-line network provider or the Greenfield-operator receives an ISUP: IAM-message *(bullet 1b)* as well, however for the E.213-number: +49-721-957829-0.

The MGCF does not need a HSS-application but rather translates by itself the E.213-number into a TEL-URI and forwards the application to an I-CSCF to the IMS. Here the a- and b-variant converges and we return to the described procedures from bullet 6 onward.

The exchange of information, bullet 6 and 7, deal with the DIAMETER: LIR/LIA-procedure which is described in 3GTS 29.229 (6.1.5 and 6.1.6). Basically the address of S-CSCF is asked through the I-CSCF and from the HSS.

So the I-CSCF can route the received SIP: INVITE-message for "tel: +49-171-540-7090" or "tel. +49-721-9577829-0" to the responsible S-CSCF *(bullet 8).*

The S-CSCF analyses where the user is registered and forwards the SIP: INVITE-message to three terminal-equipments which have to be reached via two different P-CSCFs *(bullet 9).* Finally the application reaches the end-user or on his end-terminal: In the presented case *(bullet 9)*, three terminal-equipments ring at the same time. This is called "Simultaneous Forking".
Alternatively these three terminal-equipments can be called one after another, e. g. by 30 seconds ringing before it switched further ("Sequential Forking"). This must be configured by S-CSCF. As already mentioned, it is sort of a proposal for the resolution of the problem. We would like to outline again that this proposal is not yet standardised. And also we want to point out some advantages of this resolution:

The already integrated GMSC with SGW will switch ISUP to SIP and then so to IP. The data part which is not displayed for the actual speech is transformed from the associated MGW to VoIP.

This advantage is especially important if a so-called "Hosted IMS" variant is used, whereas, the IMS of the operating company geographically and politically is somewhere else then its network.

The necessary modifications at the existing architecture are fractional. For the I-CSCF the incoming SIP: INVITE-message appears just like every other VoIP-call application.

Resolution approach for problem 2: "Availability from real-time QoS in the access network (IP-CAN)" and 4: "Availability from every access network".

Again for repetition: Problem 2 results the expectations of the client, that to be able to communicate and other real-time-services effectively. Problem 4 aggravates possible methods of resolution by the expectations of the client who can use IP-based services from every IP-based access network. Best example: The client comes home, and wants to change his WLAN-compliant mobile phone from the expensive GSM/GPRS access to WLAN and wants to be called via WLAN.

To clarify at the beginning: For problem 2 in connection with problem 4, in principle there is no real technical solution for the solution of problem 1.

But you can suggest the following recommendation to the operator, which may not solve the problem but also not let it affected.

You should allow your client to access from optional access-network after you have demerged your charging infrastructure!

This demerger must be comprised of the division of charges in pure access (Access Network Charges) and services (Service based Charges).

If the client uses only one access-network of the IMS-operator with "QoS-Awareness", accordingly, the higher costs are to be charged as if the available "Best Effort"-WLAN/DSL-network is used by any ISP.

Advantage: The client cannot hold the operator responsible for possible quality defects at the end.

This statement does not mean that the IMS-operator no longer run its own access-network. But it allows that the IMS-service provider and the provider of the one or other access-network are two independent corporates.

The following advantages results from political reasons for the operator:

Towards the customer rather pro-active instead of strict behaviour is signalled which is always remunerated by the market.

The operator does not need to discuss and validate countless MoUs with access-network-operators for to guarantee their QoS and other skills. Administrative costs and other expenses are minimised. At the end, it has to be pointed out that

the access of IMS from optional access-networks shows other difficulties and other holes in the security areas, which are mentioned below (approach to solve problems 4a, 5 and 6).

Resolution approach for problem 3: Interoperability: As mentioned in the previous edition the problem 3 results in, a) the installation from IMS-resolutions with at least proprietary parts and procedures; b) considerable differences between the underlying standards. The point (b) must be again split into different IMS-standards, like e. g. TISPAN, 3GPP, 3GPP2 and different protocol-standards in the domain of end terminals. The last point addresses particular to the protocols SIP and SDP, which in the meantime differ considerably from the generic IETF-SIP/SDP and the different IMS-SIP/SDP-versions. As an example, the decisive questions are:

Does my terminal-equipment function at operator B even if originally used at operator A?

Can I connect my terminal-equipment via the access-network of my previous operator A to the IMS of my new operator B?

The last point shall receive attention because in such cases the MoUs and technical agreements are required for the synchronisation between the IMS-operators.

The proposed solution in figure 2 concentrates on the first two mentioned problems, that is, communication between terminal-equipment and IMS. The web server (http) is in the centre, which is provided and operated by IMS-operators. This web server is used to transport and install configuration data from the operator to the end terminal. The solution becomes possible by the fact that IMS-roaming is indeed technically possible but this does not necessarily have to be in real. But already at the configuration of the terminal-equipment you can guarantee that a P-CSCF is always used in the home-IMS. The S-CSCF is anyway always at the home-IMS. However, there is a disadvantage which is connected directly with the problem of usage of the access-network: To achieve QoS from the access-network it is usually required to have a so-called “Policing” of the requested QoS, e. g. an edge-router or the GGSN on one side along the parts which were mentioned in the first part of this article and the PDF on the other side. If this has to function then MoUs are required, that is mentioned previously.

Resolution approach for problems 4a: ”Utilisation of NAT/NAPT in IP-CAN”; 5: “Intrusion and DoS-attacks against the IMS”; 6: “Identification and authentication of the end customer or the end terminal” and 7: “IPv4- or IPv6-addresses?”

Again a short repetition from the first part for a better understanding: The topic NAT/NAPT is extremely critical at the application of SIP/SDP because the embedded private IP-addresses after the “NATing” and outside of the private network are useless, e. g. for registration or for routing of data. There are some further problems between SIP/SDP and NAT/NAPT which cannot be focused here.

The presented problems related to security in problem 5 are mainly applied when the IMS is opened for any access-networks.

Problem 6 comes in action when the used end terminals are without SIM. Actually problem 6 always exists if a number of “Credentials” of the client for the authentication should have to be used.

Problem 7 describes the difficulty, if a UA has to support both, IPv4 or IPv6. And here is the surprise: All these problems can be handled by only one extension: The utilisation EAP-based authen-

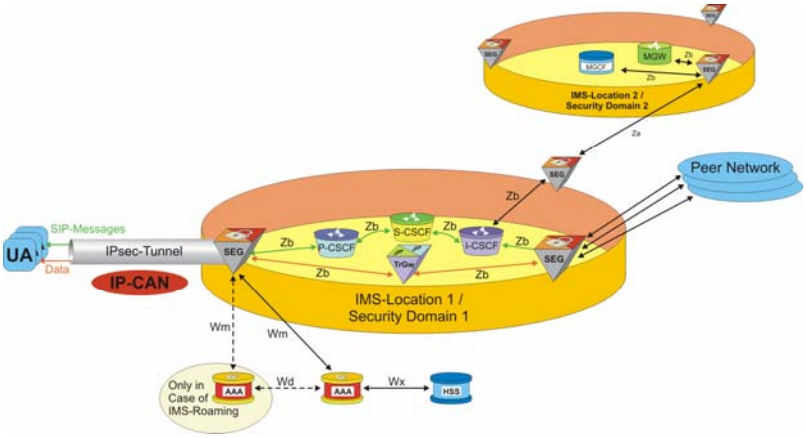

Figure 3: IMS with entire reconstructed IPsec-safety-architecture

tication-method. The basic standardised generic system-architecture is presented in figure 3. It shows the ancient open IMS as “Gaelic village” with wall and IPsec-based SEGs as watch-tower.

For our view, essential is the IPsec-tunnel between the SEG displayed on the left and the user agent. It could be argued that the IPsec- tunnel between the UA and IMS has already been part of the 3GPP-release 5 standard to the IMS. This is correct, however with the following limitations: According to 3GPP the establishment of an IPsec-tunnel between IMS and UA requires first of all the presence of a USIM at the client or in the registered end terminal equipment. Secondly this established IPsec-tunnel is 3GPP-specefic not generic and – very important – it is built up between the P-CSCF and the UA. What does that mean? It is easy: The DoS-attack which was presented in the first part will not be prevented from the 3GPP standardised procedure!

Quite different to the procedure which is illustrated here: The IPsec- tunnel is built-on between the UA and a SEG before the UA is allowed to correspond via SIP with the P-CSCF, generally. SEGs are immune against DoS-attacks innately. The setup of the IPsec-tunnel between UA and SEG is

done, shown in figure 4, on the basis of IKEv2-procedure, accordingly.

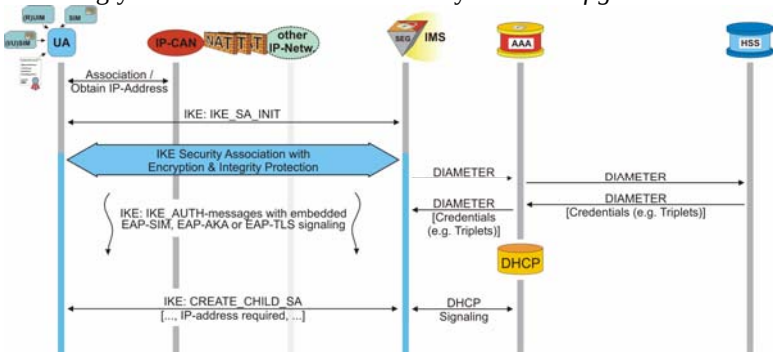

Figure 4: Overview of IKEv2-procedure used at IMS (part 1 of 2)

The detailed explanation of IKEv2-procedure would go beyond the scope here, but the following important details in figure 4 should be referred:

At the UA side (on the left at the top at figure 4), IKEv2 allows the use of every kind of "credentials" for the authentication. So the problem of the absolute SIM-based authentication is solved.

The UA or the used IP-module (e. g. WLAN- or Ethernet-card, UMTS-card …) is connected to the local IP-based access-network long before the start of IKEv2 and receives probably a private IP-address.

From start of the IKEv2-procedure the UA, at first, identifies via DNS the IP-address of SEG and afterwards installs a quite secure IKE-Security association via Diffie-Helman.

After having protected against eavesdropping, below the blue double-headed arrow, starts already encrypted the real authentication using the EAP-method. Every type of "credential" can be supported here, this is pure configuration, and the method itself does not change at all.

Very important: For the success of the presented procedure that it does not matter how many NAT/NAPT-routers are between UA and SEG. And, please recapitulate: Until now there were no SIP-messages sent or received.

However, the EAP-based authentication ends in any case with the generation of digital key-material, which is used for the coding in the real IPsec-tunnel (tunnel-modus and ESP), that is established and as shown at the very bottom in *figure 4*. The eminent fact is that the establishment of the IPsec-tunnel give the UA the possibility to get an own IP-address from the IMS. This is obviously done to solve the problems related to NAT/NAPT issues, which will be shown in figure 5.

At the same time you can settle the problem 7 that which type of IP-address should be provided within the UA. An operator can define e. g. that all its UAs should always use IPv6. This can be realised with the help of IKEv2. The NIC for the pure preparation of IP-connectivity, which lays under the UA, is decoupled from the actual UA or the higher layer.

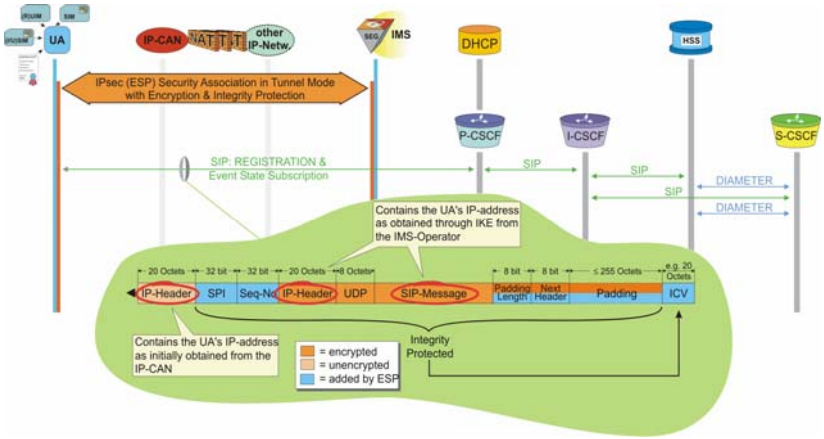

Figure 5: Overview of IKEv2-procedure which is used at the IMS (part 2 of 2) and frame structure of ESP-tunnel

After establishing the IPsec-tunnel (tunnel-modus / ESP), all information which is sent in the tunnel are authenticated, i. e. they are checked for changes. This will be done with help of the ICV at the end of such a tunnel. Very important is the fact that the frame parts displayed in orange colour, in figure 5, are additionally encoded.

Related to this security, the necessity of a SIP-based authentication via the IMS is lost.

As displayed, the SIP-messages can be packed inside UDP/IP-frames and with the IP-addresses provided by the IMS, the UA on one side and on the other side the P-CSCF can be identified. Certainly because of encryption now no one can listen in-between the UA and the IMS.

These inner IP-frames are entirely encoded via IPsec and extended with an incremental sequence number and a pointer (SPI). For this frame the ICV is calculated and attached.

Afterwards, the whole structure will be packed in to the external IP-frame which uses the IP-addresses as private IP-addresses of the UA as well as of the SGW.

The same tunnel in-between UA and P-CSCF is used for data-transfer as well which reduces the complexity in the area of security and NAT/NAPT-issues, essentially.

If you want to be on the safe side, you can additionally embed the ESP-frame (starting with SPI) in the UDP (accordingly to RFC 3948) to avoid rejection of the entire IP-frame at old NAT/NAPT-routers. Finally we want to mention the following advantages of the presented procedure: IKEv2 has its own NAT/NAPT-identification-system which can be used, e. g., to trigger an IKEv2-own "Keep-Alive" between UA and SEG. So it can be avoided that the NAT/NAPT-

routers which are located between UA and SEG delete the association between private and public IP-addresses and port-numbers. IKEv2 is the preliminary stage to the so-called MOBIKE (RFC 4555). In opposite to IKEv2, MOBIKE allows even the uninterruptible switching of the IPsec-tunnel to another IP-CAN, e. g. from WLAND/DSL to WIMAX or UMTS. Finally, because of this you can raise the mobility-management to the IP-level.