3GPP TSG SA WG3 Security — S3#31 **S3-030727**
18 - 21 November 2003
Munich, Germany

1. Introduction

During SA3#30 meeting, the Rel-5 IMS interworking has been agreed (Figure 1, the blue part) and the read part is agreed to be resolved for Rel-6 network. According to [1], the interface between CSCFs and an IP multimedia network is called Mm interface.

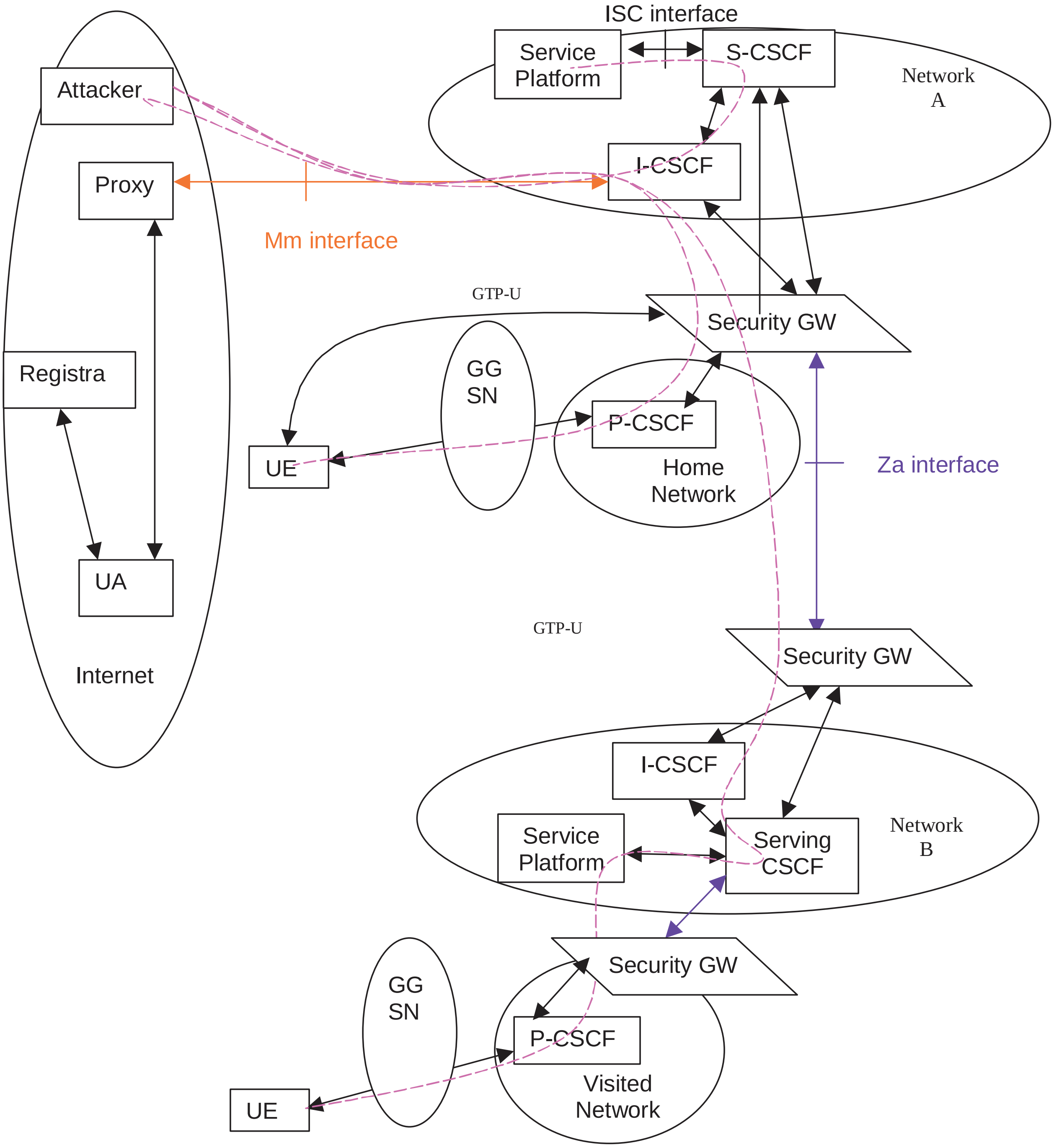

Figure 1: IMS topology with Rel-5 and Rel-6

Note: For simplicity reason, only connection between I-CSCF and Proxy is drawn in Figure 1. In fact, both I-CSCF and S-CSCF connect with Proxy for SIP routing. Thus the consideration is conceptually the same as for CSCFs.

For the REL-5, NDS guarantees an operator's IMS is behind a Security GW, so all SIP traffic cross the border of the operator's network will be protected by IPsec. Therefor it is reasonable assumption that if the operators IMS are interworking via Secure GWs, then the trusted relation is established. In other words, the connectivity equals to the trust relation. This was agreed for REL-5.

2. Privacy reflecting to the network topology

RFC3325 requires that network inserts the P-Asserted-Id header to inform the whole trusted network domain about client's identity. This P-Asserted-Id header must be removed at the edge of the trusted network. It involves two concerns: should the SIP hop remove the P-Asserted-Id before deliver to next hop, and should the SIP hop trust the P-Asserted-Id from previous hop. Therefore the issue behind is about the trust relationship of the two interoperating networks and the provision mechanism of it.

In REL-5 IMS network, according to the agreed CR (S3-030648) the S-CSCF will not remove any P-Asserted-Id header if Privacy 'id' is required by UE. Instead, the S-CSCF will simply forward the whole SIP message to the destination. If there is no Secure GW available, the whole message is simply dropped. As a consequence a REL-5 IMS SIP network hop will always trust the P-Asserted-Id from previous hop.

For REL-6, the S-CSCF may not maintain a Security GW with Internet SIP provider, therefore the solution for REL-5 is not compliant. New solutions must be discovered to resolve the concerns, with consideration of backword compatibility of REL-5.

3. Situation in Rel-6

3.1 The specifications in other working groups

- SA2 23.228 v6.3.0, section 5.4.2, regarding to interworking with Internet.

- CN3 TR 29.962 v6.0.0, Signalling interworking between the 3GPP profile of the Session Initiation Protocol (SIP) and non-3GPP SIP usage. This TR was approved at NP#20. The specification studies how the session setup from calling 3GPP UA towards called non-3GPP UA, and the other way round.

- TR 22.800 v6.0.0, IP Multimedia Subsystem (IMS) subscription and access scenarios. The TR was approved in SA#21 as v2.0.0 and copied to be v6.0.0.

3.2 Security analysis of Rel-6

For the REL-6, the network topology turned to be complicated when interworking with non-IMS SIP service providers (see Figure 1 read part). The Mm interface provides connectivity to IMS, meanwhile it also introduces a new data path behind the Security GW, thus beyond the protection of Security GW offering. The closed edge of REL-5 is opened in REL-6. Obviously, the opennes should not affect the established REL-5 networking, thus as **the first level of security**, CSCFs need to differentiate the traffic from non-IMS networks and that from IMS networks, for latter one is trusted while the former one is not. So the REQ1 is:

1. *I-CSCF shall be able to differentiate the traffic from non-IMS networks and that from IMS networks.*

Suppose no any other security mechanism deployed over the Mm interface, attackers reside in the Internet have opportunity to launch all kinds of attacks, such as DoS, spamming of SIP message (see

Figure 1, pathes in pink dash line). As the counter-measure, Firewall should be deployed in front of CSCFs to block these unsolicited traffic.

But Firewall is seen insufficient solution against many other attacks. An attacker may spoof the source IP address, impersonate a valid UA reside in a non-IMS network, and send BYE to terminate an on-going session between the UA and a UE in IMS.

To prevent these attacks, we need to guarantee that source of the traffic is as claimed to be, and whether have the data been moliciously modified. Thus the security is improved to **the second level**, so that IMS network should be able to protect any IMS traffic against traffic from Mm interface.

It suggests the protection for the Mm interface. This would require that

2. *The two network elements communicating with each other can authenticate each other as who they claimed to be*
3. *The SIP traffic over the interface can be integrity protected for receiver to identify any unwilling manipulation*
4. *(Optionally) the confidentiality should be provided to protect the privacy of the data*

The REQ2-4 can guarantee who is the sender and receiver; are data authenticated from the sender, but they do not guarantee the trust relation. Therefore additionally **service agreement** mayb be enforced between the IMS provider and the Internet SIP service providers as **the third level of security**. This agreement is then deployed as the policy of trustness, to distwinguish the two sides from other IMS and Internet SIP service providers. This agreement can strengen the reqirement 2 by adding requirement 5:

5. The service agreement shall be possible to enforce the trust relationship

3.3 Further remarks

The REQ2-4 provides the authenticity of the end entity as well as the data. Thus, CSCFs can distwinguish the source of the Mm traffice from rest of IMS. In other wods, fulfilling the REQ2-4 will automatically fulfil the REQ1. On the other hand, REQ2-4 would impose the requirements on to the non-IMS network as well, which may be not always feasible.

The REQ5 is to enhance the trust relation. It extends the area of a trust network, thus privacy can be handled based on the existance of REQ5. However, REQ2-4 as the provision means of the trustness, can not be replaced by REQ5.

4. Solutions for first level protection over Mm interface

There are a few potential solutions for first level protection, relying on IP address and network topology.

1. Using the ingress filter function in router sitting on border of IMS. Set the CSCFs with multiple IP interfaces, one (IP_CSCF1) for IMS and one (IP_CSCF2) for non-IMS, so that only the topologically correct package will pass to the CSCFs directly. If the destination is (IP_CSCF1), it will be always forwarded to the Security GW for processing.

This suggests that CSCFs must hide the IMS inner IP interface from the outside world so the DNS query will not reveal the internal IP address.

Inner router will not connect to border router.

2. Deploying Zb interface, thus router requirement would be dismissed.

3. Deploying NAT.

5. Solutions for second level protection over Mm interface

Three alternatives are discussed in this section as potential solution for second level protection.

5.1 TLS session

TLS provides transport-layer security over connection-oriented protocols such as TCP. A RFC3261 compliant SIP proxy would support TLS implementation, as well as both TCP and UDP (a MUST requirement). So for a session initiated over UDP, nobody blocks a proxy or CSCFs to convert transport to TCP, i.e. always use TCP towards another proxy. If the proxy indicates its URI as a sips URI, this would then be stored in the DNS (to declare its capability) and could be resolved by NAPTR / SRV [2] records to indicate the domain should be reached only through TLS.

In SIP RFC3261 [3], it reads:
"A SIPS URI can be used as an address-of-record for a particular user - the URI by which the user is canonically known (on their business cards, in the From header field of their requests, in the To headerfield of REGISTER requests). When used as the Request-URI of a request, the SIPS scheme signifies that each hop over which the request is forwarded, until the request reaches the SIP entity responsible for the domain portion of the Request-URI, must be secured with TLS; once it reaches the domain in question it is handled in accordance with local security and routing policy, quite possibly using TLS for any last hop to a UAS. When used by the originator of a request (as would be the case if they employed a SIPS URI as the address-of-record of the target), SIPS dictates that the entire request path to the target domain be so secured."

The paragraph tries to convey the idea that a sips request should traverse over TLS to the home domain; after that it is then up to the home domain (and user in question) how to route the request. For instance, if an Internet UA makes a call to <sips:IMPU@operator.com>, then the UA uses TLS to send INVITE request to his outbound proxy, and the outbound proxy use TLS to send INVITE to icscf.operator.net. Next the icscf.operator.com can use UDP, TCP or TLS to send the INVITE to the phone that IMPU resides.

In SIP RFC3261 [3], it also means a detail regarding to ciphersuite usage of TLS for SIP security:

"The use of SIPS in particular entails that mutual TLS authentication SHOULD be employed, as SHOULD the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA. Certificates received in the authentication process SHOULD be validated with root certificates held by the client; failure to validate a certificate SHOULD result in the failure of the request."
Note, the TLS allows not only the multiple SIP sessions transported over a single TLS, but it also allows the session resumption. Thus, within the lifetime of a session defined in policy, no need to do certificate calculation as described above.

5.1.1 Handling Privacy

In case REQ5 is presenting, the CSCFs can maintain a list of trusted domain names. Handling Privacy will rely on the list. Otherwise the connectivity based on TLS will be sufficient to handle the P-Asserted-id header. There is no need to maintaint the IP address of them, since the domain names are provided in TLS handshaking phase.

5.1.2 Rel-5 backword compatibility

A RREL-5 UA will still initiate INVITE session towards to a foreign UA via sip:ua@foreign.com. This accessing security is protected with IPsec as defined in REL-5. Then the outbound CSCF will contact the foreign domain by TLS. Since the termination point of TLS is in CSCF, there is no problem to distwinguish traffic between Mm interface and that from Security GW.

5.2 IPsec tunnel

An obvious solution is to provide IPsec tunnel over Mm interface, similar as the Secure GW. For example the Proxy in the Internet cloud can run a IPsec tunnel towards the I-CSCF.

In this case, multiple SAs and policy are stored in local IPsec tunnel database:

Source IP address	Destination IP address	Policy
I-CSCF (A) IP_addr1	S-CSCF (B)	process
I-CSCF (A) IP_addr2	Proxy (Internet)	process
S-CSCF (A)	S-CSCF (B)	process
S-CSCF (A)	I-CSCF (B)	process

Note: the table shows uni-direction traffic; the other direction applies same principle.

5.2.1 Handling privacy

For the next hop forwarding, the CSCF needs to understand the domain name of destination, and making the DNS query for the IP address. Meanwhile if the REQ5 presents, the I-CSCF **needs to check the domain name** is among the **trusted partners**, and removes/keep the P-Asserted-id header accordingly. Next is to send the SIP package to IPsec tunnel or Secure GW for IPsec processing.

For the message received from previous hop, the CSCFs can check against the SPD list associated with domain name of the trusted partners. If it is on the list, then I-CSCF is confident to the message and the P-Asserted-Id header; otherwise I-CSCF should remove the header.

The two checking suggest that CSCFs contain a Service partner table:

Trusted partner (domain name)	IP address a.b.x.x range

5.2.2 Rel-5 compatibility

The REL-5 compatibility is solved. The network B (in Figure 1) that does not have interoperation with Interenet, would pass data over the SAs that are ended in IMS only (In this scenario, network A, the REL-6 IMS).

The certificate may be used to authenticate two end points before IPsec tunnel is established and refreshed. The domain name (or DNS name) stored in the certificate would be checked against the I-CSCF locally stored service partner list.

5.3 S/MIME

SIP deployes S/MIME to protect a SIP message in 3 modes: Payload only, Tunneling and Sipfrag [4]. Figure 2 shows a scenario of a received SIP message using S/MIME protection in either tunneling or sipfrag mode. In particular, message authenticity and integrity protection are selected by the sending party, using either detached signature or SignedData. The message consists of the outer SIP headers, an inner SIP message or sipfrag, and a signature. An inner SIP message contains both headers and payload, while a sipfrag contains headers but may or may not contain payload.

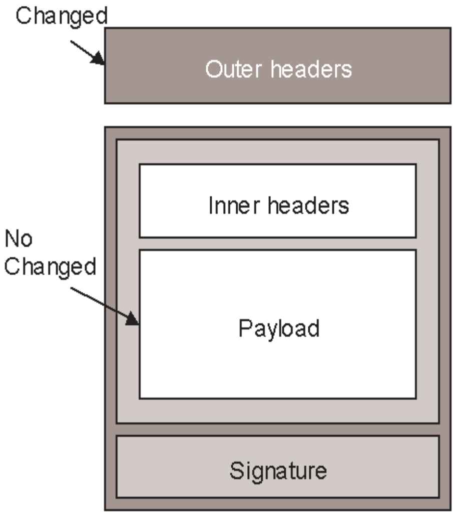

Figure 2: Scenario of a received SIP message using S/MIME

The Payload only mode does not help to solve the privacy issue, because the SIP headers shown initiator's identity are in plain text.

If tunneling mode or sipfrag is used, there will be both an inner and outer versions for certain headers. The inner headers refer to those headers that are being protected by S/MIME, while the outer headers are the headers of the wrapper, which can be read and modified by SIP proxies. These headers are Route, Record-route, Path, Via, Service-Route. Inner headers are supposed to be read only by the endpoints. Obviously the Privacy header (P-Preferred-Identity by UE) cannot be inserted into the Inner header; since it has to be deleted at the edge of a trust domain.

If we assume that IMS CSCF will process S/MIME towards non-IMS network Proxy or UA, it suggests that

- It breaks the end-to-end usage of S/MIME.
- CSCF needs to update S/MIME functionality.
- CSCF needs to exchange the certificate with the other non-IMS SIP entity. This function brings pros and cons. Maintaining certificate is a pain, but certificate can also indicate the domain name and the strongly bind with service agreement by using another secured channel for the exchange of certificates.
- Processing of S/MIME is per SIP message work load. The handling of P-Asserted-Id to next/previous hop in S-CSCF shall be based on the domain name and that in the certificate.

If the sipfrag is used end-to-end between UE and non-IMS UA, the implications are here:

- UE has to support S/MIME
- CSCFs have to support S/MIME
- Double/triple protection in IMS accessing
- IMS Subscriber's Certificate required
- Full PKI and CA required

5.4 External identity provision and corresponding transport used

It is possible for 3GPP to use some external identity provision mechanism. For example the Liberty Alliance could rely on 3GPP provided identity for non-3gpp network, and vice versa. The detail and the corresponding transport are yet for further studying.

Conclusion: From the analysis in last section, it looks like that TLS based solution suites most to current network topology, compared to other mechanisms. Next choice would be IPsec tunnel. And S/MIME is the 3rd preference.

6. Specifications for security mechanisms placeholder

It is clearly that SA3 should consider further work to cover the interworking with non-IMS networks in REL-6 timeframe. Two alternatives are potentially workable:

- Expand TS 33.210 NDS/IP to REL-6, and cover the interworking mechanisms there, no matter what solution is chosen;
- initiate a new TS covering the interworking mechanisms.

As there are many specifications initiated by SA3, it is suggested to continue progress the issue in NDS/IP TS to REL-6.

7. Proposal

There is only 2 SA3 meetings (including this one) before the REL-6 frozen deadline. To save the time, this meeting is proposed to endorse the conclusions below:

1. SA3 should decide the levels of security listed in section 3, and the security requirements associated with, for REL-6.
2. The NDS/IP TS 33.210 is proposed to cover the first level security in the informative annex
3. TLS is proposed to resolve the second level of security for interworking scenario with non-IMS as the baseline for further development.

8. REFERENCE

[1] TS 23.002, v 6.2.0.

[2] "Session Initiation Protocol (SIP): Locating SIP Servers", J. Rosenberg, H. Schulzrinne. RFC3263, IETF.

[3] "Session Initiation Protocol (SIP)", J. Rosenberg, et. Al. RFC3261, IETF.

[4] Internet Media Type message/sipfrag, R. Sparks. RFC3420.