3GPP TSG SA WG3 Security — S3#34 **S3-040558**

July 6 - 9, 2004

Acapulco, Mexico

Source:	**Nokia**
Title:	**Authenticating the CSCF peer in a hybrid network (IMS and non-IMS interworking)**
Document for:	Discussion/Decision
Release:	**Rel-6**
Agenda Item:	IMS

1. Background

During SA3#33 meeting in Beijing, an issue about authenticating the CSCF peer in a Rel-6 IMS was raised. Concern was also raised why not to re-use the available Rel-5 IMS to IMS internetwork signalling. Later on in the meeting, an action was allocated to Nokia, to lead the further discussion by email to resolve the issue. The mail started on 24th May and ended on 11th June.

During the discussion a few questions and new proposal, were raised:

Q1 what outstanding specification work would the TLS certificates mean to 3GPP network if using TLS as solution? TLS certificates enrollment and revocation, TLS certificate profiling? Would the work complete within Rel-6 timeframe?
Q2: To what extend will SA3 be able to re-use NDS/AF ideas for TLS?

This paper is a follow-up work, for resolving the questions above in section 3, on privacy handling of Rel-6 IMS. And a proposal was made by T-mobile, why not to use a trust peer table in each CSCF to indicate the security mechanism should be used (NDS/IP or TLS). This is analyzed in the end of section 2.

It is worth of noting that problem present here is bigger than privacy handling. **It is the fundamental issue on how to authenticating the CSCF peer in a hybrid network, based on which the privacy is handled.**

2. The Problem description

Before we move on to the justification of the solutions and issues, may be the problem should be re-visited in this section.

Current security mechanism for Rel-5 IMS is to use connectivity of Security Gateway (SEG). This was introduced in Povoa meeting with a CR to section 5.3 of TS33.203:

"NOTE 2: In particular when a SIP message is routed through the SEG towards an IP address, which is not operating the Za interface, i.e. there is no SA available in the SEG for applying IPsec ESP the SEG will, in compliance with TS 33.210 [5], drop the packet."

In other words, between the SIP peers there isn't direct authentication; the interworking is based on SEGs pre-shared key for SA establishment. The Rel-5 IMS does not attempt to understand the other end; it just blindly trusts all inter-connected networks based on the presence of the SEG. In case of a compromised network (CSCF or SEG) sending malicious traffic (e.g. impersonate others in SIP layer, not IP layer), the destination CSCF has no possibility to detect the attack. In short, the NDS/IP only provides the protection to the signalling, but it doesn't help a Rel-6 CSCF to recognize the existence of trust relationship, i.e. it doesn't provide means to logic judgement whether the received SIP message is trustful.

In the Rel-6 hybrid IMS network, the non-IMS interworks with a CSCF by using TLS. If one of the SIP peer does not support TLS, then the path shall transfer unprotected SIP message. Figure 1 depicts the whole architecture.

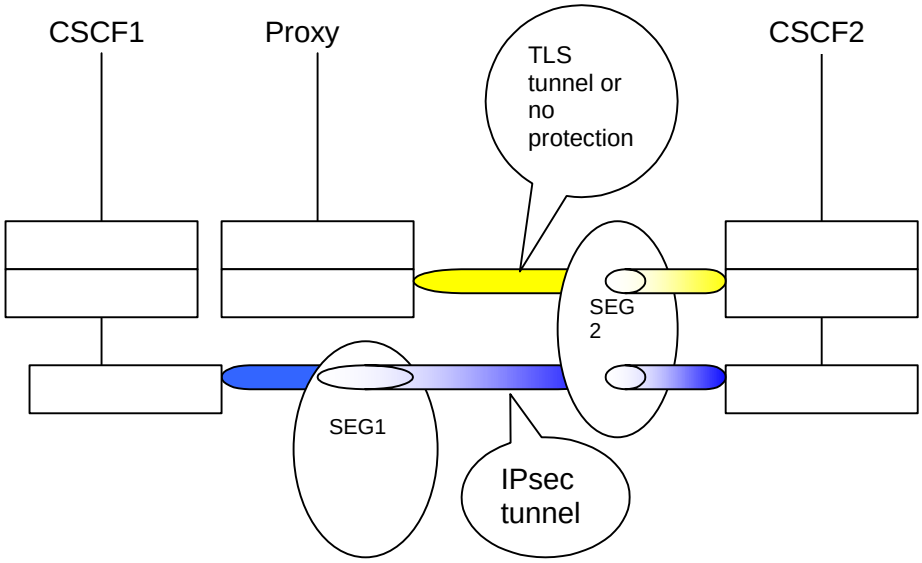

Figure 1: The hybrid mode of IMS interworking in Rel-6 environment

Note in the yellow tunnel, due to the usage of SEG2 which is in different layer as the transport layer (SIP), the destination CSCF cannot detect the SIP message is unprotected. This opens a hole for a proxy to impersonate other SIP peer, not only the non-IMS SIP peer, but also the IMS SIP peer CSCF1, towards the destination CSCF2. For example, the proxy can spoof an IP address (for hiding its identity), and send an unprotected SIP message with source of an IMS CSCF1, via SEG2. In such a way, the attack affects also to the Rel-5 IMS security, which demonstrates that the NOTE in section 6.5 of TS33.203 is insufficient. It reads below:

"NOTE 2: The security mechanism between the CSCFs within IMS is covered by NDS/IP security specified in TS 33.210 [5]."

Similarly, suppose the proxy is not malicious, but just sending SIP traffic without TLS (because it does not support TLS) protection, how could the destination CSCF2 do to identify whether the message comes from an IMS or a foreign network and whether it is protected or not? Note from the capability announcement (DNS), there is no way to differentiate that non-IMS network proxy with the IMS network CSCF1 which supports SEG but not TLS.

When the message flow is the other way around, i.e. the CSCF2 sending message to the proxy, problem is still present. If a non-IMS proxy does support TLS, then everything is fine over Mm interface. But if it doesn't, there should be still the means to interwork with IMS using SEG, and unprotected mechanism if policy allows. In former case the SIP message should be still trusted and privacy of SIP is passed to that network till the edge of it; in later case, the SIP message should not be trusted (In current section 6.5 of TS33.203, it is still allowed not to use TLS.). Unfortunately, there seems to be no way the CSCF2 can conclude whether the destination/source is an IMS or non-IMS network, if the non-IMS proxy doesn't support TLS.

One possible solution by re-using SEG, is to maintain an IP address table in each CSCF, suggesting the destination/source IP address is an IMS trusted entity. As a solution it was already identified in Nokia's earlier contribution [S3-030565]. But the difficulty was also highlighted, since the CSCF has to check every SIP message's IP address against the table. Note it is not sufficient to maintain a table of SIP domain names and the security mechanism needed, because it doesn't help in case

- when receiving a SIP message, it is stated from an IMS domain; there is no mean to detect it was really protected by SEG

- when sending a SIP message with only IP address in SIP header

As a summary of the problem, **in a hybrid interworking topology, the currently specified SEG mechanism is not sufficient** to guarantee a CSCF whether the destination/source is an IMS or non-IMS network before any protection is deployed. New solution is needed for interworking of IMS networks so as to identify the trust relationship with the other end.

3. The general solution for interworking

This section provides a solution to the issue presented in section 2. We propose to use TLS as general solution, not only for non-IMS but also for IMS, for authenticating the SIP peer, because TLS works end-to-end, and therefore solves the issue best way.

Let's take a look on how the solution works for Mm interface. This is specified in TS 33.203 section 6.5. An IMS CSCF first discovers the TLS capability of a SIP proxy before connection is established. If the TLS is not supported in the next hop, then the network is untrusted. If TLS is supported, the IMS SIP CSCF requests a certificate from the other SIP proxy. And once the TLS connection is established, the IMS can tell that the other end is trusted. Therefore the user required privacy could be handled accordingly.

Similarly the TLS is proposed for IMS interworking. If the request is not received via TLS, the sender SIP CSCF is not trusted. If the request is sent via TLS, the IMS CSCF requests a certificate from the sending SIP proxy, and start handshaking. Each IMS network will configure the DNS NAPTR/SRV records. It needs to give higher preference to TLS over UDP, TCP, SCTP (or other transport protocols) for the SIP service the SIPs:(colon). This allows an IMS network to always try first TLS as a transport protocol.

As we demonstrated in section 2, a trusted peer list does not work smoothly with SEG solution. If it is IP address list, it shall introduce big operation overload; and if it is domain name list, it leaves several scenarios unsolved. On the other hand, the trust peer list can work together with TLS to provide finer granularity of trust relationship. This is due to the **binding of SIP peer's identity with the protection mechanism that is already supported by the TLS implementation.** When negotiating the TLS session the identity in the certificate must be stored for later on verifying against the application layer identity received. This verification is needed only once during a session, and is not required in further session resumption. Note, multiple SIP sessions can use the same TLS session simultaneously. In contrast, if the IPsec is used, the CSCF would need to check every message's IP address against the SIP layer address. We feel it is a more painful solution.

A list of IMS trusted domains could be based on signed interworking agreement. As the consequence, the CSCF when sending and receiving a SIP message, shall sort the domain name of the other end from the trust domain list, together with the security parameters visible in a certificate (e.g., certificate authority, common name or organization). The CSCF can identity an IMS that is not on the list as an untrusted network. Then the IMS SIP proxy verifies the certificate against the list of trusted networks, determining whether the sending SIP proxy is trusted or not. The same logic would work with non-IMS interworking scenario.

3.1 TLS PKI model

We propose to re-use the PKI model already specified in TS33.310 as much as it possible. To our understanding the maintenance of the certificate (enrolment and revocation list management, etc.) should be fairly similar in IPSec/IKE and TLS case.

Similar work has been done in WAP forum (today's OMA). WAP2.0 specifications are already used by 3GPP Presence service in TS33.141 for Presence server. We feel these specifications could be re-used here for TLS profile of the CSCF server as well.

4. Comparison between TLS and IPsec

This section analyses the cost of two solutions and their impact to the overall network deployment.

4.1 Implementation

We feel before Rel-5 is fully mature to be deployed, there is still a window to consider the other alternative. For cause of interworking with non-IMS network, the TLS function will be implemented to be part of Rel-6 IMS anyway. This implies that no function is wasted or duplicated in investment to CSCF if TLS is chosen.

SEG was established for general purpose of security protection. Originally SEG was used only to protect the GTP-C signalling, and by pass GTP-U where SIP message belongs. Later on due to the privacy of the SIP session, it was agreed to use SEG for SIP as well. It then extends the SA database in each SEG to several times bigger. Since the SA between each CSCF with another CSCF must be configured in the database, other than the GSN's SAs.

In TLS case, the trust relationship could be either purely based on usage of TLS and certificates, or maintained by a table of trusted peer's certificates. One could either pre-install them for later verification, or accumulated from each successful handshaking of TLS session.

4.2 NAT consideration

It is possible some of the non-IMS SIP node might be IPv4-only, also it is possible an IMS interworks with another Interim IMS network that is IPv4 only. In such cased, the IMS SIP needs to consider it, and especially address translation between networks. TLS passes IPv4 NAT (and IPv4/v6 NAT-PT) without problems, but IPSec requires that all the boxes between the nodes support IPSec NAT Traversal. The policy database and firewalls need careful configurations to support it. From this perspective, the TLS is a better choice.

4.3 IETF standard consideration

TLS is part of SIP security mechanism. Though IPsec is also mentioned in the RFC as hop-by-hop solution, a SIP entity must support TLS. We foresee the compatibility in this solution will be beneficial in long run.

5. Consideration of backward compatibility

When a Rel-6 IMS network interworking with Rel-5 IMS, clearly IPsec tunnel and SEG should be used. The receiving SEG needs to update the port number of the SIP messages. If there is interconnection agreement, then the privacy identity shall be forwarded and accepted. Otherwise the privacy identity shall be removed. We do not recommend this solution as it would request rather complicated function in SEG. It is recommended to use SEG for GTP-C related function, and apply TLS for IMS.

When a Rel-6 IMS networks passes SEG, the encryption could be still applied by the SEGs. TLS can negotiate null encryption end-to-end. The SEGs in between are supposed to know if IPSec encryption is required. This is another option. Due to the reason described in section 4, we do not recommend this way.

6. Suggested change over Rel-5 IMS Privacy

Based on the solution discussed in section 3, a proposal of change is shown below. There are two companion CRs, one is against TS33.210 v6.5.0, the other one is updated from S3-040429 (approved in last meeting) to add changes regarding to reference, and throughout the TS33.203 regarding to NDS/IP usage in IMS. It is also proposed in this CR to remove the editor's notes in section 5.6, and explain in a NOTE that the 'foreign network' to the general case applicable to both IMS and non-IMS interworking.

5.3 SIP Privacy ~~for IMS~~ when interworking with foreign Networks

Privacy may in many instances be equivalent with confidentiality i.e. to hide the information (using encryption and encryption keys) from all entities except those who are authorized to understand the information. The SIP Privacy Extensions for IMS Networks do not provide with such confidentiality. The purpose of the mechanism is rather to give an IMS subscriber the possibility to withhold certain identity information of the subscriber as specified in IETF RFC 3602 [22] and IETF RFC 3263 [23].

NOTE 1: It is useful that the privacy mechanism for IMS networks does not create states in the CSCFs other than the normal SIP states.

~~Editors' note: The exact mechanism for building the trust relation for privacy handling is ffs.~~

~~The IMS Network shall, from the Privacy function point of view, be a closed network by the implementation of Security Gateways for IMS signalling as defined in TS 33.210 [5].~~

~~NOTE 2: In particular when a SIP message is routed through the SEG towards an IP address, which is not operating the Za interface, i.e. there is no SA available in the SEG for applying IPsec ESP the SEG will, in compliance with TS 33.210 [5], drop the packet.~~

When a Rel-6 IMS interworking with a foreign network, the CSCF in IMS network shall decide the trust relation with the other end, based on whether the security mechanism for the interworking (cf. section 6.5) is applied as well

as the availability of an inter-working agreement. If the interworking network is not trusted, the privacy information shall be removed from the traffic towards to the foreign network. When receiving SIP signalling, the CSCF shall also verify if any privacy information is already contained. If the interworking network is not trusted, the information shall be removed by the CSCF, and retained otherwise.

7. Conclusion and proposal

We conclude that IPsec based tunnel is insufficient to resolve the authenticating issue in hybrid-mode of IMS in Rel-6. It is proposed to SA3 to identify the issue and endorse the main idea.