3GPP TSG SA WG3 Security — S3#21 **S3-010628**

November 26th– 30th, 2001

Sophia Antipolis, France

Source:	Ericsson
Title:	On Protection of IMS using NDS-IP
Document for:	Discussion/Decision
Agenda Item:	TBD

1. Scope

In the update information document of TS 33.210 v0.6.0, our TS rapporteur highliths, amongst others, this point for S3 to consider …

- o *Clause 7: IMS protection. We don't yet have any content for this section. Since there in general seems to be some confusion about the exact relationship between NDS/IP and aSIP, this clause could be important. Unless I see any other contributions for this clause when we draw nearer to S3#20 I will make an attempt myself.*

This contribution is the first attempt to introduce in TS 33.210 how NDS-IP procedures shall be applied in order to protect the IMS CN SS.

S3 members are kindly asked to review and discuss the proposed changes to 33.210 presented below and marked with change bars for an easier introduction into the spec.

2. Proposal

This contribution is the first attempt to introduce in TS 33.210 how NDS-IP procedures shall be applied in order to protect the IMS CN SS.

Find below a summary of this proposal …

- In order to concentrate all the IMS related information in one part of the specification, it is proposed that list of IMS protocols and interfaces (table 2 currently in chapter 4.4.1) is moved to chapter 7 where the rest of particularities related to NDS/IP aplication to IMS will be specified. This also applies to the list of GTP interfaces and protocols which is removed from chapter 4.4.1 and proposed to be moved to chapter 6 in another Ericsson contribution presented to this meeting.

  By doing this, it would be easy to move chapters 6 and 7 to annexes within 33.210 or even to other more suitable specifications (Chapter 7 on IMS moved to TS 33.203) as already proposed by other parties.

- Until this potential change on the structure of TS 33.210 is decided, proposed text in chapter 7 includes a reference to TS 33.203 where IMS security architecture and the working assumption of hop by hop protection are defined.

- Also a reference to 23.002, where ALL the interfaces related to IMS are specified, is included. It is Ericsson understanding that in order to provide a complete view on how IMS core network is protected with NDS/IP one should consider ALL its potential interfaces and not limit to Mm, Mw and Go as currently proposed.

  One could argue the value of the column ‘affected protocols‘ in this table, since most of them are SIP and some of them are not even selected. Regardless of this fact, this information might not be even relevant on how NDS/IP mechanisms are applied.

- Finally, due to the rather long list of IMS interfaces and the different NW configurations we may find, it is just proposed that IMS control plane traffic shall be routed through SEGs when it takes place between different security domains and in particular when it takes place between IMS operators domains.

  For example, SIP signalling over Mm interface between P-CSCF and I-CSCF will normally take place between IMS operators in roaming scenarios and SEGs shall be used in these cases. However, it is also possible that P-CSCF is controlled by the same HE-IMS operator. In this case, there is no need to route SIP signalling over SEGs.

  In the other hand it could be also possible that GGSN and P-CSCF, which belong to same Network operator, are phisically configured in different security domains. In this case it will be also possible to use the SEG infrastructure in order to protect control signalling between PS and IMS domains in the visited network.

  It shall be noted that this proposal is quite dependant on the definition of Security Domain.

3. Proposed Changes

4.4.1 Security domains and interfaces

The UMTS network domain shall be logically and physically divided into security domains. These control plane security domains may closely correspond to the core network of a single operator and shall be separated by means of security gateways.

The specific network domain security interfaces are found in table 1. The definitions for Zd, Ze and Zf only apply to NDS/MAP (TS33.200, [9]).

Table 1: Network domain security specific interfaces

Interface	Description	Network type
Za	Network domain security interface between SEGs. The interface is used for both the negotiation of security associations aiming at setting up ESP tunnels between SEGs and the protection of traffic within the negotiated ESP tunnels between SEGs (no third party negotiation).	IP
Zb	Network domain security interface between SEGs and NEs within the same network. The interface is used for both the negotiation of security associations aiming at setting up ESP tunnels between a NE and a SEG and the protection of traffic within the negotiated ESP tunnels.	IP
Zc	Network domain security interface between NEs within the same network. The interface is used for both the negotiation of security associations aiming at setting up ESP tunnels between NEs and the protection of traffic within the negotiated ESP tunnels.	IP

~~The interfaces, which affects/is affected by the network domain security specification, are described in the table below. Notice that when security protection is employed over an interface, this specification will refer to the Z-interface name.~~

~~Table 2: 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~~
~~Mw~~	~~Interface between CSCFs within the same network~~	~~SIP~~
~~Mm~~	~~Interface between CSCF and Multimedia IP network~~	~~SIP~~

7 Security protection of IMS protocols

~~[Editor's note: According to my noteds we agreed to add a clause to specify the IMS protocol protection.~~

~~Contribution to this clause is wanted!]~~

This section details how NDS/IP shall be used to protect IMS protocols and interfaces.

7.1 The need for security protection

The security architecture of the IP multimedia Core Network Subsystem (IM CN SS) is specified in 3G TS 33.203 [aSIP]. This specification, defines that the confidentiality and integrity protection for SIP-signaling is provided in a hop-by-hop fashion.

The first hop i.e. between the UE and the P-CSCF through the IM CN SS access network is protected by security mechanisms specified in [aSIP].

The other hops, within the IM CN SS core network including interfaces within same security domain or between different security domains are protected by NDS/IP security mechanisms as specified by this Technical specification.

TS 23.002 [x] specifies the different interfaces defined for IMS. Table X presents a list of IMS interfaces that shall be considered by NDS/IP.

Interface	**Description**	**Affected protocol**
Cx	Reference point between CSCF and HSS	DIAMETER
Dx	Reference point between SLF and I-CSCF	TBD
Go	Reference point between GGSN and PCF (P-CSCF)	COPS
Gi	Reference point between GGSN and P-CSCF	SIP
Mc	Reference point between MGCF and IM-MGW	H.248
Mg	Reference point between MGCF and CSCF	SIP
Mm	Reference point between CSCF and Multimedia IP network	SIP
Mr	Reference point between CSCF and MRFC	SIP
Mp	Reference point between MRFC and MRFP	H.248
Mw	Reference Point between CSCFs within the same network	SIP
Mi	Reference point between CSCF and BGCF	SIP
Mj	Reference point between BGCF and MGCF	SIP
Mk	Reference point between BGCF and BGCF	SIP
Sh	Reference point between HSS and Application Servers	TBD
Sr	Reference point between Application Server and MRFC	TBD
ISC	Reference point between Application Server and S-CSCF	SIP

Table X: IMS Interfaces that are affected by NDS/IP

7.2 Protection of IM CN SS protocols and interfaces

IMS control plane traffic shall be routed via a SEG when it takes place between different security domains (in particular over those interfaces that may take place between different IMS operator domains such as Mm, Mk, Mg and Sr). In order to do so, IMS operators shall implement/support/operate NDS/IP Zb interface towards a SEG within their own security domain and Za interface between SEGs.

It will for the IMS operator to decide whether to implement Zc interfaces or not in order to protect the IMS control plane traffic over those IMS interfaces within the same security domain.