Source:	Ericsson
Title:	On Protection of IMS using NDS-IP
Document for:	Discussion/Decision
Agenda Item:	7.2

1. Scope

This contribution incorporates the updates agreed during the discussion of Ericsson Tdoc S3-010628.

The main difference with this contribution and the original proposal in Tdoc S3-010628 is that list of affected IMS interfaces and protocols is omitted (reference to 23.002 was deemed to be enough with the exception of Gm interface between UE and P-CSCF which shall be protected with IMS measures provided at TS 33.203 instead).

It is left to the discretion of the TS rapporteur to further accommodate the proposed text in chapter 7 into a corresponding annex (annex B or C) as agreed during discussion of Tdoc S3-010582.

2. Proposed Changes

*****************************   *FRIST CHANGE*   *****************************

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

*************************** **NEXT CHANGE** ***************************

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 (IMS) 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 IMS access network (i.e. Gm reference point) is protected by security mechanisms specified in [aSIP].

The other hops, within the IMS 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 reference points defined for IMS.

7.2 Protection of IMS protocols and interfaces

IMS control plane traffic within the IMS core network 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 Za interface between SEGs.

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