

January 31<sup>st</sup>– February 1<sup>st</sup>, 2002

Antwerp, Belgium

---

**Source:** Ericsson  
**Title:** On Use of IPsec for SCTP  
**Document for:** Discussion/Decision  
**Agenda Item:** 5.5

---

## 1. Scope

DIAMETER will be the protocol used at Cx interface and N4 specifications relies in our NDS/IP security architecture in order to provide it with security. As per latest version of TS 29.229 ...

### **5.2 Diameter Base Protocol**

*With exceptions listed in the following subclauses the Diameter Base Protocol defined by IETF shall apply.*

#### **5.2.1 Securing Diameter Messages**

*For secure transport of Diameter messages, see TS 33.210 [6].*

...

#### **5.2.4 Transport protocol**

*Diameter messages over the Cx interface shall make use of SCTP.*

Also as per 29.229 (Subclause 5.2.4 above), N4 recently selected SCTP as the transport protocol for DIAMETER messages over the Cx interface.

IETF is currently working in an I-D which defines/optimised the use of IPsec with SCTP. "draft-ietf-ipsec-sctp-02.txt" (<http://www.ietf.org/internet-drafts/draft-ietf-ipsec-sctp-02.txt>) presents some considerations on the use of SCTP in conjunction with IPsec. In particular, it is discussed some additional support in the form of a new ID type in IKE [RFC2409] and some implementation choices in the IPsec processing to accommodate for the multiplicity of source and destination addresses associated with a single SCTP association.

This contribution proposes that our NDS/IP TS 33.210 refers to this piece of work in order to provide right guidelines for the optimal implementation and use of IPsec in affected NDS/IP interfaces and protocols.

## 2. Proposed Changes

\*\*\*\*\* *FRIST CHANGE* \*\*\*\*\*

---

### Annex C (normative): Security protection of IMS protocols

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

#### C.1 The need for security protection

The security architecture of the IP multimedia Core Network Subsystem (IMS) is specified in 3GPP TS 33.203 [10]. 3GPP TS 33.203 [10] defines that the confidentiality and integrity protection for SIP-signalling are 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 3GPP TS 33.203 [10].

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

3GPP TS 23.002 [3] specifies the different reference points defined for IMS.

#### C.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 exist between different IMS operator domains such as Mm, Mk, Mg and Sr). In order to do so, IMS operators shall operate NDS/IP Za-interface between SEGs.

It will be for the IMS operator to decide whether and where to deploy Zb-interfaces in order to protect the IMS control plane traffic over those IMS interfaces within the same security domain.

[Diameter messages over the Cx interface shall make use of SCTP. Additional guidelines on how to apply IPSec in SCTP are specified in \[x\]. This RFC shall also apply to NDS/IP if IMS operator chooses to deploy Zb-interface at Cx interface.](#)

[Editor's Note; The reference to I-D "draft-ietf-ipsec-sctp-02.txt" shall be replaced by the corresponding RFC reference when this draft reaches RFC status.](#)