3GPP TSG SA WG3 Security S3-000687
Meeting S3#16
Sophia Antipolis, 28-30 November, 2000

**Source:** Siemens AG

**Title:** Restricting the IPsec usage

**Document for:** Discussion and decision

**Work item:** Network domain security

**Agenda item**: tbd

## Abstract

*The IPsec base protocols AH and ESP provide a flexible mechanism to provide security at the network layer for IP based communication. With the 3GPP Rel'4 standards IPsec will become part of the UMTS network domain architecture, providing security e.g. for the GTP protocol. With this contribution, we propose two restrictions that in our opinion should apply to any use of IPsec in the network domain of UMTS.*

*This contribution is meant as a starting point to collect guidelines that should be heeded for guaranteeing a secure use of IPsec in the 3GPP Rel'4 and Rel'5 core network.*

## 1 Restrictions for the use of IPsec in the network domain

**We propose to strongly discourage the use of ESP with the NULL authentication algorithm. If a network entity receives ESP protected packets with the NULL authentication algorithm, it must not use the ESP replay protection mechanism and shall be aware of the fact that the packet does not provide data origin authentication.**

S3-000663 proposes to discourage the use of AH for network domain security and to use ESP in tunnel mode. ESP in tunnel mode offers at least the same level of security as can be achieved with AH, since the original IP packet header is completely integrity protected. Anyway, in ESP it is a legal option to use ESP encryption only, without integrity protection. In the case where integrity protection is not used, the ESP header of an IP packet is not protected at all. Since the ESP header contains a sequence number used for IPsec replay protection, this sequence number is transmitted without protection as well. When ESP without integrity protection (NULL authentication algorithm) is used, the IPsec replay protection cannot operate securely and therefore cannot be used.

**Furthermore, we propose to strongly discourage the use of the ESP_DES transform for ESP encryption. Instead, support of the ESP_3DES transform or another transform of similar or better cryptographic strength (e.g. AES) shall be specified as mandatory for all network entities with ESP support.**

The DES (data encryption standard) encryption algorithm nowadays is regarded as insecure due to it's insufficient key length (see e.g. [Descracker]). In January 1999, during RSA Data Security's „DES Challenge III", a brute force attack against DES succeeded in about 22 hours.

Since ESP_DES is the only ESP encryption transform that must be supported by any ESP conformant implementation, it seems to make sense not to use DES for UMTS network domain security and to mandate the implementation of an alternative transform which offers higher security.

## 2 References

[Descracker] http://www.eff.org/descracker/

[RFC 2407] Piper, D., "The Internet IP Security Domain Of Interpretation for ISAKMP", RFC 2407, November 1998.