3GPP TSG SA WG3 Security — S3#21 **S3-010616**

27 - 30 November, 2001

Sophia Antipolis, France

Source: **Nokia**

Title: **Proposed Changes to 33.210 about the ESP Algorithms**

Document for: **Discussion/Decision**

Agenda Item:

This contribution proposes cryptographic algorithms for the ESP. The changes are edited with change marks against 33.210 v. 0.6.0.

5.3 Profiling of IPsec in NDS/IP

This section gives an overview of the features of IPsec that are used by NDS/IP. The overview given here defines a minimum set of features that must be supported. In particular, this minimum set of features is required for interworking purposes and constitutes a well-defined set of simplifications.

The accumulated effect of the simplifications is quite significant in terms of reduced complexity. This is achieved without sacrificing security in any way. It shall be noted explicitly that the simplifications are specified for NDS/IP and that they may not necessarily be valid for other network constellations and usages.

Within their own network, operators are free to use IPsec features not described in this section although there should be no security or functional reason to do so.

5.3.1 Support of IPsec payload compression

Standard IPsec allows for packet payload compression to be used in conjunction with ESP and AH (RFC-2393, [11]). For the purpose of NDS/IP, use of stateless packet-by-packet compression in general offers no benefits since the compression is not effective for the comparatively small packets that are protected by NDS/IP.

However, the disadvantages of introducing payload compression are added complexity for the SA negotiation phase since separate compression SAs must be negotiated and added complexity in the packet processing for both the sending and the receiving side.

Therefore IPsec payload compression shall not be used for interworking traffic over the Za-interface.

5.3.2 Support of ESP

When NDS/IP is applied, only the ESP (RFC-2406, [17]) security protocol shall be used for all NDS/IP inter-domain control plane traffic.~~ Furthermore, ESP shall always be used with integrity, data origin authentication, and anti-replay services. That is, the NULL authentication algorithm is explicitly not allowed for use in NDS/IP.~~

5.3.3 Support of tunnel mode

Since security gateways are an integral part of the NDS/IP architecture, tunnel mode shall be supported. For NDS/IP inter-domain communication, security gateways shall be used and consequently only tunnel mode (RFC-2401, [12]) is applicable for this case.

The operators may support transport mode within their own network, but it shall be noted that tunnel mode alone will be sufficient for all cases. There is therefore no explicit need for support of transport mode in NDS/IP.

5.3.4 Support of ESP encryption transforms

IPsec offers a fairly wide set of confidentiality transforms. The ~~only~~ transforms that compliant IPsec implementation is required to support are~~is~~ the ESP_NULL and ESP_DES transforms. However, the Data Encryption Standard (DES) transform is no longer considered to be sufficiently strong in terms of cryptographic strength. This is also noted by IESG in a note in RFC-2407 [18] to the effect that the ESP_DES transform is likely to be deprecated as a mandatory transform in the near future. A new Advanced Encryption Standard (AES) is being standardized to replace the aging DES.

It is therefore explicitly noted that for use in NDS/IP, the ESP_DES transform shall not be used and instead the ESP_AES transform shall be mandatory.

Editor's Note: The AES transforms/modes have not yet been finalized, This subclause will be updated when the AES transforms/modes are available.

5.3.5 Support of ESP authentication transforms

The transforms that compliant IPsec implementation is required to support are the ESP_NULL, the ESP_HMAC_MD5 and the ESP_HMAC_SHA-1 The ESP shall always be used to provide integrity, data origin authentication, and anti-replay services in NDS/IP, thus the ESP_NULL authentication algorithm is explicitly not allowed for use. MD5 has been shown to be vulnerable to collision search attacks and SHA-1 and AES appear to be a cryptographically stronger transforms, thus ESP_HMAC_MD5 are explicitly not allowed for use in NDS/IP. ESP shall support ESP_HMAC_SHA-1 and AES MAC algorithms in NDS/IP.