3GPP TSG-SA3 Ad Hoc on ‘Network Domain Security’ **S3z010009**

Madrid 23-24 April, 2001

3GPP TSG SA WG3 Security S3-010075

Meeting S3#17

Göteborg, 27 Feb – 2 Mar, 2001

Source: Siemens AG

Title: Mandate 3DES for use of ESP with GTP-C

Document for: Discussion / Decision

Work item: Network domain security

Agenda item: tbd

Abstract

It is proposed in this contribution to mandate the 3DES cryptographic transform if IPSec/ESP is used for GTP security.

1 Introduction

Annex A.4 of draft TS 33.200 “Network domain security” V3.2.0 explicitly notes that for use in the UMTS network domain control plane the ESP_DES transform shall not be used and instead the ESP_AES transform shall be used.

In this contribution we propose that, when using ESP to provide confidentiality for GTP-C, the ESP_3DES transform as specified in [rfc2407 IPSec DoI and rfc2451-ESP-CBC] shall be supported.

The rationale for this is that implementations of GTP security may want to rely on existing implementations of IPSec which support ESP_3DES. On the other hand, ESP_AES has not yet become a rfc and may therefore not yet be supported by existing IPSec implementations. In order to ensure interoperability it is therefore proposed to mandate the use of ESP_3DES with GTP-C.

The same problem for MAPSec is not seen as there are no existing implementations for MAPSec.

We further propose in this contribution not to mandate the use of certain transforms, but to mandate their support by implementations. Operators should have the freedom to agree on different transforms if desired.

We would also like to raise the question to be discussed at S3#17 how to handle 3G standards which make reference to IETF drafts which are still subject to change at the IETF.

2 Proposed changes to Annex A.4 of draft TS 33.200

The new text shall read as follows. The proposed changes are marked by revision marks.

“A.4 Support of ESP encryption transforms

IPsec offers a fairly wide set of confidentiality transforms. The only transform that compliant IPsec implementation is required to support is the ESP_DES transform. However, the Data Encryption Standard (DES) transform is no longer considered to sufficiently strong in terms of cryptographic strength. This is also noted by IESG in a note in RFC-2407 [19] 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 the UMTS network domain control plane the ESP_DES transform shall not be used and instead the ESP_AES transform, as specified in [draft-ietf-ipsec-ciph-aes-cbc-01], shall be supported by all implementations, with the exception of implementations which provide confidentiality for GTP-C.

When using ESP to provide confidentiality for GTP-C, the ESP_3DES transform as specified in [rfc2407-IPSec-DoI and rfc2451-ESP-CBC] shall be supported by all implementations.”