ATM Forum Technical Committee
ATM Forum/99-0336

****

TITLE: Inconsistencies and missing information in the security specification 1.0

****

SOURCE:

Maryline LAURENT
IRISA/INRIA
Campus Universitaire de Beaulieu
35042 Rennes Cedex, France
Phone: 33 2 99 12 70 20
Fax: 33 2 99 12 70 30
E-mail: Maryline.Laurent@enst-bretagne.fr

Véronique ROSSI
ENSTB
2, rue de la chataigneraie
35510 Cesson Sévigné, France
Phone: 33 2 99 12 70 20
Fax: 33 2 99 12 70 30
E-mail: Veronique.Rossi@enst-bretagne.fr

Mohammed ACHEMLAL
France Telecom-CNET
42 rue des Coutures , BP 6243
F-14066 CAEN Cedex, France
Phone: 33 2 31 75 92 28
E-mail : mohammed.achemlal@cnet.francetelecom.fr

****

DATE: July 1999, New Orleans, Louisiana

****

DISTRIBUTION: SEC Working Group

****

ABSTRACT:

This contribution reports some inconsistencies and missing information found in the Security Specifications 1.0 of February 1999 studied within the ACTS project SCAN (Secure Communications in ATM Networks).

****

NOTICE:

This contribution has been prepared to assist the ATM Forum. This proposal is made by the authors as a basis of discussion. This contribution should not be construed as a binding proposal on the authors or their companies. Specifically, the authors and their companies reserve the right to amend or modify the statements contained herein.

****

1. Additional explanations needed

- Section 6.2.2: The way to obtain the 1-byte Security Service Declaration section content should be described deeply, clarifying the encoding to be used.

- The meaning of the '*' is not explained.

- Section 6.2.2 (Security Service Specification Section): Explanations relative to the possibility to specify several algorithms for the same security service should be introduced in that section, and not only in section 5.1.1.

- Section 6.2.3.1 (Confidentiality algorithm): In the Data Confidentiality Mode Details, the DES40 algorithm requires a 64-bit random number. Explanations specifying that this field is used for the U.S. export restrictions should be given.

- Section 6.2.3.9 (Confidentiality Algorithm Profile Group): The content of the Encryption Algorithm Details is not described. It should include both the Algorithm Details and the Algorithm Mode Details information presented in section 6.2.3.1. Explanations relative to the organization of that field should be introduced (in particular when the DES40/CBC is selected).

2. Errors in the description of the SAS fields

- Section 6.2.3.9 (Confidentiality Algorithm Profile Group): The identifier for the Hash Algorithm Details should be coded as 10110100 instead of 10110010. Otherwise it is similar to the Signature Algorithm Details Identifier.

3. Inconsistencies in the examples given in section 7.3

- Section 7.3.2 (Flow1-2WE and Flow2-2WE): The authentication section ID is missing.

- Section 7.3.3 (Flow1-3WE): The length of the first Data Confidentiality Algorithm specified is 2 bytes instead of 18. The length of the second Data Confidentiality Algorithm is 10 bytes instead of 12.

- Section 7.3.3 (Flow2-3WE): The CBC mode code (00000010) should be replaced with 00000001.

- Section 7.3.3 (Flow2-3WE): The length of the Data Confidentiality Algorithm specified is 10 bytes instead of 12.

- Section 7.3.3 (Flow2-3WE): The length of the Confidential section should be specified using 2 bytes. The length of the confidential section is 27 bytes instead of 64.

- Section 7.3.3 (Flow2-3WE): The Initiator Random Number Value should be 4-byte length. As such, the Initiator Random Number Value should be described in octets 118 to 121. The same comment applies to the Responder Random Number Value.

- Section 7.3.3 (Flow2-3WE): The Digital Signature Value is in octets 137 to 156. This is not consistent to the length 64 specified above.

4. Acknowledgement

Project SCAN (Secure Communications in ATM Networks) is funded by the European Commission, Directorate General XIII, ACTS Programme 3rd call, project number AC330.

5. References

[AF99] ATM Forum, "ATM Security Specification Version 1.0", February 1999.