Title: Additional Comments on ISO CD 11577 (Network Layer Security Protocol)

Source: IBM

Reference: SC6/N7053

Item Number: 1

Type of Comment: General

Location: Various

Rationale: The text of this document includes, in addition to provisions for secure data transfer, provisions for key management functions that should not be in the scope of this activity. Key management should be considered an application and this protocol should simply provide the appropriate hooks for interaction.

Item Number: 2

Type of comment: Editorial

Location: Section 9.2

Rationale: Figure 9.1 reflects the Length of the Content Field to be one or three octets. However, the text explaining the details of this field reflect it as being one, two or three octets long.

Proposal: Change the Length of the Content Field in Figure 9.1 to "1, 2 or 3".

Item Number: 3

Type of Comment: Editorial

Location: Section 9.3 (Figure 9.2a)

Rationale: The term "Content" is used to represent a structured format for specifically defined data values that are placed in a Secure Data Exchange PDU as defined in section 9.2. However, this term is also used in Figure 9.2a to represent the total protected data in the PDU. The reader would better understand the text if it is indicated that within the protected data field are the specific Content Fields as defined in Section 9.2.

Proposal: Change the term "Protected Contents" to "Protected Data".

Item Number: 4

Type of Comment: Major Editorial

Location: Section 9.3.2

Rationale: The title and text of this section is confusing in that the word "Content" is used to designate both a specific format structure and a general data field. In addition the note above Figure 9.5 contradicts the text immediately above.

Proposal: Following is suggested replacement text for this section:

9.3.2 Protected Data

Figure 9.5 shows the data structure for the Secure Data Transfer PDU.

The content Length and Content Type fields are required. At least one Content Field must be present.

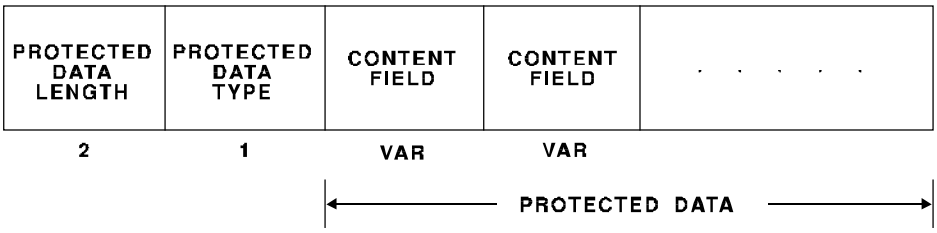


Figure 9.5 Protected Data Field

Item Number: 5

Type of Comment: Editorial

Location: Section 9.3.2.1

Rationale: The title and wording of this section is confusing in that the use of the term "Content Length" conflicts with its use in the specific Content Fields as outlined in Section 9.2.

Proposal: Change the title of this section to "Protected Data Length" and reword the first sentence as follows:

> "The Protected Data Length field contains the length of the Protected Data in Octets, excluding the Protected Data Length Field."

Item Number: 6

Type of Comment: Editorial

Location: Section 9.3.2.2

Rationale: The section is meant to identify the type of protected data carried in the secure PDU, not the specific Content Fields of which multiple may be present in a single PDU. The title is confusing in this respect.

Proposal: Rename the title of this section to "Protected Data Type".

Item Number: 7

Type of Comment: Editorial

Location: Section 9.3.3

Rationale: The paragraph in subsection b) implies that the specific characteristics of the selected ICV mechanism have been pre-defined. The objective of this protocol is to allow the user to select an ICV mechanism that meets the specific requirements of the application.

Proposal: Outlined below is proposed re-wording for the first sentence in the paragraph of subsection b):

> "If the integrity mechanism, identified in the Security Association Attributes, is used in block mode it should have known characteristics which will include block length."

Item Number: 8

Type of Comment: Editorial

Location: Section 9.3.5.1

Rationale: The Editors Note questions the need for a length field to be preceding each of the variable label contents.

The Content Field Length is defined to indicate the length of the Content Field value. In the case of Content Fields that contain multiple variable values (ie. Label) it will be necessary to provide a length field in order to accurately parse the value field.

Proposal: It is recommended that a length field be included preceding each of the fields for the label.

Item Number: 9

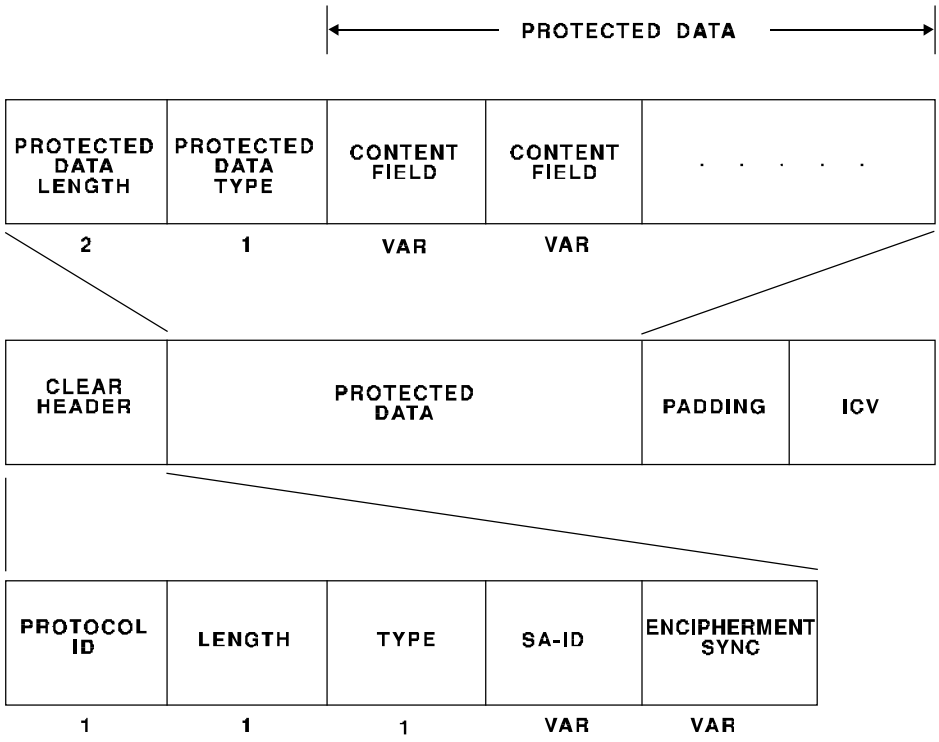
Type of Comment: Major Technical

Location: Section 9.3 and 9.5

Rationale: The SCI Exchange PDU and Connection Authentication PDU formats shown in Figures 9.8 and 9.9 respectively use the same Protocol ID (01000101) as is in the Secure Data Transfer PDU. However, the Control octet is in the same location as the Length Field of the Clear Header of the Secure Data Transfer PDU. This makes parsing of the SCI and Connection Authentication PDU impossible. In addition, it is unclear as to which fields of the SCI and Connection Authentication PDUs are in the clear and which fields are protected.

Proposal: It is recommended that the SCI Exchange PDU and Connection Authentication PDU have the same general format as the Secure Data PDU as shown on the following page.

The "Control Octet" field in sections 9.4.2 and 9.5.2 should be renamed "Type" to be consistent with the definition of "PDU Type" as defined in Section 9.3.1.3.

The "Content Length" field in section 9.4.3 should be renamed "Protected Data Length" and this field should be included in the parameters associated with the Connection Authentication PDU (Section 9.5).

Proposed PDU structure for SCI Exchange PDU and Connection Authentication PDU: