GERMAN POSITION ON TRADE/WP.4/R.1214/1215,
TRADE/WP.4/R.1245/1246

(Syntax version 4 - Parts 5 and 6 for security)
Documents R.1214/1215 were made available for the March session of WP.4/GE.1. At this session countries were requested to review and comment on these documents. Accordingly, Germany has taken the opportunity to review the documents taking into account the revised documents R.1245/1246 distributed for the September session of WP.4/GE.1.

Germany supports the inclusion of security functions as part of the overall UN/EDIFACT architecture. However there are a number of areas which still need to be addressed to ensure that the security functions can be implemented in a straightforward and consistent manner.

The following points summarise general concerns that Germany holds:

1. Germany considers it important to include a detailed description of the interrelationship of the various security methods (e.g. hashing, filtering, encryption, compression) with respect to the security services (authentication, integrity, non-repudiation, confidentiality).

2. In order to assist in understanding how the security structures can be applied, Germany considers it important to include scenarios (e.g. diagrams, graphical figures) that depict the overall flow from the sender’s application to the receiver’s application, step by step (e.g. data flow, control flow) with respect to security. The user should be able to easily relate the required security functions to the specified security structures.

In addition, Germany would like to suggest that the Security Sub-Group produces ‘Message Implementation Guides’.

Furthermore we want to add the following specific comments:

3. Segment USA - Security algorithm: Germany believes that data element 0525 (Cryptographic mode of operation, coded) in S502 should be specified as mandatory instead of conditional. Our understanding is that the absence of this data element in transmission would make the identification of the security mode of operation implicit rather than explicit.

4. In attempting to map various security processes difficulties were encountered when constructing specific test examples.

   For example, when using segment USH - Security header - data element 0501 and segment USA - Security algorithm - data elements 0523, 0525 and 0527), it is possible to assign incompatible values to these data elements. Therefore, Germany suggests, that either a matrix of the valid code combinations for these data elements is provided - or - a single data element is defined whereby specific code values can be assigned to achieve the same functionality.

Despite of the comments, Germany is able to approve R.1245/R.1246 (Part 5 and 6 of Syntax version 4), but Germany requests that the above points will have been taken care of before the final documents will be passed to ISO.