PIDX/RN Revision Project
Data Encryption Guidelines

PIDX requires that encryption be used to ensure data confidentiality. PIDX requires that encryption be available at the application (message payload) layer in addition to any encryption that may be applied at the transport (transmission) layer.

Use of HTTPS to encrypt the data during transport is considered sufficient for direct integrations between partners. When data is transmitted though a RNIF messaging hub, transport layer encryption is not sufficient and payload encryption (encryption of the RN service header document is optional) should be utilized to ensure data privacy. Payload encryption is described in the "Packaging with Encryption" section of 2.3.3 of the RosettaNet 2.0 specification. Below are diagrams from the RosettaNet 2.0 specification related to encrypting the RosettaNet message payload.

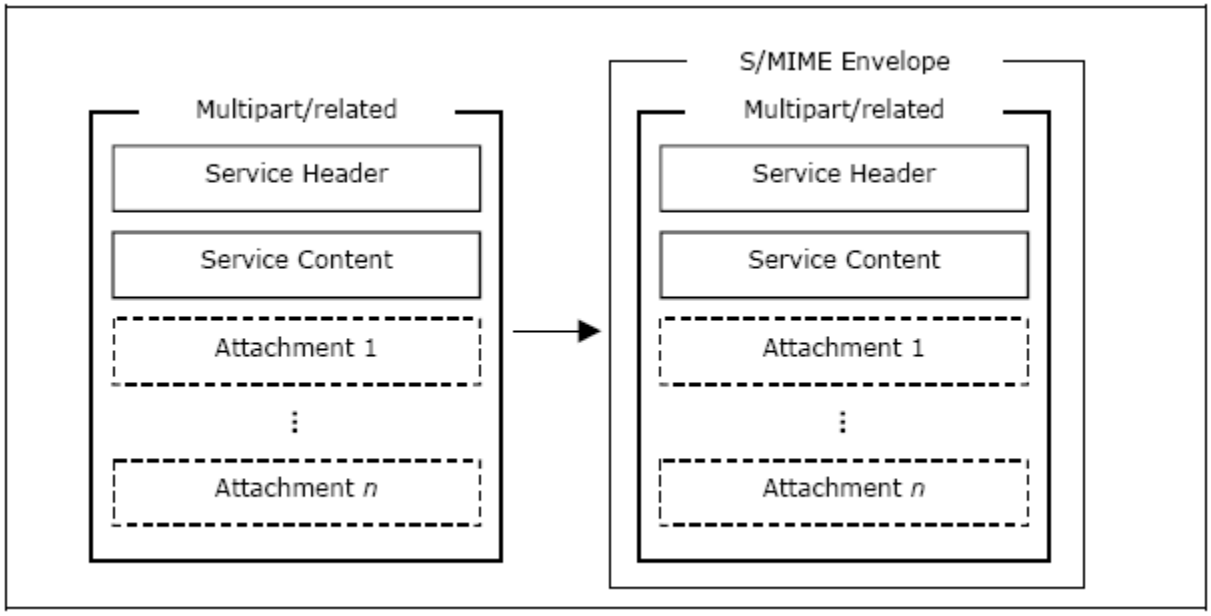

Figure 10. Encrypting the Payload Container

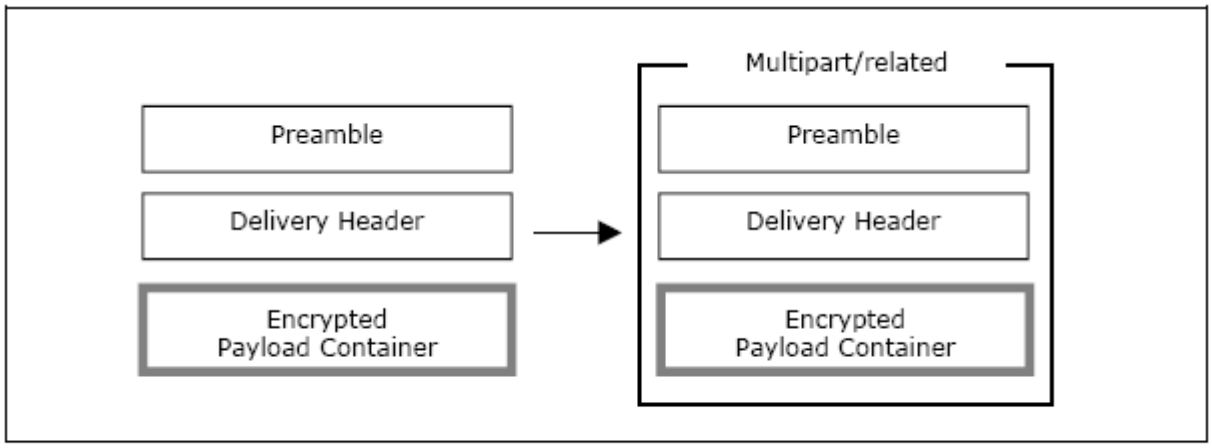

Figure 11. Packaging RosettaNet Message with Encrypted Payload Container