# PIDX/RN Revision Project

## Mandatory use of digital signatures

PIDX requires that every messaging system for exchange of PIDX XML Schemas support both non-repudiation of receipt and non-repudiation of origin and content. Non-Repudiation is the mechanism for making sure that an originating trading partner can not deny having originated and sent a message (called Non-Repudiation of Origin and Content) and that a receiving trading partner cannot deny having received a message sent by its partner (called Non-Repudiation of Receipt).

All PIDX/RN message envelopes must include a detached PCKS7 digital signature and the receipt acknowledgement document must contain a message digest of the document being acknowledged to ensure end-to-end non-repudiation. Signing of the RosettaNet Business Message is described in Section 2.3.3 of the RNIF2.0 specification. Below are diagrams from the RosettaNet 2.0 specification related to digitally signing messages.

**Example 11. Signed RosettaNet Business Message**

```
Content-Type: multipart/signed;
              boundary="RN-Signature-Boundary";
              protocol="application/pkcs7-signature";
              micalg=sha1
Content-Description: This is a Signed RosettaNet Business Message

--RN-Signature-Boundary
[The RosettaNet Business Message to be signed goes here]

--RN-Signature-Boundary
Content-Type: Application/pkcs7-signature; name="detached.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s
Content-Description: This is the signature for the Business Message

[The base64-encoded PKCS7 Detached Signature goes here]

--RN-Signature-Boundary--
```

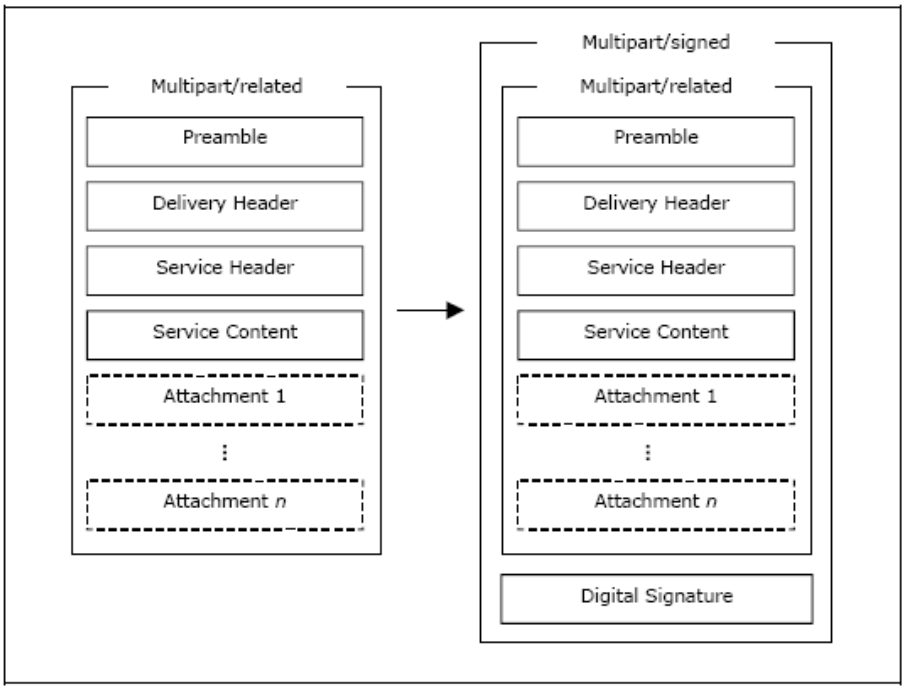


**Figure 15. Signing the Unencrypted RosettaNet Business Message**