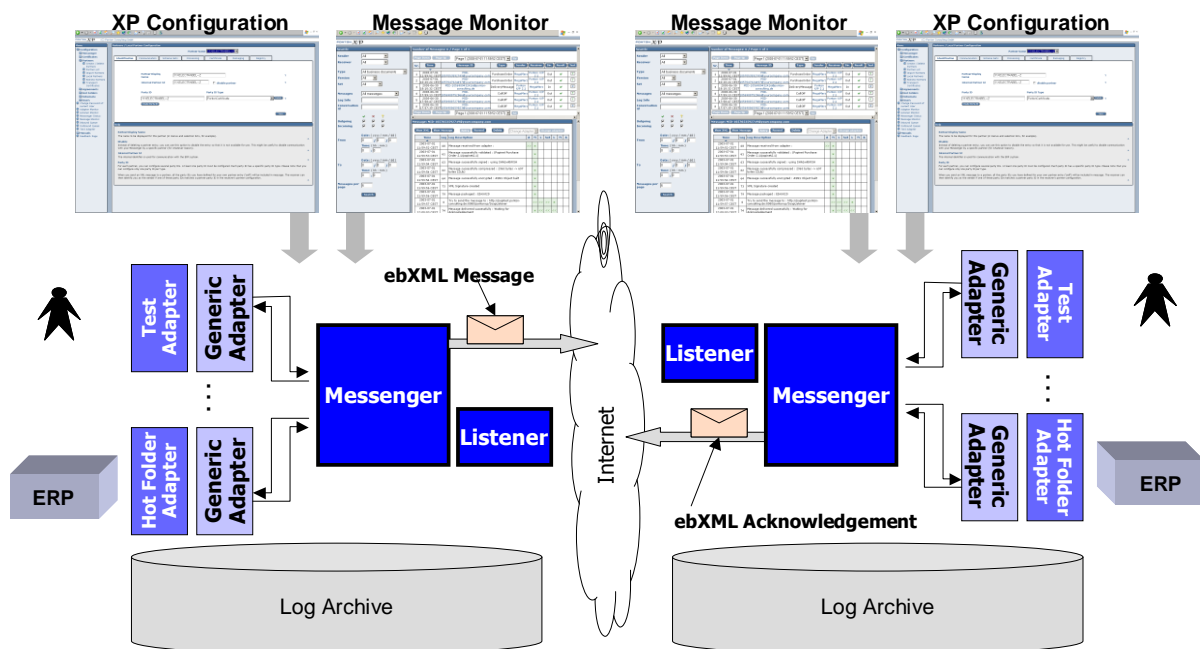


Information regarding security and reliability aspects for end-to-end application integration using the Ponton X technology

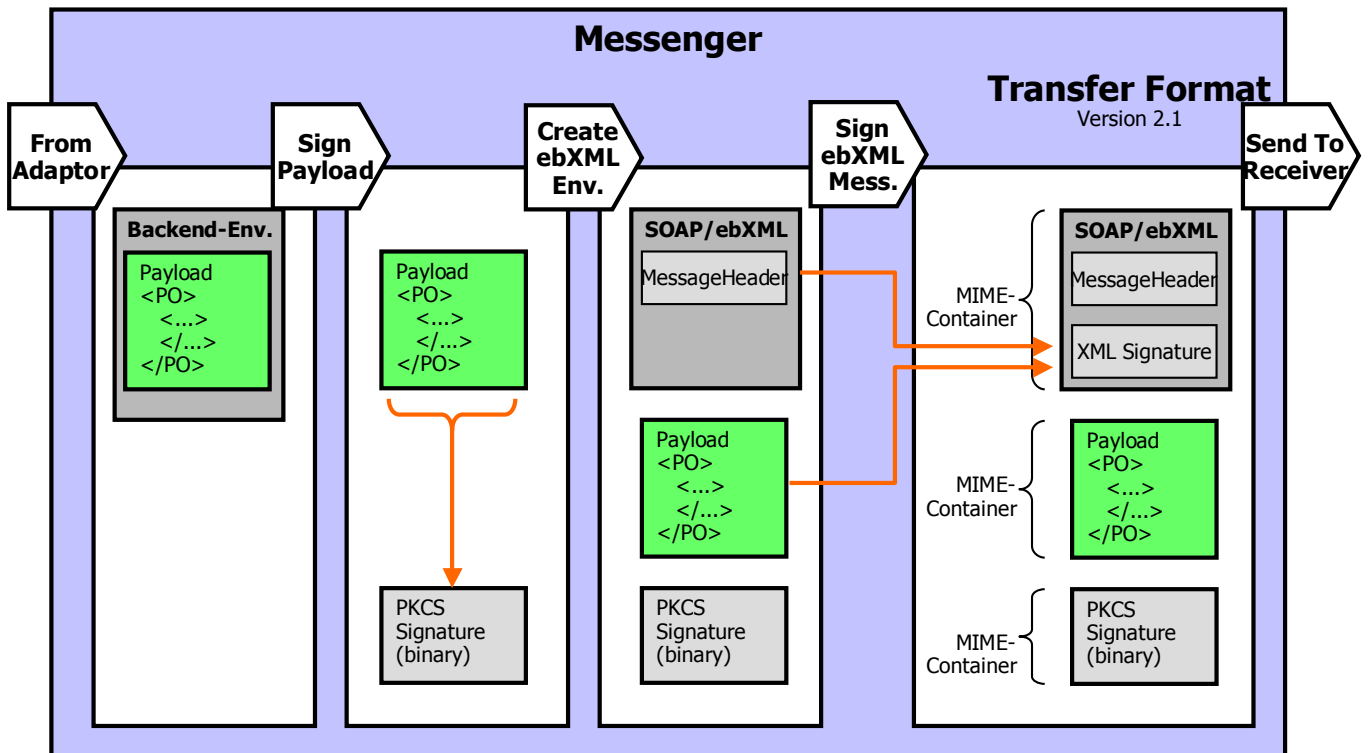
The product Ponton X/P is currently used by over 120 enterprises worldwide to automatically exchange data with their business partners directly from ERP system to ERP system. Some of those customers (Energy Traders) use the software to exchange XML data at high speed and highest security levels. Reliability and permanent availability are key elements required for this exchange of complex business data.

The software favors the communication protocol ebXML which has been standardized by UN/CEFACT and OASIS. Both organizations are absolutely vendor neutral. The UN/CEFACT is the successor to UN/EDIFACT which has focused on standardizing data exchange formats for the last 20 years. In addition to ebXML, Ponton X/P also supports the AS1, AS2, and AS3 communication protocols.



The transfer of documents with ebXML is done based on protocols such as http(s), SMIME, or SMTP. Once the communication partners have agreed to use any of these protocols, they can be configured within Ponton X/P. In any case (http vs. E-mail), a dual security mechanism can be used for communication:

- On the transport level, it is possible to use channel encryption and authentication (SSL with server and client authentication (SSL with Server and Client Authentication or SMIME)
- In an end-to-end integration scenario, the sending ebXML message client (Ponton X/P) encrypts the document on the basis of the 3DES, RSA, or AES standards and creates an electronic signature based on PKCS7 (RSA with 2048 bit key length).



The documents are transferred between installations of Ponton X/P located in the secure network zones of the communication partners. Incoming http(s) messages can be handled by the optional Listener component of Ponton X/P. The Listener, located in the DMZ, does the client authorization and forwards messages to the Messenger component of Ponton X/P. During that process all communication is initiated by the Messenger from within the secure zone (inside-out) so that the firewall is never opened from outside of the secure zone. The ports used for this communication can be chosen based on customer preferences or their IT policies.

This technology along with the dual security mechanism at the document level protects against unauthorized access.

The signature used by Ponton X/P is an enhanced signature. Ponton acts as a Trust Center and issues electronic certificates after a verification process. These certificates can be installed in Ponton X/P for future use. If the customer already has an agreement with another Certificate Authority such as VersiSign®, Thawte® or GlobalSign®, those certificates can be used alternatively. The creation of the pair of keys and the usage of the signing mechanism are electronically automated.

In addition to the payload of the message (an XML document or any binary file) the acknowledgement of reception on the communication partner's side is signed as well to ensure fully transparent communication and non-repudiability.

In addition to encryption, signature mechanisms and the Public-Key Infrastructure Ponton X/P uses, it is important to note that for a fully transparent communication (also from a legal perspective) a complete protocol of the interactions (audit trail) is required. For this reason Ponton X/P can use database systems such as IBM DB2, Oracle 7-10g, MS SQL Server, Informix, MySQL, HSQL, etc. to archive all exchanged documents, acknowledgements, etc. By comparing the archived signature to the document the authenticity of a document can be checked at any time.