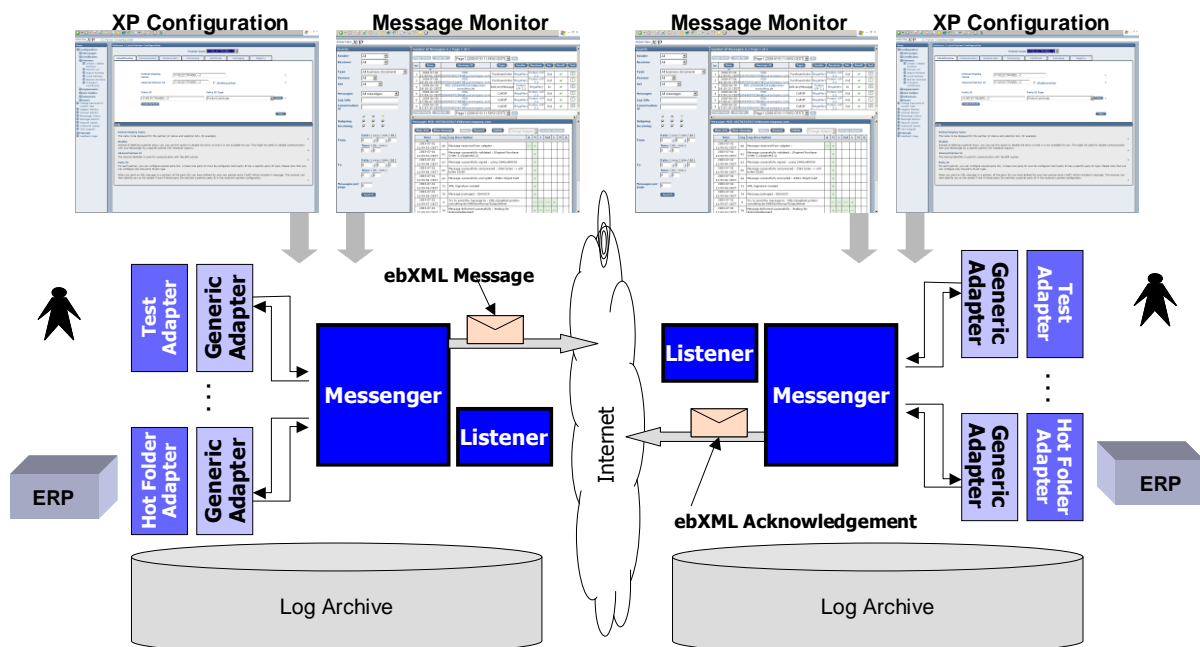


Informationen zu Sicherheits- und Zuverlässigkeitsaspekten bei der End-to-End-Applikationsintegration mit der Ponton X Technologie

Die Software „Ponton X/P“ wird heute bei über 120 Unternehmen weltweit eingesetzt, um direkt zwischen deren Anwendungssystemen Daten auszutauschen. Einige dieser Kunden (Energiehändler) setzen die Software ein, um bei sehr hohem Sicherheitsniveau mit hoher Geschwindigkeit XML-Daten auszutauschen. Weder ein Ausfall der Software noch Sicherheitslöcher sind in diesem Bereich tolerierbar.

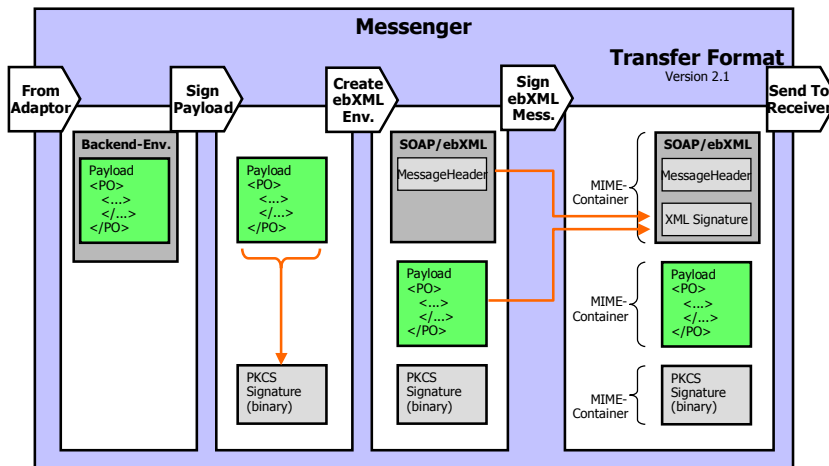
Die Software favorisiert das Kommunikationsprotokoll **ebXML** welches von der **UN/CEFACT** zusammen mit der OASIS standardisiert wurde. Beide Organisationen sind dabei absolut neutral. Die UN/CEFACT ist die Nachfolgeorganisation der UN/EDIFACT, welche über die letzten 20 Jahre Datenaustauschformate standardisiert hat. Alternativ dazu werden auch die Protokolle AS1, AS2 und AS3 unterstützt.



Informationen zu Sicherheits- und Zuverlässigkeitsaspekten

Die Übertragung von Dokumenten erfolgt bei ebXML auf Basis von Protokollen wie **HTTP(s)**, **SMIME** oder **SMTP**. Diese Protokolle lassen sich im Rahmen von ebXML bilateral zwischen Kunden vereinbaren und über die Software konfigurieren. In jedem Fall (http vs. E-Mail) besteht jedoch die Möglichkeit, eine **doppelte Sicherung der Kommunikation** zu verwenden:

- Auf Transportebene besteht die Möglichkeit zur **Kanalverschlüsselung und – authentication** (SSL mit Server- und Client-Authentisierung bzw. SMIME).
- Bei der End-to-End-Integration wird durch den sendenden ebXML Message Service eine weitere Verschlüsselung vorgenommen auf Basis des 3DES, RSA oder AES Standards sowie eine elektronische Signatur auf Basis des PKCS7 Standards (RSA mit 2048 Bit Schlüssellänge) erzeugt (**Dokumentenverschlüsselung bzw. -authentication**).



Die Übertragung von Dokumenten erfolgt in der Regel zwischen zwei Instanzen von Ponton X/P, die sich jeweils im sicheren Bereich des Netzwerkes befinden. Zur Überwindung der **Firewall** wird im Falle von eingehenden Nachrichten per HTTP(s) eine weitere Komponente – der Listener – in der DMZ eingesetzt. Dieser Listener, führt die Client-Authentisierung durch und leitet Dokumente weiter an den Messenger. Dabei werden alle Kommunikationsverbindungen zwischen Messenger und Listener eines Teilnehmers **inside-out** aufgebaut, d.h., der Listener wird niemals die Firewall von aussen nach innen per Socket-Verbindung öffnen. Stattdessen wird ein vom Messenger initiiertes Kommunikationskanal genutzt.

Dieses Verfahren in Kombination mit der doppelten Sicherung der Kommunikation bietet den **höchstmöglichen Schutz gegen Einbruchsversuche seitens Dritter**.

Die Signatur entspricht der **enhanced Signature** im Sinne des SigG. D.h., Ponton (oder eine andere CA) tritt als TrustCenter auf und vergibt nach einem Überprüfungsprozess elektronische Zertifikate, die in der Ponton X/P Software installiert werden. Der Erstellungsprozess des erforderlichen Schlüsselpaars sowie die Nutzung der Signiervorrichtung erfolgen dabei rein elektronisch.

Zusätzlich zur Nutzlast (dem XML Dokument oder einfach einer beliebigen Binärdatei) wird auch das ebXML-Acknowledgement (die Empfangsbestätigung) der Gegenseite signiert, um eine komplette Kommunikationstransparenz zu gewährleisten.

Neben den verwendeten Verschlüsselungs- und Signialgorithmen sowie der verwendeten Public-Key-Infrastruktur ist darauf hinzuweisen, dass auch die Protokollierung der Kommunikationsabläufe von besonderer Bedeutung ist (**Revisionssichere Protokollierung**). Hier besteht bei Ponton X/P die Möglichkeit, Protokollinformationen zur Datenübertragung selektiv im lokal verwendeten DBMS abzuspeichern.

Unterstützt werden dazu bislang IBM DB2, Oracle 7-10g, MS SQL Server, Informix, MySQL, HSQL, etc. Zudem kann im Nachhinein die **Authentizität** eines empfangenen oder gesendeten Dokumentes nachgewiesen werden, indem die archivierte Signatur gegen das XML-Dokument überprüft wird.

Weitere Informationen zum Funktionsumfang entnehmen Sie bitte unserem Datenblatt.