EDI ANWENDERKREIS HANDEL

AS2 (Applicability Statement 2):

Beschreibung und Parameter

Einleitung

In diesem Dokument werden zum Thema AS2 folgende Fragen erläutert:

- Was ist AS2?
- Wie funktioniert AS2 & welche Voraussetzungen müssen erfüllt sein?
- Welche Vorteile hat AS2?
- Wie gestalten sich die Kosten von AS2 im Vergleich zu VANs?

Anschließend folgt eine Darstellung der Parameter samt dazugehöriger kurzer Erläuterungen, auf die sich die AG Kommunikation des Anwenderkreises Handel geeinigt hat.

Was ist AS2?

AS2 (Applicability Statemenent 2) ist eine Version von EDIINT (EDI über das Internet), welches das Wachstum des Internets nutzt und damit Unternehmen die Gelegenheit für einen unkomplizierten und kostengünstigen Anschluss ihrer bestehenden und neuen B2B-Partner bietet.

Das bedeutet also: wer „im Web surfen“ kann, besitzt die erforderliche Infrastruktur, um AS2-konforme Software einzusetzen, und kann mit anderen Unternehmen, die ebenfalls eine solche Software benutzen, Dokumente austauschen.

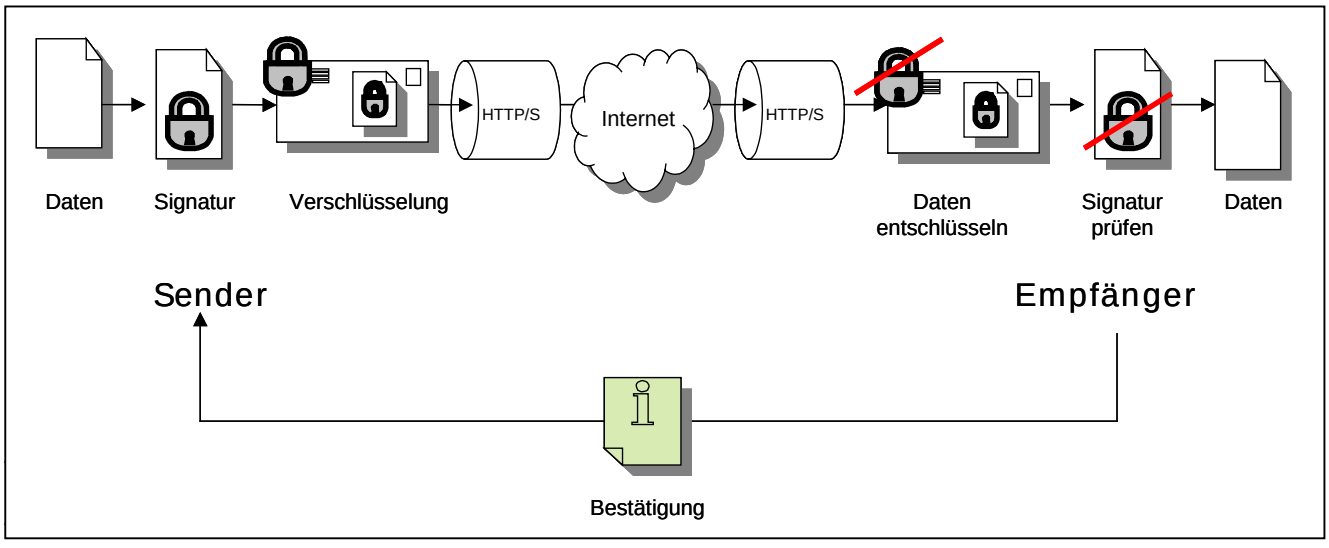
AS2 ist eine Spezifikation für den Datenaustausch, dessen Aufgabe im Versenden und Empfangen von Dateien über eine gesicherte Verbindung besteht. Eine Prüfung oder Validierung der Dateninhalte findet jedoch nicht statt.
AS2 arbeitet dabei mit einer Art „Briefumschlag“, in dem Daten eingebettet sind, so dass sie mit dem HTTP-Protokoll, der Kerntechnologie des World Wide Web, über das Internet (oder ein anderes Netzwerk, das auf TCP/IP basiert) übermittelt werden können. Es stellt eine schnelle und direkte Übertragung dar, ohne dass eine Mailbox (z.B. Telebox) dazwischen geschaltet ist.
AS2 kann dabei jedes Dokument übertragen, ist aber besonders für den Großteil der herkömmlichen EDI-Transaktionen geeignet. Die zu versendenden Daten werden hierbei von den internen Systemen aufbereitet und über eine AS2 Kommunikationssoftware übermittelt.

Wie funktioniert AS2 & welche Voraussetzungen müssen erfüllt sein?

Für den Datenaustausch via AS2 wird ein Kommunikationsmodul – sowohl auf Seiten des Senders als auch auf der des Empfängers – benötigt (eine Liste mit zertifizierter Software finden Sie unter http://www.drummondgroup.com).
Dieses arbeitet mit einem „Umschlag“, in dem Daten bzw. elektronische Geschäftsdokumente beliebigen Formats (EDI, XML, csv, txt etc.) eingebettet werden. Die Nachricht wird mit einer elektronischen Signatur (keine qualifizierte digitale Signatur im Sinne des Signaturgesetzes) versehen, verschlüsselt - und gegebenenfalls komprimiert - an den Geschäftspartner übermittelt. Die elektronische Signatur der Nachrichten garantiert, dass Sender und Adressat auch die tatsächlichen Geschäftspartner sind. Um sicherzustellen, dass der Empfänger die Nachricht in unveränderter Form empfangen, sowie fehlerfrei dekomprimiert und entschlüsselt hat, wird das empfangene Dokument auf Originalität und Integrität geprüft und eine Bestätigungsnachricht automatisiert zurückgesendet.

Die Übermittlung erfolgt in Form eines HTTP/HTTPS-Protokolls über eine Punkt-zu-Punkt-Verbindung. Die Wahl des Protokolls wird bilateral zwischen den Partner abgestimmt. Für die Datenübertragung ist damit lediglich eine auf dem Webserver installierte EDIINT Software sowie eine Standleitung zum Internet erforderlich. Denn wie bei einem Telefon ohne Anrufbeantworter, wird die Nachricht von ihrem Server nicht erfasst, wenn er nicht verfügbar ist. Demzufolge muss auch der Empfangsrechner zu dem Zeitpunkt des Nachrichtenversands am Internet angeschlossen sein.

Nach erfolgreicher Übertragung kann der Nachrichteninhalt zur Weiterverarbeitung bereitgestellt werden.



Welche Vorteile hat AS2?

AS2 Anwender können insbesondere bei der Versendung von großen Datenvolumen die Kosten für die elektronische Datenübertragung senken.
Durch die zeitnahe und ereignisgesteuerte Versendung von Geschäftsdokumenten werden zukünftige Anforderungen an Supply Chain Prozesse abgedeckt. Anwender profitieren dadurch von einer Beschleunigung des Informationsflusses entlang der gesamten Prozesskette.
Bei der Nutzung des Internets ist es wichtig, dass die Nachrichtenübertragung mit AS2 Sicherheit und Zuverlässigkeit bietet, welche durch EDIINT-Standards gewährleistet wird. Beispielsweise digitale Zertifikate können sicherstellen, dass Nachrichten ausschließlich den gewünschten Empfänger erreichen, dass der Datentransfer sicher ist und dass der Absender überprüft werden kann. Des Weiteren kann auf die Zwischenschaltung eines Value Added Networks (VANs, z.B. x.400) verzichtet werden, da Daten direkt übertragen werden. Ein unberechtigtes Lesen oder Verändern der Daten ist demzufolge nicht möglich.

Wie gestalten sich die Kosten von AS2 im Vergleich zu VANs?

Die Nutzung von VANs, wie beispielsweise das X.400 Mailboxverfahren für den elektronischen Austausch von Geschäftsdaten (z. B. Bestellungen, Rechnungen), verursacht vor allem volumenabhängige Kosten. Aufgrund der zunehmenden Vernetzung zwischen Handelspartnern und des dadurch ansteigenden Datenvolumens steigen diese Kosten kontinuierlich an. Sobald ein Übergang von einem VAN zu einem weiteren erforderlich wird, um einen bestimmten beispielsweise internationalen Partner zu erreichen, erhöhen sich die verursachten Kommunikationskosten signifikant.

Durch den elektronischen Datenaustausch über das Internet auf Basis des neuen, in den USA bereits etablierten Standards AS2 entfallen diese Kosten komplett. Die einzigen verbleibenden Kostenfaktoren ergeben sich zum einen aus der Bereitstellung und Nutzung der Internetverbindung und zum anderen aus der Investition in eine AS2 unterstützende Kommunikationssoftware.

EDI ANWENDERKREIS HANDEL

Parametereinstellungen & -erläuterungen der AG Kommunikation des AKH

AS2 Parameters		AKH AG Kommunikation	Erläuterung
Sicherheit (Security)	**Kommunikationszertifikate (Communication-Certificates)**	- Class 2 type - self-signed - minimum validity period 2, max. 5 years	**One certificate for the signature and encryption.** **Trusted:** Certificate Authorities (3. Instanz) vergibt, verwaltet, kontrolliert Zertifikate **Self-Signed:** Selbstgenerierung von Zertifikaten vereinfacht Verwaltungsproblematik **Zertifikate müssen mind. alle 5 Jahre aktualisiert werden.**
	Digitale Kommunikationssignatur (Communication-Digital-signature)	SHA1	Bevor die Daten verschlüsselt werden, wird eine Signatur erstellt und der Übertragung beigefügt. Beim Empfang der Nachricht prüft der Empfänger die Signatur. Dies stellt sicher, dass die Nachricht wirklich vom Absender stammt. SHA1 ist eine Option des Signatur-Algorithmus und wird empfohlen.
	Verschlüsselung (Encryption)	TripleDES	Der Sender verschlüsselt die Daten, der Empfänger entschlüsselt die Daten und überprüft die Datenintegrität, um zu gewährleisten, dass keine unbefugten Änderungen vorgenommen wurden. TripleDES sind nach heutigem Stand der Technik stabil und sicher.
	Länge des Schlüssels (Length of session key)	>= 128 bits	Sessionverschlüsselung für sichere HTTPS-Übertragung.
	Länge des öffentlichen/ privaten Schlüssels (Length of public/private key)	2048 bits	Der Public bzw. Private Key ist der bei asymmetrischen Verschlüsselungsverfahren erzeugte öffentliche bzw. vertrauliche Schlüssel (verbleibt beim Inhaber). Der Sender einer Nachricht kann mit dem Public Key des Empfängers den Inhalt dieser Nachricht für Dritte unlesbar verschlüsseln. Nur der Empfänger kann dann noch mit seinem Private Key die Nachricht entschlüsseln. Der Private Key ist die einzige Möglichkeit, Inhalte, die mit dem Public Key des Inhabers verschlüsselt wurden, wieder zu entschlüsseln. Der Sender einer Nachricht benutzt seinen Private Key zum Signieren. Mit Hilfe des Public Keys des Senders kann der Empfänger die Unversehrtheit der Nachricht prüfen.
Transportebene (transport layer)	**Internetverbindung (Internet connection)**	- permanent internet connection - fixed and public URL address mandatory	Eine permanente Internetverbindung muss gegeben sein.
	Übertragungsprotokoll (Transport Protocol)	HTTPS to secure AS2-From and AS2-To HTTP	HTTPS ist eine Sonderform des HTTP, das über SSL erhöhte Sicherheit bietet (Vertraulichkeit & Authentizität). Dies wird benutzt, um bei der Übertragung sensibler Daten das „Mithören" zu verhindern.
Authentifizierung des Klienten (Client Authentication)		optional	**HTTPS:** verschlüsselt und sicherer **HTTP:** Klartext (Name und Passwort sichtbar)
AS2 Kopfdaten (AS2 Header)	**Sender (AS2-From)**	GLN of the trading partner's AS2 server MUST be used. Exception: when a hub is used, the GLN of the trading partner MAY be used when the AS2-FROM field is used for routing.	Senderkennung
	Empfänger (AS2-To)	GLN of the trading partner's AS2 server MUST be used. Exception: when a hub is used, the GLN of the trading partner MAY be used when the AS2-TO field is used for routing.	Empfängerkennung
Empfangsbestätigung (Message Disposition Notification=MDN)	**MDN**	mandatory	Eine MDN wird zurückgeschickt. Sie liefert den stärksten Nachweis, da sie den Nachrichtenempfang bestätigt und so auch höchstwahrscheinlich den gewünschten Empfänger erreicht hat, da dieser im Besitz des privaten Schlüssels war.
	MDN signed	Yes	Signierung der Empfangsbestätigung
	MDN encrypted	No	Verschlüsselung der Empfangsbestätigung
	Synchron/ Asynchron	Synchronous (asynchronous allowed; transmission mode bilaterally agreed)	**Synchron:** Die MDN wird innerhalb der bestehenden Verbindung an den Sender der Nachricht gesendet, um den erfolgreichen Empfang der Daten beim Empfänger zu bestätigen. **Asynchron:** Die MDN wird in einer separaten Verbindung an den Sender der Nachricht gesendet, um den erfolgreichen Empfang der Daten beim Empfänger zu bestätigen.
Zeitstempel (timestamp)		optional	Zeitstempel zur eindeutigen Identifikation der Nachricht

Formats	**Multipurpose Internet Mail Extensions (MIME)**	MIME type coherent with content	MIME nennt sich ein Internet-Standard, um Dateitypen anzugeben. Im erweiterten Sinne ergibt sich bei einem MIME-fähigen Client die Möglichkeit, beliebige binäre Dateien zu einer Nachricht hinzuzufügen.
	Secure Multipurpose Mail Extension (S/MIME)	Yes	S/MIME ist ein Vorschlag über das Verschlüsseln und Signieren von Nachrichten zur Standardisierung an das IETF (Internet Engineering Task Force = eine offene, internationale Gemeinschaft von Entwicklern, Betreibern, Forschern usw. des Internet).
	Komprimierung (Compressed)	Accepted and optional (mode bilaterally agreed)	Durch eine Komprimierung der Daten wird das Übertragungsvolumen verringert.
AS2 Version		Nach Vereinbarung	
Eingans-/ Ausgangsport (Port inbound/ outbound)		port bilaterally agreed	Definierte, bilateral abgestimmte Kommunikationskanäle (Ports) müssen für den Datenaustausch freigeschaltet werden.