

e-AS2 Überblick und Lösung

AS2 – Ein Überblick

AS2 (Applicability Statement 2) ist der neue Standard zur sicheren Übermittlung von Dateien zwischen zwei Teilnehmern im Internet.

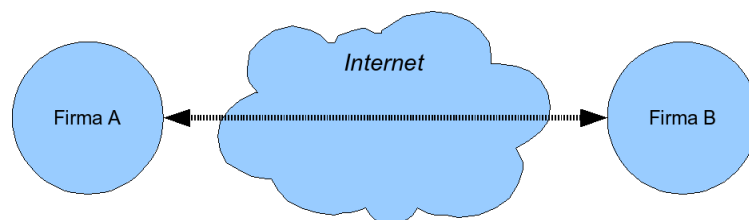
Hinter dem Kürzel AS2 verbirgt sich ein sicheres Peer-to-Peer Übertragungsprotokoll für Geschäftsdaten auf **MIME (Multipurpose Internet Mail Extensions)** Basis unter Verwendung von **HTTP (Hypertext Transfer Protocol)**. Im Detail ist AS2 im **RFC 4130** dokumentiert und auf der Web Site der Internet Organisation **IETF (Internet Engineering Task Force)** nachzulesen (<http://www.ietf.org/rfc/rfc4130.txt>).

Die wichtigsten AS2-Eigenschaften sind:

- Sichere Übertragung von strukturierten Geschäftsdaten (in unterschiedlichen Formaten wie XML, UN/EDIFACT, ANSI X.12, CSV, etc.) unter Verwendung des HTTP Protokolls
- Die Teilnehmer müssen immer empfangsbereit sein, um evtl. Daten von einem Partner empfangen zu können. Dieses Verhalten unterscheidet AS2 grundsätzlich von Mail-Systemen.
- Strukturierung der übermittelten Daten entsprechend dem **MIME** Standard
- Authentifizierung und Verschlüsselung der übermittelten Daten entsprechend S/MIME unter Verwendung von privaten oder öffentlichen Zertifikaten
- Authentifizierte Quittungen werden zu den ursprünglichen HTTP Nachrichten als **MDN (Message Disposition Notification)** generiert, so dass der Empfänger der Daten nicht leugnen kann, diese erhalten zu haben. MDNs werden nur auf Anforderung des Senders von Daten erzeugt.

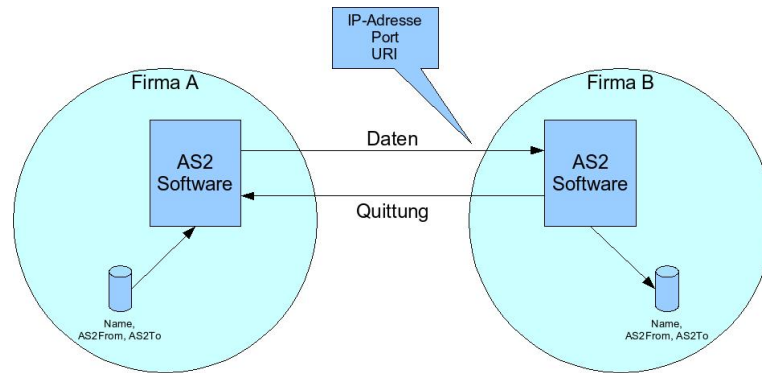
Allgemeiner Ablauf

AS2 ist als Protokoll zur sicheren Datenübertragung über das Internet definiert. In unserem Beispiel tauschen Firma A und Firma B Geschäftsdaten miteinander aus. Beide besitzen eine Anbindung an das Internet. Es besteht aber keine direkte Kopplung der EDV-Systeme dieser beiden Firmen.



AS2 setzt auf HTTP auf und ermöglicht es den beiden Unternehmen, Daten auszutauschen, wobei die verfügbare ständige Internet-Verbindung als Basis genutzt wird.

Der Ablauf ist in etwa wie folgt. Firma A möchte eine Datei zu Firma B übertragen. Die AS2-Software bei Firma A ordnet der Datei drei wesentliche Attribute zu, ihren Namen sowie das Paar (AS2From, AS2To). Das sind die AS2-bezogenen Kennungen der beiden Datenaustausch-Partner. D.h. Firma A und Firma B vereinbaren vor Beginn des Datenaustauschs dieses Paar von Kennungen, um ihre Datenaustausch-Beziehung eindeutig zu identifizieren.



Dateiname, AS2From und AS2To werden bei Firma A zusammen mit dem Datei-Inhalt gemäß MIME¹-Standard verpackt. Danach baut die AS2-Software von Firma A eine HTTP-Verbindung über das Internet zu Firma B auf und sendet das MIME-Paket in einem Rutsch zur AS2-Software von Firma B. Firma B quittiert in derselben Session, worauf diese beendet wird. Die AS2-Software von Firma B kann dem empfangenen MIME-Paket den Namen der Datei sowie das (AS2From, AS2To)-Paar entnehmen und für die weitere Verarbeitung der Daten nutzen.

Verbindungsaufbau

Wie aus dem Bild im vorigen Abschnitt hervorgeht, werden für den Verbindungsaufbau drei Parameter benötigt:

- IP-Adresse
- Port
- URI

Die Grundzüge von TCP/IP-basierter Kommunikation zu erklären, übersteigt die Möglichkeiten dieses Dokuments. Die folgenden Ausführungen mögen als Erläuterung reichen. Wer detailliertere Informationen sucht, sei auf die reichhaltig verfügbare Literatur zum Thema verwiesen.

IP-Adresse

Über die IP-Adresse wird der Computer, zu dem die Verbindung aufgebaut werden soll, eindeutig identifiziert. Während IP-Adressen in lokalen Netzen weitgehend frei definiert werden können, müssen IP-Adressen von Computern, die im Internet stehen, global registriert werden, wodurch sichergestellt ist, dass es nicht zu Doppel-Vergaben kommt. Die IP-Adresse besteht aus vier durch Punkt getrennten Zahlenwerten, z.B. 66 . 249 . 93 . 99.²

Port

Die IP-Adresse bietet Zugang zu einem eindeutig identifizierten Computer im Internet. Nun können allerdings auf einem Computer diverse unterschiedliche Dienste gleichzeitig implementiert sein, z.B. FTP, Mail, Web-Server oder AS2-Server. Zur Auswahl des Dienstes auf dem Zielsystem wird daher neben der IP-Adresse eine weitere Zahl benötigt, nämlich die Port-Nummer.

¹ Multipurpose Internet Mail Extensions, s. <http://www.ietf.org/rfc/rfc2045.txt>

² Um den Zugriff auf Rechner im Internet komfortabler zu gestalten, werden in den meisten Fällen Rechnernamen anstelle von IP-Adressen verwendet, die über DNS (Domain Name Service) auf IP-Adressen abgebildet werden

URI

Innerhalb eines über IP-Adresse und Port ausgewählten Dienstes auf einem bestimmten Computer im Internet kann es wiederum verschiedene Angebote geben, die unterschieden werden müssen. Bei HTTP erfolgt dies über den POST-Request-URI, kurz URI³.

Beispiel

<http://www.google.de/microsoft>

Hiermit wird die Microsoft-spezifische Google-Suchseite ausgewählt. Http ist die Protokoll-Kennung, www.google.de ist der Rechnername und /microsoft ist der URI, der innerhalb des Dienstes „Web-Server“ auf www.google.de das Angebot „Microsoft-spezifische Suche“ auswählt.

Da AS2 auf HTTP aufsetzt, wird auch hier ein URI verwendet, um potenziell verschiedene Anwendungen innerhalb eines per IP-Adresse und Port identifizierten AS2-Servers anzusprechen.

Quittungen

Standardmäßig schickt die AS2-Software von Firma B eine sehr kurze Quittungs-Nachricht an den Sender der Daten zurück, die besagt, dass das MIME-Paket komplett empfangen wurde. Diese Quittung sagt nichts darüber aus, ob die Daten erfolgreich verarbeitet werden konnten.

Das AS2-Protokoll sieht weitergehende Quittungen, sogenannte Message Disposition Notifications (MDN) vor, mit denen zusätzliche Informationen über den Erfolg der Verarbeitung an den Absender der Daten geschickt werden können.

Die Entscheidung, welche Quittungs-Form verwendet werden soll, liegt beim Sender der Daten. Fordert der Sender eine MDN an, so muss der Empfänger diese Anforderung erfüllen.

Innerhalb von e-AS2 bezeichnen wir die Quittungen auch als Acknowledgements, kurz: Ack. Die Art des Ack, die vom Empfänger angefordert wird, ist konfigurierbar.

Verschlüsselung und Signatur

AS2 sieht den Einsatz von asymmetrischen Kryptographie-Verfahren vor, um den Datenversand abzusichern. Auch an dieser Stelle muss gesagt werden, dass eine erschöpfende Darstellung dieser Thematik den Rahmen dieser Dokumentation sprengen würde. Es sei wiederum auf die verfügbare Literatur zum Thema verwiesen. Hier nur einige grundsätzlich Erläuterungen.

Verschlüsselung bewirkt, dass die Daten, die zwischen zwei Kommunikations-Partnern ausgetauscht werden, von Dritten nicht eingesehen werden können. Verschlüsselt wird zielgerichtet für den gewünschten Empfänger der Daten. Nur dieser kann die verschlüsselten Daten wieder lesbar machen. Die Daten sind so auch auf dem Kommunikationsweg durch das Internet gegen unbefugten Zugriff geschützt.

Signatur bewirkt, dass der Empfänger der Daten diese eindeutig dem Absender zuordnen kann. Ist die Signatur-Prüfung nach dem Empfang erfolgreich, weiß er nicht nur, dass der Absender wirklich der war, für den er sich beim Einliefern des MIME-Pakets ausgegeben hat, sondern auch, dass die Daten auf dem Übertragungsweg nicht verändert wurden. Die Integrität der Daten ist sichergestellt.

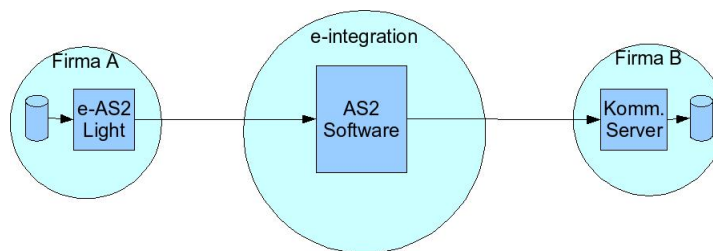
³ Die Abkürzung URI steht für Uniform Resource Identifier (einheitlicher Bezeichner für Ressourcen).

Verschlüsselung und Signatur können miteinander kombiniert werden. Die Entscheidung, ob verschlüsselt und/oder signiert werden soll, liegt beim Absender der Daten. Der Einsatz von Kryptographie ist nicht obligatorisch.

Die AS2-Kryptographie basiert auf sogenannten Zertifikaten, die vorab zwischen den beiden Kommunikations-Partnern ausgetauscht werden müssen.

Abwicklung über das e-integration Clearing Center

Die bisherige Darstellung ging davon aus, dass die beiden Geschäftspartner Firma A und Firma B direkt Daten miteinander austauschen. Die Lösung e-AS2 von e-integration ermöglicht es, dass Sie all ihre Geschäftspartner über das Clearing Center von e-integration erreichen. Sie etablieren nur eine einzige AS2-Verbindung, nämlich zum e-integration Clearing Center.



e-integration leitet ihre Daten an Ihre Geschäftspartner weiter und umgekehrt. Dabei ist die Weiterleitung in beiden Richtungen auch möglich, wenn Ihr Geschäftspartner nicht das AS2-Protokoll für die Kommunikation verwendet.

Das Bild gibt eine Situation wieder, bei der die Daten mit dem AS2-Protokoll zwischen Firma A und e-integration übertragen werden. Die Daten werden dann mit einem nicht näher spezifizierten Kommunikationsprotokoll⁴ zu Firma B weitergeleitet.

Die e-AS2-Lösung in der Version „Light“ wurde zielgerichtet für diese Art des Datenaustauschs über das e-integration Clearing Centers entworfen

Der AS2-Betrieb über e-integration hat für den Anwender den Vorteil von äußerst geringen Investitions- und Betriebskosten. Über diesen Weg kann der elektronische Datenaustausch mit AS2 und nicht AS2-fähigen Partnern unabhängig vom Datenformat erfolgen: Je nach Partner-Profil übernimmt e-integration nicht nur eine Protokollkonvertierung zur Anbindung sämtlicher Partner sondern auf Wunsch auch die Konvertierung der Datenformate.

⁴ Das e-integration Clearing Center stellt eine Reihe unterschiedlicher Leitungen (ISDN, Internet) und Protokolle (X.400 P1 oder P7, FTP, Secure-FTP, OFTP, SMTP und AS2) zur Verfügung. Diese Protokolle können beliebig untereinander kombiniert werden.