AS2 (Applicability Statement 2):

Description and Parameter

Introduction

This document clarifies the following questions concerning the topic AS2:

- What is AS2?
- How does AS2 work and which prerequisites have to be fulfilled?
- What are the advantages of AS2?
- What about the costs of AS2 compared to Value Added Networks (VANs)?

A list of parameters and their short description will follow which is an agreement of the workgroup “Communication” of EDI Users of Trade.

What is AS2?

AS2 (Applicability Statement 2) is a version of EDIINT (EDI via internet), which uses the growth of the internet and which offers companies a possibility for an uncomplicated and cheap involvement of already existing and new B2B-partners.

This means: everyone who is able “to surf in the internet”, already uses the necessary infrastructure and is able to establish an AS2 conforming software in order to exchange documents with other companies, also using an AS2 software.

AS2 is a specification for data exchange, to perform the task of sending and receiving data via a secure connection. A check or validation of the data content doesn’t take place.
AS2 works with a kind of “envelope”, in which data is imbedded, so that it is possible to send it with HTTP-protocol, which is a core technology of the World Wide Web, via the internet (or within another network, which is based on TCP/IP). It is a quick and direct transfer, without using a mailbox (for example Telebox X.400).

AS2 is able to transmit every kind of document and it’s suited especially for the traditional EDI transactions. The data to be sent will be prepared by internal systems and will be transferred via an AS2 communication software.

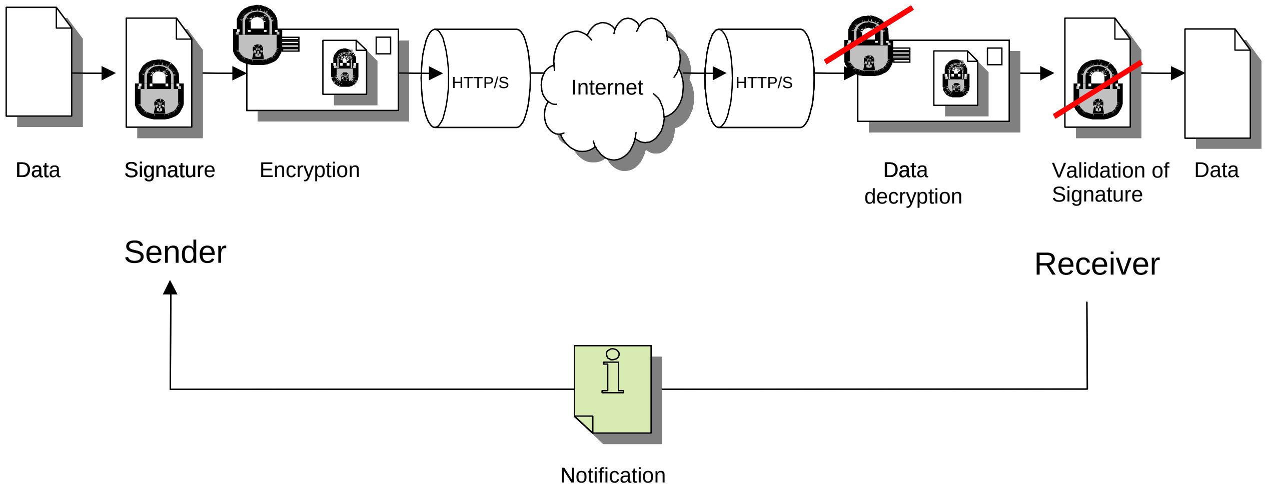
How does AS2 work and which prerequisites have to be fulfilled?

For the data exchange via AS2 a communication module is needed both on the side of the sender and on the side of the receiver. You can find a list of certified software at http://www.drummondgroup.com.

This module works with an “envelope”, which imbeds electronically business documents independent of the format (EDI, XML, csv, txt, etc.). The message is signed electronically (no qualified digital signature by the meaning of the signature law), encrypted – and where required compressed – and is sent to the business partner. The electronic signature of the message guarantees, that sender and receiver are de facto the business partners they pretend to be. To make sure, that the recipient received the document unmodified and was able to decompress and decrypt the message error-free, the received document is validated with regard to originality and integrity and a confirming message is sent back automatically.

The transmission uses the HTTP/HTTPS-protocol in form of a point-to-point connection. The choice of the protocol will be agreed on bilaterally. To exchange data, only an EDIINT software (installed on the web-server) and a dedicated line to the internet are necessary. Similar to the telephone without an answering machine, the message wouldn’t be received by your server if it isn’t available. As a result, the receiving server, too, has to be connected to the internet at the time of sending the message.

After a successful transmission the message content is available for further processing.



What are the advantages of AS2?

AS2 users are in the position to decrease the costs for the electronic data transmission of big data volume.
Because of the real time and event driven exchange of business documents, future demands on the supply chain processes will be fulfilled. Users have a benefit from an acceleration of the information flow along the whole process chain.

While using the internet it is important that the message transmission by AS2 offers security and reliability, which will be guaranteed by the EDIINT standards. For example digital certificates are able to assure, that messages reach exclusively the addressed recipient, that the data transfer is secure and that the sender is revisable. Furthermore the interposition of a VAN, (e.g. X.400) can be neglected, because the data will be transferred directly. As a result an unauthorized reading or modification of the data is not possible.

What about the costs of AS2 compared to VANs?

The usage of VANs, such as for example the mailbox system of X.400 for the electronic exchange of business data (e.g. orders, invoices), causes among other primarily volume dependent costs. Because of the rising cross-linking between trade partners and because of the rising data volume the costs are increasing continuously. As soon as a transition point from one VAN to another VAN is necessary, in order to reach for example a certain international partner, the costs will raise significantly.

The electronic exchange of data via the internet on the base of the new, in the USA already established standard AS2 causes no expenses anymore. The only remaining expense factors are the provision and usage of the internet connection and the investment in an AS2 supporting software.

Parameter adjustments & specifications of the workgroup “Communication” of AKH

AS2 Parameters		**AKH workgroup Communication**	**Description**
Security	**Communication-Certificates**	- Class 2 type - self-signed - minimum validity period 2, max. 5 years	**One certificate for the signature and encryption.** **Trusted:** Certificate Authority (3. level) assigns, administrates, controls certificates **Self-Signed:** Using Self-signed certificates simplifies the management of certificates **Certificates must be renewed at least every 5 years.**
	Communication-Digital-signature	SHA1	Before the data will be encrypted, a signature will be created and added to the transfer. After the reception the receiver checks the signature. This method ensures that the message was really created by the original sender. SHA1 is one option of the signature algorithm and is recommended.
	Encryption	TripleDES	The sender encrypts the data, the receiver decrypts the data and checks the data integrity, to ensure, that no unauthorised modifications were done. Triple DES are state-of-the-art stable and secure.
	Length of session key	>= 128 bits	Encryption of session for a secure HTTPS-transfer.
	Length of public/private key	2048 bits	The public resp. private key (stays at the owner) will be created during the asymmetric encryption method . By using the public key of the receiver the sender of a message is able to encrypt the content of a message against the reading of third. Then only the receiver is able to decrypt the data with his private key. The usage of the private key is the only possibility to encrypt data which was decrypted with the public key. The sender of a message uses the private key for signing. By using the public key of the sender the receiver is able to check the integrity of a message.
Transport layer	**Internet connection**	- permanent internet connection - fixed and public URL address mandatory	A permanent internet connection must be given.
	Transport Protocol	HTTPS to secure AS2-From and AS2-To HTTP	HTTPS is a special form of HTTP, which offers more security (reliability and authenticity) by using SSL. This will be used to avoid "listening" during the transmittance of sensitive data.
Client Authentication		optional	**HTTPS:** encrypts and is more secure **HTTP:** clear text (Name und password are visible)
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.	A string to identify the sender.
	Receiver (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.	A string to identify the receiver.

Message Disposition Notification=MDN	**MDN**	mandatory	A MDN will be sent back. It provides the strongest evidence, because it confirms the reception of the message and most likely the designated receiver, because he was the owner of the private certificate.
	MDN signed	Yes	Signing of the delivery notification
	MDN encrypted	No	Encrypting of the delivery notification
	Synchronous/ Asynchronous	Synchronous (asynchronous allowed; transmission mode bilaterally agreed)	Synchronous: The MDN will be sent within the exisiting connection to the sender of the message, to confirm the successful receipt of the data at the receiver. Asynchronous: The MDN will be sent in a separate connection to the sender of the message, to confirm the successful receipt of the data at the receiver.
Formats	**Multipurpose Internet Mail Extensions (MIME)**	MIME type coherent with content	MIME is an Internet standard to define data types. In the broader sense a MIME-capable client has the possibility to add any binary files to a message.
	Secure Multipurpose Mail Extension (S/MIME)	Yes	S/MIME is a proposal for the IETF (Internet Engineering Task Force = an open, international community of developers, users, researchers, etc. of the internet) with regard to encryption and signing of messages as a standard.
	Compressed	Accepted and optional (mode bilaterally agreed)	The compression of data will decrease the transfer volume .
AS2 Version		bilaterally agreed	
Port inbound/ outbound		port bilaterally agreed	Defined, bilaterally agreed ports have to be cleared for the interchange.