BDEW Bundesverband
der Energie- und
Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin

Energie-Info

Leitfaden "Implementierung von AS2 in Unternehmen der Energiewirtschaft"

Empfehlungen zur Implementierung des Übertragungsweges AS2 für Electronic Data Interchange in der deutschen Energiewirtschaft

BDEW-Projektgruppe Sicherheit beim elektronischen Datenaustausch

Guideline "Implementation of AS2 in energy industry companies"

Recommendations on implementation of the AS2 standard for secure electronic data interchange in the German energy industry

BDEW project group for security in electronic data exchange

Version: 1.0

Berlin, 5. November 2009

Inhalt

Seite

Contents

page

1. Ziel des Leitfadens

Die "Studie über sichere webbasierte Übertragungswege" von VEDIS beschreibt anschaulich welche Standards es bei den Übertragungswegen gibt und unter welchen Bedingungen welcher Kommunikationsstandard zum Einsatz kommen sollte. Dieser Leitfaden bietet für den Übertragungsweg AS2 drei Hilfen:

- VEDIS-Empfehlungen für standardisierte AS2-Parameter in der Energiewirtschaft
- VEDIS-Formulare für standardisierte Marktpartneranbindungen
- VEDIS-Empfehlungen zum Betrieb hinsichtlich Technik und Organisation

Alle drei Hilfen sind für Energieversorgungsunternehmen interessant, unabhängig ob diese den elektronischen Nachrichtenaustausch in Eigenregie mit eigenem Personal und System betreiben oder dafür einen Dienstleister nutzen (in der Energiewirtschaft bspw. EDI-Dienstleister, EDI-Clearing-Center oder DataHub genannt).

Der BDEW wird seine Marktpartnerdatenbank (BDEW-Codenummerdatenbank) um Angaben zur AS2-Kommunikation erweitern. Der BDEW bittet die Marktpartner ihre AS2-Kommunikationseinstellungen entsprechend dem BDEW bereitzustellen.

1. Purpose of the Guideline

The VEDIS "Study on secure web-based file transfer" describes clearly what standards regarding transfer channels already exist and under what conditions the various communications standards should be applied. This Guideline offers three aids in the implementation of AS2:

- VEDIS recommendations for standardised AS2 parameters in the energy industry
- VEDIS forms for standardised market partner connections
- VEDIS operational recommendations on technology and organization

All three of these aids are of interest to energy supply companies, irrespective of whether these operate their own electronic information exchange system using their own staff or whether they use the services of an external provider (in the energy industry, for example, these are EDI service providers, so-called EDI clearing centres or DataHubs).

BDEW [German Association of Energy and Water Industries] will extend its market partner database (BDEW code number database) by information concerning AS2 communication. BDEW is therefore requesting its market partners to provide information on their AS2 communication parameters to BDEW.

2. AS2-Parameter

2.1 AS2-ID

Die AS2-ID muss eine Marktpartner-Identifikationsnummer[1] sein.

2.2 AS2-Zertifikat

2.2.1 Zertifikat-Umfang

Nutzung eines Zertifikates ausschließlich für die AS2-Kommunikation.

Das AS2-Zertifikat dient der Signatur und Verschlüsselung.[3]

Wahlfreiheit: Es kann pro AS2-ID ein eigenes Zertifikat verwendet werden oder es kann pro AS2-Server ein eigenes Zertifikat verwendet werden (das dann für mehrere AS2-IDs verwendet wird).

2.2.2 Zertifikats-Art

X.509 v3 beglaubigt nach VEDIS-CP.[5]

2. AS2 parameters

2.1 AS2 ID

The AS2 ID must be a market partner identification number[2].

2.2 AS2 certificate

2.2.1 Scope of certificate

The certificate shall be used solely for AS2 communications.

The AS2 certificate is used for digital signatures and encryption.[4]

Options: It is possible to use one certificate per AS2 ID or one certificate per AS2 Server (in the latter case, this is then used for several AS2 IDs).

2.2.2 Type of certificate

X.509 v3 certified according to VEDIS-CP.[6]

---

[1] In Deutschland kann die Marktpartneridentifikationsnummer je nach Geschäftsprozess beispielsweise eine ILN (Internationale Lokationsnummer), eine BDEW-Nummer, eine DVGW-Nummer oder ein Edigas-Code sein (Vgl. Kommunikationsrichtlinie unter www.edi-energy.de).

[2] In Germany, the market partner identification number can, for example, be an ILN (International Location Number), a BDEW number, a DVGW number or an Edigas code, depending on the business process involved (cp. Kommunikationsrichtlinie [communication guideline] on www.edi-energy.de).

[3] Zertifikate die von Menschen benutzt werden, bspw. bei manueller Mail-Kommunikation sind als getrennte Zertifikate für Signatur und Verschlüsselung zu verwenden (vgl. VEDIS-Dokument CP).

[4] Certificates that are to be used by people, e.g. for manual mail communications, have to be used as separate certificates for digital signature and encryption (cf. VEDIS document CP).

[5] Energie-Info PKI-Zertifizierungsrichtlinie vom Januar 2007.

[6] Energy information PKI certification guideline dated January 2007.

2.2.3 Gültigkeitsdauer

Minimale Gültigkeitsdauer: 2 Jahre.
Maximale Gültigkeitsdauer: 5 Jahre.

2.2.4 Digitale Signatur

SHA1.

2.2.5 Verschlüsselung

3DES.

2.2.6 Länge des öffentlichen/privaten Schlüssels (X.509)

Gemäß den Empfehlungen der Bundesnetzagentur ≥ 1024 Bit Länge des öffentlichen/
privaten Schlüssels (X.509).

2.2.7 Sonstige Zertifikat-Felder

So wenig wie möglich angeben, damit das Zertifikat so lange wie möglich aktuell bleibt, daher reichen Antragsteller und Aussteller.

- Felder Antragsteller:

  CN = Name des Servers/Dienstes/Anwendung, bspw. Domain inkl. Subdomain.

- Freiwillige Felder, sofern nicht über CN ersichtlich:

  O = Name der Firma/Behörde, von der die technischen Komponenten betrieben werden. Der Organisationsname O muss der komplette Firmenname oder Behördenname aus dem Handelsregister o. ä. sein.

  C = Länderkürzel nach ISO 3166, bspw. DE.

2.2.8 Dateityp

.cer

2.2.9 Dateiname

<Marktpartneridentifikationsnummer>_<Kurzname>_<Ausstellungsjahr>.cer

2.2.3 Validity

Minimum period of validity: 2 years.
Maximum period of validity: 5 years

2.2.4 Digital signature

SHA1.

2.2.5 Encryption

3DES.

2.2.6 Length of the public/private key (X.509)

According to the recommendations of the German Federal Network Agency ≥ 1024 bit length of the public / private key (X.509).

2.2.7 Other certificate fields

Enter as little information as possible to ensure that the certificate remains valid for as long as possible, therefore the names of applicant and issuer are sufficient.

- Fields concerning applicant:

  CN = name of the server/service/application, e.g. domain including sub-domain.

- Optional fields if not obvious from CN :

  O = name of company/organisation operating the technical components. The organisation name O has to be the complete name of the company or organisation as it appears in the companies register or similar record.

  C = country code according to ISO 3166, e.g. DE for Germany.

2.2.8 File type

.cer

2.2.9 File name

<Market partner identification number>_<abbreviated name>_<year of issue>.cer

2.3 Transportschicht

2.3.1 Transport-Protokoll

http (Empfohlen).

https kann benutzt werden, um den Header (u. a. AS2-To and AS2-From) abzusichern.[7]

2.3.2 URL zum AS2-Adapter (AS2-URL)

Vollständig qualifizierter Name der Domäne (URL) muss angegeben werden.

2.3.3 Verbindung zum Internet

Permanente Internet-Verbindung mit mindestens einer festen IP-Adresse.

2.3.4 Freischalten von IP-Adressen in den Firewalls

Die Verwendung eines IP-Adressfilters in den Firewall-Systemen wird dringend empfohlen. Der HTTP-Standardport 80 bzw. der HTTPS-Standardport 443 sollte bevorzugt verwendet werden.

2.4 Sonstige AS2-Parameter

Aus Interoperabilitätsgründen sollte von der Angabe weiterer AS2-Parameter über die in diesem Text spezifizierten hinaus gänzlich abgesehen werden. Da die Header-Informationen bei der Übertragung nicht mit der Nachricht verschlüsselt werden, sollten sie auf den notwendigen Umfang reduziert bleiben.

2.3 Transport layer

2.3.1 Transport protocol

http (recommended)

https can be used to make the header secure (including AS2-To and AS2-From).[8]

2.3.2 URL to AS2 adapter (AS2-URL)

Full qualified name of the domain (URL) must be entered.

2.3.3 Internet connection

Permanent Internet connection with at least one fixed IP address.

2.3.4 Activation/unlocking of IP addresses in the Firewalls

We urgently recommend the use of an IP address filter in Firewall systems. HTTP standard port 80 or HTTPS standard port 443 should be preferred.

2.4 Other AS2 parameters

In order to ensure interoperability, no other AS2 parameters whatsoever other than those specified in this text should be used. Header information should be kept to a minimum since the header information is not encrypted with the remaining message when the message is transmitted.

---

[7] Eine doppelte Verschlüsselung (Nachricht und Transportweg) ist nicht erforderlich, weil die Nachricht bereits verschlüsselt ist und im Regelfall die Kommunikationspartner öffentlich bekannt sind bspw. bei Bilanzierung oder Fahrplangeschäften.

[8] Double encryption (message and transport path) is not required since the message is already encrypted and communication partners are normally publicly known, e.g. for account balancing or schedule-based transactions.

2.5 Exkurs: Prüfung von AS2-Parametern

Das EDI-System bzw. der AS2-Adapter sollte folgende Prüfung beim Empfang durchführen:

1. Prüfung auf bekannte Kombination von Absender AS2-ID mit Empfänger AS2-ID.
2. Prüfung AS2-ID mit dem zugehörigen AS2-Zertifikates (d. h. dem Signatur-Teil für Authentizität des Absenders und Unversehrtheit der Nachricht).
3. Optional: Prüfung, ob die Marktpartner-ID in der EDIFACT-Nachricht zur AS2-ID passt, weil bei den meisten EDI-Systemen in der Weiterverarbeitung die Nachricht (EDIFACT-Datei) vom "Umschlag" (des AS2-Kommunikations-standards) getrennt erfolgen wird.

2.5 Digression: Verification of AS2 parameters

The EDI system or the AS2 adapter should carry out the following tests when receiving messages:

1. Test for known combination of sender AS2 ID with recipient AS2-ID.
2. Check the AS2 ID against the corresponding AS2 certificate (i.e. check the digital signature part for authenticity of sender and integrity of message).
3. Optional: Check whether the market partner ID matches the AS2 ID in the EDIFACT message, since most EDI systems separate the message (EDIFACT file) from the “envelope” (of the AS2 communication standard).

3. Standardisierter Austausch von AS2-Parametern

Es sind grundsätzlich zwei Arten von AS2-Formularen möglich:

a) AS2-Kommunikationsformular mit individuellen Vereinbarungen zur AS2-Strecken.

b) AS2-Steckbrief mit einheitlichen Einstellungen für alle Marktpartner.

Ob ein Kommunikationsformular oder ein Steckbrief zum Einsatz kommt muss jedes Unternehmen individuell entscheiden. Grundsätzlich ist der Steckbrief das wirtschaftlichere Verfahren und wird auch von VEDIS empfohlen, weil sich der Steckbrief in eine spätere Verbandsveröffentlichung integrieren lässt mit welcher die Marktpartner nicht mehr einzeln jede Einstellung von jedem Marktpartner abfragen müssen.

Die Anbindung eines neuen Marktpartners sollte bei zeitkritischen Geschäftsprozessen über einen Verbindungstest erfolgen. Für diesen ist ein standardisiertes Kommunikationsformular zu verwenden. Im Anhang sind das VEDIS AS2-Kommunikationsformular und der VEDIS AS2-Steckbrief aufgeführt.

3. Standardised exchanging of AS2 parameters

Basically, two kinds of AS2 forms are available:

a) AS2 contact form with individual agreements on AS2 links.

b) AS2 profile with uniform parameters for all market partners.

Each company must decide for itself whether it wants to use a contact form or a profile. Essentially, the profile is the more efficient method and is also recommended by VEDIS because the profile can be integrated into a later association publication by means of which various market partners no longer have to request every parameter from each individual market partner .

Connection of a new market partner should be made using a connection test for all time-critical business processes. A standardised contact form is to be used for this purpose. The appendix contains the VEDIS AS2 contact form and the VEDIS AS2 profile.

4. Technik

Der Übertragungsweg AS2 erfordert auf Absender- wie Empfängerseite einen sogenannten AS2-Adapter. Technisch kann dieser AS2-Adapter auf drei verschiedenen Wegen implementiert werden:

a) AS2-Adapter integriert im EDI-System

b) AS2-Adapter integriert im Anwendungssystem

c) AS2-Adapter separat zur eigenen System-Landschaft

Für den professionellen Dauereinsatz empfiehlt sich ein vollwertiges EDI-System, das auch die Anforderungen zur sogenannten 1:1 Kommunikation umfassend beherrscht[9].

Für eine Übergangszeit sind auch die Varianten b und c möglich, da nicht alle Geschäftsprozesse in GPKE/GeLi Gas, GABi usw. gleichzeitig auf AS2 umgestellt werden müssen.

4. Technology

Communications using AS2 requires an AS2 adapter both on the sending and the receiving side. Technically speaking, this AS2 adapter can be implemented in three different ways:

a) AS2 adapter is integrated in the EDI system

b) AS2 adapter is integrated in the application system

c) AS2 adapter is implemented separately for the company's own system environment

For long-term professional use, a full-scale EDI system that also fulfils all the requirements of so-called 1:1 communication is recommended[10].

For an interim period, the b and c variants are possible, since in these cases not all business processes - GPKE/GeLi, GaBI etc. - have to be converted to AS2 all at the same time.

[9] Vgl. Kommunikationsrichtlinie (aktuelle Fassung siehe www.edi-energy.de).

[10] Cp. Kommunikationsrichtlinie (current version see www.edi-energy.de).

5. Eigene AS2-Kompetenzen

Es sollte ein grundsätzliches Verständnis zum Ablauf der Kommunikation über AS2 vorhanden sein. Die Kommunikation über AS2 ist für die Sachbearbeiter in der Fachabteilung zunächst ungewohnt, aber im Alltag einfacher in der Abwicklung, weil viele Probleme der Mailkommunikation bei AS2 gar nicht auftreten können.

5.1 Prinzip der AS2-Kommunikation

Das Prinzip wird im Ablaufdiagramm der VEDIS-Studie „Studie über sichere webbasierte Übertragungswege“ (Kapitel 6.3) eingehend beschrieben.

5.2 MDN

Es sollte sicher gestellt werden, dass Mitarbeiter von ihrem Anbieter auch gezeigt bekommen, wie sie sich eine MDN (digitale Zustell-Quittung) anzeigen können, falls es zum Klärungsfall einer fristgerechten Zustellung kommt. Die MDN wird im AS2-Adapter erzeugt und kann im Regelfall im EDI-System oder über ein Web-Fontend mit wenigen Mausklicks heruntergeladen werden. Sollten ein EDI-Dienstleister eingesetzt werden, sollte das Verfahren getestet werden, damit die Mitarbeiter damit vertraut sind.

5. Own AS2 competencies

Staff should have a basic understanding of communications processes using AS2. Initially, the persons responsible in a specialist department will be unfamiliar with communications via AS2, but these are easier to handle in everyday use because a lot of problems involved in mail communications no longer occur if AS2 is used.

5.1 Principle of AS2 communication

The principle is described in detail in the flowchart of the VEDIS study “Study on secure web-based file transfer” (Chapter 6.3).

5.2 MDN

It should be ensured that your provider shows your staff how to display an MDN (digital delivery receipt) in case there is any dispute about the meeting of delivery deadlines. The MDN is created in the AS2 adapter and can normally be downloaded in the EDI system or with just a few mouse clicks via a Web front-end. If an EDI provider is to be used, the procedure should be tested so that the staff can become familiar with it.

5.3 Zertifikatswechsel

AS2-Zertifikate müssen wie jedes Zertifikat nach einer gewissen Zeit durch ein neues Zertifikat ersetzt werden. Die AS2-Zertifikatswechsel sollten beim Eigenbetrieb mit eigenem Personal durchgeführt werden können. Je nach verwendeten AS2-Adapter ist das mit einigen Mausklicks nach Anleitung erledigt, so dass auf die Beauftragung von externem Personal auf Dauer verzichtet werden kann und auch die terminliche Abstimmung vereinfacht werden kann. Ein Zertifikatswechsel sollte drei Wochen im Voraus angekündigt werden, um dem Partner eine angemessene Reaktionszeit zu gewähren.

5.3 Certificate renewal

AS2 certificates – as any other certificates – have to be renewed at periodic intervals. It should be possible for AS2 certificate renewal to be carried out by the company's own staff if they are using a proprietary system. Depending on what AS2 adapter is being used, this can be done with a few simple mouse clicks following a set of instructions, meaning that in the long-run external staff does not have to be called in to do this, and it also makes the coordination of deadlines easier. A certificate renewal should be announced three weeks in advance so that partners have sufficient time to respond.

Ansprechpartner:

Rainer Lautenbacher
Telefon: +49 30 300199-1661
rainer.lautenbacher@bdew.de

6. Anhang

6. Annexes

AS2 Steckbrief

AS2 Profile

	Partnername	Partner name
	Marktpartner-ID	GLN

Contact Administration

1.	**Ansprechpartner**	**Primary Contact**
	Name	Name
	Telefon	Phone
	E-Mail	E-mail
2.	**Ansprechpartner**	**Backup Contact**
	Name	Name
	Telefon	Phone
	E-Mail	E-mail

Contact Technical

1.	**Ansprechpartner**	**Primary Contact**
	Name	Name
	Telefon	Phone
	E-Mail	E-mail
2.	**Ansprechpartner**	**Backup Contact**
	Name	Name
	Telefon	Phone
	E-Mail	E-mail

Network Production

AS2-URL	
Inbound public IP-Address	(Firewall)
Outbound public IP-Address(es)	(Firewall)
Port	(provide access if necessary)

AS2-Parameter Production	
AS2-ID	
MDN Mode	Synchronous
MDN Signed	Yes
Signature Algorithm	SHA-1
Encryption Algorithm	3DES
Compression	Yes
Content-Type	Binary
Certificate valid to (yyyy-mn-dd)	
Public Certificate file Advice: Insert per Drag-and-Drop	
Certificate Validation (optional) Advice: use download URL	

AS2 Kommunikationsformular

AS2 Contact form

Partnername	Partner name	e.g. Partner 1	e.g. Partner 2
Marktpartner-ID	GLN		
Contact Administration			
1. Ansprechpartner	**Primary Contact**		
Name	Name		
Telefon	Phone		
E-Mail	E-mail		
2. Ansprechpartner	**Backup Contact**		
Name	Name		
Telefon	Phone		
E-Mail	E-mail		
Contact Technical			
1. Ansprechpartner	**Primary Contact**		
Name	Name		
Telefon	Phone		
E-Mail	E-mail		
2. Ansprechpartner	**Backup Contact**		
Name	Name		
Telefon	Phone		
E-Mail	E-mail		

Network Production		
AS2-URL		
Inbound public IP-Address (Firewall)		
Outbound public IP-Address(es) (Firewall)		
Port (provide access if necessary)		
AS2-Parameter Production		
AS2-ID		
MDN-Mode	Synchronous	Synchronous
MDN Signed	Yes	Yes
Signature Algorithm	SHA-1	SHA-1
Encryption Algorithm	3DES	3DES
Compression	Yes	Yes
Content-Type	Binary	Binary
Certificate valid to (yyyy-mn-dd)		
Public Certificate file Advice: Insert per Drag-and-Drop		
Certificate Validation (optional) Advice: use download URL		