This document is a translation of the specifications issued by the Federal Network Agency (Bundesnetzagentur – BNetzA) as well as on the most recent version of the edi@energy document "Regelungen zum Übertragungsweg 2.2 (Rules of transmission 2.2)" valid at the time of translation, namely the version published on 2 April 2024, and contains an excerpt of the most important communication elements.

The complete document in German language is published at the following link:

https://www.edi-energy.de/index.php?id=38&tx_bdew_bdew%5Buid%5D=2305&tx_bdew_bdew%5Baction%5D=download&tx_bdew_bdew%5Bcontroller%5D=Dokument&cHash=d146bff7cf320096c23a94c55f59fcb4

Updated versions in German language will be published at this link:

https://www.edi-energy.de/index.php?id=38&tx_bdew_bdew%5Bview%5D=future&tx_bdew_bdew%5Baction%5D=list&tx_bdew_bdew%5Bcontroller%5D=Dokument&cHash=325de212fe24061e83e018a2223e6185

The translation shall be considered a convenience translation only; in the event of any conflict in meaning between the German and this English version, the German language version shall prevail.

This English version is published on the website of Trading Hub Europe GmbH

Rules for the secure exchange of transfer files via BDEW-AS4-Profile

Version:	**2.2**
Publication date:	2 April 2024
Applicable from:	1 October 2024
Original Document Owner:	BDEW

Table of contents

1 Introduction

This document governs the security and protection mechanisms to be used for electronic data transfer between the German energy industry's market partners involving the use of the transfer protocol[1] AS4 in market communication.

According to a Federal Network Agency (BNetzA) ruling[2], the cryptographic requirements of BSI TR 03116-3 must always be observed and complied with, and the use of the BSI's Smart Metering PKI must be provided for in accordance with Section 52 (4) of the Metering Point Operation Act (MsbG).

This document describes the parameters to be used and the deviations to be applied.

1.1 Scope

The rules set out below apply to the following electricity and gas market processes[3] defined by the BNetzA, which are processed via EDIFACT: GPKE, MPES, MaBiS, WiM, GeLi Gas, GaBi Gas and KoV[4].

According to BK6-21-282, market communication for Redispatch 2.0 process data[5] via XML and the transmission of Redispatch EDIFACT messages that are not covered by MaBiS are excluded from the introduction of AS4 communication for the time being. In principle, however, AS4 can also be used for all Redispatch EDIFACT messages in the event of a bilateral and voluntary agreement between the two market partners involved.

Note: The introduction of AS4 for schedule management is described in the document "Regelungen zum sicheren Austausch im Fahrplanprozess".

This document does not address the legal consequences that may arise if the electronic data exchange is not secure because a different procedure is used.

Therefore, the following rules on transfer protocol AS4 currently apply. They also contain the associated organisational rules to be observed by the German energy industry.

---

1 In this document, "transfer protocol " refers to what is also known as "communication channel", "communication path", "transmission path" or "transmission protocol".

2 Cf. BK6-21-282 [1] and BK7-19-001 [2].

3 Cf. BK6-21-282 (tenor figure 1) [1] and BK7-19-001 [2].

4 The national regulations on the transfer protocol only apply in full to purely national business processes in accordance with KoV Annex 3. For KoV Annexes 1 and 2 (entry-exit system) only for the processes according to the application aid "Process description for capacity billing at exit points to end users" *("Prozessbeschreibung zur Kapazitätsabrechnung an Ausspeisepunkten zu Letztverbrauchern"),* as well as Appendices 4 and 5 to KoV Annex 4.

5 Cf. BK6-20-059, Annex 2, II Basic data exchange and call order processes [3] via XML (Note: All other chapters of Annex 2 fall under "Market processes"). However, this annex does not apply to installations that are already obliged to provide data in accordance with the approval of 20 December 2018 (ref. BK6-18-122) [4].

1.2 Document structure

Unless otherwise indicated, the rules apply to data exchange as part of market processes.

1.3 Introduction and delimitation for gas

The rules specified in this document must be implemented by all market partners in the gas sector participating in the electronic data exchange for the processes specified in Section 1.1 by 00:00 hrs. on 1 April 2025 at the latest. In order to ensure that the switch of the transfer protocol with all its market partners is completed by this date, it is strongly recommended to start the switch to AS4 well before this date. The period in which everyone affected by this transfer protocol switch should already have mastered the necessary functions therefore commences on 1 October 2024 at 00:00 hrs[6].

Before and during the period of the phased introduction of AS4 communication in gas market processes, from 00:00 hrs. on 1 October 2024 until 00:00 hrs. on 1 April 2025, two different versions of the rules on the transfer protocol will temporarily apply simultaneously:

> **E-mail or AS2 communication:**

"Rules on transfer protocols" with the order number **/ version 1.x**. This version of the rules on transfer protocol describes the exchange of messages as part of market processes by e-mail via SMTP or AS2 transfer protocols. They remain valid for the market processes in their current published version and are to be used for gas market processes until 00:00 hrs. on 1 April 2025 the latest for the exchange of messages by e-mail via SMTP or AS2 transfer protocols.

> **AS4 communication:**

"Rules on transfer protocols for AS4" (this document) **/ version 2.x**. This version of the rules on the transfer protocol and its successor versions describe the exchange of transfer files as part of the market processes via an AS4 web service. They are applicable for gas market processes from 00:00 hrs. on 1 October 2024 or, by voluntarily arrangement, also prior to that date.

According to the BNetzA decision[7], the use of other transfer protocols is no longer permitted for the gas-related processes mentioned in Chapter 1.1 from 00:00 hrs. on 1 April 2025.

1.4 Certificate Treble

The term "certificates" is used below to refer to the certificate treble consisting of the certificates for signature (SIG), encryption (ENC) and establishment of the TLS channel (TLS).

---

[6] The recommendation described here is based on the procedure defined by decision BK6-21-282 [1], among others, for data exchange in the electricity industry as part of the GPKE.

[7] Cf. BK7-19-001 [2].

According to the CP of the SM PKI, these three certificates cannot be applied for or exchanged individually, hence certificate treble.

2 Notifying the information recipient

In order to achieve the greatest possible level of automation in data exchange, the market partners must agree on the data exchange addresses, including the certificates to be used, before the data is sent for the first time. This includes as a minimum the URI of the AS4 web service (AS4 address) and the certificate with the public key for encrypting a transfer file for the recipient[8] of the transfer file. The URI of the AS4 web service must be taken from the available certificates in the field of the alternative name of the URI type.

The aforementioned data must be exchanged between the two parties no later than three working days (as per GPKE/GeLi Gas calendar[9]) after a market partner has been contacted for the first time. Within three working days after the exchange of the communication data, each party must have entered or made available the data of the other market partner in all systems used for market communication, so that all prerequisites for electronic data exchange are met.

Transfer files that are rejected because the transfer protocol was set up late for reasons attributable to the recipient will be deemed to have been delivered on time. In this case, the recipient is obliged to process the files according to the original date of receipt. This provision only applies to error-free transfer files.

The transfer protocol between two market partners must be retained for at least three years from the day after the last data exchange (between these two market partners). If a market partner's transfer protocol changes, the market partner is obliged to inform all market partners with whom it has exchanged transfer files within the last three years about the change. The information must be provided in good time at least 10 working days before the changeover.

Retaining the transfer protocol does not mean that an AS4 address used for data transfer and replaced by another AS4 address may not be deleted for three years.

---

8 The public keys and certificates for validating the signature and establishing the TLS channel do not need to be exchanged in advance. The signature certificate is included in every AS4 message, the certificate for establishing the TLS channel is exchanged during the connection setup.

9 Note: The working day definitions in GPKE and GeLi Gas are identical.

2.1 Initial exchange of communication parameters – notification to information recipient

When contact is made for the first time, the certificate exchange must be coordinated by telephone and e-mail if necessary, and it is always possible by calling up the issuing CA.

2.2 Updating communication parameters

As soon as a certificate of a market partner expires or has been revoked, all market partners using this certificate must search the CA for a certificate valid for this MP ID and update their communication parameters with the information contained in the certificate.

3 Transfer protocol

The AS4 protocol based on the BDEW AS4 profile is the transfer protocol used.

The Server Name Indication (SNI) extension in accordance with IETF RFC 6066 or IETF RFC 8449 must be supported and used to establish the TLS connection.

4 Communication rules

Only one transfer protocol with exactly one end point may be used between two different MP IDs. The basic idea of 1-on-1 communication is that a market partner must ensure that its internal organisational structures do not generate any additional workload for the other market partners when it comes to the transfer of the EDIFACT transfer files.

If a market partner uses several certificates for one MP ID at the same time, other market partners are permitted to communicate with this market partner using any of the valid published certificates.

Each AS4 endpoint must be accessible at all times without firewall activation.

5 Certificates and PKI

Communication is secured by using the BSI's Smart Metering PKI (SM PKI). The requirements of the Certificate Policy (CP) of the SM PKI must be complied with.

5.1 Trust service provider

The trust service providers must be a sub-CA instance within the meaning of the CP of the SM PKI.

5.2 Certificates: Parameters and requirements

The requirements for the certificates are derived from the CP of the SM-PKI used; the following applies in particular:

> The Organisational Unit ("OU") field of the subject must contain the MP-ID.

> The parameter in the "Alternative applicant name" *("Alternativer Antragstellername")* field with the UniformResourceIdentifier attribute must be present and filled with the communication address of the WebService. Multiple communication addresses in one certificate are not permitted.

5.3 Changing certificates

The holder of these certificates must have made the successor certificates available no later than 10 working days before the certificates become invalid (see Section 2 and 8). This results in an overlap period of at least 10 working days during which the previous and new certificates

are still valid at the same time. The following shall apply to this period: This overlap period allows all market partners to switch from the certificates used previously to the new certificates.

The public key for signing is transmitted with the associated certificate in every AS4 message and may therefore be used immediately by the sender of an AS4 message. The recipient of the message can validate the signature using the transmitted certificate.

A new certificate with the associated public key for establishing the TLS channel may be used immediately by both the sender and the recipient of an AS4 message, as it is transmitted when the TLS channel is established.

During the overlap period, all market partners must be able to process signed and encrypted AS4 messages with both the certificates used previously and the new certificates.

5.4 Recall and certificate revocation lists

If a certificate owner no longer wants to use the certificate or wishes to declare the certificate invalid before the validity period expires, it must have the certificate revoked via the revocation lists (CRL) of its CA provider. The rules and requirements for the revocation of certificates, the processing of revocation lists and the update and verification times are set out in the Certificate Policy (CP) of the SM PKI.

If the CRL of a CA cannot be retrieved by a CA via the Certificate Revocation List Distribution Point (CRL DP) entered in the certificate for more than 3 days or has not been renewed during the validity period, the issuing CA and all certificates listed under it must be mistrusted until a current CRL is published in accordance with the provisions of the CP. The specific possible consequences can be found in Chapter 9.

6 Rules for exchanging meta information

For the exchange of transfer files for market processes, the fields within the "PartProperties" element are filled as follows:

> BDEWDocumentType: EDIFACT name of the message type according to UNH DE0065
> BDEWDocumentNo: Data exchange reference from UNB DE0020
> BDEWDocumentDate: Date stamp for creation in YYYY-MM-DD format

Not used:

> BDEWFulfillmentDate
> BDEWSubjectPartyID
> BDEWSubjectPartyRole

7 AS4 profile services

7.1 Test service

Before transfer files are exchanged for the first time, the test service should be used to test the basic availability and the establishment of the connection to the target of the AS4 web service call (see BDEW AS4 profile)).

Service = "http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service"
Action = "http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test"

Calling up the test service involves sending a transfer file, the text content of which can be arbitrary, and the synchronised receipt of the AS4 delivery acknowledgement.

7.2 Changing the transfer protocol

Before transfer files are exchanged for the first time using the services described in the BDEW AS4 profile, it should be ensured that the receipt and dispatch of AS4 messages between the market partners involved is actually possible. The general availability and the establishment of the connection to the destination of the web service call can be ensured by means of the test service.

To provide additional security for the exchange of data, the BDEW AS4 profile defines a further service for changing the transfer protocol in addition to the services for transmitting transfer files and a test service:

Service = "https://www.bdew.de/as4/communication/services/pathSwitch"

This service recognises two actions:

- Request to change the transfer protocol:
  Action = "https://www.bdew.de/as4/communication/actions/requestSwitch"
- Consent to change the transfer protocol:
  Action = "https://www.bdew.de/as4/communication/actions/confirmSwitch"

A market partner who wishes to use the AS4 transfer protocol to exchange transfer files with another market partner must indicate this with the "Request to change transfer protocol" *("Aufforderung zum Wechsel des Übertragungswegs").* The recipient of this message responds with the "Consent to change transfer protocol" *("Zustimmung zum Wechsel des Übertragungswegs")* and uses AS4 to transfer files.

The recipient of the "Consent to change transfer protocol" then also uses AS4 to transfer files.

7.3 Exchange of transfer files

The following Service and Action combination is used for data exchange as part of market processes:

Service = "https://www.bdew.de/as4/communication/services/MP"
Action = "http://docs.oasis-open.org/ebxml-msg/as4/200902/action"

Other services described in the AS4 profile are not permitted.

7.4 Response codes

Transmission via AS4 is only successful upon the synchronised receipt of the non-repudiation AS4 delivery receipt (NRR)[10].

The "Timestamp" contained in the delivery receipt and assigned to the "ResponseMessageInfo" is used when an NRR is received for further processing of the message content in accordance with the corresponding time limits.

If an error message (error code) of the (severity) type "failure" is received, the transmission has failed.

8 Organisational rules for handling certificates

A market partner A can only send an encrypted e-mail to a market partner B if market partner B provides a valid certificate that meets the requirements specified in Chapter 5.5. Therefore, in addition to these technical requirements, the following organisational rules also apply:

> As soon as a certificate is revoked or invalid and no valid follow-up certificate is yet available, further transfer files that originate from the associated sender address and are signed with the revoked or invalid certificate must not be processed.
> The market partner whose certificate is blocked or invalid must immediately procure a new certificate and must distribute it to all its market communication partners.

> If market partner A receives an AS4 message that does not contain a valid signature certificate from market partner B that meets the minimum technical requirements for verifying the signature of market partner B, the processing of the data received from market partner A can be refused in accordance with section 9 until market partner B uses an appropriate certificate.

[10] The NRR corresponds to the Message Disposition Notification for AS2 (MDN).

> If market partner A is not provided with a certificate from market partner B that meets the minimum technical requirements for encrypting the message to market partner B, market partner A may refrain from exchanging data with market partner B until market partner B has provided an appropriate certificate.

- If the signature check fails because the signature was damaged during transfer or if the AS4 message cannot be decrypted as a result, this situation shall have the same consequences in terms of market communication as if the attached transfer file had not arrived at the recipient.
  If the recipient sends a CONTRL (EDIFACT) message or an acknowledgement (RD2.0 process data) in response to the transfer file, the sender of the transfer file can assume that the signature check and the decryption of the transfer file were successful.
- The preceding rule does not apply if the recipient was unable to check the signature of an error-free signed and encrypted AS4 message or to decrypt it (e.g. due to technical problems). In this case, the attached transfer file shall be treated by the recipient (especially in terms of deadlines) as if the problem had not existed at the recipient's end.

9 Consequences of non-compliance with these requirements

The following procedures have been agreed with the Federal Network Agency in case the sender or the recipient fail to comply with the rules:

Breach type 1: The sender has not been provided with a valid certificate by the recipient for encrypting transfer files, and the sender is therefore unable to encrypt the transfer file.

Procedure: The sender is entitled to decide not to carry out the communication. If the recipient is a network operator, the sender may also complain to the Federal Network Agency. The consequences of any failure to communicate will have to be borne by the market partner responsible for providing the certificate (recipient). The sender must inform the recipient (responsible party) at least once by e-mail of the fact that the communication will not be carried out due to the lack of a valid certificate. The responsible party (recipient) will have to inform the sender by e-mail about the further steps taken in response to the e-mail received and nominate a contact person for this purpose. This reply will also serve as confirmation of receipt of the information.

The information must be sent at least to the e-mail address of the contact person for the transfer protocol / data exchange specified in the communication data sheet (in accordance with BK6-20-160, GPKE Chapter III, 6). If the communication data sheet (in accordance with BK6-20-160, GPKE Chapter III, 6) is not exchanged between the market roles, the e-mail must be sent at least to the e-mail address of the communication parameter "Contact person for electronic data exchange" *("Ansprechpartner für den elektronischen Datenaustausch")* stored in the BDEW code number database.

Breach type 2: The recipient receives an e-mail

- which is not signed, or
- which is signed with an invalid certificate, or
- which has been provided with a signature that cannot be validated with the valid certificate.

As a result, the recipient is unable, among other things, to unambiguously identify the sender and, furthermore, it cannot rule out the possibility that the received transfer file may have been compromised.

Procedure: The recipient is entitled to refuse to process the transfer file in question. The AS4 error message is returned with the code "EBMS:0101" (FailedAuthentication). The consequences of any such non-processing must be borne by the sender.

Breach type 3: The recipient receives an encrypted transfer file that was encrypted with a key that does not belong to the recipient's current certificate.

Procedure: The recipient is unable to decrypt the transfer file and is therefore entitled to refuse to process the transfer file. The error message is returned with the code EBMS:0102 (FailedDecryption). The consequences of any such non-processing must be borne by the sender.

Breach type 4: The recipient receives an unencrypted but validly signed transfer file.
This means the transfer file was not protected against inspection by a third party, but there can be no denying the content of the transfer file and the sender of the message.

Procedure: The recipient is entitled to refuse to process the transfer file in question. The error is reported with the code EBMS:0103 (PolicyNoncompliance). The consequences of any such non-processing must be borne by the sender.

10 Sources

[1] Beschluss (BK6-21-282) und Anlagen zur Absicherung der elektronischen Marktkommunikation Strom, Bundesnetzagentur, 31.03.2022.
Decision BK6-21-282 of the Federal Network Agency on safeguarding electronic market communication for electricity, Federal Network Agency, 21 March 2022.

[2] Beschluss (BK7-19-001) und Anlagen zum Beschluss (BK7-19-001), Anpassung der einheitlichen Geschäftsprozesse und Datenformate beim Wechsel des Lieferanten bei der Belieferung mit Gas und des Messstellenbetreiberrahmenvertrags, Bundesnetzagentur, 22.11.2023.
Decision (BK7-19-001) and annexes to the decision (BK7-19-001), Adaptation of the standardised business processes and data formats when changing the supplier for the supply of gas and the metering point operator framework agreement, Federal Network Agency, 22 November 2023.

[3] Beschluss (BK6-20-059) und Anlagen zum Beschluss (BK6-20-059) zum bilanziellen Ausgleich von Redispatch-Maßnahmen, Bundesnetzagentur, 06.11.2021.
Decision (BK6-20-059) and annexes to the decision (BK6-20-059) on the balancing of Redispatch measures, Federal Network Agency, 6 November 2021.

[4] Beschluss (BK6-18-122) und Anlagen zum Datenaustauschs mit Verteilernetzbetreibern und signifikanten Netznutzern, Bundesnetzagentur, 20.12.2018.
Decision (BK6-18-122) and annexes on data exchange with distribution system operators and significant grid users, Federal Network Agency, 20 December 2018.

[5] Beschluss (BK6-20-160) und Anlagen zur Weiterentwicklung der Netzzugangsbedingungen Strom, Bundesnetzagentur, 21.12.2020.
Decision (BK6-20-160) and annexes regarding further development of network access conditions, Federal Network Agency, 21 December 2020.