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 1.8 (Rules of transmission 1.8)" 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=2307&tx_bdew_bdew%5Baction%5D=download&tx_bdew_bdew%5Bcontroller%5D=Dokument&cHash=c6d817b4e8038cfea85ba643f2a26df7

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 EDIFACT and Redispatch 2.0 process data

Version:	1.8
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 AS2, e-mail via SMTP, SFTP and REST transfer protocols[1] in market communication.

According to a Federal Network Agency (BNetzA) decision[2], the cryptographic requirements of BSI TR 03116-4 (as of 7 March 2022)[3] must always be observed and complied with. This document describes the parameters to be used and the deviations to be applied.

1.1 Scope

The rules set out below apply to

> all gas market processes[4] defined by BNetzA that are processed via EDIFACT, such as GeLi Gas, WiM Gas, GaBi Gas, KoV[5],

> all market processes defined by BNetzA for Redispatch 2.0 that are handled via EDIFACT and are not covered by the market rules for balancing group settlement ("MaBiS"),

> the data exchange of Redispatch 2.0 process data[6] via XML and to

> processes for the exchange of information between network operators and the Federal Environment Agency's register of guarantees of origin (data exchange with authorities) via EDIFACT[7].

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. Moreover, this document does not cover the exchange of qualified signed transfer files.[8]

Therefore, the following rules on transfer protocols 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. BK6-18-032 [6] and BK7-16-142 [2], Decision to adapt the requirements for electronic market communication to the requirements of the Act on the Digitalisation of the Energy Transition (GDEW).

3 If this version is no longer available for public download, it can be requested from BSI.

4 Cf. BK6-18-032 (operative part 6) [6] and decision (BK7-16-142) [2].

5 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.

6 Cf. BK6-20-059, Annex 2, II Basic data exchange and call order processes [9] 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) [10].

7 Cf. section 42 EnWG, Federal Environment Agency, Guarantees of origin for electricity.

8 Cf. Federal Network Agency, Communication No. 3 on the data formats for market communication [7].

1.2 Document structure

Unless otherwise indicated, the rules apply to both data exchange as part of market processes and to Redispatch 2.0 process data. Where these two areas of application are subject to different rules, the relevant chapter is divided into two sub-chapters:

> **"Market processes"**

denotes the part that applies to the data exchange of all market processes defined by BNetzA that are handled via EDIFACT.

> **"Redispatch 2.0 process data"**

denotes the part that applies to data exchange within the scope of Redispatch 2.0 via XML (RD2.0 process data).

Any minor differences between the processes are explicitly stated in the text.

1.3 Transitional provisions for the gas sector

Before and during the phased introduction of AS4 communication involving the use of smart metering PKI 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 transfer protocols will temporarily apply simultaneously:

> **E-mail or AS2 communication:**
"Rules on transfer protocols" with the order number / version 1.x (this document). This version of the rules on transfer protocols 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 at the latest for the exchange of messages by e-mail via SMTP or AS2 transfer protocols.[9]

> **AS4 communication:**
"Rules on transfer protocols for AS4" / version 2.x. This version of the rules on the transfer protocols and its successor versions describe the exchange of transmission files as part of market processes via an AS4 web service.

2 Notifying the information recipient

In order to achieve the greatest possible level of automation in data exchange, the market partners must agree on details such as the transfer protocol and the data exchange addresses, including the certificates to be used, before sending data for the first time.

2.1 Market processes

According to Chapter 3.1 below, the exchange of data for all EDIFACT-based market processes specified by BNetzA may be carried out by e-mail via SMTP or AS2.

The communication parameters are exchanged after the initial contact has been established by

[9] Cf. Decision BK7-19-001 [12].

telephone or e-mail.

The aforementioned data must be exchanged between the two parties no later than three working days (as per the GPKE/GeLi Gas calendar[10]) after a market partner has been contacted for the first time. One working day 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.

EDIFACT 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[11]. This provision only applies to error-free EDIFACT 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 EDIFACT 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 and must be sent at least to the address data of the market partners with whom the relevant market partner has exchanged EDIFACT files within the last three years and which are stored in the BDEW or DVGW code number databases at the time the information is transmitted.

The changeover must be scheduled for a working day as per the GPKE/GeLi Gas calendar. It is recommended to agree a time during regular office hours to allow the necessary checks to be made and, if any errors are detected, to be able to contact the other side and rectify the error promptly and inexpensively.

Retaining the transfer protocol does not mean that an e-mail address used for data transfer and replaced by another e-mail address may not be deleted for three years. If such an in-box of an e-mail address has been "shut down" and all market partners have been informed of the new e-mail address to be used in accordance with the preceding rule, the previously used e-mail address may be deleted. This rule also applies mutatis mutandis to AS2.

The e-mail address, phone and fax number published in the DVGW code number database or BDEW code number database shall serve for contacting a market partner.

2.2 Redispatch 2.0 process data

AS2, e-mail via SMTP, SFTP or REST are used for the data exchange of RD2.0 process data. Further rules are defined in Chapter 3.2.

[10] Note: The working day definitions in GPKE and GeLi Gas are identical.

[11] As a rule, where a transfer protocol is established, the date of receipt is the relevant date for deadlines.

The certificates must be exchanged between the two parties no later than 10 working days (as per the GPKE/GeLi Gas calendar[10]) before the first XML file is sent by a market partner.

No later than three working days after the exchange of communication data, both parties must have mutually exchanged the certificates and entered the certificates of the other market partner in their systems involved in the process.

3 Transfer protocols

3.1 Market processes

The transfer protocols used for transferring files are AS2 or e-mail via SMTP.

If the parties cannot agree on a transfer protocol, the e-mail option (as per Chapter 6) must be offered in any case.

3.2 Redispatch 2.0 process data

The transfer protocols used for XML files are AS2, e-mail via SMTP, SFTP or REST.

If agreement is reached on one of the two transfer protocols AS2 or e-mail via SMTP, it must be checked whether the same transfer protocol already exists between the market partners with their MP ID for market process communication. If this is the case, the same communication address must be used (1-on-1 communication).

If it is not possible to agree on a transfer protocol, but an agreed transfer protocol already exists between the market partners with their MP ID for communicating market processes, this must be used. Otherwise, the e-mail option (as per Chapter 6) must be offered in any case.

In addition, the market partners are free to agree on and use blackout-proof transfer protocols as a backup to the aforementioned transfer protocols.

4 Communication rules

4.1 Market processes

Only one transfer protocol is permitted between two different MP IDs. Either an e-mail address or an AS2 address may be used for the transfer protocol.

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.

It is permissible to use the same e-mail address or AS2 URL for several MP IDs.

An EDIFACT transfer file sent from an e-mail address other than the agreed e-mail address does not have to be processed[12] by the recipient. Accordingly, it will be deemed not to have been delivered and there will be no response returned to the market partner. Any and all consequences resulting therefrom will have to be borne by the sender of the e-mail.

4.2 Redispatch 2.0 process data

Only one of the following transfer protocols may be used for the exchange of RD2.0 process data between two market partners (with different MP IDs):

- E-mail (in accordance with Chapter 6)
- AS2 (in accordance with Chapter 7)
- SFTP (in accordance with Chapter 9), or
- REST webservice (in accordance with Chapter 10).

It is permissible to use the same communication address for several MP IDs. It is permissible to use different communication addresses for one MP ID in different areas of application (market processes and RD2.0 process data).

An XML file that is sent from a communication address other than the agreed communication address does not have to be processed by the recipient. Accordingly, it will be deemed not to have been delivered and there will be no response returned to the market partner. Any and all consequences resulting therefrom will have to be borne by the sender of the e-mail.

5 Signature and encryption

This section provides binding rules on the organisation and technical requirements for signatures and encryption.

5.1 Trust service provider

In the following, the technical term "certification authority" or "CA" is used instead of the legal term "trust service provider" as used by the German Trust Services Act *("Vertrauensdienste-gesetz"* or *"VDG")*.

The certificate must be issued by a CA[13] which offers certificates in a non-discriminatory manner to market partners of the German energy industry. It must not be what is known as a "self-issued certificate".

The provisions of Chapter 6.1.1 Certification bodies / trusted anchors *("Zertifizierungsstellen / Vertrauensanker")* in [1] apply with the following addition:

[12] This means that the e-mail does not have to be decrypted, the signature does not have to be verified and the transmission file contained in the e-mail does not have to be processed.

[13] Supervision is the responsibility of the Federal Network Agency in accordance with the German Trust Service Act. The corresponding English term according to the eIDAS Regulation is "trust service provider".

> The CA has a recall service via which certificates can be revoked. For this purpose, the CA maintains a so-called certificate revocation list (CRL), which is publicly accessible.

> The certificate revocation list must be made publicly accessible at least via http.

5.2 Certificates: Parameters and requirements for S/MIME

The certificates must fulfil the following requirements according to Chapter 6.1.2 Certificates in [1] with the following exceptions and additions.

By way of derogation, the following regulations apply:

> All certificates must contain information for a recall check, i.e. a `CRLDistributionPoint` under which current CRLs are available at all times.

> An *`AuthorityInfoAccess` extension* does not have to be provided.

> The certificate must have been issued by a CA that fulfils the requirements specified in Chapter 5.1.

> In deviation from [1], the validity period of the certificates of the root and sub-CAs must be limited to a cryptographically acceptable period. For newly issued end-user certificates, the issued certificate for sub-CAs should be no more than five years old. However, the suitability of the cryptographic algorithms must be ensured for the entire validity period in accordance with [1], provided they are available. This implies in particular that the certificates must be updated when the suitability as per [1] expires.

> The same certificate (combined certificate) shall be used for signature and encryption.[14]

In addition, the following rules apply:

> All certificates must be signed with RSASSA-PSS.

> See Chapter 5.3 for the key length.

> The certificate must fulfil the requirements for an advanced electronic signature or an advanced electronic seal.[15]

> The certificate must guarantee identification of and assignment to the company/service provider or organisation that operates the e-mail address. This means that the O field of the certificate must contain the legal entity that operates the e-mail inbox for the e-mail address for which the certificate was issued and under which the signed and encrypted e-mails are sent and received.

> The parameter in the "Alternative applicant name" field with the value "RFC822-Name=" must be filled with the communication address (e-mail address). It is not permissible to have several communication addresses in one certificate.

[14] Cf. BK7 [2] to [5] or BK6 [6].

[15] Requirements for signatures and seals can be found in the eIDAS Regulation (Regulation (EU) No. 910/2014). CA operators often use the term "organisation-validated" certificates for this purpose.

> The certificate name field "CN" is not used and is not analysed. It is recommended to enter a pseudonym in this field. The assignment of a certificate to a natural or legal person takes place exclusively via the CA and does not have to be recognisable from the certificate itself.[16]

For the exchange of public certificates, the coding DER is either binary X.509 or base-64 X.509 with the file extension .cer.

5.3 Algorithms and key lengths for S/MIME

The following algorithms and keys with the specified key lengths must be used[17]:
Software settings:

> Signature:

- Hash algorithm: SHA-256 or SHA-512 (according to IETF RFC 5754).
- Signature algorithm: RSASSA-PSS (according to IETF RFC 4056).

> Encryption:

- Content encryption: AES-128 CBC, AES-192 CBC or AES-256 CBC (according to IETF RFC 3565).

  From 1 August 2024, the following algorithms must be supported: AES-128 CBC, AES-256 CBC and AES- 128 GCM.

  From 1 October 2024, only AES-128 GCM (in accordance with IETF RFC 5084) may be used.
- Key encryption: RSAES-OAEP (according to IETF RFC 8017).

  The key encryption has hash functions as parameters. SHA-256 or SHA-512 must be used here.

The key length used is derived from the public RSA key of the certificate. The following transitional regulations for key lengths apply:

> Until 31 March 2022:
Existing certificates that have an RSA key length of 2048 bits may be used until their expiry date.

[16] Cf. BNetzA clarification [7].

[17] Selection taken from [1], Chapters 3.2 to 3.4.

> Certificates that are newly issued or renewed by 31 March 2022 should already have an RSA key length of at least 3072 bits.

> From 1 April 2022:
Certificates issued from 1 April 2022 must have an RSA key length of at least 3072 bits.

The ways in which RSA encryption is implemented must provide for suitable countermeasures against chosen ciphertext attacks.[18]

In addition, the following applies with regard to the algorithms used for signing and encryption:

> From 1 October 2023, the receipt of S/MIME messages that use the ECDSA signature and ECDH for key encryption in accordance with [1] must be supported. It is recommended to accept the BrainpoolP256r1 curve for ECC procedures in order to fulfil the minimum requirements for interoperability according to Chapter 4.7 in [1].

> When S/MIME messages are sent, these algorithms must not initially be used even after 1 October 2023.

5.4 S/MIME version

Signing and encryption are only permitted in accordance with the S/MIME standard permitted in Chapter 4.1 of [1]. S/MIME 4.0 is therefore recommended in particular. Only the procedures evaluated, described and selected in this document, which are specified in more detail in Chapter 5.3, may be used.

5.5 Changing certificates and revocation lists

No later than 10 working days before a certificate expires, the owner of the certificate must have provided the follow-up certificate (see Chapter 11). This means there is an overlap period of at least ten working days during which both the old and the new certificate are valid.

During this overlap period, all market partners can switch from the previously used certificate to the new certificate. The owner of the certificate must use the new certificate for signing no earlier than three working days after making it available to its market partners. Each of its market partners may independently determine the point in time within the overlap period from which it uses the new certificate to encrypt e-mails sent to the owner of the certificate.

During the overlap period, all market partners must be able to process signed and encrypted e-mails with both the previously used certificate and the new certificate, whereby the aforementioned restriction applies to the owner of the certificate.

From the time the old certificate becomes invalid, it may be used neither for signing nor for encryption.

[18] Derived by analogy from [1], Chapter 4.6 Further requirements and Chapter 4.8 Transitional regulations.

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 through the revocation lists of its CA provider.

Each market partner is obliged to check at least once a day that none of its market partners' certificates have been revoked by checking all the certificates it uses against the revocation lists (CRL).

If a CRL cannot be retrieved from a CA via the certificate revocation list distribution point (CRL-DP) published in the certificates for more than three days, the issuing CA and all certificates listed under it must be distrusted until an up-to-date CRL is published. The specific potential consequences are described in Chapter 12.

6 Rules for data exchange via e-mail

The rules described in this Chapter 6 only apply to e-mail transmission via SMTP involving the exchange of market process files or RD2.0 process data.

The high degree of variation in e-mail use requires the following rules to be applied in order to achieve a high degree of automation on the part of the e-mail recipient.

6.1 E-mail address

> The e-mail addresses specified for the exchange of EDIFACT transfer files or RD2.0 process data between two market partners must be used exclusively for the exchange of EDIFACT transfer files or RD2.0 process data.

> The e-mail address must be a non-personal, function-related e-mail address (e.g. without an individual’s first and last name).

> A market partner who sends e-mails relating to business matters to the e-mail address of another market partner specified for the exchange of data cannot expect these e-mails to be read, let alone answered. The market partner must assume that the non-EDIFACT information or non-RD2.0 process data sent with the e-mail will be ignored.

> The sender of an e-mail must use its own e-mail address in the FROM field of the e-mail. The TO field of the e-mail is to be filled only with the e-mail address of the recipient. Both fields must be filled.

> Only the "pure" address components of the e-mail address (LocalPart@Domain.TLD) will be analysed. The sender is not entitled to have the "phrase" analysed or addressed.

> Example: "Datenaustausch Marktpartner"<Daten@Marktpartner.de>

- Only the address part Daten@Marktpartner.de may be used for addressing the e-mail.

- If the "Datenaustausch Marktpartner" phrase is also sent, it must not be used for analysis.
- The e-mail address must not be interpreted case-sensitively, i.e. in the above example, Daten@Marktpartner.de and Daten@MarktPartner.de are identical.

6.2 E-mail attachments

> An e-mail may only ever contain one EDIFACT transfer file or one RD2.0 process data file.

> An e-mail must not contain any other attachments.

> Business correspondence sent by e-mail or any text components of the e-mail will be ignored.

> Rule for naming the transfer file: The naming convention described in the relevant chapter of the EDI@Energy document entitled General Specifications *("Allgemeine Festlegungen")* shall apply.

> The attachment does not have to be separately encrypted or signed, as this is already done by S/MIME.

> The attachment must be Base64 encoded so that mail servers do not insert line breaks during transfer.

> The content type of the MIME part with the attachment must be the application/octet-stream. If the attachment is an EDIFACT message file, the content type may alternatively be application/edifact.

> EDIFACT transmission files may, but do not have to be, compressed. RD2.0 process data files must be compressed.

> Only gzip compression[19] is permitted for compressing the transfer file. The content type must be adapted accordingly.

6.3 E-mail body

> Information required for further processing must not be contained in the e-mail outside of the actual transfer file (i.e. in the e-mail body). The message recipient will only process the content of the transfer file. Any other information contained in the body of the e-mail, i.e. business correspondence or text components sent in the same e-mail, will be ignored.

> Certain software products currently used for the entire processing chain of market communication via e-mail require some text in the e-mail body. For this reason, the e-mail body must be filled with plain text, while always complying with requirements described in the previous paragraph. This means above all that the e-mail body may not be coded in HTML, and it must not contain any images or company logos.

19 gzip is platform-independent.

6.4 E-mail subject

The e-mail subject must be the same as the file name, including the file extension. See Chapter 6.2 (E-mail attachments) for the file naming convention.

6.5 Signature and encryption of e-mails

Every e-mail used in the German energy industry to exchange an EDIFACT transfer file or an RD2.0 process data file must be signed and encrypted. Further details can be found in Chapter 5.

7 Rules for file exchange via AS2

If transfer files are exchanged via AS2, the AS2 profile version 3 must be used for standardised communication of the own AS2 address parameters. This PDF document also contains the AS2 profile as a Word template.

AS2 is abstractly standardised via RFC 4130. This section incorporates extensions and further algorithms in addition to RFC 4130 that meet current safety requirements.

The algorithms and parameters to be used, which are mandatory for the German energy market, are listed below.

7.1 AS2 address

In this document, the AS2 address is the combination of AS2 ID and AS2 URL.

Note: Technically, the AS2 ID must be unique for each AS2 adapter.

7.1.1 AS2 ID

The market partner ID is also the AS2 ID. The AS2 ID must not contain any prefixes or suffixes.

Note: The AS2 ID is used to assign the AS2 certificate for the S/MIME technology.

7.1.2 AS2 URL

The AS2 adapter URL must be specified as a fully qualified name of the domain (instead of IP address). The URL must not be interpreted in a case-sensitive manner.

7.2 Requirements for AS2 certificates

The certificate must only be used for AS2 communication.

The AS2 certificate is used for signature and encryption purposes.

Technically, it is necessary to assign the AS2 certificate to an AS2 ID. At least one certificate must be assigned to each AS2 URL. If several AS2 IDs are assigned to an AS2 URL (in this document, the number of AS2 IDs assigned to this AS2 URL is given as n), all AS2 IDs assigned to this AS2 URL can be operated with different certificates or 1 to n identical certificates.

The AS2 certificate must meet the requirements specified in Chapter 5.

7.3 Content data backup

For algorithms and key lengths, see Chapter 5.3, and for the S/MIME version, see Chapter 5.4.

7.4 Transport layer

The IP addresses used must be fixed IP addresses. https is to be offered via port 443. Optionally http with standard port 80 may also be offered. If https is used, TLS version 1.2 or 1.3 must be used. Parameterisation should be carried out in accordance with [1], Chapters 2.2 or 2.3.

A renewal of the TLS certificate does not need to be reported if the *Issuer* and *Subject DN* remain the same, otherwise this must be communicated to the communication partners via the AS2 profile.

7.5 MDN (digital delivery receipt)

For the Message Disposition Notification (MDN), the MDN mode must be selected synchronously (immediate delivery note) and the MDN must be signed.

7.6 Subject and file name

For the subject and file name, the naming convention of the corresponding chapter of the EDI@Energy document "Allgemeine Festlegungen" ("General Specifications") shall be applied.

8 Rules on content data backup for SFTP and REST transfer protocols

This chapter describes general requirements for the structure and handling of content data backup containers for SFTP and REST transfer protocols.

The XML message to be transferred is first compressed. It is then signed and encrypted using S/MIME. The algorithms specified in Chapter 5.3 must be used with the key lengths specified there.

The steps in detail:

0. Create XML message file -> "Message.xml".
1. File compression using gzip -> "Message.xml.gz"
2. Signing:
    - A detached signature is generated, i.e. a base-64 encoded MIME object of the type "multipart/signed" is generated.
    - RFC 8551; Chapter "3.5.3 Signing using the multipart/signed format".
    - For algorithms, see Chapter 5.3.
3. The resulting MIME object is then encrypted.
    - RFC 8551 Chapter 3.3. Creating an enveloped-only message.
    - For algorithms, see Chapter 5.3.
4. The MIME object is a valid e-mail body and is saved with a file name in accordance with the naming convention and the file name extension ".eml". -> "Message.eml".

This message file can be opened, decrypted and read in an e-mail client.

9 Rules for the exchange via SFTP (for RD2.0 process data only)

The SFTP[20] is a protocol for data transfer based on Secure Shell (SSH)[21]. With this transfer protocol, the connection is established, transport is secured, and authentication is carried out via SSH, for which BSI-TR-02102-4 (as of 31 January 2020) is authoritative.

This section describes the algorithms and parameters to be used, which are mandatory for the German energy market.

If the exchange takes place via SFTP, the SFTP profile version 1 must be used for the standardised communication of the market partner's own address parameters. This document also contains the SFTP profile as a Word template.

If the SFTP communication channel is used, the market partner must operate its own corresponding SFTP server to receive the data, on which its market partners can store their containers (Chapter 8).

9.1 SFTP address

The SFTP server must be accessible as a fully qualified domain name (FQDN). The DNS name must refer to an IPv4 address. Connections are only permitted via the standard port 22 (TCP).

The sender is the SFTP client, the recipient is the SFTP server. When exchanging data, everyone must therefore operate an SFTP server that can be reached under a unique SFTP address.

9.2 SSH version

SSH version 2.0 must be used.[22]

9.3 SSH key pairs

To establish an SFTP connection, the recipient (server) and sender (client) must each generate a key pair. The public key must be made available to the respective market partner. A total of four key pairs are therefore required for the mutual exchange of transfer files, one client and one server key for each market partner.

The unique SSH key pairs must be generated for the SFTP sender (client) and SFTP receiver (server) roles by each market partner themselves.

The SFTP receiver (server) must properly store its private server key and all public client keys on its server.

The SFTP sender (client) must properly store its private client key and the public keys of all servers in its client.

---

[20] In accordance with the IETF Internet Draft on the SSH File Transfer Protocol (SFTP v3), document version 2: https://tools.ietf.org/html/draft-ietf-secsh-filexfer-02.

[21] Chapter 2 in [11] shows a list of RFCs that cover all SSH variants. ITEF RFC 4250 to 4256, ITEF RFC 4335, ITEF RFC 4344, ITEF RFC 4819, ITEF RFC 5647, ITEF RFC 5656 and ITEF RFC 6668 are relevant for this document.

[22] In accordance with Chapter 3.2 in [11].

The server keys must be stored on the client in such a way that there is no confirmation request for the fingerprint. If confirmation of a fingerprint is requested when a connection is established, the connection must be terminated immediately, and a clarification process initiated.

9.4 Algorithms and key lengths for SSH

To ensure a secure SSH connection, at least the following methods must be supported for the key exchange between server and client:[23]

> Key exchange method:

- `ecdh-sha2-nistp256` (according to Chapter 6.4 in IETF RFC 5656).

> Encryption algorithm:

- `aes256-ctr` (according to Chapter 4 in IETF RFC 3444).

9.5 MAC backup

At least the following methods must be supported for MAC backup unterstützen: [24]

- `hmac-sha2-256` (according to Chapter 2 in IETF RFC 6668).

9.6 Authentication

Authentication must be carried out for both the client and the server using the previously exchanged SSH key pairs.

As a minimum, the algorithm for the digital signature must be used for authentication:[25]

> Server authentication:

- `ecdsa-sha2-nistp256` (according to Chapter 3 in IETF RFC 5656).
  Key length: 250 bits

According to ITEF RFC 4252 Chapter 7, the same algorithm must be used for server and client authentication.

In addition, a previously exchanged username (see Chapter 17, SFTP profile) is required to establish a connection for logging on to the SFTP server, as SSH authentication requires public keys and a user name in accordance with IETF RFC 4252. For successful authentication, the corresponding user must be created on the SFTP server and the market partner's public key must be assigned to this user.

9.7 Authorisation

The communication partners are obliged to grant each other access based on valid SSH key pairs.

---

[23] Derived by analogy from [11], Chapters 3.3 and 3.4.

[24] Derived by analogy from [11], Chapter 3.5.

[25] Derived by analogy from [11], Chapter 3.6.

9.8 Handling SSH key pairs

The SSH key pairs must be renewed after three years at the latest and the public keys must be made known to the market partners. In order to ensure a smooth process, the specifications from Chapter 5.5 must be observed analogously when keys are renewed.

If the private key is no longer trustworthy, the affected market partners must be notified immediately. The private key must be deactivated immediately, a new key pair must be generated, and the public key must be made available to the market partners.

9.9 Conventions for file storage and avoidance of access conflicts

The files must be created in accordance with Chapter 8 (container).

The communication partner (sender/client) stores the files directly in its directory at the recipient (server). No subdirectories are to be created, either by the sender or by the recipient.

To avoid possible access conflicts during the write process in the SFTP transfer, the files must be written with a temporary prefix (".") during the write process and renamed as a file without the prefix once the write process is complete. This avoids access conflicts between sender and recipient. The market partner (sender/client) must have the appropriate rights to write/rename in its root directory at the recipient (server).

10 Rules for exchange via REST

If REST is used for data exchange, REST profile version 1 must be used for the standardised communication of the market partner's own REST address parameters. This document also contains the REST profile as a Word template.

Representational State Transfer (REST) utilises the functionality of the http protocol and its transport security. Content data is backed up to containers (see Chapter 8). Accordingly, each market participant requires certificates for two tasks:

> certificates for securing the transport layer (TLS certificate) and

> the certificate for content data security via S/MIME (S/MIME certificate).

REST is a web service (WS) and works unidirectionally. The client implementation of the WS can send data; the server implementation can receive data. In order for two market partners to be able to exchange data bidirectionally, they must implement the WS in both versions (as a client and as a server).

10.1 REST transport layer

The WS URL is referred to as the WS address in this document.

The WS must be accessible via a URL in the format https://{domain}/{api} (e.g. https://example.org/api). The {domain} part must be a fully qualified domain name (FQDN) and must not contain a port number. The DNS name must refer to an IPv4 address.

The connection must be secured at least via TLS 1.2[26]. The TLS extension for Server Name Indication (SNI), defined in Chapter 3 of ITEF RFC 6066, must be implemented by all WS clients. It must also be implemented by every WS server that is known by multiple names. Otherwise, it is not possible for a server with multiple host names to present the correct certificate to the client.

Only one connection via the standard port 443 is permitted.

The WS has two functions (document acceptance and communication test), each of which is addressed via its own sub-path (/data and /comtest) (e.g. https://example.org/api/data and https://example.org/api/comtest).

10.2 TLS certificate and mutual TLS

Security and authentication are carried out via mutual TLS (TLS with client certificate)[27]. The server and client certificates used for this must be confirmed via CA.

The identity of a communication partner is determined based on the *Issuer DN* (details of issuer/CA) and the *Subject DN* (details of certificate holder) of a certificate (certificate-based trust). A renewal of the certificate does not have to be indicated (*Issuer* and *Subject DN* remain the same). A certificate change (at least one of the values changes) must be communicated to

[26] According to [1], Chapter 2 SSL/TLS specifications

[27] See IETF RFC 5246 (Chapter 7.4.6; Client Certificate)

the communication partners via the REST profile.

A market participant requires a separate certificate with a unique *Subject DN* for each MP ID. This means that the combination Issuer / Subject is assigned to exactly one MP ID.

The specifications for the TLS certificate are listed below:

> Certificate in X.509v3 format[28].

> Certificates with identical *Issuer DN* and *Subject DN* are used for sending documents (client) and receiving documents (server).

> The Issuer DN and Subject DN must remain the same for certificate renewals (otherwise the changes must be communicated to the communication partners via the REST profile).

> The certificate must contain exactly one domain name in the SAN (Subject Alternative Names) attribute.

> The same rules apply to the CA as in Chapter 5.1.

10.3 Algorithms and key lengths for TLS

The TLS cipher suites must be used in accordance with BSI TR 03116-4, Chapter 2.

For TLS 1.2, at least the following cipher suites must be offered:[29]

- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` (according to IETF RFC 5289).

For TLS 1.3, at least the following cipher suites must be offered:[30]

- `TLS_AES_128_GCM_SHA256` (according to IETF RFC 8446).

10.4 REST API

The WS has two functions (document acceptance and communication test), each of which is addressed via its own subpath (/data and /comtest). Communication takes place via POST calls.

10.4.1 Operating modes for the WS

The WS can work in different operating modes. The operating mode is used in particular to differentiate whether the transmitted messages are to be used productively for "productive operation" (PROD) or whether a "test operation" (TEST) is being carried out. By specifying the operating mode by the sender (client), the receiver (server) can ensure that both communication participants are in the same operating mode. In particular, this can prevent test messages from being incorrectly sent to a production system.

The identifiers for the following two operating modes are reserved and must be used

---

28 Cf. IETF RFC 6187.

29 According to [1], Chapter 2.2.

30 According to [1], Chapter 2.2.

accordingly. Further operating modes can be agreed between the market partners:

- `PROD` Production mode: This operating mode indicates that the message was sent from a sender in production mode to a receiver in production mode. In this operating mode, the messages are processed in full with all the consequences described in this document.
- `TEST` Test mode: This operating mode indicates that the message is to be sent from a sender in test mode to a recipient in test mode. Tests of the system landscape can be carried out in this operating mode. The exact scope of the tests can be determined by the testing market partners and is not part of this document. In particular, the message content does not have to be processed by the recipients in test mode.

10.4.2 Communication test

The communication test is carried out via a POST request to the `/comtest` path.

As part of the communication test, information is only exchanged via header parameters. The request body does not contain any information. A successful communication test is signalled by the response code 204.

10.4.2.1 Header parameters

The POST request for the communication test contains two header parameters, all of which must be of type string:

- `api-version` API version of the WS.
  The API version of the WS defined here is "1.0.0".
- `operating-mode` Operating mode. The following modes must be supported as a minimum: "TEST" and "PROD" (see Chapter 10.4.1).

10.4.2.2 Response codes

The server must respond to the request with one of the following response codes:

- `204` No Content – This status code is only used for a *successful* connection test.
- `400` Bad Request – The data could not be read correctly.
- `401` Unauthorised – Authentication has failed.
- `404` Not Found – The specified URL is incorrect.
- `405` Method Not Allowed – Only POST requests are permitted.
- `429` Too Many Requests – The sender has sent too many requests in too short a time.
- `500` Internal Server Error – An error has occurred on the receiver side.
  This error is not the fault of the sender. The sender can try to repeat the request.

10.4.3 Document transfer

This section describes the WS for document transmission. Documents are transmitted via a POST request to the `/data` path.

The container object of the XML document created according to Chapter 8 is transmitted BASE64-encoded within the JSON-formatted request body. Successful transmission is signalled by the response code 202.

10.4.3.1 Parameters

The POST request for document transmission contains three header parameters, all of which are mandatory and of type string:

- `api-version` — API version of the WS. (The API version of the WS defined here is "1.0.0")
- `operating-mode` — Operating mode. The following modes must be supported as a minimum: "TEST" (test mode) and "PROD" (production mode).
- `filename` — File name of the XML file including file name extension, which is transmitted in this message. The file name must follow the naming convention from the corresponding chapter of the EDI@Energy document "General specifications".

10.4.3.2 Request Body

The request body must be formatted as "application/json".

10.4.3.3 Request Content

The request content includes two mandatory properties:

- `creationTime` — Creation time in UTC of the document that is transmitted in this message (datetime string).
- `document` — BASE64-encoded version of the container object according to Chapter 8 (string byte).

Example:

```
{
   "creationTime": "2020-08-11T10:27:45.702Z",
   "document":
"PHhtbD5JY2ggYmluIGVpbiBCZWlzcGllbGRva3VtZW50PC94bWw+"
}
```

10.4.3.4 Response Codes

The server must respond to the request with one of the following response codes:

- > 202 Accepted – The data has been *successfully* received and will now be processed further. Any response (e.g. ACK) is transmitted via the return channel.
- > 400 Bad Request – The data could not be read correctly. This status code is returned if required parameters or properties of the request are missing or invalid (e.g. sending a request with operating mode "TEST" to a production system or missing "document").
- > 401 Unauthorised – Authentication has failed.
- > 404 Not Found – The specified URL is incorrect.
- > 405 Method Not Allowed – Only POST requests are allowed.
- > 406 Not Acceptable – The valid "Content Type" value of the request must correspond to the "application/json" value.
- > 429 Too Many Requests – The sender has sent too many requests in too short a time.
- > 500 Internal Server Error – An error has occurred on the receiver side. This error is not the fault of the sender. The sender can try to repeat the request.

11 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. This also applies analogously to the exchange via the other transfer protocols mentioned in this document. 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 e-mail 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.
When AS2, SFTP or REST is used, no transfer files can be exchanged if revoked or invalid certificates are employed.

> If market partner A is not provided with a certificate from market partner B that meets the minimum technical requirements for checking the e-mail signature market partner B, then, according to Chapter 12, market partner A is entitled to refuse processing of the data received from market partner A until market partner B has provided an appropriate certificate.

> If market partner A is not provided with a certificate from market partner B that meets the minimum technical requirements for encrypting the e-mail 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.

> Market processes: No later than 10 working days before the expiry of a certificate in the market processes, the owner of this certificate must send the follow-up certificate to all its market partners with whom it has exchanged EDIFACT transfer files in the last three years. The e-mail addresses entered in the BDEW or DVGW code number database shall be used for this purpose, unless agreed otherwise between the market partners.

> RD2.0 process data: At the latest 10 working days before a certificate expires, the holder of the certificate must send the successor certificate to the respective contact person.

> The certificate to be exchanged shall be sent by the market partner as a gzip-compressed attachment. Alternatively, a url can be sent which refers directly to the certificate to be downloaded. With the sending of the certificate or the link, the certificate will be deemed to have been exchanged. The requirements for the test to be carried out can be found in Chapter 5.

> If the signature check fails because the signature was damaged during transfer or if the e-mail 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 e-mail recipient, i.e. the e-mail had never been sent. 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 e-mail or to decrypt it (e.g. due to technical problems). In this case, the attached transfer file shall be treated by the recipient (especially with regard to deadlines) as if the problem had not existed at the recipient's end.

12 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 fails to comply with the rules:

12.1 Data transfer by e-mail

Breach type 1: The sender has not been provided with a valid certificate by the recipient, and the sender is therefore unable to encrypt the e-mail.

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.
Market processes: The information must be sent at least to the e-mail address stored in the BDEW or DVGW code number databases and, as an option, to a market partner e-mail address made available, e.g., via the contact data sheet.
RD2.0 process data: The information must be sent at least to the e-mail addresses of the market partner exchanged via the contact data sheet of the communication partners.

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 consequences of any such non-processing must be borne by the sender. The recipient must inform the sender (responsible party) at least once by e-mail of the fact that transfer files will not be processed due to a missing or invalid signature the recipient must inform the sender (originator) at least once by e-mail that remittance files will not be processed due to a missing or invalid signature. Based on this e-mail, the sender of the original message must inform the recipient of the original message via e-mail about the further procedure and name a contact

person who is responsible for this purpose.
Note: The message from the recipient to the responsible party (sender) will be sent once using a transfer file selected as an example.
Market processes: The selection of all affected transfer files will be made by the responsible party based on the missing CONTRL messages. The information must be sent at least to the e-mail address stored in the BDEW or DVGW code number databases and optionally to a market partner e-mail address exchanged, e.g., via a contact sheet. The market partner will be assigned based on the market partner ID in the subject of the e-mail.
RD2.0 process data: The information must be sent at least to the e-mail addresses of the market partner exchanged via the contact data sheet of the communication partners.

Breach type 3: The recipient receives an encrypted e-mail that was encrypted with a key that does not belong to the recipient's current certificate. As a result, the recipient is unable to decrypt the e-mail and process the content of the transfer file.

Procedure: The recipient is unable to decrypt the e-mail and is therefore entitled to refuse to process the e-mail. The consequences of any such non-processing must be borne by the sender. The recipient must inform the sender (responsible party) at least once by e-mail of the fact that e-mails cannot be decrypted due to an invalid key and that the corresponding transfer files cannot therefore be processed. In response to this e-mail notification, the sender of the original message must inform the recipient of the original message via e-mail about the further procedure and name a contact person who is responsible for this purpose.

Note: The message from the recipient to the responsible party (sender) will be sent once using a transfer file selected as an example.
Market processes: The selection of all affected transfer files will be made by the responsible party based on the missing CONTRL messages. The information must be sent at least to the e-mail address stored in the BDEW or DVGW code number databases and optionally to a market partner e-mail address exchanged, e.g., via contact data sheet. The market partner will be assigned based on the market partner ID in the subject of the e-mail.
RD2.0 process data: The information must be sent at least to the e-mail addresses of the market partner exchanged via the contact data sheet of the communication partners.

Breach type 4: The recipient receives an unencrypted but validly signed e-mail. 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 consequences of any such non-processing must be borne by the sender. The recipient must inform the sender (responsible party) at least once by e-mail of the fact that transfer files will not be processed due to a lack of encryption. In response to the e-mail notification, the sender of the original message must inform the recipient of the original message via e-mail about the further procedure and name a contact person who is responsible for this purpose. This reply will also serve as confirmation of receipt of the information.
Note: The message from the recipient to the responsible party (sender) will be sent once using a transfer file selected as an example.

Market processes: The selection of all affected transfer files will be made by the responsible party based on the missing CONTRL messages. The information shall be sent at least to the e-mail address stored in the BDEW or DVGW code number databases and optionally to a market partner e-mail address exchanged, e.g., via contact data sheet. The market partner will be assigned based on the market partner ID in the subject of the e-mail.

RD2.0 process data: The information must be sent at least to the e-mail addresses of the market partner exchanged via the contact data sheet of the communication partners.

Breach type 5 (R2.0 process data only): The recipient receives uncompressed or non-standard-compliant compressed (see Chapter 8) messages.

Procedure: The recipient is entitled to refuse processing of the transmission file in question. The consequences of such non-processing shall be borne by the sender. The recipient must inform the sender (responsible party) at least once via e-mail of the fact that the file cannot be processed due to missing or incorrect compression. In response to this e-mail received, the responsible party shall inform the sender via e-mail about the further steps and nominate a contact person for this purpose. This reply also serves as confirmation of receipt of the information.
Note: The information message from the recipient to the responsible party (sender) is sent once based on an exemplary selected transmission file.

The information must be sent at least to the e-mail addresses of the market partner exchanged via the contact data sheet of the communication partners.

12.2 Data transfer via AS2

Breach type 1: The recipient has not provided the sender with a valid certificate.
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. The sender must inform the recipient (responsible party) at least once of the fact that the communication is not being carried out due to the lack of a valid certificate. The responsible party shall inform the sender about the further steps taken in response to the received e-mail 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 stored in the BDEW or DVGW code number databases and optionally to a market partner e-mail address exchanged, e.g., via contact data sheet.

Breach type 2: The recipient receives a transfer file

- 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 may refuse to process the transfer file in question. The consequences of any such non-processing must be borne by the sender. The recipient must inform the sender (responsible party) at least once of the fact that transfer files will not be processed due to a missing or invalid signature. The responsible party must inform the sender about the further steps taken based on the received e-mail and nominate a contact person for this purpose. This reply will also serve as confirmation of receipt of the information.
Note: The message from the recipient to the responsible party (sender) will be sent once using a transfer file selected as an example. The selection of all transfer files concerned will be made by the responsible party based on the missing CONTRL messages. The information must be sent at least to the e-mail address stored in the BDEW or DVGW code number databases and optionally to a market partner e-mail address exchanged, e.g., via contact data sheet. The market partner will be assigned based on the AS2 ID.

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. As a result, the recipient is unable to decrypt and process the transfer file.

Procedure: The recipient is unable to decrypt the transfer file and is therefore entitled to refuse to process the transfer file. The consequences of any such non-processing must be borne by the sender. The recipient must inform the sender (responsible party) at least once of the fact that transfer files cannot be decrypted and will therefore not be processed. In response to this e-mail, the responsible party has to inform the recipient of the original message via e-mail about the further procedure and nominate a contact person for this purpose. This reply will also serve as confirmation of receipt of the information.
Note: The message from the recipient to the responsible party (sender) will be sent once based on a transfer file selected as an example. The selection of all transfer files concerned will be made by the responsible party based on the missing CONTRL messages.
The information must be sent at least to the e-mail address stored in the BDEW or DVGW code number databases and optionally to a market partner e-mail address exchanged, e.g., via a contact sheet. The market partner will be assigned based on the AS2 ID.

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 consequences of any such non-processing must be borne by the sender. The recipient must inform the sender (responsible party) at least once of the fact that transfer files will not be processed due to a lack of encryption. In response to this e-mail received, the responsible party has to inform recipient of the original message about the further steps and nominate a contact person for this purpose. This reply will also serve as confirmation of receipt of the information.
Note: The message from the recipient to the responsible party (sender) will be sent once using a transfer file selected as an example. The selection of all transfer files concerned will be made by the responsible party based on the missing CONTRL messages.

The information must be sent at least to the e-mail address stored in the BDEW or DVGW code number databases and optionally to a market partner e-mail address exchanged, e.g., via contact data sheet. The market partner will be assigned based on the AS2 ID.

12.3 Data transfer by SFTP and REST

A content-secured container must be created for the SFTP and REST transfer protocols. The same consequences apply here as in Chapter 12.1.

If a secure connection cannot be established due to missing or invalid certificates or keys, no transfer files can be exchanged. The consequences are borne by the party that has not provided valid certificates or keys or the party that does not use valid certificates or keys correctly.

Procedure: The sender informs the recipient of the lack of valid certificates or keys from the recipient. The sender must inform the recipient (responsible party) at least once by e-mail about the fact that transfer files cannot be exchanged due to missing or invalid certificates or keys. Based on this e-mail, the responsible party must inform the recipient of the original message via e-mail about the further procedure and specify a contact person for this purpose. This reply also serves as confirmation of receipt of the information.
RD2.0 process data: The information must be sent at least to the e-mail addresses of the market partner exchanged via the contact data sheet of the communication partner.

13 Sources

[1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, Bundesamt für Informationssicherheit, 07.03.2023.
Technical guideline BSI TR-03116 Cryptographic specifications for federal government projects, Part 4: Communication procedures in applications, Federal Office for Information Security, 7 March 2023.

[2] Beschluss (BK7-16-142) und Anlagen zum Beschluss (BK7-16-142), zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende (Tenorziffer 4), Bundesnetzagentur, 20.12.2016.
Decision (BK7-16-142) and annexes to the decision (BK7-16-142) on the adaptation of the regulations for electronic market communication to the requirements of the Act on the Digitalisation of the Energy Transition (Operative Part 4), Federal Network Agency, 20 December 2016.

[3] Mitteilung Nr. 3 (BK7-16-142), Festlegungsverfahren zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, Bundesnetzagentur, 16.05.2017.
Communication No. 3 (BK7-16-142), Determination procedure for adapting the regulations on electronic market communication to the requirements of the Act on the Digitalisation of the Energy Transition, Federal Network Agency, 16 May 2017.

[4] Mitteilung Nr. 7 (BK7-16-142), Festlegungsverfahren zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, Bundesnetzagentur, 12.12.2017.
Communication No. 7 (BK7-16-142), Determination procedure for adapting the regulations for electronic market communication to the requirements of the Act on the Digitalisation of the Energy Transition, Federal Network Agency, 12 December 2017.

[5] Mitteilung Nr. 8 (BK7-16-142), Festlegungsverfahren zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, Bundesnetzagentur, 13.04.2018.
Communication No. 8 (BK7-16-142), Determination procedure for adapting the regulations for electronic market communication to the requirements of the Act on the Digitalisation of the Energy Transition, Federal Network Agency, 13 April 2018.

[6] Beschluss (BK6-18-032) und Anlagen zum Beschluss (BK6-18-032), zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende (Tenorziffer 5 und Tenorziffer 6), Bundesnetzagentur, 20.12.2018.
Decision (BK6-18-032) and annexes to the decision (BK6-18-032) on the adaptation of the regulations on electronic market communication to the requirements of the Act on the Digitalisation of the Energy Transition (Operative Part 5 and Operative Part 6), Federal Network Agency, 20 December 2018.

[7] Mitteilung Nr. 3 zu den Datenformaten zur Abwicklung der Marktkommunikation: Verwendung von Zertifikaten zur Signatur bzw. Verschlüsselung der Marktkommunikation, Bundesnetzagentur, 03.04.2019.

Communication No. 3 on data formats for handling market communication: Use of certificates for signing or encrypting market communication, Federal Network Agency, 3 April 2019.

[8] Mitteilung Nr. 2 zur Festlegung zur künftigen Absicherung der elektronischen Marktkommunikation Strom (BK6-21-282), Bundesnetzagentur, 31.08.2022.
Communication No. 2 on the specification for the future safeguarding of electronic market communication for electricity (BK6-21-282), Federal Network Agency, 31 August 2022.

[9] 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.

[10] 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.

[11] Technische Richtlinie BSI TR-02102-4 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 4: Verwendung von Secure Shell (SSH), Bundesamt für Informationssicherheit, 24.01.2023.
Technical Guideline BSI TR-02102-4 Cryptographic methods: Recommendations and key lengths, Part 4: Use of Secure Shell (SSH), Federal Office for Information Security, 24 January 2023.

[12] 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 in the event of a change of supplier for the supply of gas and the metering point operator framework agreement, Federal Network Agency, 22 November 2023.

14 Annex 1: AS2 profile; version 4

Company name of market partner according to commercial register	*<Name>*
Market partner ID and market role	*<MP ID> <market role>*
Market partner ID and market role (further details are optional)	*further <MP ID> if applicable; further <market role> if applicable*
Market partner ID and market role (further details are optional)	*further <MP ID> if applicable; further <market role> if applicable*
Market partner ID and market role (further details are optional)	*further <MP ID> if applicable; further <market role> if applicable*
AS2 market partner contact	
Contact No. 1	
Name	*<Surname>, <First name>*
Phone	*<Phone number>*
E-mail	*<E-mail address>*
Contact No. 2	
Name	*<Surname>, <First name>*
Phone	*<Phone number>*
E-mail	*<E-mail address>*
AS2 technology contact	
Contact No. 1	
Name	*<Surname>, <First name>*
Phone	*<Phone number>*
E-mail	*<E-mail address>*
Contact No. 2	
Name	*<Surname>, <First name>*
Phone	*<Phone number>*
E-mail	*<E-mail address>*
Contact No. 3	
Name	*<Surname>, <First name>*
Phone	*<Phone number>*
E-mail	*<E-mail address>*

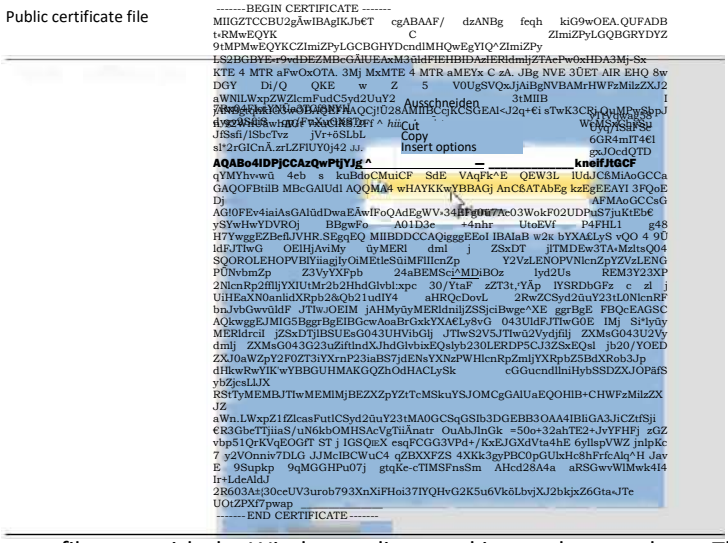
Network	
AS2 URL	***xxx.com/xxx***
IP address (firewall); additional sender IP address (optional)	***xxx.xxx. xxx.xxx -/-***
AS2 certificate	
AS2 ID	The AS2 ID to be used is the MP ID. The MI IDs shown on the previous page determine the MP ID for which the following certificate is used.
Public AS2 certificate	---- BEGIN CERTIFICATE----- ***< Certificate string >*** ---- END CERTIFICATE-----
TLS certificate	
1. Issuer (Issuer DN)	
CN	***<Common Name>***
OU (optional)	***<Organisational Unit>***
O	***<Organisation>***
L (optional)	***<Place>***
ST (optional)	***<Federal State>***
C	***<Country>***
2. Applicant (Subject DN)	
CN	***<Common Name>***
OU (optional)	***<Organisational Unit>***
O	***<Organisation>***
L (optional)	***<Place>***
ST (optional)	***<Federal State>***
C	***<Country>***
3. Alternative applicant (SAN)	
DNS name	***<Domain Name>***

Note: This profile is also embedded as a Word template in this pdf document.

15 Annex 2: Generating a certificate (cer file) from the profile

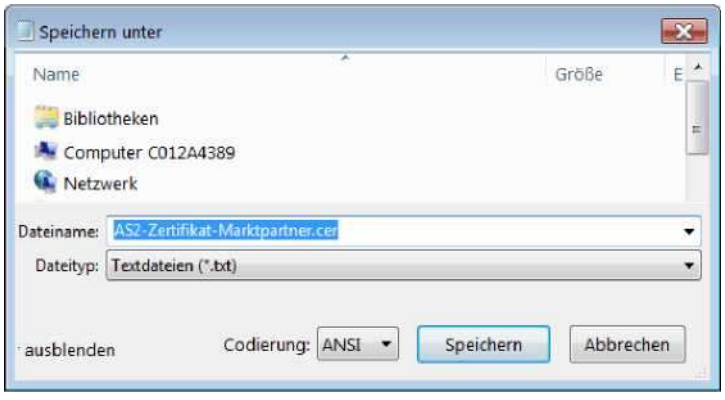
This Annex 2 describes the steps for generating the certificate from the string contained in the profile based on screenshots.

(1) Copy the text from the profile:



(2) Create a new text file, e.g. with the Windows editor, and insert the text there. The last line should not have a line break (CR/LF).

(3) Finally, save the file as a ".cer" file:



16 Annex 3: SFTP profile; version 1

This Annex 3 provides general and organisational information on data exchange via SFTP.

Company name of market partner according to commercial register	*<Name>*	
Market partner ID and market role	*MP ID>*	*< market role>*
Market partner ID and market role (further details are optional)	*further <MP ID> if applicable*	*further <market role> if applicable*
Market partner ID and market role (further details are optional)	*further <MP ID> if applicable*	*further <market role> if applicable*
Market partner ID and market role (further details are optional)	*further <MP ID> if applicable*	*further <market role> if applicable*

SFTP market partner contact

Contact No. 1	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***
Contact No. 2	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***

SFTP technology contact

Contact No. 1	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***
Contact No. 2	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***
Contact No. 3	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***

SFTP server	
SFTP Server Address (receipt)	e.g. sftp://servera.com/wurzelverzeichnis
IP Port (Firewall)	22 (Standard SFTP)
SSH Public Key Fingerprint	
SSH Public Key	---- BEGIN SSH2 PUBLIC KEY ------ ***< Key string >*** ---- END SSH2 PUBLIC KEY ------
SFTP client	
SFTP user name	USERNAME
SSH Public Key Fingerprint	
SSH Public Key	---- BEGIN SSH2 PUBLIC KEY ------ ***< Key string >*** ---- END SSH2 PUBLIC KEY ------
S/MIME certificate	
Public S/MIME certificate (content data security for sending & receiving)	---- BEGIN CERTIFICATE ----- ***< Key string >*** ---- END CERTIFICATE -----

Note: In accordance with Chapter 9.9, it must be ensured that files that are stored on the SFTP server are stored with a dot in front of the name. The dot may only be removed by renaming the files after the write process.

17 Annex 4: REST profile; version 1

This Annex 4 provides general and organisational information on data exchange via the REST webservice.

Company name of market partner according to commercial register	*<Name>*	
Market partner ID and market role	*MP ID>*	*< market role>*
Market partner ID and market role (further details are optional)	*further <MP ID> if applicable*	*further <market role> if applicable*
Market partner ID and market role (further details are optional)	*further <MP ID> if applicable*	*further <market role> if applicable*
Market partner ID and market role (further details are optional)	*further <MP ID> if applicable*	*further <market role> if applicable*

WS market partner contact

Contact No. 1	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***
Contact No. 2	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***

WS technology contact

Contact No. 1	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***
Contact No. 2	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***
Contact No. 3	
Name	***<Surname>, <First name>***
Phone	***<Phone number>***
E-mail	***<E-mail address>***

WS details:

Network	
WS URL	https://xxx.com/xxx
Public TLS certificate for	***<MPID>***
1. Issuer (Issuer DN)	
CN	***<Common Name>***
OU (optional)	***<Organisational Unit>***
O	***<Organisation>***
L (optional)	***<Place>***
ST (optional)	***<Federal State>***
C	***<Country>***
2. Applicant (Subject DN)	
CN	***<Common Name>***
OU (optional)	***<Organisational Unit>***
O	***<Organisation>***
L (optional)	***<Place>***
ST (optional)	***<Federal State>***
C	***<Country>***
3. Alternative applicant (SAN)	
DNS name	***<Domain Name>***
Public TLS certificate for	***further <MPID> if applicable***
1. Issuer (Issuer DN)	
CN	***<Common Name>***
OU (optional)	***<Organisational Unit>***
O	***<Organisation>***
L (optional)	***<Place>***
ST (optional)	***<Federal State>***
C	***<Country>***
2. Applicant (Subject DN)	
CN	***<Common Name>***
OU (optional)	***<Organisational Unit>***
O	***<Organisation>***
L (optional)	***<Place>***
ST (optional)	***<Federal State>***
C	***<Country>***
3. Alternative applicant (SAN)	
DNS-name	***<Domain Name>***

Information on combined ("Kombi") certificate:

Public S/MIME certificate

1. Issuer (Issuer DN)	
CN	***<Common Name>***
OU (optional)	***<Organisational Unit>***
O	***<Organisation>***
L (optional)	***<Place>***
ST (optional)	***<Federal State>***
C	***<Country>***
2. Applicant (Subject DN)	
CN	***<Common Name>***
OU (optional)	***<Organisational Unit>***
O	***<Organisation>***
L (optional)	***<Place>***
ST (optional)	***<Federal State>***
C	***<Country>***
3. Alternative applicant (SAN)	
RFC822 Name	***<email address> or <domain name>***[31]

Note: This profile is also embedded as a Word template in this pdf document.

The optional certificate fields are based on the CAB Forum;
https://cabforum.org/baseline-requirements-documents

[31] Certificates issued with RSASSA-PSS on domain names are available as so-called "AS2 certificates".