This document is based on 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 1.3 (Rules of transmission 1.3)" valid at the time of translation, namely the version published on 1 April 2020, 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=953&tx_bdew_bdew%5Baction%5D=download&tx_bdew_bdew%5Bcontroller%5D=Dokument&cHash=80debae27afd94199b70243485bfa11f

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

https://www.edi-energy.de/index.php?id=38&tx_bdew_bdew[view]=now&tx_bdew_bdew[action]=list&tx_bdew_bdew[controller]=Dokument&cHash=5d1142e54d8f3a1913af8e4cc56c71b2

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

The English version is also published on the homepage of Trading Hub Europe GmbH

Table of contents

1 Introduction

1.1 Scope

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 and e-mail (SMTP) transfer protocols in market communication. It does not govern the transfer protocol requirements applicable in the target model.

The following rules apply to all market processes established by the Federal Network Agency that are processed via EDIFACT, such as GPKE, MPES, GeLi Gas, GaBi Gas, MaBiS, WiM and KoV.

This document does not specify any legal consequences that may arise if secure electronic data exchange cannot take place because a different procedure is used. This document does not consider the exchange of qualified signed EDIFACT transfer files. [7]

According to a Federal Network Agency (BNetzA) ruling, the cryptographic requirements of BSI TR 03116-4 (last revised 31 January 2019) must always be observed and complied with. The parameters to be used and deviations therefrom to be applied are described in this document. [2][6]

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

2 Notifying the information recipient

In order to achieve the greatest possible level of automation in data exchange, the market partners must agree 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 3.2 below, the exchange of data for all EDIFACT-based market processes specified by BNetzA may be carried out by e-mail via SMPT or AS2.

The communication parameters are exchanged after the initial contact has been established by telephone or e-mail.

The aforementioned data must be exchanged between the two parties no later than three working days (in accordance with the GPKE/GeLi Gas calendar) 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 shall 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 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 changes its transfer protocol, it is obliged to inform all market partners with whom it has exchanged EDIFACT transfer files within the last three years of the change. The information must be provided in good time at least 10 working days before the changeover and must be addressed 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 in order to be able to do the necessary checks and, if any faults or errors are detected, 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 shall also apply mutatis mutandis to AS2.

The e-mail address, telephone and fax number published in the DVGW code number database or BDEW code number database shall be used to contact a market partner.

3 Transfer protocols

3.1 Market processes

The transfer protocols to be used for the transfer of transfer files are AS2 or e-mail via SMTP.

If the parties cannot agree on a transfer protocol, the e-mail option (as per Chapter 5) shall be offered in any case.

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 1:1 communication is that a market partner must ensure that its internal organisational structures do not generate any additional workload for the other market partners as part of 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 by the recipient. Accordingly, it shall 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 Rules for data exchange via e-mail

The rules described in this Chapter 5 only apply to the e-mail addresses used to exchange EDIFACT transfer files.

The high degree of variation in the use of e-mail is an obstacle to e-mail use for EDIFACT transfer files. In order to nevertheless achieve a high level of automation on the part of the e-mail recipient, the following rules apply:

5.1 E-mail address

- The e-mail addresses specified for the exchange of EDIFACT transfer files between two market partners must be used exclusively for the exchange of EDIFACT transfer files.
- It 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 EDIFACT transfer files cannot expect these e-mails to be read, let alone answered. The market partner must assume that the non-EDIFACT information sent with the e-mail will go unnoticed.
- The sender of an e-mail must use his 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 can 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.

5.2 E-mail attachment

- An e-mail may only ever contain one EDIFACT transfer 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 disregarded.
- Only gzip compression shall be used for any compression of EDIFACT transfer files.
- Rule for naming the transfer file:
  - The naming convention described in the relevant chapter of the EDI@Energy document entitled "*Allgemeine Festlegungen*" shall apply to the EDIFACT transfer file.▪ The attachment does not need 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.

5.3 E-mail body

- No information that is required for further processing must be included with the actual transmission file in the email (i.e. in the e-mail body). The recipient of the message will only process the content of the EDIFACT 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 disregarded.

- 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 describe 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.

5.4 E-mail subject

The e-mail subject must be the same as the file name. This includes the file extension. Please refer to Chapter 5.2 (e-mail attachment) for the file naming convention.

5.5 Signature and encryption of e-mails

Every e-mail used in the German energy industry to exchange an EDIFACT transfer file must be signed and encrypted.

- The signing and encryption of e-mails must comply with the S/MIME standard. At least version 4.0 (IETF RFC 8551, release year 2019) must be used. [1]
- Every market partner must use exactly one certificate (more precisely the associated private key) for signature generation for each e-mail address used by him. [2] The same private key is used to decrypt the encrypted e-mail sent to this e-mail address by the other market partners. Conversely, certificates of the market partners (one for each e-mail address) must be used for both encryption and signature verification. In this way, only one certificate must be maintained for each e-mail address used by the market partner for market communication, a so-called "combination certificate" with an advanced electronic signature or advanced electronic seal.

5.5.1 Trust service provider

In the following, the technical term "certification authority" (CA) is used instead of the legal term "trust service provider" from the Trust Services Act (*Vertrauensdienstegesetz - VDG*).

The certificate must be issued by a CA which offers certificates in a non-discriminatory manner to market partners of the German energy industry. It must not be a self-issued certificate.

The CA issuing the certificate must meet the following requirements: [1]

- 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.

In addition, the following criteria in particular should be taken into account:

- The IT security department of the CA organisation has been verified by way of an audit/certification process according to a recognised audit/certification standard. Certification according to BSI TR-03145, Secure Certification Authority Operation is recommended.
- The registration service, including services outsourced to service providers (registrars), is performed in accordance with high security standards.
- The operator and the operation are deemed to be trustworthy, also when considering intervention rights of third parties.
- The legal status, in particular with regard to applicable liability and data protection laws, meets the requirements of the company applying for the certificate.

5.5.2 Certificates: Parameters and requirements

All certificates must meet the following requirements: [1][2][5][6]

- The certificate must be issued by a CA that meets the requirements under Chapter 5.5.1.
- All certificates issued up to and including 31.12.2018 must be signed either with the RSASSA-PKCS1-v1_5 signature procedure (signature algorithms sha-256RSA or sha-512RSA) or RSASSA-PSS. These certificates can be used up to the maximum certificate validity (for a maximum period of 3 years) in market communication.
- All new certificates issued from 01.01.2019 onwards must be signed with RSASSA-PSS.
- Each certificate must contain information for a revocation checking, i.e. a CRLDistributionPoint under which current CRLs are available at all times.
- The certificate must not be valid for more than 3 years.
- As a minimum, the certificate must contain the usage purposes of key encryption and digital signature in the KeyUsage field.
- The same key pair must be generated for the different purposes of use "signature" and "encryption" required for market communication and a so-called combination certificate must be issued and used accordingly.
- The certificate must meet the requirements of an advanced electronic signature or an advanced electronic seal.
- The certificate must ensure identification and assignment to the company/service provider or to the organisation operating the e-mail address. So field O of the certificate must contain the legal entity that operates the e-mail box 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 completed with the communication address (specification of the e-mail address). Multiple communication addresses for the same certificate are not permitted.
- The certificate name field "CN" has no process-related, functional meaning in electronic communication and is not evaluated. It is recommended to fill the field with a pseudonym. It is recommended to fill the field with a pseudonym. A certificate is assigned to a natural person or legal entity solely through the CA, and it may not be possible to identify this from the certificate itself. [7]

The following encoding applies to the exchange of public certificates:

- DER-encoded-binary X.509 (with file extension: .cer) or
- Base-64-encoded X.509 (with file extension: .cer).

5.5.3 Algorithms and key specifications for S/MIME

The following algorithms and keys with the specified key lengths shall be used: [1]

- Signature:
  - Hash algorithm: SHA-256 or SHA-512 (according to IETF RFC 5754).
  - Signature algorithm: RSASSA-PSS (according to IETF RFC 4056). The key length of the RSA keys used is at least 2048 bit.
- Encryption:
  - Content encryption: AES-128 CBC, AES-192 CBC or AES-256 CBC (according to IETF RFC 3565).
  - 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. Key length of the RSA keys used at least 2048 bits.

In the implementation of RSA encryption, appropriate countermeasures against chosen-ciphertext attacks must be taken. [1]

5.5.4 Changing certificates and revocation lists

No later than 10 working days before a certificate expires, the owner of this certificate must have provided the follow-up certificate (see Chapter 7). This means there is an overlap period if at least ten working days in which both the old and new certificate are valid.

In 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 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 neither be used for signing nor for encryption.

If a certificate owner no longer wants to use the certificate before the validity period expires or wishes to declare the certificate invalid, it must have this certificate withdrawn 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). The revocation list shall be made publicly accessible at least via http.

Each market partner is obliged to check at least once a day whether certificates of its market partners have been revoked by checking all certificates used by it against the 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.

6 Rules for the exchange via AS2

If the EDIFACT files are exchanged via AS2, the AS2 profile version 2 must be used for standardised communication of the own AS2 address parameters. This document also contains the AS2 profile as a Word template.

AS2 is abstractly standardised via RFC 4130. This chapter 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.

6.1 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.

6.1.1 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.

6.1.2 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.

6.2 Requirements for AS2 certificates

The certificate must be only 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 5.5.

6.3 Algorithms and key lengths

See Chapter 5.5.3.

6.4 Transport layer

The IP addresses used must be fixed IP addresses. http must be offered via port 80, optionally https with standard port 443 may also be offered. If https is used, at least TLS version 1.2 or higher must be used to maintain conformity with BSI TR-03116-4. [1]

6.5 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.

6.6 Subject and file name

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

7 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:

- If market partner A is not provided with a certificate from market partner B that meets the minimum technical requirements in order to be able to check the e-mail signature of market partner B, the processing of the data received from market partner A can be refused in accordance with Chapter 8 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 (or for establishing a secure AS2 connection to it), market partner A may refrain from exchanging EDIFACT with market partner B as set out in Chapter 8 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.
- 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. By sending the certificate or the link, the certificate will be deemed to have been exchanged.
- 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, the sender of the transfer file can assume that the signature check and the decryption of the transfer file were successful.
- The preceding rule shall 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.
- 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. Only for market processes: When AS2 is used, transfer files cannot be exchanged if blocked or invalid certificates are used.

8 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:

8.1 For e-mail transfer:

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 optionally to a market partner e-mail address made available e.g. via the contact data sheet.

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 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 by e-mail of the fact that transfer files will not be processed due to a missing or invalid signature. In response to the e-mail received, the responsible party has to inform the sender by e-mail about the further steps taken 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.

Market processes: The selection of all affected transfer files will be made by the responsible party on the basis of the missing CONTRL messages. The information must to 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 on the basis of the market partner ID in the subject of the e-mail.

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 and that the corresponding transfer files cannot therefore be processed. In response to the e-mail received, the responsible party has to inform the sender by 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 using a transfer file selected as an example.

Market processes: The selection of all affected transfer files will be made by the responsible party on the basis of 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 on the basis of the market partner ID in the subject of the e-mail.

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 received, the responsible party has to inform the sender by e-mail 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.

Market processes: The selection of all affected transfer files will be made by the responsible party on the basis of the missing CONTRL messages. The information has to 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 on the basis of the market partner ID in the subject of the e-mail.

8.2 During transfer via AS2

Breach type 1: The recipient has not provided the sender with a valid certificate. Therefore, the sender is 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 has to 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 on the basis of 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 on the basis of 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 on the basis of 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 the e-mail received, the responsible party has to inform the sender by 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 on the basis of an exemplarily selected transfer file. The selection of all transfer files concerned will be made by the responsible party on the basis of 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 on the basis of 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 are will not be processed due to a lack of encryption. In response to the e-mail received, the responsible party has to inform the sender 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 on the basis of 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 on the basis of the AS2 ID.

9 Sources

[1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, Bundesamt für Informationssicherheit, 31.01.2019.
Technical guideline BSI TR-03116 Cryptographic specifications for federal government projects, Part 4: Communication procedures in applications, Federal Office for Information Security, 31.01.2019.

[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 (Tenor No. 4), Federal Network Agency, 20.12.2016.

[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, 16.05.2017.

[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, 12.12.2017.

[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, 13.04.2018.

[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 (Tenor 5 and Tenor 6), Federal Network Agency, 20.12.2018.

[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, 03.04.2019.