

EDI@Energy

Rules on secure data exchange in the schedule process

This English version is for information only.

**In case of divergent interpretations between the German and English
texts, the German text shall prevail.**

Version:	1.5
Publication date:	1 st of October 2021
Applicable from:	1 st of April 2022
Author:	EDI@Energy, AG FPM

Table of contents

1	Introduction	4
2	Notifying the information recipient	5
2.1	Schedule Management	5
3	Transmission channels.....	6
3.1	Schedule Management	6
4	Rules of communication	7
4.1	Schedule Management	7
4.1.1	General information.....	7
4.1.2	Communication in the event of malfunctions	7
5	Rules for exchange via email.....	8
5.1	Email address	8
5.2	Email attachment	8
5.3	Email body	9
5.4	Email subject.....	9
5.5	Signature and encryption of emails	9
5.5.1	Certification authorities.....	10
5.5.2	Certificates: Parameters and requirements	11
5.5.3	Algorithms and key specifications for S/MIME	12
5.5.4	Changing certificates and revocation lists.....	14
6	Rules for exchange via AS2	15
7	Organisational rules relating to certificate management	16
8	Consequences of failure to meet these requirements.....	17
8.1	Error scenario 1.....	17
8.2	Error scenario 2.....	17
8.3	Error scenario 3.....	18
9	Sources.....	19

Disclaimer

This English version is for information only.

In case of divergent interpretations between the German and English texts, the German text shall prevail.

This Document is an extract of the „Regelungen zum Übertragungsweg“ [1] and describes only the part for the scheduling process.

A translation of the part for the EDIFACT process is out of scope of this document.

1 Introduction

This document regulates the security and protection mechanisms that must be maintained for electronic data exchange between the balance responsible parties (BRP) and transmission system operators (TSO) during schedule data exchange using email via SMTP, AS2, SFTP or REST as the transmission channel. For this reason, the communication channel is defined in the following as part of schedule data exchange between the BRP and TSO. The following schedule data of the document “Prozessbeschreibung Fahrplananmeldung in Deutschland” (engl. “Process description Schedule messaging in Germany”) is affected:

- Schedule and reservation from BRP to TSO
- Status request from BRP to TSO
- Acknowledgement from TSO to BRP
- Confirmation report from TSO to BRP
- Anomaly report from TSO to BRP
- Text file “Filenotvalid” / “Wartephase”

This document does not specify any existing legal consequences of following a different procedure that implies secure electronic data exchange cannot take place.

In standard cases, the cryptographic requirements of BSI TR 03116-4 (see [2]) must be applied and maintained. This document describes the parameters to be used and the relevant deviations to be applied.

The following diagram outlines the basic principle of secure schedule data exchange.

2 Notifying the information recipient

In order to achieve the maximum possible automation during data exchange, the market partners must agree to email addresses for data exchange, including the certificates to be used, before sending data for the first time.

2.1 Schedule Management

The email addresses for data exchange are defined in Appendix 2 of the “Bilanzkreisvertrag” (engl. balancing contract).

The exchange of certificates requires contact between the TSO and BRP.

The certificates must be exchanged between the two parties no later than ten working days before a schedule file is first sent by a BRP.

No later than three working days after exchanging the communication data, the two parties must each have exchanged the certificates and have entered the other party’s certificate in all of their systems involved in schedule communication.

3 Transmission channels

3.1 Schedule Management

For the transmission of schedule data the transmission channels email via SMTP, AS2, SFTP or REST are possible. If TSO and BRP cannot agree on one of these transmission channels, email via SMTP is to be used. Signature and encryption are required for data exchange.

The implementation deadlines are defined by the “Bundesnetzagentur” (engl. Federal Network Agency/ the German NRA).

4 Rules of communication

4.1 Schedule Management

4.1.1 General information

- 1) The BRP can use up to two email addresses and/or REST and / or AS2 and/or SFTP for exchanging schedule data between the TSO and BRP.
These must be used in the regular signed and encrypted process, as well as in exceptional case in the event of a technical malfunction (Chapter 4.1.2) for unsigned and/or unencrypted transmission.
- 2) It is possible to use the same email address and associated certificate that is used in data exchange in conventional market processes in accordance with “Regelungen zum sicheren Austausch von EDIFACT-Übertragungsdateien” from EDI@Energy.
- 3) It is permissible to use the same email address for multiple BRPs. This may particularly be the case for service providers.
- 4) If the sender uses a different email address/communication channel than the agreed email addresses/communication channels, the recipient will not process this schedule data exchange.
Accordingly, schedule data exchange will not be deemed as sent and no response will be sent to the sender. In such cases, the sender of the email is responsible for handling the consequences.
- 5) The recipient is responsible for providing the sender with a valid certificate for encryption (see Chapter 5.5.4).
- 6) The sender is responsible for providing the recipient with a valid certificate for signature check (see Chapter 5.5.4).

4.1.2 Communication in the event of malfunctions

The rules listed in this section apply solely in the event of technical malfunctions during schedule data exchange. In other words, one of the communication partners is unable to send or receive signed and encrypted emails due to a technical malfunction in its systems.

In this case, the TSO and BRP can decide through bilateral coordination to process the communication unsigned and unencrypted.

This solution ensures that communication can be resumed very quickly even in the sometimes extremely time-critical scenario of the schedule comparison, which may have a major impact on the grid or market participants.

This requires activities on the part of the TSO and BRP.

In order to keep the period of time taken for unsigned and unencrypted communication as short as possible, the communication partner affected by the malfunction must begin fixing the malfunction immediately.

Problems caused by certificates that are not exchanged or renewed, or that have expired, are not considered to be technical malfunctions.

5 Rules for exchange via email

The rules in chapter 5 are only for data exchange via email, using SMTP.

5.1 Email address

- 1) The email addresses which are given for the data exchange of schedule messages shall only be used to transmit schedule data (no business correspondence).
- 2) The email address must be function-related and not personal (in particular, it does not contain a first name or surname).
- 3) The sender of an email must use their own email address in the FROM field of the email. The TO field of the email must only contain the recipient's email address. Both fields must be completed.
- 4) Processing of business correspondence being sent to email addresses being issued for schedule data exchange cannot be expected.
- 5) Only the "pure" address components of the email address are evaluated (Local-Part@Domain.TLD). No claim exists in relation to the evaluation or addressing of the "phrase".
For example: "Schedule data exchange" <Schedule@Marketpartner.de>
Only the address component Schedule@Marketpartner.de can be used for addressing. If the phrase "Schedule data exchange" (additional information) is sent as well, it is not used in the evaluation.
- 6) The email address must not be interpreted in a case-sensitive way. So in the following example, Schedule@Marketpartner.de and Schedule@MarketPartner.de are identical.

5.2 Email attachment

- 1) An email must contain only one schedule data exchange file and must not contain any further attachments.
- 2) Any business correspondence or text components that are also sent in the email will not be taken into consideration.
- 3) Schedule data must be compressed. Only gzip compression shall be used for compression of the schedule exchange data.¹
- 4) Schedule Message File naming rules:
The file from the schedule data exchange is subject to the naming convention in the document "Prozessbeschreibung Fahrplananmeldung in Deutschland" (engl. "Nomination of schedules in Germany").
- 5) The attachment must not be encrypted separately as this will be done by S/MIME.
- 6) Base64 encoding must be used.
- 7) The Content-Type of the MIME-Parts has to be Application/octet-stream.

¹ gzip is platform-independent

5.3 Email body

- 1) No information that is required for further processing must be included with the actual transmission file in the email (i.e. in the email body). The recipient of the message will only process the content of the schedule transmission file.
Any other information contained in the email body will not be taken into consideration, i.e. business correspondence or text components of the email.
- 2) Certain software products currently used in the overall processing chain for schedule communication via email require text in the email body. For this reason, the email body must be filled purely with text, taking the previous point into consideration. This means in particular that the email body must not be encoded in HTML or contain images or company logos.

5.4 Email subject

The email subject must be the same as the file name from the schedule data exchange.
(File naming rules: See chapter 5.2 Pos. 4)

5.5 Signature and encryption of emails

Every email involved in schedule data exchange must be signed and encrypted:

- 1) Emails must be signed and encrypted in accordance with the S/MIME standard. Version 4.0 is recommended.² Hereby, only methods described in chapter 5.5.3 are permitted.
- 2) Each market partner must use exactly one certificate (or more precisely, the associated private key) for every email address that he or she uses for signature creation.

A market participant uses the same private key for decryption of encrypted emails he has received from other market partner's.

Certificates of the market partners (one per email address) must be used for signature checking and encryption.

This ensures that each email address used by the market partner for communication only needs to maintain one "combined certificate" with advanced signature.

² Taken from Chapter 3.1 [2]

5.5.1 Certification authorities

The certificate must be issued by a certification authority (CA) that offers certificates in a non-discriminatory way to market partners in the German energy industry.

No self-issued certificate may be used.³

The CA⁴ that issues the certificate must satisfy the following requirements:⁵

- 1) The CA has a revocation service for revoking certificates. It maintains a publicly accessible certificate revocation list (CRL) for this purpose.
- 2) The revocation list must be at least accessible via http.
- 3) In addition, the following criteria in particular should be taken into consideration:
 - a) The CA organisation's IT security has been verified by an audit/certification in accordance with a recognised audit/certification standard. Certification in accordance with BSI TR-03145, Secure Certification Authority operation, is recommended.
 - b) The registration service, including services outsourced to service providers (registrars), is conducted at a high level of security.
 - c) The trustworthiness of the operator and the organisation, including third-party access rights, is assured.
 - d) Transparent rules for certificate creation and CA-handling are published within the CA organisations certificate policy.

³ see BK7 [3] bzw. BK6 [4].

⁴ The rules for the „trust service provider“ shall be hold from the eIDAS-Regulation.

⁵ Taken from Chapter 6.1.1 Certification authorities/trust anchors from [2].

5.5.2 Certificates: Parameters and requirements

The certificates must be issued by a CA that satisfies the requirements specified under 5.5.1 and furthermore must meet the following requirements in addition to⁶:

The certificate must be issued by a CA that satisfies the requirements specified under 5.5.1.

- 1) All certificates must be signed with RSASSA-PSS. The key-length is specified in chapter 5.5.3
- 2) Each certificate must contain information for revocation checking, i.e. a `CRLDistributionPoint`, under which current CRL are available.
- 3) Deviating from [2], the validity of the certificate (root and sub certificate) is limited in accordance to a cryptographical reasonable time. For new end user certificates, the sub certificate should not be older than five years. The cryptographic adequacy has to be guaranteed for the whole validity period. Specially, implying actualisation of the certificate, once the adequacy ends according to [2].
- 4) An `AuthorityInfoAccess-Extension` need not be provided.
- 5) The identical certificate must be used for signature and encryption.
- 6) As a minimum, the certificate must contain the usage purposes of key encryption and digital signature in the `KeyUsage` field.
- 7) The certificate must meet the requirements of an advanced electronic signature or an advanced electronic seal.⁷
- 8) The certificate must ensure identification and assignment to companies/service providers or to the organisation that operates the email address. So field `O` of the certificate must contain the legal person who operates the email inbox for the email address for which the certificate was issued and under which the signed and encrypted emails are sent and received.
- 9) The parameter in the field "Subject Alternative Name" with the value "RFC822-Name=" must be completed with the communication address (specification of email address). In this way, exactly one communication address must be specified. Multiple communication addresses for the same certificate are not permissible.
- 10) 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. A certificate is assigned to a natural or legal person solely through the CA, and it may not be possible to identify this from the certificate itself.⁸

⁶ Taken from 6.1.2 Certificates from [2].

⁷ Requirements for signatures and seals can be found in the eIDAS Regulation (Regulation (EU) No. 910/2014). Operators of CAs frequently use the term "class 2" certificates for this purpose.

⁸ It is recommended to add an additional marker for pseudonyms ("PN") in the "CN" field (for example: "pseudonym:PN").

The following encoding applies to the exchange of public certificates:

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

5.5.3 Algorithms and key specifications for S/MIME

The following algorithms and keys must be used with the specified key lengths⁹:

SIGNATURE:

Hash algorithm	SHA-256 or SHA-512 (in accordance with IETF RFC 5754).
Signature algorithm	RSASSA-PSS (in accordance with IETF RFC 4056) RSA key length at least 2048 bit.

ENCRYPTION:

Content encryption	AES-128 CBC or AES-192 CBC or AES-256 CBC (in accordance with IETF RFC 3565) From 1 st of October 2024 AES-128 GCM must be used.
Key encryption	RSAES-OAEP (in accordance with IETF RFC 8017). Key encryption has hash functions as parameters. SHA-256 or SHA-512 must be used in this case. Following rules apply for certificate key length: <ul style="list-style-type: none"> - Till 31st of March 2022: Existing certificates with RSA key length with at least 2048 bit can be used till expiration. - Certificates newly issued before 31st of March 2022, should already use a RSA key length with at least 3072 bit. - From 1st of April 2022 onwards: RSA key length with at least 3072 bit.

In the implementation of RSA encryption, appropriate countermeasures against chosen-cipher text attacks must be taken.¹⁰

Regarding algorithms for signature and encryption following is applicable additionally:

- 1) From 1st of October 2023, recipient of S-MIME messages, using ECDSA and ECDH for signature and key encryption, must be supported. Acceptance of the curve Brain-

⁹ Taken from Chapter 4.2 to 4.4. from [2].

¹⁰ Taken from Chapter 4.6. and 4.8. from [2].

poolP256r1 for ECC-processes is recommended to comply with the minimal requirements addressed in chapter 4.7 in [2].

- 2) For Sending S/MIMI messages, algorithms in 1) must not be used from 1st of October on. The earliest possible moment for usage is currently aligned on in the procedure BK6-21-282, describing the future protection of the electronic market communication electricity. A final decision is still expected in Q1 2022, hence, implementation of ECDSA and ECDH support does not necessarily have to be started prior to the final decision of the procedure BK6-21-282, subject to reservation of no major delays.

5.5.4 Changing certificates and revocation lists

- 1) No later than ten 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.

- 2) In this overlap period, all market partners sending data can make the switch from the previously used certificate to the new certificate.

Each market partner can independently define the point in time within the overlap period from which he or she will use the new certificate to encrypt emails sent to the certificate owner.

- 3) During the overlapping period, all recipient market partners must be able to process signed and encrypted emails with the previously used certificate and the new certificate, whereby the aforementioned restriction applies to the owner of the certificate.
- 4) From the time at which the old certificate becomes invalid, this can no longer be used for signing and encryption.
- 5) If an owner of a certificate no longer wants to use the certificate before the validity period has elapsed, or wishes to declare this certificate invalid, he or she must have this certificate revoked through the certificate revocations lists of its CA provider.
- 6) Each market partner is obliged check at least once a day whether its market partners' certificates have been revoked by checking all the certificates he or she uses against the CRL.
- 7) If a CRL cannot be accessed via the certificate revocation list distribution point (CRL-DP) published in the certificates by a CA for three days, the issuing CA and all certificates listed under it must be distrusted until an up-to-date CRL is published. Item 7) of Chapter 7 must be followed in this regard. Potential consequences of misuse are describe in chapter 8.

6 Rules for exchange via AS2

A data exchange via AS2 is not used in the scheduling process.

Due to this, the Chapter 6 “Rules for exchange via AS2” was not translated.

7 Organisational rules relating to certificate management

The following organisational rules apply:

- 1) Market partner A can only send an encrypted email to market partner B if market partner B provides a valid certificate that satisfies the requirements specified in Chapter 5.5.
- 2) Once a certificate is revoked or invalid and no valid follow-up certificate is available, no more schedule data exchange can be processed that comes from the associated email address and is signed with the revoked or invalid certificate.
The market partner whose certificate is revoked or invalid must procure a new certificate immediately and must share it with the communication partners.
- 3) If market partner A is not provided with a certificate by market partner B that satisfies the minimum technical requirements for checking the email signature of market partner B, the schedule data exchange can be rejected by market partner A in accordance with Chapter 8 until market partner B has provided an appropriate certificate.
- 4) No later than ten working days before a certificate expires, the owner of this certificate must transmit the follow-up certificate to the relevant contact person.
- 5) Once the certificate (as a gzip-compressed file) or the link to the direct download of the necessary certificate has been transmitted, the certificate is deemed to have been exchanged.
- 6) If the signature check fails because the signature was damaged during transmission, or if the email cannot be decrypted for this reason, then with regard to communication, the parties must proceed as though the schedule data exchange had not been received by the email recipient.
- 7) The aforementioned rule does not apply in the event that the recipient was unable to check the signature of a correctly signed and encrypted email, or to decrypt this email (e.g. due to technical problems).
In this case, the schedule data exchange (in particular with regard to deadlines) must be treated by the recipient as though the problem had not occurred for the recipient.

8 Consequences of failure to meet these requirements

In the event of non-compliance with the rules, the following procedures have been agreed with the federal network agency (Bundesnetzagentur).

8.1 Error scenario 1

The certificates were correctly exchanged between the sender and recipient, but due to current technical problems the sender is not able to conduct signed and encrypted communication correctly.

How to proceed:

- The sent schedule data in this email will not be processed automatically.
The sender is responsible for handling the consequences of the schedule data not being processed.
- The sender (initiator) must contact the recipient and clarify whether this error scenario means that communication can be processed as part of bilateral coordination between the TSO and BRP in accordance with Chapter 4.1.2.

8.2 Error scenario 2

The recipient has not received a valid certificate from the sender.
This means the recipient cannot check the email signature.

How to proceed:

- The recipient is not obliged to process the schedule data in this email.
- The consequences of a lack of communication must be handled by the market partner with responsibility for providing the certificate (sender).
- The recipient must inform the sender (initiator) at least once by email of the fact that no communication can take place due to the lack of a valid certificate.
On the basis of the received email, the initiator (sender) must inform the recipient by email of the next steps and specify an appropriate contact person. This response also serves as confirmation of receipt of this information.
- As a minimum, this information must be sent to the contact persons for “Vertragsmanagement und allgemeine Fragen” (engl. “contract management and general questions”) and the contact person for “allgemeine technische Fragen” (engl. “general technical questions”) specified in the balancing contract.

8.3 Error scenario 3

The sender has not received a valid certificate from the recipient.
This means the sender cannot encrypt the email.

How to proceed:

- The sender is not obliged to proceed with communication.
- The consequences of a lack of communication must be handled by the market partner with responsibility for providing the certificate (recipient).
- The sender must inform the recipient (initiator) at least once by email of the fact that no communication can take place due to the lack of a valid certificate.
On the basis of the received email, the initiator (recipient) must inform the sender by email of the next steps and specify an appropriate contact person. This response also serves as confirmation of receipt of this information.
- As a minimum, this information must be sent to the contact persons for “Vertragsmanagement und allgemeine Fragen” (engl. “contract management and general questions”) and the contact person for “allgemeine technische Fragen” (engl. “general technical questions”) specified in the balancing contract.

9 Sources

- [1] EDI@Energy Regelungen zum Übertragungsweg; Regelungen zum sicheren Austausch von EDIFACT und Fahrplan Übertragungsdateien; Version 1.4; 01.04.2021
- [2] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen (Technical Guideline BSI TR-03116 Cryptographic requirements for Federal Government projects, Part 4: Communication procedures in applications), 24.01.2022.
- [3] 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
- [4] 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.