Rules for secure exchange in the schedule process

Corrected Version

This English version is for information only.

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

Version:	2.2 Corrected Version
Publication date:	03/01/2025
Applicable from:	04/01/2025
Author:	AG FPM
Document Status:	Final

Table of contents

1 Introduction 4
2 Roles, areas, and objects, Glossar 5
2.1 Roles, areas, and objects 5
2.2 Glossar 5
3 Disclosure to the recipient of the information 7
3.1 AS4 Data exchange 7
3.2 E-mail emergency communication 8
4 Communication rules 9
4.1 AS4 communication 9
4.1.1 Futher information 9
4.2 Emergency communication 10
5 AS4 Communication 12
5.1 Certificates and PKI 12
5.1.1 Certification authorities 12
5.1.2 Certificates: Parameters and Requirements 12
5.1.3 Certificate changes 12
5.1.4 Recall and blacklists 13
5.2 Rules for the exchange of meta-information 13
5.3 Services AS4 Profile 14
5.3.1 Test service 14
5.3.2 Exchange of message files 14
5.4 Response-Codes 14
5.5 Organizational regulations for handling Smart Meter PKI certificates 14
5.6 Maximum schedules in an AS4 message 15
6 E-mail Emergency communication 19
6.1 Signature and encryption of E-mails 19
6.1.1 Certification authorities 19
6.1.2 Certificates: Parameters and Requirements for S/MIME 19
6.1.3 Algorithms and key lengths for S/MIME 21
6.1.4 S/MIME-Version 22
6.1.5 Certificate changes and revocation lists 22
6.2 Regulations for exchange via E-mail 23
6.2.1 E-mail address 23
6.2.2 E-mail attachment 24
6.2.3 E-mail-Body 24
6.2.4 E-mail subject 24
6.2.5 File name 25
6.2.5.1 Schedule messages from BRP 25
6.2.5.2 TSO responses 25
6.3 Organizational regulations for handling E-mail certificates 26
7 Consequences of non-compliance with these requirements 28

7.1 AS4 Communication....28
7.1.1 Error scenario 1....28
7.1.2 Error scenario 2....28
7.1.3 Error scenario 3....29
7.1.4 Error scenario 4....29
7.2 E-mail Emergency Communication....30
7.2.1 Error scenario 1....30
7.2.2 Error scenario 2....30
7.2.3 Error scenario 3....31
7.2.4 Error scenario 4....31
8 Sources....33
9 Change History....33

1 Introduction

This document regulates the security and protection mechanisms to comply with the electronic data exchange between the balance responsible parties (BRP) and transmission system operators (TSO) within the framework of the scheduling data exchange, using the communication service E-mail via SMTP and AS4. For this reason, the communication channel within the framework of the scheduling data exchange between the BRPs and TSOs is defined below.

The following data exchange processes according to the document "Process description Nomination of schedules in Germany" are affected:

- Scheduling 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

This document does not specify the possible legal consequences if no secure electronic data exchange can take place due to a deviating procedure.

In general, Tthe cryptographic specifications of BSI TR-03116-4 [1] must be applied and complied with. The parameters to be used and the deviations to be applied are described in this document.

2 Roles, areas, and objects, Glossar

2.1 Roles, areas, and objects

The roles, areas and objects are based on the definitions of the BDEW document "Role Model for Market Communication in the German Energy Market" [5]

Roles: BRP, TSO

Objects balance group

Areas: Control area

2.2 Glossar

Term	Description
Nomination	A schedule nomination is sending a schedule to the TSO.
Balance Responsible Party (BRP)	Balance Responsible Party (BRP), according to the ENTSO-E Harmonized Electricity Market Role Model [HRM]. One or more balance groups are assigned to a BRP. The BRP reports schedules for the balance groups assigned to it.
Balance Group (BG)	A Balance Group is assigned to a Balance Responsible Party. As part of the schedule process, a Balance Group is uniquely identified via an EIC.
Schedule	A schedule contains all transaction and forecast time series of a BG for one calendar day.
Time Series	The time series is either a transaction time series specifying how much electrical power is exchanged between two Balance Groups for one calendar day in each time unit (¼-h), or a forecast time series specifying how much electrical power is fed in or taken out from the feed-in or withdrawal points assigned to the Balance Group for one calendar day in each time unit (¼-h).

Term	Description
Market participant	The term market participant is used as a collective term when both the BRP and the TSO could be meant. Example: Market participant A sends a message to market participant B.

3 Disclosure to the recipient of the information

To achieve a high degree of automation in the data exchange, the market participants must agree on the data exchange addresses, including the certificates to be used, before sending the data for the first time. before sending data for the first time.

3.1 AS4 Data exchange

This is at least the URI of the AS4 web service call (AS4 address) and the certificate with the public key for encrypting a transfer file for the recipient of the transfer file.

The URI of the AS4 web service must be taken from the alternative name field of type URI in the available certificates. The above data must be exchanged between these two parties no later than three working days after a market partner first makes contact. No later than three working days after the exchange of communication data, both parties must have entered or made available the data of the other market partner in all of their systems involved in market communication, so that all requirements for carrying out the electronic data exchange are met.

For data exchange via AS4, the market partner ID must be specified in the BKV/BRP role in Annex 2 of the balancing group contract.

For the AS4 communication “certificate” means the triple-certificate consisting of the three certificates for signature (SIG), encryption (ENC) and link connection of the TLS channel (TLS). This holds for this chapter and the following ones.

In order to achieve the best possible automation in data exchange, the market partners must agree on the data exchange addresses including the certificates to be used before sending the data for the first time. This is at least the certificate with the public key for encrypting a file for the recipient [1] of the file and the URL of the AS4 web service call (AS4 address), which must be taken from the alternative name field of the certificate.

As part of AS4 communication, the TSO uses an AS4 certificate that contains its market partner ID in the role “TSO/ÜNB”.

As part of AS4 communication, the BRP must use an AS4 certificate that contains its market partner ID in the role “BKV/BRP”. This is the same certificate that is also used for certain EDIFACT communication . In this case, a certificate change always affects both processes.

[1] The public keys and certificates for validating the signature or establishing the TLS channel do not need to be exchanged in advance. The signature certificate is included in every AS4 message, and the certificate for establishing the TLS channel is exchanged when the connection is established.

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

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

New certificates, so-called successor certificates, are published automatically via the CA and can be retrieved by the market partners there.

3.2 E-mail emergency communication

The e-mail address for e-mail emergency communication is specified in Annex 2 of the balancing group contract and must be kept up to date.

1. The communication partners are obliged to exchange the certificates and to keep them up to date.
2. The e-mail certificates must be sent as a gzip-compressed attachment by e-mail to the contact person “Certificates for schedule data exchange” from Annex 2 of the balancing group contract [3].
   Alternatively, a URL can be sent that refers directly to the certificate to be downloaded.
3. By transmitting the certificate or the link, the certificate is considered to have been exchanged. The specifications for the test to be carried out can be found in Chapter 6.1.3.
4. The certificates must comply with the specifications in Chapter 6.1.

4 Communication rules

4.1 AS4 communication

1. The data exchange in the scheduling process must be handled via signed and encrypted AS4 communication.
2. For the exchange of scheduling data between TSO and BRP, the BRP must specify its market partner ID in the BDEW role “BRP/BKV”.
3. For AS4 communication, the rules for data exchange in the schedule process mentioned in Chapter 5 must be applied.
4. The BRP announces via balancing group contract the balance groups for which it would like to send schedules (Annex 1.1). It may only nominate schedules for these balance groups to the corresponding TSO using its market partner ID.
5. The responsibility to provide the sender with a valid certificate via the CA for encryption lies with the recipient (see Chapter 5.1.2 ff.).
6. The responsibility to provide the recipent with a valid certificate via the CA for encryption lies with the sender (see Chapter 5.1.2 ff.).

4.1.1 Futher information

1. EDIFACT messages and XML schedules between BRP and TSO must be sent towards the same URL, and therefore usually via the same AS4 server system (AS4 endpoint).
   In both cases, the same market partner ID (MP-ID) must be used in the same market role (BKV/BRP).
   The distinction in the processes (MAKO and schedule) lies in setting the correct parameters in the service field of the AS4 message and the recipient.
   XML schedules between BRP and TSO are exchanged with the AS4 service “FP” in the AS4 message header
2. The market partner ID (MP-ID) is a component and the unique identifier of the certificate triplet and may only exist once. A separate certificate triplet must therefore be obtained for each market role of a company.
3. If several valid certificates exist on the recipient's side for the same MP-ID, the sender can choose which of these certificates to use.
   The recipient must ensure that it can receive data via all URLs in its valid certificates.
4. The URL addresses are freely visible in the "Alternative applicant name" field in all three certificates of a public certificate triple.

The URL of the AS4 web service must be taken from the certificates to be used.
The certificates must be retrieved from the issuer.
Since communication may only take place within Smart Meter PKI (SM-PKI), certificates for a market partner can be searched for directly in the SM-PKI directory services using the associated unique MP ID.

4.2 Emergency communication

The rules listed in this section apply exclusively in the event of technical disturbances in the scheduling data exchange. This means that one of the communication partners cannot send or receive AS4 messages due to a technical fault.

Emergency communication can be used in the event of technical faults on the part of the BRP as well as on the part of the TSO. The emergency communication itself is done by E-mail. The conditions for this and the process are described below:

1. In the event of a possible disruption in AS4 communication, the communication partners are obliged to provide exactly one E-mail communication address for E-mail-based emergency communication in accordance with Annex 2 of the Balance group contract [2].
    - The E-mail address for emergency communication must be specified in Annex 2 of the Balance group contract [2] and kept up to date.
    - The communication partners are obliged to exchange the certificates necessary for emergency communication and to keep them up to date. For the exchange of certificates for emergency communication, the same process applies as in the case of "normal" communication, see Chapter 3.1 and Chapter 6
2. In this case, the communication can be handled by signed and encrypted E-mail. This approach ensures that communication can be resumed at short notice even in the sometimes time-critical situations of scheduling comparison, which may have a major impact on the grid operation or Market Participants.
    - If a BRP wants to switch to emergency communication with a TSO, this must be done by telephone call from the BRP to the TSO.
    - If a TSO wants to switch to emergency communication with all BRP in its control area, it is sufficient to inform the TSO by E-mail to all BRP in deviation from the previous sentence. Approval by the BRP is not necessary in this case. This should make it possible to maintain the scheduling exchange in the event of a technical disturbance on the part of a TSO.

3. To keep the time range of E-mail-based emergency communication as short as possible, the communication partner affected by the fault is obliged to start rectifying the fault immediately.
4. Problems arising from certificates that have not been replaced, renewed or expired are not considered technical faults.

5 AS4 Communication

The AS4 protocol based on the AS4 profile of the BDEW [5] is used as the communication service.

5.1 Certificates and PKI

Communication is secured by using the Smart Metering PKI (SM-PKI) of the BSI [7]The requirements of the Certificate Policy (CP) of the SM-PKI must be kept.

5.1.1 Certification authorities

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

5.1.2 Certificates: Parameters and Requirements

The requirements for the certificates result from the CP of the PKI being used. In particular, the MP ID of the Market Participant must be included in the “Organisational Unit” ("OU") field of the subject of the subject in the certificate.

5.1.3 Certificate changes

1. No later than 10 working days before certificates become invalid, the holder of these certificates must have provided the successor certificates (see Chapter 2 and Chapter 5.5). This creates an overlapping period of at least 10 working days, during which the previous and the new certificates are still valid at the same time.
2. Within this overlapping period, all Market Participants can switch from the previously used to the new certificates.
3. The public key for signing is transmitted with the associated certificate in every AS4 message and may therefore be used immediately by the sender of an AS4 message. The recipient of the message can validate the signature against the submitted certificate.
4. A new certificate, with the associated public key for establishing the TLS channel, may be used immediately by both the sender and the receiver of an AS message, as this is transmitted when the TLS channel is established.
5. During the overlapping period, all Market Participants must be able to process AS4 messages signed and encrypted with both the previously used and the new certificates.

5.1.4 Recall and blacklists

1. If a certificate holder no longer wishes to use his certificate or to declare it invalid before the expiration date of the validity period, he must have his certificate withdrawn via the CRL lists of his CA provider. The specifications and regulations for the revocation of certificates, processing of revocation lists and the update and review times are set out in the Certificate Policy (CP) der SM-PKI [7].
2. If a CRL is not available from a CA for more than three days in a row via the certificate revocation list distribution point (CRL-DP) published in the certificates, or if it is invalid, the issuing CA and all certificates listed below it are to be distrusted until a current CRL is published. The possible consequences in chapter 7.1

5.2 Rules for the exchange of meta-information

For the exchange of schedule files in market communication, the fields within the "PartProperties" element are filled according to tables 5-1 5-2 and 5.3. (See page 16 to 18)

5.3 Services AS4 Profile

5.3.1 Test service

Before using the AS4 web service for the first time to transfer message files, the test service is to be used to test the basic availability and the connection establishment to the target of the web service call.

5.3.2 Exchange of message files

The following combination of service and action is used for data exchange within the framework of market processes.

Service: https://www.bdew.de/as4/communication/services/FP

Action: http://docs.oasis-open.org/ebxml-msg/as4/200902/action

Other services described in the AS4 profile are not permitted in the scheduling process.

5.4 Response-Codes

The transfer via AS4 is only successful upon receipt of the non-repudiation receipt (NRR) on AS4 message level.

In case of receipt of an error message (Error Code) of type (Severity) “failure”, the transfer has failed.

5.5 Organizational regulations for handling Smart Meter PKI certificates

Market Participant A can only send an encrypted message to Market Participant B if Market Participant B has provided a valid certificate that meets the requirements specified in Chapter5.1 Therefore, in addition to these technical requirements, the following organizational regulations also apply:

1. As soon as a certificate is revoked or invalid and no valid successor certificate exists, transfer files may no longer be processed that originate from the corresponding sender address and are signed with the revoked or invalid certificate.
   The Market Participant whose certificate is blocked or invalid must immediately obtain a new certificate and distribute it to all its market communication partners.
2. If Market Participant A receives an AS4 message that does not contain a valid signature certificate from Market Participant B that meets the minimum technical requirements to verify the signature of Market Participant B, Market Partner A may refuse the processing

of the received data in accordance with Chapter 7.1until Market Participant B uses a corresponding certificate.

3. If Market Participant A does not provide a certificate from Market Participant B that meets the minimum technical requirements to encrypt the message to Market Participant B, Market Participant A may omit the data exchange to Market Participant B until Market Participant B has provided a corresponding certificate.

    a. If the signature verification fails because the signature was damaged during transmission or if the E-mail cannot be decrypted as a result, this is considered equivalent as if the attached transfer file has not arrived at the recipient. If an ACKNOWLEDGEMENT message is sent to the transfer file by the recipient, the sender of the transfer file can assume that the signature verification and decryption of the transfer file were successful.

    b. The preceding rule does not apply if the recipient has not been able to verify the signature of a correctly signed and encrypted E-mail or to decrypt it (e.g. due to technical problems). In this case, the attached transfer file must be treated by the recipient as if the problem had not existed with the recipient, especially regarding the deadlines.

5.6 Maximum schedules in an AS4 message

In each AS4 request exactly one schedule must be sent. The AS4 request must consist of exactly two MIME parts according to [5], Chapter 2.3.3.

The first MIME part must contain the SOAP envelop, the second MIME part the file to be delivered.

Table 5-1: Part Properties for the ESS 2.3 format

	Schedule Message	ACK	Confirmation Report	Anomaly Report	Status Request
BDEWDocumentType:	A01 [Balance responsible schedule]	A17 [Acknowledgement Document]	A07 [Intermediate Confirmation report] A08 [Final confirmation Report] A09 [Finalised Schedules] (DayAhead Confirmation Report)	A16 [Anomaly Report]	A59 [Information request]
BDEWFulfillmentDate: *)	Schedule time interval (Scheduleday) "YYYY-MM-DD"	Acknowledged time interval "YYYY-MM-DD"	Schedule time interval "YYYY-MM-DD"	Schedule time interval "YYYY-MM-DD"	Requested time interval (Requested Scheduleday) "YYYY-MM-DD"
BDEWDocumentNo:	Message Version	ReceivingMessage Version	Confirmed Message Version	Last accepted Schedule Message: Message Version	1
BDEWSubjectPartyID:	SenderIdenticication (EIC of the Balance Group, the Message is send)	SenderIdenticication (EIC of the Balance Group, the ACK is send)	SenderIdenticication (EIC of the Balance Group, the CNF is send)	SenderIdenticication (EIC of the Balance Group, the ANO is send)	SenderIdenticication (EIC of the Balance Group, the SRQ is send)
BDEWSubjectPartyRole	SenderRole	SenderRole	SenderRole	SenderRole	SenderRole

*) The **BDEWFulfillmentDate** element must be filled with the date of the schedule day in the form YYYY-MM-DD, regardless of the data format used.

Table 5-2: Part Properties for the data format IEC / CIM

	Schedule Message	ACK	Confirmation Report	Anomaly Report	Status Request
BDEWDocumentType:	A01 [Balance responsible schedule]	A17 [Acknowledgement Document]	A07 [Intermediate Confirmation report] A08 [Final confirmation Report] A09 [Finalised Schedules] (DayAhead Confirmation Report)	A16 [Anomaly Report]	A59 [Information request]
BDEWFulfillmentDate: *)	schedule_Time_Period.timeInterval (Scheduleday) "YYYY-MM-DD"	Acknowledged time interval "YYYY-MM-DD"	schedule_Period.timeInterval "YYYY-MM-DD"	schedule_Time_Period.timeInterval "YYYY-MM-DD"	schedule_Time_Period.timeInterval "YYYY-MM-DD"
BDEWDocumentNo:	revisionNumber	Received_MarketDocument revisionNumber	confirmed_MarketDocument.revisionNumber	Last accepted Schedule Message: revision number	1
BDEWSubjectPartyID:	subject_MarketParticipant.mRID (EIC of the Balance Group, the Message is send)	sender_MarketParticipant.mRID (EIC of the Balance Group, the ACK is send)	sender_MarketParticipant.mRID (EIC of the Balance Group, the CNF is send)	sender_MarketParticipant.mRID (EIC of the Balance Group, the ANO is send)	sender_MarketParticipant.mRID (EIC of the Balance Group, the SRQ is send)
BDEWSubjectPartyRole	subject_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type

*) The **BDEWFulfillmentDate** element must be filled with the date of the schedule day in the form YYYY-MM-DD, regardless of the data format used.

Table 5-3: Part Properties for the Auction Message 1.0

(Long Term Reservation Process at the Border DE / CH)

	Auction Message	ACK
BDEWDocumentType:	X02 [Longtime Reservation]	A17 [Acknowledgement Document]
BDEWFulfillmentDate: *)	Schedule time interval (Scheduleday) "YYYY-MM-DD"	Acknowledged time interval "YYYY-MM-DD"
BDEWDocumentNo:	MessageVersion	Acknowledged Version
BDEWSubjectPartyID:	SenderIdentification (EIC of the Balance Group, the Longterm Reservation is send)	SenderIdentification (EIC of the Balance Group, the ACK is send)
BDEWSubjectPartyRole	SenderRole	SenderRole

Remark:
The Receiver of the AS4 Message (Longterm Reservation) is „TransnetBW" in the BDEW Role "ÜNB"
The Rolle „Auktionskoordinator" (Capacity Corrodinator) does not exist in the BDEW Role Modell.

*) The **BDEWFulfillmentDate** element must be filled with the date of the schedule day in the form YYYY-MM-DD, regardless of the data format used.

6 E-mail Emergency communication

6.1 Signature and encryption of E-mails

This section regulates the organization and technical specifications for signature and encryption.
The certificates must meet the following requirements according to Chapter 4.1.2 from BSI TR 03116-4 [1] with the following exceptions and supplements.

6.1.1 Certification authorities

In the following, instead of the legal term "trust service provider" from the Trust Services Act, the technical term "certification body" or Certification Authority (CA) is used.

The certificate must be issued by a CA[2] that offers certificates on a non-discriminatory basis for Market Participants of the German energy industry. It must not be a so-called self-issued certificate.

The conditions of Chapter 6.1.1 Certification Authorities/Trusted Anchors from [1] apply, with the following addition:

- The CA has a callback service that can be used to revoke certificates. For this purpose, it maintains certificate revocation list (CRL), which is publicly accessible.
- The blacklist must be made publicly accessible at least via http.

6.1.2 Certificates: Parameters and Requirements for S/MIME

1. All certificates must contain information for a callback check, which is a `CRLDistributionPoint` where up to date CRL are always available.
2. It is not mandatory to deploy an `AuthorityInfoAccess` extension.
3. The certificate must be issued by a CA that meets the requirements set out in Chapter 6.1.
4. In deviation from BSI TR-03116-4 [1], the validity period of the certificates of the root and sub-CAs shall be limited to a cryptographically justifiable time.
   For new 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 shall be

[2] According to the Trust Services Act, supervision is the responsibility of the Federal Network Agency (BNetzA). The corresponding English term is "trust service provider" according to the eIDAS Regulation.

ensured for the entire period of validity referred to in [1], where available. This implies that a certificate must be renewed when its validity expires in accordance with [1].

5. The same certificate (combined certificate) must be used for signature and encryption.
6. All certificates must be signed with RSASSA-PSS.
7. The key length is described in Chapter 5.1.3. of this document
8. The certificate must meet the requirements for an advanced electronic signature or an advanced electronic seal.[3]
9. The certificate must ensure identification and assignment to the company/service provider or organization that operates the E-mail address. The field O of the certificate must contain the legal entity that operates the E-mail mailbox to the E-mail address for which the certificate was issued and under which the signed and encrypted E-mails are sent and received.
10. The parameter in the field "Alternative subject name" with the value "RFC822-Name=" must be filled with the communication address (specify the E-mail address). Multiple communication addresses in a certificate are not allowed.

    The certificate name field "CN" is not used and is not evaluated It is recommended to assign a pseudonym to the field.

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

[3] Requirements for signatures and seals can be found in the eIDAS Regulation (Regulation (EU) No. 910/2014). CAs often use the term "class 2" certificates for this purpose.

6.1.3 Algorithms and key lengths for S/MIME

The following algorithms and keys with the specified key lengths shall be used:[4]

SIGNATURE:

Hash algorithm	SHA-256 or SHA-512 (according to IETF RFC 5754).
Signature algorithm	RSA key length at least 3072 Bit RSASSA-PSS (according to IETF RFC 4056)

ENCRYPTION:

Content encryption	AES-128 CBC (according to IETF RFC 3565)
Key encryption	RSA key length at least 3072 Bit. RSAES-OAEP (according to IETF RFC 8017). Key encryption has hash functions as parameters. SHA-256 or SHA-512 shall be used.

Implementations of RSA encryption shall include appropriate countermeasures against chosen-ciphertext attacks.[5]

[4] Selection from the Chapters 4.2 to 4.4; taken from [1]

[5] Analogous to the Chapters 4.6 Further requirements and 4.8 Transitional arrangements; taken from [1].

6.1.4 S/MIME-Version

Signing and encryption are only permitted according to the S/MIME standard of Chapter 4.1 of [1].
Only the cryptographic methods evaluated, described and selected in this document are permitted, which are specified in Chapter 5.1.3.

6.1.5 Certificate changes and revocation lists

1. No later than 10 working days before a certificate expires, the holder of this certificate must have provided the successor certificate (see Chapter 6.3). This creates an overlap time interval of at least 10 working days, in which the old and the new certificate are still valid.
2. Within this overlapping period, all Market Participants can switch from the previously used certificate to the new certificate. The certificate holder may use the new certificate for signing at the earliest three working days after he has made it available to his Market Participants. Each of its Market Participants can independently determine the time within the overlap period from which it uses the new certificate to encrypt E-mails to the certificate holder.
3. During the overlap period, all Market Participants must be able to process E-mails signed and encrypted with both the previously used certificate and the new certificate, whereby the certificate holder is subject to the described restriction.
4. From the time the old certificate becomes invalid, it must not be used for signing or encryption anymore.
5. If a certificate holder no longer wants to use his certificate or declares it invalid before the expiration date of the validity period, the certificate holder must have his certificate withdrawn via the revocation lists of his CA provider.
6. Each Market Participant is obliged to check at least once a day whether certificates of its Market Participants have been blocked by checking all certificates used by it against the CRL.
7. If a CRL is not available from a CA for more than three days in a row via the certificate revocation list distribution point (CRL-DP) published in the certificates, the issuing CA and all certificates listed below it are to be distrusted until a current CRL is published. The concrete possible consequences can be found in Chapter 7.2.

6.2 Regulations for exchange via E-mail

The rules described in this section apply only the transmission of E-mails via SMTP.

The high variety of variants in E-mail use requires rules to achieve a high degree of automation on the part of the E-mail recipient.

6.2.1 E-mail address

1. The E-mail addresses specified for the exchange of scheduling data between two Market Participants shall only be used for the exchange of scheduling data.
2. It must be a person-neutral, function-related E-mail address (especially without first and last name).
3. A Market Participant who sends E-mails with business correspondence to the E-mail address of another Market Participant specified for data exchange, cannot expect these E-mails to be read or even answered.
   The market participant must assume that the non-scheduling data sent along will not be considered.
4. The sender of an E-mail must use his own E-mail address in the FROM field (= FROM) of the E-mail. The TO field (= TO) of the E-mail must be filled exclusively with the E-mail address of the recipient. Both fields must be filled.
5. For the E-mail address, only the "pure" address components are evaluated (Local-Part@Domain.TLD). There is no entitlement to evaluation or addressing of the "phrase". Example: "Datenaustausch Fahrplan" <Fahrplan@Marktpartner.de>
   - Only the address part Fahrplan@Marktpartner.de is used.
   - If the phrase "Datenaustausch Fahrplan" (additional information) is sent, it will not be used for evaluation.
   - The E-mail address must not be interpreted in a case-sensitive manner. For example, `Fahrplan@Markt`**`p`**`artner.de` and `Fahrplan@Markt`**`P`**`artner.de` are identical.

6.2.2 E-mail attachment

1. An E-mail may contain only a single file of the scheduling data exchange.
2. No other annexes may be included.
3. Business correspondence or text components of the E-mail will not be considered.
4. For the file from the scheduling data exchange, the naming convention of chapter 6.2.5 applies.
5. The attachment does not need to be encrypted separately, as this is already done by S/MIME.
6. A Base64 encoding must be used.
7. The content type of the MIME part with the attachment must be Application/octet-stream.
8. The scheduling file must be compressed.
9. Only gzip compression may be used for compression.[6]

6.2.3 E-mail-Body

1. No information necessary for further processing may be contained outside the actual transfer file in the E-mail (i.e. in the E-mail body). The message receiver processes only the content of the attached schedule transfer files.
   Other information contained in the E-mail body will not be considered, i.e. Business correspondence sent with it or text elements of the E-mail will not be taken into account.
2. Some software products that are currently used in the entire processing chain of schedule communication via E-mail require a text in the E-mail body. For this reason, the E-mail body must be filled with plain text, considering the previous point. This means that the E-mail body must not be coded in HTML or contain images or company logos.

6.2.4 E-mail subject

The E-mail subject must be the same as the file name of the file from the schedule data exchange.

For the File naming convention, see Chapter 6.2.5.

[6] gzip is platform-independent

6.2.5 File name

The following principles apply for the naming conventions presented below:

- The naming conventions for the subject and file name are mandatory.
- The naming is intended to ensure the prompt, manual identification of the relevant file or email (rule: email subject = file name) to find the original file in case of problems.

6.2.5.1 Schedule messages from BRP

- **BRP schedule message:**
  `<YYYYMMDD>_TPS_<EIC-NAME-BALANCEGROUP>_<EIC-NAME-TSO>_<VVV>.XML`
- **BRP status request:**
  `<YYYYMMDD>_SRQ_<EIC-NAME-BALANCEGROUP>_<EIC-NAME-TSO>.XML`

6.2.5.2 TSO responses

The file names of the responses are generated as follows by the TSOs:

- **Acknowledgement message to a BRP schedule message**
  `<YYYYMMDD>_TPS_<EIC-NAME-BALANCEGROUP>_<EIC-NAME-TSO>_<VVV>_ACK_<YYYY-MM-DDTHH-MM-SSZ>.XML`
- **Acknowledgement message to a BRP status request**
  `<YYYYMMDD>_SRQ_<EIC-NAME-BALANCEGROUP>_<EIC-NAME-TSO>_ACK_<YYYY-MM-DDTHH-MM-SSZ>.XML`
- **Anomaly Report**
  `<YYYYMMDD>_TPS_<EIC-NAME-BALANCEGROUP>_<EIC-NAME-TSO>_<VVV>_ANO_<YYYY-MM-DDTHH-MM-SSZ>.XML`
- **Confirmation Report**
  `<YYYYMMDD>_TPS_<EIC-NAME-BALANCEGROUP>_<EIC-NAME-TSO>_<VVV>_CNF_<YYYY-MM-DDTHH-MM-SSZ>.XML`

Table 6-1: TSO responses: Description of the elements

Placeholder	Meaning
<YYYYMMDD>	Schedule validity date based on the actual calendar day.
<VVV>	Version of the schedule message. The version consists of 3 digits with leading zeroes.
<YYYY-MM-DDTHH-MM-SSZ>	Time of creation of the ACK, anomaly or confirmation message. The time stamp is used to distinguish between several ACK, anomaly (and, where applicable, also confirmation) messages for a schedule message. The format of the MessageDateandTime element from the ESS 2.3 data format or creationDateTime [CIM'] is used. In this case, "T" and "Z" are fixed letters, "T" is used as a separator between the date and time and "Z" refers to the use of UTC (coordinated universal time). In addition, the colons ":" are replaced by hyphens "-" as colons are not permitted in a file name.

6.3 Organizational regulations for handling E-mail certificates

A Market Participant A can only send an encrypted E-mail to a Market Participant B if Market Participant B provides a valid certificate that fulfill the requirements set out in Chapter 6.1. This also applies analogously to the exchange via the other transmission channels mentioned in this document. Therefore, in addition to these technical requirements, the following organizational regulations also apply:

1. As soon as a certificate is revoked or invalid and there is no valid successor certificate, transfer files originating from the associated E-mail address and signed with the revoked or invalid certificate may no longer be processed. The Market Participant whose certificate is blocked or invalid must immediately obtain a new certificate and distribute it to all its market communication partners.
2. If Market Participant A has not been provided with a certificate from Market Participant B that meets the minimum technical requirements to verify the E-mail signature of Market Participant B, Market Partner A can refuse the mail, see chapter E-mail Emergency Communication7.2.

3. If Market Participant A has not been provided with a certificate from Market Participant B that meets the minimum technical requirements to encrypt the E-mail to Market Participant B, Market Participant A can omit the data exchange to Market Participant B until Market Participant B has provided a corresponding certificate.
4. At the latest 10 working days before a certificate expires in the schedule process, the holder of this certificate must transmit the successor certificate to the respective contact person.
5. The certificate to be exchanged must be sent by the Market Participant as a gzip-compressed attachment. Alternatively, an URL can be sent with a direct download link to the certificate. By submitting the certificate or the link, the certificate is considered as replaced. The specifications for the test to be carried out are given in Chapter 6.1.
6. If the signature verification fails because the signature was damaged during transmission or if the E-mail cannot be decrypted, this is considered equivalent as if the attached transfer file has not arrived at the E-mail recipient, i.e., this E-mail is considered as never have been sent. If an acknowledgement message is sent to the transfer file by the recipient, the sender of the transfer file can assume that the signature verification and the decryption of the transfer file were successful.
7. The preceding rule does not apply if the recipient has not been able to verify the signature of a correctly signed and encrypted E-mail or to decrypt it (e.g., due to technical problems). In this case, the attached transfer file (in particular regarding the nomination deadlines) must be treated by the recipient as if the problem had not existed with the recipient.

7 Consequences of non-compliance with these requirements

7.1 AS4 Communication

7.1.1 Error scenario 1

The recipient cannot obtain a valid certificate for encrypting from a registered sub-CA. The sender cannot encrypt the payload.

Procedure:

The sender is entitled not to carry out the communication. If the recipient is a system operator, a complaint to the Federal Network Agency is admissible in addition. The consequences of a lack of communication are to be borne by the Market Participant who has the responsibility to provide the certificate (recipient). The sender must inform the recipient (originator) at least once by E-mail about the fact that the communication will not be carried out due to the lack of a valid certificate. Based on the E-mail received, the originator (recipient) must inform the sender by E-mail about the further procedure and specify a contact person for this purpose. This reply also serves as an acknowledgement of receipt of the information.

Next steps:

This information shall be sent at least to the contact partners for "contract management and general questions" and the contact person for "general technical questions" named in the balancing group contract.

7.1.2 Error scenario 2

The recipient receives a transfer file,

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

Thus, the receiver cannot, inter alia, clearly assign the sender and, moreover, cannot rule out the possibility that the received transmission file could be compromised.

Procedure:

The recipient has the right to refuse to process the transfer file in question.
The Error code “EBMS 0101” (FailedAuthentication) will be send.
The consequences of this non-processing are to be borne by the sender.

7.1.3 Error scenario 3

The recipient receives an encrypted transfer file encrypted with a key that does not belong to the recipient's current certificate. Thus, the recipient cannot decrypt the message and process the contents of 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 Error code “EBMS 0102” (FailedDecryption) will be send.
The consequences of this non-processing are to be borne by the sender.

7.1.4 Error scenario 4

The recipient receives an unencrypted but validly signed transfer file. Thus, the transmission file was not protected against third-party inspection, but the content of the transmission file and sender of the message are not deniable.

Procedure:

The recipient has the right to refuse to process the transfer file in question.
The Error code “EBMS 0103” (PolicyNoncompliance) will be send.
The consequences of this non-processing are to be borne by the sender.

7.2 E-mail Emergency Communication

7.2.1 Error scenario 1

The sender has not received a valid certificate from the recipient. Thus, the sender cannot encrypt the E-mail.

Procedure:

The sender is entitled not to carry out the communication. If the recipient is a system operator, a complaint to the Federal Network Agency is admissible in addition. The consequences of a lack of communication are to be borne by the Market Participant who has the responsibility to provide the certificate (recipient). The sender must inform the recipient (originator) at least once by E-mail about the fact that the communication will not be carried out due to the lack of a valid certificate. Based on the E-mail received, the originator (recipient) must inform the sender by E-mail about the further procedure and specify a contact person for this purpose. This reply also serves as an acknowledgement of receipt of the information.

Next steps:

This information shall be sent at least to the contact partners for "contract management and general questions" and the contact person for "general technical questions" named in Annex 2 of the balancing contract for electricity.

7.2.2 Error scenario 2

The recipient receives an E-mail,

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

The receiver cannot clearly assign the sender and, moreover, cannot rule out the possibility that the received transmission file could be compromised.

Procedure:

The recipient has the right to refuse to process the transfer file in question. The consequences of this non-processing are to be borne by the sender. The recipient must inform the sender (originator) at least once by E-mail about the fact that transmission files are not processed due to a missing or invalid signature. Based on the E-mail received, the originator of the issue (i.e. sender of the schedule date) must inform the other party via E-mail about the

further procedure and specify a contact person for this purpose. This reply also serves as an acknowledgement of receipt of the information.

Note: The information message from the receiver to the originator (sender) is made once based on an exemplarily selected scheduling file.

Next steps:

This information shall be sent at least to the contact partners for "contract management and general questions" and the contact person for "general technical questions" named in the balancing group contract.

7.2.3 Error scenario 3

The recipient receives an encrypted E-mail that has been encrypted with a key that does not belong to the recipient's current certificate. Thus, the recipient cannot decrypt the E-mail and process the contents of the transfer file.

Procedure:

The recipient is unable to decrypt the E-mail and is therefore entitled to refuse processing of the E-mail. The consequences of this non-processing shall be borne by the sender. The recipient must inform the sender (originator) at least once by E-mail about the fact that E-mails cannot be decrypted due to an invalid key and thus the corresponding transmission files are not processed. Based on the E-mail received, the perpetrator must inform the sender by E-mail about the further procedure and specify a contact person for this purpose. This reply also serves as an acknowledgement of receipt of the information.

Note: The information message from the recipient to the originator (sender) is sent once based on an exemplarily selected scheduling file

Next steps:

This information shall be sent at least to the contact partners for "contract management and general questions" and the contact person for "general technical questions" named in the balancing group contract.

7.2.4 Error scenario 4

The recipient receives an unencrypted but validly signed E-mail. Thus, the schedule was not protected against third-party inspection, but the content of the transmission file and sender of the message are not deniable.

Procedure:

The recipient has the right to refuse to process the transfer file in question. The consequences of this non-processing are to be borne by the sender. The recipient must inform the sender (originator) at least once by E-mail about the fact that transmission files are not processed due to a lack of encryption. Based on the E-mail received, the recipient must inform the sender via E-mail about the further procedure and specify a contact person for this purpose. At the same time, this answer also serves as confirmation of receipt of the information.

Note: The information message from the receiver to the originator (sender) is made once based on an exemplary transmission file.

Next steps:

This information shall be sent at least to the contact partners for "contract management and general questions" and the contact person for "general technical questions" named in the balancing group contract.

8 Sources

[1] Technical Guideline BSI TR-03116 Cryptographic specifications for projects of the Federal Government, Part 4: Communication procedures in applications, Federal Office for Information Security [BSI], 24.01.2022.

[2] Decision (BK7-16-142) and annexes to the decision (BK7-16-142), on the adaptation of the requirements for electronic market communication to the requirements of the Act on the Digitisation of the Energy Transition (operative part 4), Federal Network Agency, 20.12.2016.

[3] balancing group contract for electricity on the management of balancing groups; in the currently valid version

[4] BDEW AS4 profile; in the current version; www.edi-energy.de; Currently valid documents

[5] Role model for market communication in the German energy market in the currently valid version https://www.BDEW.de/service/anwendungshilfen/rollenmodell-fuer-die-marktkommunikation-im-deutschen-energiemarkt/

[6] Process description schedule management; in the current version

[7] Certificate Policy of Smart Meter PKI; Federal Office for Information Security, 25.01.2023

9 Change History

See German document