Regelungen zum sicheren Austausch im Fahrplanprozess

Version:	**2.4**
Veröffentlichungsdatum:	01.10.2026
Anzuwenden ab:	01.10.2027
Autor:	AG FPM
Dokumentstatus	Festgelegt

Inhaltsverzeichnis

1 Einführung 4
2 Beteiligte Rollen, Gebiete, Objekte und Begriffsbestimmungen 5
2.1 Rollen, Gebiete und Objekte 5
2.2 Begriffsbestimmungen 5
3 Bekanntmachen beim Informationsempfänger 7
3.1 Übertragungsweg AS4 7
3.2 E-Mail Notfallkommunikation 8
4 Kommunikationsregeln 9
4.1 Übertragungsweg AS4 9
4.1.1 Weitere Punkte 9
4.2 E-Mail Notfallkommunikation 10
4.3 Testmöglichkeiten 12
4.3.1 Test der AS4 Kommunikation 12
5 Übertragungsweg AS4 13
5.1 Zertifikate und PKI 13
5.1.1 Vertrauensdienstanbieter 13
5.1.2 Zertifikate: Parameter und Anforderungen 13
5.1.3 Zertifikatswechsel 13
5.1.4 Rückruf und Sperrlisten 14
5.2 Regelungen für den Austausch von Metainformationen 14
5.3 Services des AS4-Profils 14
5.4 Response-Codes 15
5.5 Organisatorische Regelungen zum Umgang mit Smart Meter PKI Zertifikaten 15
5.6 Anzahl von Fahrplänen in einer AS4 Nachricht 16
6 E-Mail Notfallkommunikation 20
6.1 Signatur und Verschlüsselung von E-Mails 20
6.1.1 Vertrauensdiensteanbieter 20
6.1.2 Zertifikate: Parameter und Anforderungen für S/MIME 20
6.1.3 Algorithmen und Schlüssellängen für S/MIME 22
6.1.4 S/MIME-Version 23
6.1.5 Zertifikatswechsel und Sperrlisten 23
6.2 Regelungen für den Austausch via E-Mail 24
6.2.1 E-Mail-Adresse 24
6.2.2 E-Mail-Anhang 25
6.2.3 E-Mail-Body 25
6.2.4 E-Mail-Betreff 26
6.2.5 Namenskonventionen für den E-Mail-Betreff und den E-Mail-Anhang 26
6.2.5.1 Fahrplananmeldungen eines BKV 26
6.2.5.2 Rückmeldungen des ÜNB 26
6.3 Organisatorische Regelungen zum Umgang mit E-Mail Zertifikaten 27

7 Konsequenzen bei Nicht-Einhaltung dieser Vorgaben 29
7.1 Beim Übertragungsweg AS4 29
7.1.1 Verstoßvariante 1 29
7.1.2 Verstoßvariante 2 29
7.1.3 Verstoßvariante 3 30
7.1.4 Verstoßvariante 4 30
7.2 Bei der E-Mail Notfallkommunikation 31
7.2.1 Verstoßvariante 1 31
7.2.2 Verstoßvariante 2 31
7.2.3 Verstoßvariante 3 32
7.2.4 Verstoßvariante 4 33
8 Quellen 34
9 Änderungshistorie 35

1 Einführung

Dieses Dokument regelt die Sicherheits- und Schutzmechanismen, die für den elektronischen Datenaustausch zwischen den Bilanzkreisverantwortlichen (BKV) und Übertragungsnetzbetreibern (ÜNB) im Rahmen des Fahrplandatenaustausches, unter Nutzung der Übertragungswege AS4 und E-Mail via SMTP, einzuhalten sind.
Deshalb wird im Folgenden der Kommunikationsweg im Rahmen des Fahrplandatenaustausches zwischen den BKV und ÜNB definiert.

Die folgenden Datenaustauschprozesse gemäß dem Dokument „Prozessbeschreibung Fahrplananmeldung in Deutschland“ [6] sind davon betroffen:

- Fahrplan und Reservierung von BKV an ÜNB
- Status Request von BKV an ÜNB
- Acknowledgement von ÜNB an BKV
- Confirmation Report von ÜNB an BKV
- Anomaly Report von ÜNB an BKV

Dieses Dokument benennt nicht die ggf. existierenden rechtlichen Folgen, wenn aufgrund eines abweichenden Vorgehens kein gesicherter elektronischer Datenaustausch stattfinden kann.

Im Standardfall sind grundsätzlich die kryptographischen Vorgaben der BSI TR 03116-4 (siehe [1]) anzuwenden und einzuhalten. Die zu nutzenden Parameter und hiervon anzuwendenden Abweichungen sind in diesem Dokument beschrieben.

2 Beteiligte Rollen, Gebiete, Objekte und Begriffsbestimmungen

2.1 Rollen, Gebiete und Objekte

Die Rollen, Gebiete und Objekte basieren auf den Definitionen der BDEW-Anwendungshilfe „Rollenmodell für die Marktkommunikation im deutschen Energiemarkt“ (siehe [5]).

Prozessbeteiligte: BKV, ÜNB

Objekte: Bilanzkreis

Gebiete: Regelzone

2.2 Begriffsbestimmungen

Begriff	Beschreibung
Anmeldung / Nominierung	Eine Fahrplananmeldung / Fahrplannominierung ist der Versand eines Fahrplans an den ÜNB.
Bilanzkreisverantwortlicher (BKV)	Bilanzkreisverantwortlicher bzw. englisch „Balance Responsible Party“ (BRP), entsprechend dem entso-e Harmonized Electricity Market Role Model [HRM] Einem Bilanzkreisverantwortlichem sind ein oder mehrere Bilanzkreise zugeordnet. Der BKV meldet Fahrpläne für die ihm zugeordneten Bilanzkreise an.
Bilanzkreis (BK)	Ein Bilanzkreis ist einem Bilanzkreisverantwortlichem zugeordnet. Im Rahmen des Fahrplanprozesses wird ein Bilanzkreis über einen EIC identifiziert.
Fahrplan	Ein Fahrplan enthält alle Transaktions- und Prognosezeitreihen eines BK für einen Kalendertag.

Begriff	Beschreibung
Zeitreihe	Die Zeitreihe ist entweder • eine **Transaktionszeitreihe** mit der Angabe wieviel elektrische Leistung an einem Kalendertag in jeder Zeiteinheit (in der Regel in jeder Viertelstunde) zwischen zwei Bilanzkreisen ausgetauscht wird, • oder eine **Prognosezeitreihe** mit der Angabe wieviel elektrische Leistung an einem Kalendertag in jeder Zeiteinheit (in der Regel in jeder Viertelstunde) aus dem Bilanzkreis zugeordneten Einspeise- oder Entnahmestellen eingespeist oder entnommen wird.
Marktpartner	Der Begriff **Marktpartner** wird als Sammelbegriff verwendet, wenn an der Stelle sowohl der BKV als auch der ÜNB gemeint sein könnten. Beispiel: Der Marktpartner A sendet dem Marktpartner B eine Nachricht.

3 Bekanntmachen beim Informationsempfänger

Um beim Datenaustausch eine größtmögliche Automatisierung zu erreichen, müssen sich die Marktpartner vor dem erstmaligen Datenversand unter anderem über die Datenaustauschadressen inklusive der zu verwendenden Zertifikate verständigen.

3.1 Übertragungsweg AS4

Im Rahmen der AS4 Kommunikation ist dies mindestens die Marktpartner-ID des betreffenden Marktpartners. Über diese ID kann der Empfänger die notwendigen Zertifikate bei der Sub-CA abrufen.
Spätestens drei Werktage, nach der erstmaligen Kontaktaufnahme eines Marktpartners, müssen die oben genannten Daten zwischen diesen beiden Parteien ausgetauscht sein.

Spätestens drei Werktage nach Austausch der Kommunikationsdaten müssen beide Parteien die Daten des jeweils anderen Marktpartners in allen ihren an der Marktkommunikation beteiligten Systemen eingetragen bzw. zur Verfügung gestellt haben, so dass alle Voraussetzungen für die Durchführung des elektronischen Datenaustauschs erfüllt sind.

Für den Datenaustausch per AS4 muss die Marktpartner-ID in der Rolle BKV in der Anlage 2 des Bilanzkreisvertrages angegeben werden.

In Bezug auf die AS4-Kommunikation wird in diesem und den folgenden Kapiteln von "Zertifikaten" gesprochen, gemeint ist damit das Zertifikatstripel bestehend aus den Zertifikaten für Signatur (SIG), Verschlüsselung (ENC) und Aufbau des TLS Kanals (TLS).

Die URL des AS4-Webservices muss aus den vorliegenden Zertifikaten dem Feld des Alternativnamens vom Typ URL entnommen werden.

Im Rahmen der AS4-Kommunikation nutzt der ÜNB ein AS4 Zertifikat, das seine Marktpartner ID in der Rolle „ÜNB“ enthält.

Im Rahmen der AS4-Kommunikation muss der BKV ein AS4 Zertifikat nutzen, das seine Marktpartner ID in der Rolle „BKV“ enthält. Dies ist das gleiche Zertifikat, das auch in der Kommunikation für die Marktprozesse genutzt wird. Ein Zertifikatswechsel betrifft in diesem Fall immer beide Prozesse.

Verwendet ein Marktpartner für eine Marktpartner ID mehrere Zertifikate zur gleichen Zeit, ist es anderen Marktpartnern gestattet, mit jedem der gültigen, veröffentlichten Zertifikate mit diesem zu kommunizieren.

Jeder AS4-Endpunkt muss jederzeit ohne Firewall-Freischaltung erreichbar sein.

Neue Zertifikate, sog. Nachfolgezertifikate, werden über die CA automatisiert veröffentlicht und sind von den Marktpartnern dort abzurufen.

3.2 E-Mail Notfallkommunikation

Die E-Mail-Adresse für die E-Mail Notfallkommunikation wird in der Anlage 2 des Bilanzkreisvertrages festgelegt und ist aktuell zu halten.

1. Die Kommunikationspartner sind verpflichtet, die notwendigen Zertifikate auszutauschen und aktuell zu halten.
2. Für den Austausch bzw. die Übermittlung der E-Mail-Zertifikate bestehen folgende Möglichkeiten:
    a. Übermittlung als gzip-komprimierter Anhang per E-Mail an die E-Mailadresse „E-Mail zum Austausch der Zertifikate für Fahrplan-Datenaustausch“ aus der Anlage 2 des Bilanzkreisvertrages [3].
    b. Upload über das jeweilige BKV-Portal des ÜNB (sofern die Funktionalität angeboten wird).
3. Durch die Übermittlung des Zertifikats bzw. des Links gilt das Zertifikat als ausgetauscht. Die Vorgaben zur durchzuführenden Prüfung sind Kapitel 6.1.3 zu entnehmen.
4. Die Zertifikate müssen den Vorgaben aus Kapitel 6.1 entsprechen.
5. Der ÜNB ist berechtigt, Tests von den BKV für die Funktion der E-Mail Notfallkommunikation zu verlangen. Es sind maximal zwei Tests pro Kalenderjahr zulässig.

4 Kommunikationsregeln

Grundsätzlich ist zwischen der technischen Rückmeldung der AS4 Kommunikation (NRR) und der fachlichen Rückmeldung (ACK) des Zielsystems zu unterscheiden. Für den Fahrplanprozess ist der ACK maßgeblich.

4.1 Übertragungsweg AS4

1. Der Datenaustausch im Fahrplanprozess muss über eine signierte und verschlüsselte AS4-Kommunikation abgewickelt werden.
2. Für den Austausch von Fahrplandaten zwischen ÜNB und BKV muss der BKV seine Marktpartner-ID in der Rolle „BKV“ benennen.
3. Für die AS4-Kommunikation sind die im Kapitel 5 genannten Regeln für den Datenaustausch im Fahrplanprozess anzuwenden.
4. Der BKV benennt über den Bilanzkreisvertrag die EIC, für die er Fahrpläne versenden möchte (Anlage 1.1). Nur für diese darf er mit seiner Marktpartner-ID Fahrpläne beim ÜNB anmelden.
5. Die Verantwortung, dem Sender ein gültiges Zertifikat über die CA für die Verschlüsselung bereit stellen zu lassen, liegt beim Empfänger (siehe Kapitel 5.1.2 ff.).
6. Die Verantwortung, dem Empfänger ein gültiges Zertifikat über die CA für die Signaturprüfung bereit stellen zu lassen, liegt beim Sender (siehe Kapitel 5.1.2 ff.).

4.1.1 Weitere Punkte

1. EDIFACT Nachrichten und XML-Fahrpläne müssen zwingend über die gleiche URL, und damit in der Regel über dasselbe AS4 Server System (AS4 Endpunkt), versendet werden.
   In beiden Fällen muss die gleiche Marktpartner-ID (MP-ID) in der gleichen Marktrolle (BKV) genutzt werden.
   Die Unterscheidung in den Prozessen (MAKO und Fahrplan) liegt im Setzen der korrekten Parameter im Feld Service der AS4 Nachricht und des Empfängers.
   Der ÜNB erhält die XML-Fahrpläne in der BDEW Marktrolle „ÜNB“ mit dem AS4 Service „FP“.

2. Die Marktpartner-ID (MP-ID) ist Bestandteil und der alleinige Identifikator des Zertifikatstripels und darf nur einmal vorhanden sein. Es muss daher für jede Marktrolle eines Unternehmens ein eigenes Zertifikatstripel beschafft werden.
3. Wenn mehrere gültige Zertifikate auf Seiten des Empfängers existieren, kann der Sender wählen welches dieser Zertifikate er nutzt.
   Der Empfänger muss sicherstellen, dass er über alle URLs in seinen gültigen Zertifikaten Daten empfangen kann.
4. Die URL-Adressen sind frei einsehbar im Feld „Alternativer Antragstellername“ in allen drei Zertifikaten eines öffentlichen Zertifikatstripels.
   Die URL des AS4 Web-Service muss den zu nutzenden Zertifikaten entnommen werden.
   Die Zertifikate müssen beim Aussteller abgerufen werden.
   Da die Kommunikation ausschließlich innerhalb Smart-Meter-PKI (SM-PKI) erfolgen darf, können Zertifikate für einen Marktpartner direkt mittels der zugehörigen eindeutigen MP-ID in den Verzeichnisdiensten der SM-PKI gesucht werden.

4.2 E-Mail Notfallkommunikation

Die in diesem Abschnitt aufgeführten Regeln gelten ausschließlich im Falle technischer Störungen im Bereich des Fahrplandatenaustausches. Das heißt, einer der Kommunikationspartner kann auf Grund einer technischen Störung keine AS4 Nachrichten versenden bzw. empfangen.

Die Notfallkommunikation kann bei technischen Störungen auf Seiten des BKV sowie auf Seiten des ÜNB zum Einsatz kommen. Die Notfallkommunikation selbst erfolgt per E-Mail. Die Voraussetzungen hierfür und der Prozess sind im Folgenden beschrieben:

1. Für den möglichen Fall einer Störung in der AS4-Kommunikation sind die Kommunikationspartner gemäß der Anlage 2 des Bilanzkreisvertrages [2] verpflichtet, eine E-Mail-Kommunikationsadresse für eine E-Mail basierte Notfallkommunikation anzugeben.
   I. Die E-Mail-Adresse für die Notfallkommunikation ist in der Anlage 2 des BK-Vertrages [2] zu benennen und aktuell zu halten.
   II. Die Kommunikationspartner sind verpflichtet, die für die Notfallkommunikation notwendigen Zertifikate auszutauschen und aktuell zu halten. Für den Austausch der Zertifikate für die Notfallkommunikation gilt der in Kapitel 3.2 und Kapitel 6 beschriebene Prozess.

2. In diesem Fall kann die Kommunikation per signierter und verschlüsselter E-Mail abgewickelt werden. Dieser Lösungsansatz stellt sicher, dass auch in teilweise sehr zeitkritischen Situationen des Fahrplanabgleichs die Kommunikation kurzfristig weitergeführt werden kann.

   I. Aktivierung durch den BKV:

   - Möchte ein BKV mit einem ÜNB auf die Notfallkommunikation wechseln, kann er dazu einen Fahrplan oder einen SRQ per signierter und verschlüsselter E-Mail an den ÜNB senden. Die Absenderadresse muss dabei der für die Notfallkommunikation hinterlegten E-Mail-Adresse aus Anlage 2 des Bilanzkreisvertrags entsprechen.
     Kann der ÜNB den Anhang der E-Mail fehlerfrei verarbeiten, aktiviert der ÜNB für den im Fahrplan oder SRQ genannten Bilanzkreis zusätzlich den E-Mail-Ausgangsweg.
     Der ÜNB ist berechtigt, eine schriftliche Begründung per E-Mail zu verlangen.
   - Die E-Mail Notfallkommunikation bleibt aktiv, bis der ÜNB einen Fahrplan oder SRQ via AS4 für diesen Bilanzkreis vom BKV erhält und fehlerfrei verarbeiten kann.

   II. Aktivierung durch den ÜNB:
   Für den Fall, dass ein ÜNB mit allen BKV in seiner Regelzone auf die Notfallkommunikation wechseln möchte, so genügt abweichend zu vorherigem Satz eine Information des ÜNB per E-Mail an alle BKV.
   Eine Zustimmung durch den BKV ist in diesem Fall nicht notwendig.
   Damit soll im Fall einer technischen Störung auf Seiten eines ÜNB der Fahrplanaustausch aufrechterhalten werden können.
   Die Details zu diesem Prozess sind in der Unterlage „Info-Blatt_Notfallkommunikation“ beschrieben, die auf den Internet-Seiten der ÜNB abrufbar ist.

3. Um den Zeitbereich der E-Mail basierten Notfallkommunikation möglichst kurz zu halten, ist der von der Störung betroffene Kommunikationspartner verpflichtet, unverzüglich mit der Störungsbehebung zu beginnen.
   Besteht die Notfallkommunikation für mehr als drei Tage am Stück, ist in jedem Fall unaufgefordert eine schriftliche Begründung per Mail an die betroffenen Kommunikationspartner zu senden, mit Informationen zur bisherigen Fehleranalyse, sowie eine Abschätzung der voraussichtlichen Dauer der Störungsbehebung.

4. Probleme, die auf Grund nicht ausgetauschter oder nicht erneuerter bzw. abgelaufener Zertifikate entstehen, gelten nicht als technische Störung.

4.3 Testmöglichkeiten

4.3.1 Test der AS4 Kommunikation

Ein Marktpartner kann mit dem Versenden einer AS4 Nachricht mit der Action Einstellung „Test“ prüfen, ob eine Kommunikation mit der angefragten AS4 Gegenstelle möglich ist.
Dazu ist eine AS4 Nachricht mit der Action Einstellung „test“ und dem Service „FP“ zu senden.
Diese AS4 Nachricht, darf keinen weiteren Nutzinhalt haben, d.h. keine Payload und auch keine Part Properties.
Wenn das AS4 Gateway der angefragten Gegenstelle erreichbar ist, wird diese mit einem NRR antworten.
Die Testnachricht wird ausschließlich vom AS4 Gateway des Empfängers bearbeitet und nicht an die Endsysteme des Empfängers weitergegeben. D.h. sollte die AS4 Test Nachricht einen Nutzinhalt haben, wird dieser nicht weiterverarbeitet.

5 Übertragungsweg AS4

Als Übertragungsweg wird das AS4-Protokoll basierend auf dem AS4-Profil des BDEW [4] verwendet.

5.1 Zertifikate und PKI

Die Kommunikation wird durch Verwendung der Smart Metering PKI (SM-PKI) des BSI abgesichert. (siehe [7]) Die Vorgaben der Certificate Policy (CP) der SM-PKI müssen eingehalten werden.

5.1.1 Vertrauensdienstanbieter

Die Vertrauensdienstanbieter müssen eine Sub-CA-Instanz im Sinne der CP der SM-PKI sein.

5.1.2 Zertifikate: Parameter und Anforderungen

Die Anforderungen an die Zertifikate ergeben sich aus der CP der genutzten PKI. Insbesondere muss die MP-ID des Marktpartners muss im Feld Organisational Unit („OU“) des Subject des Antragstellers im Zertifikats enthalten sein.

5.1.3 Zertifikatswechsel

1. Spätestens 10 Werktage, bevor Zertifikate ungültig werden, muss der Inhaber dieser Zertifikate die Nachfolgezertifikate zur Verfügung gestellt haben (vgl. Kapitel 3.1 und Kapitel 5.5).
   Somit entsteht ein Überlappungszeitraum von mindestens 10 Werktagen, in dem noch die bisherigen und die neuen Zertifikate gleichzeitig gültig sind.
2. Innerhalb dieses Überlappungszeitraums muss bei allen Marktpartnern die Umstellung von den bisher genutzten auf die neuen Zertifikate erfolgen.
3. Der öffentliche Schlüssel zum Signieren wird mit dem zugehörigen Zertifikat in jeder AS4-Nachricht übermittelt und darf daher vom Sender einer AS4-Nachricht sofort verwendet werden. Der Empfänger der Nachricht kann die Signatur anhand des übermittelten Zertifikats validieren.

4. Ein neues Zertifikat mit dem dazugehörigen öffentlichen Schlüssel zum Aufbau des TLS-Kanals dürfen sowohl vom Sender als auch vom Empfänger einer AS-Nachricht sofort genutzt werden, da dieses beim Aufbau des TLS-Kanals übermittelt wird.
5. Im Überlappungszeitraum müssen alle Marktpartner in der Lage sein, sowohl mit dem bisher genutzten als auch mit den neuen Zertifikaten signierte und verschlüsselte AS4-Nachrichten zu verarbeiten.

5.1.4 Rückruf und Sperrlisten

1. Will ein Zertifikatsinhaber sein Zertifikat vor Ablauf der Gültigkeitsfrist nicht mehr verwenden oder für ungültig erklären, so muss er sein Zertifikat über die Sperrlisten (CRL) seines CA-Anbieters zurückziehen lassen. Die Vorgaben und Regelungen für die Sperrung von Zertifikaten, Verarbeitung von Sperrlisten und der Aktualisierungs- und Prüfungszeiten ergeben sich aus der Certificate Policy (CP) der SM-PKI [7].
2. Ist eine CRL über den in den Zertifikaten veröffentlichten certificate revocation list distribution point (CRL-DP) von einer CA über 3 Tage nicht abrufbar oder ungültig, ist der ausstellenden CA und aller darunter gelisteten Zertifikate bis zur Veröffentlichung einer aktuellen CRL zu misstrauen. Die möglichen Konsequenzen sind Kapitel 7.1 zu entnehmen.

5.2 Regelungen für den Austausch von Metainformationen

Für den Austausch von Fahrplänen sind die Felder innerhalb des Elements „PartProperties“ entsprechend der Tabellen 5-1 bis 5-3 verpflichtend zu füllen.
(Siehe Seiten: 16-18)

5.3 Services des AS4-Profils

Für den Austausch von Fahrplänen wird die folgende Kombination von Service und Action verwendet.

Service	https://www.bdew.de/as4/communication/services/FP
Action	Im Produktiv Betrieb muss folgender Action-Wert verwendet werden: http://docs.oasis-open.org/ebxml-msg/as4/200902/action Für den AS4-Testservice muss folgender Action-Wert verwendet werden: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test

Andere Service und Action Angaben, welche im AS4-Profil beschrieben sind, sind im Rahmen der Kommunikation im Fahrplanprozesses nicht zulässig.

5.4 Response-Codes

Die Übertragung per AS4 ist erst bei synchronem Erhalt der nicht abstreitbaren AS4-Zustellquittung (non-repudiation receipt) erfolgreich.

Bei Erhalt einer Fehlermeldung (Error Code) vom Typ (Severity) „failure“ gilt die Übertragung als gescheitert.

5.5 Organisatorische Regelungen zum Umgang mit Smart Meter PKI Zertifikaten

Ein Marktpartner A kann nur dann eine Nachricht verschlüsselt an einen Markpartner B versenden, wenn Marktpartner B ein gültiges Zertifikat zur Verfügung stellt, das den unter Kapitel 5.1 genannten Anforderungen genügt. Daher gelten über diese technischen Anforderungen hinaus auch die nachfolgenden organisatorischen Regelungen:

1. Sobald ein Zertifikat gesperrt oder ungültig ist und noch kein gültiges Nachfolgezertifikat vorliegt, dürfen keine AS4-Nachrichten mehr verarbeitet werden, die von der zugehörigen Absender-Adresse stammen und mit dem gesperrten oder ungültigen Zertifikat signiert sind.
   Der Marktpartner, dessen Zertifikat gesperrt oder ungültig ist, hat unverzüglich ein neues Zertifikat zu beschaffen.
2. Sollte Marktpartner A eine AS4-Nachricht empfangen, welche kein gültiges Signaturzertifikat vom Marktpartner B enthält, das den technischen Mindestanforderungen genügt, um die Signatur von Marktpartner B prüfen zu können, so kann gemäß Kapitel 7.1 die Verarbeitung der empfangenen Daten von Marktpartner A so lange abgelehnt werden, bis Marktpartner B ein entsprechendes Zertifikat verwendet.
3. Sollte Marktpartner A kein Zertifikat vom Marktpartner B zur Verfügung gestellt werden, welche den technischen Mindestanforderungen genügt um die Nachricht an den Marktpartner B verschlüsseln zu können, so kann der Datenaustausch durch Marktpartner A an Marktpartner B so lange unterbleiben, bis Marktpartner B ein entsprechendes Zertifikat zur Verfügung gestellt hat.

a. Scheitert die Signaturprüfung, weil die Signatur oder kann die AS4 Nachricht nicht entschlüsselt werden, so ist dies in Bezug auf die Kommunikation im Fahrplanprozess gleichzusetzen, als ob der angefügte Fahrplan nicht beim Empfänger angekommen wäre.
   Wird auf den angefügten Fahrplan der AS4 Nachricht vom Empfänger eine ACK-Nachricht gesendet, kann der Sender der AS4 Nachricht davon ausgehen, dass die Prüfung der Signatur und die Entschlüsselung der AS4 Nachricht erfolgreich war.

b. Die voranstehende Regel findet keine Anwendung für den Fall, dass der Empfänger nicht in der Lage war, die Signatur einer fehlerfrei signierten und verschlüsselten AS4 Nachricht zu prüfen, bzw. diese zu entschlüsseln (z. B. aufgrund technischer Probleme).
   In diesem Fall ist der angefügte Fahrplan (insbesondere bezüglich der Fristen) vom Empfänger so zu behandeln, als hätte das Problem beim Empfänger nicht bestanden.

5.6 Anzahl von Fahrplänen in einer AS4 Nachricht

In einem AS4-Aufruf muss genau ein Fahrplan bzw. SRQ übermittelt werden.[1]
Der AS4-Aufruf darf gemäß des AS4-Profils [4] (Kapitel 2.3.3) aus genau zwei MIME Parts bestehen.
Der erste MIME Part muss den SOAP Envelope enthalten, der zweite MIME Part das zu übertragende Dokument.

[1] Dies ist analog zur Vorgabe im E-Mail Datenaustauch.
Dort ist festgelegt, dass eine E-Mail nur ein Attachement besitzen darf. (Siehe in diesem Dokument Kap. 6.2.2 Abs. 1)

Tabelle 5-1: Part Properties für das Datenformat ESS 2.3

	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 (Fahrplantag) "YYYY-MM-DD"	Acknowledged time interval "YYYY-MM-DD"	ScheduleTimeInterval "YYYY-MM-DD"	ScheduleTimeTnterval "YYYY-MM-DD"	Requested time interval (Angefragter Fahrplantag) "YYYY-MM-DD"
BDEWDocumentNo:	MessageVersion	Acknowledged Version	ConfirmedMessageVersion	Last accepted Schedule Message: MessageVersion	1
BDEWSubjectPartyID:	SenderIdentification (d.h. EIC des Bilanzkreises für den gesendet wird)	SenderIdentification (d.h. EIC des Bilanzkreises für den der ACK gesendet wird)	SenderIdentification (d.h. EIC des Bilanzkreises für den der CNF gesendet wird)	SenderIdentification (d.h. EIC des Bilanzkreises für den der ANO gesendet wird)	SenderIdentification (d.h. EIC des Bilanzkreises für den der SRQ gesendet wird)
BDEWSubjectPartyRole	SenderRole	SenderRole	SenderRole	SenderRole	SenderRole

*) Das Element **BDEWFulfillmentDate** ist, unabhängig vom verwendeten Datenformat, mit dem Datum des Fahrplantages in der Form YYYY-MM-DD zu befüllen.

Tabelle 5-2: Part Properties für das Datenformat 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: *)	Fahrplantag "YYYY-MM-DD"	Acknowledged time interval "YYYY-MM-DD"	schedule_Period.timeInterval "YYYY-MM-DD"	schedule_Time_Period.timeInterval "YYYY-MM-DD"	Angefragter Fahrplantag "YYYY-MM-DD"
BDEWDocumentNo:	revisionNumber	Received_MarketDocument revisionNumber	confirmed_MarketDocument.revisionNumber	Last accepted Schedule Message: revision number	1
BDEWSubjectPartyID:	SenderIdentification (d.h. EIC des Bilanzkreises für den gesendet wird)	SenderIdentification (d.h. EIC des Bilanzkreises für den der ACK gesendet wird)	SenderIdentification (d.h. EIC des Bilanzkreises für den der CNF gesendet wird)	SenderIdentification (d.h. EIC des Bilanzkreises für den der ANO gesendet wird)	SenderIdentification (d.h. EIC des Bilanzkreises für den der SRQ gesendet wird)
BDEWSubjectPartyRole	subject_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type

*) Das Element **BDEWFulfillmentDate** ist, unabhängig vom verwendeten Datenformat, mit dem Datum des Fahrplantages in der Form YYYY-MM-DD zu befüllen.

Tabelle 5-3: Part Properties für die Auction Message 1.0
(Long Term Reservation an der Grenze DE / CH)

	Auction Message	ACK
BDEWDocumentType:	X02 [Longtime Reservation]	A17 [Acknowledgement Document]
BDEWFulfillmentDate: *)	Schedule time interval (Fahrplantag) "YYYY-MM-DD"	Acknowledged time interval "YYYY-MM-DD"
BDEWDocumentNo:	MessageVersion	Acknowledged Version
BDEWSubjectPartyID:	SenderIdentification (d.h. EIC des Bilanzkreises für den die Reservierung durchgeführt wird)	SenderIdentification (d.h. EIC des Bilanzkreises für den der ACK gesendet wird)
BDEWSubjectPartyRole	SenderRole	SenderRole

Anmerkung:
Der Empfänger der AS4 Nachricht (Auction Message) ist die TransnetBW in der BDEW Role "ÜNB"
Im BDEW Rollenmodell gibt es die Rolle „Auktionskoordinator" nicht.

*) Das Element **BDEWFulfillmentDate** ist, unabhängig vom verwendeten Datenformat, mit dem Datum des Fahrplantages in der Form YYYY-MM-DD zu befüllen.

6 E-Mail Notfallkommunikation

6.1 Signatur und Verschlüsselung von E-Mails

Dieser Abschnitt regelt verbindlich die Organisation und technischen Vorgaben zur Signatur und Verschlüsselung.

Die Zertifikate müssen die Anforderungen nach Kapitel 6.1.1 aus der BSI TR 03116-4 [1] mit folgenden Ausnahmen und Ergänzungen erfüllen.

6.1.1 Vertrauensdiensteanbieter

Im Folgenden wird statt dem juristischen Begriff „Vertrauensdiensteanbieter“ aus dem Vertrauensdienstegesetz der technische Begriff „Zertifizierungsstelle“ bzw. „CA“ (engl. Certification Authority) verwendet.

Das Zertifikat muss von einer CA[2] ausgestellt sein, die Zertifikate diskriminierungsfrei für Marktpartner der deutschen Energiewirtschaft anbietet. Es darf kein sogenanntes selbstausgestelltes Zertifikat sein.

Es gelten die Bedingungen des Kapitels 6.1.2 Zertifizierungsstellen/Vertrauensanker aus [1] mit folgender Ergänzung:

- Die CA verfügt über einen Rückrufservice, über den Zertifikate widerrufen werden können. Dazu führt sie eine sogenannte Zertifikatsperrliste (englisch certificate revocation list, CRL), welche öffentlich zugängig ist.
- Die Sperrliste ist öffentlich mindestens per http zugänglich zu machen.

6.1.2 Zertifikate: Parameter und Anforderungen für S/MIME

1. Alle Zertifikate müssen Informationen für eine Rückrufprüfung enthalten, d. h. einen `CRLDistributionPoint`, unter dem jederzeit aktuelle CRLs zur Verfügung stehen.
2. Eine `AuthorityInfoAccess`-*Extension* muss nicht bereitgestellt werden.
3. Das Zertifikat muss von einer CA ausgestellt sein, die den unter Kapitel 6.1 genannten Anforderungen genügt.

[2] Die Aufsicht obliegt nach dem Vertrauensdienstegesetz der Bundesnetzagentur.
Der entsprechende englische Begriff lautet „trust service provider“ nach der eIDAS-Verordnung.

4. In Abweichung zu [1] ist die Gültigkeitsdauer der Zertifikate der Root- und Sub-CAs auf eine kryptographisch vertretbare Zeit zu limitieren.
   Für neu ausgestellte Endnutzer-Zertifikate sollte das ausgestellte Zertifikat für Sub-CAs höchstens fünf Jahre alt sein. Die Eignung der kryptographischen Algorithmen muss jedoch für die gesamte Gültigkeitsdauer gemäß [1] sichergestellt sein, sofern diese verfügbar sind. Dies impliziert insbesondere, dass die Zertifikate aktualisiert werden müssen, wenn die Eignung gemäß [1] ausläuft.
5. Für Signatur und Verschlüsselung muss dasselbe Zertifikat (Kombizertifikat) verwendet werden.
6. Alle Zertifikate müssen mit RSASSA-PSS signiert sein.
7. Die Schlüssellänge wird in Kapitel 6.1.3 beschrieben.
8. Das Zertifikat muss die Anforderungen an eine fortgeschrittene elektronische Signatur oder eines fortgeschrittenen elektronischen Siegels erfüllen.[3]
9. Das Zertifikat muss eine Identifizierung und Zuordnung zum Unternehmen/Dienstleister oder zur Organisation gewährleisten, dass die E-Mail-Adresse betreibt. Somit muss im Feld O des Zertifikats die juristische Person stehen, die das E-Mail-Postfach zu der E-Mail-Adresse betreibt, für die das Zertifikat ausgestellt wurde und unter der die signierten und verschlüsselten E-Mails versendet und empfangen werden.
10. Der Parameter im Feld "Alternativer Antragstellername" mit dem Wert "RFC822-Name=" muss mit der Kommunikationsadresse (Angabe der E-Mail-Adresse) befüllt werden. Mehrere Kommunikationsadressen in einem Zertifikat sind nicht zulässig.

    Das Zertifikatsnamensfeld "CN" kommt nicht zur Anwendung und wird nicht ausgewertet. Es wird empfohlen, das Feld mit einem Pseudonym zu belegen.

    Für den Austausch der öffentlichen Zertifikate gilt die Codierung DER entweder binär X.509 oder Base-64 X.509 mit der Datei-Extension .cer.

[3] Anforderungen an Signaturen und Siegel sind der eIDAS Verordnung (Verordnung (EU) Nr. 910/2014) zu entnehmen. Betreiber von CAs verwenden hierfür häufig den Begriff Zertifikate der „class 2“.

6.1.3 Algorithmen und Schlüssellängen für S/MIME

Es sind folgende Algorithmen und Schlüssel mit den genannten Schlüssellängen zu verwenden [4]:

SIGNATUR:

Hashfunktion (Hash algorithm)	SHA-256 oder SHA-512 (gemäß IETF RFC 5754).
Signaturverfahren (Signature algorithm)	RSA Schlüssellänge mindestens 3072 Bit RSASSA-PSS (gemäß IETF RFC 4056)

VERSCHLÜSSELUNG:

Inhaltsverschlüsselung (Content encryption)	AES-128 GCM
Schlüsselverschlüsselung (Key encryption)	RSA Schlüssellänge mindestens 3072 Bit. RSAES-OAEP (gemäß IETF RFC 8017). Die Schlüsselverschlüsselung hat Hashfunktionen als Parameter. Hierbei sind SHA-256 oder SHA-512 zu verwenden.

In den Implementierungen der RSA-Verschlüsselung sind geeignete Gegenmaßnahmen gegen Chosen-Ciphertext-Angriffe vorzusehen.[5]

Hinsichtlich der Algorithmen zum Signieren und Verschlüsseln gilt zusätzlich folgendes:

- Es muss der Empfang von S/MIME-Nachrichten unterstützt werden, die gemäß [1] die Signatur ECDSA und für die Key Encryption ECDH verwenden.
  Es wird empfohlen, die Kurve BrainpoolP256r1 bei den ECC-Verfahren zu akzeptieren, um den Mindestanforderungen an die Interoperabilität aus Abschnitt 4.7 in [1] zu genügen.

[4] Auswahl aus den Kapiteln 4.2 bis 4.4 aus [1] entnommen

[5] Sinngemäß dem ersten Spiegelstrich aus Kapitel 4.6 Weitere Vorgaben aus [1] entnommen.

6.1.4 S/MIME-Version

Signieren und Verschlüsseln sind ausschließlich nach dem Kapitel 4.1 aus [1] zulässigen S/MIME-Standard gestattet.
Es sind dabei nur die in diesem Dokument bewerteten, beschriebenen und ausgewählten kryptographischen Verfahren zulässig, die in Kapitel 6.1.3 [dieses Dokuments] konkretisiert werden.

6.1.5 Zertifikatswechsel und Sperrlisten

1. Spätestens 10 Werktage, bevor ein Zertifikat abläuft, muss der Inhaber dieses Zertifikats das Nachfolgezertifikat zur Verfügung gestellt haben (vgl. Kapitel 6.3 [dieses Dokuments]). Somit entsteht ein Überlappungszeitintervall von mindestens 10 Werktagen, in dem noch das alte und auch schon das neue Zertifikat gültig sind.
2. Innerhalb dieses Überlappungszeitraums kann bei allen Marktpartnern die Umstellung vom bisher genutzten auf das neue Zertifikat erfolgen. Der Zertifikatsinhaber darf das neue Zertifikat frühestens drei Werktage nach dem er es seinen Marktpartnern zur Verfügung gestellt hat zur Signierung verwenden. Jeder seiner Marktpartner kann eigenständig den Zeitpunkt innerhalb des Überlappungszeitraums festlegen, ab dem er das neue Zertifikat verwendet, um E-Mails an den Zertifikatsinhaber zu verschlüsseln.
3. Im Überlappungszeitraum müssen alle Marktpartner in der Lage sein, sowohl mit dem bisher genutzten als auch mit dem neuen Zertifikat signierte und verschlüsselte E-Mails zu verarbeiten, wobei für den Zertifikatsinhaber die vorgenannte Einschränkung gilt.
4. Ab dem Zeitpunkt, zu dem das alte Zertifikat ungültig wird, darf mit diesem weder signiert noch verschlüsselt werden.
5. Will ein Zertifikatsinhaber sein Zertifikat vor Ablauf der Gültigkeitsfrist nicht mehr verwenden oder für ungültig erklären, so muss er sein Zertifikat über die Sperrlisten seines CA-Anbieters zurückziehen lassen.
6. Jeder Marktpartner ist verpflichtet, mindestens einmal täglich zu prüfen, ob Zertifikate seiner Marktpartner gesperrt wurden, in dem er alle von ihm verwendeten Zertifikate gegen die CRL prüft.
7. Ist eine CRL über die in den Zertifikaten veröffentlichten certificate revocation list distribution point (CRL-DP) von einer CA über 3 Tage nicht abrufbar, ist der ausstellenden CA und aller darunter gelisteten Zertifikate bis zur Veröffentlichung einer aktuellen CRL zu misstrauen. Die konkreten, möglichen Konsequenzen sind Kapitel 12 zu entnehmen.

6.2 Regelungen für den Austausch via E-Mail

Die in diesem Abschnitt beschriebenen Regeln gelten ausschließlich für den Übertragungsweg E-Mail via SMTP.

Die hohe Variantenvielfalt in der E-Mail-Nutzung erfordert Regeln, um dennoch einen hohen Automatisierungsgrad auf Seiten des E-Mail-Empfängers zu erreichen.

6.2.1 E-Mail-Adresse

1. Die für den Austausch von Fahrplandaten zwischen zwei Marktpartnern festgelegte E-Mail-Adresse ist ausschließlich für den Austausch von Fahrplandaten zu nutzen.
2. Es muss sich um eine personenneutrale, funktionsbezogene E-Mail-Adresse handeln (insbesondere ohne Vor- und Nachnamen).
3. Ein Marktpartner, der E-Mails mit Geschäftskorrespondenz an die für Datenaustausch festgelegte E-Mail-Adresse eines anderen Marktpartners sendet, kann nicht erwarten, dass diese E-Mails gelesen oder gar beantwortet werden. Er muss davon ausgehen, dass die mitgesendeten Nicht-Fahrplandaten nicht beachtet werden.
4. Der Versender einer E-Mail hat seine eigene E-Mail-Adresse im VON-Feld (= FROM) der E-Mail zu verwenden. Das AN-Feld (= TO) der E-Mail ist ausschließlich mit der E-Mail-Adresse des Empfängers zu befüllen. Beide Felder müssen gefüllt sein.
5. Bei der E-Mail-Adresse werden nur die „reinen" Adressbestandteile ausgewertet (Local-Part@Domain.TLD). Ein Anspruch auf Auswertung oder Adressierung der „Phrase" besteht nicht.
   Beispiel: „Datenaustausch Fahrplan" <Fahrplan@Marktpartner.de>
   - Zur Adressierung wird nur der Adressteil Fahrplan@Marktpartner.de verwendet.
   - Wird die Phrase „Datenaustausch Fahrplan" (Zusatzinformation) mitgeschickt, wird sie nicht zur Auswertung herangezogen.
   - Die E-Mail-Adresse darf nicht case-sensitiv interpretiert werden. Beispielsweise sind Fahrplan@Markt**p**artner.de und Fahrplan@Markt**P**artner.de identisch.

6.2.2 E-Mail-Anhang

1. In einer E-Mail darf immer nur eine einzige Datei des Fahrplandatenaustausches enthalten sein.
2. Es dürfen keine weiteren Anhänge enthalten sein.
3. Mitgesendete Geschäftskorrespondenz bzw. Textbestandteile der E-Mail werden nicht berücksichtigt.
4. Für die Datei aus dem Fahrplandatenaustausch gilt die Namenskonvention gemäß Kapitel 6.2.5 in diesem Dokument.
5. Der Anhang ist nicht separat zu verschlüsseln, da dies bereits durch S/MIME erfolgt.
6. Es ist eine Base64 Kodierung zu verwenden.
7. Der Content-Type des MIME-Parts mit dem Anhang muss Application/octet-stream sein.
8. Die Fahrplandatei muss komprimiert werden.
9. Zur Komprimierung ist ausschließlich die gzip-Komprimierung zu verwenden.[6]

6.2.3 E-Mail-Body

1. Es dürfen keine Informationen, die zur weiteren Verarbeitung notwendig sind, außerhalb des angehängten Fahrplans in der E-Mail (d. h. im E-Mail-Body) enthalten sein.
   Beim Nachrichtenempfänger wird ausschließlich der Inhalt des angehängten Fahrplans verarbeitet.
   Andere Informationen, die im E-Mail-Body enthalten sind, werden nicht beachtet, d.h. mitgesendete Geschäftskorrespondenz bzw. Textbestandteile der E-Mail werden nicht berücksichtigt.
2. Einige Softwareprodukte, die in der gesamten Verarbeitungskette der Fahrplankommunikation via E-Mail derzeit eingesetzt werden, benötigen im E-Mail-Body einen Text. Aus diesem Grund ist der E-Mail-Body mit reinem Text zu füllen, wobei der vorgenannte Punkt zu beachten ist. Dies bedeutet insbesondere, dass der E-Mail-Body weder in HTML codiert sein darf noch das er Bilder oder Unternehmenslogos enthalten darf.

[6] gzip ist plattformunabhängig

6.2.4 E-Mail-Betreff

Der E-Mail-Betreff muss gleichlautend mit dem Dateinamen der Datei aus dem Fahrplandatenaustausch sein.

Zur Namenskonvention des Dateinamens siehe Kapitel 6.2.5

6.2.5 Namenskonventionen für den E-Mail-Betreff und den E-Mail-Anhang

Für den Austausch von Fahrplandaten via E-Mail gelten die im Folgenden vorgestellten Grundsätze:

- Die Namenskonventionen für den E-Mail-Betreff und dem Dateinamen des Attachements sind verpflichtend.
- Die Namensgebung dient der zeitnahen, manuellen Identifikation der entsprechenden Datei bzw. der E-Mail (Regel: E-Mail-Betreff = Dateiname), um bei Problemen die entsprechende Originaldatei und die dazugehörigen Meldungen schneller zu finden.

6.2.5.1 Fahrplananmeldungen eines BKV

- **Anmeldung Fahrplan des BKV:**
  `<YYYYMMDD>_TPS_<EIC-NAME-BILANZKREIS>_<EIC-NAME-ÜNB>_<VVV>.XML`
- **Status Request des BKV:**
  `<YYYYMMDD>_SRQ_<EIC-NAME-BILANZKREIS>_<EIC-NAME-ÜNB>.XML`

6.2.5.2 Rückmeldungen des ÜNB

Die Dateinamen der Rückmeldungen werden von den ÜNB wie folgt generiert:

- **Acknowledgement Message auf eine Fahrplananmeldung des BKV**
  `<YYYYMMDD>_TPS_<EIC-NAME-BILANZKREIS>_<EIC-NAME-ÜNB>_<VVV>_ACK_<YYYY-MM-DDTHH-MM-SSZ>.XML`
- **Acknowledgement Message auf einen Status Request des BKV**
  `<YYYYMMDD>_SRQ_<EIC-NAME-BILANZKREIS>_<EIC-NAME-ÜNB>_ACK_<YYYY-MM-DDTHH-MM-SSZ>.XML`
- **Anomaly Report**
  `<YYYYMMDD>_TPS_<EIC-NAME-BILANZKREIS>_<EIC-NAME-ÜNB>_<VVV>_ANO_<YYYY-MM-DDTHH-MM-SSZ>.XML`
- **Confirmation Report**
  `<YYYYMMDD>_TPS_<EIC-NAME-BILANZKREIS>_<EIC-NAME-ÜNB>_<VVV>_CNF_<YYYY-MM-DDTHH-MM-SSZ>.XML`

Tabelle 6-1: Rückmeldungen des ÜNB: Beschreibung der Elemente

Platzhalter	Bedeutung
<YYYYMMTT>	Fahrplantag
<VVV>	Version der Fahrplananmeldung. Die Version ist dreistellig mit führenden Nullen.
<YYYY-MM-DDTHH-MM-SSZ>	Zeitpunkt der Erstellung des ACK, der Anomaly oder Confirmation Meldung. Der Zeitstempel dient zur Unterscheidung mehrerer ACK, Anomaly- (und ggf. auch Confirmation-) Meldungen zu einer Fahrplananmeldung. Dabei wird das Format des MessageDateandTime Elements aus dem ESS 2.3 Datenformat bzw. ceationDateTime [CIM] verwendet. Hierbei sind „T“ und „Z“ fixe Buchstaben, „T“ dient als Trennzeichen zwischen Datum und Zeit und „Z“ verweist auf die Verwendung der UTC (koordinierte Weltzeit). Zudem werden die Doppelpunkte ":" durch Bindestriche "-" ersetzt, da Doppelpunkte in einem Dateinamen nicht erlaubt sind.

6.3 Organisatorische Regelungen zum Umgang mit E-Mail Zertifikaten

Ein Marktpartner A kann nur dann eine E-Mail verschlüsselt an einen Markpartner B versenden, wenn Marktpartner B ein gültiges Zertifikat zur Verfügung stellt, das den unter Kapitel 5 genannten Anforderungen genügt. Dies gilt analog auch für den Austausch über die weiteren in diesem Dokument genannten Übertragungswege. Daher gelten über diese technischen Anforderungen hinaus auch die nachfolgenden organisatorischen Regelungen:

1. Sobald ein Zertifikat gesperrt oder ungültig ist und noch kein gültiges Nachfolgezertifikat vorliegt, dürfen keine E-Mails mehr verarbeitet werden, die von der zugehörigen E-Mail-Adresse stammen und mit dem gesperrten oder ungültigen Zertifikat signiert sind. Der Marktpartner, dessen Zertifikat gesperrt oder ungültig ist, hat unverzüglich ein neues Zertifikat zu beschaffen und muss es an alle seine Marktkommunikationspartner verteilen.
2. Sollte dem Marktpartner A kein Zertifikat vom Marktpartner B zur Verfügung gestellt werden, das den technischen Mindestanforderungen genügt, um die E-Mail-Signatur von

Marktpartner B prüfen zu können, so kann gemäß Kapitel 7.2 die Verarbeitung der empfangenen Daten von Marktpartner A so lange abgelehnt werden, bis Marktpartner B ein entsprechendes Zertifikat zur Verfügung gestellt hat.

3. Sollte dem Marktpartner A kein Zertifikat vom Marktpartner B zur Verfügung gestellt werden, welche den technischen Mindestanforderungen genügt, um die E-Mail an den Marktpartner B verschlüsseln zu können, so kann der Datenaustausch durch Marktpartner A an Marktpartner B so lange unterbleiben, bis Marktpartner B ein entsprechendes Zertifikat zur Verfügung gestellt hat.
4. Spätestens 10 Werktage bevor ein Zertifikat im Fahrplanprozess abläuft, muss der Inhaber dieses Zertifikats das Nachfolgezertifikat an den jeweiligen Ansprechpartner übermitteln.
5. Das auszutauschende Zertifikat ist vom Marktpartner als gzip-komprimierter Anhang zu versenden. Alternativ hierzu kann eine URL versendet werden, die direkt auf das herunterzuladende Zertifikat verweist. Durch die Übermittlung des Zertifikats bzw. des Links gilt das Zertifikat als ausgetauscht. Die Vorgaben zur durchzuführenden Prüfung sind Kapitel 5 zu entnehmen.
6. Scheitert die Signaturprüfung oder kann die E-Mail nicht entschlüsselt werden, so ist dies in Bezug auf die Kommunikation im Fahrpanprozess gleichzusetzen, als ob der angefügte Fahrplan nicht beim E-Mail-Empfänger angekommen wäre, d.h., als wäre eine derartige E-Mail nie versendet worden.
   Wird auf den angefügten Fahrplan vom Empfänger eine ACK-Nachricht gesendet, kann der Sender der E-Mail davon ausgehen, dass die Prüfung der Signatur und die Entschlüsselung der E-Mail erfolgreich war.
7. Die voranstehende Regel findet keine Anwendung für den Fall, dass der Empfänger nicht in der Lage war, die Signatur einer fehlerfrei signierten und verschlüsselten E-Mail zu prüfen, bzw. diese zu entschlüsseln (z. B. aufgrund technischer Probleme).
   In diesem Fall ist der angefügte Fahrplan (insbesondere bezüglich der Fristen) vom Empfänger so zu behandeln, als hätte das Problem beim Empfänger nicht bestanden.

7 Konsequenzen bei Nicht-Einhaltung dieser Vorgaben

7.1 Beim Übertragungsweg AS4

7.1.1 Verstoßvariante 1

Für den Empfänger kann kein gültiges Zertifikat zum Verschlüsseln von AS4-Nachrichten bei einer registrierten Sub-CA abgerufen werden.
Somit kann der Sender die AS4-Nachricht nicht verschlüsseln.

Verfahrensweise:

Der Sender ist berechtigt, die Kommunikation nicht durchzuführen. Sofern der Empfänger ein Netzbetreiber ist, ist zusätzlich eine Beschwerde bei der Bundesnetzagentur zulässig. Die Konsequenzen einer ausbleibenden Kommunikation sind von demjenigen Marktpartner zu tragen, der die Verantwortung hat, das Zertifikat zur Verfügung zu stellen (Empfänger). Der Sender hat den Empfänger (Verursacher) mindestens einmal per E-Mail über die Tatsache zu informieren, dass die Kommunikation aufgrund des fehlenden gültigen Zertifikats nicht durchgeführt wird. Der Verursacher (Empfänger) hat auf Basis der eingegangenen E-Mail den Absender per E-Mail über das weitere Vorgehen zu informieren und einen Ansprechpartner hierzu anzugeben. Diese Antwort dient zugleich auch als Eingangsbestätigung der Information.

Weiteres Vorgehen:

Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.

7.1.2 Verstoßvariante 2

Der Empfänger erhält eine AS4-Nachricht,

- die nicht signiert ist oder
- die mit einem ungültigen Zertifikat signiert ist oder
- die mit einer Signatur versehen ist, die nicht mit dem gültigen Zertifikat validiert werden kann.

Somit kann der Empfänger u. a. den Sender nicht eindeutig zuordnen und kann darüber hinaus nicht ausschließen, dass die empfangene AS4-Nachricht kompromittiert sein könnte.

Verfahrensweise:

Der Empfänger ist berechtigt, die Verarbeitung der betreffenden AS4-Nachricht zu verweigern.

Die AS4-Fehlerrückmeldung erfolgt mit dem Code „EBMS:0101“ (FailedAuthentication).

Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen.

7.1.3 Verstoßvariante 3

Der Empfänger erhält eine verschlüsselte AS4-Nachricht, die mit einem Schlüssel verschlüsselt wurde, der nicht zum aktuellen Zertifikat des Empfängers gehört.

Somit kann der Empfänger die AS4-Nachricht nicht entschlüsseln und den Inhalt der AS4-Nachricht nicht verarbeiten.

Verfahrensweise:

Der Empfänger ist nicht in der Lage, die AS4-Nachricht zu entschlüsseln und daher berechtigt, die Verarbeitung der AS4-Nachricht zu verweigern.

Die Fehlerrückmeldung erfolgt mit dem Code „EBMS:0102“ (FailedDecryption).

Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen.

7.1.4 Verstoßvariante 4

Der Empfänger erhält eine nicht verschlüsselte, aber gültig signierte AS4-Nachricht.

Somit war die AS4-Nachricht nicht gegen fremde Einsichtnahme geschützt, der Inhalt der AS4-Nachrichtund Sender der Nachricht sind jedoch nicht abstreitbar.

Verfahrensweise:

Der Empfänger ist berechtigt, die Verarbeitung der betreffenden AS4-Nachricht zu verweigern.

Die Fehlerrückmeldung erfolgt mit dem Code „EBMS:0103“ (PolicyNoncompliance).

Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen.

7.2 Bei der E-Mail Notfallkommunikation

7.2.1 Verstoßvariante 1

Der Sender hat vom Empfänger kein gültiges Zertifikat zur Verfügung gestellt bekommen. Somit kann der Sender die E-Mail nicht verschlüsseln.

Verfahrensweise:

Der Sender ist berechtigt, die Kommunikation nicht durchzuführen. Sofern der Empfänger ein Netzbetreiber ist, ist zusätzlich eine Beschwerde bei der Bundesnetzagentur zulässig. Die Konsequenzen einer ausbleibenden Kommunikation sind von demjenigen Marktpartner zu tragen, der die Verantwortung hat, das Zertifikat zur Verfügung zu stellen (Empfänger). Der Sender hat den Empfänger (Verursacher) mindestens einmal per E-Mail über die Tatsache zu informieren, dass die Kommunikation aufgrund des fehlenden gültigen Zertifikats nicht durchgeführt wird. Der Verursacher (Empfänger) hat auf Basis der eingegangenen E-Mail den Absender per E-Mail über das weitere Vorgehen zu informieren und einen Ansprechpartner hierzu anzugeben. Diese Antwort dient zugleich auch als Eingangsbestätigung der Information.

Weiteres Vorgehen:

Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.

7.2.2 Verstoßvariante 2

Der Empfänger erhält eine E-Mail,

- die nicht signiert ist oder
- die mit einem ungültigen Zertifikat signiert ist oder
- die mit einer Signatur versehen ist, die nicht mit dem gültigen Zertifikat validiert werden kann.

Somit kann der Empfänger u. a. den Sender nicht eindeutig zuordnen und kann darüber hinaus nicht ausschließen, dass die empfangene E-Mail kompromittiert sein könnte.

Verfahrensweise:

Der Empfänger ist berechtigt, die Verarbeitung der betreffenden E-Mail zu verweigern. Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen. Der Empfänger hat

den Sender (Verursacher) insgesamt mindestens einmal per E-Mail über die Tatsache zu informieren, dass E-Mails aufgrund einer fehlenden oder ungültigen Signatur nicht verarbeitet werden. Der Verursacher hat auf Basis der eingegangenen E-Mail den Absender per E-Mail über das weitere Vorgehen zu informieren und einen Ansprechpartner hierzu anzugeben. Diese Antwort dient zugleich auch als Eingangsbestätigung der Information.
Hinweis: Die Informationsmeldung vom Empfänger an den Verursacher (Sender) erfolgt einmalig auf Basis einer exemplarisch ausgewählten Fahrplandatei.

Weiteres Vorgehen:

Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.

7.2.3 Verstoßvariante 3

Der Empfänger erhält eine verschlüsselte E-Mail, die mit einem Schlüssel verschlüsselt wurde, der nicht zum aktuellen Zertifikat des Empfängers gehört. Somit kann der Empfänger die E-Mail nicht entschlüsseln und den Inhalt der E-Mail nicht verarbeiten.

Verfahrensweise:

Der Empfänger ist nicht in der Lage, die E-Mail zu entschlüsseln und daher berechtigt, die Verarbeitung der E-Mail zu verweigern. Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen. Der Empfänger hat den Sender (Verursacher) insgesamt mindestens einmal per E-Mail über die Tatsache zu informieren, dass E-Mails aufgrund eines ungültigen Schlüssels nicht entschlüsselt werden können und somit die entsprechenden E-Mails nicht verarbeitet werden. Der Verursacher hat auf Basis der eingegangenen E-Mail den Absender per E-Mail über das weitere Vorgehen zu informieren und einen Ansprechpartner hierzu anzugeben. Diese Antwort dient zugleich auch als Eingangsbestätigung der Information.

Hinweis: Die Informationsmeldung vom Empfänger an den Verursacher (Sender) erfolgt einmalig auf Basis einer exemplarisch ausgewählten Fahrplandatei.

Weiteres Vorgehen:

Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.

7.2.4 Verstoßvariante 4

Der Empfänger erhält eine nicht verschlüsselte, aber gültig signierte E-Mail. Somit war die E-Mail nicht gegen fremde Einsichtnahme geschützt, der Inhalt der E-Mail und Sender der Nachricht sind jedoch nicht abstreitbar.

Verfahrensweise:

Der Empfänger ist berechtigt, die Verarbeitung der betreffenden E-Mail zu verweigern. Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen. Der Empfänger hat den Sender (Verursacher) insgesamt mindestens einmal per E-Mail über die Tatsache zu informieren, dass E-Mails aufgrund einer fehlenden Verschlüsselung nicht verarbeitet werden. Der Verursacher hat auf Basis der eingegangenen E-Mail den Absender per E-Mail über das weitere Vorgehen zu informieren und einen Ansprechpartner hierzu anzugeben. Diese Antwort dient zeitgleich auch als Eingangsbestätigung der Information.

Hinweis: Die Informationsmeldung vom Empfänger an den Verursacher (Sender) erfolgt einmalig auf Basis einer exemplarisch ausgewählten E-Mail.

Weiteres Vorgehen:

Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.

8 Quellen

[1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, Bundesamt für Informationssicherheit, 03.07.2025.

[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.

[3] Bilanzkreisvertrag Strom über die Führung von Bilanzkreisen;
in der jeweils gültigen Version

[4] BDEW AS4-Profil; in der jeweils aktuellen Version;
www.edi-energy.de; aktuell gültige Dokumente

[5] Rollenmodell für die Marktkommunikation im deutschen Energiemarkt
in der jeweils gültigen Version
https://www.bdew.de/service/anwendungshilfen/rollenmodell-fuer-die-marktkommunikation-im-deutschen-energiemarkt/

[6] Prozessbeschreibung Fahrplanmanagement;
in der jeweils aktuellen Version

[7] Certificate Policy der Smart Meter PKI; Bundesamt für Informationssicherheit, 25.01.2023

9 Änderungshistorie

Tabelle 9-1: Änderungshistorie

Lfd. Nr.	Ort	Fehlerkorrektur / Änderungen		Grund der Anpassung
		Bisher	**Änderung**	
1.	Deckblatt	Version 2.3 Veröffentlichungsdatum 01.04.2026 Anzuwenden ab: 01.10.2026	Version 2.4 Veröffentlichungsdatum 01.10.2026 Anzuwenden ab: 01.04.2027	
2.	Kapitel 4.3 Ziffer 2	In diesem Fall kann die Kommunikation per signierter und verschlüsselter E-Mail abgewickelt werden. Dieser Lösungsansatz stellt sicher, dass auch in den teilweise sehr zeitkritischen Situationen des Fahrplanabgleichs, welche möglicherweise große Auswirkungen auf das Netz oder Marktpartner haben können, die Kommunikation sehr kurzfristig wieder aufgenommen werden kann. • Möchte ein BKV mit einem ÜNB auf die Notfallkommunikation wechseln, so hat dies durch einen Anruf vom BKV beim ÜNB zu erfolgen. Der ÜNB ist berechtigt, eine schriftliche Begründung per E-Mail zu verlangen.	In diesem Fall kann die Kommunikation per signierter und verschlüsselter E-Mail abgewickelt werden. Dieser Lösungsansatz stellt sicher, dass auch in teilweise sehr zeitkritischen Situationen des Fahrplanabgleichs, die Kommunikation kurzfristig weitergeführt werden kann. I. Aktivierung durch den BKV: • Möchte ein BKV mit einem ÜNB auf die Notfallkommunikation wechseln, kann er dazu einen Fahrplan oder einen SRQ per signierter und verschlüsselter E-Mail an den ÜNB senden. Die Absenderadresse muss dabei der für die Notfallkommunikation hinterlegten E-Mail-Adresse aus Anlage 2 des Bilanzkreisvertrags entsprechen. Kann der ÜNB den Anhang der E-Mail fehlerfrei verarbeiten, aktiviert der ÜNB für den im Fahrplan oder SRQ genannten Bilanzkreis zusätzlich den E-Mail-Ausgangsweg. Der ÜNB ist berechtigt, eine schriftliche Begründung per E-Mail zu verlangen. • Die E-Mail Notfallkommunikation bleibt aktiv, bis der ÜNB einen Fahrplan oder SRQ via AS4 für diesen Bilanzkreis vom BKV erhält und fehlerfrei verarbeiten kann.	Neue Funktion: Automatisiertes Ein- und Ausschalten der E-Mail Notfallkommunikation
3.	Kapitel 4.3 Ziffer 3	Um den Zeitbereich der E-Mail basierten Notfallkommunikation möglichst kurz zu halten, ist der von der Störung betroffene Kommunikationspartner verpflichtet, unverzüglich mit der Störungsbehebung zu beginnen. Besteht für einen BKV die Notfallkommunikation für mehr als drei Tage am Stück, ist in jedem Fall unaufgefordert eine schriftliche Begründung des BKV zu den betroffenen Marktpartner-IDs und EICs sowie zur bisherigen Fehleranalyse per E-Mail verpflichtend an den ÜNB zu senden.	Um den Zeitbereich der E-Mail basierten Notfallkommunikation möglichst kurz zu halten, ist der von der Störung betroffene Kommunikationspartner verpflichtet, unverzüglich mit der Störungsbehebung zu beginnen. Besteht die Notfallkommunikation für mehr als drei Tage am Stück, ist in jedem Fall unaufgefordert eine schriftliche Begründung per Mail an die betroffenen Kommunikationspartner zu senden, mit Informationen zur bisherigen Fehleranalyse, sowie	Neue Funktion: Automatisiertes Ein- und Ausschalten der E-Mail Notfallkommunikation

Tabelle 9-1: Änderungshistorie

Lfd. Nr.	Ort	Fehlerkorrektur / Änderungen		Grund der Anpassung
		Bisher	**Änderung**	
			eine Abschätzung der voraussichtlichen Dauer der Störungsbehebung.	
4.	Kapitel 4.3.2	4.3.2 End to End Test (FPM BKV <> FPM ÜNB) Zusätzlich besteht für einen Marktpartner die Möglichkeit die gesamte Kommunikation, von seinem IT System bis zum ÜNB FPM System, und zurück, zu testen. Dazu müssen die Stammdaten der Marktpartner in den Systemen hinterlegt sein. Dazu kann der Marktpartner eine Status Request Nachricht an den ÜNB senden. Das FPM System des ÜNB antwortet auf diesen Status Request wie in der „Prozessbe-schreibung zur Fahrplanabwicklung in Deutschland“ beschrieben. Dieser Test ist sowohl im Rahmen der AS4 Kommunikation, als auch über die E-Mail Notfall Kommunikation möglich. Im Rahmen eines End to End Tests der AS4 Kommunikation ist dazu eine AS4 Nachricht mit der Action Einstellung „action“ und dem Service „FP“ zu senden. Als Payload ist ein Status Request einzufügen. Ebenso müssen die Part Property Angaben korrekt gefüllt sein.		Das Kapitel wird gestrichen, da diese Art der Testmöglichkeit nicht mehr benötigt wird.
5.	Kapitel 6.1	Die Zertifikate müssen die Anforderungen nach Kapitel 4.1.2 aus der BSI TR 03116-4 [1] mit folgenden Ausnahmen und Ergänzungen erfüllen.	Die Zertifikate müssen die Anforderungen nach Kapitel **6.1.1** aus der BSI TR 03116-4 [1] mit folgenden Ausnahmen und Ergänzungen erfüllen.	Redaktionelle Änderung: Anpassung an die neue Kapitelstruktur der BSI TR 03116-4
6.	Kapitel 6.1.1	Es gelten die Bedingungen des Kapitels 6.1.1 Zertifizierungsstellen/Vertrauensanker aus [1] mit folgender Ergänzung:	Es gelten die Bedingungen des Kapitels 6.1.2 Zertifizierungsstellen/Vertrauensanker aus [1] mit folgender Ergänzung:	Redaktionelle Änderung: Anpassung an die neue Kapitelstruktur der BSI TR 03116-4
7.	Fußnote 5	Sinngemäß den Kapiteln 4.6 Weitere Vorgaben und 4.8 Übergangsregelungen aus [1] entnommen.	Sinngemäß dem ersten Spiegelstrich aus Kapitel 4.6 Weitere Vorgaben aus [1] entnommen.	Redaktionelle Änderung: Anpassung an die neue Kapitelstruktur der BSI TR 03116-4