Regelungen zum sicheren Austausch im Fahrplanprozess

Version:	2.0
Veröffentlichungsdatum:	01.04.2023
Anzuwenden ab:	01.10.2023
Autor:	AG FPM
Dokumentstatus	Konsultationsfassung

Inhaltsverzeichnis

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 des Übertragungsweges E-Mail via SMTP und AS4, 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“ 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
- Textdatei „Filenotvalid“ / „Wartephase“

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 Bekanntmachen beim Informationsempfänger

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

Für den Austausch der Zertifikate wird eine Kontaktaufnahme zwischen dem ÜNB und dem BKV vorausgesetzt.

Spätestens 10 Werktage vor dem erstmaligen Versand einer Fahrplandatei durch einen BKV müssen die Zertifikate zwischen beiden Parteien ausgetauscht sein.

Spätestens drei Werktage nach dem Austausch der Kommunikationsdaten müssen beide Parteien die Zertifikate gegenseitig ausgetauscht und die Zertifikate des jeweils anderen

Marktpartners in allen ihren, an der Fahrplankommunikation beteiligten, Systemen eingetragen haben.

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 [6]).

Prozessbeteiligte:	BKV, ÜNB
Objekte:	Bilanzkreis
Gebiete:	Regelzone

2.2 Übertragungsweg E-Mail

Die E-Mail-Adressen für den Datenaustausch per E-Mail werden in Anlage 2 des Bilanzkreisvertrages festgelegt. Die E-Mail-Zertifikate sind als gzip-komprimierter Anhang per E-Mail mit dem Ansprechpartner „Zertifikate für Fahrplan-Datenaustausch“ aus Anlage 2 des Bilanzkreisvertrages [4] auszutauschen.
Alternativ hierzu kann eine URL versendet werden, die direkt auf das herunterzuladende Zertifikat verweist.

2.3 Übertragungsweg AS4

Die Kommunikationsadressen für den Datenaustausch per AS4-Nachricht werden in Anlage 2 des Bilanzkreisvertrages festgelegt.
Das AS4-Zertifikat ist als gzip-komprimierter Anhang per E-Mail mit dem Ansprechpartner „Zertifikate für Fahrplan-Datenaustausch“ aus Anlage 2 des Bilanzkreisvertrages [4] auszutauschen.
Alternativ hierzu kann eine URL versendet werden, die direkt auf das herunterzuladende Zertifikat verweist.

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

Der BKV muss ein AS4 Zertifikat angeben, das seine bdew Marktpartner ID in der bdew Rolle „BKV“ enthält.

2.3.1 Initialer Austausch der Kommunikationsparameter

Der Austausch der Kommunikationsparameter erfolgt nach erstmaliger Kontaktaufnahme per E-Mail wie in Kapitel 2.3 beschrieben.

2.3.2 Aktualisierung der Kommunikationsparameter

Eine Aktualisierung von Kommunikationsparametern ist wie folgt bekannt zu machen:

Aktualisierte E-Mail-Zertifikate oder AS4-Zertifikate

Neue Zertifikate, sog. Nachfolgezertifikate, werden folgendermaßen bekannt gemacht:

Alle Marktpartner sind verpflichtet, über Aktualisierungen ihrer Zertifikate für die E-Mail-Kommunikation bzw. für die AS4-Kommunikation per E-Mail zu informieren 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.

3 Umstellung von der E-Mail-Kommunikation auf eine AS4-Kommunikation

Für die Übertragung der prozessrelevanten Dateien kommt der Übertragungsweg E-Mail via SMTP zum Einsatz. Der Übertragungsweg soll auf AS4 per Webservice umgestellt werden. Der Wechsel vom Übertragungsweg E-Mail via SMTP (kurz „E-Mail“) auf den Übertragungsweg AS4 per Webservice (kurz „AS4“) wird nachfolgend beschrieben.

Der Übertragungsweg für den Datenaustausch im Fahrplanprozess wird 3 Monate nach Abschluss der AS4 Umstellung in der MAKO [1] von E-Mail auf AS4 umgestellt. Der Übertragungsweg E-Mail ist ab diesen Datum nur noch für eine Notfall-Kommunikation verwendbar.

Basis für die Umstellung der Kommunikationsart ist die Festlegung BK6-22-282 der Bundesnetzagentur und die darauf basierenden Dokumente des BDEW.

3.1 Umstellungsprozess

Die Umstellung auf die AS4 Kommunikation startet 3 Monate nach Abschluss der AS4 Umstellung in der MAKO mit einem Parallelbetrieb in dem ÜNB die Marktteilnehmer nach und nach auffordern, die Kommunikation ihrer produktiven Systeme von einer E-Mail-Kommunikation auf eine AS4 Kommunikation umstellen. Erhält ein BKV eine solche Aufforderung, ist der Übertragungsweg entsprechend den dort genannten Fristen zwingend auf AS4 umzustellen.

Ohne eine solche Aufforderung ist eine Umstellung des Übertragungsweges nicht erlaubt.

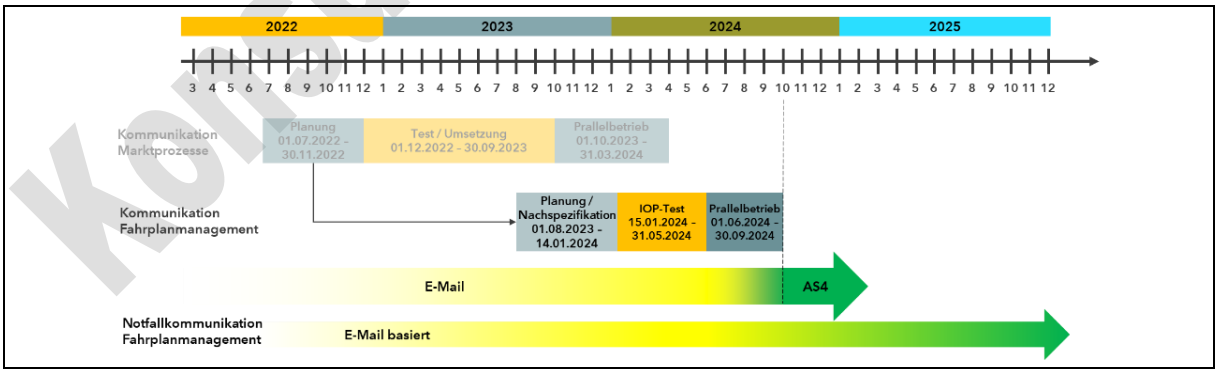

Abbildung 3-1: Umstellungsprozess E-Mail-Kommunikation auf AS4-Kommunikation
Die Datumsangaben im Bild entsprechen dem Planungsstand 31.12.2022

[1] Sollte sich die Einführung der As4 Kommunikation in der MAKO verzögern, so verschiebt sich der Einführungszeitpunkt der AS4 Kommunikation im Fahrplanprozess entsprechend.

4 Kommunikationsregeln

4.1 Übertragungsweg E-Mail

4.1.1 Allgemeines

1. Der Datenaustausch im Fahrplanprozess kann längstens 6 Monate nach Abschluss der AS4 Umstellung in der MAKO über eine signierte und verschlüsselte E-Mail-Kommunikation abgewickelt werden.
2. Für den Austausch von Fahrplandaten zwischen ÜNB und BKV kann der BKV bis zu zwei E-Mail-Adressen verwenden.
   Diese sind sowohl im regulären Prozess, als auch bei einer technischen Störung (Kapitel 4.1.2) im Falle der Notfall-Kommunikation zu nutzen.
3. Es ist zulässig, für mehrere BKV die gleiche E-Mail-Adresse zu verwenden. Dies kann insbesondere bei Dienstleistern der Fall sein.
4. Verwendet der Sender eine andere E-Mail-Adresse als die vereinbarten E-Mail-Adressen, so wird der Empfänger diesen Fahrplandatenaustausch nicht verarbeiten.
   Sie gilt dementsprechend als nicht zugestellt und es erfolgt keine Rückmeldung an den Sender. Die sich daraus ergebenden Konsequenzen hat der Versender der E-Mail zu tragen.
5. Die Verantwortung, dem Sender ein gültiges Zertifikat für die Verschlüsselung bereit zu stellen liegt beim Empfänger (siehe Kapitel 5.1.5).
6. Die Verantwortung, dem Empfänger ein gültiges Zertifikat für die Signaturprüfung bereit zu stellen liegt beim Sender (siehe Kapitel 5.1.5).

4.1.2 Notfall-Kommunikation

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

1. Die verwendeten E-Mail-Adressen für den Fahrplanaustausch im Normalprozess werden ebenfalls für die Notfall-Kommunikation herangezogen.
2. 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 in seinen Systemen keine Fahrpläne per signierter und verschlüsselter E-Mail versenden bzw. empfangen.

3. In diesem Fall kann die Kommunikation unsigniert und unverschlüsselt abgewickelt werden.

   Dieser Lösungsansatz stellt sicher, dass auch in den teilweise extrem zeitkritischen Situationen des Fahrplanabgleichs, welche möglicherweise große Auswirkungen auf das Netz oder Marktteilnehmer haben, die Kommunikation sehr kurzfristig wieder fortgeführt werden kann.

   - Möchte ein BKV mit einem ÜNB auf die Notfall-Kommunikation wechseln, so hat dies durch einen telefonischen Anruf vom BKV an den ÜNB zu erfolgen.
   - Für den Fall, dass ein ÜNB mit allen BKV in seiner Regelzone auf die Notfall-Kommunikation 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.

4. Um den Zeitbereich der unsignierten und unverschlüsselten Kommunikation möglichst kurz zu halten, ist der von der Störung betroffene Kommunikationspartner verpflichtet, unverzüglich mit der Störungsbehebung zu beginnen.
5. Probleme, die auf Grund nicht ausgetauschter oder nicht erneuerter bzw. abgelaufener Zertifikate entstehen, gelten nicht als technische Störung.

4.2 Übertragungsweg AS4

4.2.1 Allgemeines

1. Der Datenaustausch im Fahrplanprozess muss spätestens 6 Monate nach Abschluss der AS4 Umstellung in der MAKO über eine signierte und verschlüsselte AS4-Kommunikation abgewickelt werden.
2. Für den Austausch von Fahrplandaten zwischen ÜNB und BKV muss der BKV genau eine AS4 Kommunikationsadresse benennen.
3. Für die AS4-Kommunikation sind die im Kapitel 6 genannten Regeln für den Datenaustausch im Fahrplanprozess anzuwenden.
4. Verwendet der Sender eine andere bdew Marktpartner ID als zuvor vereinbart, so gilt die Nachricht dementsprechend als nicht zugestellt. Die sich daraus ergebenden Konsequenzen hat der Versender Nachricht zu tragen.
5. Die Verantwortung, dem Sender ein gültiges Zertifikat für die Verschlüsselung bereit zu stellen liegt beim Empfänger (siehe Kapitel 6.1.2 ff.).

6. Die Verantwortung, dem Empfänger ein gültiges Zertifikat für die Signaturprüfung bereit zu stellen liegt beim Sender (siehe Kapitel 6.1.2 ff.).

4.2.2 Notfall-Kommunikation

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 Notfall-Kommunikation kann bei technischen Störungen auf Seiten des BKV sowie auf Seiten des ÜNB zum Einsatz kommen. Die Notfall-Kommunikation 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 Notfall-Kommunikation anzugeben.
    - Die E-Mail-Adresse für die Notfall-Kommunikation ist in der Anlage 2 des BK-Vertrages [2] zu benennen und aktuell zu halten.
    - Die Kommunikationspartner sind verpflichtet, die für die Notfall-Kommunikation notwendigen Sicherheitszertifikate auszutauschen und aktuell zu halten. Für den Austausch der Zertifikate für die Notfall-Kommunikation gilt der gleiche Prozess wie im Falle der „normalen“ Kommunikation, also Kapitel 2.3.
2. In diesem Fall kann die Kommunikation per signierter und verschlüsselter E-Mail abgewickelt werden. Dieser Lösungsansatz stellt sicher, dass auch in den teilweise extrem zeitkritischen Situationen des Fahrplanabgleichs, welche möglicherweise große Auswirkungen auf das Netz oder Marktteilnehmer haben, die Kommunikation sehr kurzfristig wieder fortgeführt werden kann.
    - Möchte ein BKV mit einem ÜNB auf die Notfall-Kommunikation wechseln, so hat dies durch einen telefonischen Anruf vom BKV an den ÜNB zu erfolgen.
    - Für den Fall, dass ein ÜNB mit allen BKV in seiner Regelzone auf die Notfall-Kommunikation 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.

3. Um den Zeitbereich der E-Mail basierten Notfall-Kommunikation möglichst kurz zu halten, ist der von der Störung betroffene Kommunikationspartner verpflichtet, unverzüglich mit der Störungsbehebung zu beginnen.
4. Probleme, die auf Grund nicht ausgetauschter oder nicht erneuerter bzw. abgelaufener Zertifikate entstehen, gelten nicht als technische Störung.

4.2.3 Stammdaten für die Notfall-Kommunikation

Die E-Mail-Adresse für die Notfall-Kommunikation ist in der Anlage 2 des Bilanzkreisvertrages [2] zu benennen und aktuell zu halten. Es gelten hierfür folgende Regeln:

- Die Kommunikationspartner sind verpflichtet, die für die Notfall-Kommunikation notwendigen Sicherheitszertifikate auszutauschen und aktuell zu halten. Das auszutauschende Zertifikat ist vom Marktpartner als gzip-komprimierter Anhang an den in Anlage 2 des Bilanzkreisvertrages [2] genannten Zertifikatsansprechpartner 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.
- Die Zertifikate müssen den Vorgaben aus Kapitel 5 entsprechen.

5 Signatur und Verschlüsselung Übertragungsweg E-Mail

Die Zertifikate müssen die nachfolgenden Anforderungen nach Kapitel 4.1.2 aus der BSI TR 03116-4 [1] mit folgenden Ausnahmen und Ergänzungen erfüllen.

5.1 Signatur und Verschlüsselung von E-Mails

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

5.1.1 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 6.1.1 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.

5.1.2 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 5.1.3 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.[4]

    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“.

[4] Es wird eine zusätzliche Kennzeichnung bei Pseudonymen („PN“) im Feld „CN“ empfohlen (Beispiel: „pseudonym:PN“).

5.1.3 Algorithmen und Schlüssellängen für S/MIME

Es sind folgende Algorithmen und Schlüssel mit den genannten Schlüssellängen zu verwenden [5]:

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 CBC oder AES-192 CBC oder AES-256 CBC (gemäß IETF RFC 3565)
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.[6]

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

[6] Sinngemäß den Kapiteln 4.6 Weitere Vorgaben und 4.8 Übergangsregelungen aus [1] entnommen.

5.1.4 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 5.1.3 konkretisiert werden.

5.1.5 Zertifikatswechsel und Sperrlisten

1. Spätestens 10 Werktage, bevor ein Zertifikat abläuft, muss der Inhaber dieses Zertifikats das Nachfolgezertifikat zur Verfügung gestellt haben (vgl. Kapitel 5.3). 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.

5.2 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.

5.2.1 E-Mail-Adresse

1. Die für den Austausch von Fahrplandaten zwischen zwei Marktpartnern festgelegten E-Mail-Adressen sind 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 non-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.

5.2.2 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 aus dem Dokument „Prozessbeschreibung Fahrplananmeldung in Deutschland“.
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.[7]

5.2.3 E-Mail-Body

1. Es dürfen keine Informationen, die zur weiteren Verarbeitung notwendig sind, außerhalb der eigentlichen Übertragungsdatei in der E-Mail (d. h. im E-Mail-Body) enthalten sein. Beim Nachrichtenempfänger wird ausschließlich der Inhalt der angehängten Fahrplanübertragungsdatei 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.

[7] gzip ist plattformunabhängig

5.2.4 E-Mail-Betreff

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

Zur Namenskonvention des Dateinamens siehe Kapitel 5.2.2 Abs. 4 (E-Mail-Anhang).

5.3 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 Übertragungsdateien 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 7.1 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, das 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, weil die Signatur bei der Übertragung beschädigt wurde oder kann die E-Mail deswegen nicht entschlüsselt werden, so ist dies in Bezug auf die Markt-kommunikation gleichzusetzen, als ob die angefügte Übertragungsdatei nicht beim E-Mail-Empfänger angekommen wäre, d.h., als wäre eine derartige E-Mail nie versendet worden. Wird auf die Übertragungsdatei vom Empfänger eine Acknowledgement-Nachricht gesendet, kann der Sender der Übertragungsdatei davon ausgehen, dass die Prüfung der Signatur und die Entschlüsselung der Übertragungsdatei erfolgreich waren.
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 die angefügte Übertragungsdatei (insbesondere bezüglich der Fristen) vom Empfänger so zu behandeln, als hätte das Problem beim Empfänger nicht bestanden.

6 Übertragungsweg AS4

Als Übertragungsweg wird das AS4-Protokoll basierend auf dem AS4-Profil des BDEW [5] verwendet.

6.1 Zertifikate und PKI

Die Kommunikation wird durch Verwendung der Smart Metering PKI (SM-PKI) des BSI abgesichert. (siehe [8]) Die Vorgaben der Certificate Policy (CP) der SM-PKI müssen eingehalten werden.

6.1.1 Vertrauensdiensteanbieter

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

6.1.2 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.

6.1.3 Zertifikatswechsel

1. Spätestens 10 Werktage, bevor Zertifikate ungültig werden, muss der Inhaber dieser Zertifikate die Nachfolgezertifikate zur Verfügung gestellt haben (vgl. Kapitel 2 und Kapitel 6.5).
   Somit entsteht ein Überlappungszeitraum von mindestens 10 Werktagen, in dem noch die bisherigen und die neuen Zertifikate gleichzeitig gültig sind.
2. Innerhalb dieses Überlappungszeitraums kann 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. Erhält der Sender einer AS4-Nachricht ein neues Zertifikat mit dem darin enthaltenen öffentlichen Schlüssel zum Verschlüsseln von Übertragungsdateien, so darf er diesen sofort nutzen. Der Empfänger ist mindestens im Besitz des zugehörigen privaten Schlüssels und kann mit diesem die Übertragungsdatei entschlüsseln.
5. Ein neues Zertifikat, mit zugehörigem 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.
6. 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.

6.1.4 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. Jeder Marktpartner ist verpflichtet, die Gültigkeit der genutzten Zertifikate seiner Marktpartner anhand von Sperrinformationen in Form von Sperrlisten zu prüfen, wobei die verwendeten Sperrinformationen nicht älter als 24 Stunden sein dürfen.
2. Ist eine CRL über die in den Zertifikaten veröffentlichten certificate revocation list distribution point (CRL-DP) von einer CA über 3 Tage nicht abrufbar, oder diese ungültig ist, ist der ausstellenden CA und aller darunter gelisteten Zertifikate bis zur Veröffentlichung einer aktuellen CRL zu misstrauen. Die konkreten, möglichen Konsequenzen sind Kapitel 7.2 zu entnehmen.

6.2 Regelungen für den Austausch von Metainformationen

Für den Austausch von Fahrplandateien in der Marktkommunikation werden die Felder innerhalb des Elements „PartProperties“ entsprechend der Tabellen 6-1 und 6-2 gefüllt.
(Siehe Seite: 24)

Für die Datei aus dem Fahrplandatenaustausch gilt die Namenskonvention aus dem Dokument „Prozessbeschreibung Fahrplananmeldung in Deutschland“.

6.3 Services des AS 4 Profil

6.3.1 Testservice

Vor der erstmaligen Nutzung des AS4-Webservice zur Übertragung von Nachrichtendateien soll mittels des Testservice die grundsätzliche Verfügbarkeit und der Verbindungsaufbau zum Ziel des Webservice Aufrufs getestet werden.

6.3.2 Austausch von Nachrichtendateien

Für den Datenaustausch im Rahmen der Marktprozesse wird die folgende Kombination von Service und Action verwendet.

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

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

Andere Services, welche im AS4 Profil beschrieben sind, sind nicht zulässig.

6.4 Response-Codes

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

6.5 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 6.1 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 Übertragungsdateien 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 und muss es an alle seine Marktkommunikationspartner verteilen.
2. Sollte dem 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 7.2

die Verarbeitung der empfangenen Daten von Marktpartner A so lange abgelehnt werden, bis Marktpartner B ein entsprechendes Zertifikat verwendet.

3. Sollte dem Marktpartner A kein Zertifikat vom Marktpartner B zur Verfügung gestellt werden, das 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 bei der Übertragung beschädigt wurde oder kann die E-Mail deswegen nicht entschlüsselt werden, so ist dies in Bezug auf die Marktkommunikation gleichzusetzen, als ob die angefügte Übertragungsdatei nicht beim Empfänger angekommen wäre.
    Wird auf die Übertragungsdatei vom Empfänger eine ACKNOWLEDGEMENT-Nachricht gesendet, kann der Sender der Übertragungsdatei davon ausgehen, dass die Prüfung der Signatur und die Entschlüsselung der Übertragungsdatei erfolgreich waren.

    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 E-Mail zu prüfen, bzw. diese zu entschlüsseln (z. B. aufgrund technischer Probleme). In diesem Fall ist die angefügte Übertragungsdatei (insbesondere bezüglich der Fristen) vom Empfänger so zu behandeln, als hätte das Problem beim Empfänger nicht bestanden.

Tabelle 6-1: Part Properties für das Datenformat ESS 2.3

	Schedule Message	ACK	Confirmation Report	Anomaly Report	Status Request
BDEWDocumentType:	Message type	Nicht genutzt	Message Type	Nicht genutzt	Message Type
BDEWFulfillmentDate:	Schedule time interval	Schedule time interval	Schedule time interval	Schedule time interval	Schedule time interval
BDEWDocumentNo:	Message Version	ReceivingMessage Version	Confirmed Message Version	Last accepted Schedule Message: Message Version	Nicht genutzt
BDEWSubjectPartyID:	SenderID	SenderID	SenderID	SenderID	SenderID
BDEWSubjectPartyRole	SenderRole	SenderRole	SenderRole	SenderRole	SenderRole

Tabelle 6-2: Part Properties für das Datenformat IEC / CIM

	Schedule Message	ACK	Confirmation Report	Anomaly Report	Status Request
BDEWDocumentType:	type	Nicht genutzt	type	Nicht genutzt	type
BDEWFulfillmentDate:	schedule_Time_Period.timeInterval	schedule_Time_Period.timeInterval	schedule_Time_Period.timeInterval	schedule_Time_Period.timeInterval	schedule_Time_Period.timeInterval
BDEWDocumentNo:	revisionNumber	Received_MarketDocument revisionNumber	confirmed_MarketDocument.revisionNumber	Last accepted Schedule Message: revision number	Nicht genutzt
BDEWSubjectPartyID:	subject_MarketParticipant.mRID	sender_MarketParticipant.mRID	sender_MarketParticipant.mRID	sender_MarketParticipant.mRID	sender_MarketParticipant.mRID
BDEWSubjectPartyRole	subject_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type	sender_MarketParticipant.marketRole.type

7 Konsequenzen bei Nicht-Einhaltung dieser Vorgaben

7.1 Beim Übertragungsweg E-Mail

7.1.1 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.

7.1.2 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 Übertragungsdatei kompromittiert sein könnte.

Verfahrensweise:

Der Empfänger ist berechtigt, die Verarbeitung der betreffenden Übertragungsdatei zu ver-

weigern. 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 Übertragungsdateien 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.

7.1.3 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 Übertragungsdatei 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 Übertragungsdateien 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.

7.1.4 Verstoßvariante 4

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

Verfahrensweise:

Der Empfänger ist berechtigt, die Verarbeitung der betreffenden Übertragungsdatei 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 Übertragungsdateien 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 Übertragungsdatei.

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.

7.1.5 Verstoßvariante 5

Die Zertifikate wurden zwischen Sender und Empfänger korrekt ausgetauscht, aber der Sender ist auf Grund aktueller technischer Probleme nicht in der Lage, eine signierte und verschlüsselte Kommunikation korrekt durchzuführen.

Verfahrensweise:

Die in dieser Mail gesendeten Übertragungsdateien werden nicht automatisch verarbeitet. Die Konsequenzen dieser Nichtverarbeitung sind vom Sender zu tragen.

Der Sender (Verursacher) hat den Empfänger zu kontaktieren und mit ihm zu klären, ob in diesem Fehlerfall die Kommunikation im Rahmen einer bilateralen Abstimmung erfolgen kann. In diesem Fall kann der Fahrplanaustausch zwischen ÜNB und BKV gemäß Kapitel 4.1.2 abgewickelt werden.

7.2 Beim Übertragungsweg AS4

7.2.1 Verstoßvariante 1

Der Sender hat vom Empfänger kein gültiges Zertifikat zum Verschlüsseln von Übertragungsdateien zur Verfügung gestellt bekommen.
Somit kann der Sender die Übertragungsdatei 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 Übertragungsdatei,

- 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 Übertragungsdatei kompromittiert sein könnte.

Verfahrensweise:

Der Empfänger ist berechtigt, die Verarbeitung der betreffenden Übertragungsdatei zu verweigern. Beim Übertragungsweg AS4 wird automatisch mit einer negativen NRR die Annahme verweigert und der Absender erhält über die synchrone negative NRRMeldung eine

Rückmeldung per AS4 über einen nicht erfolgreichen Versand. Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen.

7.2.3 Verstoßvariante 3

Der Empfänger erhält eine verschlüsselte Übertragungsdatei, 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 Übertragungsdatei nicht verarbeiten.

Verfahrensweise:
Der Empfänger ist nicht in der Lage, die Übertragungsdatei zu entschlüsseln und daher berechtigt, die Verarbeitung der Übertragungsdatei zu verweigern. Beim Übertragungsweg AS4 wird automatisch mit einer negativen NRR die Annahme verweigert und der Absender erhält über die synchrone negative NRR-Meldung eine Rückmeldung per AS4 über einen nicht erfolgreichen Versand. Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen.

7.2.4 Verstoßvariante 4

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

Verfahrensweise:
Der Empfänger ist berechtigt, die Verarbeitung der betreffenden Übertragungsdatei zu verweigern. Beim Übertragungsweg AS4 wird automatisch mit einer negativen NRR die Annahme verweigert und der Absender erhält über die synchrone negative NRR-Meldung eine Rückmeldung per AS4 über einen nicht erfolgreichen Versand. Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen.

7.2.5 Verstoßvariante 5

Die Zertifikate wurden zwischen Sender und Empfänger korrekt ausgetauscht, aber der Sender ist auf Grund aktueller technischer Probleme nicht in der Lage, eine signierte und verschlüsselte Kommunikation korrekt durchzuführen.

Verfahrensweise:
Die in dieser Mail gesendeten Übertragungsdateien werden nicht automatisch verarbeitet.
Die Konsequenzen dieser Nichtverarbeitung sind vom Sender zu tragen.

Der Sender (Verursacher) hat den Empfänger zu kontaktieren und mit ihm zu klären, ob in diesem Fehlerfall die Kommunikation im Rahmen einer bilateralen Abstimmung erfolgen kann. In diesem Fall kann der Fahrplanaustausch zwischen ÜNB und BKV gemäß Kapitel 4.2.2 abgewickelt werden.

8 Quellen

[1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, Bundesamt für Informationssicherheit, 24.01.2022.

[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] EDI@Energy - Allgemeine Festlegungen; Allgemeine Festlegungen zu den EDIFACT-Nachrichten;
www.edi-energy.de; aktuell gültige Dokumente

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

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

[6] 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/

[7] Prozessbeschreibung Fahrplanmanagement;
in der jeweils aktuellen Version

[8] Certificate Policy der Smart Meter PKI; Bundesamt für Informationssicherheit,
TT.MM.JJJJ

9 Änderungshistorie

Es gibt noch keine Änderungshistorie, da es sich um ein neu erstelltes Dokument handelt.