Regelungen zum sicheren Austausch im Fahrplanprozess

Version:	1.0
Veröffentlichungsdatum:	01.04.2019
Anzuwenden ab:	01.10.2019
Autor:	AG FPM

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, 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.

Das Grundprinzip des sicheren Fahrplandatenaustausches ist im folgenden Bild skizziert.

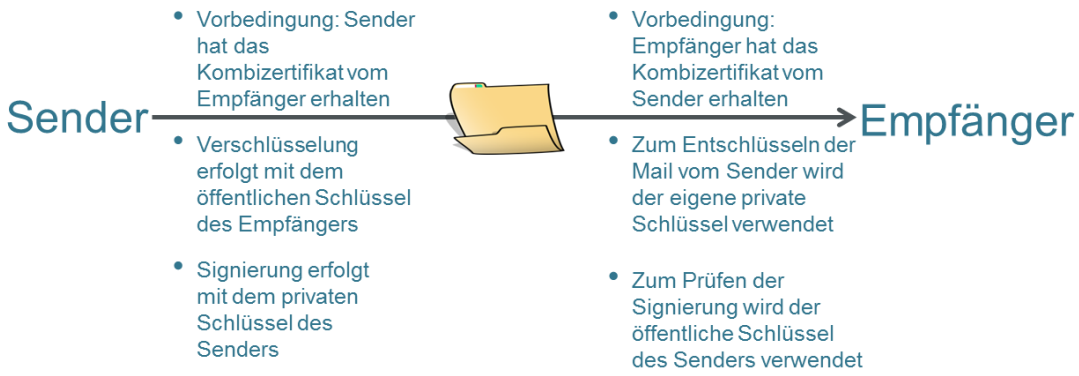

Abbildung 1: Unverbindliche vereinfachte Darstellung des Prozesses zur Signierung und Verschlüsselung.

2 Bekanntmachen beim Informationsempfänger

Um beim Datenaustausch eine größtmögliche Automatisierung zu erreichen, müssen sich die Marktpartner vor dem erstmaligen Datenversand über die E-Mail-Adressen für den Datenaustausch inkl. der zu verwendenden Zertifikate verständigen.

Die E-Mail-Adressen für den Datenaustausch werden in Anlage 2 des Bilanzkreisvertrages festgelegt.

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.

3 Übertragungswege

Für die Übertragung der prozessrelevanten Dateien kommt der Übertragungsweg E-Mail via SMTP zum Einsatz.

Die Einführung des sicheren Datenaustausches erfolgt in zwei Stufen.

1. Stufe:
   Der Datenaustausch ist nur zu signieren. Eine Verschlüsselung findet nicht statt.
   Die Umsetzungsfristen sind gemäß Festlegung der Bundesnetzagentur definiert.

2. Stufe:
   Der Datenaustausch ist zu signieren und zu verschlüsseln.
   Die Umsetzungsfristen sind gemäß Festlegung der Bundesnetzagentur definiert.

4 Kommunikationsregeln

4.1 Allgemeines

1) 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 4.2) zur unsignierten und unverschlüsselten Übermittlung zu nutzen.
2) Es ist möglich, die gleiche E-Mail-Adresse und zugehöriges Zertifikat zu verwenden, die auch im Datenaustausch in den klassischen Marktprozessen gemäß den „Regelungen zum sicheren Austausch von EDIFACT-Übertragungsdateien“ der EDI@Energy genutzt werden.
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 Verantwortlichkeit, dem Sender ein gültiges Zertifikat für die Verschlüsselung bereit zu stellen liegt beim Empfänger (siehe Kapitel 5.5.4).
6) Die Verantwortlichkeit, dem Empfänger ein gültiges Zertifikat für die Signaturprüfung bereit zu stellen liegt beim Sender (siehe Kapitel 5.5.4).

4.2 Störungsbedingte Kommunikation

Die in diesem Abschnitt aufgeführten Regeln gelten ausschließlich im Falle technischer Störungen im Bereich des Fahrplandatenaustausches. D. h. einer der Kommunikationspartner kann auf Grund einer technischen Störung in seinen Systemen keine signierten (1. Stufe) bzw. keine signierten und verschlüsselten (2. Stufe) E-Mails versenden bzw. empfangen.

In diesem Fall kann im Rahmen einer bilateralen Abstimmung zwischen ÜNB und BKV entschieden werden, die Kommunikation unsigniert und unverschlüsselt abzuwickeln.
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. Dazu sind Aktivitäten auf Seiten der ÜNB und BKV nötig.

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.

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

5 Regelungen für den Austausch via E-Mail

5.1 E-Mail-Adresse

1) Es muss sich um eine personenneutrale, funktionsbezogene E-Mail-Adresse handeln (bspw. ohne Vor- und Nachnamen).
2) 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.
3) 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 verwendet werden kann nur der Adressteil Fahrplan@Marktpartner.de. Wird die Phrase „Datenaustausch Fahrplan" (Zusatzinformation) mitgeschickt, wird sie nicht zur Auswertung herangezogen werden.
4) Die E-Mail-Adresse darf nicht case-sensitiv interpretiert werden. D. h. im folgenden Beispiel sind Fahrplan@Markt**p**artner.de und Fahrplan@Markt**P**artner.de identisch.

5.2 E-Mail-Anhang

1) In einer E-Mail darf immer nur eine Datei des Fahrplandatenaustausches enthalten sein und es dürfen keine weiteren Anhänge enthalten sein.
   Mitgesendete Geschäftskorrespondenz bzw. Textbestandteile der E-Mail werden nicht berücksichtigt.
2) Zur möglichen Komprimierung des Fahrplandatenaustausches ist ausschließlich gzip-Komprimierung zu verwenden.[1]
3) Für die Datei aus dem Fahrplandatenaustausch gilt die Namenskonvention aus dem Dokument „Prozessbeschreibung Fahrplananmeldung in Deutschland".
4) Der Anhang ist nicht separat zu verschlüsseln, da dies bereits durch S/MIME erfolgt (2. Stufe).
5) Es ist eine Base64 Kodierung zu verwenden.

[1] gzip ist plattformunabhängig

5.3 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 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, dass er Bilder oder Unternehmenslogos enthalten darf.

5.4 E-Mail Betreff

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

5.5 Signatur und Verschlüsselung von E-Mails

Jede E-Mail, mit der der Fahrplandatenaustausch erfolgt, ist im Standardfall zu signieren (1. Stufe) bzw. zu signieren und zu verschlüsseln (2. Stufe):

1) Der Datenaustausch ist geschäftsprozessunspezifisch zu betreiben, d.h. es müssen alle E-Mails im Rahmen des Fahrplandatenaustausches von einem Absender an einen Empfänger signiert (1. Stufe) bzw. signiert und verschlüsselt (2. Stufe) werden.
2) Das Signieren (1. Stufe) bzw. Signieren und Verschlüsseln (2. Stufe) von E-Mails ist ausschließlich nach dem S/MIME-Standard gestattet. Es muss mindestens die Version 3.2 (IETF RFC 5751, Veröffentlichungsjahr 2010) verwendet werden.[2]
3) Jeder Marktpartner muss für jede von ihm genutzte E-Mail-Adresse jeweils genau ein Zertifikat (genauer den dazugehörigen privaten Schlüssel) zur Signaturerzeugung verwenden.

   Für die 2. Stufe gilt zudem:
   Zur Entschlüsselung der an seine E-Mail-Adresse von den jeweils anderen Marktpartnern verschlüsselt gesendeten E-Mail wird der gleiche private Schlüssel genutzt.

   Umgekehrt müssen Zertifikate der Marktpartner (eines je E-Mail-Adresse) sowohl zur Signaturprüfung als auch zur Verschlüsselung (2.Stufe) verwendet werden.
   Auf diese Weise muss je vom Marktpartner für die Kommunikation verwendeter E-Mail-Adresse nur ein sogenanntes „Kombizertifikat“ mit fortgeschrittener Signatur gepflegt werden.

[2] Sinngemäß dem Kapitel 3.1 Versionen aus [1] entnommen

5.5.1 Zertifizierungsstellen

Das Zertifikat muss von einer Zertifizierungsstelle (engl. Certification Authority = CA) ausgestellt sein, die Zertifikate diskriminierungsfrei für Marktpartner der deutschen Energiewirtschaft anbietet. Es darf kein sogenanntes selbstausgestelltes Zertifikat verwendet werden.

Die CA, von der das Zertifikat ausgestellt ist, muss den nachfolgenden Anforderungen genügen:[3]

1) Die CA verfügt über einen Rückrufservice, über den Zertifikate widerrufen werden können. Dazu führt sie eine Zertifikatsperrliste (englisch certificate revocation list, CRL), welche öffentlich zugängig ist.
2) Darüber hinaus sollten insbesondere die folgenden Kriterien berücksichtigt werden:
   a) Die IT-Sicherheit des CA-Betriebs ist durch ein Audit / eine Zertifizierung nach einem anerkannten Audit / Zertifizierungs-Standard geprüft. Es wird eine Zertifizierung nach BSI TR-03145, Secure Certification Authority operation empfohlen.
   b) Der Registrierungsservice, einschließlich an Dienstleister (Registrare) ausgelagerter Services, erfolgt auf einem hohen Sicherheitsniveau.
   c) Die Vertrauenswürdigkeit des Betreibers und des Betriebs, auch unter Berücksichtigung von Eingriffsrechten Dritter, ist gegeben.

[3] Sinngemäß dem Kapitel 5.1.1 Zertifizierungsstellen/Vertrauensanker aus [1] entnommen.

5.5.2 Zertifikate: Parameter und Anforderungen

Die End-Zertifikate müssen die nachfolgenden Anforderungen erfüllen[4]:

1) Das Zertifikat muss von einer CA ausgestellt sein, die den unter Kapitel 5.5.1 genannten Anforderungen genügt.
2) Alle bis zum 31.12.2018 ausgestellte Zertifikate sind entweder mit dem Signaturverfahren RSASSA-PKCS1-v1_5 (Signaturalgorithmen sha-256RSA oder sha-512RSA) oder RSASSA-PSS zu signieren. Diese Zertifikate sind bis zur maximalen Zertifikatsgültigkeit (maximal 3 Jahre) in der Marktkommunikation verwendbar.
3) Alle ab dem 01.01.2019 neu ausgestellten Zertifikate müssen mit RSASSA-PSS signiert sein.
4) Jedes Zertifikat muss Informationen für eine Rückrufprüfung enthalten, d. h. einen `CRLDistributionPoint`, unter dem jederzeit aktuelle CRL zur Verfügung stehen.
5) Die Gültigkeit des Zertifikats darf maximal 3 Jahre betragen.
6) Das Zertifikat muss mindestens die Verwendungszwecke Schlüsselverschlüsselung und digitale Signatur im Feld `KeyUsage` enthalten.
7) Das Zertifikat muss die Anforderungen an eine fortgeschrittene elektronische Signatur oder eines fortgeschrittenen elektronischen Siegels erfüllen.[5]
8) 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 (1. Stufe) bzw. die signierten und verschlüsselten (2. Stufe) E-Mails versendet und empfangen werden.
9) Der Parameter im Feld "Alternativer Antragstellername" mit dem Wert "RFC822-Name=" muss mit der Kommunikationsadresse (Angabe der E-Mail-Adresse) befüllt werden.
   Auf diese Weise muss genau eine Kommunikationsadresse angegeben werden. Mehrere Kommunikationsadressen für dasselbe Zertifikat sind nicht zulässig.
10) Das Zertifikatsnamensfeld "CN" hat prozessual in der elektronischen Kommunikation keine funktionale Bedeutung und wird nicht ausgewertet. Es wird empfohlen, das Feld mit einem Pseudonym zu belegen. Die Zuordnung eines Zertifikats zu einer natürlichen oder juristischen Person erfolgt ausschließlich über die CA und muss nicht aus dem Zertifikat selbst erkenntlich sein.[6]

[4] Sinngemäß dem Kapitel 5.1.2 Zertifikate aus [1] entnommen.

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

Für den Austausch der öffentlichen Zertifikate gilt die Codierung:

1) DER-codiert-binär X.509 (mit der Datei-Extension: .cer) oder
2) Base-64-codiert X.509 (mit der Datei-Extension: .cer).

5.5.3 Algorithmen und Schlüsselspezifikationen für S/MIME

Es sind folgende Algorithmen und Schlüssel mit den genannten Schlüssellängen zu verwenden[7]:

SIGNATUR:

Hashfunktion (Hash algorithm)	SHA-256 oder SHA-512 (gemäß IETF RFC 5754).
Signaturverfahren (Signature algorithm)	RSA Schlüssellänge mindestens 2048 Bit RSASSA-PSS (gemäß IETF RFC 4056)

VERSCHLÜSSELUNG (2. STUFE):

Inhaltsverschlüsselung (Content encryption)	AES-128 CBC oder AES-192 CBC (gemäß IETF RFC 3565) bzw. AES-256 CBC
Schlüsselverschlüsselung (Key encryption)	RSA Schlüssellänge mindestens 2048 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.[8]

[7] Sinngemäß dem Kapitel 3.2 bis 3.4. aus [1] entnommen.

[8] Sinngemäß dem Kapitel 3.6. Weitere Vorgaben und 3.8. Übergangsregelungen aus [1] entnommen.

5.5.4 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). Somit entsteht ein Überlappungszeitraum von mindestens 10 Werktagen, in dem noch das alte und auch schon das neue Zertifikat gültig sind.
2) Innerhalb dieses Überlappungszeitraums kann bei allen versendenden Marktpartnern die Umstellung vom bisher genutzten auf das neue Zertifikat erfolgen.
   a) Der Zertifikatsinhaber darf das neue Zertifikat frühestens drei Werktage nachdem er es seinen Marktpartnern zur Verfügung gestellt hat zur Signierung verwenden.
   b) Für die 2. Stufe gilt:
   Jeder Marktpartner kann eigenständig den Zeitpunkt innerhalb des Überlappungszeitraums festlegen, ab dem er das neue Zertifikat verwendet, um E-Mails an den Zertifikatsinhaber verschlüsseln.
3) Im Überlappungszeitraum müssen alle empfangenden Marktpartner in der Lage sein, sowohl mit dem bisher genutzten, als auch mit dem neuen Zertifikat signierte (1. Stufe) bzw. signierte und verschlüsselte (2. Stufe) E-Mails zu verarbeiten, wobei für den Zertifikatsinhaber die vorgenannte Einschränkung beim Versand gilt.
4) Ab dem Zeitpunkt, zu dem das alte Zertifikat ungültig wird, darf mit diesem nicht mehr signiert 1. Stufe) bzw. signiert und verschlüsselt (2. Stufe) 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. Dabei ist der Punkt 7) aus Kapitel 6 zu beachten.

6 Organisatorische Regelungen zum Umgang mit Zertifikaten

Es gelten die nachfolgenden organisatorischen Regelungen:

1) Für Stufe 2: Ein Marktpartner A kann nur dann eine E-Mail verschlüsselt an einen Marktpartner B versenden, wenn Marktpartner B ein gültiges Zertifikat zur Verfügung stellt, das den unter Kapitel 5.5 genannten Anforderungen genügt.

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 der Fahrplandatenaustausch durch Marktpartner A so lange abgelehnt werden, bis Marktpartner B ein entsprechendes Zertifikat zur Verfügung gestellt hat.

3) Spätestens 10 Werktage bevor ein Zertifikat abläuft, muss der Inhaber dieses Zertifikats das Nachfolgezertifikat an den jeweiligen Ansprechpartner übermitteln.

4) Durch die Übermittlung des Zertifikats (als gzip-komprimierte Datei) bzw. des Links zum direkten Download des benötigten Zertifikats gilt das Zertifikat als ausgetauscht.

5) Scheitert die Signaturprüfung, weil die Signatur bei der Übertragung beschädigt wurde, oder kann die E-Mail deswegen nicht entschlüsselt werden (2. Stufe), so ist dies in Bezug auf die Kommunikation gleichzusetzen, als ob der Fahrplandatenaustausch nicht beim E-Mail Empfänger angekommen wäre.

6) Die voranstehende Regel findet keine Anwendung für den Fall, dass der Empfänger nicht in der Lage war, die Signatur einer fehlerfrei signierten (1. Stufe) bzw. fehlerfrei signierten und verschlüsselten (2. Stufe) E-Mail zu prüfen, bzw. diese zu entschlüsseln (2. Stufe) (z. B. aufgrund technischer Probleme).
   In diesem Fall ist der Fahrplandatenaustausch (insbesondere bezüglich der Fristen) vom Empfänger so zu behandeln, als hätte das Problem beim Empfänger nicht bestanden.

7) Sobald ein Zertifikat gesperrt oder ungültig ist und noch kein gültiges Nachfolgezertifikat vorliegt, darf kein Fahrplandatenaustausch mehr verarbeitet werden, der von der zugehörigen E-Mail-Adresse stammt und mit dem gesperrten oder ungültigen Zertifikat signiert ist.
   Der Marktpartner, dessen Zertifikat gesperrt oder ungültig ist, hat unverzüglich ein neues Zertifikat zu beschaffen und muss es an die Kommunikationspartner verteilen.

7 Konsequenzen bei Nicht-Einhaltung dieser Vorgaben

7.1 Fehlerfall 1

Die Zertifikate wurden zwischen Sender und Empfänger korrekt ausgetauscht, aber der Sender ist auf Grund aktueller technischer Probleme nicht in der Lage, eine signierte (1. Stufe) bzw. signierte und verschlüsselte (2. Stufe) Kommunikation korrekt durchzuführen.

Verfahrensweise:

- Die gesendeten Fahrplandaten in dieser Mail 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 zwischen ÜNB und BKV gemäß Kapitel 4.2 abgewickelt werden kann.

7.2 Fehlerfall 2

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

Verfahrensweise:

- Der Empfänger ist nicht verpflichtet die Fahrplandaten in dieser Mail zu verarbeiten.
- Die Konsequenzen einer ausbleibenden Kommunikation sind von demjenigen Marktpartner zu tragen, der die Verantwortung hat, das Zertifikat zur Verfügung zu stellen (Sender).
- Der Empfänger hat den Sender (Verursacher) mindestens einmal per E-Mail über die Tatsache zu informieren, dass die Kommunikation aufgrund des fehlenden gültigen Zertifikats nicht durchgeführt wird.
  Der Verursacher (Sender) hat auf Basis der eingegangen E-Mail den Empfänger per E-Mail über das weitere Vorgehen zu informieren und einen Ansprechpartner hierzu anzugeben. Diese Antwort dient zeitgleich auch als Eingangsbestätigung der Information.
- Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.

7.3 Fehlerfall 3

Dieser Fehlerfall kann erst mit Umsetzung der 2. Stufe auftreten.

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 nicht verpflichtet die Kommunikation durchzuführen.
- 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 eingegangen 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.
- 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, vom 23. April 2018.

[2] EDI@Energy - Allgemeine Festlegungen; Allgemeine Festlegungen zu den EDIFACT-Nachrichten; Version 4.5; vom 01. Oktober 2018

9 Abkürzungsverzeichnis

Eine Erklärung der verwendeten Abkürzungen findet sich in [2].

10 Änderungshistorie

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