EDI@Energy – Regelungen zum Übertragungsweg

Regelungen zum sicheren Austausch von EDIFACT- und Fahrplan-Übertragungsdateien

Konsolidierte Lesefassung mit Fehlerkorrekturen Stand: 30. September 2020

Version:	1.3
Ursprüngliches Publikationsdatum:	01.04.2020
Anzuwenden ab:	01.10.2020
Autor:	BDEW

Inhaltsverzeichnis

1 Einführung

1.1 Regelungsumfang

Dieses Dokument regelt die Sicherheits- und Schutzmechanismen, die im Rahmen des elektronischen Datenaustauschs zwischen den Marktpartnern der deutschen Energiewirtschaft für die Übertragungswege[1] AS2 und E-Mail via SMTP in der Marktkommunikation und im Fahrplanaustauschprozess Strom einzuhalten sind. Es wird keine Aussage über die im Zielmodell geltenden Anforderungen an die Übertragungswege getroffen.

Die nachfolgenden Regeln finden Anwendung auf alle von der BNetzA festgelegten Marktprozesse[2] die per EDIFACT abgewickelt werden, wie beispielsweise GPKE, MPES, GeLi Gas, GaBi Gas, MaBiS, WiM und KoV[3] als auch den Datenaustausch im Rahmen der Fahrplanprozesse Strom[4]. Die Fahrplanprozesse umfassen den Fahrplandatenaustausch zwischen den BKV und ÜNB, wobei die folgenden Datenaustauschprozesse gemäß dem Dokument „Prozessbeschreibung Fahrplananmeldung in Deutschland“[4] davon betroffen sind:

- 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. In diesem Dokument wird der Austausch von qualifiziert signierten EDIFACT-Übertragungsdateien nicht betrachtet.[5]

Gemäß BNetzA-Beschluss[6] sind grundsätzlich die kryptographischen Vorgaben der BSI TR 03116-4 (Stand: 31. Januar 2019) anzuwenden und einzuhalten. Die zu nutzenden Parameter und hiervon anzuwendenden Abweichungen sind in diesem Dokument beschrieben.

Aktuell gelten somit die nachfolgenden Regelungen zum Übertragungsweg, welche auch die damit verbundenen organisatorischen Regelungen für die deutsche Energiewirtschaft enthalten.

---

[1] Mit „Übertragungsweg“ wird in diesem Dokument das bezeichnet, was auch als „Kommunikationskanal“, „Kommunikationsweg“ „Transportprotokoll“ oder „Übertragungsprotokoll“ bezeichnet wird.

[2] Vgl. BK6-18-032 (Tenorziffer 6) [6] und Beschluss (BK7-16-142) [2].

[3] Die nationalen Regelungen zum Übertragungsweg gelten bei der KoV nur für die rein nationalen Geschäftsprozesse nach KoV Anlage 3 vollumfänglich. Für KoV Anlage 1 und 2 (entry-exit-System) nur für die Prozesse nach Anwendungshilfe „Prozessbeschreibung zur Kapazitätsabrechnung an Ausspeisepunkten zu Letztverbrauchern“.

[4] Vgl. BK6-18-061 [8].

[5] Vgl. Bundesnetzagentur, Mitteilung Nr. 3 zu den Datenformaten zur Abwicklung der Marktkommunikation [7].

[6] Vgl. BK6-18-032 [6] und BK7-16-142 [2], Beschluss zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende.

1.2 Struktur des Dokuments

Soweit nicht anders gekennzeichnet, gelten die Regelungen sowohl für den Datenaustausch im Rahmen der Fahrplanprozesse als auch für den Datenaustausch aller von der BNetzA festgelegten Marktprozesse, die per EDIFACT abgewickelt werden.

Sollten die Regeln für diese beiden Anwendungsgebiete unterschiedlich sein, ist das entsprechende Kapitel in zwei Unterkapitel aufgeteilt:

- „Fahrplan“ kennzeichnet den Teil, der für den Datenaustausch im Rahmen der Fahrplanprozesse gilt,
- „Marktprozesse“ kennzeichnet den Teil, der für den Datenaustausch aller von der BNetzA festgelegten Marktprozesse gilt, die per EDIFACT abgewickelt werden.

Bei nur kleinen Unterschieden zwischen den Prozessen sind diese im Text explizit vermerkt.

2 Bekanntmachen beim Informationsempfänger

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

2.1 Fahrplan

Wie in Kapitel 3.1 festgelegt, kommt für den Datenaustausch im Rahmen der Fahrplanprozesse nur E-Mail via SMPT zum Einsatz. 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 (gemäß GPKE/GeLi Gas-Kalender[7]) 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.

2.2 Marktprozesse

Wie in Kapitel 3.2 festgelegt, kann der Datenaustausch aller von der BNetzA festgelegten Marktprozesse, die per EDIFACT abgewickelt werden, per E-Mail via SMPT oder AS2 erfolgen.

Der Austausch der Kommunikationsparameter erfolgt nach erstmaliger Kontaktaufnahme per Telefon oder E-Mail.

Spätestens drei Werktage (gemäß GPKE/GeLi Gas-Kalender[7]) nach der erstmaligen Kontaktaufnahme eines Marktpartners müssen die oben genannten Daten zwischen diesen beiden Parteien ausgetauscht sein. Einen Werktag nach Austausch der Kommunikationsdaten müssen beide Parteien die Daten des jeweils anderen Marktpartners in allen ihren an der Marktkommunikation

[7] Hinweis: Die Werktagsdefinitionen in GPKE und GeLi Gas sind identisch.

beteiligten Systemen eingetragen bzw. zur Verfügung gestellt haben, so dass alle Voraussetzungen für die Durchführung des elektronischen Datenaustauschs erfüllt sind.

EDIFACT-Übertragungsdateien, die aufgrund einer vom Empfänger verschuldeten, verspäteten Einrichtung des Übertragungswegs abgelehnt werden, gelten als fristgerecht zugestellt. Der Empfänger ist in diesem Fall verpflichtet, diese entsprechend des ursprünglichen Empfangsdatums zu prozessieren[8]. Diese Regelung gilt ausschließlich für fehlerfreie EDIFACT-Übertragungsdateien.

Der Übertragungsweg zwischen zwei Marktpartnern ist mindestens für drei Jahre ab dem Tage nach dem letzten Datenaustausch (zwischen diesen beiden Marktpartnern) aufrecht zu halten. Ändert sich bei einem Marktpartner der Übertragungsweg, so ist er verpflichtet, all seine Marktpartner mit denen er in den letzten drei Jahren EDIFACT-Übertragungsdateien ausgetauscht hat, über die Änderung zu informieren. Die Information erfolgt rechtzeitig mindestens 10 Werktage vor Umstellung. Die Adressierung erfolgt wenigstens an die Adressdaten der Marktpartner, mit denen er in den letzten drei Jahren EDIFACT-Dateien ausgetauscht hat, welche zum Zeitpunkt der Informationsübermittlung in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegt sind.

Der Umstellungszeitpunkt ist auf einen Werktag gemäß GPKE/GeLi Gas-Kalender zu terminieren. Empfohlen wird eine Uhrzeit zu Büroarbeitszeiten festzulegen, um Kontrolle und im Fehlerfall Kontaktaufnahme und Fehlerbehebung zeitnah und preiswert durchführen zu können.

Eine Aufrechterhaltung des Übertragungswegs bedeutet nicht, dass eine E-Mail-Adresse, die für den Datenaustausch verwendet und durch eine andere E-Mail-Adresse ersetzt wurde, drei Jahre lang nicht gelöscht werden darf. Wurde ein derartiges E-Mail-Postfach zu einer E-Mail-Adresse „stillgelegt", und alle Marktpartner entsprechend der voranstehenden Regel über die neue zu nutzende E-Mail-Adresse informiert, so kann die bisher genutzte E-Mail-Adresse gelöscht werden. Diese Regelung gilt sinngemäß auch für AS2.

Zur Kontaktaufnahme mit einem Marktpartner dienen die in der DVGW-Codenummerndatenbank bzw. BDEW-Codenummerndatenbank veröffentlichte E-Mail-Adresse, Telefon- und Faxnummer.

3 Übertragungswege

3.1 Fahrplan

Für die Übertragung der prozessrelevanten Dateien kommt der Übertragungsweg E-Mail via SMTP (gemäß Kapitel 5) zum Einsatz.

3.2 Marktprozesse

Für die Übertragung von Übertragungsdateien kommen die Übertragungswege AS2 oder E-Mail via SMTP zum Einsatz.

Wenn keine Einigung auf einen Übertragungsweg möglich ist, ist auf jeden Fall E-Mail (gemäß Kapitel 5) anzubieten.

[8] Im Regelfall, in dem ein Übertragungsweg eingerichtet ist, ist das Zugangsdatum das für die Fristen relevante Datum.

4 Kommunikationsregeln

4.1 Fahrplan

4.1.1 Allgemeines

- 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) zur unsignierten und unverschlüsselten Übermittlung zu nutzen.
- Für den BKV ist es möglich, dieselbe E-Mail-Adresse mit dem zugehörigen Zertifikat zu verwenden, die der BKV auch im Datenaustausch in den von der BNetzA festgelegten Marktprozessen verwendet.
- Es ist zulässig, dass mehrere BKV dieselbe E-Mail-Adresse verwenden. Dies kann insbesondere bei Dienstleistern der Fall sein.
- Verwendet der Sender eine andere E-Mail-Adresse als vereinbart, so wird der Empfänger diesen Fahrplandatenaustausch nicht verarbeiten. Die davon betroffenen Fahrplandaten gelten somit als nicht zugestellt und es erfolgt keine Rückmeldung an den Sender. Die sich daraus ergebenden Konsequenzen hat der Sender der E-Mail zu tragen.
- Die Verantwortlichkeit, dem Sender ein gültiges Zertifikat für die Verschlüsselung bereit zu stellen, liegt beim Empfänger (siehe Kapitel 5.5.4).
- Die Verantwortlichkeit, dem Empfänger ein gültiges Zertifikat für die Signaturprüfung bereit zu stellen, liegt beim Sender (siehe Kapitel 5.5.4).

4.1.2 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 und verschlüsselten 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.

4.2 Marktprozesse

Zwischen zwei unterschiedlichen MP-ID ist genau ein Übertragungsweg zulässig. Für den Übertragungsweg kann entweder eine E-Mail-Adresse oder eine AS2-Adresse verwendet werden.

Die Grundidee der 1:1-Kommunikation ist, dass ein Marktpartner dafür zu sorgen hat, dass seine internen Organisationsstrukturen bei den anderen Marktpartnern keinen Zusatzaufwand im Rahmen der Übermittlung der EDIFACT-Übertragungsdateien generieren.

Es ist zulässig, für mehrere MP-ID die gleiche E-Mail-Adresse bzw. AS2-URL zu verwenden.

Eine EDIFACT-Übertragungsdatei, die von einer anderen E-Mail-Adresse als der vereinbarten E-Mail-Adresse versandt wird, muss vom Empfänger nicht verarbeitet[9] werden. Sie gilt dementsprechend als nicht zugestellt und es erfolgt keine Rückmeldung an den Marktpartner. Die sich daraus ergebenden Konsequenzen hat der Versender der E-Mail zu tragen.

5 Regelungen für den Austausch via E-Mail

Die in diesem Abschnitt 5 beschriebenen Regeln gelten ausschließlich für die E-Mail-Adressen, über die die EDIFACT-Übertragungsdateien bzw. Fahrplandaten ausgetauscht werden.

Die hohe Variantenvielfalt in der E-Mail-Nutzung steht einem Einsatz zur Übermittlung von EDIFACT-Übertragungsdateien bzw. Fahrplandaten entgegen. Um dennoch einen hohen Automatisierungsgrad auf Seiten des E-Mail-Empfängers zu erreichen, gelten folgende Regeln:

5.1 E-Mail-Adresse

- Die für den Austausch von EDIFACT-Übertragungsdateien bzw. Fahrplandaten zwischen zwei Marktpartnern festgelegten E-Mail-Adressen sind ausschließlich für den Austausch von EDIFACT-Übertragungsdateien bzw. Fahrplandaten zu nutzen.
- Es muss sich um eine personenneutrale, funktionsbezogene E-Mail-Adresse handeln (bspw. ohne Vor- und Nachnamen).
- Ein Marktpartner, der E-Mails mit Geschäftskorrespondenz an die für den Austausch von EDIFACT-Übertragungsdateien bzw. Fahrplandaten 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-EDIFACT Informationen bzw. non-Fahrplandaten nicht beachtet werden.
- 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.
- Bei der E-Mail-Adresse werden nur die „reinen" Adressbestandteile ausgewertet (LocalPart@Domain.TLD). Ein Anspruch auf Auswertung oder Adressierung der „Phrase" besteht nicht.

  Beispiel: „Datenaustausch Marktpartner" <Daten@Marktpartner.de>

  Zur Adressierung verwendet werden kann nur der Adressteil Daten@Marktpartner.de.

  Wird die Phrase „Datenaustausch Marktpartner" mitgeschickt, darf sie nicht zur Auswertung herangezogen werden.
- Die E-Mail-Adresse darf nicht case-sensitiv interpretiert werden. D. h. im oben genannten Beispiel sind Daten@Markt**p**artner.de und Daten@Markt**P**artner.de identisch.

[9] D. h. die E-Mail muss weder entschlüsselt, noch die Signatur geprüft, noch muss die in der E-Mail enthaltene Übertragungsdatei verarbeitet werden.

5.2 E-Mail-Anhang

- In einer E-Mail darf immer nur eine EDIFACT-Übertragungsdatei oder eine Datei des Fahrplandatenaustausches enthalten sein.
- Eine E-Mail darf keine weiteren Anhänge enthalten.
- In einer E-Mail mitgesendete Geschäftskorrespondenz bzw. Textbestandteile der E-Mail werden nicht berücksichtigt.
- Zur möglichen Komprimierung einer EDIFACT-Übertragungsdatei oder einer Datei des Fahrplandatenaustausches ist ausschließlich gzip-Komprimierung[10] zu verwenden.
- Regel zur Benennung der Übertragungsdatei
  - Für die EDIFACT-Übertragungsdatei gilt die Namenskonvention aus dem entsprechenden Kapitel des EDI@Energy-Dokuments „Allgemeine Festlegungen“.
  - Für den Fahrplandatenaustausch gilt die Namenskonvention aus dem Dokument „Prozessbeschreibung Fahrplananmeldung in Deutschland“.
- Der Anhang ist nicht separat zu verschlüsseln und auch nicht zu signieren, da dies bereits durch S/MIME erfolgt.
- Der Anhang muss Base64 kodiert sein, damit Mailserver keine Zeilenumbrüche während des Transportes einfügen.
- Der Content-Type des MIME-Parts mit dem Anhang muss Application/octet-stream sein. Ist der Anhang eine EDIFACT-Nachrichtendatei darf der Content-Type alternativ auch Application/edifact sein.

5.3 E-Mail-Body

- 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 EDIFACT-Übertragungsdatei bzw. 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.
- Einige Softwareprodukte, die in der gesamten Verarbeitungskette der Marktkommunikation 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 sein. Dies schließt die Dateiendung ein. Zur Namenskonvention des Dateinamens siehe Kapitel 5.2 (E-Mail-Anhang).

5.5 Signatur und Verschlüsselung von E-Mails

Jede E-Mail, mit der in der deutschen Energiewirtschaft eine EDIFACT-Übertragungsdatei oder eine Fahrplandatei ausgetauscht wird, ist zu signieren und zu verschlüsseln.

- Das Signieren und Verschlüsseln von E-Mails ist ausschließlich nach dem S/MIME-Standard gestattet. Es muss mindestens die Version 4.0 (IETF RFC 8551, Veröffentlichungsjahr 2019) verwendet werden.[11]

[10] gzip ist plattformunabhängig.

[11] Sinngemäß dem Kapitel 3.1 Versionen aus [1] entnommen.

- Jeder Marktpartner muss für jede von ihm genutzte E-Mail-Adresse[12] genau ein Zertifikat[13] (genauer den dazugehörigen privaten Schlüssel) zur Signaturerzeugung verwenden. Zur Entschlüsselung der an diese 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 Verschlüsselung als auch zur Signaturprüfung verwendet werden. Auf diese Weise muss für jede vom Marktpartner für die Marktkommunikation verwendete E-Mail-Adresse nur ein Zertifikat gepflegt werden, ein sogenanntes „Kombizertifikat“ mit fortgeschrittener elektronischer Signatur bzw. fortgeschrittenen elektronischen Siegel.

5.5.1 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[14] ausgestellt sein, die Zertifikate diskriminierungsfrei für Marktpartner der deutschen Energiewirtschaft anbietet. Es darf kein sogenanntes selbstausgestelltes Zertifikat sein.[13]

Die CA, von der das Zertifikat ausgestellt ist, muss den nachfolgenden Anforderungen genügen:[15]

- 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.

Darüber hinaus sollten insbesondere die folgenden Kriterien berücksichtigt werden:

- 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.
- Der Registrierungsservice, einschließlich an Dienstleister (Registrare) ausgelagerter Service, erfolgt auf einem hohen Sicherheitsniveau.
- Die Vertrauenswürdigkeit des Betreibers und des Betriebs, auch unter Berücksichtigung von Eingriffsrechten Dritter, ist gegeben.
- Der Rechtsstand, insbesondere in Bezug auf das geltende Haftungs- und Datenschutzrecht genügt den Anforderungen des Unternehmens, dass das Zertifikat beantragt.

5.5.2 Zertifikate: Parameter und Anforderungen

Die Zertifikate müssen die nachfolgenden Anforderungen erfüllen[16]:

- Das Zertifikat muss von einer CA ausgestellt sein, die den unter Kapitel 5.5.1 genannten Anforderungen genügt.
- 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.

---

[12] Ein Marktpartner kann je Marktrolle (und damit je MP-ID) ein (EDIFACT) oder zwei (Fahrplan) eigene E-Mail-Postfächer verwenden (siehe Kapitel 4).

[13] Vgl. BK6-18-032 [6] und BK7-16-142 [2], Beschluss zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende.

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

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

[16] Sinngemäß dem Kapitel 5.1.2 Zertifikate aus [1] entnommen und um BK7 [2] bis [5] bzw. BK6 [6] ergänzt.

- Alle ab dem 01.01.2019 neu ausgestellten Zertifikate müssen mit RSASSA-PSS signiert sein.
- Jedes Zertifikat muss Informationen für eine Rückrufprüfung enthalten, d. h. einen `CRLDistributionPoint`, unter dem jederzeit aktuelle CRL zur Verfügung stehen.
- Die Gültigkeit des Zertifikats darf maximal 3 Jahre betragen.
- Das Zertifikat muss mindestens die Verwendungszwecke Schlüsselverschlüsselung und digitale Signatur im Feld `KeyUsage` enthalten.
- Für die verschiedenen, für die Marktkommunikation nötigen Anwendungszwecke „Signatur“ und „Verschlüsselung“ ist dasselbe Schlüsselpaar zu generieren und dementsprechend ein sogenanntes Kombizertifikat auszustellen und zu verwenden.
- Das Zertifikat muss die Anforderungen an eine fortgeschrittene elektronische Signatur oder eines fortgeschrittenen elektronischen Siegels erfüllen.[17]
- 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.
- 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" hat prozessual in der elektronischen Marktkommunikation keine funktionale Bedeutung und wird nicht ausgewertet. Es wird empfohlen, das Feld mit einem Pseudonym zu belegen.[18] Die Zuordnung eines Zertifikats zu einer natürlichen oder juristischen Person erfolgt ausschließlich über die CA und muss nicht aus dem Zertifikat selbst erkenntlich sein.[19]

Für den Austausch der öffentlichen Zertifikate gilt die Codierung:

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

5.5.3 Algorithmen und Schlüssellängen für S/MIME

Es sind folgende Algorithmen und Schlüssel mit den genannten Schlüssellängen zu verwenden[20]:

- Signatur:
  - Hashfunktion (Hash algorithm): SHA-256 oder SHA-512 (gemäß IETF RFC 5754).
  - Signaturverfahren (Signature algorithm): RSASSA-PSS (gemäß IETF RFC 4056).

    Schlüssellänge der verwendeten RSA-Schlüssel mindestens 2048 Bit.

[17] 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“.

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

[19] Vgl. BNetzA-Klarstellung [7].

[20] Sinngemäß den Kapiteln 3.2 bis 3.4 aus [1] entnommen.

- Verschlüsselung:
  - Inhaltsverschlüsselung (Content encryption): AES-128 CBC, AES-192 CBC oder AES-256 CBC (gemäß IETF RFC 3565).
  - Schlüsselverschlüsselung (Key encryption): RSAES-OAEP (gemäß IETF RFC 8017). Die Schlüsselverschlüsselung hat Hashfunktionen als Parameter. Hierbei sind SHA-256 oder SHA-512 zu verwenden.
    Schlüssellänge der verwendeten RSA-Schlüssel mindestens 2048 Bit.

In den Implementierungen der RSA-Verschlüsselung sind geeignete Gegenmaßnahmen gegen Chosen-Ciphertext-Angriffe vorzusehen.[21]

5.5.4 Zertifikatswechsel und Sperrlisten

Spätestens 10 Werktage bevor ein Zertifikat abläuft muss der Inhaber dieses Zertifikats das Nachfolgezertifikat zur Verfügung gestellt haben (vgl. Kapitel 7). Somit entsteht ein Überlappungszeitintervall von mindestens 10 Werktagen, in dem noch das alte und auch schon das neue Zertifikat gültig sind.

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.

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.

Ab dem Zeitpunkt, zu dem das alte Zertifikat ungültig wird, darf mit diesem weder signiert noch verschlüsselt werden.

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.

Jeder Marktpartner ist verpflichtet, mindestens einmal täglich zu prüfen, ob keines der Zertifikate seiner Marktpartner gesperrt wurde, in dem er alle von ihm verwendeten Zertifikate gegen die Sperrlisten (CRL) prüft. Die Sperrliste ist öffentlich mindestens per http zugänglich zu machen.

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.

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.

[21] Sinngemäß den Kapiteln 3.6 Weitere Vorgaben und 3.8 Übergangsregelungen aus [1] entnommen.

6 Regelungen für den Austausch via AS2

Erfolgt der Austausch der EDIFACT-Dateien via AS2 so ist der AS2-Steckbrief Version 2 zur standardisierten Mitteilung der eigenen AS2-Adressparameter zu verwenden. Dieses Dokument enthält den AS2-Steckbrief auch als Word-Vorlage.

AS2 wird nicht verwendet im Rahmen des Fahrplandatenaustausches.

AS2 ist abstrakt über RFC 4130 standardisiert. Dieses Kapitel nimmt Erweiterungen und zusätzliche Algorithmen zur RFC 4130 auf, die den aktuellen Sicherheitsanforderungen genügen.

Nachfolgend werden die zu verwendenden Algorithmen und Parameter aufgeführt, die für den deutschen Energiemarkt verpflichtend anzuwenden sind.

6.1 AS2-Adresse

Als AS2-Adresse wird in diesem Dokument die Kombination AS2-ID mit AS2-URL bezeichnet.

Hinweis: Technisch muss die AS2-ID bei jedem AS2-Adapter eineindeutig sein.

6.1.1 AS2-ID

Die Marktpartner-ID ist gleichzeitig die AS2-ID. Die AS2-ID darf keinerlei Präfixe oder Suffixe enthalten.

Hinweis: Unter der AS2-ID erfolgt die Zuordnung des AS2-Zertifikats für die S/MIME-Technik.

6.1.2 AS2-URL

Die URL zum AS2-Adapter muss als vollständig qualifizierter Name der Domäne angegeben sein (statt IP-Adresse). Die URL darf nicht case-sensitiv interpretiert werden.

6.2 Anforderungen an AS2-Zertifikate

Das Zertifikat darf ausschließlich für die AS2-Kommunikation genutzt werden.

Das AS2-Zertifikat dient der Signatur und Verschlüsselung.

Technisch ist es notwendig das AS2-Zertifikat einer AS2-ID zuzuordnen. Jeder AS2-URL muss mindestens ein eigenes Zertifikat zugeordnet sein. Sind einer AS2-URL mehrere AS2-IDs zugeordnet (im nachfolgenden wird die Anzahl der dieser AS2-URL zugeordneten AS2-IDs mit n angegeben), können alle AS2-IDs, die dieser AS2-URL zugeordnet sind, mit unterschiedlichen Zertifikaten oder 1 bis n identischen Zertifikaten betrieben werden.

Das AS2-Zertifikat muss den unter Kapitel 5.5 genannten Anforderungen genügen.

6.3 Algorithmen und Schlüssellängen

Siehe Kapitel 5.5.3.

6.4 Transportschicht

Es müssen feste IP-Adressen verwendet werden. Es muss http über Port 80 angeboten werden, optional kann zusätzlich https mit Standardport 443 angeboten werden.[22] Sofern https verwendet wird, muss zur Wahrung der Konformität mit der BSI TR-03116-4 mindestens TLS Version 1.2 oder höher verwendet werden.[23]

6.5 MDN (digitale Zustell-Quittung)

Für die Message Disposition Notification (MDN) gilt, dass der MDN-Modus synchron zu wählen ist (unmittelbare Zustellquittung), und die MDN signiert sein muss.

6.6 Betreff und Dateiname

Für Betreff und Dateiname ist die Namenskonvention des entsprechenden Kapitels des EDI@Energy-Dokuments „Allgemeine Festlegungen“ anzuwenden.

[22] Eine doppelte Verschlüsselung (Nachricht und Transportweg) bei HTTPS ist nicht erforderlich, da die Nachricht bereits mit S/MIME verschlüsselt ist und die Kommunikationspartner öffentlich bekannt sind. Der Einsatz von AS2 dient nicht für ein höheres Sicherheitsniveau gegenüber E-Mail mit S/MIME per SMTP, sondern für einen zuverlässigen und kostengünstigeren Transport von Massendaten bei gleichzeitig schnelleren Prozessen.

[23] Siehe Kapitel 2 Vorgaben SSL/TLS aus [1].

7 Organisatorische Regelungen zum Umgang mit 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 5.5 genannten Anforderungen genügt. Daher gelten über diese technischen Anforderungen hinaus auch die nachfolgenden organisatorischen Regelungen:

- 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 8 die Verarbeitung der empfangenen Daten von Marktpartner A so lange abgelehnt werden, bis Marktpartner B ein entsprechendes Zertifikat zur Verfügung gestellt hat.
- 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 (bzw. eine sichere AS2-Verbindung zu diesem herstellen zu können), so kann gemäß Kapitel 8 der EDIFACT- und Fahrplan-Datenaustausch durch Marktpartner A an Marktpartner B so lange unterbleiben, bis Marktpartner B ein entsprechendes Zertifikat zur Verfügung gestellt hat.
- Fahrplanprozess: Spätestens 10 Werktage bevor ein Zertifikat im Fahrplanprozess abläuft, muss der Inhaber dieses Zertifikats das Nachfolgezertifikat an den jeweiligen Ansprechpartner übermitteln.
- Marktprozesse: Spätestens 10 Werktage bevor ein Zertifikat in den Marktprozessen abläuft, muss der Inhaber dieses Zertifikats das Nachfolgezertifikat an alle seine Marktpartner, mit denen er in den letzten drei Jahren EDIFACT-Übertragungsdateien ausgetauscht hat, senden. Dafür sind die in der BDEW bzw. DVGW Codenummern-Datenbank eingetragenen E-Mail-Adressen zu verwenden, soweit keine weiteren Vereinbarungen zwischen den Marktpartnern vorliegen.
- 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.
- 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 E-Mail Empfänger angekommen wäre, d. h. als wäre eine derartige E-Mail nie versendet worden. Wird auf die Übertragungsdatei vom Empfänger eine CONTRL-(EDIFACT) Meldung oder ein Acknowledgement (Fahrplan) gesendet, kann der Sender der Übertragungsdatei davon ausgehen, dass die Prüfung der Signatur und die Entschlüsselung der Übertragungsdatei erfolgreich waren.
- 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.
- 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.
  Gilt nur für Marktprozesse: Bei Nutzung von AS2 können keine Übertragungsdateien ausgetauscht werden, wenn gesperrte oder ungültige Zertifikate eingesetzt werden.

8 Konsequenzen bei Nicht-Einhaltung dieser Vorgaben

Bei Nicht-Einhaltung der Regeln sind mit der Bundesnetzagentur die folgenden Verfahrensweisen abgestimmt:

8.1 Beim Übertragungsweg E-Mail:

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.
Fahrplan: Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.
Marktprozesse: Die Information ist mindestens an die in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional an eine z. B. über das Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden.

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 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 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 Übertragungsdatei.
Fahrplan: Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.
Marktprozesse: Die Selektion aller betroffenen Übertragungsdateien wird vom Verursacher an Hand der fehlenden CONTRL-Meldungen zusammengeführt. Die Information ist mindestens an die

in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional an eine z. B. über Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden. Die Zuordnung des Markpartners erfolgt anhand der Marktpartner-ID im Betreff der E-Mail.

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 Übertragungsdatei.
Fahrplan: Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.
Marktprozesse: Die Selektion aller betroffenen Übertragungsdateien wird vom Verursacher an Hand der fehlenden CONTRL-Meldungen zusammengeführt. Die Information ist mindestens an die in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional an eine z. B. über Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden. Die Zuordnung des Marktpartners erfolgt anhand der Marktpartner-ID im Betreff der E-Mail.

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.
Fahrplan: Diese Information ist mindestens an die im Bilanzkreisvertrag genannten Kontaktpartner für „Vertragsmanagement und allgemeine Fragen“ und den Ansprechpartner für „allgemeine technische Fragen“ zu senden.
Marktprozesse: Die Selektion aller betroffenen Übertragungsdateien wird vom Verursacher an Hand der fehlenden CONTRL-Meldungen zusammengeführt. Die Information ist mindestens an die in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional

an eine z. B. über Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden. Die Zuordnung des Markpartners erfolgt anhand der Marktpartner-ID im Betreff der E-Mail.

Verstoßvariante 5 (nur Fahrplan): 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.

8.2 Beim Übertragungsweg per AS2

Verstoßvariante 1: Der Empfänger hat dem Sender kein gültiges Zertifikat zur Verfügung gestellt. 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. Der Sender hat den Empfänger (Verursacher) mindestens einmal über die Tatsache zu informieren, dass die Kommunikation aufgrund des fehlenden gültigen Zertifikats nicht durchgeführt wird. Der Verursacher hat auf Basis der eingegangenen E-Mail den Absender über das weitere Vorgehen zu informieren und einen Ansprechpartner hierzu anzugeben. Diese Antwort dient zeitgleich auch als Eingangsbestätigung der Information.
Die Information ist mindestens an die in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional an eine z. B. über Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden.

Verstoßvariante 2: Der Empfänger erhält eine Übertragungsdatei,

- die nicht signiert ist oder
- die mit einem ungültigen Zertifikat signiert ist oder
- 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. Die Konsequenzen dieser nicht-Verarbeitung sind vom Sender zu tragen. Der Empfänger hat den Sender (Verursacher) insgesamt mindestens einmal 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 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. Die Selektion aller betroffenen

Übertragungsdateien wird vom Verursacher an Hand der fehlenden CONTRL-Meldungen zusammengeführt. Die Information ist mindestens an die in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional an eine z. B. über Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden. Die Zuordnung des Markpartners erfolgt anhand der AS2-ID.

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 Übertragungsdatei nicht entschlüsseln und verarbeiten.

Verfahrensweise: Der Empfänger ist nicht in der Lage, die Übertragungsdatei zu entschlüsseln und daher berechtigt, die Verarbeitung der Übertragungsdatei zu verweigern. Die Konsequenzen dieser nicht-Verarbeitung sind vom Sender zu tragen. Der Empfänger hat den Sender (Verursacher) insgesamt mindestens einmal über die Tatsache zu informieren, dass Übertragungsdateien nicht entschlüsselt werden können und somit nicht verarbeitet werden. Der Verursacher hat auf Basis der eingegangenen E-Mail den Absender 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. Die Selektion aller betroffenen Übertragungsdateien wird vom Verursacher an Hand der fehlenden CONTRL-Meldungen zusammengeführt.
Die Information ist mindestens an die in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional an eine z. B. über Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden. Die Zuordnung des Markpartners erfolgt anhand AS2-ID.

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 Übertragungsdatei 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 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 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. Die Selektion aller betroffenen Übertragungsdateien wird vom Verursacher an Hand der fehlenden CONTRL-Meldungen zusammengeführt.
Die Information ist mindestens an die in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional an eine z. B. über Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden. Die Zuordnung des Markpartners erfolgt anhand der AS2-ID.

9 Quellen

[1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, Bundesamt für Informationssicherheit, 31.01.2019.

[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] Mitteilung Nr. 3 (BK7-16-142), Festlegungsverfahren zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, Bundesnetzagentur, 16.05.2017.

[4] Mitteilung Nr. 7 (BK7-16-142), Festlegungsverfahren zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, Bundesnetzagentur, 12.12.2017.

[5] Mitteilung Nr. 8 (BK7-16-142), Festlegungsverfahren zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, Bundesnetzagentur, 13.04.2018.

[6] Beschluss (BK6-18-032) und Anlagen zum Beschluss (BK6-18-032), zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende (Tenorziffer 5 und Tenorziffer 6), Bundesnetzagentur, 20.12.2018.

[7] Mitteilung Nr. 3 zu den Datenformaten zur Abwicklung der Marktkommunikation: Verwendung von Zertifikaten zur Signatur bzw. Verschlüsselung der Marktkommunikation, Bundesnetzagentur, 03.04.2019.

[8] Beschluss (BK6-18-061) und Anlagen zum Beschluss (BK6-18-061) zur Genehmigung der Modalitäten für Bilanzkreisverantwortliche (Standardbilanzkreisvertrag), Bundesnetzagentur, 12.04.2019.

10 Ansprechpartner

Yassin Bendjebbour
E-Mail: yassin.bendjebbour@bdew.de
Telefon: +49 30 300 199 1526

11 Änderungshistorie

Die angegebenen Änderungen beziehen sich auf die jeweils letzte veröffentlichte Version. Zwischenversionen werden nicht veröffentlicht.

Version 1.2

Änd-ID	Ort	Fehlerkorrektur / Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
12132	Kapitel Änderungshistorie	Status der Änderungsanträge welche in der letzten Konsultationsfassung dieses Dokuments durch die BNetzA genehmigt wurden: Liegt dem Markt zur Konsultation vor	Korrekter Status der Änderungsanträge welche in der letzten Konsultationsfassung dieses Dokuments durch die BNetzA genehmigt wurden: Genehmigt.	In der Version 1.3 dieses Dokuments waren alle Änderungsanträge, die in der Konsultation angenommen wurden, fälschlicherweise im Status „Liegt dem Markt zur Konsultation vor“ veröffentlicht worden. Die Änderungsanträge hätten im Status „Genehmigt“ veröffentlicht werden müssen.	Fehler (30.09.2020)
12133	Kapitel 1.1 Regelungsumfang	Fußnote 3: Die nationalen Regelungen zum Übertragungsweg gelten bei der KoV nur für die rein nationalen Geschäftsprozesse nach KoV Anlage 3.	Fußnote 3: Die nationalen Regelungen zum Übertragungsweg gelten bei der KoV nur für die rein nationalen Geschäftsprozesse nach KoV Anlage 3 **vollumfänglich**. **Für KoV Anlage 1 und 2 (entry-exit-System) nur für die Prozesse nach Anwendungshilfe „Prozessbeschreibung zur Kapazitätsabrechnung an Ausspeisepunkten zu Letztverbrauchern“**.	Der Geltungsbereich der RzÜ wird in Fußnote 3 aktualisiert.	Fehler (30.09.2020)

12 Anhang 1: AS2-Steckbrief Version 2

Unternehmensname des Marktpartners laut Handelsregister	*<Name>*	
Marktpartner-ID und Marktrolle	*<MP-ID>*	*<Marktrolle>*
Marktpartner-ID und Marktrolle (weitere optional)	*ggf. weitere <MP-ID>*	*ggf. weitere <Marktrolle>*
Marktpartner-ID und Marktrolle (weitere optional)	*ggf. weitere <MP-ID>*	*ggf. weitere <Marktrolle>*
Marktpartner-ID und Marktrolle (weitere optional)	*ggf. weitere <MP-ID>*	*ggf. weitere <Marktrolle>*

Kontakt Marktpartner AS2

1. Ansprechpartner	
Name	*<Nachname>, <Vorname>*
Telefon	*<Telefonnummer>*
E-Mail	*<E-Mail-Adresse>*
2. Ansprechpartner	
Name	*<Nachname>, <Vorname>*
Telefon	*<Telefonnummer>*
E-Mail	*<E-Mail-Adresse>*

Kontakt Technik AS2

1. Ansprechpartner	
Name	*<Nachname>, <Vorname>*
Telefon	*<Telefonnummer>*
E-Mail	*<E-Mail-Adresse>*
2. Ansprechpartner	
Name	*<Nachname>, <Vorname>*
Telefon	*<Telefonnummer>*
E-Mail	*<E-Mail-Adresse>*
3. Ansprechpartner	
Name	*<Nachname>, <Vorname>*
Telefon	*<Telefonnummer>*
E-Mail	*<E-Mail-Adresse>*

Netzwerk	
AS2-URL	http://***xxx.com/xxx***
IP-Adresse (Firewall)	***xxx.xxx.xxx.xx***
IP Port (Firewall)	80 (Standard http)
Zusätzliche Absender-IP-Adresse (optional)	-/-

AS2-Zertifikat	
AS2-ID	Als AS2-ID ist die MP-ID zu verwenden. Für welche MP-ID das nachfolgend genannte Zertifikat verwendet wird, ergibt sich anhand der auf der vorherigen Seite genannten MI-IDs.
Öffentliche AS2-Zertifikat	-----BEGIN CERTIFICATE----- ***<String des Zertifikats>*** -----END CERTIFICATE-----

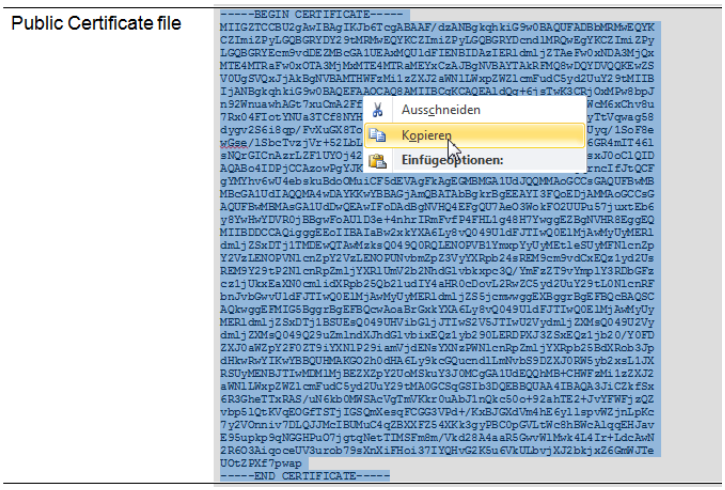
AS2-Parameter	
MDN Mode	Synchron
MDN Signed	Ja
Komprimierung	Ja
Content-Type	Binary
RSA Signaturschemata	RSASSA-PPS
Signatur-Hash-Algorithmus	SHA-256 oder SHA-512
RSA Schlüsselverschlüsselungs-Algorithmus	RSAES-OAEP
Datenverschlüsselungs-Algorithmus	AES-128 CBC, AES-192 CBC oder AES-256 CBC

Hinweis: Dieser Steckbrief ist auch als Word-Vorlage in dieses pdf-Dokument eingebettet.

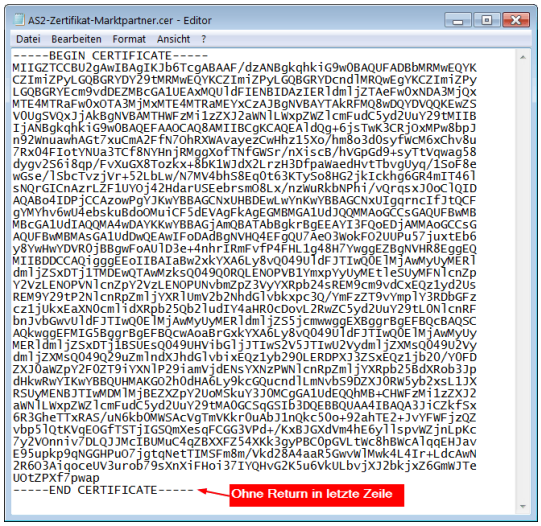
13 Anhang 2: Erzeugung eines Zertifikats (cer-Datei) aus dem AS2-Steckbrief

Nachfolgend sind die Schritte zur Erzeugung des AS2-Zertifikats aus dem im AS2-Steckbrief enthaltenen String über Screenshots dargestellt.

1) Text aus dem AS2-Steckbrief kopieren:



2) Eine neue Textdatei z. B. mit dem Windows-Editor erzeugen und dort den Text einfügen. Die letzte Zeile sollte keinen Zeilenwechsel aufweisen (CR/LF).



3) Zuletzt die Datei mit Dateityp „.cer“ abspeichern: