edi@energy.
Datenformate Strom & Gas

Konsultationsfassung

Regelungen zum Übertragungsweg

Regelungen zum sicheren Austausch von EDIFACT- und Fahrplan-Übertragungsdateien sowie Redispatch 2.0-Prozessdaten

Version:	1.5
Publikationsdatum:	30.07.2021
Anzuwenden ab:	01.04.2022
Autor:	BDEW

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument regelt die Sicherheits- und Schutzmechanismen, die im Rahmen des elektronischen Datenaustauschs für regulierten Prozesse zwischen den Marktpartnern der deutschen Energiewirtschaft für die Übertragungswege[1] AS2, E-Mail via SMTP, SFTP und REST in der Marktkommunikation, im Fahrplanaustauschprozess Strom und im Redispatch 2.0 einzuhalten sind. Es wird keine Aussage über die im Zielmodell geltenden Anforderungen an die Übertragungswege getroffen.

Gemäß BNetzA-Beschluss[2] sind grundsätzlich die kryptographischen Vorgaben der BSI TR 03116-4 (Stand: 23. Februar 2021)[3] anzuwenden und einzuhalten. Die zu nutzenden Parameter und hiervon anzuwendenden Abweichungen sind in diesem Dokument beschrieben.

1.1 Regelungsumfang

Die nachfolgenden Regeln finden Anwendung

- auf alle von der BNetzA festgelegten Marktprozesse[4] die per EDIFACT abgewickelt werden, wie beispielsweise GPKE, MPES, GeLi Gas, GaBi Gas, MaBiS, WiM, KoV[5] Redispatch 2.0,
- auf den Datenaustausch im Rahmen der Fahrplanprozesse Strom[6] und
- auf den Datenaustausch der Redispatch 2.0-Prozessdaten[7] per XML.

Die Fahrplanprozesse umfassen den Fahrplandatenaustausch zwischen den BKV und ÜNB, wobei die folgenden Datenaustauschprozesse gemäß dem Dokument „Prozessbeschreibung Fahrplananmeldung in Deutschland“[6] 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“

---

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

2 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.

3 Falls diese Version nicht mehr zum öffentlichen Download bereitsteht, so kann diese beim BSI angefragt werden.

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

5 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“.

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

7 Vgl. BK6-20-059, Anlage 2, II. Basisdatenaustausch und Abrufprozesse [9] per XML (Hinweis: Alle anderen Kapitel der Anlage 2 fallen unter „Marktprozesse“). Dies Anlage gilt jedoch nicht für Anlagen, die bereits gemäß der Genehmigung vom 20.12.2018 (Az. BK6-18-122) zur Datenlieferung verpflichtet sind [10].

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 Übertragungsdateien nicht betrachtet.[8]

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

1.2 Struktur des Dokuments

Soweit nicht anders gekennzeichnet, gelten die Regelungen sowohl für den Datenaustausch im Rahmen der Marktprozesse, Fahrplanprozesse und Redispatch 2.0-Prozessdaten. Sollten die Regeln für diese drei Anwendungsgebiete unterschiedlich sein, ist das entsprechende Kapitel in drei Unterkapitel aufgeteilt:

- **„Marktprozesse“**
  kennzeichnet den Teil, der für den Datenaustausch aller von der BNetzA festgelegten Marktprozesse gilt, die per EDIFACT abgewickelt werden.
- **„Fahrplan“**
  kennzeichnet den Teil, der für den Datenaustausch im Rahmen der Fahrplanprozesse gilt,
- **„Redispatch 2.0-Prozessdaten“**
  kennzeichnet den Teil, der für den Datenaustausch im Rahmen Redispatch 2.0 per XML gilt (RD2.0-Prozessdaten).

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 Marktprozesse

Wie in Kapitel 3.1 festgelegt, kann der Datenaustausch aller von der BNetzA festgelegten Marktprozesse, die per EDIFACT abgewickelt werden, per E-Mail via SMTP oder AS2 erfolgen.

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

Spätestens drei Werktage (gemäß GPKE/GeLi Gas-Kalender[9]) nach der erstmaligen Kontaktaufnahme eines Marktpartners müssen die oben genannten Daten zwischen diesen beiden Parteien ausgetauscht sein. Einen Werktag nach Austausch der Kommunikationsdaten müssen

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

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

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

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[10]. 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.

2.2 Fahrplan

Es gelten die in Kapitel 3.2 festgelegten Übertragungswege für den Datenaustausch im Rahmen der Fahrplanprozesse.

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

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

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

Spätestens 10 Werktage (gemäß GPKE/GeLi Gas-Kalender[9]) 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.

2.3 Redispatch 2.0-Prozessdaten

Für den Datenaustausch der RD2.0-Prozessdaten kommen AS2, E-Mail via SMTP, SFTP oder REST zum Einsatz. Weiterführende Regelungen werden in Kapitel 3.3 festgelegt.

Spätestens 10 Werktage (gemäß GPKE/GeLi Gas-Kalender[9]) vor dem erstmaligen Versand einer XML-Datei durch einen Marktpartner 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 ihren am Prozess beteiligten Systemen eingetragen haben.

3 Übertragungswege

3.1 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 6) anzubieten.

3.2 Fahrplan

Für die Übertragung der prozessrelevanten Dateien kommen die Übertragungswege E-Mail via SMTP, AS2, SFTP oder REST zum Einsatz.

Wenn keine Einigung auf einen Übertragungsweg möglich ist, ist auf jeden Fall E-Mail (gemäß Kapitel 6) anzubieten.

3.3 Redispatch 2.0-Prozessdaten

Für die Übertragung der XML-Dateien kommen die Übertragungswege AS2, E-Mail via SMTP, SFTP oder REST zum Einsatz.

Erfolgt eine Einigung auf einen der beiden Übertragungswege AS2 oder E-Mail via SMTP ist zu prüfen, ob bereits derselbe Übertragungsweg zwischen den Marktpartnern mit ihrer MP-ID für die Kommunikation der Marktprozesse existiert. Ist dies der Fall, ist dieselbe Kommunikationsadresse zu verwenden (1:1 Kommunikation).

Wenn keine Einigung auf einen Übertragungsweg möglich ist, aber bereits ein vereinbarter Übertragungsweg zwischen den Marktpartnern mit ihrer MP-ID für die Kommunikation der

Marktprozesse existiert, ist dieser zu verwenden. Andernfalls ist auf jeden Fall E-Mail (gemäß Kapitel 6) anzubieten.

Zudem steht es den Marktpartnern offen, schwarzfallsichere Übertragungswege als Redundanz zu den genannten Übertragungswegen zu vereinbaren und zu nutzen.

4 Kommunikationsregeln

4.1 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[11] 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.

4.2 Fahrplan

4.2.1 Allgemeines

- Für den Austausch von Fahrplandaten zwischen ÜNB und BKV kann der BKV bis zu zwei E-Mail-Adressen verwenden und/oder REST und/oder AS2 und/oder SFTP verwenden. Diese sind sowohl im regulären Prozess für die verschlüsselte und signierte Übermittlung als auch im Ausnahmefall bei einer technischen Störung (Kapitel 4.2.2) für die unsignierte und/oder unverschlüsselte 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 einen anderen Kommunikationsweg 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 zu tragen.

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

- Die Verantwortlichkeit, dem Sender ein gültiges Zertifikat für die Verschlüsselung bereit zu stellen, liegt beim Empfänger (siehe Kapitel 5.5).
- Die Verantwortlichkeit, dem Empfänger ein gültiges Zertifikat für die Signaturprüfung bereit zu stellen, liegt beim Sender (siehe Kapitel 5.5).

4.2.2 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 signierte und verschlüsselte Kommunikation durchführen kann.

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. Die konkreten, möglichen Konsequenzen sind Kapitel 12 zu entnehmen.

4.3 Redispatch 2.0-Prozessdaten

Für den Austausch von RD2.0-Prozessdaten zwischen zwei Marktpartnern (mit unterschiedlichen MP-ID) ist genau ein Übertragungsweg der folgenden Übertragungswege zulässig:

- E-Mail (gemäß Kapitel 6),
- AS2 (gemäß Kapitel 7),
- SFTP (gemäß Kapitel 9) oder
- REST-Webservice (gemäß Kapitel 10).

Es ist zulässig, für mehrere MP-ID die gleiche Kommunikationsadresse zu verwenden. Es ist zulässig, für eine MP-ID in unterschiedlichen Anwendungsgebieten (Marktprozesse, Fahrplandatenaustausch und RD2.0-Prozessdaten) unterschiedliche Kommunikationsadressen zu verwenden.

Eine XML-Datei, die von einer anderen als der vereinbarten Kommunikationsadresse versandt wird, muss vom Empfänger nicht verarbeitet werden. Sie gilt dementsprechend als nicht zugestellt und es erfolgt keine Rückmeldung an den Marktpartner. Die sich daraus ergebenden Konsequenzen hat der Versender der Nachricht zu tragen.

5 Signatur und Verschlüsselung

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

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

Es gelten die Bedingungen des Kapitels 5.1.1 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.

5.2 Zertifikate: Parameter und Anforderungen für S/MIME

Die Zertifikate müssen die nachfolgenden Anforderungen nach Kapitel 5.1.2 Zertifikate aus [1] mit folgenden Ausnahmen und Ergänzungen erfüllen.

In Abweichung gelten folgende Regelungen:

- Alle Zertifikate müssen Informationen für eine Rückrufprüfung enthalten, d. h. einen `CRLDistributionPoint`, unter dem jederzeit aktuelle CRLs zur Verfügung stehen.
- Eine `AuthorityInfoAccess`-*Extension* muss nicht bereitgestellt werden.
- Das Zertifikat muss von einer CA ausgestellt sein, die den unter Kapitel 5.1 genannten Anforderungen genügt.
- Die Gültigkeitsdauer der CAs ist auf eine kryptographisch vertretbare Zeit zu limitieren, die auch länger als in [1] empfohlen sein kann.
- Müssen für Signatur und Verschlüsselung dasselbe Zertifikat (Kombizertifikat) verwendet werden.[13]

Zusätzlich gelten folgende Regelungen:

- Alle Zertifikate müssen mit RSASSA-PSS signiert sein.

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

[13] Vgl. BK7 [2] bis [5] bzw. BK6 [6].

- Das Zertifikat muss die Anforderungen an eine fortgeschrittene elektronische Signatur oder eines fortgeschrittenen elektronischen Siegels erfüllen.[14]
- 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" kommt nicht zur Anwendung und wird nicht ausgewertet Es wird empfohlen, das Feld mit einem Pseudonym zu belegen.[15] Die Zuordnung eines Zertifikats zu einer natürlichen oder juristischen Person erfolgt ausschließlich über die CA und muss nicht aus dem Zertifikat selbst erkenntlich sein.[16]

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

5.3 Algorithmen und Schlüssellängen für S/MIME

Es sind folgende Algorithmen und Schlüssel mit den genannten Schlüssellängen zu verwenden[17]:

- 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.

    Ab dem 01.01.2023 muss die Schlüssellänge der verwendeten RSA-Schlüssel mindestens 3072 Bit betragen.

    Des Weiteren sind die Übergangsregelungen für Schlüssellängen weiter unten zu beachten.

[14] 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“.

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

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

[17] Auswahl aus 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). Ab dem 01.10.2024 muss AES-128 GCM verwendet werden.
• 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. Ab dem 01.01.2023 muss die Schlüssellänge der verwendeten RSA-Schlüssel mindestens 3072 Bit betragen. Des Weiteren sind die Übergangsregelungen für Schlüssellängen weiter unten zu beachten.

Die verwendete Schlüssellänge ergibt sich aus dem öffentlichen RSA-Schlüssel des Zertifikats. Es gelten folgende Übergangsregelungen für Schlüssellängen:

› Bis 31.03.2022:
Existierende Zertifikate, die eine RSA-Schlüssellänge von 2048 Bit besitzen, dürfen bis zu ihrem Auslaufdatum verwendet werden.

› Zertifikate, die bis zum 31.03.2022 neu ausgestellt bzw. erneuert werden, sollten bereits eine RSA-Schlüssellänge von mindestens 3072 Bit besitzen.

› Ab 01.04.2022:
Zertifikate die ab dem 01.04.2022 ausgestellt werden, müssen eine RSA-Schlüssellänge von mindestens 3072 Bit besitzen.

In den Implementierungen der RSA-Verschlüsselung sind geeignete Gegenmaßnahmen gegen Chosen-Ciphertext-Angriffe vorzusehen.[18]

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

Aus Sicht des Bundesamts für Sicherheit in der Informationstechnik und der Bundesnetzagentur gilt für die Algorithmen zum Signieren und Verschlüsseln zusätzlich folgendes:

Ab dem 01.01.2023 muss der Empfang von S/MIME-Nachrichten unterstützt werden, die gemäß [1] die Signatur ECDSA und für die Key Encryption ECDH verwenden. Es wird empfohlen, die Kurve BrainpoolP256r1 bei den ECC-Verfahren zu akzeptieren, um den Mindestanforderungen an die Interoperabilität aus Abschnitt 3.7 in [1] zu genügen.

Beim Versand von S/MIME-Nachrichten dürfen diese Algorithmen auch nach dem 01.01.2023 nicht verwendet werden. In einer folgenden zu konsultierenden Festlegung wird über den frühestmöglichen Verwendungszeitpunkt entschieden sowie die Verfügbarkeit der einzusetzenden Zertifikate behandelt.

5.4 S/MIME-Version

Signieren und Verschlüsseln sind ausschließlich nach dem Kapitel 3.1 aus [1] zulässigen S/MIME-Standard gestattet. Es sind dabei nur die in diesem Dokument bewerteten, beschriebenen und ausgewählten Verfahren zulässig.

5.5 Zertifikatswechsel und Sperrlisten

Spätestens 10 Werktage bevor ein Zertifikat abläuft muss der Inhaber dieses Zertifikats das Nachfolgezertifikat zur Verfügung gestellt haben (vgl. Kapitel 11). 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.

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. Die konkreten, möglichen Konsequenzen sind Kapitel 12 zu entnehmen.

6 Regelungen für den Austausch via E-Mail

Die in diesem Abschnitt 6 beschriebenen Regeln gelten ausschließlich für den Übertragungsweg E-Mail via SMTP über die Übertragungsdateien der Marktprozesse bzw. Fahrplandaten bzw. RD2.0-Prozessdaten ausgetauscht werden.

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

6.1 E-Mail-Adresse

- Die für den Austausch von EDIFACT-Übertragungsdateien bzw., Fahrplandaten bzw. RD2.0-Prozessdaten zwischen zwei Marktpartnern festgelegten E-Mail-Adressen sind ausschließlich für den Austausch von EDIFACT-Übertragungsdateien bzw. Fahrplandaten, bzw. RD2.0-Prozessdatenzu 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 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-EDIFACT Informationen bzw. non-Fahrplandaten bzw. non-RD2.0-Prozessdaten 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.

6.2 E-Mail-Anhang

› In einer E-Mail darf immer nur eine EDIFACT-Übertragungsdatei bzw. eine Datei des Fahrplandatenaustausches bzw. eine Datei der RD2.0-Prozessdaten 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 Komprimierung einer EDIFACT-Übertragungsdatei bzw. einer Datei des Fahrplandatenaustausches bzw. einer Datei der RD2.0-Prozessdaten ist ausschließlich gzip-Komprimierung[19] zulässig.

› EDIFACT-Übertragungsdateien dürfen, müssen aber nicht komprimiert werden. Dateien des Fahrplandatenaustauschs und Dateien der RD2.0-Prozessdaten müssen komprimiert werden.

› 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“.
- Für die RD2.0-Prozessdaten gilt die Namenskonvention aus dem entsprechenden Kapitel des EDI@Energy-Dokuments „Allgemeine Festlegungen“.

› 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.

6.3 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 Übertragungsdatei 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

19 gzip ist plattformunabhängig.

beachten ist. Dies bedeutet insbesondere, dass der E-Mail-Body weder in HTML codiert sein darf, noch, dass er Bilder oder Unternehmenslogos enthalten darf.

6.4 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 6.2 (E-Mail-Anhang).

6.5 Signatur und Verschlüsselung von E-Mails

Jede E-Mail, mit der in der deutschen Energiewirtschaft eine EDIFACT-Übertragungsdatei oder eine Fahrplandatei oder eine RD2.0-Prozessdatendatei ausgetauscht wird, ist zu signieren und zu verschlüsseln. Details sind Kapitel 5 zu entnehmen.

7 Regelungen für den Austausch via AS2

Erfolgt der Austausch der Übertragungsdatei via AS2 so ist der AS2-Steckbrief Version 3 zur standardisierten Mitteilung der eigenen AS2-Adressparameter zu verwenden. Dieses Dokument enthält den AS2-Steckbrief auch als Word-Vorlage.

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.

7.1 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.

7.1.1 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.

7.1.2 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.

7.2 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 genannten Anforderungen genügen.

7.3 Inhaltsdatensicherung

Zu Algorithmen und Schlüssellängen siehe Kapitel 5.3 und zur S/MIME-Version siehe Kapitel 5.4.

7.4 Transportschicht

Es müssen feste IP-Adressen verwendet werden. Es soll https über Port 443 angeboten werden, optional kann zusätzlich http mit Standardport 80 angeboten werden. Sofern https verwendet wird, muss TLS in der Version 1.2 oder 1.3 verwendet werden. Die Parametrisierung soll gemäß Kapitel 2.2 bzw. Kapitel 2.3 aus [1] erfolgen.

7.5 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.

7.6 Betreff und Dateiname

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

8 Regelungen zu inhaltsdatengesicherten Containern für die Übertragungswege SFTP und REST

In diesem Kapitel werden generelle Vorgaben für den Aufbau und die Handhabung von inhaltsdatengesicherten Containern für die Übertragungswege SFTP und REST beschrieben.

Die zu übertragende XML-Nachricht wird zuerst komprimiert. Anschließend erfolgen die Signierung und Verschlüsselung mittels S/MIME. Es müssen die in Kapitel 5.3 vorgegebenen Algorithmen mit den dort angegebenen Schlüssellängen verwendet werden.

Die Schritte im Einzelnen:

0. XML-Nachrichtendatei erzeugen → „Nachricht.xml“.

1. Komprimierung mittels gzip → „Nachricht.xml.gz“.

2. Signierung:
   - Es wird eine abgesetzte Signatur erzeugt, d. h. es wird ein Base-64 codiertes MIME-Objekt vom Typ „multipart/signed“ erzeugt.
   - RFC 8551; Kapitel „3.5.3. Signing Using the multipart/signed Format“.
   - Algorithmen siehe Kapitel 5.3.

3. Das so entstandene MIME-Objekt wird anschließend verschlüsselt.
   - RFC 8551 Kapitel 3.3. Creating an Enveloped-Only Message.
   - Algorithmen siehe Kapitel 5.3.

4. Das MIME-Objekt ist ein gültiger E-Mail-Body und wird mit einem Dateinamen entsprechend der Namenskonvention und der Dateinamenserweiterung “.eml” gesichert. → „Nachricht.eml“.

Diese Nachrichten-Datei kann in einem E-Mail-Client geöffnet, entschlüsselt und gelesen werden.

9 Regelungen für den Austausch via SFTP (ausschließlich für RD2.0-Prozessdaten)

Das Protokoll SFTP[20] ist ein Protokoll zur Datenübertragung basierend auf Secure Shell (SSH)[21]. Bei diesem Übertragungsweg erfolgen der Verbindungsaufbau, die Transportabsicherung und die Authentifizierung über SSH. Für SSH ist die BSI-TR-02102-4 (Stand: 31. Januar 2020) maßgeblich.

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

Erfolgt der Austausch via SFTP, so ist der SFTP-Steckbrief Version 1 zur standardisierten Mitteilung der eigenen Adressparameter zu verwenden. Dieses Dokument enthält den SFTP-Steckbrief auch als Word-Vorlage.

Wird der Kommunikationsweg SFTP genutzt, muss der Marktpartner einen eigenen entsprechenden SFTP-Server zum Empfang der Daten betreiben, auf dem seine Marktpartner ihre Container (Kapitel 8) ablegen können.

9.1 SFTP-Adresse

Der SFTP-Server muss als vollständig qualifizierter Domainname (FQDN) erreichbar sein. Der DNS-Name muss sich auf eine IPv4-Adresse beziehen. Verbindungen sind nur über den Standard-Port 22 (TCP) erlaubt.

Der Sender ist SFTP-Client, der Empfänger ist SFTP-Servers. Beim Datenaustausch muss also jeder einen SFTP-Server betreiben, der unter einer eindeutigen SFTP-Adresse zu erreichen ist.

9.2 SSH Version

Es ist die SSH-Version 2.0 zu verwenden.[22]

9.3 SSH Schlüsselpaare

Für den Aufbau einer SFTP Verbindung müssen der Empfänger (Server) und Sender (Client) je ein Schlüsselpaar erzeugen. Der öffentliche Schlüssel muss dem jeweiligen Marktpartner zur Verfügung gestellt werden. Für den wechselseitigen Austausch von Übertragungsdateien werden also insgesamt 4 Schlüsselpaare benötigt, je Marktpartner ein Client- und ein Server-Schlüssel.

Die eineindeutigen SSH Schlüsselpaare müssen für die in der Rolle SFTP-Sender (Client) bzw. SFTP-Empfänger (Server) durch jeden Marktpartner selber generiert werden.

Der SFTP-Empfänger (Server) muss seinen privaten Server-Schlüssel sowie alle öffentlichen Client-Schlüssel ordnungsgemäß auf seinem Server hinterlegen.

---

[20] Gemäß IETF Internet Draft zum SSH File Transfer Protocol (SFTP v3), Dokument-Version 2: https://tools.ietf.org/html/draft-ietf-secsh-filexfer-02.

[21] Kapitel 2 aus [11] zeigt eine Liste der RFC die alle SSH-Varianten abdeckt. Für dieses Dokument maßgeblich sind ITEF RFC 4250 bis 4256, ITEF RFC 4335, ITEF RFC 4344, ITEF RFC 4819, ITEF RFC5647, ITEF RFC5656 und ITEF RFC 6668.

[22] Gemäß Kapitel 3.2 aus [11].

Der SFTP-Sender (Client) muss seinen privaten Client-Schlüssel sowie die öffentlichen Schlüssel aller Server ordnungsgemäß in seinem Client hinterlegen.

Die Server-Schlüssel sind beim Client so zu hinterlegen, dass es nicht zu einer Bestätigungsanfrage für den Fingerprint kommt. Wird bei Verbindungsaufbau die Bestätigung eines Fingerprints angefordert, so ist die Verbindung unverzüglich zu beenden und ein Klärungsprozess einzuleiten.

9.4 Algorithmen und Schlüssellängen für SSH

Um eine sichere SSH-Verbindung zu gewährleisten, sind mindestens folgende Methoden für den Schlüsselaustausch zwischen Server und Client zu unterstützen:[23]

› Key Exchange Method:

- `ecdh-sha2-nistp256` (gemäß Abschnitt 6.4 in IETF RFC5656).

› Verschlüsselungsalgorithmus:

- `aes256-ctr` (gemäß Abschnitt 4 in IETF RFC3444).

9.5 MAC-Sicherung

Für die MAC-Sicherung sind mindestens die folgenden Verfahren zu unterstützen:[24]

- `hmac-sha2-256` (gemäß Kapitel 2 in IETF RFC6668).

9.6 Authentisierung

Die Authentisierung muss sowohl für den Client, als auch für den Server, über die zuvor ausgetauschten SSH Schlüsselpaare erfolgen.

Für die Authentisierung ist mindestens der Algorithmus für die digitale Signatur zu verwenden:[25]

› Server-Authentisierung:

- `ecdsa-sha2-nistp256` (gemäß Abschnitt 3 in IETF RFC5656). Schlüssellänge 250 Bit.

Für die Server- und Client-Authentisierung ist nach ITEF RFC4252 Kapitel 7 der gleiche Algorithmus zu verwenden.

Zudem ist für den Verbindungsaufbau bei der Anmeldung am SFTP-Server die Angabe eines zuvor ausgetauschten Benutzernamens (siehe Kapitel 17, SFTP-Steckbrief) erforderlich, da die SSH Authentifizierung gemäß IETF RFC 4252 öffentliche Schlüssel und einen Benutzernamen erfordert. Für eine erfolgreiche Authentifizierung muss der entsprechende Benutzer auf dem

[23] Sinngemäß den Kapitel 3.3 und 3.4 aus [11] entnommen.

[24] Sinngemäß den Kapitel 3.5 aus [11] entnommen.

[25] Sinngemäß den Kapitel 3.6 aus [11] entnommen.

SFTP-Server angelegt sein und der öffentliche Schlüssel des Marktpartners muss diesem Benutzer zugewiesen sein.

9.7 Autorisierung

Die Kommunikationspartner sind verpflichtet, dem jeweils anderen basierend auf gültigen SSH Schlüsselpaaren einen Zugang zu gewähren.

9.8 Handhabung von SSH Schlüsselpaaren

Die SSH Schlüsselpaare sind spätestens nach drei Jahren zu erneuern und die öffentlichen Schlüssel den Marktpartnern bekannt zu machen. Um einen reibungslosen Ablauf zu gewährleisten, müssen bei einer Schlüsselerneuerung die Vorgaben aus Kapitel 5.5 analog eingehalten werden.

Sofern der private Schlüssel nicht mehr vertrauenswürdig ist, müssen die betroffenen Marktpartner unverzüglich benachrichtigt werden. Der private Schlüssel ist unverzüglich zu deaktivieren und es ist ein neues Schlüsselpaar zu generieren und der öffentliche Schlüssel ist den Marktpartnern zur Verfügung zu stellen.

9.9 Konventionen für die Dateiablage und Vermeidung von Zugriffskonflikten

Die Dateien sind nach Kapitel 8 zu erzeugen (Container).

Der Kommunikationspartner (Sender / Client) legt die Dateien direkt in seinem Verzeichnis beim Empfänger (Server) ab. Es sind keine Unterverzeichnisse anzulegen, weder vom Sender noch vom Empfänger.

Zur Vermeidung möglicher Zugriffskonflikte während des Schreibvorgangs bei der SFTP-Übertragung müssen die Dateien während des Schreibvorganges mit einem temporären Präfix („.“) geschrieben werden und nach Beendigung des Schreibvorgangs in eine Datei ohne das Präfix umbenannt werden. Hierdurch werden Zugriffskonflikte zwischen Sender und Empfänger vermeiden. Der Marktpartner (Sender / Client) muss entsprechende Rechte zum Schreiben/Umbenennen in seinem Root-Verzeichnis beim Empfänger (Server) besitzen.

10 Regelungen für den Austausch via REST

Erfolgt der Datenaustausch via REST so ist der REST-Steckbrief Version 1 zur standardisierten Mitteilung der eigenen REST-Adressparameter zu verwenden. Dieses Dokument enthält den REST-Steckbrief auch als Word-Vorlage.

Representational State Transfer (REST) nutzt die Funktionalität des http-Protokolls und seiner Transportsicherung. Die Inhaltsdatensicherung erfolgt mit Containern (siehe Kapitel 8). Entsprechend benötigt jeder Marktteilnehmer jeweils Zertifikate für zwei Aufgabenstellungen:

› Zertifikate für die Absicherung der Transportschicht (TLS-Zertifikat) und

› das Zertifikat für die Inhaltsdatensicherung via S/MIME (S/MIME-Zertifikat).

REST ist ein Webservice (WS) und arbeitet unidirektional. Die Client-Implementierung des WS kann Daten versenden, die Server-Implementierung kann Daten empfangen. Damit zwei Marktpartner bidirektional Daten austauschen können, müssen diese den WS in beiden Ausprägungen (als Client und als Server) implementieren.

10.1 REST-Transport-Layer

Als WS-Adresse wird in diesem Dokument die WS-URL bezeichnet.

Der WS muss über eine URL im Format https://{domain}/{api} (z. B. https://example.org/api) erreichbar sein. Der Part {domain} muss ein vollständig qualifizierter Domainname (FQDN) sein und darf keine Portnummer enthalten. Der DNS-Name muss sich auf eine IPv4-Adresse beziehen.

Die Verbindung muss mindestens über TLS 1.2[26] gesichert sein. Die TLS-Erweiterung für Server Name Indication (SNI), definiert in Abschnitt 3 von ITEF RFC6066, muss von allen WS-Clients implementiert werden. Es muss auch von jedem WS-Server implementiert werden, der unter mehreren Namen bekannt ist. Andernfalls ist es für einen Server mit mehreren Hostnamen nicht möglich dem Client das richtige Zertifikat vorzulegen.

Es ist nur eine Verbindung über den Standard-Port 443 erlaubt.

Der WS verfügt über zwei Funktionen (Dokumentenannahme und Kommunikationstest), die jeweils über einen eigenen Subpfad (/data und /comtest) angesprochen werden (z. B. https://example.org/api/data und https://example.org/api/comtest).

10.2 TLS-Zertifikat und mutual TLS

Die Absicherung und Authentifizierung erfolgen via mutual TLS (TLS mit Client-Zertifikat)[27]. Die dafür eingesetzten Server- und Client-Zertifikate sind über CA zu bestätigen.

Die Identität eines Kommunikationspartners wird auf Basis des *Issuer DN* (Angaben zum Aussteller/CA) und des *Subject DN* (Angaben zum Zertifikatinhaber) eines Zertifikats ermittelt (Certificate based trust). Eine Erneuerung des Zertifikats ist nicht anzuzeigen (*Issuer* und *Subject*

[26] Gemäß Kapitel 2 Vorgaben SSL/TLS aus [1].

[27] Siehe IETF RFC 5246 (Abs. 7.4.6. Client Certificate).

DN bleiben gleich). Ein Zertifikatswechsel (mindestens einer der Werte ändert sich) muss den Kommunikationspartnern über den REST-Steckbrief mitgeteilt werden.

Ein Marktteilnehmer benötigt je MP-ID ein eigenes Zertifikat mit einem eineindeutigen *Subject DN*. D. h. die Kombination Issuer / Subject ist genau einer MP-ID zugeordnet.

Die Vorgaben zum TLS-Zertifikat sind nachfolgend aufgeführt:

› Zertifikat im X.509v3-Format[28].

› Es werden für den Dokumentenversand (Client) und Dokumentenempfang (Server) Zertifikate mit identischen *Issuer DN* und *Subject DN* verwendet.

› Issuer DN und Subject DN müssen bei Zertifikatserneuerungen gleichbleiben (ansonsten müssen die Änderungen über den REST-Steckbrief den Kommunikationspartnern mitgeteilt werden).

› Das Zertifikat muss genau einen Domänennamen im SAN-Attribut (Subject Alternative Names) enthalten.

› Für die CA gelten dieselben Regeln wie in Kapitel 5.1.

10.3 Algorithmen und Schlüssellängen für TLS

Die TLS Cipher Suites sind gemäß BSI TR 03116-4 Kapitel 2 einzusetzen.

Bei TLS 1.2 sind mindestens folgende Cipher Suites anzubieten:[29]

- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` (gemäß IETF RFC5289).

Bei TLS 1.3 sind mindestens folgende Cipher Suites anzubieten:[30]

- `TLS_AES_128_GCM_SHA256` (gemäß IETF RFC8446).

10.4 REST-API

Der WS verfügt über zwei Funktionen (Dokumentenannahme und Kommunikationstest), die jeweils über einen eigenen Subpfad (/data und /comtest) angesprochen werden. Die Kommunikation erfolgt über POST-Aufrufe.

10.4.1 Betriebsmodi für den WS (operating-mode)

Der WS kann in unterschiedlichen Betriebsmodi arbeiten. Der Betriebsmodus dient insbesondere der Unterscheidung, ob die übermittelten Nachrichten für den „Produktivbetrieb“ (PROD) produktiv genutzt werden sollen, oder ob ein „Testbetrieb“ (TEST) durchgeführt wird. Durch die Angabe des Betriebsmodus durch den Sendenden (Client) kann auf Seite des

[28] Siehe IETF RFC 6187.

[29] Gemäß Kapitel 2.2 aus [1].

[30] Gemäß Kapitel 2.3 aus [1].

Empfängers (Server) sichergestellt werden, dass sich beide Kommunikationsteilnehmer im selben Betriebsmodus befinden. Insbesondere kann damit vermieden werden, dass Testnachrichten fälschlicherweise an ein Produktivsystem gesendet werden.

Die Bezeichner für die folgenden beiden Betriebsmodi sind reserviert und müssen entsprechend genutzt werden. Weitere Betriebsmodi können zwischen den Marktpartnern vereinbart werden:

- `PROD` Produktivbetrieb: Dieser Betriebsmodus zeigt an, dass die Nachricht von einem Sender im Produktivbetrieb an einen Empfänger im Produktivbetrieb gesendet werden soll. In diesem Betriebsmodus erfolgt die vollständige fachliche Bearbeitung der Nachrichten mit allen in diesem Dokument genannten Konsequenzen.
- `TEST` Testbetrieb: Dieser Betriebsmodus zeigt an, dass die Nachricht von einem Sender im Testbetrieb an einen Empfänger im Testbetrieb gesendet werden soll. In diesem Betriebsmodus können Tests der Systemlandschaft durchgeführt werden. Der genaue Umfang der Tests kann durch die testenden Marktpartner bestimmt werden und ist nicht Teil dieses Dokuments. Insbesondere müssen die Nachrichteninhalte im Testbetrieb nicht fachlich durch die Empfänger bearbeitet werden.

10.4.2 Kommunikationstest

Der Kommunikationstest erfolgt über einen POST-Request an den Pfad `/comtest`.

Im Rahmen des Kommunikationstests werden Informationen ausschließlich über Header-Parameter ausgetauscht. Der Request-Body enthält keine Informationen. Ein erfolgreicher Kommunikationstest wird durch den Response-Code 204 signalisiert.

10.4.2.1 Header-Parameter

Der POST-Request zum Kommunikationstest enthält zwei Header-Parameter die alle verpflichtend zu befüllen sind vom Typ string:

- `api-version` API-Version des WS.
  Die API-Version des hier definierten WS ist „1.0.0“.
- `operating-mode` Betriebsmodus. Die folgenden Modi sind mindestens zu unterstützen: „TEST“ und „PROD“ (siehe Kapitel 10.4.1).

10.4.2.2 Response-Codes

Der Server muss mit einem der folgenden Response-Codes auf den Request antworten:

- `204` No Content - Dieser Status-Code wird nur für einen *erfolgreichen* Verbindungstest genutzt.
- `400` Bad Request - Die Daten konnten nicht korrekt gelesen werden.
- `401` Unauthorized - Die Authentifizierung ist fehlgeschlagen.
- `404` Not Found - Die angegebene URL ist falsch.
- `405` Method Not Allowed - Es sind nur POST-Requests erlaubt.

- `429` Too Many Requests - Der Sender hat zu viele Anfragen in zu kurzer Zeit gesendet.
- `500` Internal Server Error - Auf Seiten des Empfängers ist ein Fehler aufgetreten. Dieser Fehler ist nicht die Schuld des Senders. Der Sender kann versuchen die Anfrage zu wiederholen.

10.4.3 Dokumentenübermittlung

Dieser Abschnitt beschreibt den WS für die Dokumentenübermittlung. Die Dokumentenübermittlung erfolgen über einen POST-Request an den Pfad `/data`.

Das nach Kapitel 8 erzeugte Containerobjekt des XML-Dokuments, wird BASE64-kodiert innerhalb des JSON-formatierten Request-Bodys übermittelt. Eine erfolgreiche Übermittlung wird durch den Response-Code 202 signalisiert.

10.4.3.1 Parameters

Der POST-Request zur Dokumentenübermittlung enthält drei Header-Parameter die alle verpflichtend zu befüllen sind vom Typ string:

- `api-version` API-Version des WS.
  (Die API-Version des hier definierten WS ist „1.0.0“)
- `operating-mode` Betriebsmodus. Die folgenden Modi sind mindestens zu unterstützen: „TEST“ (Testbetrieb) und „PROD“ (Produktivbetrieb).
- `filename` Dateiname der XML-Datei inklusive Dateinamenerweiterung, welche in dieser Nachricht übermittelt wird. Der Dateiname hat der Namenskonvention aus dem entsprechenden Kapitel des EDI@Energy-Dokuments „Allgemeine Festlegungen“ zu folgen.

10.4.3.2 Request Body

Der Request-Body muss als „application/json“ formatiert sein.

10.4.3.3 Request Content

Der Request-Content enthält zwei verpflichtende Eigenschaften:

- `creationTime` Erstellungszeitpunkt in UTC des Dokuments, welches in dieser Nachricht übermittelt wird (String datetime).
- `document` BASE64-kodierte Version des Containerobjekts gemäß Kapitel 8 (string byte).

Beispiel:

```
{
  "creationTime": "2020-08-11T10:27:45.702Z",
  "document":
"PHhtbD5JY2ggYmluIGVpbiBCZWlzcGllbGRva3VtZW50PC94bWw+"
}
```

10.4.3.4 Response-Codes

Der Server muss mit einem der folgenden Response-Codes auf den Request antworten:

- 202 Accepted - Die Daten wurden *erfolgreich* empfangen und werden nun weiterverarbeitet. Eine ggf. zu erfolgende Antwort (z. B. ACK) wird über den Rückkanal übermittelt.
- 400 Bad Request - Die Daten konnten nicht korrekt gelesen werden.
  Dieser Status-Code wird zurückgeliefert, wenn erforderliche Parameter oder Eigenschaften des Requests fehlen oder ungültig sind (z. B. senden eines Requests mit Betriebsmodus „TEST“ an ein Produktivsystem oder fehlendes „document“).
- 401 Unauthorized - Die Authentifizierung ist fehlgeschlagen.
- 404 Not Found - Die angegebene URL ist falsch.
- 405 Method Not Allowed - Es sind nur POST-Requests erlaubt.
- 406 Not Acceptable - Der gültige „Content-Type“-Wert des Requests muss dem Wert „application/json“ entsprechen.
- 429 Too Many Requests - Der Sender hat zu viele Anfragen in zu kurzer Zeit gesendet
- 500 Internal Server Error - Auf Seiten des Empfängers ist ein Fehler aufgetreten. Dieser Fehler ist nicht die Schuld des Senders. Der Sender kann versuchen die Anfrage zu wiederholen.

11 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 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:

- 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.
  Bei der Nutzung von AS2, SFTP oder REST können keine Übertragungsdateien ausgetauscht werden, wenn gesperrte oder ungültige Zertifikate eingesetzt werden.
- 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 12 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, so kann der 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.
- RD2.0-Prozessdaten: Spätestens 10 Werktage bevor ein Zertifikat abläuft, muss der Inhaber dieses Zertifikats das Nachfolgezertifikat an den jeweiligen Ansprechpartner übermitteln.
- 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.

- 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) oder Acknowledgement (RD2.0-Prozessdaten) 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.

12 Konsequenzen bei Nicht-Einhaltung dieser Vorgaben

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

12.1 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.
RD2.0-Prozessdaten: Die Information ist mindestens an die über das Kontaktdatenblatt der Kommunikationspartner ausgetauschten E-Mailadressen 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.
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.
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.
RD2.0-Prozessdaten: Die Information ist mindestens an die über das Kontaktdatenblatt der Kommunikationspartner ausgetauschten E-Mailadressen des Marktpartners zu senden.

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.
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.
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.
RD2.0-Prozessdaten: Die Information ist mindestens an die über das Kontaktdatenblatt der Kommunikationspartner ausgetauschten E-Mailadressen des Marktpartners zu senden.

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.
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.
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.
RD2.0-Prozessdaten: Die Information ist mindestens an die über das Kontaktdatenblatt der Kommunikationspartner ausgetauschten E-Mailadressen des Marktpartners zu senden.

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 4.2.2 abgewickelt werden.

Verstoßvariante 6 (nur R2.0-Prozessdaten): Der Empfänger erhält unkomprimierte oder nicht standardkonform komprimierte (vgl. Kapitel 8) Nachrichten.

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 die Datei aufgrund einer fehlenden oder fehlerhaften Komprimierung 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.

Die Information ist mindestens an die über das Kontaktdatenblatt der Kommunikationspartner ausgetauschten E-Mailadressen des Marktpartners zu senden.

12.2 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 Datei,

- 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.

12.3 Beim Übertragungsweg per SFTP und REST

Bei den Übertragungswegen SFTP und REST muss ein inhaltsgesicherter Container gebildet werden. Hier gelten die gleichen Konsequenzen wie in Kapitel 12.1.

Kann Aufgrund fehlender oder ungültiger Zertifikate bzw. Schlüssel keine abgesicherte Verbindung aufgebaut werden, können auch keine Übertragungsdateien ausgetauscht werden. Die Konsequenzen trägt derjenige, der keine gültigen Zertifikate bzw. Schlüssel zur Verfügung gestellt hat, bzw. derjenige der gültige, zur Verfügung gestellte Zertifikate bzw. Schlüssel nicht korrekt nutzen.

Verfahrensweise: Über das Fehlen von gültigen Zertifikaten bzw. Schlüsseln des Empfängers wird dieser durch den Sender informiert. Der Sender hat den Empfänger (Verursacher) insgesamt mindestens einmal per E-Mail über die Tatsache zu informieren, dass Übertragungsdateien aufgrund fehlender oder ungültiger Zertifikate bzw. Schlüssel nicht ausgetauscht werden können. 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.
RD2.0-Prozessdaten: Die Information ist mindestens an die über das Kontaktdatenblatt der Kommunikationspartner ausgetauschten E-Mailadressen des Marktpartners zu senden.

13 Quellen

[1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, Bundesamt für Informationssicherheit, 23.02.2021.

[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.

[9] Beschluss (BK6-20-059) und Anlagen zum Beschluss (BK6-20-059) zum bilanziellen Ausgleich von Redispatch-Maßnahmen, Bundesnetzagentur, 06.11.2021.

[10] Beschluss (BK6-18-122) und Anlagen zum Datenaustauschs mit Verteilernetzbetreibern und signifikanten Netznutzern, Bundesnetzagentur, 20.12.2018.

[11] Technische Richtlinie BSI TR-02102-4 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 4: Verwendung von Secure Shell (SSH), Bundesamt für Informationssicherheit, 31.01.2020.

14 Ansprechpartner

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

15 Anhang 1: AS2-Steckbrief Version 3

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>*	

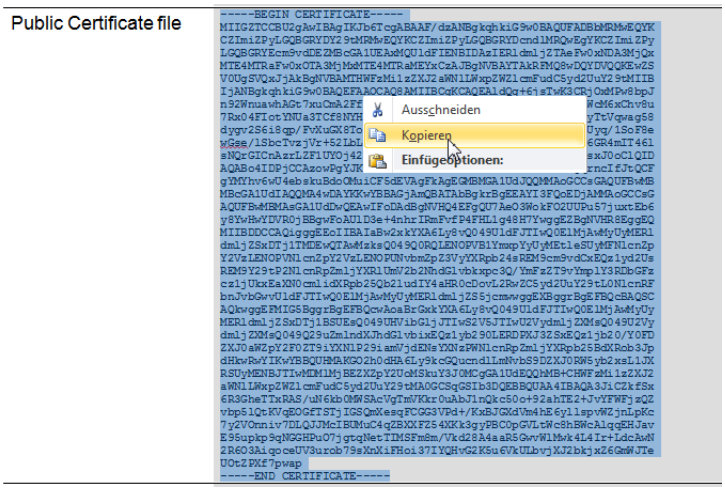
Netzwerk	
AS2-URL	***xxx.com/xxx***
IP-Adresse (Firewall)	***xxx.xxx.xxx.xxx***
Zusätzliche Absender-IP-Adresse (optional)	***-/-***
AS2-Zertifikat	
AS2-ID	Als AS2-ID ist die MP-ID zu verwenden. Für welche MP-ID das nachfolgend genannte Zertifikat verwendet wird, ergibt sich anhand der auf der vorherigen Seite genannten MI-IDs.
Öffentliches AS2-Zertifikat	-----BEGIN CERTIFICATE----- ***<String des Zertifikats>*** -----END CERTIFICATE-----
TLS-Zertifikat	
Öffentliches TLS-Zertifikat	-----BEGIN CERTIFICATE----- ***<String des Zertifikats>*** -----END CERTIFICATE-----

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

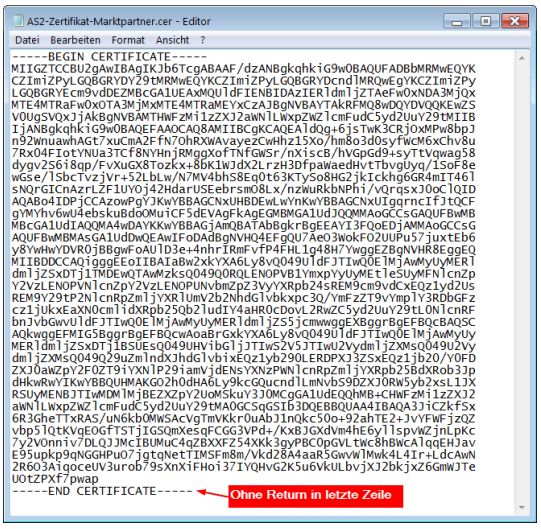
16 Anhang 2: Erzeugung eines Zertifikats (cer-Datei) aus dem AS2-Steckbrief

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

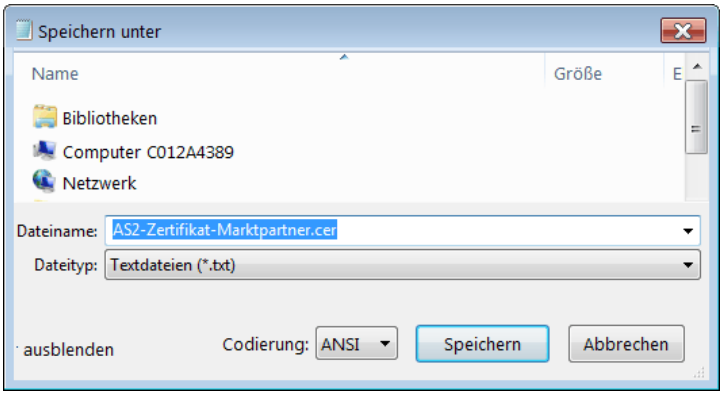
1) Text aus dem AS2-Steckbrief kopieren:



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:



17 Anhang 3: Steckbrief SFTP Version 1

Nachfolgend sind die allgemeinen und organisatorischen Angaben zum Datenaustausch via SFTP aufgeführt.

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 SFTP	
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 SFTP	
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>*

SFTP Server		
SFTP-Server Adresse	(Empfang)	**z. B. sftp://servera.*com/wurzelverzeichnis***
IP-Port	(Firewall)	22 (Standard SFTP)
SSH Public Key Fingerprint		
SSH Public Key		-----BEGIN SSH2 PUBLIC KEY----- ***<String des Schlüssels>*** -----END SSH2 PUBLIC KEY-----

SFTP-Client	
SFTP Benutzername	**USERNAME**
SSH Public Key Fingerprint	
SSH Public Key	-----BEGIN SSH2 PUBLIC KEY----- ***<String des Schlüssels>*** -----END SSH2 PUBLIC KEY-----

S/MIME Zertifikat	
Öffentliches S/MIME-Zertifikat (Inhaltsdatensicherung für Senden & Empfang)	-----BEGIN CERTIFICATE----- ***<String des Zertifikats>*** -----END CERTIFICATE-----

Hinweis: Es ist gemäß Kapitel 9.9 sicherzustellen, dass Dateien, die auf dem SFTP-Server abgelegt werden, mit einem Punkt vor dem Namen abgelegt werden. Erst nach dem Schreibvorgang darf der Punkt durch Umbenennen der Dateien entfernt werden.

18 Anhang 4: REST-Steckbrief Version 1

Nachfolgend sind die allgemeinen und organisatorischen Angaben zum Datenaustausch via REST-Webservice aufgeführt:

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 WS		
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 WS		
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>*	

Nachfolgend die Angaben zum WS-Aufruf:

Netzwerk		
WS-URL		https://***xxx.com/xxx***
Öffentliches TLS-Zertifikat für		***<MPID>***
1. Aussteller (Issuer DN)		
CN		***<Common Name>***
OU	(optional)	***<Organisationseinheit>***
O		***<Organisation>***
L	(optional)	***<Ort>***
ST	(optional)	***<Bundesland>***
C		***<Land>***
2. Antragsteller (Subject DN)		
CN		***<Common Name>***
OU	(optional)	***<Organisationseinheit>***
O		***<Organisation>***
L	(optional)	***<Ort>***
ST	(optional)	***<Bundesland>***
C		***<Land>***
3. Alternativer Antragsteller (SAN)		
DNS-name		***<Domänenname>***
Öffentliches TLS-Zertifikat für		***ggf. weitere <MPID>***
1. Aussteller (Issuer DN)		
CN		***<Common Name>***
OU	(optional)	***<Organisationseinheit>***
O		***<Organisation>***
L	(optional)	***<Ort>***
ST	(optional)	***<Bundesland>***
C		***<Land>***
2. Antragsteller (Subject DN)		
CN		***<Common Name>***
OU	(optional)	***<Organisationseinheit>***
O		***<Organisation>***
L	(optional)	***<Ort>***
ST	(optional)	***<Bundesland>***
C		***<Land>***
3. Alternativer Antragsteller (SAN)		
DNS-name		***<Domänenname>***

Nachfolgend die Angaben zum Kombi-Zertifikat:

Öffentliches S/MIME-Zertifikat		
1. Aussteller (Issuer DN)		
CN		***<Common Name>***
OU	(optional)	***<Organisationseinheit>***
O		***<Organisation>***
L	(optional)	***<Ort>***
ST	(optional)	***<Bundesland>***
C		***<Land>***
2. Antragsteller (Subject DN)		
CN		***<Common Name>***
OU	(optional)	***<Organisationseinheit>***
O		***<Organisation>***
L	(optional)	***<Ort>***
ST	(optional)	***<Bundesland>***
C		***<Land>***
3. Alternativer Antragsteller (SAN)		
RFC822-Name		***<Mailadresse> oder <Domainname>***[31]

[31] Ausgestellte Zertifikate mit RSASSA-PSS auf Domainname sind u. a. als sogenannte „AS2-Zertifikate“ verfügbar.

19 Änderungshistorie

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
12300	Deckblatt	Version: 1.4 Publikationsdatum: 01.04.2021	Version: 1.5 Konsultationsfassung Publikationsdatum: 30.07.2021	Version aktualisiert. Zusätzlich wurden im gesamten Dokument Schreibfehler, Layout, Beispiele etc. geändert, die keinen Einfluss auf die inhaltliche Aussage haben.	Liegt dem Markt zur Konsultation vor.
12301	Kapitel 1 Einleitung	[….] die Übertragungswege getroffen. **1.1 Regelungsumfang** […] Gemäß BNetzA-Beschluss[2] sind grundsätzlich die kryptographischen Vorgaben der BSI TR 03116 4 (Stand: **10. Januar 2020)** anzuwenden und einzuhalten. Die zu nutzenden Parameter und hiervon anzuwendenden Abweichungen sind in diesem Dokument beschrieben.	[…] die Übertragungswege getroffen. Gemäß BNetzA-Beschluss[2] sind grundsätzlich die kryptographischen Vorgaben der BSI TR 03116-4 (Stand: **23. Februar 2021**)[3] anzuwenden und einzuhalten. Die zu nutzenden Parameter und hiervon anzuwendenden Abweichungen sind in diesem Dokument beschrieben. **1.1 Regelungsumfang** […] Fußnote 3 (neu)**:** Falls diese Version nicht zum öffentlichen Download bereit-steht, so kann diese beim BSI angefragt werden**.**	Aktualisierung Versionsdatum der BSI TR 03116-4. Neue Fußnote als Beschaffungshinweis. Verschiebung Absatz in das erste Kapitel, da es sonst das neue Layout auf die zweite Seite fällt.	Liegt dem Markt zur Konsultation vor.
12302	Kapitel 2.2 Fahrplan	Wie in Kapitel 3.2 festgelegt, kommt für den Datenaustausch im Rahmen der Fahrplanprozesse nur E-Mail via SMTP zum Einsatz.	Es gelten die in Kapitel 3.2 festgelegten Übertragungswege für den Datenaustausch im Rahmen der Fahrplanprozesse.	Fehlerkorrektur.	Liegt dem Markt zur Konsultation vor.
12303	Kapitel 3.3 Fahrplan	Für die Übertragung der prozessrelevanten Dateien kommen die Übertragungswege AS2, E-Mail via SMTP oder REST zum Einsatz.	Für die Übertragung der prozessrelevanten Dateien kommen die Übertragungswege E-Mail via SMTP, AS2**, SFTP** oder REST zum Einsatz.	Ergänzung um SFTP.	Liegt dem Markt zur Konsultation vor.
12304	Kapitel 4.2.1 Allgemeines [Fahrplan]	• Für den Austausch von Fahrplandaten zwischen ÜNB und BKV kann der BKV bis zu zwei E-Mail-Adressen verwenden und/oder REST und/oder AS2 verwenden. Diese sind sowohl im	• Für den Austausch von Fahrplandaten zwischen ÜNB und BKV kann der BKV bis zu zwei E-Mail-Adressen verwenden und/oder REST und/oder AS2 **und/oder SFTP** verwenden. Diese sind sowohl im regulären Prozess **für die verschlüsselte**	Ergänzung SFTP gemäß 12303. Der erste Punkt im Kapitel 4.2.1 suggeriert, auch im regulären Prozess sei eine unsignierte und	Liegt dem Markt zur Konsultation vor.

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	**Neu**		
		regulären Prozess als auch bei einer technischen Störung (Kapitel 4.2.2) zur unsignierten und unverschlüsselten Übermittlung zu nutzen.	**und signierte Übermittlung als auch im Ausnahmefall** bei einer technischen Störung (Kapitel 4.2.2) **für die** unsignierte **und/oder** unverschlüsselte Übermittlung zu nutzen.	unverschlüsselte Übertragung von Fahrplandaten möglich.	
12305	Kapitel 4.2.2 Störungsbedingte Kommunikation	Probleme, die auf Grund nicht ausgetauschter oder nicht erneuerter bzw. abgelaufener Zertifikate entstehen, gelten nicht als technische Störung.	Probleme, die auf Grund nicht ausgetauschter oder nicht erneuerter bzw. abgelaufener Zertifikate entstehen, gelten nicht als technische Störung. **Die konkreten, möglichen Konsequenzen sind Kapitel 12 zu entnehmen.**	Präzisierung.	Liegt dem Markt zur Konsultation vor.
12306	Kapitel 5.1 Vertrauensdienste-anbieter	Im Folgenden […]. Das Zertifikat […]. Die CA, von der das Zertifikat ausgestellt ist, muss den nachfolgenden Anforderungen genügen:[xx] • 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~~	Im Folgenden […]. Das Zertifikat […]. **Es gelten die Bedingungen des Kapitels 5.1.1 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**.	Präzisierung. Verschiebung eines Satzes (Sperrliste http) von Kapitel 5.5 in das Kapitel 5.1, weil es eine Anforderung an die CA ist.	Liegt dem Markt zur Konsultation vor.

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
		~~des Unternehmens, dass das Zertifikat beantragt.~~ ~~Fußnote [xx]:~~ ~~Sinngemäß dem Kapitel 5.1.1 Zertifizierungsstellen/Vertrauensanker aus [1] entnommen.~~			
12307	Kapitel 5.2 Zertifikate: Parameter und Anforderungen für S/MIME	Die Zertifikate müssen die nachfolgenden Anforderungen erfüllen[xx]: • Das Zertifikat muss von einer CA ausgestellt sein, die den unter Kapitel 6.1.1 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.~~ • 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. • […] • Für die nötigen Anwendungszwecke „Signatur“ und „Verschlüsselung“ ist dasselbe Schlüsselpaar zu generieren und dementsprechend ein sogenanntes Kombizertifikat auszustellen und zu verwenden. • […] 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).	Die Zertifikate müssen die nachfolgenden Anforderungen **nach Kapitel 5.1.2 Zertifikate aus [1] mit folgenden Ausnahmen und Ergänzungen erfüllen.** **In Abweichung gelten folgende Regelungen:** • **Alle** Zertifikate **müssen** Information**en** für eine Rückrufprüfung enthalten, d. h. einen `CRLDistributionPoint`, unter dem jederzeit aktuelle CRL**s** zur Verfügung stehen. • **Eine `AuthorityInfoAccess`-Extension muss nicht bereitgestellt werden.** • Das Zertifikat muss von einer CA ausgestellt sein, die den unter Kapitel **5.1** genannten Anforderungen genügt. • **In Abweichung zu [1] ist die Gültigkeitsdauer der CAs auf eine kryptographisch vertretbare Zeit zu limitieren.** • **Müssen für Signatur und Verschlüsselung** dasselbe **Zertifikat (**Kombizertifikat **) verwendet werden.**[xx] **Zusätzlich gelten folgende Regelungen:** • Alle Zertifikate müssen mit RSASSA-PSS signiert sein. • […] Für den Austausch der öffentlichen Zertifikate gilt die Codierung **DER entweder binär X.509 oder Base-64 X.509 mit der Datei-Extension .cer.** Fußnote [xx]: Vgl. BK7 [2] bis [5] bzw. BK6 [6].	Präzisierung. Löschen abgelaufene Regelungen.	Liegt dem Markt zur Konsultation vor.

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
		Fußnote [xx]: ~~Sinngemäß dem Kapitel 5.1.2 Zertifikate aus [1] entnommen und um~~ BK7 [2] bis [5] bzw. BK6 [6] ~~ergänzt~~.			
12308	Kapitel 5.3 Algorithmen und Schlüssellängen für S/MIME	• Signaturverfahren (Signature algorithm […] Schlüssellänge der verwendeten RSA-Schlüssel mindestens 2048 Bit.	• Signaturverfahren (Signature algorithm […] Schlüssellänge der verwendeten RSA-Schlüssel mindestens 2048 Bit. **Ab dem 01.01.2023 muss die Schlüssellänge der verwendeten RSA-Schlüssel mindestens 3072 Bit betragen.** **Des Weiteren sind die Übergangsregelungen für Schlüssellängen weiter unten zu beachten.**	Anforderung aus BSI TR-03116-4, Kapitel 3.3 Signaturen.	Liegt dem Markt zur Konsultation vor.
12309	Kapitel 5.3	• Inhaltsverschlüsselung (Content encryption): AES-128 CBC, AES-192 CBC oder AES-256 CBC (gemäß IETF RFC 3565).	• Inhaltsverschlüsselung (Content encryption): AES-128 CBC, AES-192 CBC oder AES-256 CBC (gemäß IETF RFC 3565). **Ab dem 01.10.2024 muss AES-128 GCM verwendet werden.**	Anforderung aus BSI TR-03116-4, Kapitel 3.4.1 Content Encryption.	Liegt dem Markt zur Konsultation vor.
12310	Kapitel 5.3	• Schlüsselverschlüsselung (Key encryption): RSAES-OAEP […] […] Schlüssellänge der verwendeten RSA-Schlüssel mindestens 2048 Bit.	• Schlüsselverschlüsselung (Key encryption): RSAES-OAEP […] […] Schlüssellänge der verwendeten RSA-Schlüssel mindestens 2048 Bit **Ab dem 01.01.2023 muss die Schlüssellänge der verwendeten RSA-Schlüssel mindestens 3072 Bit betragen.** **Des Weiteren sind die Übergangsregelungen für Schlüssellängen weiter unten zu beachten.**	Anforderung aus BSI TR-03116-4, Kapitel 3.4.2 Key Encryption.	Liegt dem Markt zur Konsultation vor.
12311	Kapitel 5.3	-/-	Die verwendete Schlüssellänge ergibt sich aus dem öffentlichen RSA-Schlüssel des Zertifikats. Es gelten folgende Übergangsregelungen für Schlüssellängen: • Bis 31.03.2022: Existierende Zertifikate, die eine RSA-Schlüssellänge von 2048 Bit	Hinweis und Übergangsregelung.	Liegt dem Markt zur Konsultation vor.

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
			besitzen, dürfen bis zu ihrem Auslaufdatum verwendet werden. • Zertifikate, die bis zum 31.03.2022 neu ausgestellt bzw. erneuert werden, sollten bereits eine RSA-Schlüssellänge von mindestens 3072 Bit besitzen. • Ab 01.04.2022: Zertifikate die ab dem 01.04.2022 ausgestellt werden, müssen eine RSA-Schlüssellänge von mindestens 3072 Bit besitzen.		
12312	Kapitel 5.3		**Aus Sicht des Bundesamts für Sicherheit in der Informationstechnik und der Bundesnetzagentur gilt für die Algorithmen zum Signieren und Verschlüsseln zusätzlich folgendes:** Ab dem 01.01.2023 muss der Empfang von S/MIME-Nachrichten unterstützt werden, die gemäß [1] die Signatur ECDSA und für die Key Encryption ECDH verwenden. Es wird empfohlen, die Kurve BrainpoolP256r1 bei den ECC-Verfahren zu akzeptieren, um den Mindestanforderungen an die Interoperabilität aus Abschnitt 3.7 in [1] zu genügen. Beim Versand von S/MIME-Nachrichten dürfen diese Algorithmen auch nach dem 01.01.2023 nicht verwendet werden. In einer folgenden zu konsultierenden Festlegung wird über den frühestmöglichen Verwendungszeitpunkt entschieden sowie die Verfügbarkeit der einzusetzenden Zertifikate behandelt.	Es liegt eine Forderung des BSI vor, ab 01.01.2023 die Verfahren ECDSA und ECDH via S/MIME zu unterstützen. Auf Wunsch der BNetzA wird es zur Konsultation gestellt.	Liegt dem Markt zur Konsultation vor.
12313	Kapitel 5.4 S/MIME-Version	Signieren und Verschlüsseln sind ausschließlich nach dem S/MIME-Standard gestattet. Es muss mindestens die Version 4.0 (IETF RFC 8551, Veröffentlichungsjahr 2019) verwendet werden.[xx] ~~Fußnote [xx]:~~	Signieren und Verschlüsseln sind ausschließlich **nach dem Kapitel 3.1 aus [1] zulässigen** S/MIME-Standard gestattet. **Es sind dabei nur die in diesem Dokument bewerteten, beschriebenen und ausgewählten Verfahren zulässig.**	Präzisierung.	Liegt dem Markt zur Konsultation vor.

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
		~~Sinngemäß den Kapiteln 3.6 Weitere Vorgaben und 3.8 Übergangsregelungen aus [1] entnommen~~.			
12314	Kapitel 5.5 Zertifikatswechsel und Sperrlisten	• 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 keines der Zertifikate seiner Marktpartner gesperrt wurde, in dem er alle von ihm verwendeten Zertifikate gegen die Sperrlisten (CRL) prüft.	Anpassung gemäß 12306.	-/-.
12315	Kapitel 5.5	• 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.	• 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.**	Präzisierung.	Liegt dem Markt zur Konsultation vor.
12316	Kapitel 6.2 E-Mail-Anhang	• EDIFACT-Übertragungsdateien dürfen, müssen aber nicht komprimiert werden. Dateien des Fahrplandatenaustauschs ~~dürfen komprimiert werden, ab dem 1.10.2021 müssen sie komprimiert werden.~~ Dateien der RD2.0-Prozessdaten müssen komprimiert werden.	• EDIFACT-Übertragungsdateien dürfen, müssen aber nicht komprimiert werden. Dateien des Fahrplandatenaustauschs **und** Dateien der RD2.0-Prozessdaten müssen komprimiert werden.	Löschung abgelaufene Ausnahme.	Liegt dem Markt zur Konsultation vor.
12317	Kapitel 6.5 Signatur und Verschlüsselung von E-Mails	Hinweise (aus Kapitel 4 und 5): • Das Signieren und Verschlüsseln von E-Mails sind ausschließlich nach dem S/MIME-Standard gestattet. Es muss mindestens die Version 4.0 (IETF RFC 8551, Veröffentlichungsjahr 2019) verwendet werden. • Jeder Marktpartner muss für jede von ihm genutzte E-Mail-Adresse genau ein Zertifikat (genauer den dazugehörigen privaten Schlüssel) zur Signaturerzeugung verwenden. Zur Entschlüsselung der an diese E-Mail-Adresse von den jeweils anderen Marktpartnern	-/-	Streichung, da Formulierungen an unterschiedlicher Stelle zum gleichen Thema nicht sachdienlich sind.	Liegt dem Markt zur Konsultation vor.

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	**Neu**		
		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.			
12318	Kapitel 7 Regelungen für den Austausch via AS2	[…] AS2-Steckbrief Version 2 […].	[…] AS2-Steckbrief Version **3** […].	Aktualisierung auf neue Steckbriefversion.	Liegt dem Markt zur Konsultation vor.
12319	Kapitel 7.4 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.[xx] Sofern https verwendet wird, muss zur Wahrung der Konformität mit der BSI TR-03116-4 mindestens TLS Version 1.2 oder höher verwendet werden.[yy] Fußnote [xx]: 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. Fußnote [yy]: Siehe Kapitel 2 Vorgaben SSL/TLS aus [1]	Es müssen feste IP-Adressen verwendet werden. Es **soll https über Port 443** angeboten werden, optional kann zusätzlich **http mit Standardport 80** angeboten werden**.** Sofern https verwendet wird, muss **TLS in der Version 1.2 oder 1.3 verwendet werden. Die Parametrisierung soll gemäß Kapitel 2.2 bzw. Kapitel 2.3 aus [1] erfolgen.**	Anforderung aus BSI TR-03116-4.	Liegt dem Markt zur Konsultation vor.

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
12320	Kapitel 11 Organisatorische Regelungen zum Umgang mit Zertifikaten	Ein Marktpartner A kann nur dann […]: • […] • […] • […] • […] • […] • […] • […] • […] • 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. Bei der Nutzung von AS2, SFTP oder REST können keine Übertragungsdateien ausgetauscht werden, wenn gesperrte oder ungültige Zertifikate eingesetzt werden.	"Ein Marktpartner A kann nur dann [...]: • 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. Bei der Nutzung von AS2, SFTP oder REST können keine Übertragungsdateien ausgetauscht werden, wenn gesperrte oder ungültige Zertifikate eingesetzt werden. • […]	Reihenfolge der Absätze korrigiert.	Liegt dem Markt zur Konsultation vor.
12321	Kapitel 11	• 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.	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.**	Präzisierung.	Liegt dem Markt zur Konsultation vor.
12322	Kapitel 13 Quellen	[1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, Bundesamt für Informationssicherheit, 10.01.2020.	[1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, Bundesamt für Informationssicherheit, **23.02.2021**.	Aktualisierung Versionsdatum der BSI TR 03116-4 gemäß Festlegung.	Liegt dem Markt zur Konsultation vor.

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
12323	Kapitel 15 Anhang 1: AS2-Steckbrief Version 2	Anhang 1: AS2-Steckbrief Version 2	Anhang 1: AS2-Steckbrief Version **3**	Gemäß Änderung 12318.	Liegt dem Markt zur Konsultation vor.
12324	Kapitel 15	Netzwerk: • AS2-URL ~~http://~~xxx.com/xxx • IP-Adresse (Firewall) • ~~IP-Port~~ • Zusätzliche Absender-IP-Adresse (optional)	Netzwerk: • AS2-URL xxx.com/xxx • IP-Adresse (Firewall) • Zusätzliche Absender-IP-Adresse (optional)	Gemäß Änderung 12319.	Liegt dem Markt zur Konsultation vor.
12325	Kapitel 15	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 Schlüssselverschlüsselungs-Algorithmus RSAES-OAEP • Datenverschlüsselungs-Algorithmus AES-128 CBC, AES-192 CBC oder AES-256 CBC	-/-	Streichung in Konsitenz zu anderen RzÜ-Steckbriefen.	Liegt dem Markt zur Konsultation vor.

12326	Kapitel 15	-/-	TLS-Zertifikat
			• Öffentliches TLS-Zertifikat
			`-----BEGIN CERTIFICATE-----`
			<String des Zertifikats>
			`-----END CERTIFICATE-----`
				Gemäß Änderung 12319.	Liegt dem Markt zur Konsultation vor.