

EDI@Energy – Regelungen zum Übertragungsweg

Regelungen zum sicheren Austausch von EDIFACT- Übertragungsdateien

Konsolidierte Lesefassung mit Fehlerkorrekturen Stand: 12. Dezember 2017

Version:	1.1
Ursprüngliches Publikationsdatum:	01.04.2017
Anzuwenden ab:	01.06.2017
Autor:	BDEW

Inhaltsverzeichnis

1	Einführung	4
2	Bekanntmachen beim Informationsempfänger	4
3	Übertragungswege	5
4	1:1-Kommunikation	5
5	Regelungen für den Austausch via E-Mail	6
5.1	E-Mail-Adresse	6
5.2	E-Mail-Anhang	6
5.3	E-Mail-Body	7
5.4	E-Mail Betreff	7
5.5	Verschlüsselung und Signatur von E-Mails	7
5.5.1	Zertifizierungsstellen.....	8
5.5.2	Zertifikate: Parameter und Anforderungen.....	8
5.5.3	Algorithmen und Schlüssellängen für S/MIME.....	9
5.5.4	Zertifikatswechsel und Sperrlisten.....	10
6	Regelungen für den Austausch via AS2	11
6.1	AS2-Adresse	11
6.1.1	AS2-ID.....	11
6.1.2	AS2-URL.....	11
6.2	Anforderungen an AS2-Zertifikate	11
6.3	Algorithmen und Schlüssellängen	11
6.4	Transportschicht	12
6.5	MDN (digitale Zustell-Quittung)	12
6.6	Betreff und Dateiname	12
7	Organisatorische Regelungen zum Umgang mit Zertifikaten	13
8	Konsequenzen bei Nicht-Einhaltung dieser Vorgaben	14
8.1	Beim Übertragungsweg E-Mail:	14
8.2	Beim Übertragungsweg per AS2:	15

9	Quellen	18
10	Ansprechpartner	18
11	Änderungshistorie.....	19
12	Anhang 1: AS2-Steckbrief Version 2.....	24
13	Anhang 2: Erzeugung eines Zertifikats (cer-Datei) aus dem AS2-Steckbrief.....	26

1 Einführung

Dieses Dokument regelt die Sicherheits- und Schutzmechanismen, die im Rahmen des elektronischen Datenaustauschs zwischen den Marktpartnern der deutschen Energiewirtschaft für die Übertragungswege¹ AS2 und E-Mail via SMTP in der aktuellen Prozesswelt und für das Interimsmodell² in der Marktkommunikation einzuhalten sind. Es wird keine Aussage über die im Zielmodell geltenden Anforderungen an die Übertragungswege getroffen.

Die nachfolgenden Regeln finden Anwendung auf alle von der BNetzA festgelegten Marktprozesse, die per EDIFACT abgewickelt werden, wie beispielsweise GPKE, MPES, GeLi Gas, GaBi Gas, MaBiS, WiM und KoV³.

Dieses Dokument benennt nicht die ggf. existierenden rechtlichen Folgen, wenn aufgrund eines abweichenden Vorgehens kein gesicherter elektronischer Datenaustausch stattfinden kann. In diesem Dokument wird der Austausch von qualifiziert signierten EDIFACT-Übertragungsdateien nicht betrachtet.

Gemäß BNetzA-Beschluss² sind grundsätzlich die kryptographischen Vorgaben der BSI TR 03116-4 (Stand: 23. Februar 2016) anzuwenden und einzuhalten. Die zu nutzenden Parameter und hiervon anzuwendenden Abweichungen sind in diesem Dokument beschrieben.

Während der Phase des Interimsmodells gelten somit die nachfolgenden Regelungen zum Übertragungsweg, welche auch die damit verbundenen organisatorischen Regelungen für die deutsche Energiewirtschaft enthalten.

2 Bekanntmachen beim Informationsempfänger

Um beim Datenaustausch gemäß § 42a GasNZV bzw. § 22 StromNZV eine größtmögliche Automatisierung zu erreichen, müssen sich die Marktpartner vor dem erstmaligen Datenversand unter anderem über den Übertragungsweg und die Datenaustauschadressen inkl. der zu verwendenden Zertifikate verständigen. Dazu wird eine Kontaktaufnahme zum Austausch dieser Kommunikationsparameter (per Telefon oder E-Mail) vorausgesetzt, um nachfolgend einen reibungslosen elektronischen Datenaustausch zu ermöglichen, und so Verzögerungen in der Bearbeitung aufgrund fehlender Informationen über den Sender einer Übertragungsdatei seitens des Empfängers auszuschließen.

Spätestens drei Werktage (gemäß GPKE/GeLi Gas-Kalender⁴) nach erstmaliger Kontaktaufnahme eines Marktpartners müssen die oben genannten Daten zwischen diesen beiden Parteien ausgetauscht sein. Ein Werktag nach Austausch der Kommunikationsdaten müssen beide Parteien die Daten des jeweils anderen Marktpartners in allen ihren an der Marktkommunikation beteiligten Systemen eingetragen bzw. zur Verfügung gestellt haben, so dass alle Voraussetzungen für die Durchführung des elektronischen Datenaustauschs erfüllt sind.

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

² Vgl. BK6-16-200 und BK7-16-142, Beschluss zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, vom 20.12.2016.

³ Die nationalen Regelungen zum Übertragungsweg gelten bei der KoV nur für die rein nationalen Geschäftsprozesse nach KoV Anlage 3.

⁴ Hinweis: Die Werktagsdefinitionen in GPKE und GeLi Gas sind identisch.

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 prozessieren⁵. 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 zwei Wochen vor Umstellung. Die Adressierung erfolgt wenigstens an die Adressdaten der Marktpartner, mit denen er in den letzten drei Jahren EDIFACT-Dateien ausgetauscht hat, welche zum Zeitpunkt der Informationsübermittlung in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegt sind.

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

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

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

3 Übertragungswege

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

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

4 1:1-Kommunikation

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-Nachrichten generieren.

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

⁵ Im Regelfall, in dem ein Übertragungsweg eingerichtet ist, ist das Zugangsdatum das für die Fristen relevante Datum.

Eine EDIFACT-Übertragungsdatei, die von einer anderen E-Mail-Adresse als der vereinbarten E-Mail-Adresse versandt wird, muss vom Empfänger nicht verarbeitet⁶ werden. Sie gilt dementsprechend als nicht zugestellt und es erfolgt keine Rückmeldung an den Marktpartner. Die sich daraus ergebenden Konsequenzen hat der Versender der E-Mail zu tragen.

5 Regelungen für den Austausch via E-Mail

Die in diesem Abschnitt 5 beschriebenen Regeln gelten ausschließlich für die E-Mail-Adresse, über die die EDIFACT-Übertragungsdateien ausgetauscht werden. Diese E-Mail-Adresse darf nicht mit der E-Mail-Adresse verwechselt werden, welche in der BDEW- bzw. DVGW-Codenummerndatenbank veröffentlicht ist und u. a. der erstmaligen Kontaktaufnahme mit dem Marktpartner, bzw. bei einem Problem im Datenaustausch mit dem Marktpartner zur Kontaktaufnahme mit ihm dient.

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

5.1 E-Mail-Adresse

- Die für den Austausch von EDIFACT-Übertragungsdateien zwischen zwei Marktpartnern festgelegte E-Mail-Adresse ist ausschließlich für den Austausch von EDIFACT-Nachrichten zu nutzen.
- Im Sinne der 1:1-Kommunikation muss es eine personenneutrale, funktionsbezogene E-Mail-Adresse sein (bspw. ohne Vor- und Nachnamen).
- Ein Marktpartner, der E-Mails mit Geschäftskorrespondenz an die für den Austausch von EDIFACT-Übertragungsdateien 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 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 Empfänger 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 EDIFACT“ <edifact@Marktpartner.de>

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

Wird die Phrase „Datenaustausch EDIFACT“ 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 edifact@Marktpartner.de und EDIFACT@MarktPartner.de identisch.

5.2 E-Mail-Anhang

- In einer E-Mail darf immer nur eine EDIFACT-Übertragungsdatei enthalten sein.
- Eine E-Mail darf keine weiteren Anhänge enthalten.

⁶ D. h. die E-Mail muss weder entschlüsselt, noch die Signatur geprüft, noch muss die in der E-Mail enthaltene Übertragungsdatei verarbeitet werden.

- Soll die EDIFACT-Übertragungsdatei komprimiert werden, so ist dafür die gzip-Komprimierung⁷ zu verwenden.
- Für die EDIFACT-Übertragungsdatei gilt die Namenskonvention aus dem entsprechenden Kapitel des EDI@Energy-Dokuments „Allgemeine Festlegungen“.
- Der Anhang ist nicht separat zu verschlüsseln, da dies bereits durch S/MIME erfolgt.
- Der Anhang muss Base64 kodiert sein, damit Mailserver keine Zeilenumbrüche während des Transportes einfügen.

5.3 E-Mail-Body

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

5.4 E-Mail Betreff

Der E-Mail-Betreff muss gleichlautend mit dem Dateinamen der EDIFACT-Übertragungsdatei gefüllt sein. Für den Dateinamen gilt die Namenskonvention, aus dem entsprechenden Kapitel des EDI@Energy-Dokuments „Allgemeine Festlegungen“.

5.5 Verschlüsselung und Signatur von E-Mails

Jede E-Mail, mit der in der deutschen Energiewirtschaft eine EDIFACT-Übertragungsdatei ausgetauscht wird, ist zu verschlüsseln und zu signieren, spätestens ab dem 01.06.2017. Dabei sind die in diesem Kapitel genannten Regelungen einzuhalten:

- Im Sinne der 1:1-Kommunikation ist der Datenaustausch geschäftsprozessunspecifisch zu betreiben, d. h. die Verschlüsselung und Signatur der E-Mail erfolgt für alle Nachrichtentypen⁸ einheitlich. Es müssen somit alle Übertragungsdateien von einem Absender an einen Empfänger verschlüsselt und signiert werden.
- Das Verschlüsseln und Signieren von E-Mails ist ausschließlich nach dem S/MIME-Standard gestattet. Es muss mindestens die Version 3.2 (IETF RFC 5751, Veröffentlichungsjahr 2010) verwendet werden.⁹
- Jeder Marktpartner muss für die von ihm genutzte E-Mail-Adresse¹⁰ genau ein Zertifikat (genauer den dazugehörigen privaten Schlüssel) zur Signaturerzeugung verwenden. Zur Entschlüsselung der an diese E-Mail-Adresse von den jeweils anderen Marktpartnern verschlüsselt gesendeten E-Mail wird der gleiche private Schlüssel genutzt. Umgekehrt müssen Zertifikate der Marktpartner (je eines, je E-Mail-Adresse) sowohl zur Verschlüsselung als auch zur Signaturprüfung verwendet werden. Auf diese Weise muss je vom Marktpartner

⁷ gzip ist plattformunabhängig.

⁸ Beispiele für unterschiedliche Nachrichtentypen: APERAK, CONTRL, INVOIC, MSCONS, ORDERS (auch z. B. in der Ausprägung NOMINT), ORDRSP (auch z. B. in der Ausprägung ALOCAT oder NOMRES).

⁹ Singgemäß dem Kapitel 3.1 Versionen aus [1] entnommen.

¹⁰ Ein Marktpartner kann je Marktrolle (und damit je MP-ID) ein eigenes E-Mail-Postfach verwenden (siehe Kapitel 3).

für die Marktkommunikation verwendeter E-Mail-Adresse nur ein Zertifikat gepflegt werden, ein sogenanntes „Kombizertifikat“ mit fortgeschrittener Signatur.

5.5.1 Zertifizierungsstellen

Das Zertifikat muss von einer Zertifizierungsstelle (engl. Certification Authority = CA) ausgestellt sein, die Zertifikate diskriminierungsfrei für Marktpartner der deutschen Energiewirtschaft anbietet. Es darf kein sogenanntes selbstausstelltes Zertifikat sein.¹¹

Die CA, von der das Zertifikat ausgestellt ist, muss den nachfolgenden Anforderungen genügen:¹²

- 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 zugänglich ist.

Darüber hinaus sollten insbesondere die folgenden Kriterien berücksichtigt werden:

- Die IT-Sicherheit des CA-Betriebs ist durch ein Audit / eine Zertifizierung nach einem anerkannten Audit / Zertifizierungs-Standard geprüft. Es wird eine Zertifizierung nach BSI TR-03145, Secure Certification Authority operation empfohlen.
- Der Registrierungsservice, einschließlich an Dienstleister (Registrare) ausgelagerter Service, erfolgt auf einem hohen Sicherheitsniveau.
- Die Vertrauenswürdigkeit des Betreibers und des Betriebs, auch unter Berücksichtigung von Eingriffsrechten Dritter, ist gegeben.
- Der Rechtsstand, insbesondere in Bezug auf das geltende Haftungs- und Datenschutzrecht genügt den Anforderungen des Unternehmens, dass das Zertifikat beantragt.

5.5.2 Zertifikate: Parameter und Anforderungen

Die Zertifikate müssen die nachfolgenden Anforderungen erfüllen¹³:

- Das Zertifikat muss von einer CA ausgestellt sein, die den unter Kapitel 5.5.1 genannten Anforderungen genügt.
- Alle bis zum 31.12.2017 ausgestellten Zertifikate sind mit den Signaturalgorithmen sha-256RSA oder sha-512RSA (Signaturverfahren RSASSA-PKCS1-v1_5) zu signieren. Ab dem 01.01.2018 bis zum 31.12.2018 neu ausgestellte Zertifikate sind entweder mit dem Signaturverfahren RSASSA-PKCS1-v1_5 (Signaturalgorithmen sha-256RSA oder sha-512RSA) oder RSASSA-PSS zu signieren, wobei bei der Verwendung von mit RSASSA-PSS signierten Zertifikaten zunächst beide beteiligten Marktpartner zustimmen müssen. Diese Zertifikate sind bis zur maximalen Zertifikatsgültigkeit (maximal 3 Jahre) im Interimsmodell der Marktkommunikation verwendbar.
- Alle ab dem 01.01.2019 neu ausgestellten Zertifikate müssen mit RSASSA-PSS signiert sein.
- Nach Ablauf von drei Monaten nachdem die Bundesnetzagentur per Mitteilung die Verfügbarkeit von mindestens drei Anbietern von RSASSA-PSS signierten Zertifikaten veröffentlicht, in jedem Fall aber spätestens ab dem 01.01.2019, müssen RSASSA-PSS-signierte Zertifikate von jedem Marktteilnehmer für die Verifikation unterstützt werden.
- Jedes Zertifikat muss Informationen für eine Rückrufprüfung enthalten, d. h. einen `CRLDistributionPoint`, unter dem jederzeit aktuelle CRL zur Verfügung stehen.
- Die Gültigkeit des Zertifikats darf maximal 3 Jahre betragen.
- Das Zertifikat muss mindestens die Verwendungszwecke Schlüsselverschlüsselung und digitale Signatur im Feld `KeyUsage` enthalten.

¹¹ Vgl. Absatz 5c bzw. 4c aus [2].

¹² Sinngemäß dem Kapitel 5.1.1 Zertifizierungsstellen/Vertrauensanker aus [1] entnommen.

¹³ Sinngemäß dem Kapitel 5.1.2 Zertifikate aus [1] entnommen und um 5b bzw. 4b aus [2] ergänzt.

- Für die verschiedenen, für die Marktkommunikation nötigen Anwendungszwecke „Signatur“ und „Verschlüsselung“ ist dasselbe Schlüsselpaar zu generieren und dementsprechend ein sogenanntes Kombizertifikat auszustellen und zu verwenden.
- Das Zertifikat muss eine fortgeschrittene elektronische Signatur ermöglichen.¹⁴
- Das Zertifikat muss eine Identifizierung und Zuordnung zum Unternehmen/Dienstleister oder zur Organisation gewährleisten, das 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 1:1 Kommunikationsadresse (Angabe der E-Mailadresse) befüllt werden.

Für den Austausch der öffentlichen Zertifikate gilt die Codierung:

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

5.5.3 Algorithmen und Schlüssellängen für S/MIME

Es sind folgende Algorithmen und Schlüssel mit den genannten Schlüssellängen zu verwenden¹⁵:

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

Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden:
RSASSA-PSS
(gemäß IETF RFC 4056).
Vom 01.06.2017 bis 31.12.2017 muss zur Wahrung der Interoperabilität unterstützt werden:
sha256RSA / sha512RSA
(RSASSA-PKCS1-v1_5)
Ab 01.01.2018 muss ausschließlich eingesetzt werden:
RSASSA-PSS
(gemäß IETF RFC 4056)

- Verschlüsselung:
 - Inhaltsverschlüsselung (Content encryption): AES-128 CBC oder AES-192 CBC
(gemäß IETF RFC 3565).
 - Schlüsselverschlüsselung (Key encryption): RSA Schlüssellänge mindestens 2048 Bit.

Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden:
RSAES-OAEP
(gemäß IETF RFC 3447).

¹⁴ Betreiber von CAs verwenden hierfür häufig den Begriff Zertifikate der „class 2“.

¹⁵ Sinngemäß dem Kapitel 3.2 Domainparameter und Schlüssellängen aus [1] entnommen.

Vom 01.06.2017 bis 31.12.2017 muss zur Wahrung der Interoperabilität unterstützt werden:
RSAES-PKCS1-v1_5
Ab 01.01.2018 muss ausschließlich eingesetzt werden:
RSAES-OAEP
(gemäß IETF RFC 3447). Die Schlüsselverschlüsselung hat Hashfunktionen als Parameter. Hierbei sind SHA-256 oder SHA-512 zu verwenden.

Ausnahmeregelung bis 31.12.2018:
Anstelle von SHA-256 oder SHA-512 darf als Parameter für die Schlüsselverschlüsselung befristet die Hashfunktion SHA-1 verwendet werden.

In den Implementierungen der RSA-Verschlüsselung sind geeignete Gegenmaßnahmen gegen Chosen-Ciphertext-Angriffe vorzusehen.¹⁶

5.5.4 Zertifikatswechsel und Sperrlisten

Spätestens 2 Wochen bevor ein Zertifikat abläuft muss der Inhaber dieses Zertifikats das Nachfolgezertifikat zur Verfügung gestellt haben (vgl. Kapitel 7). Somit entsteht ein Überlappungszeitintervall von mindestens 2 Wochen, in dem noch das alte und auch schon das neue Zertifikat gültig sind.

Innerhalb dieses Überlappungszeitraums kann bei allen Marktpartnern die Umstellung vom bisher genutzten auf das neue Zertifikat erfolgen. Der Zertifikatsinhaber darf das neue Zertifikat frühestens drei Werktage nach dem er es seinen Marktpartnern zur Verfügung gestellt hat zur Signierung verwenden. Jeder seiner Marktpartner kann eigenständig den Zeitpunkt innerhalb des Überlappungszeitraums festlegen, ab dem er das neue Zertifikat verwendet, um E-Mails an den Zertifikatsinhaber zu verschlüsseln.

Im Überlappungszeitraum müssen alle Marktpartner in der Lage sein, sowohl mit dem bisher genutzten als auch mit dem neuen Zertifikat signierte und verschlüsselte E-Mails zu verarbeiten, wobei für den Zertifikatsinhaber die vorgenannte Einschränkung gilt.

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

Will ein Zertifikatsinhaber sein Zertifikat vor Ablauf der Gültigkeitsfrist nicht mehr verwenden oder für ungültig erklären, so muss er sein Zertifikat über die Sperrlisten seines CA-Anbieters zurückziehen lassen.

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

¹⁶ Sinngemäß dem Kapitel 3.3 Weitere Vorgaben und 3.5 Übergangsregelungen aus [1] entnommen.

Ist eine CRL über die in den Zertifikaten veröffentlichten 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.

6 Regelungen für den Austausch via AS2

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

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

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

6.1 AS2-Adresse

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

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

6.1.1 AS2-ID

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

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

6.1.2 AS2-URL

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

6.2 Anforderungen an AS2-Zertifikate

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

Das AS2-Zertifikat dient der Signatur und Verschlüsselung.

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

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

6.3 Algorithmen und Schlüssellängen

Siehe Kapitel 5.5.3.

6.4 Transportschicht

Es müssen feste IP-Adressen verwendet werden. Es muss http über Port 80 angeboten werden, optional kann zusätzlich https mit Standardport 443 angeboten werden.¹⁷ Sofern https verwendet wird, muss zur Wahrung der Konformität mit der BSI TR-03116-4 mindestens TLS Version 1.2 oder höher verwendet werden.¹⁸

6.5 MDN (digitale Zustell-Quittung)

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

6.6 Betreff und Dateiname

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

¹⁷ 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.

¹⁸ Siehe Kapitel 2 Vorgaben SSL/TLS aus [1].

7 Organisatorische Regelungen zum Umgang mit Zertifikaten

Ein Marktpartner A kann nur dann eine E-Mail verschlüsselt an einen Marktpartner B versenden, wenn Marktpartner B ein gültiges Zertifikat zur Verfügung stellt, das den unter Kapitel 5.5 genannten Anforderungen genügt. Daher gelten über diese technischen Anforderungen hinaus auch die nachfolgenden organisatorischen Regelungen:

- Sollte dem Marktpartner A kein Zertifikat vom Marktpartner B zur Verfügung gestellt werden, das den technischen Mindestanforderungen genügt um die E-Mail an den Marktpartner B verschlüsseln zu können (bzw. eine sichere AS2-Verbindung zu diesem herstellen zu können), so kann gemäß Kapitel 8 der EDIFACT-Datenaustausch durch Marktpartner A an Marktpartner B so lange unterbleiben, bis Marktpartner B ein entsprechendes Zertifikat zur Verfügung gestellt hat.
- Spätestens 2 Wochen bevor ein Zertifikat 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. Durch die Übermittlung des Zertifikats bzw. des Links zum direkten Download des benötigten Zertifikats an die in der BDEW bzw. DVGW Codenummern-Datenbank eingetragenen E-Mail-Adressen gilt das Zertifikat als ausgetauscht.
- Das auszutauschende Zertifikat ist vom Marktpartner als gzip-komprimierter Anhang zu versenden. Alternativ hierzu kann ein Link zum direkten Download des benötigten Zertifikates versendet werden.
- 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-Meldung gesendet, kann der Sender der Übertragungsdatei davon ausgehen, dass die Prüfung der Signatur und die Entschlüsselung der Übertragungsdatei erfolgreich waren.
- Die voranstehende Regel findet keine Anwendung für den Fall, dass der Empfänger nicht in der Lage war, die Signatur einer fehlerfrei signierten und verschlüsselten E-Mail zu prüfen, bzw. diese zu entschlüsseln (z. B. aufgrund technischer Probleme). In diesem Fall ist die angefügte Übertragungsdatei (insbesondere bezüglich der Fristen) vom Empfänger so zu behandeln, als hätte das Problem beim Empfänger nicht bestanden.
- Sobald ein Zertifikat gesperrt oder ungültig ist und noch kein gültiges Nachfolgezertifikat vorliegt, dürfen keine Übertragungsdateien mehr verarbeitet werden, die von der E-Mail-Adresse stammen und mit dem gesperrten oder ungültigen Zertifikat signiert sind. Bei Nutzung von AS2 können keine Übertragungsdateien ausgetauscht werden, wenn gesperrte oder ungültige Zertifikate eingesetzt werden.
Der Marktpartner, dessen Zertifikat gesperrt oder ungültig ist, hat unverzüglich ein neues Zertifikat zu beschaffen und muss es an alle seine Marktkommunikationspartner verteilen.

8 Konsequenzen bei Nicht-Einhaltung dieser Vorgaben

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

8.1 Beim Übertragungsweg E-Mail:

Verstoßvariante 1: Der Sender hat vom Empfänger kein gültiges Zertifikat zur Verfügung gestellt bekommen.

Somit kann der Sender die E-Mail nicht verschlüsseln.

Verfahrensweise: Der Sender ist berechtigt, die Kommunikation nicht durchzuführen. Sofern der Empfänger ein Netzbetreiber ist, ist zusätzlich eine Beschwerde bei der Bundesnetzagentur zulässig. Die Konsequenzen einer ausbleibenden Kommunikation sind von demjenigen Marktpartner zu tragen, der die Verantwortung hat, das Zertifikat zur Verfügung zu stellen. 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 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 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 Marktpartners erfolgt anhand der Marktpartner-ID im Betreff der E-Mail.

Verstoßvariante 3: Der Empfänger erhält eine verschlüsselte E-Mail, die mit einem Schlüssel ver-

schlüsselt 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 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 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 Marktpartners erfolgt anhand der Marktpartner-ID im Betreff der E-Mail.

Verstoßvariante 4: Der Empfänger erhält eine nicht verschlüsselte, aber gültig signierte E-Mail. Somit war die Übertragungsdatei nicht gegen fremde Einsichtnahme geschützt, der Inhalt der Übertragungsdatei und Sender der Nachricht sind jedoch nicht abstreitbar.

Verfahrensweise: Der Empfänger ist berechtigt, die Verarbeitung der betreffenden Übertragungsdatei zu verweigern. Die Konsequenzen dieser nicht-Verarbeitung sind vom Sender zu tragen. Der Empfänger hat den Sender (Verursacher) insgesamt mindestens einmal 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 Marktpartners erfolgt anhand der Marktpartner-ID im Betreff der E-Mail.

8.2 Beim Übertragungsweg per AS2:

Verstoßvariante 1: Der Empfänger hat dem Sender kein gültiges Zertifikat zur Verfügung gestellt. Somit kann der Sender die Übertragungsdatei nicht verschlüsseln.

Verfahrensweise: Der Sender ist berechtigt, die Kommunikation nicht durchzuführen. Sofern der Empfänger ein Netzbetreiber ist, ist zusätzlich eine Beschwerde bei der Bundesnetzagentur zuläs-

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

Die Information ist mindestens an die in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional an eine z. B. über Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden.

Verstoßvariante 2: Der Empfänger erhält eine Übertragungsdatei,

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

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

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

Hinweis: Die Informationsmeldung vom Empfänger an den Verursacher (Sender) erfolgt einmalig auf Basis einer exemplarisch ausgewählten Übertragungsdatei. Die Selektion aller betroffenen Übertragungsdateien wird vom Verursacher an Hand der fehlenden CONTRL-Meldungen zusammengeführt. Die Information ist mindestens an die in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegte E-Mailadresse sowie optional an eine z. B. über Kontaktdatenblatt ausgetauschte E-Mailadresse des Marktpartners zu senden. Die Zuordnung des Marktpartners 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 Marktpartners 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 Marktpartners erfolgt anhand der AS2-ID.

9 Quellen

- [1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, vom 23. Februar 2016.
- [2] BK6-16-200 und BK7-16-142, Beschluss zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, vom 20. Dezember 2016.
- [3] BK6-16-200 und BK7-16-142, Festlegungsverfahren zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, Mitteilung Nr. 3 vom 16. Mai 2017.
- [4] BK6-16-200 und BK7-16-142, Festlegungsverfahren zur Anpassung der Vorgaben zur elektronischen Marktkommunikation an die Erfordernisse des Gesetzes zur Digitalisierung der Energiewende, Mitteilung Nr. 7 vom 12. Dezember 2017.

10 Ansprechpartner

Kay Tidten

E-Mail: kay.tidten@bdew.de

Telefon: +49 30 300 199 1526

11 Änderungshistorie

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

Version 1.0a

Änd-ID	Ort	Fehlerkorrektur / Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
12029	Kapitel 5.5 Verschlüsselung und Signatur von E-Mails	<ul style="list-style-type: none"> ▪ Das Verschlüsseln und Signieren von E-Mails ist ausschließlich nach dem S/MIME-Standard gestattet. Es muss mindestens die Version 3.2 (IETF RFC 5751, Veröffentlichungsjahr 2010) verwendet werden. Die Verwendung eines qualifizierten Signaturzertifikates innerhalb von S/MIME ist technisch nicht möglich. ▪ Jeder Marktpartner muss für die 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 verschlüsselt gesendeten E-Mail wird der gleiche private Schlüssel genutzt. Umgekehrt müssen Zertifikate der Marktpartner (je eines, je E-Mail-Adresse) sowohl zur Verschlüsselung als auch zur Signaturprüfung verwendet werden. Auf diese Weise muss je vom Marktpartner für die Marktkommunikation verwendeter E-Mail-Adresse nur ein Zertifikat gepflegt werden. 	<ul style="list-style-type: none"> ▪ Das Verschlüsseln und Signieren von E-Mails ist ausschließlich nach dem S/MIME-Standard gestattet. Es muss mindestens die Version 3.2 (IETF RFC 5751, Veröffentlichungsjahr 2010) verwendet werden. ▪ Jeder Marktpartner muss für die 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 verschlüsselt gesendeten E-Mail wird der gleiche private Schlüssel genutzt. Umgekehrt müssen Zertifikate der Marktpartner (je eines, je E-Mail-Adresse) sowohl zur Verschlüsselung als auch zur Signaturprüfung verwendet werden. Auf diese Weise muss je vom Marktpartner für die Marktkommunikation verwendeter E-Mail-Adresse nur ein Zertifikat gepflegt werden, ein sogenanntes „Kombizertifikat“ mit fortgeschrittener Signatur. 	Klarstellung der Anforderung, dass keine qualifizierten Signaturzertifikate genutzt werden.	Fehler (08.05.2017)

Änd-ID	Ort	Fehlerkorrektur / Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
12030	Kapitel 5.5.1 Zertifizierungsstellen	<p>Die CA, von der das Zertifikat ausgestellt ist, muss den nachfolgenden Anforderungen genügen:</p> <ul style="list-style-type: none"> - 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. - Die CA verfügt über einen Rückrufservice, über den Zertifikate widerrufen werden können. Dazu führt es eine sogenannte Zertifikatsperrliste (englisch certificate revocation list, CRL), welche öffentlich zugänglich ist. - Der Rechtsstand, insbesondere in Bezug auf das geltende Haftungs- und Datenschutzrecht genügt den Anforderungen des Unternehmens, dass das Zertifikat beantragt. 	<p>Die CA, von der das Zertifikat ausgestellt ist, muss den nachfolgenden Anforderungen genügen:</p> <ul style="list-style-type: none"> - Die CA verfügt über einen Rückrufservice, über den Zertifikate widerrufen werden können. Dazu führt es eine sogenannte Zertifikatsperrliste (englisch certificate revocation list, CRL), welche öffentlich zugänglich ist. <p>Darüber hinaus sollten insbesondere die folgenden Kriterien berücksichtigt werden:</p> <ul style="list-style-type: none"> - Die IT-Sicherheit des CA-Betriebs ist durch ein Audit / eine Zertifizierung nach einem anerkannten Audit / Zertifizierungs-Standard geprüft. Es wird eine Zertifizierung nach BSI TR-03145, Secure Certification Authority operation empfohlen. - Der Registrierungsservice, einschließlich an Dienstleister (Registrare) ausgelagerter Service, erfolgt auf einem hohen Sicherheitsniveau. - Die Vertrauenswürdigkeit des Betreibers und des Betriebs, auch unter Berücksichtigung von Eingriffsrechten Dritter, ist gegeben. - Der Rechtsstand, insbesondere in Bezug auf das geltende Haftungs- und Datenschutzrecht genügt den Anforderungen des Unternehmens, dass das Zertifikat beantragt. 	Angleichung an Formulierung in [1]	Fehler (08.05.2017)

Änd-ID	Ort	Fehlerkorrektur / Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
12031	Kapitel 5.5.2 5.5.2 Zertifikate: Parameter und Anforderungen	<ul style="list-style-type: none"> [...] von einer CA ausgestellt sein, die den unter Kapitel 5.5.1 genannten Anforderungen genügt. Jedes Zertifikat muss Informationen für eine Rückrufprüfung enthalten [...] 	<ul style="list-style-type: none"> [...] von einer CA ausgestellt sein, die den unter Kapitel 5.5.1 genannten Anforderungen genügt. Alle bis zum 31.12.2017 ausgestellten Zertifikate sind mit den Signaturalgorithmen sha-256RSA oder sha-512RSA (Signaturverfahren RSASSA-PKCS1-v1_5) zu signieren. Sie sind bis zur maximalen Zertifikatsgültigkeit (maximal 3 Jahre) im Interimsmodell der Marktkommunikation verwendbar. Alle ab dem 01.01.2018 neu ausgestellten Zertifikate müssen mit RSASSA-PSS signiert sein.^{xx} Jedes Zertifikat muss Informationen für eine Rückrufprüfung enthalten [...] <p>Fußnote: xx Das hiergenannte Datum kann verschoben werden, wenn keine ausreichende Anzahl an öffentlichen Zertifizierungsstellen Zertifikate ausstellen, die diese Anforderungen erfüllen.</p>	Klarstellung, dass bis zum 31.12.2017 ausgestellte Zertifikate weiterhin mit den gängigen Signaturalgorithmen sha256RSA oder sha512RSA signiert werden sollen.	Fehler (08.05.2017)
12032	Kapitel 5.5.2 Zertifikate:Parameter und Anforderungen	Das Zertifikat muss beide Verwendungszwecke (Verschlüsselung und Signatur) im Feld KeyUsage enthalten.	Das Zertifikat muss mindestens die Verwendungszwecke Schlüsselverschlüsselung und digitale Signatur im Feld KeyUsage enthalten.	Dopplung in Kapitel 5.5.2 und 5.5.3 beseitigt	Fehler (08.05.2017)
12033	Kapitel 5.5.3 Algorithmen und Schlüssellängen	5.5.3 Algorithmen und Schlüssellängen	5.5.3 Algorithmen und Schlüssellängen für S/MIME	Präzisierung, dass sich diese Anforderungen auf S/MIME beziehen, und nicht auf das Zertifikat	Fehler (08.05.2017)
12034	Kapitel 5.5.3 Algorithmen und Schlüssellängen	Signaturverfahren (Signature algorithm) RSASSA-PSS (gemäß IETF RFC 4056)	Signaturverfahren (Signature algorithm): Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden: RSASSA-PSS (gemäß IETF RFC 4056). Vom 01.06.2017 bis 31.12.2017 muss zur Wahrung der Interoperabilität unterstützt werden: sha256RSA oder sha512RSA (RSASSA-PKCS1-v1_5) Ab 01.01.2018 muss ausschließlich eingesetzt werden: RSASSA-PSS (gemäß IETF RFC 4056)	Ermöglichung einer Übergangsfrist in Abstimmung mit dem BSI bis zum 31.12.2017.	Fehler (08.05.2017)

Änd-ID	Ort	Fehlerkorrektur / Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
12035	Kapitel 5.5.3 Algorithmen und Schlüssellängen	Schlüsselverschlüsselung (Key encryption): RSAES-OAEP (gemäß IETF RFC 3447)	Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden: RSAES-OAEP (gemäß IETF RFC 3447). Vom 01.06.2017 bis 31.12.2017 muss zur Wahrung der Interoperabilität unterstützt werden: RSAES-PKCS1-v1_5 Ab 01.01.2018 muss ausschließlich eingesetzt werden: RSAES-OAEP (gemäß IETF RFC 3447)	Ermöglichung einer Übergangsfrist in Abstimmung mit dem BSI bis zum 31.12.2017.	Fehler (08.05.2017)
12036	Kapitel 5.5.3 Algorithmen und Schlüssellängen	Schlüsselnutzung (Key-Usage): Digitale Signatur, Schlüsselverschlüsselung	In den Implementierungen der RSA-Verschlüsselung sind geeignete Gegenmaßnahmen gegen Chosen-Ciphertext-Angriffe vorzusehen.	Schlüsselnutzung aus Konsistenzgründen verschoben in Kapitel 5.5.2, Hinweis auf Maßnahmen gegen Chosen-Ciphertext-Angriffe aus [1] aufgenommen.	Fehler (08.05.2017)
12037	Kapitel 5.5.2 Zertifikate: Parameter und Anforderungen	Alle bis zum 31.12.2017 ausgestellten Zertifikate sind mit den Signaturalgorithmen sha-256RSA oder sha-512RSA (Signaturverfahren RSASSA-PKCS1-v1_5) zu signieren. Sie sind bis zur maximalen Zertifikatsgültigkeit (maximal 3 Jahre) im Interimsmodell der Marktkommunikation verwendbar. Alle ab dem 01.01.2018 neu ausgestellten Zertifikate müssen mit RSASSA-PSS signiert sein. ^{xx} Fußnote xx Das hiergenannte Datum kann verschoben werden, wenn keine ausreichende Anzahl an öffentlichen Zertifizierungsstellen Zertifikate ausstellen, die diese Anforderungen erfüllen.	Alle bis zum 31.12.2017 ausgestellten Zertifikate sind mit den Signaturalgorithmen sha-256RSA oder sha-512RSA (Signaturverfahren RSASSA-PKCS1-v1_5) zu signieren. Ab dem 01.01.2018 bis zum 31.12.2018 neu ausgestellte Zertifikate sind entweder mit dem Signaturverfahren RSASSA-PKCS1-v1_5 (Signaturalgorithmen sha-256RSA oder sha-512RSA) oder RSASSA-PSS zu signieren, wobei bei der Verwendung von mit RSASSA-PSS signierten Zertifikaten zunächst beide beteiligten Marktpartner zustimmen müssen. Diese Zertifikate sind bis zur maximalen Zertifikatsgültigkeit (maximal 3 Jahre) im Interimsmodell der Marktkommunikation verwendbar. Alle ab dem 01.01.2019 neu ausgestellten Zertifikate müssen mit RSASSA-PSS signiert sein. Nach Ablauf von drei Monaten nachdem die Bundesnetzagentur per Mitteilung die Verfügbarkeit von mindestens drei Anbietern von RSASSA-PSS signierten Zertifikaten veröffentlicht, in jedem Fall aber spätestens ab dem 01.01.2019, müssen RSASSA-PSS-signierte Zertifikate von jedem Marktteilnehmer für die Verifikation unterstützt werden. xx: <u>gelöscht</u>	Aktualisierung der Übergangsregelung durch die BNetzA Mitteilung [4].	Fehler (12.12.2017)

Änd-ID	Ort	Fehlerkorrektur / Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
12038	Kapitel 5.5.2 Zertifikate: Parameter und Anforderungen	Das Zertifikat muss eine fortgeschrittene elektronische Signatur ermöglichen. ^{xx} Fußnote xx: Die EU-Verordnung eIDAS benutzt hierfür den Begriff „fortgeschrittenes Siegel“; Betreiber von CAs oft Zertifikate der „class 2“.	Das Zertifikat muss eine fortgeschrittene elektronische Signatur ermöglichen. ^{xx} Fußnote xx: Betreiber von CAs verwenden hierfür häufig den Begriff Zertifikate der „class 2“.	Anpassung an Formulierung der BNetzA Festlegung BK6-16-200 vom 20.12.2016 [2]	Fehler (12.12.2017)
12039	Kapitel 5.5.3 Algorithmen und Schlüssellängen für S/MIME	- Signaturverfahren (Signature algorithm): Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden: (...) RSA Schlüssellänge mindestens 2048 Bit (...) - Schlüsselverschlüsselung (Key encryption): Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden: (...) RSA Schlüssellänge mindestens 2048 Bit	- Signaturverfahren (Signature algorithm): RSA Schlüssellänge mindestens 2048 Bit (...) Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden: (...) - Schlüsselverschlüsselung (Key encryption): RSA Schlüssellänge mindestens 2048 Bit Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden: (...)	Redaktionelle Änderung, Anpassung der Reihenfolge für bessere Lesbarkeit	Fehler (12.12.2017)
12040	Kapitel 5.5.3 Algorithmen und Schlüssellängen für S/MIME	- Schlüsselverschlüsselung (Key encryption): (...) Ab 01.01.2018 muss ausschließlich eingesetzt werden: RSAES-OAEP (gemäß IETF RFC 3447)	- Schlüsselverschlüsselung (Key encryption): (...) Ab 01.01.2018 muss ausschließlich eingesetzt werden: RSAES-OAEP (gemäß IETF RFC 3447). Die Schlüsselverschlüsselung hat Hashfunktionen als Parameter. Hierbei sind SHA-256 oder SHA-512 zu verwenden. Ausnahmeregelung bis 31.12.2018: Anstelle von SHA-256 oder SHA-512 darf als Parameter für die Schlüsselverschlüsselung befristet die Hashfunktion SHA-1 verwendet werden.	Konkretisierung aufgrund BNetzA Mitteilung [4]	Fehler (12.12.2017)

12 Anhang 1: AS2-Steckbrief Version 2

Unternehmensname des Marktpartners laut Handelsregister	<Name>	
Marktpartner-ID und Marktrolle	<MP-ID>	<Marktrolle>
Marktpartner-ID und Marktrolle (weitere optional)	ggf. weitere <MP-ID>	ggf. weitere <Marktrolle>
Marktpartner-ID und Marktrolle (weitere optional)	ggf. weitere <MP-ID>	ggf. weitere <Marktrolle>
Marktpartner-ID und Marktrolle (weitere optional)	ggf. weitere <MP-ID>	ggf. weitere <Marktrolle>
Kontakt Marktpartner AS2		
1. Ansprechpartner		
Name	<Nachname>, <Vorname>	
Telefon	<Telefonnummer>	
E-Mail	<E-Mail-Adresse>	
2. Ansprechpartner		
Name	<Nachname>, <Vorname>	
Telefon	<Telefonnummer>	
E-Mail	<E-Mail-Adresse>	
Kontakt Technik AS2		
1. Ansprechpartner		
Name	<Nachname>, <Vorname>	
Telefon	<Telefonnummer>	
E-Mail	<E-Mail-Adresse>	
2. Ansprechpartner		
Name	<Nachname>, <Vorname>	
Telefon	<Telefonnummer>	
E-Mail	<E-Mail-Adresse>	
3. Ansprechpartner		
Name	<Nachname>, <Vorname>	
Telefon	<Telefonnummer>	
E-Mail	<E-Mail-Adresse>	

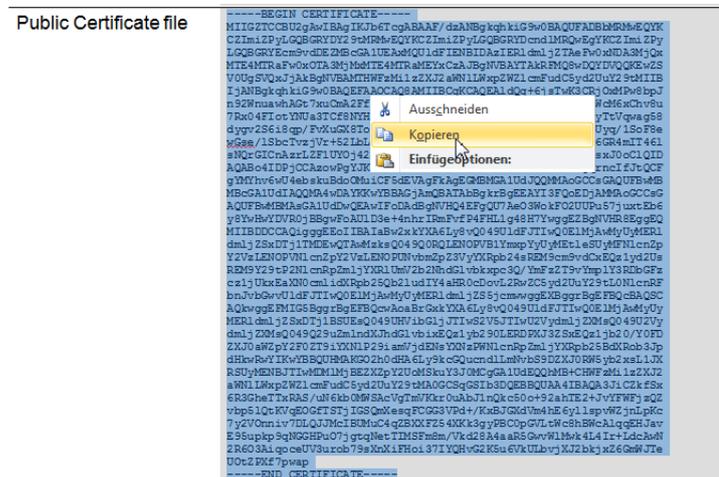
Netzwerk	
AS2-URL	http:// xxx.com/xxx
IP-Adresse (Firewall)	xxx.xxx.xxx.xx
IP Port (Firewall)	80 (Standard http)
Zusätzliche Absender-IP-Adresse (optional)	-/-
AS2-Zertifikat	
AS2-ID	Als AS2-ID ist die MP-ID zu verwenden. Für welche MP-ID das nachfolgend genannte Zertifikat verwendet wird, ergibt sich anhand der auf der vorherigen Seite genannten MI-IDs.
Öffentliche AS2-Zertifikat	<pre> -----BEGIN CERTIFICATE----- <String des Zertifikats> -----END CERTIFICATE----- </pre>
AS2-Parameter	
MDN Mode	Synchron
MDN Signed	Ja
Komprimierung	Ja
Content-Type	Binary
RSA Signaturschemata	RSASSSA-PPS (ab 01.01.2018)
Signatur-Hash-Algorithmus	SHA-256 oder SHA-512
RSA Schlüsselverschlüsselungs-Algorithmus	RSAES-OAEP (ab 01.01.2018)
Datenverschlüsselungs-Algorithmus	AES-128 CBC oder AES-192 CBC

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

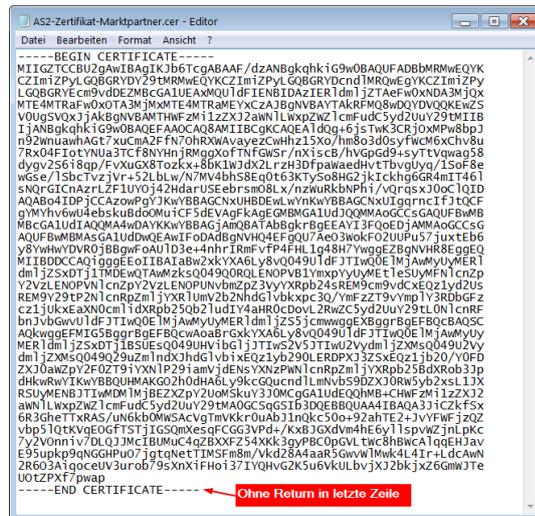
13 Anhang 2: Erzeugung eines Zertifikats (cer-Datei) aus dem AS2-Steckbrief

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

- 1) Text aus dem AS2-Steckbrief kopieren:



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



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

