Anlage 5 zum Beschluss
BK6-16-200

EDI@Energy – Regelungen zum Übertragungsweg -Konzept-

Regelungen zum sicheren Austausch von EDIFACT-Übertragungsdateien

Version:	1.0
Publikationsdatum:	01.10.2016
Autor:	BDEW

Inhaltsverzeichnis

1 Einführung

Dieses Dokument regelt die Sicherheits- und Schutzmechanismen, die im Rahmen des elektronischen Datenaustauschs zwischen den Marktteilnehmern der deutschen Energiewirtschaft für die Übertragungswege[1] AS2 und E-Mail via SMTP in der aktuellen Prozesswelt und im sogenannten Interimsmodell und zu den bereits etablierten Datenaustauschprozessen 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 und WiM.

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

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-Kalender[2]) nach erstmaliger Kontaktaufnahme eines Marktteilnehmers 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 Marktteilnehmers 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 EDIFACT-Übertragungswegs abgelehnt werden, gelten als fristgerecht zugestellt. Der Empfänger ist in diesem Fall verpflichtet, diese entsprechend des ursprünglichen Empfangsdatums zu prozessieren[3]. Diese Regelung gilt ausschließlich für fehlerfreie EDIFACT-Übertragungsdateien.

Der EDIFACT-Übertragungsweg zwischen zwei Marktpartnern ist mindestens für drei Jahre ab dem Tage nach dem letzten Datenaustausch (zwischen diesen beiden Marktpartnern) aufrecht zu

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

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

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

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 in den BDEW- bzw. DVGW-Codenummerndatenbanken hinterlegt sind.

Eine Aufrechterhaltung des EDIFACT-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 kostenneutral 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. Grundidee der 1:1-Kommunikation ist, dass ein Marktteilnehmer dafür zu sorgen hat, dass seine internen Organisationsstrukturen bei den anderen Marktteilnehmern 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.

Eine EDIFACT-Übertragungsdatei, die von einer anderen E-Mail-Adresse als der vereinbarten E-Mail-Adresse versandt wird, muss vom Empfänger nicht verarbeitet[4] werden. Sie gilt dementsprechend als nicht zugestellt. Die sich daraus ergebenden Konsequenzen hat der Versender der E-Mail zu tragen.

Die 1:1-Adressierung gilt unabhängig vom Übertragungsweg, z. B. AS2. Zwischen zwei Marktpartnern darf für alle EDIFACT-Übertragungsdateien nur ein Übertragungsweg genutzt werden.

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

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 Marktteilnehmer, der E-Mails mit Geschäftskorrespondenz an die für den Austausch von EDIFACT-Übertragungsdateien festgelegte E-Mail-Adresse eines anderen Marktteilnehmers sendet, kann nicht erwarten, dass diese E-Mails gelesen oder gar beantwortet werden. Er muss davon ausgehen, dass die mitgeschickten 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.
- Soll die EDIFACT-Übertragungsdatei komprimiert werden, so ist dafür die gzip-Komprimierung[5] 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.

[5] gzip ist plattformunabhängig.

- 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. Dabei sind die in diesem Kapitel genannten Regelungen einzuhalten:

- Im Sinne der 1:1-Kommunikation ist der Datenaustausch geschäftsprozessunspezifisch zu betreiben, d. h. die Verschlüsselung und Signatur der E-Mail erfolgt für alle Nachrichtentypen[6] 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 3.1 (RFC 3851, Veröffentlichungsjahr 2004) verwendet werden. Die Verwendung eines qualifizierten Signaturzertifikates innerhalb von S/MIME ist technisch nicht möglich.
- Das Zertifikat muss beide Verwendungszwecke (Verschlüsselung und Signatur) im Feld `KeyUsage` enthalten.
- Jeder Marktpartner muss für die von ihm genutzte E-Mail-Adresse[7] 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 fortgeschrittenes Zertifikat gepflegt werden.

5.5.1 Zertifizierungsstellen

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

[6] 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).

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

- Die CA, von der das Zertifikat ausgestellt ist, muss den nachfolgenden Anforderungen genügen[8]:
  - 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 zugängig ist.
  - Der Rechtsstand, insbesondere in Bezug auf das geltende Haftungs- und Datenschutzrecht genügt den Anforderungen des Unternehmens, dass das Zertifikat beantragt.

5.5.2 Parameter der und weitere Anforderungen an die Zertifikate

Die Zertifikate müssen die nachfolgenden Anforderungen erfüllen[9]:

- Das Zertifikat muss von einer CA ausgestellt sein, die den unter Kapitel 5.5.1 genannten Anforderungen genügt.
- 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.
- Für die verschiedenen, für die Marktkommunikation nötigen Anwendungszwecke „Signatur“ und „Verschlüsselung“ ist dasselbe Schlüsselpaar zu generieren und dementsprechend ein sog. Kombizertifikat auszustellen und zu verwenden.
- Das Zertifikat muss eine fortgeschrittene elektronische Signatur ermöglichen.
- 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.

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

Es sind die folgenden Algorithmen und Schlüssel mit den genannten Schlüssellängen zu verwenden[10]:

- Signatur:
  - Hash algorithm (Hashalgorithmus): SHA-256 oder SHA-512
  - Signature algorithm (Signaturalgorithmus): RSA with SHA-256 oder RSA with SHA-512

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

[9] Vieles sinngemäß dem Kapitel 5.1.2 Zertifikate aus [1] entnommen.

[10] Die Anforderungen orientieren sich an den in [2] getroffenen Aussagen.

- Verschlüsselung:
  - Key encryption (Schlüsselverschlüsselung): RSA
  - Content encryption (Inhalteverschlüsselung): AES-128 oder AES-192
- RSA key length (RSA Schlüssellänge): mindestens 2048 Bit
- Key-Usage (Schlüsselnutzung): Digitale Signatur, Schlüsselverschlüsselung

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.

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 über RFC 4130 standardisiert. Dieses Kapitel nimmt Festlegungen zur Konfiguration und Anwendung auf dieser Basis vor.

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 Transportschicht

Es müssen feste IP-Adressen verwendet werden. Es ist ausschließlich der http-Standardport 80 anzuwenden.[11]

6.4 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.

6.5 Betreff und Dateiname

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

[11] 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.

7 Organisatorische Regelungen zum Umgang mit Zertifikaten

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

- Sollte dem Marktpartner A kein Zertifikat vom Marktpartner B zur Verfügung gestellt werden, das den technischen Mindestanforderungen genügt um die E-Mail an den Marktpartner B verschlüsseln zu können (bzw. eine sichere AS2-Verbindung zu diesem herstellen zu können), so unterbleibt der EDIFACT-Datenaustausch durch Marktpartner A an Marktpartner B so lange, 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 der Zertifikate bzw. der Links zum Download an die in der BDEW bzw. DVGW Codenummern-Datenbank eingetragenen E-Mail-Adressen gelten die Zertifikate als ausgetauscht.
- Die auszutauschenden Zertifikate sind vom Marktpartner als gzip-komprimierter Anhang zu versenden. Alternativ hierzu kann ein Link zum Download des 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 Quellen

[1] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, vom 23. Februar 2016.

[2] Signatur nach dem Signaturgesetz und der Signaturverordnung, (Übersicht über geeignete Algorithmen), vom 9.12.2015; auf der Seite der Bundesnetzagentur als Algorithmenkatalog 2016 bezeichnet.

9 Ansprechpartner

Kay Tidten
E-Mail: kay.tidten@bdew.de
Telefon: +49 30 300 199 1526

Anhang 1: AS2-Steckbrief Version 2

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

Kontakt Marktpartner AS2

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

Kontakt Technik AS2

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

Netzwerk		
AS2-URL		http://***xxx.com/xxx***
IP-Adresse	(Firewall)	***xxx.xxx.xxx.xx***
IP Port	(Firewall)	80 (Standard http)
Zusätzliche Absender-IP-Adresse (optional)		-/-
AS2-Zertifikat		
AS2-ID		Als AS2-ID ist die MP-ID zu verwenden. Für welche MP-ID das nachfolgend genannte Zertifikat verwendet wird, ergibt sich anhand der auf der vorherigen Seite genannten MI-IDs.
Öffentliche AS2-Zertifikat		-----BEGIN CERTIFICATE----- ***<String des Zertifikats>*** -----END CERTIFICATE-----
AS2-Parameter		
MDN Mode		Synchron
MDN Signed		Ja
Signaturalgorithmus		<SHA-256 | SHA-512>[12]
Verschlüsselungsalgorithmus		<AES-128 | AES-192>[13]
Komprimierung		Ja
Content-Type		Binary

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

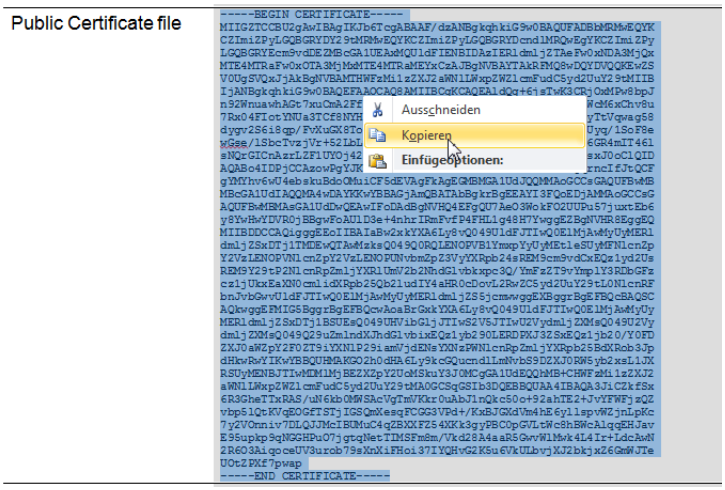
[12] Als Signaturalgorithmus ist entweder SHA-256 oder SHA-512 auszuwählen. Der ausgewählte Signaturalgorithmus ist in dieses Feld einzutragen.

[13] Als Verschlüsselungsalgorithmus ist entweder AES-128 oder AES-192 auszuwählen. Der ausgewählte Verschlüsselungsalgorithmus ist in dieses Feld einzutragen.

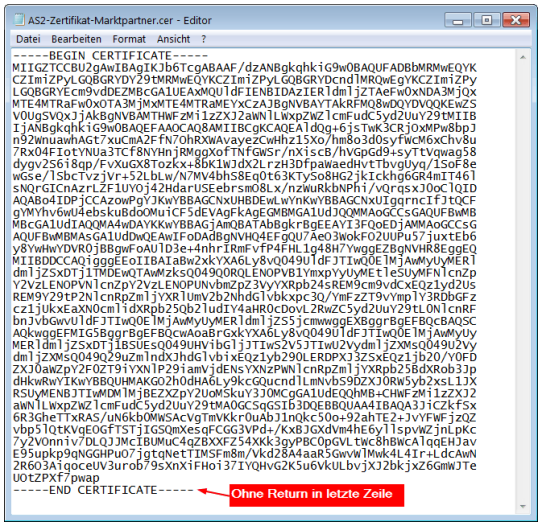
Anhang 2: Erzeugung eines Zertifikats (cer-Datei) aus dem AS2-Steckbrief

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: