Regelungen zum Übertragungsweg für AS4

Regelungen zum sicheren Austausch von EDIFACT-Übertragungsdateien

Version:	2.0
Publikationsdatum:	01.06.2022
Anzuwenden ab:	
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 den Übertragungsweg[1] AS4 in der Marktkommunikation einzuhalten sind.

Gemäß BNetzA-Beschluss[2] sind grundsätzlich die kryptographischen Vorgaben der BSI TR 03116-3 anzuwenden und einzuhalten, sowie die Nutzung der Smart Metering-PKI des BSI, nach § 52 Abs. 4 MsbG vorzusehen.

Die zu nutzenden Parameter und hiervon anzuwendenden Abweichungen sind in diesem Dokument insoweit beschrieben, insofern diese nicht die Certificate Policy der SM-PKI betreffen, da diese in der aktuell vorliegenden Version die Anforderungen noch nicht berücksichtigt.

1.1 Regelungsumfang

Die nachfolgenden Regeln finden Anwendung auf folgende von der BNetzA festgelegten Marktprozesse[3] Medium Strom, die per EDIFACT abgewickelt werden: GPKE, MPES, MaBiS und WiM.

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.[4]

Aktuell gelten somit die nachfolgenden Regelungen zum Übertragungsweg AS4, welche auch die damit verbundenen organisatorischen Regelungen für die deutsche Energiewirtschaft enthalten.

1.2 Struktur des Dokuments

Soweit nicht anders gekennzeichnet, gelten die Regelungen für den Datenaustausch im Rahmen der Marktprozesse.

1.3 Einführung und Abgrenzung

Die in diesem Dokument benannten Regelungen sind von allen Teilnehmern am elektronischen Datenaustausch zu den unter Kapitel 1.1 genannten Prozessen bis zum 01.10.2023 umzusetzen und der Empfang von Nachrichtendateien zu ermöglichen.

Vor und während des Zeitraums der gestuften Einführung der AS4 Kommunikation in den Marktprozessen, vom 01.10.2023 bis zum 01.04.2024, gelten vorrübergehend zwei unterschiedliche Versionen der Regelungen zum Übertragungsweg gleichzeitig:

---

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

[2] Vgl. BK6-21-282 [1].

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

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

› E-Mail oder AS2 Kommunikation:
„Regelungen zum Übertragungsweg“ mit der Ordnungsnummer **/ Version 1.x**
Diese Version der Regelungen zum Übertragungsweg beschreiben den Austausch von Nachrichten im Rahmen der Marktprozesse über die Übertragungswege E-Mail oder AS2. Sie bleiben für die Marktprozesse in ihrer jeweils aktuellen veröffentlichten Fassung gültig.
Sie sind für die Marktprozesse längstens bis zum 31.03.2024 für die Übertragungswege E-Mail oder AS2 anzuwenden.

› AS4 Kommunikation:
„Regelungen zum Übertragungsweg“ mit der Ordnungsnummer / **Version 2.x**
(dieses Dokument)
Diese Version der Regelungen zum Übertragungsweg und ihre Nachfolgefassungen beschreiben den Austausch von EDIFACT-Übertragungsdateien im Rahmen der Marktprozesse über einen AS4 Web Service. Sie sind für die Marktprozesse spätestens ab dem 01.04.2024 anzuwenden.

Nach BNetzA-Beschluss[5] ist die Nutzung anderer Übertragungswege für die unter Kapitel 1.1 genannten Prozesse nach dem 01.04.2024 nicht mehr zulässig.

2 Bekanntmachen beim Informationsempfänger

Um beim Datenaustausch eine größtmögliche Automatisierung zu erreichen, müssen sich die Marktpartner vor dem erstmaligen Datenversand unter anderem über die Datenaustauschadressen inklusive der zu verwendenden Zertifikate verständigen. Das ist mindestens die URL des AS4-Webservice-Aufrufs (AS4 Adresse) sowie das Zertifikat mit dem öffentlichen Schlüssel zum Verschlüsseln einer Nachrichtenübertragungsdatei für den Nachrichtenempfänger[6].

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

---

[5] Vgl. BK6-21-282 [1].

[6] Die öffentlichen Schlüssel nebst Zertifikaten zum Validieren der Signatur bzw. zum Aufbau des TLS-Kanals müssen nicht vorab ausgetauscht werden. Das Signaturzertifikat ist in jeder AS4 Nachricht enthalten, das Zertifikat für den Aufbau des TLS Kanals wird während des Verbindungsaufbaus ausgetauscht.

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

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.

Eine Aufrechterhaltung des Übertragungswegs bedeutet nicht, dass eine AS4-Adresse, die für den Datenaustausch verwendet und durch eine andere AS4-Adresse ersetzt wurde, drei Jahre lang nicht gelöscht werden darf.

2.1 Initialer Austausch der Kommunikationsparameter

Es wird empfohlen, die Codenummerndatenbank für das Medium Strom[8] Zurverfügungstellung der Kommunikationsdaten zu nutzen. Dabei sollte die genutzte CA (mit der URL für den Zertifikatsabruf) und die URL für den AS4-Webservice hinterlegt werden. Eingabe und Einsicht in die in der Codenummerndatenbank hinterlegten Daten sind kostenlos.

Der Austausch der Kommunikationsparameter kann nach erstmaliger Kontaktaufnahme aber auch per Telefon oder E-Mail erfolgen.

2.2 Aktualisierung der Kommunikationsparameter

Sollten die Kommunikationsparameter in der BDEW- bzw. DVGW-Codenummerndatenbank hinterlegt sein, so reicht eine einfache Information über E-Mail über die geänderten Daten. Eine Information der Marktpartner über eine Änderung der URL für den Aufruf des AS4 Webservice oder aktualisierte Zertifikate nicht erforderlich.

Andernfalls werden Aktualisierungen wie folgt bekannt gemacht:

- Aktualisierte Zertifikate. Neue Zertifikate werden folgende Maßen bekannt gemacht:

  Alle Marktpartner sind verpflichtet über Aktualisierungen ihrer Zertifikate für die AS4-Kommunikation per E-Mail zu informieren. Die Information muss mindesten die URL zum Download des neuen Zertifikats bei der ausstellenden CA beinhalten. Die E-Mail 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.

- Aktualisierte URL für den Aufruf des AS4 Web-Service: Alle Marktpartner sind verpflichtet über Aktualisierungen der URL für den Aufruf des AS4 Web-Service per E-Mail zu informieren. Die E-Mail 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.

8 https://bdew-codes.de/Codenumbers/BDEWCodes

3 Übertragungsweg

Als Übertragungsweg wird das AS4-Protokoll basierend auf dem im Anhang verwiesene AS4-Profil des BDEW verwendet.

4 Kommunikationsregeln

Zwischen zwei unterschiedlichen MP-ID ist genau ein Übertragungsweg zulässig.

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.

Jeder AS4-Endpunkt muss jederzeit ohne Firewall-Freischaltung erreichbar sein. Im Fehlerfall gilt die Empfehlung bei der Codenummerndatenbank eine kurzfristige Aktualisierung einzuholen.

5 Zertifikate und PKI

Die Kommunikation wird durch Verwendung der Smart Metering PKI (SM-PKI) des BSI abgesichert. Die Vorgaben der Certificate Policy (CP) der SM-PKI müssen eingehalten werden.

5.1 Vertrauensdiensteanbieter

Die Vertrauensdiensteanbieter müssen eine Sub-CA-Instanz im Sinne der CP der SM-PKI sein.

5.2 Zertifikate: Parameter und Anforderungen

Die Anforderungen an die Zertifikate ergeben sich aus der CP der genutzten PKI. Insbesondere muss die MP-ID des Marktpartners muss im Feld Organisational Unit („OU“) des Subject des Antragstellers im Zertifikats enthalten sein.

5.3 Zertifikatswechsel

Spätestens 10 Werktage, bevor Zertifikate ungültig werden, muss der Inhaber dieser Zertifikate die Nachfolgezertifikate zur Verfügung gestellt haben (vgl. Kapitel 2 und Kapitel 8). Somit entsteht ein Überlappungszeitraum von mindestens 10 Werktagen, in dem noch die bisherigen und die neuen Zertifikate gleichzeitig gültig sind.

Innerhalb dieses Überlappungszeitraums kann bei allen Marktpartnern die Umstellung von den bisher genutzten auf die neuen Zertifikate erfolgen.

Der öffentliche Schlüssel zum Signieren wird mit dem zugehörigen Zertifikat in jeder AS4-Nachricht übermittelt und darf daher vom Sender einer AS4-Nachricht sofort verwendet werden. Der Empfänger der Nachricht kann die Signatur anhand des übermittelten Zertifikats validieren.

Erhält der Sender einer AS4-Nachricht ein neues Zertifikat mit dem darin enthaltenen öffentlichen Schlüssel zum Verschlüsseln von Übertragungsdateien, so darf er diesen sofort nutzen. Der Empfänger ist mindestens im Besitz des zugehörigen privaten Schlüssels und kann mit diesem die Übertragungsdatei entschlüsseln.

Ein neues Zertifikat mit zugehörigem öffentlichem Schlüssel zum Aufbau des TLS-Kanals dürfen sowohl vom Sender als auch vom Empfänger einer AS-Nachricht sofort genutzt werden, da dieses beim Aufbau des TLS-Kanals übermittelt wird.

Im Überlappungszeitraum müssen alle Marktpartner in der Lage sein, sowohl mit dem bisher genutzten als auch mit den neuen Zertifikaten signierte und verschlüsselte AS4-Nachrichten zu verarbeiten.

5.4 Rückruf und Sperrlisten

Will ein Zertifikatsinhaber sein Zertifikat vor Ablauf der Gültigkeitsfrist nicht mehr verwenden oder für ungültig erklären, so muss er sein Zertifikat über die Sperrlisten (CRL) seines CA-Anbieters zurückziehen lassen. Die Vorgaben und Regelungen für die Sperrung von Zertifikaten, Verarbeitung von Sperrlisten und der Aktualisierungs- und Prüfungszeiten ergeben sich aus der Certificate Policy (CP) der SM-PKI.

Wenn eine CRL über die in den Zertifikaten veröffentlichten certificate revocation list distribution point (CRL-DP) von einer CA über 3 Tage nicht abrufbar oder ungültig ist, dann ist der ausstellenden CA und aller darunter gelisteten Zertifikate bis zur Veröffentlichung einer aktuellen CRL nach den Regelungen der CP zu misstrauen. Die konkreten, möglichen Konsequenzen sind Kapitel 9 zu entnehmen.

6 Regelungen für den Austausch von Metainformationen

Für den Austausch von EDIFACT Nachrichtendateien in der Marktkommunikation werden die Felder innerhalb des Elements „PartProperties“ wie folgt gefüllt:

- BDEWDocumentType: EDIFACT-Name des Nachrichten-Typs gem. UNH DE0065
- BDEWDocumentNo: Datenaustauschreferenz aus UNB DE0020

Nicht verwendet werden:

- BDEWFulfillmentDate
- BDEWSubjectPartyID
- BDEWSubjectPartyRole

7 Services des AS 4 Profil

7.1 Testservice

Vor der erstmaligen Nutzung des AS4-Webservice zur Übertragung von Nachrichtendateien soll mittels des Testservice die grundsätzliche Verfügbarkeit und der Verbindungsaufbau zum Ziel des Webservice Aufrufs getestet werden (vgl. BDEW AS4 Profil).

Service = „http://docs.oasis-open.org/ebxml- msg/ebms/v3.0/ns/core/200704/test“
Action = „http://docs.oasis-open.org/ebxml- msg/ebms/v3.0/ns/core/200704/test“

7.2 Wechsel des Übertragungsweges

Vor dem ersten Austausch von Nachrichtendateien mittels der im AS4-Profil des BDEW beschrieben Services soll sichergestellt werden, dass der Empfang und der Versand von AS4-Nachrichten zwischen den beteiligten Marktpartnern möglich ist. Die grundsätzliche Verfügbarkeit und der Verbindungsaufbau zum Ziel des Webservice-Aufrufs kann mittels des Test-Service sichergestellt werden.

Zur weiteren Absicherung eines sicheren Datenaustausches definiert das AS4-Profil des BDEW neben den Services zum Übertragen von Nachrichtendateien und einem Test-Service einen weiteren Service zum Wechsel des Übertragungswegs:

Service = https://www.bdew.de/as4/communication/services/pathSwitch

Dieser Service kennt zwei Aktionen:

- Aufforderung zum Wechsel des Übertragungsweg
  Action = https://www.bdew.de/as4/communication/actions/requestSwitch
- Zustimmung zum Wechsel des Übertragungsweg
  Action = https://www.bdew.de/as4/communication/actions/confirmSwitch

Ein Marktpartner, der den Übertragungsweg AS4 zum Übertragen von Nachrichtendateien zu einem anderen Marktpartner nutzen möchte, hat dieses mit der „Aufforderung zum Wechsel des Übertragungsweg“ anzuzeigen. Der Empfänger dieser Nachricht antwortet mit der „Zustimmung zum Wechsel des Übertragungsweg“ und nutzt den AS4 Web-Service zum Übertragen von Nachrichtendateien.

Der Empfänger der „Zustimmung zum Wechsel des Übertragungsweg“ nutzt dann ebenfalls den AS4 Web-Service zum Übertragen von Nachrichtendateien.

7.3 Austausch von Nachrichtendateien

Für den Datenaustausch im Rahmen der Marktprozesse wird die folgende Kombination von Service und Action verwendet.

Service = https://www.bdew.de/as4/communication/services/MP
Action = http://docs.oasis-open.org/ebxml-msg/as4/200902/action

Andere Services, welche im AS4 Profil beschrieben sind, sind nicht zulässig.

7.4 Response-Codes

Die Übertragung per AS4 ist erst erfolgreich bei synchronem Erhalt der nicht abstreitbaren AS4-Zustellquittung non-repudiation receipt (NRR).[9]

9 Die NRR entspricht bei AS2 der MDN.

8 Organisatorische Regelungen zum Umgang mit Zertifikaten

Ein Marktpartner A kann nur dann eine Nachricht verschlüsselt an einen Markpartner B versenden, wenn Marktpartner B ein gültiges Zertifikat zur Verfügung stellt, das den unter Kapitel 5 genannten Anforderungen genügt. 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 Absender-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.
- Sollte dem Marktpartner A eine AS4-Nachricht empfangen, welche kein gültiges Signaturzertifikat vom Marktpartner B enthält, das den technischen Mindestanforderungen genügt um die Signatur von Marktpartner B prüfen zu können, so kann gemäß Kapitel 9 die Verarbeitung der empfangenen Daten von Marktpartner A so lange abgelehnt werden, bis Marktpartner B ein entsprechendes Zertifikat verwendet.
- Sollte dem Marktpartner A kein Zertifikat vom Marktpartner B zur Verfügung gestellt werden, das den technischen Mindestanforderungen genügt um die Nachricht 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.
  - Scheitert die Signaturprüfung, weil die Signatur bei der Übertragung beschädigt wurde oder kann die AS4-Nachricht deswegen nicht entschlüsselt werden, so ist dies in Bezug auf die Marktkommunikation gleichzusetzen, als ob die angefügte Übertragungsdatei nicht beim Empfänger angekommen wäre.
    Wird auf die Übertragungsdatei vom Empfänger eine CONTRL-(EDIFACT) 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 AS4-Nachricht 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.

9 Konsequenzen bei Nicht-Einhaltung dieser Vorgaben

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

Verstoßvariante 1: Der Sender hat vom Empfänger kein gültiges Zertifikat zum Verschlüsseln von Übertragungsdateien zur Verfügung gestellt bekommen.
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 (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.

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

Verstoßvariante 2: Der Empfänger erhält eine Übertragungsdatei,

- 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. Beim Übertragungsweg AS4 wird automatisch mit einer negativen NRR die Annahme verweigert und der Absender erhält über die synchrone negative NRR-Meldung eine Rückmeldung per AS4 über einen nicht erfolgreichen Versand. Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen.

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 den Inhalt der Übertragungsdatei nicht verarbeiten.

Verfahrensweise: Der Empfänger ist nicht in der Lage, die Übertragungsdatei zu entschlüsseln und

daher berechtigt, die Verarbeitung der Übertragungsdatei zu verweigern. Beim Übertragungsweg AS4 wird automatisch mit einer negativen NRR die Annahme verweigert und der Absender erhält über die synchrone negative NRR-Meldung eine Rückmeldung per AS4 über einen nicht erfolgreichen Versand. Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen.

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 Nachricht sind jedoch nicht abstreitbar.

Verfahrensweise: Der Empfänger ist berechtigt, die Verarbeitung der betreffenden Übertragungsdatei zu verweigern. Beim Übertragungsweg AS4 wird automatisch mit einer negativen NRR die Annahme verweigert und der Absender erhält über die synchrone negative NRR-Meldung eine Rückmeldung per AS4 über einen nicht erfolgreichen Versand. Die Konsequenzen dieser Nicht-Verarbeitung sind vom Sender zu tragen.

10 Quellen

[1] Beschluss (BK6-21-282) und Anlagen zur Absicherung der elektronischen Marktkommunikation Strom, Bundesnetzagentur, 31.03.2022.

[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.

11 Ansprechpartner

Mathias Böswetter
E-Mail: Mathias.Boeswetter@bdew.de
Telefon: +49 30 300 199 1526

ANHANG: AS4-Profil

BDEW AS4-Profil

Regelungen zum sicheren Austausch von EDIFACT-Übertragungsdateien

Version:	1.0
Publikationsdatum:	01.06.2022
Anzuwenden ab:	
Autor:	BDEW

Inhalt

1 Einleitung

Dieses Dokument definiert ein AS4-Nutzungsprofil für den Datenaustausch in der elektronischen Marktkommunikation im deutschen Strom- und Gasmarkt. Es basiert auf dem von der Connecting Europe Facility [CEF] entwickelten eDelivery-Profil.

Das hier definierte Profil zielt auf eine größtmögliche Kompatibilität mit dem CEF eDelivery AS4-Profil [EDEL-AS4] ab und erweitert dieses, wo es technisch notwendig ist. In diesem Sinne werden zusätzliche Optionen vorgeschlagen, die nur Empfehlungen bleiben, da sie in der deutschen Marktkommunikation nicht verwendet werden. Ziel ist es, die Anforderungen der Bundesnetzagentur (BNetzA) an die zukünftige technologische Basis des Übertragungsweges in der elektronischen Marktkommunikation unter Nutzung der Smart Metering Public Key Infrastructure (SM-PKI) des Bundesamtes für Sicherheit in der Informationstechnik zu erfüllen sowie funktionale Erweiterungen anzubieten, um die Einführung in der deutschen Marktkommunikation kosteneffizient zu ermöglichen.

1.1 Terminologie

Die Schlüsselwörter "MÜSSEN" [Englisch “MUST”], “DÜRFEN NICHT” [Englisch "MUST NOT"], “ERFORDERLICH” (Englisch "REQUIRED"], "SOLL" [Englisch "SHALL"], "SOLL NICHT" [Englisch "SHALL NOT"], "SOLLTE" [Englisch "SHOULD"], "SOLLTE NICHT" [Englisch "SHOULD NOT"], "EMPFOHLEN" [Englisch "RECOMMENDED"], "DÜRFEN" [Englisch "MAY"], and "FREIWILLIG" [Englisch "OPTIONAL"] in diesem Dokument sind zu interpretieren nach [RFC2119].

1.2 Bezüge zu Normen und Standards

Zusätzlich zu den Normen, die in AS4 als verbindlich aufgeführt sind, sind die folgenden Normen für dieses Profil verbindlich:

[XMLDSIG1] XML Signature Syntax and Processing Version 1.1. W3C Recommendation, 11. April 2013. http://www.w3.org/TR/xmldsig-core1/

[XMLENC1] XML Encryption Syntax and Processing Version 1.1. W3C Recommendation, 11. April 2013. http://www.w3.org/TR/xmlenc-core1/

[AS4] AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard, 23. Januar 2013. http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/

[AU] ebCore Agreement Update Specification Version 1.0. OASIS Committee Specification, 19. September 2016. http://docs.oasis-open.org/ebcore/ebcore-au/v1.0/

[BSIALG] Entwurf Algorithmenkatalog 2014. Bundesamt für Sicherheit in der Informationstechnik (BSI). Bonn, 11. Oktober 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf_2013.pdf?__blob=publicationFile.

[BSITLS] Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung. Bundesamt für Sicherheit in der Informationstechnik (BSI). Bonn, 08. Oktober 2013.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf

[TR-02102-1] BSI TR-02102-1. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Version 2016-01.

[TR-02102-2] Technische Richtlinie TR-02102-2. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2. Verwendung von Transport Layer Security (TLS).

[TR-03116-3] Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3: Intelligente Messsysteme.

[TR-03116-4] Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen.

2 BDEW AS4-Profil

Diese Spezifikation definiert das AS4-Profil des BDEW. Sie besteht aus:

- Auswahl eines Konformitätsprofils (Abschnitt 2.1)
- Weitere Profilerstellung dieses Konformitätsprofils (Abschnitt 2.2)
- Nutzungsprofil (Abschnitt 2.3).

Die Einhaltung des eDelivery AS4-Profils [EDEL-AS4] kann aufgrund der für dieses Profil erforderlichen kryptografischen Anforderungen nicht vollständig erreicht werden (Abschnitt 2.2.6.2).

Die für dieses Profil spezifischen Sicherheitsanforderungen gelten für:

- Transportverschlüsselung (TLS)
- Hash-Function
- Signaturverfahren und -algorithmen
- Verschlüsselungsmethoden und -algorithmen

2.1 AS4-Konformitätsprofil

2.1.1 AS4-Standard

Dieses Profil basiert auf dem CEF eDelivery AS4-Profil [EDEL-AS4], das auf AS4 aufbaut. AS4 basiert auf weiteren Standards, insbesondere dem OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features OASIS Standard [EBMS3], die wiederum auf verschiedenen Webservice-Spezifikationen beruhen.

2.1.2 AS4-ebHandler-Konformitätsprofil

Die AS4-Spezifikation [AS4] definiert mehrere Konformitätsprofile, die spezifische funktionale Teilmengen der Version 3.0 ebXML Messaging, Core-Spezifikationen definieren. Ein Konformitätsprofil entspricht einer Klasse von konformen Anwendungen. Das AS4-Profil des BDEW basiert auf erweiterten Unterfällen des **AS4-ebHandle-Konformitätsprofil**, einer Auswahl von AS4-Advanced-Features und einem Nutzungsprofil. Es unterstützt die Punkt-zu-Punkt-Kommunikation

von Sendern zu Empfängern unter Verwendung von eDelivery-Access-Points sowie der ebMS3-"Push"-Transportkanalbindung.

2.2 Profilerstellung des AS4-ebHandler-Konformitätsprofils

Die in diesem Profil spezifizierten Anforderungen, Eigenschaften und Algorithmen sind, mit einigen Ausnahmen, Unterfälle des AS4-ebHandler-Konformitätsprofil. Dieser Abschnitt wählt spezifische Optionen aus, bei denen das AS4-ebHandler-Konformitätsprofil mehrere Möglichkeiten bietet, und definiert die technischen Anforderungen, die Lieferanten und Anbieter in ihrer AS4-Software implementieren müssen. Die Struktur dieses Abschnitts spiegelt die Struktur der ebMS3-Core-Spezifikation wider [CEF] eDelivery Specification. Connecting Europe Facility (CEF). Brüssel, 11. November 2020. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.15

[EBMS3].

Im Vergleich zum AS4-ebHandler-Konformitätsprofil aktualisiert und ergänzt dieses AS4-Profil des BDEW einige Funktionen:

- Transport Layer Security ist im Profil enthalten (siehe 2.2.6.1).
- Die Algorithmen zur Sicherung der Integrität, Authentizität und Vertraulichkeit von Nachrichten auf der Nachrichtenschicht wurden aktualisiert (siehe 2.2.6.2).
- Unterstützung des **Pull**-Modes wird EMPFOHLEN (siehe 2.2.2).
- Unterstützung für Zwei-Wege-MEP ist nicht erforderlich und FREIWILLIG (siehe 2.2.1).
- Alle Payload-Dateien sind separate MIME-Bestandteile (siehe 2.2.3.2).
- Fehlermeldung und Quittung sind immer synchronisiert (siehe 2.2.4).
- WS-Security ist auf das X.509-Token-Profil beschränkt (siehe 2.2.6.2).

2.2.1 Modell zur Nachrichtenübermittlung

Dieses Profil legt die Kanalbindungen des Nachrichtenaustauschs zwischen zwei AS4-Message Service Handlern (MSH) fest, von denen einer als sendender MSH und der andere als empfangender MSH fungiert. Das folgende Diagramm (aus [EBMS3]) zeigt die verschiedenen Akteure und Operationen beim Nachrichtenaustausch:

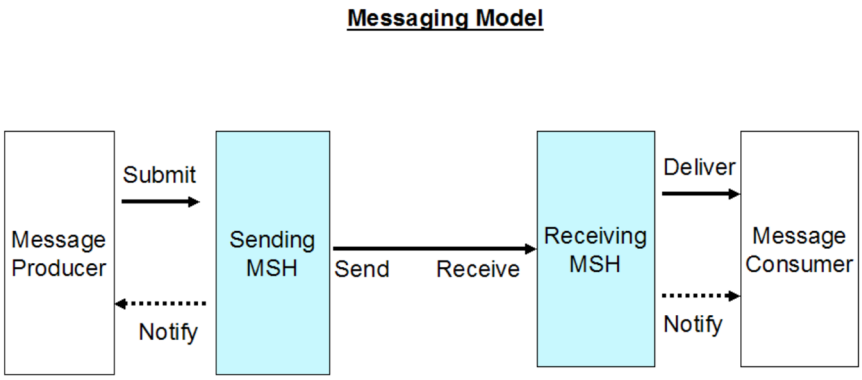

Abbildung 1. Entitäten des AS4-Nachrichtenmodells und ihre Interaktionen [EBMS3]

Geschäftsanwendungen oder Middleware, die als *Producer* fungieren, *übermitteln* Nachrichteninhalte und Metadaten an den sendenden MSH, der diese Inhalte verpackt und an den empfangenden MSH des Geschäftspartners sendet, der sie *empfängt* und seinerseits die Nachricht an eine andere Geschäftsanwendung oder Middleware *weiterleitet*, die die Nachricht konsumiert. Je nach Konfiguration können der sendende und der empfangende MSH den Producer oder den *Consumer* über bestimmte Ereignisse *benachrichtigen*. Beachten Sie, dass es einen Unterschied zwischen *Sender* und *Initiator* gibt. Beim **Push**-Austausch initiiert der sendende MSH die Übertragung der Nachricht. Bei **Pull**-Austauschvorgängen wird die Übertragung vom empfangenden MSH initiiert.

Dieses Profil ist Push-basiert und die Unterstützung des folgenden Nachrichtenaustauschmusters ist ERFORDERLICH:

› **One Way / Push**

Im Kontext des ebMS-Nachrichtenaustauschs bedeutet *pushing,* dass der Absender den Nachrichtenaustausch initiiert. Für HTTP bedeutet dies, dass der sendende MSH als HTTP-Client und der empfangende MSH als HTTP-Server fungiert.

Für **PMode.MEP** ist die Verwendung des folgenden Festwerts ERFORDERLICH:

› http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay

Für **PMode.MEPbinding,** ist die Unterstützung ERFORDERLICH für:

› http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push

Die Interkationen der ebMS 3.0 Two-Way Message Exchange Pattern (MEP) werden in diesem Profil nicht unterstützt.

2.2.2 Nachrichten-Pulling und Nachrichten-Partitionierung

Die in diesem Profil betrachteten Geschäftsprozesse erfordern nur die Verwendung des Message Exchange Patterns **Push**.

Bitte beachten Sie, dass eine Standardimplementierung von AS4 ebHandler auch die Unterstützung von **Pull** erfordert. Dieses Message Exchange Pattern muss in diesem Profil nicht unterstützt werden, aber die Unterstützung wird, wie im eDelivery AS4 Profil [EDEL-AS4] (Abschnitt 4.5) beschrieben, EMPFOHLEN.

Für PMode.MEPbinding SOLLTEN die Anwendungen daher auch unterstützen:

› http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/pull

Gründe für die Unterstützung von Pull Transport Channel Binding können die folgenden sein:

› Ein Empfänger hat keine feste IP-Adresse und/oder DNS-auflösbare Serveradresse.

› Ein Empfänger lässt keine eingehenden TCP/IP-Verbindungen zu. Dies wird von einigen Organisationen aus Sicherheitsgründen oder zur Vereinfachung der Netzwerkverwaltung bevorzugt.

› Ein Empfänger ist nicht garantiert rund um die Uhr verfügbar. Dies ist manchmal der Fall bei kleineren Organisationen oder Organisationen mit geringeren IT-Budgets.

2.2.3 Nachrichtenverpackung

Das folgende Diagramm zeigt die AS4-Nachrichtenstruktur, die auf SOAP und MIME basiert. Gestrichelte Linien kennzeichnen optionale Komponenten.

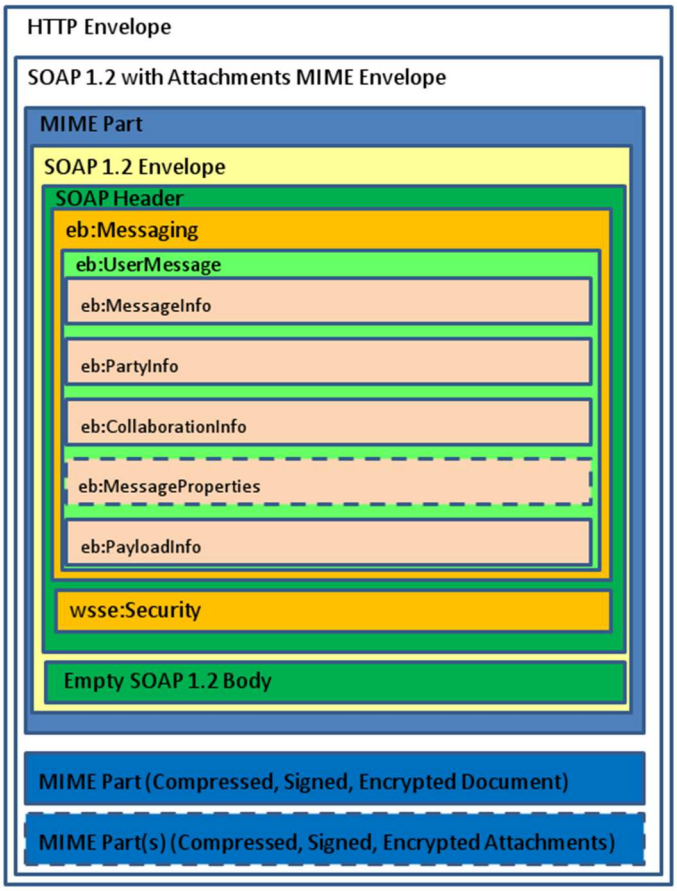

Figure 1 AS4 Message Structure

Der SOAP-Umschlag MUSS als UTF-8 kodiert sein ([EBMS3], Absatz 5.1.2.5). Ein SOAP-Umschlag, der korrekt als UTF-8 kodiert ist und dessen Zeichensatz-Header auf UTF-8 gesetzt ist, kann ein Unicode Byte Order Mark (BOM; [BP20], Absatz 3.1.2) enthalten.

2.2.3.1 UserMessage

AS4 definiert den ebMS3 **Messaging** SOAP-Header, der **UserMessage** XML-Strukturen umhüllt, die geschäftlichen Metadaten für ausgetauschte Nutzdaten bereitstellen. In AS4 enthalten ebMS3-Nachrichten mit Ausnahme von Quittungen oder Fehlern eine einzige UserMessage. Dieses Profil folgt dem AS4 ebHandler-Konformitätsprofil, indem es volle Konfigurierbarkeit für "General" und "BusinessInfo" P-Mode Parameter gemäß Abschnitt 2.1.3.1 und 2.1.3.3 von [AS4] fordert.

Ein konformes Produkt MUSS in der Lage sein, Nachrichten zu senden und zu empfangen, bei denen das optionale Attribut *pmode* von **AgreementRef** nicht gesetzt ist.

Die ebMS3- und AS4-Spezifikationen schränken den Wert von **MessageId** nicht über die Konformität mit dem Internet Message Format [RFC2822] hinaus ein, dass die Eindeutigkeit des Wertes verlangt. Es wird EMPFOHLEN, dass der Wert universell eindeutig ist. Produkte können dies erreichen, indem sie eine UUID-Zeichenkette in den linken Teil des Identifizierungssatzes einfügen und dabei zufällig (oder pseudo-zufällig) ausgewählte Werte verwenden.

Wie im AS4 ebHandler Profil ist die Unterstützung von **MessageProperties** in diesem Profil ERFORDERLICH.

2.2.3.2 Payload

Abschnitt 5.1.1 der ebMS3 Core-Spezifikation [EBMS3] verlangt von Implementierungen, dass sie sowohl Non-Multipart (Simple SOAP) Nachrichten als auch Multipart (SOAP-with-attachments) Nachrichten verarbeiten können, und dies ist eine Anforderung für das AS4 ebHandler-Konformitätsprofil. Aufgrund der obligatorischen Verwendung von AS4-Kompression in diesem Profil (siehe Abschnitt 2.2.3.3) werden die Nutzdaten in binäre Daten umgewandelt, die in einem separaten MIME-Teil mit der MIME-Eigenschaft Content-Type auf "application/octet-stream" und nicht im SOAP-Body übertragen werden. AS4-Nachrichten, die auf diesem Profil basieren, haben immer einen leeren SOAP-Body.

Der ebMS3-Mechanismus zur Unterstützung "externer" Nutzdaten über Hyperlink-Referenzen (wie in Abschnitt 5.2.2.12 von [EBMS3] erwähnt) MUSS NICHT verwendet werden.

2.2.3.3 Nachrichtenkomprimierung

Die AS4-Spezifikation definiert die Komprimierung von Nutzdaten als eine ihrer zusätzlichen Funktionen. Die Komprimierung von Nutzdaten ist eine nützliche Funktion für viele Inhaltstypen, einschließlich XML-Inhalten.

Der Parameter **PMode[1].PayloadService.CompressionType** MUSS auf den Wert application/gzip gesetzt werden. (Beachten Sie, dass GZIP der einzige Kompressionstyp ist, der derzeit in AS4 unterstützt wird).

Die obligatorische Verwendung der Komprimierung steht im Einklang mit den aktuellen Praktiken für den B2B-Datenaustausch im Gasbereich, wie z. B. dem EASEE-gas AS2-Profil [EGMTP]. Komprimierte Nutzdaten sind in separaten MIME-Teilen enthalten.

2.2.4 Fehlerbehandlung

Dieses Profil legt fest, dass Fehler synchron an den Sender gemeldet und übertragen werden MÜSSEN und an den Verbraucher gemeldet werden SOLLEN.

› Der Parameter **PMode[1].ErrorHandling.Report.AsResponse** MUSS auf den Wert *true* gesetzt werden.

› Der Parameter **PMode[1].ErrorHandling.Report.ProcessErrorNotifyConsumer** SOLLTE auf den Wert *true* gesetzt werden.

2.2.5 Zuverlässige Nachrichtenübermittlung und Empfangswahrnehmung

Dieses Profil legt fest, den *Non-Repudiation-Receipts* (NRR) für jeden Nachrichtentyp synchron gesendet werden MÜSSEN.

› Der Parameter **PMode[1].Security.SendReceipt.NonRepudiation** MUSS auf den Wert *true* gesetzt werden.

› Der Parameter **PMode[1].Security.SendReceipt.ReplyPattern** Muss auf den Wert *Response* gesetzt werden.

Dieses Profil erfordert die Verwendung der Funktion AS4-Empfangswahnehmung. Diese Funktion bietet einen eingebauten Wiederholungsmechanismus, der bei der Überwindung vorübergehender Netzwerk- oder anderer Probleme und der Erkennung von Nachrichtenduplikaten helfen kann.

› Der Parameter **PMode[1].ReceptionAwareness** MUSS auf den Wert *true* gesetzt werden.

› Der Parameter **PMode[1].ReceptionAwareness.Retry** MUSS auf den Wert *true* gesetzt werden.

› Der Parameter **PMode[1].ReceptionAwareness.DuplicateDetection** MUSS auf den Wert *true* gesetzt werden.

Bei den Parametern **PMode[1].ReceptionAwareness.Retry.Parameters** und den zugehörigen **PMode[1].ReceptionAwareness.DuplicateDetection.Parameters** handelt es sich um eine Reihe von Parametern zur Konfiguration von Wiederholungen und Duplikat Erkennung. Diese Parameter sind in [AS4] nicht vollständig spezifiziert und hängen von der Implementierung ab. Produkte MÜSSEN die Konfiguration von Parametern für Wiederholungen und Duplikat Erkennung unterstützen.

Vom Absender erzeugte Fehler bei der Empfangserkennung MÜSSEN der einreichenden Anwendung gemeldet werden:

› Der Parameter **PMode[1].ErrorHandling.Report.MissingReceiptNotifyProducer** MUSS auf den Wert *true* gesetzt werden.

› Der Parameter **PMode[1].ErrorHandling.Report.SenderErrorsTo** DARF NICHT gesetzt werden. Es gibt keine Unterstützung für die Meldung von Absenderfehlern an einen Dritten.

2.2.6 Sicherheit

Der AS4-Nachrichtenaustausch kann auf mehreren Kommunikationsschichten gesichert werden: der Netzwerkschicht, der Transportschicht, der Nachrichtenschicht und der Nutzdatenschicht. Die erste und die letzte Ebene werden normalerweise nicht von B2B-Kommunikationssoftware behandelt und sind daher nicht Gegenstand dieses Unterabschnitts. Die Sicherheit auf der Transportschicht wird behandelt, auch wenn ihre Funktionalität auf eine andere Infrastrukturkomponente ausgelagert werden kann.

Dieser Abschnitt enthält Parametereinstellungen, die auf mehreren veröffentlichten Best-Practice-Lösungen beruhen. Es wird darauf hingewiesen, dass nach der Veröffentlichung dieser Spezifikation bisher unbekannte Schwachstellen in den in diesem Abschnitt genannten Sicherheitsalgorithmen, Formaten und Austauschprotokollen entdeckt werden können. Solche Entdeckungen SOLLTEN zu Überarbeitungen dieser Spezifikation führen.

In diesem Profil ist der AS4 Nachrichtenverkehr gesichert auf der Transport- und auf der Message-Schicht.

2.2.6.1 Transport-Layer

Für AS4 ist Transport Layer Security (TLS) eine Option, um die Vertraulichkeit und Authentifizierung von Nachrichten zu gewährleisten. Bei der Server-Authentifizierung mit einem Server-Zertifikat muss der Client überprüfen, ob er mit dem richtigen Server verbunden ist.

Wenn die TLS Verbindung im AS4 Message Handler beendet wird, MUSS diese TLS Verbindung den Regeln in [TR 03116-3] entsprechen. Sie ersetzen die Anforderungen der AS4 Spezifikation. Eine Server- und Client-Authentifizierung ist erforderlich.

Im Besonderen gilt dabei:

› Es MUSS mindestens[RFC5246]vorliegen [RFC5246] [BSITLS].

› Es MUSS die Cipher Suites unterstützen, die empfohlen werden in [TR 03116-3] (Kapitel 4)

› Client-Authentifizierung ist ERFORDERLICH

Wenn die TLS-Verbindung nicht im AS4 Message-Handler, sondern in einer anderen Komponente beendet wird, dann MUSS diese andere Komponente folgende Anforderungen erfüllen (cf. 2.3.4.2).

2.2.6.2 Message-Layer

Um den Schutz der Nachrichtenebene für AS4-Nachrichten zu gewährleisten, VERPFLICHTET dieses Profil die Verwendung der folgenden OASIS-Standards für die Sicherheit von Webdiensten der Version 1.1.1, die in ebMS3.0 beschrieben sind [CEF] eDelivery Specification. Connecting Europe Facility (CEF). Brüssel, 11. November 2020. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.15

[EBMS3]und AS4 [AS4]:

- Web Services Security SOAP Message Security [WSSSMS].
- Web Services Security X.509 Certificate Token Profile [WSSX509].
- Web Services Security SOAP Message with Attachments (SwA) Profile [WSSSWA].

Das X.509 Certificate Token-Profile ermöglicht die elektronische Signatur und Verschlüsselung von AS4-Nachrichten. Dieses Profil ERFORDERT die Verwendung von X.509-Zertifikaten zum Signieren und Verschlüsseln von AS4-Nachrichten.

Die AS4-Option der Verwendung von Username Tokens, die im AS4 ebHandler-Konformitätsprofil unterstützt wird, MUSS NICHT verwendet werden.

Die AS4-Nachricht MUSS vor dem Verschlüsseln signiert werden (siehe Abschnitt 7.6 of [EBMS3CORE]).

2.2.6.2.1 Signatur

Die AS4-Nachrichtensignierung basiert auf der W3C XML Signatur-Empfehlung. Die aktuelle Version dieses Standards ist die Spezifikation vom April 2013, Version 1.1 [XMLDSIG1] XMLDSIG11], die relevante neue Algorithmus-Bezeichner definiert. Eine vollständige Liste ist definiert in [RFC6931].

Dieses BDEW-AS4-Profil verwendet die AS4-Algorithmen für Hashing und Signatur, wie in [TR-03116-3] (Abschnitt 9.1) beschrieben. Die zu verwendende Kurve MUSS BrainpoolP256r1 sein.

WS-Security definiert drei Optionen für den Verweis auf ein Sicherheits-Token (Absatz 3.2 in [WSSX509]). In ebMS3 oder AS4 ist kein Parameter für die Auswahl einer bestimmten Option definiert. In diesem Profil MUSS die Option BinarySecurityToken verwendet werden, um auf das Sicherheits-Token zu verweisen, und MUSS die in Abschnitt 3.1.2 von [WSSX509] definierte Option X509PKIPathv1 Token Type verwenden. Die Verwendung dieses Token-Typs MUSS durch Setzen des Attributs ValueType von wsse:BinarySecurityToken auf den Wert http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1 angezeigt werden.

Dieses Profil verwendet die folgende AS4-Konfiguration im P-Mode:

- Der Parameter von **PMode[1].Security.X509.Sign** MUSS nach Maßgabe der Abschnitte 5.1.4 und 5.1.5 von [AS4] gesetzt werden.
- Der Parameter von **PMode[1]. Security.X509.Signature.HashFunction** MUSS auf den Festwert gesetzt werden **http://www.w3.org/2001/04/xmlenc#sha256.**
- Der Parameter von **PMode[1]. Security.X509.Signature.Algorithm** MUSS auf den Festwert gesetzt werden **http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256.**

Die in [RFC 6090] Fundamental Elliptic Curve Cryptography Algorithms und Kapitel 7 beschriebenen Interoperabilitätsanforderungen MÜSSEN implementiert werden.

Beispiel:

```
<wsse:BinarySecurityToken
  EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
  ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1"
  wsu:Id="X509-99bde7b7-932f-4dbd-82dd-3539ba51791b">
 <!-- X509PKIPathv1 binary security token base64 encoded -->
</wsse:BinarySecurityToken>
<ds:Signature Id="SIG-3541f01f-86ea-4b6e-b5c8-40a9489b1cb9">
 <ds:SignedInfo>
  <ds:CanonicalizationMethod Algorithm=" http://www.w3.org/2001/10/xml-exc-c14n#">
   <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
    PrefixList="S12 ds eb3 ebbp ebint wsa wsse wsu"/>
  </ds:CanonicalizationMethod>
  <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
  <ds:Reference URI="#d3e107">
   <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
     <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
      PrefixList="ds eb3 ebbp ebint wsa wsse"/>
    </ds:Transform>
   </ds:Transforms>
   <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
   <ds:DigestValue>UYvI+iIuppRPpTsEDtMNRMbQoJdW1YXx4pEzMAI2ss8=</ds:DigestValue>
  </ds:Reference>
  <ds:Reference URI="#id-10d2e308-dfeb-4fb5-8972-d6d2a8644c54">
   <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
     <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
      PrefixList="ds ebbp ebint wsa wsse wsu"/>
    </ds:Transform>
   </ds:Transforms>
   <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
   <ds:DigestValue>SOL/8qGz39XMw8dP6EH4BbjcjiNkgckNFnm1OAjn0WE=</ds:DigestValue>
  </ds:Reference>
 </ds:SignedInfo>
 <ds:SignatureValue>euIbT34U6p2I3KG6aTSzmO5g5QIDsByzfQ82RgjrKd8qaCSv5NxBfVrIN0565Zs6G0mldtaYUYugCRUtINnqhA==</ds:SignatureValue>
 <ds:KeyInfo Id="KI-1012015c-30a0-481a-9dc5-b791a97bf793">
  <wsse:SecurityTokenReference
   xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
   xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
   wsu:Id="STR-8e934e9f-bbeb-4c27-afd7-211def40d23f">
  <wsse:Reference URI="#X509-99bde7b7-932f-4dbd-82dd-3539ba51791b"
```

```
42            ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1"/>
43    </wsse:SecurityTokenReference>
44  </ds:KeyInfo>
45 </ds:Signature>
```

2.2.6.2.2 Verschlüsselung

Die Verschlüsselung in Web Services Security basiert auf der W3C XML Encryption-Empfehlungen. Die aktuelle Version ist die W3C Recommendation vom 11. April 2013 [XMLENC1].

In diesem Profil MUSS die Option X509SKI verwendet werden, um auf das für die Schlüsselableitung verwendete Sicherheits-Token zu verweisen.

Dieses AS4-Profil des BDEW verwendet die AS4-Algorithmen für den Schlüsseltransport und die Verschlüsselung, wie sie in [TR-03116-3] beschrieben werden (Kapitel 9.2).

Die folgenden Parameter konfigurieren die Verschlüsselung in diesem AS4-Profil:

› Der Parameter von **PMode[1. Security. X509. Encryption.Encrypt** MUSS nach Maßgaben der Abschnitte 5.1.6 und 5.1.7 von [AS4]

› Der Parameter von **PMode[1. Security.X509.Encryption.Algorithm** MUSS auf den statischen Wert gesetzt werden *http://www.w3.org/2009/xmlenc11#aes128-gcm.* Dieser Algorithmus ist der Wert des Attributs *algorithm* des Elements *xenc:EncryptionMethod in xenc:EncryptedData*.

Implementierungen MÜSSEN die folgenden Algorithmen verwenden, wie sie in [TR-03116-3] (Kapitel 9.2).

› Für Verschlüsselungsalgorithmen, *http://www.w3.org/2001/04/xmlenc#kw-aes128*. Dies ist der Algorithmus, der als Wert für das Algorithmus-**Attribut** der **xenc:EncryptionMethod** in **xenc:EncryptedKey** verwendet wird

› Für die Methode der Schlüsselvereinbarung,

http://www.w3.org/2009/xmlenc11#ECDH-ES. Dies ist der Algorithmus, der als Wert für das **Algorithmus**-Attribut von **xenc:AgreementMethod** in **ds:KeyInfo** verwendet wird

- Für die Methode der Schlüsselableitung, *http://www.w3.org/2009/xmlenc11#ConcatKDF*. Dies ist der Algorithmus, der als Wert für das **Algorithmus**-Attribut von **xenc11:KeyDerivationMethod** in **xenc:AgreementMethod** verwendet wird
- Als Digest-Generierungsfunktion, *http://www.w3.org/2001/04/xmlenc#sha256*. Dies ist der Algorithmus, der als Wert für das Algorithmus-Attribut auf **ds:DigestMethod** in **xenc11:ConcatKDFParams** verwendet wird
- Der Kurvenparameter, der für ECDH-ES verwendet werden MUSS, lautet *BrainpoolP256r1*
- Die Werte der Attribute AlgorithmID, PartyUInfo, PartyVInfo des Elements **xenc11:ConcatKDFParams** müssen auf leere Strings gesetzt werden.

Die in [RFC 6090] Fundamental Elliptic Curve Cryptography Algorithms in Kapitel 7 beschriebenen Interoperabilitätsanforderungen werden umgesetzt.

Beispiel:

```
01 <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                Id="ED-64914301-0ef1-47fc-b5b0-1297bfd00e45"
                MimeType="application/gzip"
                Type="http://docs.oasis-open.org/wss/oasis-wss-SwAProfile-1.1#Attachment-Content-Only">
02  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
03  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
04    <wsse:SecurityTokenReference
            xmlns:wsse11="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
            wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey">
05      <wsse:Reference URI="#EK-50bd3119-caab-4d31-b994-b99c2ad7c9c8"/>
06    </wsse:SecurityTokenReference>
07  </ds:KeyInfo>
08  <xenc:CipherData>
09    <xenc:CipherReference URI="cid:payload-id@bosch-si.com">
10      <xenc:Transforms>
11        <ds:Transform
            mlns:ds="http://www.w3.org/2000/09/xmldsig#"
            Algorithm="http://docs.oasis-open.org/wss/oasis-wss-SwAProfile-1.1#Attachment-Ciphertext-Transform"/>
12      </xenc:Transforms>
13    </xenc:CipherReference>
14  </xenc:CipherData>
15 </xenc:EncryptedData>
16
17 <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="EK-50bd3119-caab-4d31-b994-b99c2ad7c9c8"
              xmlns:dsig11="http://www.w3.org/2009/xmldsig11#"
              xmlns:xenc11="http://www.w3.org/2009/xmlenc11#">
18  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
19  <!-- describes the key encryption key -->
20  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
21    <xenc:AgreementMethod Algorithm="http://www.w3.org/2009/xmlenc11#ECDH-ES">
22      <xenc11:KeyDerivationMethod Algorithm="http://www.w3.org/2009/xmlenc11#ConcatKDF">
23        <xenc11:ConcatKDFParams AlgorithmID="" PartyUInfo="" PartyVInfo="">
24          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
25        </xenc11:ConcatKDFParams>
26      </xenc11:KeyDerivationMethod>
27      <xenc:OriginatorKeyInfo>
28        <ds:KeyValue>
```

```
29              <dsig11:ECKeyValue>
30                 <!-- ephemeral ECC public key of the originator -->
31                 <dsig11:NamedCurve URI="urn:oid:1.3.36.3.3.2.8.1.1.7" />
32                 <dsig11:PublicKey>
33 MFowFAYHKoZIzj0CAQYJKyQDAwIIAQEHA0IABD4nUMx3iNWJcgxP5DJeBtybV2/B
34  CTqgmAB3fqhdnmSbS9jjZuaModL7eflZfDJEzCz8pkc7V8mhWdJXhZ3kOGw=
35                 </dsig11:PublicKey>
36              </dsig11:ECKeyValue>
37           </ds:KeyValue>
38        </xenc:OriginatorKeyInfo>
39        <xenc:RecipientKeyInfo>
40           <ds:X509Data>
41              <ds:X509SKI>ae1234bd</ds:  X509SKI>
42           </ds:X509Data>
43        </xenc:RecipientKeyInfo>
44     </xenc:AgreementMethod>
45  </ds:KeyInfo>
46  <xenc:CipherData>
47     <xenc:CipherValue>
48        <!-- encrypted AES content encryption key -->
49     </xenc:CipherValue>
50  </xenc:CipherData>
51  <xenc:ReferenceList>
52     <xenc:DataReference URI="#ED-64914301-0ef1-47fc-b5b0-1297bfd00e45"/>
53  </xenc:ReferenceList>
```

2.2.7 Netzwerk

AS4-Produkte MÜSSEN IPv4 implementieren und SOLLTEN IPv6 implementieren (Dual Stack). Der Sender MUSS in der Lage sein, die AS4-Verbindung über IPv4 herzustellen. Wenn Produkte IPv6 implementieren, MUSS auch der "happy eyeball"-Algorithmus [RFC6555] implementiert werden.

2.2.8 Konfigurationsmanagement

Die AS4-Implementierung, die diesem Profil entspricht, MUSS nicht nur in der Lage sein, die Nutzlast zu übertragen (Hauptziel dieses Profils) und einen Testdienst (Abschnitt 2.3.6) zu unterstützen, sondern MUSS zusätzlich einen AS4-Übertragungspfadänderungsdienst (Abschnitt 2.3.7) implementieren.

2.3 Nutzungsprofil

Dieser Abschnitt definiert ein Nutzungsprofil für AS4. Es beschreibt, wie AS4-Produkte im Energiemarkt verwendet werden MÜSSEN, die in Bezug auf die technischen Spezifikationen in Abschnitt 2.2 implementiert sind. Das Konzept des Nutzungsprofils ist in Abschnitt 5 des AS4-

Standards definiert [AS4]. Die Zielgruppe dieses Abschnitts sind Projektgruppen, die AS4 (wie in Abschnitt 2.2 beschrieben) in ihrem Unternehmen implementieren und konfigurieren und für den elektronischen Datenaustausch mit Kommunikationspartnern verantwortlich sind.

Die Struktur dieses Abschnitts spiegelt teilweise die Struktur des ebMS3-Standards [CEF] eDelivery Specification. Connecting Europe Facility (CEF). Brüssel, 11. November 2020. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.15

[EBMS3] wider, enthält aber auch allgemeine Aspekte.

2.3.1 Message Packaging

Dieses Nutzungsprofil definiert Einschränkungen für mehrere Elemente in den AS4-Nachrichtenkopffeldern.

2.3.1.1 Identifizierung der Marktteilnehmer

Eine PartyId ist eine eindeutige Identifikation einer Organisation, die an der Geschäftstrans-aktion für den Austausch von AS4-Nachrichten beteiligt ist.

Beim Austausch von Nachrichten gemäß diesem Profil MÜSSEN die Parteien mit dem entsprechenden GLN-Code oder der MP-ID [MP-ID] identifiziert werden.

Der BDEW-Code ist die Marktpartner-Identifikationsnummer (MP-ID) für den deutschen Energiemarkt.

Mit diesem BDEW-Code kann jedes Unternehmen und seine jeweilige Rolle im deutschen Energiemarkt eindeutig identifiziert werden.

Unternehmen, die weder über eine GLN noch über eine MP-ID verfügen und dieses Profil nutzen wollen, MÜSSEN sich an den BDEW wenden und eine MP-ID beantragen.

The Die MP-ID - vergeben durch BDEW, DVGW oder GLN-Code - MUSS als Inhalt für die From/PartyId und To/PartyId verwendet werden. Es MUSS einer der folgenden Partnertypen verwendet werden:

› Bei Verwendung des GLN-Codes basiert der Partnertyp auf der ebCore PartyId [eDelivery-EBCORE]:
  - urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088

› Bei Verwendung der vom BDEW zugewiesenen MP-ID die laute der *party type*:
  - urn:oasis:names:tc:ebcore:partyid-type:unregistered:BDEW

› Bei Verwendung der vom DVGW zugewiesenen MP-ID lautet der *party type*:

› urn:oasis:names:tc:ebcore:partyid-type:unregisteredDVGW

2.3.1.2 Ausrichtung der Geschäftsprozesse

Mehrere obligatorische Kopfzeilen in AS4 werden verwendet, um Metadaten zu übermitteln, die einen Nachrichtenaustausch mit einem Geschäftsprozess oder einem technischen Dienst abgleichen.

2.3.1.2.1 Service

Ein Service identifiziert eine Sammlung zusammenhängender Geschäftsvorgänge im Kontext des Geschäftsprozesses. Der Diensttyp ermöglicht die Spezialisierung verschiedener Typen innerhalb eines Dienstes.

Im BDEW AS4-Profil ist das AS4-Protokoll nicht vom Geschäftsprozess entkoppelt. Daher ERFORDERT dieses Profil einen vordefinierten Wert für die Dienste beim Austausch von Nutzdaten:

› https://www.bdew.de/as4/communication/services/MP

› https://www.bdew.de/as4/communication/services/FP

› https://www.bdew.de/as4/communication/services/RD

› https://www.bdew.de/as4/communication/services/KW

› https://www.bdew.de/as4/communication/services/SO

Bitte beachten Sie, dass das Service-Typ *attribute* nicht erforderlich ist, wenn der Wert des Dienstes ein URI ist.

Der Test-Service (Abschnitt 2.3.6) und das ebCore Agreement-Update (Abschnitt **Fehler! Verweisquelle konnte nicht gefunden werden.**) verwenden unterschiedliche Werte für den Dienst.

Der folgende Wert MUSS verwendet werden:

› For Test Service, http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service

Der AS4-Dienst zur Änderung des Übertragungswegs (Abschnitt 2.3.7):

› https://www.bdew.de/as4/communication/services/pathSwitch

2.3.1.2.2 Action

Eine Action identifiziert die verschiedenen Arten von Geschäftsvorgängen im Kontext eines Dienstes.

Im AS4-Profil des BDEW ist das AS4-Protokoll vom Geschäftsprozess entkoppelt. Daher ERFORDERT dieses Profil einen vordefinierten Wert für die Aktion:
http://docs.oasis-open.org/ebxml-msg/as4/200902/action

Der Test-Service (Abschnitt 2.3.6) und das ebCore Agreement-Update (Abschnitt**Fehler! Verweisquelle konnte nicht gefunden werden.**) verwenden unterschiedliche Werte für die Action.

Der folgende Wert MUSS verwendet werden:

› For Test Service, http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test

Der AS4-Dienst zur Änderung des Übertragungswegs (Abschnitt 2.3.7):

› https://www.bdew.de/as4/communication/actions/**requestSwitch**

› https://www.bdew.de/as4/communication/actions/**confirmSwitch**

2.3.1.2.3 Rolle

Die obligatorischen *UserMessage/PartyInfo/ {From|To}/Role*-Elemente des AS4-Headers definieren die Rolle der Entitäten, die die AS4-Nachricht für den angegebenen Dienst und die Aktion senden und empfangen.

Im AS4-Profil des BDEW ist das AS4-Protokoll vom Geschäftsprozess entkoppelt. Daher ERFORDERT dieses Profil einen vordefinierten Festwert für die Rollen:

› Absender-Rolle: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator

› Empfänger-Rolle: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder

2.3.1.3 Message Correlation

Das Element *UserMessage/CollaborationInfo/ConversationId* dient der Prozesszuordnung.

In diesem Profil ist das Element ConversationId immer leer.

UserMessage/MessageInfo/RefToMessageId DARF NICHT verwendet werden, da dieses Profil keine Zwei-Wege-MEP verwendet.

2.3.2 Agreements

AgreementRef ist ein Festwert von **https://www.bdew.de/as4/communication/agreement**, der anzeigt, dass das dynamische Sender- und Empfängermodell dieses Profils verwendet werden soll. Die AgreementRef-Attribute *pmode* und *type* DÜRFEN NICHT verwendet werden.

Der MSH des Empfängers ist so zu konfigurieren, dass er Nachrichten mit beliebigen Werten in den Feldern ***eb:Messaging/eb:UserMessage/eb:PartyInfo/eb:From/eb:PartyId*** akzeptiert, sofern sie mit den entsprechenden Betreff-Feldern im vorgelegten Zertifikat übereinstimmen.

Die MSH des Absenders MUSS es den Produzenten ermöglichen, dynamisch einen P-Mode für eine übermittelte ausgehende Nachricht zu instanziieren und dabei Parameterwerte für **PMode.Responder.Party, PMode[].Security.X509.Encryption.Certificate** und **PMode[].Protocol.Address** zu überschreiben.

2.3.3 MPC

Das optionale ebMS3-Attribut mpc auf UserMessage wird hauptsächlich zur Unterstützung der Pull-Funktion verwendet (Abschnitt 2.2.2). Daher wird die Verwendung von mpc profiliert. Das Attribut:

- MUSS in der AS4-UserMessage vorhanden sein, wenn die Pull-Funktion verwendet wird. Ist dies der Fall, MUSS er auf den Wert http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC gesetzt werden, der die Standard-MPL kennzeichnet. Andere Werte DÜRFEN NICHT verwendet werden.
- KANN in der AS4 UserMessage weggelassen werden, wenn die Push-Funktion verwendet wird. Dies entspricht dem Vorhandensein des Standard-MPL-Wertes.

2.3.4 Sicherheit

Dieser Abschnitt definiert die Konfiguration und die Verwendung in der Sicherheit.

2.3.4.1 Network-Layer

Jede Organisation ist dafür verantwortlich, bewährte Sicherheitsverfahren in ihrer IT-Infrastruktur zu implementieren.

Die in diesem Profil beschriebenen Kommunikationsendpunkte werden durch DNS-Namen und nicht durch IP-Adressen bestimmt.

2.3.4.2 Transport-Layer

Sollte der TLS-Kanal nicht auf dem AS4-Adapter terminieren, gelten die Anforderungen aus dem Abschnitt 2.2.6.1.1.

2.3.4.3 Message-Layer

Die folgenden Parameter konfigurieren die Sicherheit auf der Nachrichtenebene:

- Der Parameter **PMode[1].Security.X509.Signature.Certificate** MUSS gemäß den in Abschnitts 2.3.4.4 Anforderungen spezifiziert werden.
- Der Parameter **PMode[1].Security.X509.Encryption.Certificate** MUSS gemäß den in Abschnitt 2.3.4.4Anforderungen spezifiziert werden.
- Die WS-Security-Option für den Verweis auf ein Sicherheits-Token beim Signieren von Nachrichten MUSS *BinarySecurityToken* sein, die WS-Security-Option für den Verweis auf ein Sicherheits-Token beim Verschlüsseln von Nachrichten MUSS *x509SKI* sein.

2.3.4.4 Zertifikate und Public Key-Infrastruktur

In diesem Nutzungsprofil werden X.509-Zertifikate verwendet, um sowohl die Kommunikation auf der Transportschicht als auch auf der Nachrichtenschicht zu sichern.

Für die Signatur, die Verschlüsselung und den Aufbau der TLS-Verbindung MÜSSEN unterschiedliche Schlüsselpaare verwendet werden. Die Schlüsselpaare MÜSSEN EC-basiert sein.

Die für die AS4-Kommunikation verwendeten Zertifikate MÜSSEN von einer CA der SM-PKI ausgestellt sein. Die MP-ID MUSS Teil des Zertifikatsgegenstandsnamens sein und mit der PartyId übereinstimmen (Abschnitt 2.3.1.1).

2.3.4.5 Zertifikatsprofil

Um die Authentizität und Vertraulichkeit der Kommunikation zwischen den einzelnen Marktkommunikationsteilnehmern (MAK) zu gewährleisten, wurde eine Smart Metering Public Key Infrastructure (SM-PKI) eingerichtet.

Marktkommunikationsteilnehmer MÜSSEN die von einer CA der SM-PKI ausgestellten Zertifikate verwenden.

Weitere Informationen über die Zeugnisvorlage finden Sie unter [CPSM-PKI].

2.3.5 Payload Data-Profil

Im AS4-Profil des BDEW ist das AS4-Protokoll vom Geschäftsprozess entkoppelt und es werden feste Werte für den Service und die Aktion verwendet.

Daher ist es für einen Empfänger nicht möglich, die Nutzdaten anhand des Tupels Service/Action zu identifizieren.

Dieses Profil verwendet strukturierte Geschäftsinformationen, die mit Hilfe von Eigenschaften namens

- BDEWDocumentType
- BDEWDocumentDate
- BDEWDocumentNo
- BDEWFulfillmentDate
- BDEWSubjectPartyID
- BDEWSubjectPartyRole

die in den *PayloadInfo/PartInfo/PartProperties* enthalten sind. Dies ermöglicht es den Empfängern, die Struktur des Dokuments zu validieren und die Payloads aus geschäftlicher Sicht zu interpretieren.

Eigenschaften KÖNNEN entsprechend den von der RzÜ definierten Nutzungsprofilen/Services verwendet werden.

Der Inhalt dieser Eigenschaften wird zusammen mit der Nutzlast an den AS4-Server übertragen. Eine empfangende Partei KANN die durch diese Eigenschaften gegebenen Informationen nutzen, indem sie die Informationen an weitere Systeme weitergibt. Die Werte und Formate der oben definierten Eigenschaften sind nicht in diesem Profil beschrieben.

Bei Verwendung des ebMS3-Testdienstes (Abschnitt 2.3.6) gelten keine XML-Schemaeinschränkungen für die enthaltenen Nutzdaten.

2.3.6 Test-Service

Abschnitt 5.2.2 von [EBMS3] definiert eine Server-Testfunktion, die es einer Organisation ermöglicht, einen Kommunikationspartner "anzupingen". Die Funktion basiert auf Nachrichten mit den Werten von:

- **UserMessage/CollaborationInfo/Service** set to http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service
- **UserMessage/CollaborationInfo/Action** set to http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test.

Bitte beachten Sie, dass das Attribut Diensttyp nicht erforderlich ist, wenn der Wert des Dienstes eine URL ist.

In diesem Profil MUSS die Funktion "Testdienst" unterstützt werden, damit die Beteiligten einen grundlegenden Test der Kommunikationskonfiguration (einschließlich Sicherheit auf Netz-, Transport- und Nachrichtenebene sowie Zuverlässigkeit) mit jedem ihrer Kommunikationspartner durchführen können.

Das AS4-Produkt MUSS so konfiguriert werden, dass Nachrichten mit diesen Werten nicht an eine Geschäftsanwendung geliefert werden.

2.3.7 AS4 Transmission Path Change

Dieses AS4-Profil beschreibt eine Kommunikation innerhalb der SM-PKI gemäß [Verweis auf TR Kapitel Marktkommunikation].

Wesentliche Merkmale sind daher:

Zertifikate der SM-PKI sind grundsätzlich vertrauenswürdig und bedürfen keiner weiteren Validierung für den Aufbau der TLS-Verbindung. Zertifikate MÜSSEN in Bezug auf eine gültige Signatur und einen Sperrstatus validiert werden. Gültige, von der SM-PKI ausgestellte Zertifikate reichen aus, um authentische Informationen über die Identität (des Marktpartners) zu liefern.

Eine Implementierung, die diesem Profil entspricht, darf neben der zertifikatsbasierten Autorisierung keine zusätzlichen Zugangsbeschränkungen wie IP-basierte Firewalls haben. Zertifikate KÖNNEN jedoch auf der Grundlage der MP-ID im OU-Feld abgelehnt werden (Whitelist).

Die aktuellen Kommunikationsregeln der Marktkommunikation beschreiben verschiedene Übertragungswege wie E-Mail oder AS2.

Mit dem hier beschriebenen Dienst "Übertragungswegwechsel" wird der Kommunikationspartner aufgefordert, zukünftig ausschließlich den Übertragungsweg AS4 für den Austausch von Nachrichten innerhalb der Marktkommunikation zu nutzen.

Vorbehaltlich der oben genannten Anforderungen kann diese Nachricht von jedem Teilnehmer der SM-PKI gesendet und empfangen werden.

Ein Teilnehmer muss die folgenden Schritte ausführen, um die AS4-Übertragungspfadmeldungen auszutauschen und zu bestätigen, dass die AS4-Kommunikation erfolgreich ist:

› Teilnehmer A sendet eine Nachricht mit dem Service https://www.bdew.de/as4/communication/services/**pathSwitch** und die Action **https://www.bdew.de/as4/communication/actions/requestSwitch**

› Teilnehmer B antwortet mit einer neuen Nachricht mit dem Service **https://www.bdew.de/as4/communication/services/pathSwitch** und die Action https://www.bdew.de/as4/communication/actions/**confirmSwitch** wenn der Wechsel des Übertragungsweges unterstützt wird

› Die zwischen Partei A und Partei B ausgetauschten Nachrichten MÜSSEN keine Nutzdaten enthalten

Wie in Abschnitt 2.3.6 beschrieben, wird die Kommunikationskonfiguration (einschließlich der Sicherheit auf Netz-, Transport- und Nachrichtenebene sowie der Zuverlässigkeit) beim Austausch von Übertragungswegnachrichten zwischen den Kommunikationspartnern geprüft.

Die in der Testnachricht verwendeten Werte für Service, Action und AgreementRef sind in den Abschnitten 2.3.6 und 2.3.2 beschrieben.

Sobald beide Parteien erfolgreich Nachrichten über den Übertragungsweg ausgetauscht haben, gilt der Wechsel zum AS4-Protokoll als erfolgreich.

Von diesem Zeitpunkt ist es für Partei A und B ERFORDERLICH, AS4 für den Nachrichtenaustausch zu verwenden.

3 Verarbeitungsmodi

P-Mode Parameter	Festwert in diesem Profil
PMode.ID	Wird in diesem Profil nicht verwendet.
PMode.Agreement	https://www.bdew.de/as4/communication/agreement Die Attribute @pmode und @type werden nicht verwendet.
PMode.MEP	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/oneWay
PMode.MEPBinding	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/push http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/pull

P-Mode Parameter	Festwert in diesem Profil
PMode.Initiator.Party	Die MP-ID des BDEW; Das Attribut @type ist erforderlich und hat einem statischen Wert urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088
PMode.Initiator.Role	Statischer Wert: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator
PMode.Initiator.Authorization.username	Wird nicht in diesem Profil verwendet.
PMode.Initiator.Authorization.password	Wird nicht in diesem Profil verwendet.
PMode.Responder.Party	Die MP-ID des BDEW; Das Attribut @type ist erforderlich und hat einen festen Wert urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088
PMode.Responder.Role	Statischer Wert: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder
PMode.Responder.Authorization.username	Wird nicht in diesem Profil verwendet.
PMode.Responder.Authorization.password	Wird nicht in diesem Profil verwendet.
PMode[1].Protocol.Address	Erforderlich, HTTPS-URL des Empfängers.
PMode[1].Protocol.SOAPVersion	1.2
PMode[1].BusinessInfo.Service	Mögliche Werte: • https://www.bdew.de/as4/communication/services/MP • https://www.bdew.de/as4/communication/services/FP • https://www.bdew.de/as4/communication/services/RD https://www.bdew.de/as4/communication/services/KW https://www.bdew.de/as4/communication/services/SO • http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test • https://www.bdew.de/as4/communication/services/pathSwitch

P-Mode Parameter	Festwert in diesem Profil
	Mehr Details finden sich in Abschnitt 2.3.1.2.1.
PMode[1].BusinessInfo.Action	Mögliche Werte: • http://docs.oasis-open.org/ebxml- msg/as4/200902/action • http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/test • https://www.bdew.de/as4/communication/actions/confirmSwitch • https://www.bdew.de/as4/communication/actions/requestSwitch Mehr Details finden sich in Abschnitt 2.3.1.2.2.
PMode[1].BusinessInfo. Properties	Unterstützung ist ERFORDERLICH.
PMode[1].BusinessInfo.MPC	Entweder nicht verwendet oder (gleichwertig) ebMS3 Standard-MPC.
PMode[1].Errorhandling.Report. SenderErrorsTo	Wird nicht in diesem Profil verwendet.
PMode[1].Errorhandling.Report. ReceiverErrorsTo	Wird nicht in diesem Profil verwendet.
PMode[1].Errorhandling.Report. AsResponse	True
PMode[1].Errorhandling.Report. ProcessErrorNotifyConsumer	True (empfohlen)
PMode[1].Errorhandling. DeliveryFailuresNotifyProducter	True (empfohlen)
PMode[1].Reliability	Wird nicht in diesem Profil verwendet.
PMode[1].Security.WSSversion	1.1.1
PMode[1].Security.X509.Sign	True[1]

[1] Support required. Encrypt.Element[] ist leer. Encrypt.Attachement[] darf nicht leer sein.

P-Mode Parameter	Festwert in diesem Profil
PMode[1].Security. X509. Signature.Certificate	Unterschriftszertifikat des Absenders.
PMode[1].Security. X509. Signature.HashFunction	http://www.w3.org/2001/04/xmlenc#sha256
PMode[1].Security.X509. Signature.Algorithm	http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
PMode[1].Security.X509. Encryption.Encrypt	True[2]
PMode[1].Security.X509. Encryption.Certificate	Verschlüsselungszertifikat des Empfängers.
PMode[1].Security.X509. Encryption.Algorithm	http://www.w3.org/2009/xmlenc11#aes128-gcm
PMode[1].Security.X509. Encryption.MinimalStrength	128
PMode[1].Security. UsernameToken. username	Wird nicht in diesem Profil verwendet.
PMode[1].Security. UsernameToken. password	Wird nicht in diesem Profil verwendet.
PMode[1].Security. UsernameToken.Digest	Wird nicht in diesem Profil verwendet.
PMode[1].Security. UsernameToken.Nonce	Wird nicht in diesem Profil verwendet.
PMode[1].Security. UsernameToken.Created	Wird nicht in diesem Profil verwendet.

[2] Support required. Encrypt.Element[] ist leer. Encrypt.Attachement[] darf nicht leer sein.

P-Mode Parameter	Festwert in diesem Profil
PMode[1].Security. PModeAuthorize	False
PMode[1].Security.SendReceipt	True
PMode[1].Security.SendReceipt. NonRepudiation	True
PMode[1].Security.SendReceipt. ReplyPattern	Response
PMode[1].PayloadService. CompressionType	application/gzip
PMode[1].ReceptionAwareness	True
PMode[1].ReceptionAwareness. Retry	True
PMode[1].ReceptionAwareness. Retry.Parameters	Wird nicht in diesem Profil verwendet.
PMode[1].ReceptionAwareness. DuplicateDetection	True
PMode[1].ReceptionAwareness. DetectDuplicates.Parameters	Wird nicht in diesem Profil verwendet.
PMode[1].BusinessInfo. subMPCext	Wird nicht in diesem Profil verwendet.

4 Beispiele

4.1 Austausch einer UserMessage

In diesem Szenario wird eine UserMessage, die ein Geschäftsdokument enthält, von einem Teilnehmer (C2) mit der MP-ID 9900000000001 an einen Teilnehmer (C3) mit der MP-ID 9900000000002 gesendet.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/"
              xmlns:ns2="http://www.w3.org/2003/05/soap-envelope" ns2:mustUnderstand="true">
    <eb:UserMessage mpc="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC">
        <eb:MessageInfo>
            <eb:Timestamp>2021-06-15T15:12:10.000Z</eb:Timestamp>
            <eb:MessageId>9a0c6088-70ac-43b1-ab57-2f9d1f0204b7@domibus.eu</eb:MessageId>
        </eb:MessageInfo>
        <eb:PartyInfo>
            <eb:From>
                <eb:PartyId type="urn:oasis:names:tc:ebcore:partyid-
type:iso6523:0088">9900000000001</eb:PartyId>
                <eb:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator</eb:Role>
            </eb:From>
            <eb:To>
                <eb:PartyId type="urn:oasis:names:tc:ebcore:partyid-
type:iso6523:0088">9900000000002</eb:PartyId>
                <eb:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder</eb:Role>
            </eb:To>
        </eb:PartyInfo>
        <eb:CollaborationInfo>
            <eb:AgreementRef>https://www.bdew.de/as4/communication/agreement</eb:AgreementRef>
            <eb:Service>http://docs.oasis-open.org/ebxml-msg/as4/200902/service</eb:Service>
            <eb:Action>http://docs.oasis-open.org/ebxml-msg/as4/200902/action</eb:Action>
            <eb:ConversationId>3d7e144f-f1ea-434d-aa4e-7a722f44a59d@domibus.eu</eb:ConversationId>
        </eb:CollaborationInfo>
        <eb:MessageProperties>
        </eb:MessageProperties>
        <eb:PayloadInfo>
            <eb:PartInfo href="cid:message">
                <eb:PartProperties>
                    <eb:Property name="MimeType">application/octet-stream</eb:Property>
                    <eb:Property name="CompressionType">application/gzip</eb:Property>
                          <eb:Property name="BDEWDocumentType">MSCONS</eb:Property>
                          <eb:Property name="BDEWDocumentDate">202205011630</eb:Property>
                          <eb:Property name="BDEWDocumentNo">1234567AB</eb:Property>
                </eb:PartProperties>
            </eb:PartInfo>
        </eb:PayloadInfo>
    </eb:UserMessage>
</eb:Messaging>
```

5 Quellenverzeichnis

[EDEL-AS4] eDelivery AS4 Profile https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4

[AES] Advanced Encryption Standard. FIPS 197. NIST, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[AS4] AS4 Profile of ebMS 3.0 Version 1.0. OASIS Standard, 23 January 2013. http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/

[AU] ebCore Agreement Update Specification Version 1.0. OASIS Committee Specification. 19 September 2016. http://docs.oasis-open.org/ebcore/ebcore-au/v1.0/

[BP20] Basic Profile Version 2.0. OASIS Committee Specification. http://docs.oasis-open.org/ws-brsp/BasicProfile/v2.0/BasicProfile-v2.0.pdf

[BSIALG] Entwurf Algorithmenkatalog 2014. Bundesamt für Sicherheit in der Informationstechnik (BSI). Bonn, 11 Oktober 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/Algorithmenkatalog_Entwurf_2013.pdf?__blob=publicationFile.

[BSITLS] Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung. Bundesamt für Sicherheit in der Informationstechnik (BSI). Bonn, 08 Oktober 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf

[CEF] eDelivery Specification. Connecting Europe Facility (CEF). Brüssel, 11. November 2020. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.15

[EBMS3] OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features. OASIS Standard. 1 October 2007. http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/

[EIC] ENTSOG. Energy Identification Coding Scheme (EIC) for natural gas transmission. Party Codes. http://www.entsog.eu/eic-codes/eic-party-codes-x

[EIN] Bundesnetzagentur. Beschluss zur Festlegung von Datenaustauschprozessen im Rahmen eines Energieinformationsnetzes (Strom). BK6-13-200.

[EN 319 411-1] European Standard. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, v1.1.1, 2016-02. (Formerly [ETSI EN 319 411-3]) http://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf

[EN 319 412-3] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons. http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf

[EN 319 412-4] Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates. http://www.etsi.org/deliver/etsi_en/319400_319499/31941204/01.01.01_60/en_31941204v010101p.pdf

[ENTSOECL] ENTSO-E Code List V46R0 and core components. https://www.entsoe.eu/publications/electronic-data-interchange-edi-library/work%20products/general/Pages/default.aspx

[ENTSOGAS4] ENTSOG AS4 Profile. http://www.entsog.eu/publications/as4#AS4-USAGE-PROFILE

[EMPAS4] AS4 Energy Market Profile https://www.nedu.nl/wp-content/uploads/2020/10/AS4-Energy-Market-Profile-v1.0.pdf

[FPM] PG-FPM. Fahrplananmeldung in Deutschland mit Hilfe des entso-e Scheduling System (ESS). Version 4.0. 27.04.2015.

[GLN] GS1 Global Location Number (GLN). http://www.gs1.org/gln

[KWNB] Formate und Prozess Kraftwerk Nichtverfügbarkeit.

[MP-ID] BDEW-Codenummern. Marktpartneridentifikationsnummer. https://bdew-codes.de/Codenumbers/BDEWCodes

[OSSLTLS] OpenSSL TLS 1.2 Cipher Suites. http://www.openssl.org/docs/apps/ciphers.html#TLS_v1_2_cipher_suites.

[RFC2119] A. Ramos. Key words for use in RFCs to Indicate Requirement Levels. IETF RFC 2119. January 1998. http://www.ietf.org/rfc/rfc2119.txt

[RFC2822] P. Resnick. Internet Message Format https://tools.ietf.org/html/rfc2822

[RFC5246] T. Dierks et al. The Transport Layer Security (TLS) Protocol Version 1.2. IETF RFC 5246. August 2008. http://tools.ietf.org/html/rfc5246

[RFC6090] Fundamental Elliptic Curve Cryptography Algorithms https://tools.ietf.org/html/rfc6090

[RFC6176] S. Turner et al.Prohibiting Secure Sockets Layer (SSL) Version 2.0. RFC 6176. March 2011. http://tools.ietf.org/html/rfc6176

[RFC6555] D. Wing et al. Happy Eyeballs: Success with Dual-Stack Hosts. http://tools.ietf.org/html/rfc6555

[TLSSP] Transport Layer Security (TLS) Parameters. Last Updated 2016-09-30. http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml

[TR-02102-1] BSI TR-02102-1. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Version 2016-01.

[TR-02102-2] Technische Richtlinie TR-02102-2. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2. Verwendung von Transport Layer Security (TLS).

[TR-03116-3] Kryptographische Vorgaben für Projekte der Bundesregierung
Teil 3: Intelligente Messsysteme

[TR-03116-4] Kryptographische Vorgaben für Projekte der Bundesregierung
Teil 4: Kommunikationsverfahren in Anwendungen

[TS119312] ETSI TS 119 312 V1.1.1 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf

[WSSSMS] OASIS Web Services Security: SOAP Message Security Version 1.1.1. OASIS Standard, May 2012. http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SOAPMessageSecurity-v1.1.1.doc

[WSSSWA] OASIS Web Services Security: Web Services Security SOAP Message with Attachments (SwA) Profile Version 1.1.1. OASIS Standard, May 2012.
http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SwAProfile-v1.1.1.doc

[WSSX509] OASIS Web Services Security: Web Services Security X.509 Certificate Token Profile Version 1.1.1. OASIS Standard, May 2012.
http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-x509TokenProfile-v1.1.1.doc

[XMLDSIG] XML Signature Syntax and Processing (Second Edition). W3C Recommendation 10 June 2008. http://www.w3.org/TR/2008/REC-xmldsig-core-20080610

[XMLDSIG1] XML Signature Syntax and Processing Version 1.1. W3C Recommendation 11 April 2013. http://www.w3.org/TR/xmldsig-core1/

[XDSIGBP] XML Signature Best Practices. W3C Working Group Note 11 April 2013.
http://www.w3.org/TR/2013/NOTE-xmldsig-bestpractices-20130411/

[XMLENC] XML Encryption Syntax and Processing. W3C Recommendation 10 December 2002. http://www.w3.org/TR/xmlenc-core/

[XMLENC1] XML Encryption Syntax and Processing Version 1.1. W3C Recommendation 11 April 2013. http://www.w3.org/TR/xmlenc-core1/

[CPSM-PKI] Certificate Policy der Smart Metering PKI 1.2.0, 2021.

[eDelivery-EBCORE] eDelivery ebCore Party Id Specification
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+ebCore+Party+ID