Konsolidierte Lesefassung mit Fehlerkorrekturen

Stand: 12.05.2023

BDEW AS4-Profil

AS4-Nutzungsprofil zum Datenaustausch für regulierte Prozesse in der Energiewirtschaft

Version:	1.0
Ursprüngliches Publikationsdatum:	01.10.2022
Anzuwenden ab:	01.10.2023
Autor:	BDEW

Inhaltsverzeichnis

1 Einleitung 4
1.1 Terminologie 4
1.2 Bezüge zu Standards 4
2 BDEW AS4-Profil 5
2.1 AS4-Konformitätsprofil 5
2.1.1 AS4-Standard 5
2.1.2 AS4-ebHandler-Konformitätsprofil 5
2.2 Profilerstellung des AS4-ebHandler-Konformitätsprofils 6
2.2.1 Modell zur Nachrichtenübermittlung 6
2.2.2 Nachrichten-Pulling und Nachrichten-Partitionierung 7
2.2.3 Nachrichtenverpackung 8
2.2.3.1 UserMessage 8
2.2.3.2 Payload 9
2.2.3.3 Nachrichtenkomprimierung 9
2.2.4 Fehlerbehandlung 9
2.2.5 Zuverlässige Nachrichtenübermittlung und Unverfälschbarkeit des Empfangs 10
2.2.6 Sicherheit 10
2.2.6.1 Transportebene 11
2.2.6.2 Inhaltsdatensicherungsebene 11
2.2.7 Netzwerk 15
2.2.8 Konfigurationsmanagement 16
2.3 Nutzungsprofil 16
2.3.1 Message Packaging 16
2.3.1.1 Identifizierung der Marktteilnehmer 16
2.3.1.2 Ausrichtung der Geschäftsprozesse 17
2.3.2 Agreements 18
2.3.3 MPC 19

2.3.4 Sicherheit 19
2.3.4.1 Netzwerk-Ebene 19
2.3.4.2 Transport-Ebene 19
2.3.4.3 Inhaltsdatensicherungsebene 19
2.3.4.4 Zertifikate und Public Key-Infrastruktur 20
2.3.4.5 Zertifikatsprofil 20
2.3.5 Payload Data-Profil 20
2.3.6 Testservice 21
2.3.7 AS4 Transmission Path Change 22
3 Parametrisierung P-Mode-Felder 23
4 Beispiele 27
4.1 Austausch einer UserMessage 27
5 Quellen 28
6 Änderungshistorie 30

1 Einleitung

Dieses Dokument definiert ein AS4-Nutzungsprofil zum Datenaustausch für regulierte Prozesse in der Energiewirtschaft im deutschen Strom- und Gasmarkt. Es basiert auf dem von der Connecting Europe Facility (CEF) entwickelten Profil eDelivery-AS4 [CEF].

Das hier definierte BDEW AS4-Profil zielt auf eine größtmögliche Kompatibilität mit dem CEF eDelivery AS4-Profil in der Version 1.15 [CEF-AS4] und erweitert dieses technisch, wo es aus regulatorischen Gründen 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 (BSI) 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 gemäß [RFC 2119].

1.2 Bezüge zu 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. https://www.w3.org/TR/xmldsig-core1/

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

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

[TR02102-1] Technische Richtlinie BSI TR-02102. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. [Teil 1]. Version 2023-01.

[TR02102-2] Technische Richtlinie BSI TR-02102-2. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2: Verwendung von Transport Layer Security (TLS). Version 2023-01.

[TR03116-3] Technische Richtlinie BSI TR-03116. Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 3: Intelligente Messsysteme. Stand 2023.

2 BDEW AS4-Profil

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

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

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

Die für dieses Profil spezifischen Sicherheitsanforderungen gelten für:

- Transportverschlüsselung (TLS)
- Hash-Funktion
- Signaturverfahren und -algorithmen
- Verschlüsselungsmethoden und -algorithmen.

2.1 AS4-Konformitätsprofil

2.1.1 AS4-Standard

Dieses Profil basiert auf dem CEF eDelivery AS4-Profil [CEF-AS4], das auf OASIS AS4 [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 BDEW AS4-Profil 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 Struktur dieses Abschnitts spiegelt die Struktur der ebMS3-Core-Spezifikation wieder [EBMS3]. Die in diesem Profil spezifizierten Anforderungen, Eigenschaften und Algorithmen sind, mit einigen Ausnahmen, Unterfälle des AS4-ebHandler-Konformitätsprofil. Dieses Kapitel wählt spezifische Optionen aus, bei denen das AS4-ebHandler-Konformitätsprofil mehrere Möglichkeiten bietet, und definiert die technischen Anforderungen, die in der AS4-Software implementiert werden müssen. Die Struktur dieses Kapitel spiegelt die Struktur der ebMS3-Core- Spezifikation wider [EBMS3].

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

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

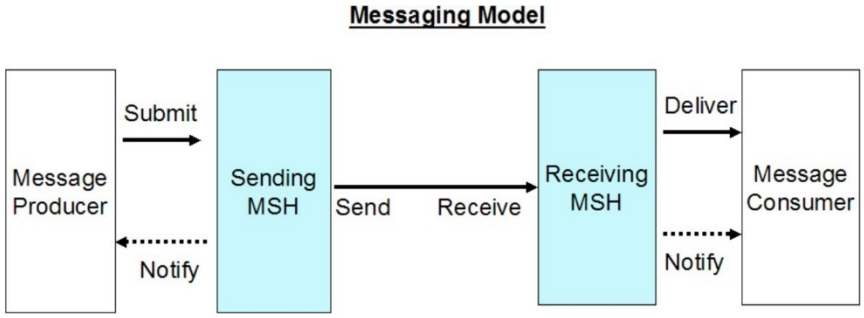

Abbildung 1: Entitäten des AS4-Nachrichtenmodells und ihre Interaktionen [EBMS3].

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 CEF eDelivery AS4 Profil [CEF-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 sein:

- Ein Empfänger hat keine feste IP-Adresse und/oder DNS-auflösbare Serveradresse.
- Ein Empfänger lässt keine eingehenden IP/TCP-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

Die Abbildung 2 zeigt die AS4-Nachrichtenstruktur, die auf SOAP und MIME basiert. Gestrichelte Linien kennzeichnen optionale Komponenten.

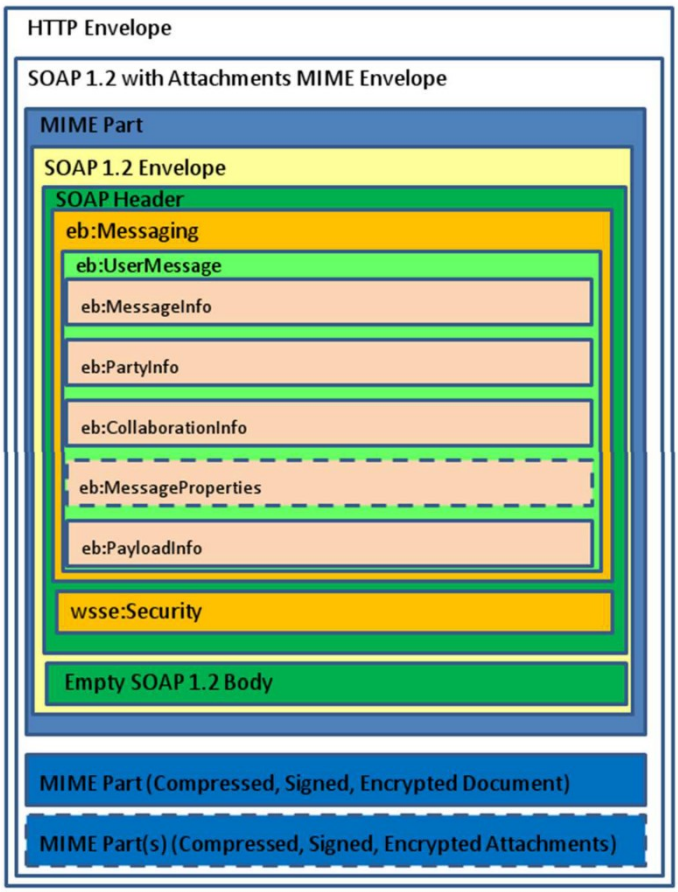

Abbildung 2: AS4 Message Structure, UserMessage [CEF-AS4].

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“ der P-Mode Parameter gemäß [AS4] (Abschnitt 2.1.3.1 und 2.1.3.3) 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 Kapitel 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.

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.

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 Unverfälschbarkeit des Empfangs

Für eine zuverlässige Nachrichtenübermittlung MUSS die nicht abstreitbare AS4-Zustellquittung, englischer Name **Non-Repudiation-Receipts (NRR)**, für jeden Nachrichtenversand synchron vom Empfänger gesendet werden; erst dann ist der Versand für den Sender erfolgreich.

› 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 AS4-Funktion ReceptionAwareness für 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 Datenaustauch über den Übertragungsweg AS4 kann auf mehreren Kommunikationsebenen gesichert werden:

Der Netzwerkebene, der Transportebene, der Nachrichtenebene und der Nutzdatenebene. Die erste und die letzte Ebene werden normalerweise nicht von der Software für AS4 behandelt

und sind daher nicht Gegenstand dieses Kapitels. Die Sicherheit auf der Transportebene wird behandelt, auch wenn ihre Funktionalität auf eine andere Infrastrukturkomponente ausgelagert werden kann.

Dieses Kapitel 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 Kapitel genannten Sicherheits-algorithmen, Formaten und Austauschprotokollen entdeckt werden können. Solche Entdeck-ungen SOLLTEN zu Überarbeitungen dieser Spezifikation führen.

In diesem Profil ist der Datenaustausch über den Übertragungsweg AS4 gesichert auf den zwei Ebenen Transportsicherung und Inhaltsdatensicherung.

2.2.6.1 Transportebene

In diesem AS4-Profil MUSS das Protokoll Transport Layer Security (TLS) eingesetzt werden.

Wenn die TLS Verbindung im AS4 Message Handler beendet wird, MUSS diese TLS Verbindung den Regeln in [TR03116-3] entsprechen. Sie ersetzen die Anforderungen der AS4 Spezifikation. Eine Server- und Client-Authentifizierung ist erforderlich.

Im Besonderen gilt dabei:

› Es MUSS mindestens TLS Version 1.2 vorliegen [RFC5246].

› Es MUSS die Cipher Suites unterstützen, die empfohlen werden in [TR03116-3] (Abschnitt 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 die Anforderungen erfüllen.

2.2.6.2 Inhaltsdatensicherungsebene

Für die Inhaltsdatensicherungsebene MUSS in diesem AS4-Profil die Verwendung folgenden OASIS-Standards für die Sicherheit von Webdiensten der Version 1.1.1, die in ebMS3.0 beschrieben sind, verwendet werden [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]).

Es soll mindestens unterstützt werden:

› CanonicalizationMethod Algorithm = „http://www.w3.org/2001/10/xml-exc-c14n#“

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], 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 [TR03116-3] (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 „http://www.w3.org/2001/04/xmlenc#sha256“ gesetzt werden.

› Der Parameter von **PMode[1]. Security.X509.Signature.Algorithm** MUSS auf den Festwert „http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256“ gesetzt werden.

Die in [RFC6090] Abschnitt 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">
      <!-- X.509 PKIPath 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"
       ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
   </wsse:SecurityTokenReference>
 </ds:KeyInfo>
</ds:Signature>
```

2.2.6.2.2 Verschlüsselung

Die Verschlüsselung in Web Services Security basiert auf der W3C XML Encryption. 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] (Abschnitt 9.2) beschrieben werden.

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] sein.

› Der Parameter von **PMode[1. Security.X509.Encryption.Algorithm** MUSS auf den Festwert „http://www.w3.org/2009/xmlenc11#aes128-gcm“ gesetzt werden. 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) festgelegt sind:

› 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 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 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 [RFC6090] (Abschnitt 7) beschriebenen Interoperabilitätsanforderungen werden umgesetzt.

Beispiel:

```
<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">
  <xenc:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
```

```
3    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
4      <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">
5        <wsse:Reference URI="#EK-50bd3119-caab-4d31-b994-b99c2ad7c9c8"/>
6      </wsse:SecurityTokenReference>
7    </ds:KeyInfo>
8    <xenc:CipherData>
9      <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>
                 MFowFAYHKoZIzj0CAQYJKyQDAwIIAQEHA0IABD4nUMx3iNWJcgxP5DJeBtybV2/B
                 CTqgmAB3fqhdnmSbS9jjZuaModL7efIZfDJEzCz8pkc7V8mhWdJXhZ3kOGw=
33             </dsig11:PublicKey>
34           </dsig11:ECKeyValue>
35         </ds:KeyValue>
36       </xenc:OriginatorKeyInfo>
37       <xenc:RecipientKeyInfo>
38         <ds:X509Data>
39            <ds:X509SKI></ds:X509SKI>
40            <!-- hint for the recipient's private key -->
41         </ds:X509Data>
42       </xenc:RecipientKeyInfo>
43     </xenc:AgreementMethod>
44   </ds:KeyInfo>
45   <xenc:CipherData>
46     <xenc:CipherValue>
47        <!-- encrypted AES content encryption key -->
48     </xenc:CipherValue>
49   </xenc:CipherData>
50   <xenc:ReferenceList>
51     <xenc:DataReference URI="#ED-64914301-0ef1-47fc-b5b0-1297bfd00e45"/>
52   </xenc:ReferenceList>
53 </xenc:EncryptedKey>
```

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 (Kapitel 2.3.6) zu unterstützen, sondern MUSS zusätzlich einen AS4-Übertragungspfadänderungsdienst (Kapitel 2.3.7) implementieren.

2.3 Nutzungsprofil

Dieses Kapitel definiert ein Nutzungsprofil für AS4. Es beschreibt wie AS4-Produkte im Energiemarkt verwendet werden MÜSSEN die in Bezug auf die technischen Spezifikationen in Kapitel 2.2 implementiert sind. Das Konzept des Nutzungsprofils ist in [AS4] Abschnitt 5 definiert. Die Zielgruppe dieses Abschnitts sind Mitarbeiter die AS4 (wie in Abschnitt 2.2 beschrieben) in ihrem Unternehmen implementieren und konfigurieren und für den elektronischen Datenaustausch mit Marktpartnern verantwortlich sind.

Die Struktur dieses Abschnitts spiegelt teilweise die Struktur des ebMS3-Standards [EBMS3] wieder, 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

Das AS4-Feld PartyId ist eine eindeutige Identifikation eines Kommunikationspartners jeweils für Sender und Empfänger.

Beim Datenaustausch gemäß diesem AS4-Profil MÜSSEN die Marktpartner eine Marktpartner-Identifikationsnummer (MP-ID)[1] für den Energiemarkt bei der Codenummerndatenbank verwenden für das Feld PartyID.

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

[1] Details siehe EDI@Energy-Dokument Allgemeine Festlegungen (ALF).

› Bei Verwendung der vom BDEW zugewiesenen MP-ID die lautet 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:unregistered:DVGW

2.3.1.2 Ausrichtung der Geschäftsprozesse

Mehrere obligatorische Felder in AS4 werden verwendet, um Metadaten zu übermitteln, die einen Datenaustausch mit einem Geschäftsprozess oder einem technischen Dienst zu kennzeichnen.

2.3.1.2.1 Service

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

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

› Marktprozesse:
„https://www.bdew.de/as4/communication/services/MP“
› Fahrplan:
„https://www.bdew.de/as4/communication/services/FP“
› Redispatch 2.0 Prozessdaten:
„https://www.bdew.de/as4/communication/services/RD“
› KWEP:
„https://www.bdew.de/as4/communication/services/KW”
› System Operation Guideline:
„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 AS4-Testservice (Kapitel 2.3.6) verwendet einen eigenen Wert für den Dienst. Der folgende Wert MUSS verwendet werden:

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

Der AS4-Service zur Änderung des Übertragungswegs (Kapitel 2.3.7). Der folgende Wert MUSS verwendet werden:

› „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 Action-Festwert für senden Übertragungsdatei:

› „http://docs.oasis-open.org/ebxml-msg/as4/200902/action“

Für den AS4-Testservice (Kapitel 2.3.6) MUSS folgender Action-Wert verwendet werden:

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

Für den AS4-Dienst zur Änderung des Übertragungswegs (Kapitel 2.3.7) MUSS folgende zwei Action unterstützt werden:

› „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”

2.3.1.2.4 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 (Kapitel 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 gesetzt werden, der den Standard-MPL kennzeichnet, also „http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/defaultMPC“. 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

Dieses Kapitel definiert die Konfiguration und die Verwendung in der Sicherheit. Jede Organisation ist dafür verantwortlich, bewährte Sicherheitsverfahren in ihre IT-Infrastruktur zu implementieren.

2.3.4.1 Netzwerk-Ebene

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

2.3.4.2 Transport-Ebene

Sollte der TLS-Kanal nicht auf dem AS4-Adapter terminieren, gelten die Anforderungen aus dem Kapitel 2.2.6.1.

2.3.4.3 Inhaltsdatensicherungsebene

Die folgenden Parameter konfigurieren die Sicherheit auf der Nachrichtenebene:

› Der Parameter **PMode[1].Security.X509.Signature.Certificate** MUSS gemäß den Anforderungen aus Kapitel 2.3.4.4 spezifiziert sein.

- Der Parameter **PMode[1].Security.X509.Encryption.Certificate** MUSS gemäß den Anforderungen aus Kapitel 2.3.4.4 spezifiziert sein.
- 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 AS4-Profil werden X.509-Zertifikate verwendet, um sowohl die Kommunikation auf der Transportebene als auch auf der Inhaltsdatensicherungsebene 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 (Kapitel 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 SM-PKI finden Sie unter [CP-SM-PKI].

2.3.5 Payload Data-Profil

Im AS4-Profil des BDEW ist der AS4-Übertragungsweg 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

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.

Die Eigenschaften KÖNNEN entsprechend den vom EDI@Energy-Dokument Regelungen zum Übertragungsweg (RzÜ) definierten Nutzungsprofilen/Services verwendet werden.

Der Inhalt dieser Metafelder wird zusammen mit der Datenübertragungsdatei 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 (Kapitel 2.3.6) gelten keine XML-Schemaeinschränkungen für die enthaltenen Nutzdaten.

2.3.6 Testservice

Der 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** = „http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/service“.
- **UserMessage/CollaborationInfo/Action** = „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 als Teilnehmer der SM-PKI [CP-SM-PKI]. Dessen Merkmale sind:

- 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 Regelungen zum Übertragungsweg (RzÜ) in der Version 1.x beschreiben verschiedene Übertragungswege wie E-Mail via SMTP oder AS2.

Mit dem hier beschriebenen Dienst Übertragungswegwechsel wird der Kommunikationspartner aufgefordert, zukünftig ausschließlich den Übertragungsweg AS4 für den Austausch von Übertragungsdateien 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, wenn dieser den Wechsel des Übertragungsweges unterstützt, 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“.

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

Wie in Kapitel 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 Kapiteln 2.3.2 und 2.3.6 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 Parametrisierung P-Mode-Felder

P-Mode Parameter	Festwert in diesem Profil
PMode.ID	Wird nicht in diesem Profil 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
PMode.Initiator.Party	Die MP-ID des BDEW. Das Attribut @type ist erforderlich und hat einem Festwert 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 Festwert urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088
PMode.Responder.Role	Festwert: http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder

P-Mode Parameter	Festwert in diesem Profil
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 (Kapitel 2.3.1.2.1): • 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
PMode[1].BusinessInfo.Action	Mögliche Werte (Kapitel 2.3.1.2.2): • 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.
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)

P-Mode Parameter	Festwert in diesem Profil
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 Hinweis: Support required. Encrypt.Element[] ist leer. Encrypt.Attachement[] darf nicht leer sein.
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 Hinweis: Support required. Encrypt.Element[] ist leer. Encrypt.Attachement[] darf nicht leer sein.
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.

P-Mode Parameter	Festwert in diesem Profil
PMode[1].Security. UsernameToken.Created	Wird nicht in diesem Profil verwendet.
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 Absender (C2) mit der MP-ID 9900000000001 an einen Empfänger (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></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 Quellen

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

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

[CEF] eDelivery AS4 Profile. Connecting Europe Facility (CEF).
https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery+AS4

[CEF AS4] eDelivery Specification. Connecting Europe Facility (CEF). 11. November 2020.
https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery+AS4+-+1.15

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

[ECAU1] OASIS ebCore Agreement Update, Version 1.0, 18 September 2016.
https://docs.oasis-open.org/ebcore/ebcore-au/v1.0/ebcore-au-v1.0.html

[RFC2119] Key words for use in RFCs to Indicate Requirement Levels.
IETF RFC 2119. March 1997. https://www.rfc-editor.org/rfc/rfc2119

[RFC2822] Internet Message Format.
IETF RFC 2822. April 2011. https://www.rfc-editor.org/rfc/rfc2822

[RFC5246] The Transport Layer Security (TLS) Protocol Version 1.2.
IETF RFC 5246. August 2008. https://www.rfc-editor.org/rfc/rfc5246

[RFC6090] Fundamental Elliptic Curve Cryptography Algorithms.
IETF RFC 6090. February2011. https://www.rfc-editor.org/rfc/rfc6090

[RFC6555] Happy Eyeballs: Success with Dual-Stack Hosts.
IETF RFC 6555. April 2012. https://www.rfc-editor.org/rfc/rfc6555

[TR02102-1] Technische Richtlinie BSI TR-02102. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. [Teil 1]. Version 2023-01.

[TR02102-2] Technische Richtlinie BSI TR-02102-2. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2: Verwendung von Transport Layer Security (TLS). Version 2023-01.

[TR03116-3] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 3: Intelligente Messsysteme. Stand 2023.

[CP-SM-PKI] Certificate Policy der Smart Metering PKI 1.1.2, 2023.

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

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

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

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

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

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

6 Änderungshistorie

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
13000	Deckblatt	Publikationsdatum: 01.09.2022 Anzuwenden ab: 01.10.2023	**Konsolidierte Lesefassung mit Fehlerkorrekturen** **Stand 12.05.2023** **Ursprüngliches** Publikationsdatum: […] Anzuwenden ab: 01.10.2023	Zusätzlich wurden im gesamten Dokument Schreibfehler, Layout, Internetadressen etc. korrigiert, die keinen Einfluss auf die inhaltliche Aussage haben.	Fehler (12.05.2023).
13001	Kapitel 1.2 Bezüge zu Standards	[TR02102-1] Technische Richtlinie BSI TR-02102. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. [Teil 1]. Version 2022-01. [TR02102-2] Technische Richtlinie BSI TR-02102-2. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2: Verwendung von Transport Layer Security (TLS). Version 2022-01. [TR03116-3] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 3: Intelligente Messsysteme. 23. Februar 2022.	[TR02102-1] Technische Richtlinie BSI TR-02102. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. [Teil 1]. Version **2023-01.** [TR02102-2] Technische Richtlinie BSI TR-02102-2. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2: Verwendung von Transport Layer Security (TLS). Version **2023-01**. [TR03116-3] Technische Richtlinie BSI TR-03116**.** Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 3: Intelligente Messsysteme. **Stand 2023.**	Aktualisierung Quellen des BSI.	Fehler (12.05.2023).
13002	Kapitel 2.2.6.2.1 Signatur	1 <wsse:BinarySecurityToken EncodingType=[…] 3 ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#**X509v3**" 4 […]> 5 <!-- X.509 **v3** binary security token base64 encoded -->	1 **<wsse:BinarySecurityToken** EncodingType= […] ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#**X509PKIPathv1**" […]> **2** *<!-- X.509 **PKIPath** binary security token base64 encoded -->*	Korrektur Code-Zeilennummerierung (inklusive Hintergrund), Code-Zeilenumbrüche und Codeformatierung (fett, kursiv). Korrektur Zeile 1 (ValueType). Korrektur Zeile 2 (Kommentar).	Fehler (12.05.2023).

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
13003	Kapitel 2.2.6.2.2 Verschlüsselung	39 <xenc:RecipientKeyInfo> 40 <ds:X509Data> 41 <ds:X509IssuerSerial> 42 <ds:X509IssuerName> CN=QuoVadis Europe Advanced CA G1,O=QuoVadis Trustlink Deutschland GmbH,2.5.4.97=#0c1156415444452d444532 3936383938333832,C=DE</ds:X509IssuerName> 43 <ds:X509SerialNumber> 48588717377041651353730336049164528487855286096</ds:X509SerialNumber> 44 </ds:X509IssuerSerial> 45 </ds:X509Data> 46 </xenc:RecipientKeyInfo>	**37** <xenc:RecipientKeyInfo> **38** <ds:X509Data> **39** **<ds:X509SKI></ds:X509SKI>** **40** ***<!-- hint for the recipient's private key -->*** **41** </ds:X509Data> **42** </xenc:RecipientKeyInfo>	Korrektur Code-Zeilennummerierung (inklusive Hintergrund), Code-Zeilenumbrüche und Codeformatierung (fett, kursiv). Korrektur Codeabschnitt <xenc:RecipientKeyInfo>.	Fehler (12.05.2023).
13004	Kapitel 2.3.1.1 Identifizierung der Marktteilnehmer	• urn:oasis:names:tc:ebcore:partyid-type:unregisteredDVGW	• urn:oasis:names:tc:ebcore:partyid-type:unregistered:DVGW	Fehlender Doppelpunkt ergänzt im Parameter.	Fehler (12.05.2023).
13005	Kapitel 4.1 Austausch einer UserMessage	<eb:ConversationId> 3d7e144f-f1ea-434d-aa4e-7a722f44a59d@domibus.eu </eb:ConversationId>	<eb:ConversationId> </eb:ConversationId>	Korrektur ConversationId ohne Inhalt.	Fehler (12.05.2023).
13006	Kapitel 5 Quellen	[AES] Advanced Encryption. […] [EIN] Bundesnetzagentur […] [EN 319 411-1] European […] [EN 319 412-3] Electronic […] [EN 319 412-4] Electronic […] [ENTSOGAS4] ENTSOG AS4 Profile […] [FPM] PG-FPM. Fahrplananmeldung [..] [GLN] GS1 Global Location Number [...] [KWNB] Formate und Prozess […] [MP-ID] BDEW-Codenummern. […] [OSSLTLS] OpenSSL TLS 1.2 […] [TLSSP] Transport Layer Security […] [XMLDSIG] XML Signature Syntax […] [XMLENC] XML Encryption Syntax […]	~~[AES] Advanced Encryption. […]~~ ~~[EIN] Bundesnetzagentur. […]~~ ~~[EN 319 411-1] European […]~~ ~~[EN 319 412-3] Electronic […]~~ ~~[EN 319 412-4] Electronic […]~~ ~~[ENTSOGAS4] ENTSOG AS4 Profile […]~~ ~~[FPM] PG-FPM. Fahrplananmeldung [..]~~ ~~[GLN] GS1 Global Location Number [...]~~ ~~[KWNB] Formate und Prozess […]~~ ~~[MP-ID] BDEW-Codenummern. […]~~ ~~[OSSLTLS] OpenSSL TLS 1.2 […]~~ ~~[TLSSP] Transport Layer Security […]~~ ~~[XMLDSIG] XML Signature Syntax […]~~ ~~[XMLENC] XML Encryption Syntax […]~~	Nicht referenzierte Quelle gestrichen.	Fehler (12.05.2023).

Änd-ID	Ort	Änderungen		Grund der Anpassung	Status
		Bisher	Neu		
13007	Kapitel 5.	[TR02102-1] Technische […]. Version 2022-01. [TR02102-2] Technische […]. Version 2022-01. [TR03116-3] Technische […]. 23. Februar 2022. [CP-SM-PKI] Certificate Policy der Smart Metering PKI 1.2.0, 2021.	[TR02102-1] Technische […]. Version **2023-01.** [TR02102-2] Technische […]. Version **2023-01**. [TR03116-3] Technische […]. **Stand 2023**. [CP-SM-PKI] Certificate Policy der Smart Metering PKI **1.1.2, 2023**.	Aktualisierung Quellen des BSI.	Fehler (12.05.2023).