

<b>Elektronische Zustellung Anzeigemodul</b>		<b>Konvention</b>
		<b>zuseamod-2.4.0</b>
		<b>Entwurf intern</b>
Kurzbeschreibung	Dieses Dokument spezifiziert die bilaterale Schnittstelle zwischen Zustellsystemen und dem Anzeigemodul. Dies umfasst die Definition sämtlicher Metadaten, die von Zustellsystemen an das Anzeigemodul im Zuge einer Zustellung bzw. Zusendung anfallen können bzw. die Übermittlung von Nachrichtenoperation zwischen Anzeigemodul und Zustellsystem sowie die Übertragung von Dateianhängen im Zuge der Abholung von Zustellungen bzw. Zusendungen.	
Autor(en):	Arne Tauber	Projektteam / Arbeitsgruppe:
		AG-II
Beiträge von:	-	

Version 2: <b>09.04.2019</b>	Fristablauf:
Abgelehnt von:	(Länderangabe bei ablehnender Stellungnahme)

Unter-Version 2.4: <b>XX.XX.2024</b>	Fristablauf: <b>XX.XX.2024</b>
Abgelehnt von:	(Länderangabe bei ablehnender Stellungnahme)

Detail-Version 2.4.0: <b>XX. XX.2024</b>	Fristablauf: <b>XX.XX.2024</b>
Anmerkungen:	(Detailangaben zur Freigabe)

## Inhaltsverzeichnis

<b>Elektronische Zustellung Anzeigemodul.....</b>	<b>1</b>
<b>1 Allgemeines .....</b>	<b>7</b>
1.1 Änderungen zu Version 2.3.0.....	7
1.2 Änderungen zu Version 2.2.0.....	8
1.3 Änderungen zu Version 2.1.3.....	8
1.4 Änderungen zu Version 2.1.2.....	9
1.5 Änderungen zu Version 2.1.1.....	9
1.6 Änderungen zu Version 2.1.0.....	9
1.7 Änderungen zu Version 2.0.0.....	9
1.1 SOAP-Webservice Kommunikation.....	10
1.2 Namespaces.....	10
1.3 Schlüsselwörter.....	11
1.4 Glossar .....	11
<b>2 Authentifizierung.....</b>	<b>12</b>
2.1 Teilnehmer des Portalverbunds .....	12
2.2 Nicht Teilnehmer des Portalverbunds .....	12
<b>3 Übermittlung von Metadaten .....</b>	<b>13</b>
3.1 Metadaten Definitionen und Verzeichnis .....	13
3.1.1 Allgemeines zur Definition von Metadaten .....	13
3.1.1.1 Syntaxangaben / Augmented BNF.....	13
3.1.1.2 BNF Syntax .....	13
3.1.2 Technische Informationen.....	13
3.1.2.1 Systemweit eindeutige Zustell-ID (ZS-DELIVERY-ID).....	13
3.1.2.2 Versender (SENDER) .....	14
3.1.2.3 Versender Identifikationsdaten (SENDER-IDENTIFIER).....	14
3.1.2.4 ID-Typ des Senders (SENDER-IDENTIFIER-TYPE).....	14
3.1.2.5 ID-Value des Senders (SENDER-IDENTIFIER-VALUE) .....	15
3.1.2.6 Versender Personendaten (SENDER-*) .....	16
3.1.2.7 Versenderdaten Unternehmen (SENDER-CB) .....	16
3.1.2.8 Versenderdaten Unternehmensname (SENDER-CB-FULLNAME).....	16
3.1.2.9 Versenderdaten Behördenname (SENDER-CB-ORGANIZATION) .....	17
3.1.2.10 Versenderdaten Behörde Target (SENDER-CB-TARGET) .....	18
3.1.2.11 Zusätzliche Daten Versender (SENDER-ADD) .....	18
3.1.2.12 Zusätzliche Daten Versender Mailbox (SENDER-ADD-MAILBOX).....	19
3.1.2.13 Zusätzliche Daten Versender Rollen (SENDER-ADD-ROLES).....	19
3.1.2.14 Zusätzliche Daten Versender Rolle (SENDER-ADD-ROLE) .....	20
3.1.2.15 Zusätzliche Daten Versender Zu Handen (SENDER-ADD-CAREOF) .....	20
3.1.2.16 Versender Zu Handen Elektronische Adresse (SENDER-ADD-CAREOF-EADDR).....	21
3.1.2.17 Versender Zu Handen E-Mail (SENDER-ADD-CAREOF-EADDR-MAIL) .....	21
3.1.2.18 Versender Zu Handen Name (SENDER-ADD-CAREOF-NAME) .....	22
3.1.2.19 Kontaktadressen (SENDER-CONTACT-ADDRESSES).....	22
3.1.2.20 Kontaktadresse Internet (SENDER-CONTACT-INTERNET).....	23
3.1.2.21 Kontaktadresse Telefon (SENDER-CONTACT-TELEPHONE).....	23
3.1.2.22 Empfänger (RECIPIENT) .....	24
3.1.2.23 Empfänger Identifikationsdaten (RECIPIENT-IDENTIFIER).....	24
3.1.2.24 ID-Typ des Empfängers (RECIPIENT-IDENTIFIER-TYPE).....	24
3.1.2.25 ID-Value des Empfängers (RECIPIENT-IDENTIFIER-VALUE) .....	25
3.1.2.26 Empfänger Personendaten (RECIPIENT-*) .....	26

3.1.2.27 Empfängerdaten Unternehmen (RECIPIENT-CB).....	26
3.1.2.28 Empfängerdaten Unternehmensname (RECIPIENT-CB-FULLNAME) .....	26
3.1.2.29 Empfängerdaten Unternehmen Organisationseinheit (RECIPIENT-CB-ORGANIZATION).....	27
3.1.2.30 Empfängerdaten Behörde Target (RECIPIENT-CB-TARGET).....	28
3.1.2.31 Empfängerdaten Natürliche Person (RECIPIENT-PP) .....	28
3.1.2.32 Empfängerdaten Natürliche Person Vorname (RECIPIENT-PP-GIVENNAME).....	29
3.1.2.33 Empfängerdaten Natürliche Person Familienname (RECIPIENT-PP-FAMILYNAME) .....	29
3.1.2.34 Empfängerdaten Natürliche Person Geburtsdatum (RECIPIENT-PP-DATEOFBIRTH).....	30
3.1.2.35 Zusätzliche Daten Empfänger (RECIPIENT-ADD) .....	30
3.1.2.36 Zusätzliche Daten Empfänger Mailbox (RECIPIENT-ADD-MAILBOX) .....	31
3.1.2.37 Zusätzliche Daten Empfänger Rollen (RECIPIENT-ADD-ROLES) .....	31
3.1.2.38 Zusätzliche Daten Empfänger Rolle (RECIPIENT-ADD-ROLE).....	32
3.1.2.39 Zusätzliche Daten Empfänger Zu Handen (RECIPIENT-ADD-CAREOF).....	32
3.1.2.40 Empfänger Zu Handen Elektronische Adresse (RECIPIENT-ADD-CAREOF-EADDR).....	33
3.1.2.41 Empfänger Zu Handen E-Mail (RECIPIENT-ADD-CAREOF-EADDR-MAIL) .....	33
3.1.2.42 Empfänger Zu Handen Name (RECIPIENT-ADD-CAREOF-NAME).....	34
3.1.2.43 Metadaten (METADATA) .....	34
3.1.2.44 Nachrichten-ID der versendenden Anwendung (APP-DELIVERY-ID) .....	35
3.1.2.45 Herkunftssystem der Zustellung (ORIGIN) .....	35
3.1.2.46 Herkunftssystem Participant-ID (ORIGIN-PARTICIPANT-ID) .....	35
3.1.2.47 Betreff (SUBJECT).....	36
3.1.2.48 Geschäftszahl (GZ) .....	37
3.1.2.49 Zustellqualität (DELIVERY-QUALITY) .....	37
3.1.2.50 Private Qualität der Zusendung (PRIVATE-DELIVERY-QUALITY).....	38
3.1.2.51 Liste der Sprachen für Verständigungen (NOTIFICATION-LANGUAGES).....	39
3.1.2.52 Sprache für Verständigungen (NOTIFICATION-LANGUAGE) .....	39
3.1.2.53 Referenz (REFERENCE) .....	40
3.1.2.54 Referenz (REFERENCE-ZS-DELIVERY-ID) .....	40
3.1.2.55 Tags (TAGS) .....	41
3.1.2.56 Tag (TAG) .....	41
3.1.2.57 Verfahrensspezifische Metadaten (APP-METADATALIST).....	42
3.1.2.58 Verfahrensspezifisches Metadatum (APP-METADATA) .....	42
3.1.2.59 Verfahrensspezifisches Metadatum OID (APP-METADATA-OID) .....	42
3.1.2.60 Verfahrensspezifisches Metadatum Wert (APP-METADATA-VALUE).....	43
3.1.2.61 Anhänge (ATTACHMENTS) .....	43
3.1.2.62 Anhang (ATTACHMENT).....	44
3.1.2.63 ID eines Anhangs (ATTACHMENT-ID).....	44
3.1.2.64 Dateiname eines Anhangs (ATTACHMENT-FILENAME).....	45
3.1.2.65 Dateityp eines Anhangs (ATTACHMENT-MIMETYPE).....	46
3.1.2.66 Dokumentenklasse eines Anhangs (ATTACHMENT-DOCUMENT-CLASS) .....	46
3.1.2.67 Anhang Dateigröße (ATTACHMENT-FILESIZE).....	47
3.1.2.68 Checksumme eines Anhangs (ATTACHMENT-CHECKSUM) .....	47
3.1.2.69 Checksummen Algorithmus eines Anhangs (ATTACHMENT-CHECKSUM-ALGORITHM).....	48
3.1.2.70 Checksummen-Wert eines Anhangs (ATTACHMENT-CHECKSUM-VALUE) .....	48
3.1.2.71 Verschlüsselter Attachmentschlüssel (ATTACHMENT-ENCRYPTED-KEY) .....	49
3.1.2.72 Subject-Key-Identifizier (ATTACHMENT-SUBJECT-KEY-IDENTIFIER) .....	50
3.1.2.73 Verfahrensspezifische Metadaten.....	50
3.1.2.74 Teilbaum, der speziell für das TNVZ bestimmt ist .....	51

3.1.2.75	<i>Zusätzliche Metadaten, die speziell für das TNVZ bestimmt sind</i>	51
3.2	Metadaten Schnittstelle	52
3.2.1	XML Format und Binding	52
3.2.1.1	Authentifizierung	52
3.2.1.2	Format	52
3.2.1.3	Binding	64
<b>4</b>	<b>Übermittlung von Nachrichtenoperationen an Zustellsysteme</b>	<b>65</b>
4.1	Nachrichtenoperationen Definitionen	65
4.2	Abfolge der Nachrichtenoperationen	67
4.2.1	Nachrichtenoperationen, die bei der Zustellqualität „Zustellung bzw. Zusendung ohne Zustellnachweis“ vom AMOD an das Zustellsystem übermittelt werden	68
4.2.2	Nachrichtenoperationen, die bei der Zustellqualität „Zustellung bzw. Zusendung mit Zustellnachweis“ vom AMOD an den Zustelldienst übermittelt werden	69
4.2.3	Nachrichtenoperationen, die bei der Weiterleitung in den ERV an das Zustellsystem übermittelt werden	71
4.3	Nachrichtenoperationen Bindings	72
4.3.1	XML Format und Binding	72
4.3.1.1	Authentifizierung	72
4.3.1.2	Format	72
4.3.1.3	Binding	82
<b>5</b>	<b>Übertragung von Attachments</b>	<b>83</b>
5.1	Authentifizierung	83
5.2	Verschlüsselung von Attachments	83
5.2.1	Symmetrischer Schlüssel	83
5.2.2	Verschlüsselung des symmetrischen Schlüssels	83
5.2.3	Subject-Key-Identifizierung	83
5.3	Attachment Übertragung	83
5.3.1	Request	84
5.3.2	Response	84
5.3.2.1	Erfolgsfall	84
5.3.2.2	Fehlerfall	85
<b>6</b>	<b>Abholung von Zustellstücken</b>	<b>87</b>
6.1	Ein-/Anbindung in Browser durch Internetportale	87
6.1.1	Authentifizierung	87
6.1.1.1	Filtern und setzen von PVP-2.1 HTTP-Headervariablen durch das Internetportal	87
6.1.2	Anbindung durch ein E-Government-Portal für natürliche und juristische Personen	87
6.1.2.1	Liste der PVP2-Header, die vom AMOD interpretiert werden	87
6.1.2.2	Externer Benutzer	89
6.1.2.3	Externer Benutzer, der im Namen einer juristischen Person agiert	90
6.1.2.4	Authentifizierungsmethode	91
6.1.3	Anbindung durch ein Behördenportal für Behördenmitarbeiter	91
6.1.3.1	Liste der PVP2-Header, die vom AMOD interpretiert werden	91
6.1.3.2	Behördenmitarbeiter	92
6.1.4	Fehler	94
6.2	Anzahl der Nachrichten ungelesen und gesamt	94
6.2.1	XML Format und Binding	94
6.2.1.1	Authentifizierung	94
6.2.1.2	Format	94
6.2.1.3	Binding	95
<b>7</b>	<b>Weiterleitung der Nachricht in den Elektronischen Rechtsverkehr der Justiz (ERV)</b>	<b>96</b>

7.1 Weiterleitung einer Zustellung oder Zusendung .....	97
7.1.1 Übermittlung der Zustellung .....	97
7.1.2 Erfolgreiche Weiterleitung in den ERV .....	98
7.1.3 Fehlschlag der Weiterleitung in den ERV .....	99
7.2 Weiterleitung einer Zustellung bzw. Zusendung mit Zustellnachweis .....	100
<b>8 Synchronisation .....</b>	<b>102</b>
8.1 Definition der Verarbeitungsarten.....	102
8.1.1 Synchrone Verarbeitung .....	102
8.1.2 Asynchrone Verarbeitung .....	102
8.1.3 Cronjob.....	102
8.1.4 Retry-Mechanismus .....	102
8.1.5 Timeout .....	102
8.2 Übermittlung einer Nachricht.....	103
8.2.1 Ablauf .....	103
8.3 Asynchrone Übermittlung der Attachments .....	104
8.3.1 Ablauf .....	104
<b>9 Ausnahmebehandlung.....</b>	<b>106</b>
9.1 Das Anzeigemodul verarbeitet den Request, der Response erreicht das Zustellsystem nicht .....	106
9.1.1 Ablauf .....	106
9.1.2 Ausnahmebehandlung .....	107
9.2 Der Request erreicht das Anzeigemodul nicht, der Retry ist erfolgreich .....	107
9.2.1 Ablauf .....	107
9.2.2 Ausnahmebehandlung .....	108
9.3 Der Request erreicht das Anzeigemodul nicht, der Retry inklusive Teilnehmerverzeichnisabfrage sind erfolgreich .....	109
9.3.1 Ablauf .....	109
9.3.2 Positive Ausnahmebehandlung .....	110
9.4 Der Request erreicht das Anzeigemodul nicht, beim Retry ist der Empfänger nicht mehr erreichbar.....	111
9.4.1 Ablauf .....	111
9.4.2 Negative Ausnahmebehandlung.....	112
<b>10 Betriebsüberwachung.....</b>	<b>113</b>
10.1 Cronjob <i>IsAlive</i> des Anzeigemoduls.....	113
10.2 Cronjob <i>IsAlive</i> der Zustellsysteme .....	113
10.3 Cronjob <i>IsAliveEcho</i> .....	113
10.4 XML Format und Binding.....	114
10.4.1 Authentifizierung .....	114
10.4.2 Format .....	114
10.4.2.1 <i>Operation IsAliveEcho</i> .....	114
10.4.2.2 <i>Operation IsAlive</i> .....	116
10.4.3 Binding .....	117
10.4.3.1 SOAP .....	117
10.4.3.2 REST.....	117
<b>11 Protokollierung.....</b>	<b>119</b>
11.1 Löschfrist für fachliche Protokollierungsdaten des Anzeigemoduls.....	119
<b>A. Anhang.....</b>	<b>120</b>
11.2 Beispiel: Blockweise Übertragung von Attachments .....	120
<b>B. Abbildungsverzeichnis .....</b>	<b>122</b>

<b>C. Tabellenverzeichnis .....</b>	<b>123</b>
<b>D. Revision History .....</b>	<b>124</b>
<b>E. Referenzen .....</b>	<b>126</b>

# 1 Allgemeines

Zwischen Zustellsystemen und dem Anzeigemodul müssen laufend Daten ausgetauscht werden. Dafür stellt die E-Zustellung diverse Schnittstellen zur Verfügung, die durch dieses Dokument spezifiziert sind. Diese sind wie folgt:

- Übermittlung von Metadaten vom Zustellsystem an das Anzeigemodul
- Übermittlung von Statusinformationen zwischen Zustellsystem und Anzeigemodul
- Übertragung von Attachments vom Zustellsystem an das Anzeigemodul

Der erste Teil dieser Spezifikation definiert im Detail sämtliche Metadaten, die bei einer Zustellung bzw. Zusendung anfallen können und prinzipiell vom Zustellsystem unterstützt und an das Anzeigemodul übertragen werden können müssen.

## 1.1 Änderungen zu Version 2.3.0

Die wesentlichen Änderungen der Version 2.4.0 zur Zustellspezifikation der Version 2.3.0 sind wie folgt:

- Der Begriff „Zielserver“ wurde auf „sendender E-Mail-Server“ umbenannt
- URL-Action-Links müssen nun wie unter 3.2.1.2.1.5 Anhänge beschrieben übergeben werden
- Aufgrund der Aufteilung des Ergänzungsregisters für sonstige Betroffene (ERsB) in vier einzelne Stammregister wurde der neue übergeordnete Stammzahlentyp **Global Location Number** (`urn:publicid:gv.at:baseid+XGLN`) etabliert, der die Ordnungsnummer des ERsB (`urn:publicid:gv.at:baseid+XERSB`) innerhalb der Elektronischen Zustellung ersetzt
- Im Header `X-PVP-ROLES` ist eine Anpassung des Präfixes des Stammzahlenwerts erforderlich. Anstelle des bisherigen Präfixes "XERSB-" ist zukünftig das Präfix "XGLN-" zu verwenden. Dies betrifft die beiden Rollenparameter `Stammzahl` und `SOURCE`, die in den Rollen `MPK_POSTBEVOLLMAECHTIGTER` und `MPK_REGISTRIERUNG` zum Einsatz kommen
- Im Kapitel 3.2.1.1 und 4.3.1.1 Authentifizierung wurde die Referenz korrigiert und auf die beiden Authentifizierungsvarianten im Detail eingegangen
- Definition von XML SimpleTypes im Namespace `http://reference.e-government.gv.at/namespace/zustellung/types/phase2/20240718#`, um die Feldlängen automatisiert prüfen zu können, wurde hinzugefügt
- Das als „deprecated“ gekennzeichnete Element `msg:ERVDeliveryTimestamp` wurde aus dem XML-Schema entfernt
- Klarstellungen in Formulierungen, Abbildungen und Beispielen, sowie Korrekturen
- Kennzeichnung des HTTP Response-Headers „Content-Length“ als optional statt verpflichtend (siehe Tabelle 7 und Tabelle 8)
- Neues `SubjectKeyIdentifier` Attribut in den Attachment-Metadaten, um den öffentlichen Schlüssel des AMOD X.509 v3 Zertifikats eindeutig identifizieren zu können, mit dem der symmetrische Sessionkey verschlüsselt wurde
- Neuer Fehlercode `ZS0400_U „Bad Request“` für den Fall, dass die Message Operation eindeutig im Widerspruch zur aktuellen Verarbeitung der Nachricht steht.

## 1.2 Änderungen zu Version 2.2.0

Die wesentlichen Änderungen der Version 2.3.0 zur Zustellspezifikation der Version 2.2.0 sind wie folgt:

- E-Mail-Adressen (`msg:InternetAddress`) in der Liste der elektronischen Verständigungsadressen (`msg:NotificationAddressList`) werden als „ungültig“ markiert (`Invalid="true"`), wenn der Zielsystem entweder nicht erreichbar war oder mit einer Bounce-Message geantwortet hat
- Das AMOD retourniert bei nachweislichen und nicht nachweislichen Zustellungen und Zusendungen die Nachrichtenoperation „*NotificationInformation*“, um das Zustellsystem über erfolgreiche und/oder fehlerhafte elektronische Verständigungen zu informieren
- Mehr Transparenz in Fehlerfällen durch zusätzliche Zustellfehler sowie durch die neuen „technischen Fehler“
- Das `msg:Logo` Element wurde aus den Metadaten des Versenders entfernt
- Der Header `X-DELIVERY-AUTH-METHOD` wird nicht mehr unterstützt. Die Authentifizierungsmethode wird nun im PVP-Header `X-PVP-ROLES` im Parameter `AUTH-LEVEL` der Rolle `ZUSE-DISPLAY-SERVICE` übermittelt.
- Die PVP-Header `X-PVP-OU` und `X-PVP-USERID` sind bei E-Government-Portalen für natürliche Personen nur noch optional
- Um Vertretungen für mehr als eine Behörde PVP-spezifikationskonform abbilden zu können, wurde der neue Rollenparameter `SOURCE` definiert. Dieser Parameter kann sowohl für die Rolle `MPK_POSTBEVOLLMAECHTIGTER` als auch die Rolle `MPK_REGISTRIERUNG` verwendet werden
- Falls ein Zustellsystem über den Portalverbund an das AMOD angebunden wird, MUSS die PVP-Rolle `ZUSE-DELIVERY-SERVICE` mitgegeben werden

## 1.3 Änderungen zu Version 2.1.3

Die wesentlichen Änderungen der Version 2.2.0 zur Zustellspezifikation der Version 2.1.3 sind wie folgt:

- Das Zustellsystem MUSS im `amod:PushDeliveryDataRequest` das `Version` Attribut verpflichtend setzen, um anzuzeigen welche Version der ZUSE-Spezifikation unterstützt wird.
- Der Versender DARF im `msg:ContactAddresses` Element elektronische Kontaktadressen übermitteln, die vom Anzeigemodul in den Text des Verständigungsformulars eingefügt werden.
- Das AMOD retourniert an Zustelldienste in den Nachrichtenoperationen „Accepted“ und „DeliveryError“ zusätzlich die elektronischen Verständigungsadressen (`msg:NotificationAddressList`), da diese verpflichtend Bestandteil des Zustellnachweises sind.
- In Nachrichtenoperationen (`amod:MessageOperation`) dürfen zur eindeutigen Identifikation von natürlichen Personen ausschließlich für das Anzeigemodul verschlüsselte bereichsspezifischen Personenkennzeichen des Bereichs „Zustellung“ verwendet werden. Der zugehörige Identifikationstyp ist gleich „`urn:publicid:gv.at:ecdid+ZUSEAMOD+ZU`“



- Benutzerinformation im `amod:MessageOperation/msg:User` Element: nur im Falle von Vertretungsbevollmächtigten einer Behörde ist auch der PVP-Benutzerkennung als eindeutiger Identifikator mit dem Typ „urn:pvp-userid“ zulässig.
- ERV-Weiterleitung: Der Zustellzeitpunkt wird vom ERV berechnet bzw. ermittelt.
- Der Zustellzeitpunkt ist auch im Falle der ERV-Weiterleitung dem `amod:MessageOperation/msg:Timestamp` Element zu entnehmen.
- Der Fehlschlag einer ERV-Weiterleitung ist asynchron an das Zustellsystem und in weiterer Folge an den Versender zurückzumelden.
- Wenn die Zustellung an einen Insolvenzverwalter umgeleitet wird, muss dies am PDF-Rückschein ersichtlich sein.

## 1.4 Änderungen zu Version 2.1.2

Die wesentlichen Änderungen der Version 2.1.3 zur Zustellspezifikation der Version 2.1.2 sind wie folgt:

- Die Zustellsysteme werden vom AMOD jedenfalls und explizit zur endgültigen Löschung einer Nachricht mittel Nachrichtenoperation „Delete“ aufgefordert.
- Präzisierung: nur bei nachweislichen Zustellungen wird vom AMOD die Nachrichtenoperation „Accepted“ an den zuständigen Zustelldienst versendet
- Präzisierung: Abfolge der Nachrichtenoperationen bei
  - Nachweislichen Zustellungen
  - Nichtnachweislichen Zustellungen
  - Weiterleitung in den ERV
- Präzisierung: Nachrichtenoperationen bei denen im Falle einer nachweislichen Zustellung eine Zustellbenachrichtigung vom Zustelldienst an den Versender übermittelt werden muss
- Zustellsysteme müssen damit umgehen können, dass sie vom AMOD mehrfach die GLEICHE MessageOperation zu einer Nachricht erhalten
- Validierung von E-Mail-Adressen

## 1.5 Änderungen zu Version 2.1.1

Die wesentlichen Änderungen der Version 2.1.2 zur Zustellspezifikation der Version 2.1.1 sind wie folgt:

- Weiterleitung von Zustellungen in den Elektronischen Rechtsverkehr der Justiz (ERV)

## 1.6 Änderungen zu Version 2.1.0

Die wesentlichen Änderungen der Version 2.1.2 zur Zustellspezifikation der Version 2.1.0 sind wie folgt:

- Beschreibung der erforderlichen und optionalen PVP2-Header, die bei der Anbindung von Behördenportalen vom Anzeigemodul verarbeitet werden

## 1.7 Änderungen zu Version 2.0.0

Die wesentlichen Änderungen der Version 2.1.0 zur Zustellspezifikation der Version 2.0.0 sind wie folgt:

- Bezogen auf den Nachrichtenstatus und der Metadaten wird das Anzeigemodul zum führenden System
- Attachments müssen von den Zustellsystemen für das Anzeigemodul verschlüsselt werden
- Sämtliche elektronischen Verständigungen werden vom AMOD versendet
- Das Anzeigemodul löscht nach Ablauf der Vorhaltdauer (Details siehe [ZUSEORG]) Nachricht automatisch. Hierbei ist es unerheblich, ob die Nachricht gelesen wurde oder nicht.

## 1.1 SOAP-Webservice Kommunikation

Es wird explizit darauf hingewiesen, dass eine „Fire-And-Forget“-Strategie im Kontext Webservice-Kommunikation generell nicht zulässig ist.

Wenn eine Applikation einen SOAP-Webservice-Call absetzt, muss sie auf die Antwort der Gegenstelle warten. Wenn keine Antwort eintrifft bzw. ein Timeout auftritt, dann war der Webservice-Call NICHT erfolgreich und muss wiederholt werden.

## 1.2 Namespaces

Die Schemata `zusetnvz_p2.xsd` und `zusengd_p2.xsd` sind normativer Bestandteil dieser Spezifikation und referenziert auf die folgenden Namespaces:

**Tabelle 1 - Namespaces**

Präfix	Namespace	Version	Erläuterung
ztyp	<code>http://reference.e-government.gv.at/namespace/zustellung/types/phase2/20240718#</code>	2.4.0-003	Definitionen der XML SimpleTypes zur Begrenzung der Feldlängen gemäß diesem Dokument
amod	<code>http://reference.e-government.gv.at/namespace/zustellung/amod/phase2/20181206#</code>	2.4.0-003	Dieses Dokument
tnvz	<code>http://reference.e-government.gv.at/namespaces/zustellung/tnvz/phase2/20181206#</code>	2.4.0-003	Abfrage des Teilnehmerverzeichnis [ZUSETNVZ]
msg	<code>http://reference.e-government.gv.at/namespace/zustellung/msg/phase2/20181206#</code>	2.4.0-003	Elektronische Zustellung - Message Spezifikation [ZUSEMSG]
p	<code>http://reference.e-government.gv.at/namespace/persondata/phase2/20181206#</code>	2.4.0-003	PersonData [PERSDATA]
dsig	<code>http://www.w3.org/2000/09/xmldsig#</code>		XML Digital Signature [XMLDSIG]
soap	<code>http://www.w3.org/2001/12/soap</code>		SOAP [SOAP12]

### 1.3 Schlüsselwörter

Dieses Dokument verwendet die Schlüsselwörter MUSS, DARF NICHT, ERFORDERLICH, SOLLTE, SOLLTE NICHT, EMPFOHLEN, DARF, und OPTIONAL zur Kategorisierung der Anforderungen. Diese Schlüsselwörter sind analog zu ihren englischsprachigen Entsprechungen MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, RECOMMENDED, MAY, und OPTIONAL zu handhaben, deren Interpretation in [RFC2119] festgelegt ist.

### 1.4 Glossar

AMOD	Anzeigemodul
ERV	Elektronischer Rechtsverkehr der Justiz
KSB	Kommunikationssystem der Behörde
TNVZ	Teilnehmerverzeichnis
HTTP	Hypertext Transfer Protocol
PVP	Portalverbund Protokoll
SOAP	Simple Object Access Protocol
bPK	Bereichsspezifisches Personenkennzeichen
bPK-ZU	bPK für den Bereich ZU (Zustellung)
vbPK-ZU(ZUSETNVZ)	bPK des Bereichs Zustellung (ZU), welches für das Teilnehmerverzeichnis (ZUSETNVZ) verschlüsselt wurde
vbPK-ZU(ZUSEAMOD)	bPK des Bereichs Zustellung (ZU), welches für das Anzeigemodul (ZUSEAMOD) verschlüsselt wurde

## 2 Authentifizierung

Für die Kommunikation mit Zustellsystemen, Internetportalen (Einbindung/Anbindung) sowie Systemen der automatisierten Abholung ist eine starke Authentifizierung notwendig. Ist die Anwendung mit der das Anzeigemodul kommuniziert Teilnehmer des Portalverbunds, so erfolgt eine PVP-basierte Authentifizierung, andernfalls erfolgt die Authentifizierung via TLS Client-Zertifikat Authentifizierung.

Zulässige TLS Protokolle und Cipher Suites und Algorithmen sind gemäß den Vorgaben der aktuellen Spezifikation der [PVPSMA] zu verwenden.

### 2.1 Teilnehmer des Portalverbunds

Sämtliche Applikationen MÜSSEN sich mittels PVP2 R-Profil [PVP2RPROFIL] gegenüber dem Anzeigemodul authentifizieren (bzw. das Anzeigemodul gegenüber dem Zustellsystem). Im Fall des R-Profils MUSS die HTTP Protokollbindung mit Zertifikatsauthentifizierung verwendet werden und das PVP-eGovToken [PVP2EGOVTOKEN] mittels HTTP Header übergeben werden.

Das Zertifikat der Anwendung MUSS für die Authentifizierung beim Anzeigemodul registriert werden.

### 2.2 Nicht Teilnehmer des Portalverbunds

Anwendungen, die nicht Teilnehmer des Portalverbunds sind, MÜSSEN sich mittels TLS Client Authentifizierung gegenüber dem Anzeigemodul authentifizieren (bzw. das Anzeigemodul gegenüber dem Zustellsystem). Das Zertifikat MUSS beim Anzeigemodul hinterlegt und der Anwendung eindeutig zugeordnet werden können. Die Umsetzung der Client-Zertifikatsprüfung ist vom Anzeigemodul nach [KIX] durchzuführen und nicht Teil dieser Spezifikation. Auch ist es im Ermessen des Anzeigemoduls, ob es eine eigene Public Key Infrastructure (PKI) bereitstellt oder TLS Client Zertifikate einer vertrauenswürdigen PKI eines Drittanbieters unterstützt.

### 3 Übermittlung von Metadaten

Dieser Abschnitt definiert die Syntax sowie Semantik der unterstützten Metadaten, die von einem Zustellsystem zum Anzeigemodul übertragen werden können.

#### 3.1 Metadaten Definitionen und Verzeichnis

##### 3.1.1 Allgemeines zur Definition von Metadaten

###### 3.1.1.1 Syntaxangaben / Augmented BNF

Für Syntaxbeschreibungen wird die *Augmented BNF* - wie in [RFC822] definiert - verwendet. Sie wird um folgende Elemente ergänzt:

###### 3.1.1.2 BNF Syntax

UCHAR = <druckbares US-ASCII (ISO-646) Zeichen ohne CRLF (dezimal 33-126)>

UTF\_CHAR = <druckbares UNICODE Zeichen (nicht druckbar sind die Zeichen 0-31 und 127)>

SPACE = " "

SLASH = "/"

ALPHA = <Alle US-ASCII Buchstaben "A".."Z" und "a".."z">

DIGIT = <Ziffer zwischen 0 und 9>

NAMECHAR = ALPHA | DIGIT | "-" | "\_"

B64CHAR = <Zeichen aus Base64-Alphabet laut [RFC2045] (A..Z, a..z, 0..9, +, /, =) oder whitespace>

##### 3.1.2 Technische Informationen

Nachfolgend werden sämtliche allgemeine Metadaten-Typen definiert.

3.1.2.1 Systemweit eindeutige Zustell-ID (ZS-DELIVERY-ID)	
<b>OID</b>	1.2.40.0.10.2.5.1.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.1
<b>Friendly Name</b>	ZS-DELIVERY-ID
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gibt die systemweit eindeutige Zustell-ID an, die vom Zustellsystem definiert wird. Zustell-IDs müssen eindeutig für jedes Zustellsystem sein und dürfen während des Lebenszyklus eines Zustellsystems nur einmal vergeben werden.
<b>Syntax</b>	zsDeliveryID := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN

<b>Beispiel</b>	3716d253-35d6-4f44-aa43-7a83bd70fac0
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

### 3.1.2.2 Versender (SENDER)

<b>OID</b>	1.2.40.0.10.2.5.1.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für alle Daten den Versender betreffend

### 3.1.2.3 Versender Identifikationsdaten (SENDER-IDENTIFIER)

<b>OID</b>	1.2.40.0.10.2.5.1.2.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.1
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für alle Daten des Identifikators des Versenders betreffend

### 3.1.2.4 ID-Typ des Versenders (SENDER-IDENTIFIER-TYPE)

<b>OID</b>	1.2.40.0.10.2.5.1.2.1.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.1.1
<b>Friendly Name</b>	SENDER-IDENTIFIER-TYPE
<b>Verpflichtend</b>	JA

<b>Bedeutung</b>	Gibt den Typ des eindeutigen Identifiers des Versenders an. Folgende Werte sind zulässig: <ul style="list-style-type: none"> <li>• urn:publicid:gv.at:cdid+ZU</li> <li>• urn:publicid:gv.at:baseid+XFN</li> <li>• urn:publicid:gv.at:baseid+XZVR</li> <li>• urn:publicid:gv.at:baseid+XGLN</li> </ul>
<b>Syntax</b>	senderIdentifierType := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	urn:publicid:gv.at:cdid+ZU (bPK für Bereich Zustellung)
<b>XML-Schema-Type</b>	ztyp:anyURI1..256

### 3.1.2.5 ID-Value des Versenders (SENDER-IDENTIFIER-VALUE)

<b>OID</b>	1.2.40.0.10.2.5.1.2.1.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.1.2
<b>Friendly Name</b>	SENDER-IDENTIFIER-VALUE
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gibt den Wert des eindeutigen Identifiers des Versenders an.
<b>Syntax</b>	senderIdentifierValue := {1-1024} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 1024
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	<ul style="list-style-type: none"> <li>• 7k7dDB8NvoxX3IroF+4iU+gCT5Y= (bPK für Bereich Zustellung)</li> <li>• 999999m (Firmenbuchnummer)</li> </ul>

<b>XML-Schema-Type</b>	<i>ztyp:string1..1024</i>
------------------------	---------------------------

### 3.1.2.6 Versender Personendaten (SENDER-\*)

<b>OID</b>	1.2.40.0.10.2.5.1.2.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für alle Personendaten des Senders betreffend

### 3.1.2.7 Versenderdaten Unternehmen (SENDER-CB)

<b>OID</b>	1.2.40.0.10.2.5.1.2.2.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.2.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für alle Daten des Versendernamens im Fall eines Unternehmens betreffend

### 3.1.2.8 Versenderdaten Unternehmensname (SENDER-CB-FULLNAME)

<b>OID</b>	1.2.40.0.10.2.5.1.2.2.2.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.2.2.1
<b>Friendly Name</b>	SENDER-CB-FULLNAME
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Voller Name des Senders im Falle eines Unternehmens



<b>Syntax</b>	senderCorporateBodyFullName := {1-1000} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 1000
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Österreichische Fluggesellschaft
<b>XML-Schema-Type</b>	<i>ztyp:token1..1000</i>

### 3.1.2.9 Versenderdaten Behördenname (SENDER-CB-ORGANIZATION)

<b>OID</b>	1.2.40.0.10.2.5.1.2.2.2.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid1.2.40.0.10.2.5.1.2.2.2.2
<b>Friendly Name</b>	SENDER-CB-ORGANIZATION
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Name einer Organisationseinheit
<b>Syntax</b>	senderCorporateBodyOrganization := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Human Resources
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

**3.1.2.10 Versenderdaten Behörde Target (SENDER-CB-TARGET)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.2.2.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.2.2.3
<b>Friendly Name</b>	SENDER-CB-TARGET
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gibt den Bereich und entweder das VKZ oder die Service-Identifikation - codiert als Identifikationstyp - der versendenden Behörde oder des versendenden Unternehmens, welches im gesetzlichen Auftrag handelt, an.
<b>Syntax</b>	senderCorporateBodyTarget := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	urn:publicid:gv.at:cdid+BMF+SA
<b>XML-Schema-Type</b>	<i>ztyp:anyURI1..256</i>

**3.1.2.11 Zusätzliche Daten Versender (SENDER-ADD)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.3
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für alle zusätzlichen Daten des Versenders betreffend

**3.1.2.12 Zusätzliche Daten Versender Mailbox (SENDER-ADD-MAILBOX)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.3.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.3.1
<b>Friendly Name</b>	SENDER-ADD-MAILBOX
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Mailbox Identifier des Versenders
<b>Syntax</b>	senderMailbox := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	Postfach 1234
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

**3.1.2.13 Zusätzliche Daten Versender Rollen (SENDER-ADD-ROLES)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.3.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.3.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für Versenderrollen

**3.1.2.14 Zusätzliche Daten Versender Rolle (SENDER-ADD-ROLE)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.3.2.X; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.3.2.X
<b>Friendly Name</b>	SENDER-ADD-ROLE
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Rolle des Versenders
<b>Syntax</b>	senderRole := {1-256} UTF_CHAR
<b>Multi-valued</b>	JA
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	Datenschutzbeauftragter
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

**3.1.2.15 Zusätzliche Daten Versender Zu Handen (SENDER-ADD-CAREOF)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.3.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.3.3
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für alle Zu Handen Daten Versender

**3.1.2.16 Versender Zu Handen Elektronische Adresse (SENDER-ADD-CAREOF-EADDR)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.3.3.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.3.3.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für elektronische Adresse des Zu Handen Teils des Versenders

**3.1.2.17 Versender Zu Handen E-Mail (SENDER-ADD-CAREOF-EADDR-MAIL)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.3.3.2.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.3.3.2.2
<b>Friendly Name</b>	SENDER-ADD-CAREOF-EADDR-MAIL
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gibt die E-Mail-Adresse des zu Handen Teil des Versenders an.
<b>Syntax</b>	senderCareofMail:= {1-1024} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 1024
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	<ul style="list-style-type: none"> <li>max@mustermann.at</li> </ul>
<b>XML-Schema-Type</b>	<i>ztyp:anyURI1..1024</i>

**3.1.2.18 Versender Zu Handen Name (SENDER-ADD-CAREOF-NAME)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.3.3.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.3.3.2
<b>Friendly Name</b>	SENDER-ADD-CAREOF-NAME
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Name des Ansprechpartners beim Versender (z.B. Sachbearbeiter). Hierbei handelt es sich um einen Freitext für die Anzeige, der als eindeutiger Identifikator für Verständigungen oder eine automatisierte Weiterleitung ungeeignet ist.
<b>Syntax</b>	senderCareofName := {1-1001} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 1001
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Max Mustermann
<b>XML-Schema-Type</b>	<i>ztyp:token1..1001</i>

**3.1.2.19 Kontaktadressen (SENDER-CONTACT-ADDRESSES)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.5; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.5
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Der Versender kann eine Liste von maximal drei elektronischen Kontaktadressen übermitteln, die vom Anzeigemodul im Verständigungsformular unter dem Titel „Rückfragen beim Versender unter“ eingefügt werden. Eine elektronische Adresse kann entweder eine Telefonnummer ( <i>msg:TelephoneAddress</i> ) oder eine E-Mail ( <i>msg:InternetAddress</i> ) sein

**3.1.2.20 Kontaktadresse Internet (SENDER-CONTACT-INTERNET)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.5.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.5.1
<b>Friendly Name</b>	SENDER-CONTACT-INTERNET
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	E-Mail-Adresse der Kontaktstelle
<b>Syntax</b>	senderContactInternet:= {1-1024} UTF_CHAR
<b>Multi-valued</b>	JA
<b>Länge</b>	Max. 1024
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	<ul style="list-style-type: none"> <li>• post@ma63.wien.gv.at</li> <li>• mailto:post@ma63.wien.gv.at</li> </ul>
<b>XML-Schema-Type</b>	ztyp:anyURI1..1024

**3.1.2.21 Kontaktadresse Telefon (SENDER-CONTACT-TELEPHONE)**

<b>OID</b>	1.2.40.0.10.2.5.1.2.5.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.2.5.2
<b>Friendly Name</b>	SENDER-CONTACT-TELEPHONE
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Telefonnummer der Servicestelle des Senders
<b>Syntax</b>	senderContactTelephone:= {1-128} UTF_CHAR

<b>Multi-valued</b>	JA
<b>Länge</b>	Max. 128
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	+43 662 123456
<b>XML-Schema-Type</b>	<i>xs:string</i> - gemäß dem regulären Ausdruck: \+?\d[\s\d]{1,126}\d

### 3.1.2.22 Empfänger (RECIPIENT)

<b>OID</b>	1.2.40.0.10.2.5.1.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für alle Daten den Empfänger betreffend

### 3.1.2.23 Empfänger Identifikationsdaten (RECIPIENT-IDENTIFIER)

<b>OID</b>	1.2.40.0.10.2.5.1.3.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.1
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für alle Daten des Identifikators des Empfängers betreffend

### 3.1.2.24 ID-Typ des Empfängers (RECIPIENT-IDENTIFIER-TYPE)

<b>OID</b>	1.2.40.0.10.2.5.1.3.1.1; definiert durch ZUSE (dieses Dokument)
------------	---



<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.1.1
<b>Friendly Name</b>	RECIPIENT-IDENTIFIER-TYPE
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gibt den Typ des eindeutigen Identifiers des Empfängers an. Folgende Werte sind zulässig: <ul style="list-style-type: none"> <li>• urn:publicid:gv.at:cdid+ZU</li> <li>• urn:publicid:gv.at:baseid+XFN</li> <li>• urn:publicid:gv.at:baseid+XZVR</li> <li>• urn:publicid:gv.at:baseid+XGLN</li> </ul>
<b>Syntax</b>	recipientIdentifierType := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	urn:publicid:gv.at:cdid+ZU (bPK für Bereich Zustellung)
<b>XML-Schema-Type</b>	<i>ztyp:anyURI1..256</i>

### 3.1.2.25 ID-Value des Empfängers (RECIPIENT-IDENTIFIER-VALUE)

<b>OID</b>	1.2.40.0.10.2.5.1.3.1.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.1.2
<b>Friendly Name</b>	RECIPIENT-IDENTIFIER-VALUE
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gibt den Wert des eindeutigen Identifiers des Empfängers an.
<b>Syntax</b>	recipientIdentifierValue := {1-1024} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 1024

<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	<ul style="list-style-type: none"> <li>• 7k7dDB8NvoxX3IroF+4iU+gCT5Y= (bPK für Bereich Zustellung)</li> <li>• 999999m (Firmenbuchnummer)</li> </ul>
<b>XML-Schema-Type</b>	<i>ztyp:string1..1024</i>

### 3.1.2.26 Empfänger Personendaten (RECIPIENT-\*)

<b>OID</b>	1.2.40.0.10.2.5.1.3.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für alle Personendaten den Empfänger betreffend

### 3.1.2.27 Empfängerdaten Unternehmen (RECIPIENT-CB)

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für alle Daten des Empfängernamens im Fall eines Unternehmens betreffend

### 3.1.2.28 Empfängerdaten Unternehmensname (RECIPIENT-CB-FULLNAME)

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.2.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.2.1

<b>Friendly Name</b>	RECIPIENT-CB-FULLNAME
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Voller Name des Empfängers im Falle eines Unternehmens
<b>Syntax</b>	recipientCorporateBodyFullName := {1-1000} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 1000
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Österreichische Fluggesellschaft
<b>XML-Schema-Type</b>	<i>ztyp:token1..1000</i>

<b>3.1.2.29 Empfängerdaten Unternehmen Organisationseinheit (RECIPIENT-CB-ORGANIZATION)</b>	
<b>OID</b>	1.2.40.0.10.2.5.1.3.2.2.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.2.2
<b>Friendly Name</b>	RECIPIENT-CB-ORGANIZATION
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Name einer Organisationseinheit
<b>Syntax</b>	recipientCorporateBodyOrganization := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Human Resources
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

**3.1.2.30 Empfängerdaten Behörde Target (RECIPIENT-CB-TARGET)**

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.2.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.2.3
<b>Friendly Name</b>	RECIPIENT-CB-TARGET
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gibt den Bereich und entweder das VKZ oder die Service-Identifikation - codiert als Identifikationstyp - der empfangenden Behörde oder des empfangenden Unternehmens, welches im gesetzlichen Auftrag handelt, an.
<b>Syntax</b>	recipientCorporateBodyTarget := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	urn:publicid:gv.at:cdid+BMF+SA
<b>XML-Schema-Type</b>	<i>ztyp:anyURI1..256</i>

**3.1.2.31 Empfängerdaten Natürliche Person (RECIPIENT-PP)**

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.3
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für alle Daten des Empfängernamens im Fall einer natürlichen Person betreffend

<b>3.1.2.32 Empfängerdaten Natürliche Person Vorname (RECIPIENT-PP-GIVENNAME)</b>	
<b>OID</b>	1.2.40.0.10.2.5.1.3.2.3.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.3.1
<b>Friendly Name</b>	RECIPIENT-PP-GIVENNAME
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Vorname des Empfängers im Fall einer natürlichen Person
<b>Syntax</b>	recipientPhysicalPersonGivenName := {1-500} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 500
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Max
<b>XML-Schema-Type</b>	<i>ztyp:string1..500</i>

<b>3.1.2.33 Empfängerdaten Natürliche Person Familienname (RECIPIENT-PP-FAMILYNAME)</b>	
<b>OID</b>	1.2.40.0.10.2.5.1.3.2.3.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.3.2
<b>Friendly Name</b>	RECIPIENT-PP-FAMILYNAME
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Familienname/Nachname des Empfängers im Fall einer natürlichen Person
<b>Syntax</b>	recipientPhysicalPersonFamilyName := {1-500} UTF_CHAR
<b>Multi-valued</b>	NEIN

<b>Länge</b>	Max. 500
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Mustermann
<b>XML-Schema-Type</b>	<i>ztyp:string1..500</i>

<b>3.1.2.34 Empfängerdaten Natürliche Person Geburtsdatum (RECIPIENT-PP-DATEOFBIRTH)</b>	
<b>OID</b>	1.2.40.0.10.2.5.1.3.2.3.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.3.3
<b>Friendly Name</b>	RECIPIENT-PP-DATEOFBIRTH
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Geburtsdatum des Empfängers im Fall einer natürlichen Person
<b>Syntax</b>	recipientPhysicalPersonDateOfBirth := <DateYearMonthDay>
<b>Multi-valued</b>	NEIN
<b>Länge</b>	
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Mustermann
<b>XML-Schema-Type</b>	<i>p:DateOfBirthType</i>

<b>3.1.2.35 Zusätzliche Daten Empfänger (RECIPIENT-ADD)</b>	
<b>OID</b>	1.2.40.0.10.2.5.1.3.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2
<b>Teilbaum</b>	JA

<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für alle zusätzlichen Daten des Empfängers betreffend

### 3.1.2.36 Zusätzliche Daten Empfänger Mailbox (RECIPIENT-ADD-MAILBOX)

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.1
<b>Friendly Name</b>	RECIPIENT-ADD-MAILBOX
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Mailbox Identifier des Empfängers. Angabe eines Subpostfachs, das eine Organisation frei definieren KANN
<b>Syntax</b>	recipientMailbox := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	Postfach 1234
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

### 3.1.2.37 Zusätzliche Daten Empfänger Rollen (RECIPIENT-ADD-ROLES)

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für Empfängerrollen

**3.1.2.38 Zusätzliche Daten Empfänger Rolle (RECIPIENT-ADD-ROLE)**

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.2.X; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.2.X
<b>Friendly Name</b>	RECIPIENT-ADD-ROLE
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Rolle des Empfängers
<b>Syntax</b>	recipientRole := {1-256} UTF_CHAR
<b>Multi-valued</b>	JA
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	Datenschutzbeauftragter
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

**3.1.2.39 Zusätzliche Daten Empfänger Zu Handen (RECIPIENT-ADD-CAREOF)**

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.3
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für alle Zu Handen Daten Empfänger



**3.1.2.40 Empfänger Zu Handen Elektronische Adresse (RECIPIENT-ADD-CAREOF-EADDR)**

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.3.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.3.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für elektronische Adresse des Zu Handen Teils des Empfängers

**3.1.2.41 Empfänger Zu Handen E-Mail (RECIPIENT-ADD-CAREOF-EADDR-MAIL)**

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.3.2.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.3.2.2
<b>Friendly Name</b>	RECIPIENT-ADD-CAREOF-EADDR-MAIL
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gibt die E-Mail Adresse des zu Handen Teil des Empfängers an.
<b>Syntax</b>	recipientCareofMail:= {1-1024} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 1024
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	<ul style="list-style-type: none"> <li>max@mustermann.at</li> </ul>
<b>XML-Schema-Type</b>	<i>ztyp:anyURI1..1024</i>

**3.1.2.42 Empfänger Zu Handen Name (RECIPIENT-ADD-CAREOF-NAME)**

<b>OID</b>	1.2.40.0.10.2.5.1.3.2.3.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.3.2.3.3
<b>Friendly Name</b>	RECIPIENT-ADD-CAREOF-NAME
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Name des physischen Empfängers zu dessen Handen zugestellt werden soll. Hierbei handelt es sich um einen Freitext für die Anzeige, der als eindeutiger Identifikator für Verständigungen oder eine automatisierte Weiterleitung ungeeignet ist.
<b>Syntax</b>	recipientCareofName := {1-1001} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 1001
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Max Mustermann
<b>XML-Schema-Type</b>	<i>ztyp:token1..1001</i>

**3.1.2.43 Metadaten (METADATA)**

<b>OID</b>	1.2.40.0.10.2.5.1.4; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für alle Metadaten der Zustellung

**3.1.2.44 Nachrichten-ID der versendenden Anwendung (APP-DELIVERY-ID)**

<b>OID</b>	1.2.40.0.10.2.5.1.4.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.2
<b>Friendly Name</b>	APP-DELIVERY-ID
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	ID der Nachrichten, die von der Anwendung des Versenders vergeben wurde. Ist erforderlich, um eine Sendung nachverfolgen zu können.
<b>Syntax</b>	appDeliveryID := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>XML-Schema-Type</b>	ztyp:token1..256

**3.1.2.45 Herkunftssystem der Zustellung (ORIGIN)**

<b>OID</b>	1.2.40.0.10.2.5.1.4.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.1
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für Metadaten zum Herkunftssystem der Zustellung

**3.1.2.46 Herkunftssystem Participant-ID (ORIGIN-PARTICIPANT-ID)**

<b>OID</b>	1.2.40.0.10.2.5.1.4.1.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.1.1

<b>Friendly Name</b>	ORIGIN-PARTICIPANT-ID
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gibt die PVP ParticipantID des Zustellsystems an, über das eine Zustellung an das Anzeigemodul übermittelt wurde.
<b>Syntax</b>	originParticipantID := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	AT:L20:0014
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

### 3.1.2.47 Betreff (SUBJECT)

<b>OID</b>	1.2.40.0.10.2.5.1.4.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.3
<b>Friendly Name</b>	Subject
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Definiert den Betreff der Zustellung und spiegelt dabei eine Zusammenfassung bzw. den Charakter der Nachricht wider.
<b>Syntax</b>	subject := {1-512} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 512
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Einkommensteuerbescheid 2017
<b>XML-Schema-Type</b>	<i>ztyp:token1..512</i>

**3.1.2.48 Geschäftszahl (GZ)**

<b>OID</b>	1.2.40.0.10.2.5.1.4.4; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.4
<b>Friendly Name</b>	GZ
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Definiert die Geschäftszahl der Zustellung.
<b>Syntax</b>	gz := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	A-BCDEF/2017
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

**3.1.2.49 Zustellqualität (DELIVERY-QUALITY)**

<b>OID</b>	1.2.40.0.10.2.5.1.4.5; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.5
<b>Friendly Name</b>	DELIVERY-QUALITY
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	<p>Definiert die behördliche Zustellqualität der Zustellung.  Als Zustellqualität MUSS eine der folgenden gewählt werden:</p> <ul style="list-style-type: none"> <li>• <b>nonRSa</b> einfache Zustellung ohne Zustellnachweis</li> <li>• <b>nonRSa+</b> einfache Zustellung ohne Zustellnachweis – nicht an Postbevollmächtigte (Abholung durch Dritte unter Verwendung von Vollmachten ist NICHT möglich)</li> <li>• <b>RSa</b> RSa-Zustellung zu eigenen Händen mit Zustellnachweis</li> <li>• <b>RSa+</b> RSa-Zustellung zu eigenen Händen mit Zustellnachweis (Abholung durch Dritte unter Verwendung von Vollmachten ist NICHT möglich)</li> </ul>

<b>Syntax</b>	deliveryQuality := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	RSa
<b>XML-Schema-Type</b>	ztyp:token1..256

### 3.1.2.50 Private Qualität der Zusendung (PRIVATE-DELIVERY-QUALITY)

<b>OID</b>	1.2.40.0.10.2.5.1.4.6; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.6
<b>Friendly Name</b>	PRIVATE-DELIVERY-QUALITY
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	<p>Definiert die private Qualität der Zusendung. Als Sendungsqualität MUSS eine der folgenden gewählt werden:</p> <ul style="list-style-type: none"> <li>• <b>RegisteredMail(+)</b> Entspricht dem eingeschriebenen Brief ist also die "Standard"-Sendungsqualität</li> <li>• <b>ConfirmReceipt(+)</b> Entspricht einem Brief mit Empfangsbestätigung</li> <li>• <b>Information</b> Diese Sendungsqualität steht nur Behörden zur Verfügung und dient dazu, Bürger und Unternehmen über Änderungen oder Neuheiten in der Verwaltung zu informieren. Diese Sendungsqualität löst in der Regel keine Rechtsfolgen aus.</li> </ul> <p>Das Postfix „+“ definiert, dass das Schriftstück ausschließlich vom Empfänger selbst und nicht durch einen Stellvertreter abgeholt werden kann. Für die Sendungsqualität Information ist die Plus-Qualität nicht zugelassen</p>
<b>Syntax</b>	privateDeliveryQuality := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	JA

<b>Beispiel</b>	Information
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

### 3.1.2.51 Liste der Sprachen für Verständigungen (NOTIFICATION-LANGUAGES)

<b>OID</b>	1.2.40.0.10.2.5.1.4.11; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.11
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für Sprachen für Verständigungen

### 3.1.2.52 Sprache für Verständigungen (NOTIFICATION-LANGUAGE)

<b>OID</b>	1.2.40.0.10.2.5.1.4.11.X; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.11.X
<b>Friendly Name</b>	NOTIFICATION-LANGUAGE
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	<p>Zwei-stelliger [ISO639-1] Code einer alternativen Sprache für Verständigungen. Neben Deutsch können folgende Minderheitensprachen angegeben gewählt werden:</p> <ul style="list-style-type: none"> <li>• HR - Kroatisch</li> <li>• HU - Ungarisch</li> <li>• SL - Slowenisch</li> </ul>
<b>Syntax</b>	notificationLanguage:= {2} UTF_CHAR
<b>Multi-valued</b>	JA
<b>Länge</b>	2

<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	HR
<b>XML-Schema-Type</b>	<i>msg:AustrianLanguageType</i>

### 3.1.2.53 Referenz (REFERENCE)

<b>OID</b>	1.2.40.0.10.2.5.1.4.7; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.7
<b>Friendly Name</b>	REFERENCE
<b>Verpflichtend</b>	NEIN
<b>Teilbaum</b>	JA
<b>Bedeutung</b>	Enthält eine Referenz auf ein anderes Zustellstück

### 3.1.2.54 Referenz (REFERENCE-ZS-DELIVERY-ID)

<b>OID</b>	1.2.40.0.10.2.5.1.4.7.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.7.1
<b>Friendly Name</b>	REFERENCE-ZS-DELIVERY-ID
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Definiert die Referenz auf ein anderes Zustellstück (vergleichbar der Message-ID bei E-Mail).
<b>Syntax</b>	referenceZsDeliveryID:= {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN



<b>Beispiel</b>	5716d253-35d6-4f44-aa43-7a83bd70fac0
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

### 3.1.2.55 Tags (TAGS)

<b>OID</b>	1.2.40.0.10.2.5.1.4.8; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.8
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für Tags der Nachricht

### 3.1.2.56 Tag (TAG)

<b>OID</b>	1.2.40.0.10.2.5.1.4.8.X; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.8.X
<b>Friendly Name</b>	TAG
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gibt einen Tag der Nachricht an.
<b>Syntax</b>	tag := {1-256} UTF_CHAR
<b>Multi-valued</b>	JA
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	USP_PORTAL
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

**3.1.2.57 Verfahrensspezifische Metadaten (APP-METADATALIST)**

<b>OID</b>	1.2.40.0.10.2.5.1.4.10; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.10
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für verfahrensspezifische Metadaten der Nachricht

**3.1.2.58 Verfahrensspezifisches Metadatum (APP-METADATA)**

<b>OID</b>	1.2.40.0.10.2.5.1.4.10.X; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.10.X
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für ein bestimmtes verfahrensspezifisches Metadatum der Nachricht

**3.1.2.59 Verfahrensspezifisches Metadatum OID (APP-METADATA-OID)**

<b>OID</b>	1.2.40.0.10.2.5.1.4.10.X.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.10.X.1
<b>Friendly Name</b>	APP-METADATA-OID
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gibt die OID eines verfahrensspezifischen Metadatums an
<b>Syntax</b>	appMetadataOID:= {1-256} UTF_CHAR

<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	1.2.40.0.10.2.5.1.4.100
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

### 3.1.2.60 Verfahrensspezifisches Metadatum Wert (APP-METADATA-VALUE)

<b>OID</b>	1.2.40.0.10.2.5.1.4.10.X.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.4.10.X.2
<b>Friendly Name</b>	APP-METADATA-VALUE
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gibt den Wert eines verfahrensspezifischen Metadatums an
<b>Syntax</b>	appMetadataValue:= {1-4096} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 4096
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	TestInhalt
<b>XML-Schema-Type</b>	<i>ztyp: anySimpleType1..4096</i>

### 3.1.2.61 Anhänge (ATTACHMENTS)

<b>OID</b>	1.2.40.0.10.2.5.1.5; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5

<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für alle Anhänge der Nachricht

### 3.1.2.62 Anhang (ATTACHMENT)

<b>OID</b>	1.2.40.0.10.2.5.1.5.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Multi-valued</b>	JA
<b>Bedeutung</b>	Gruppierung für einen Anhang einer Nachricht

### 3.1.2.63 ID eines Anhangs (ATTACHMENT-ID)

<b>OID</b>	1.2.40.0.10.2.5.1.5.1.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.1
<b>Friendly Name</b>	ATTACHMENT-ID
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	ID eines bestimmten Attachments.
<b>Syntax</b>	attachmentID:= {1-256} UTF_CHAR
<b>Bildungsvorschrift</b>	UUID basierende auf [RFC4122]
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256

<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	A-123456
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

### 3.1.2.64 Dateiname eines Anhangs (ATTACHMENT-FILENAME)

<b>OID</b>	1.2.40.0.10.2.5.1.5.1.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.2
<b>Friendly Name</b>	ATTACHMENT-FILENAME
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Dateiname eines bestimmten Attachments.
<b>Syntax</b>	attachmentFileName := {5-255} UTF_CHAR
<b>Bildungsvorschrift</b>	<ul style="list-style-type: none"> <li>• Der Dateiname DARF KEINES der folgenden Zeichen enthalten:  <div style="border: 1px solid black; padding: 2px; display: inline-block;">\ / : * ? " &lt; &gt;  </div> </li> <li>• Führende oder nachfolgende Leerzeichen MÜSSEN entfernt werden</li> <li>• Die case-insensitiven Dateinamen der Attachments innerhalb einer Nachricht müssen eindeutig sein</li> <li>• Zeichensatz ist UTF-8</li> <li>• min Länge 5</li> <li>• max. Länge 255</li> <li>• Wenn ein Dateiname in einer HTTP-Headervariable transportiert wird, muss der Dateiname gemäß RFC5987 codiert werden.</li> </ul>
<b>Multi-valued</b>	NEIN
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	Anhang1.pdf
<b>XML-Schema-Type</b>	<i>msg:FileNameType</i>

**3.1.2.65 Dateityp eines Anhangs (ATTACHMENT-MIMETYPE)**

<b>OID</b>	1.2.40.0.10.2.5.1.5.1.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.3
<b>Friendly Name</b>	ATTACHMENT-MIMETYPE
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Dateityp gemäß RFC 2048 [RFC2048] eines bestimmten Attachments.
<b>Syntax</b>	attachmentMimeType := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	application/pdf
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

**3.1.2.66 Dokumentenklasse eines Anhangs (ATTACHMENT-DOCUMENT-CLASS)**

<b>OID</b>	1.2.40.0.10.2.5.1.5.1.4; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.4
<b>Friendly Name</b>	ATTACHMENT-DOCUMENT-CLASS
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Dokumentenklasse eines bestimmten Anhangs.
<b>Syntax</b>	docClass := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN

<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	<ul style="list-style-type: none"> <li>• x-edclass-inctaxnotice</li> <li>• <a href="http://reference.e-government.gv.at/namespace/zustellung/urlaction/20180116#">http://reference.e-government.gv.at/namespace/zustellung/urlaction/20180116#</a></li> </ul>
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

### 3.1.2.67 Anhang Dateigröße (ATTACHMENT-FILESIZE)

<b>OID</b>	1.2.40.0.10.2.5.1.5.1.5; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.5
<b>Friendly Name</b>	ATTACHMENT-FILESIZE
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Dateigröße eines bestimmten Anhangs in bytes.
<b>Syntax</b>	fileSize := {1-256} UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	10345632
<b>XML-Schema-Type</b>	<i>ztyp:positiveInteger</i>

### 3.1.2.68 Checksumme eines Anhangs (ATTACHMENT-CHECKSUM)

<b>OID</b>	1.2.40.0.10.2.5.1.5.1.6; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.6

<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Gruppierung für die Checksumme eines bestimmten Anhangs

### **3.1.2.69 Checksummen Algorithmus eines Anhangs (ATTACHMENT-CHECKSUM-ALGORITHM)**

<b>OID</b>	1.2.40.0.10.2.5.1.5.1.6.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.6.1
<b>Friendly Name</b>	ATTACHMENT-CHECKSUM-ALGORITHM
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Identifiziert den Checksummen Algorithmus eines bestimmten Anhangs.
<b>Syntax</b>	attachmentChecksumAlgorithm := {1-256} UTF_CHAR
<b>Multi-valued</b>	JA
<b>Länge</b>	Max. 256
<b>Wertebereich</b>	<ul style="list-style-type: none"> <li>• SHA256</li> <li>• SHA512</li> </ul>
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	SHA256
<b>XML-Schema-Type</b>	<i>ztyp:token1..256</i>

### **3.1.2.70 Checksummen-Wert eines Anhangs (ATTACHMENT-CHECKSUM-VALUE)**

<b>OID</b>	1.2.40.0.10.2.5.1.5.1.6.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.6.2



<b>Friendly Name</b>	ATTACHMENT-CHECKSUM-VALUE
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Wert der Checksumme eines bestimmten Anhangs.
<b>Syntax</b>	attachmentChecksumValue := {1-256} UTF_CHAR
<b>Multi-valued</b>	JA
<b>Länge</b>	Max. 256
<b>Anzeige (default)</b>	JA
<b>Beispiel</b>	IrGg5W2aj41ZRJG5=
<b>XML-Schema-Type</b>	<i>ztyp:base64Binary4..256</i>

### 3.1.2.71 Verschlüsselter Attachmentschlüssel (ATTACHMENT-ENCRYPTED-KEY)

<b>OID</b>	1.2.40.0.10.2.5.1.5.1.6.3; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.6.3
<b>Friendly Name</b>	ATTACHMENT-ENCRYPTED-KEY
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Für das AMOD verschlüsselter symmetrischer Schlüssel. Dieser Schlüssel wird vom AMOD zum Entschlüsseln des Attachments verwendet. Pro Attachment ist vom Zustellsystem ein eigener symmetrischer Schlüssel zu generieren
<b>Syntax</b>	attachmentEncryptedKey := {1-4096} UTF_CHAR
<b>Multi-valued</b>	JA
<b>Länge</b>	Max. 4096
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	IrGg5W2aj41ZRJG5=

<b>XML-Schema-Type</b>	<i>ztyp:base64Binary4..4096</i>
<b>3.1.2.72 Subject-Key-Identifier (ATTACHMENT-SUBJECT-KEY-IDENTIFIER)</b>	
<b>OID</b>	1.2.40.0.10.2.5.1.5.1.6.3.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.5.1.6.3.1
<b>Friendly Name</b>	ATTACHMENT-SUBJECT-KEY-IDENTIFIER
<b>Verpflichtend</b>	JA
<b>Bedeutung</b>	Der Subject-Key-Identifier wird verwendet, um den öffentlichen Schlüssel des X.509 v3 Zertifikats eindeutig identifizieren zu können, mit dem der symmetrische Sessionkey verschlüsselt wurde. Der Austausch des Subject-Key-Identifiers erfolgt in hexadezimaler Darstellung.
<b>Syntax</b>	attachmentSubjectKeyIdIdentifier:= UTF_CHAR
<b>Multi-valued</b>	NEIN
<b>Anzeige (default)</b>	NEIN
<b>Beispiel</b>	d71d4b134efaceefcebef3032b8275f380bfbb15
<b>XML-Schema-Type</b>	<i>xs:token</i>

<b>3.1.2.73 Verfahrensspezifische Metadaten</b>	
<b>OID</b>	1.2.40.0.10.2.5.1.6; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.1.6
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Diese Gruppe beinhaltet verfahrensspezifische Metadaten, die ein Versender beim Anzeigemodul registrieren muss und deren OID in diesem Teilbaum eingeordnet wird.

**3.1.2.74 Teilbaum, der speziell für das TNVZ bestimmt ist**

<b>OID</b>	1.2.40.0.10.2.5.2; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.2
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppierung für alle Metadaten, die speziell für das TNVZ bestimmt sind. Die Metadaten dieses Teilbaums werden vom Anzeigemodul ignoriert.

**3.1.2.75 Zusätzliche Metadaten, die speziell für das TNVZ bestimmt sind**

<b>OID</b>	1.2.40.0.10.2.5.2.1; definiert durch ZUSE (dieses Dokument)
<b>ZUSE-Metadata Name</b>	urn:oid: 1.2.40.0.10.2.5.2.1
<b>Teilbaum</b>	JA
<b>Verpflichtend</b>	NEIN
<b>Bedeutung</b>	Gruppe der zusätzlichen Metadaten, die speziell für das TNVZ bestimmt sind.

## 3.2 Metadaten Schnittstelle

Dieser Abschnitt definiert die technische Schnittstelle(n) für die Übertragung von Metadaten von einem Zustellsystem zum Anzeigemodul. Aufgrund der generischen Definition von Metadaten in Abschnitt 3.1 können grundsätzlich beliebige Schnittstellenformate zum Einsatz kommen. Im Sinne der Flexibilität, d.h. wenn bspw. neue Metadatendefinitionen notwendig werden, sowie einer nachhaltigen zukunftsfähigen Schnittstellendefinition, sollen neue Technologien relativ einfach für die Umsetzung dieser Schnittstelle eingesetzt werden können. Folgende Technologien werden im Rahmen dieser Spezifikation aktuell unterstützt:

- Extensible Markup Language (XML)

Jede Technologiespezifikation der Metadaten-Schnittstelle ist unterteilt in die folgenden drei Abschnitte:

- **Authentifizierung** – definiert die beidseitige Authentifizierung zwischen Zustellsystem und Anzeigemodul
- **Format** – legt das technische Format fest, in welchem Metadaten definiert werden
- **Binding** – definiert das Protokoll, über welches die Metadaten im entsprechenden Format nach erfolgreicher Authentifizierung übertragen werden.

### 3.2.1 XML Format und Binding

#### 3.2.1.1 Authentifizierung

Die Authentifizierung der Zustellsysteme gegenüber dem Anwendungsportal des Anzeigemoduls dem MUSS gemäß den Vorgaben aus Abschnitt 2 erfolgen.

Wenn die Authentifizierung über Portalverbundtechnologie (vgl. Kapitel 2.1 Teilnehmer des Portalverbunds) erfolgt, MUSS vom Portal des Zustellsystems folgende Rolle übermittelt werden:

- ZUSE-DELIVERY-SERVICE

Beispiel für die zu setzenden PVP 2.1 Http-Header:

```
POST /abc.gv.at/anwendung2/xyz HTTP/1.1
Host:zustellsystem.at
User-Agent: .JNET 1.1
X-PVP-VERSION: 2.1
X-PVP-BINDING: http
X-PVP-PARTICIPANT-ID: AT:VKZ:XFN-999999x
X-PVP-USERID: support@zustellsystem.at
X-PVP-PRINCIPALNAME: Zustellsystem GmbH
X-PVP-SECCLASS: 2
X-PVP-ROLES: ZUSE-DELIVERY-SERVICE
Content-Type: text/xml
Content-Length: 788
```

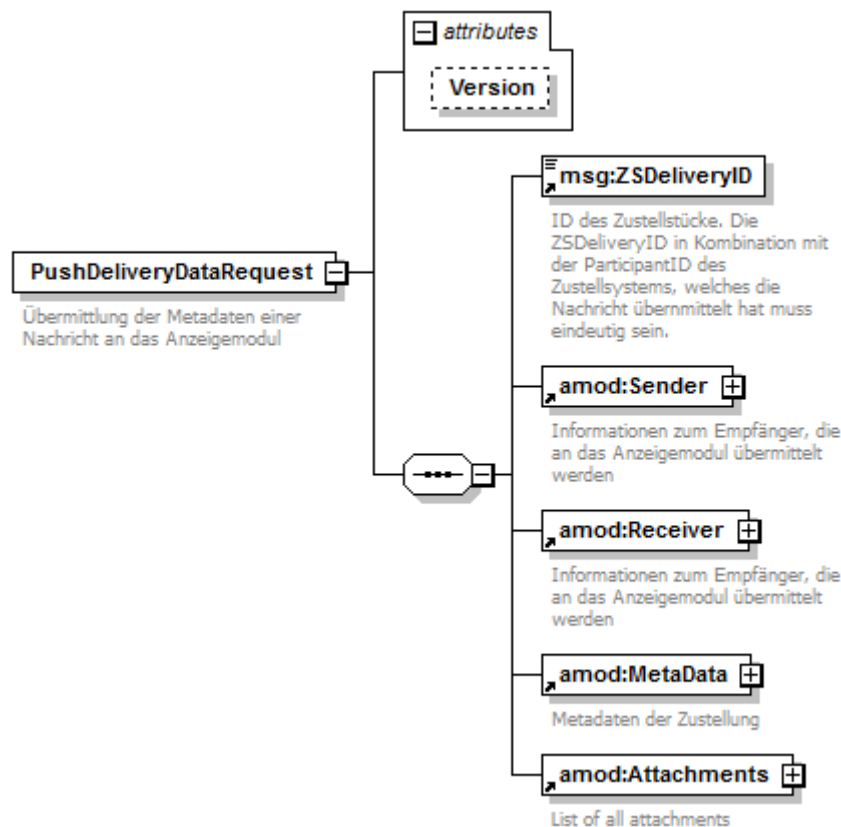
Wenn die Authentifizierung mittels Zertifikats (vgl. Kapitel 2.2 Nicht Teilnehmer des Portalverbunds) erfolgt, MUSS vom Zustellsystem nur das Zertifikat übermittelt werden und es DÜRFEN keine PVP 2.1 Http-Header übermittelt werden.

#### 3.2.1.2 Format

Dieser Abschnitt beschreibt Anfragen (Request) bzw. Antworten (Response) für die Übertragung von Metadaten im XML-Format.

##### 3.2.1.2.1 Request

Vom Zustellsystem an das Anzeigemodul zu übertragende Metadaten werden über das `amod:PushDeliveryDataRequest` Element gekapselt (siehe Abbildung 1).

Abbildung 1 – Struktur des `amod:PushDeliveryDataRequest` Elements

Ein Zustellsystem darf den Push der Metadaten erst dann ausführen, wenn alle Attachments einer Nachricht - auch jene die asynchron über HTTP-GET beim Versender abzuholen sind - beim Zustellsystem persistiert wurden.

Im `amod:PushDeliveryRequest` Element wird unterschieden zwischen Metadaten zum Versender (`amod:Sender` Element), Empfänger (`amod:Receiver` Element), den Nachrichten-Metadaten (`amod:MetaData` Element), sowie Metadaten zu den Anhängen (`amod:Attachments` Element).

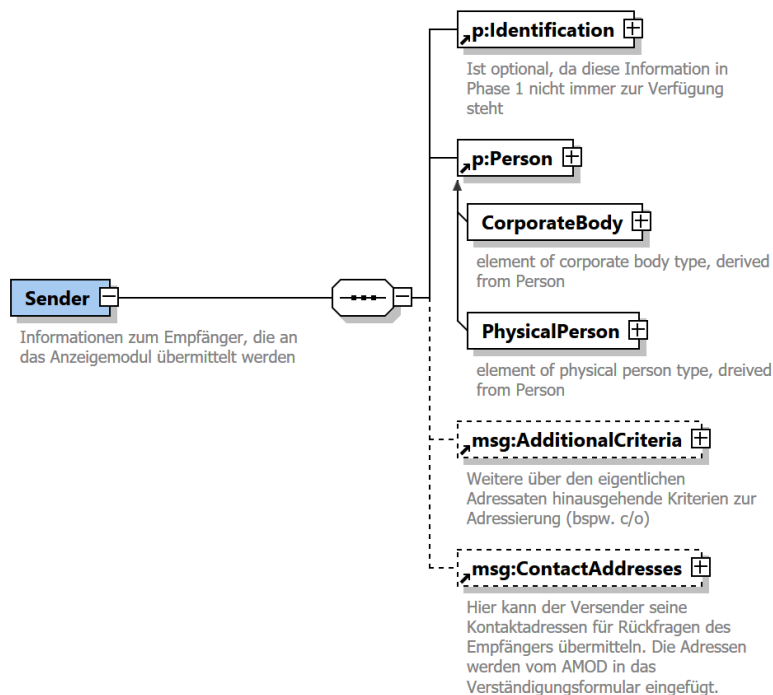
Das `Version` Attribut MUSS verpflichtend gemäß dem regulären Ausdruck `[0-9]{1,2}\.[0-9]{1,2}\.[0-9]{1,2}-[0-9]{3}` gesetzt sein. Die ersten drei Nummern repräsentieren die Versionsnummer des zugrundeliegenden ZUSEAMOD-Spezifikationsdokuments. Die vierte Nummer ist die fortlaufende Release-Nummer, die bei der Veröffentlichung einer neuen Version des XML-Schemas inkrementiert wird.

Für Definition des `msg:ZSDeliveryID` Elements siehe Abschnitt 3.1.2.1.

#### 3.2.1.2.1.1 Sender

Die Angabe des Identifikators des Versenders MUSS über die Elemente `p:Identification/p:Type` (Definition in Abschnitt 3.1.2.4) sowie `p:Identification/p:Value` (Definition in Abschnitt 3.1.2.5) erfolgen.

Abbildung 2 – Struktur des amod:Sender Elements



Abhängig vom Typ des Versenders, müssen dessen Personendaten über folgende Elemente angegeben werden:

- Ist der Versender eine Behörde oder ein Unternehmen, so MUSS der Name über das Element `msg:Sender/p:CorporateBody/p:FullName` (Definition siehe Abschnitt 3.1.2.8) angegeben werden.
- Natürliche Personen sind als Versender nicht zugelassen.

Zusätzlich KÖNNEN noch weitere Metadaten des Versenders angegeben werden, um eine organisationsinterne manuelle oder automatische Verteilung der Nachrichten zu ermöglichen:

- Mailbox über das Element `msg:AdditionalCriteria/msg:MailBox` (Definition siehe Abschnitt 3.1.2.12)
- Rollen über das Element `msg:AdditionalCriteria/msg:Roles/msg:Role` (Definition siehe Abschnitt 3.1.2.14)
- Zu Handen über das Element `msg:AdditionalCriteria/msg:CareOf`
  - Zu Handen elektronische Adresse als E-Mail über `msg:CareOf/p:ElectronicAddress/p:InternetAddress` (Definition siehe Abschnitt 3.1.2.17) als Möglichkeit zur automatisierten Verteilung von Nachrichten innerhalb der Organisation des Empfängers
  - Name der Zu-Handen-Person als Freitext. Wird nur der Name übermittelt, kann die Verteilung innerhalb der Organisation des Empfängers nur manuell erfolgen (Definition siehe Abschnitt 3.1.2.18).

Optional kann der Versender im `msg:ContactAddresses` Element eine Liste von maximal drei elektronischen Kontaktadressen übermitteln, die vom Anzeigemodul im Verständigungsformular unter dem Titel „Rückfragen beim Versender unter“ eingefügt werden. Eine elektronische Adresse kann entweder eine Telefonnummer (`msg:TelephoneAddress`) oder eine E-Mail-Adresse (`msg:InternetAddress`) sein. Internetadressen sind als Uniform Resource Locator (URL) gemäß [RFC3986] zu formulieren. Wobei der Wertebereich der zulässigen Schema-Namen auf „https:“ und „mailto:“ beschränkt ist.

### 3.2.1.2.1.2 E-Mail-Adressen (msg:InternetAddress)

E-Mail-Adressen sind eine spezielle Form einer Internet-Adresse. Internet-Adressen sind als „Uniform Resource Locator (URL)“ gemäß [RFC3986] zu formulieren.

Speziell für E-Mail-Adressen gilt zusätzlich, dass diese gemäß [RFC5322] aufgebaut sein MÜSSEN und der Schema-Name „mailto:“ auch weggelassen werdend DARF.

Folgende Beispiele stellen gültige E-Mail-Adressen dar:

mailto:max.mustermann@mail-service.at

max.mustermann@mail-service.at

mmustermann@mail-service.at

Folgende Beispiele stellen UNGÜLTIGE E-Mail-Adressen dar:

mailto: max.mustermann@mail-service.at //Leerzeichen sind nicht zulässig

.@mail-service.at

mmustermann@.mail-service.at

mmustermann@mail-service.at.

mmustermann.@mail-service.at

.mmustermann@mail-service.at

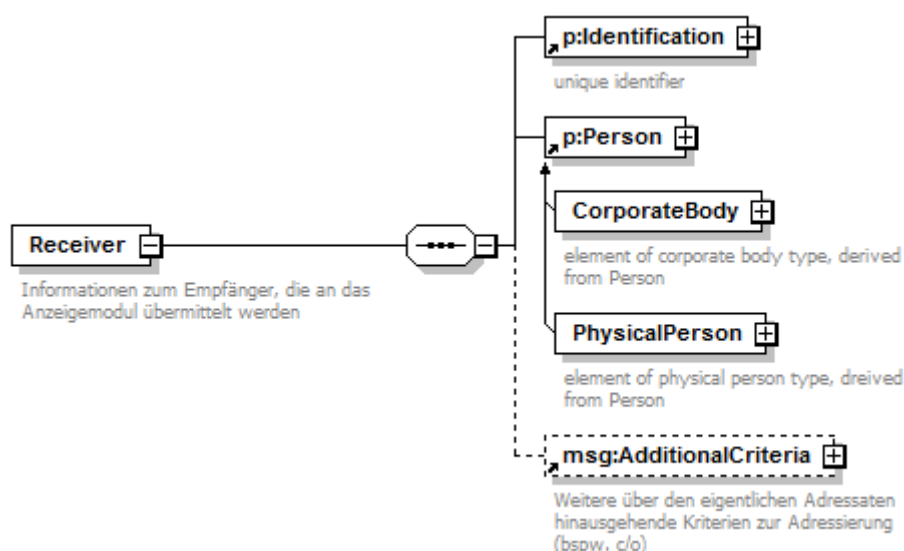
mmustermann.@.mail-service.at

mmustermann@1.1

### 3.2.1.2.1.3 Empfänger

Die verpflichtende Angabe des Identifikators des Empfängers erfolgt über die Elemente p:Identification/p:Type (Definition in Abschnitt 3.1.2.24) sowie p:Identification/p:Value (Definition in Abschnitt 3.1.2.25).

Abbildung 3 – Struktur des amod:Receiver Elements



Abhängig vom Typ des Empfängers, müssen dessen Personendaten über folgende Elemente angegeben werden:

- Ist der Empfänger eine Behörde oder ein Unternehmen, so MUSS der Name des Unternehmens über das Element p:CorporateBody/p:FullName (Definition siehe Abschnitt 3.1.2.8) angegeben werden. Optional kann zusätzlich über das Element

`p:CorporateBody/p:Organisation` eine Organisationseinheit innerhalb der Behörde oder des Unternehmens angegeben werden.

- Ist der Empfänger eine natürliche Person, so MUSS dieser über die Elemente `p:PhysicalPerson/p:Name/p:GivenName` (Definition siehe Abschnitt 3.1.2.32) `p:PhysicalPerson/p:Name/p:FamilyName` (Definition siehe Abschnitt 3.1.2.33) `p:PhysicalPerson/p:Name/p:DateOfBirth` (Definition siehe Abschnitt 3.1.2.34) angegeben werden.

Zusätzlich KÖNNEN noch weitere Metadaten des Empfängers angegeben werden, um eine organisationsinterne manuell oder automatische Verteilung von Nachrichten zu ermöglichen:

- Mailbox über das Element `msg:AdditionalCriteria/msg:MailBox` (Definition siehe Abschnitt 3.1.2.36)
- Rollen über das Element `msg:AdditionalCriteria/msg:Roles/msg:Role` (Definition siehe Abschnitt 3.1.2.38)
- Zu-Handen-Zustellung an eine natürliche Person innerhalb der Organisation über das Element `msg:AdditionalCriteria/msg:CareOf`<sup>1</sup>
  - Zu Handen elektronische Adresse, als E-Mail, über `msg:CareOf/p:ElectronicAddress/p:InternetAddress` (Definition siehe Abschnitt 3.1.2.41) als Möglichkeit zur automatisierten Verteilung von Nachrichten innerhalb der Organisation des Empfängers
  - Name der Zu-Handen-Person als Freitext. Wird nur der Name übermittelt, kann die Verteilung innerhalb der Organisation des Empfängers nur manuell erfolgen (Definition siehe Abschnitt 3.1.2.42).

---

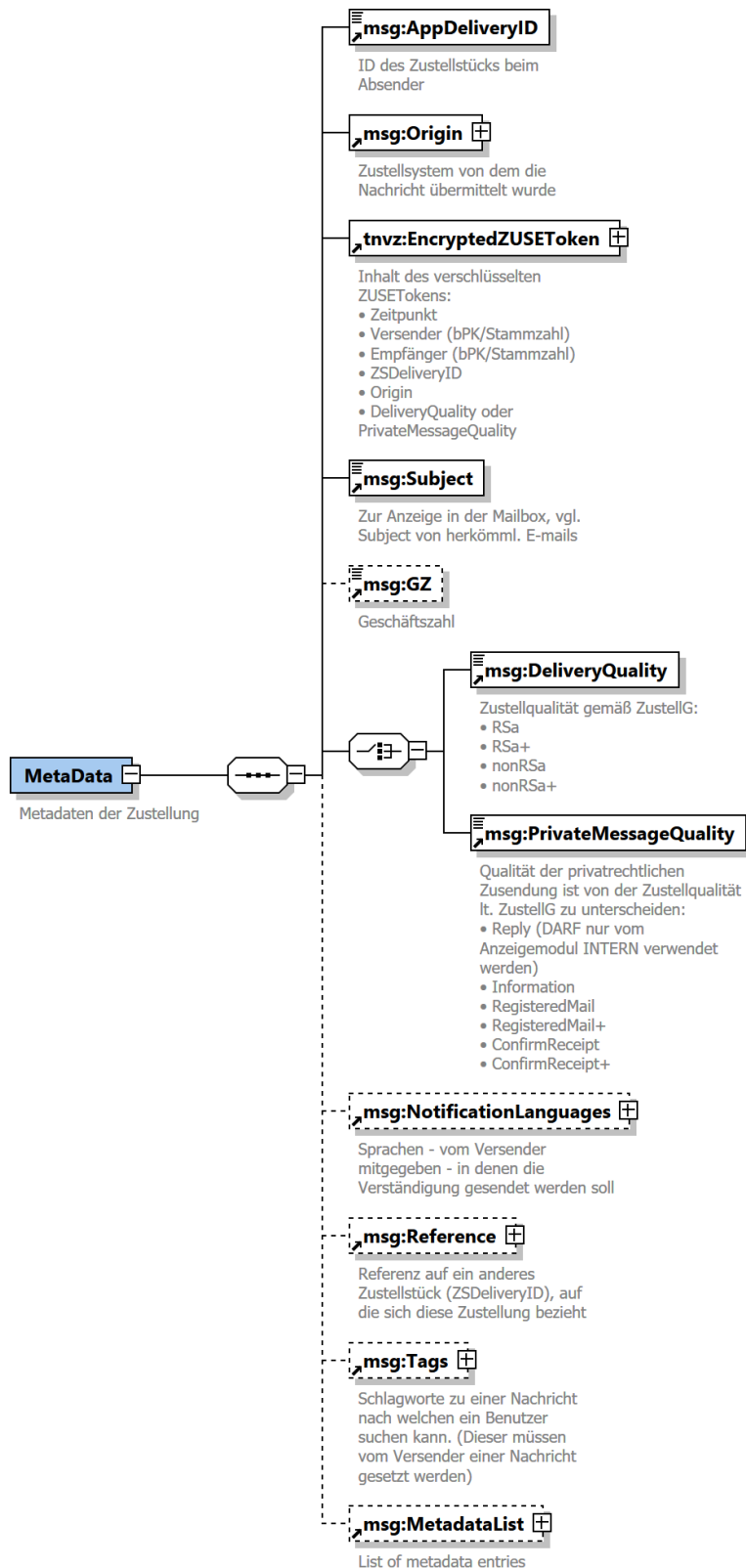
<sup>1</sup> Das englische "care of" entspricht grundsätzlich dem im deutschen Sprachraum gebräuchlichen "per Adresse". Im Kontext der elektronischen Zustellung wird das "care of" jedoch als "zu Handen" interpretiert.



### 3.2.1.2.1.4 Metadaten

Pro Request können grundsätzlich beliebig viele Metadaten übergeben werden. Es gibt vordefinierte Metadaten sowie die Möglichkeit verfahrensspezifische Metadaten zu übergeben.

Abbildung 4 – Struktur des `amod:MetaData` Elements



Um die Sendung nachverfolgen zu können, MUSS das `msg:AppDeliveryID` Element (Definition siehe [ZUSEMSG]) die Nachrichten-ID der versendenden Anwendung enthalten.

Das Herkunftssystem bzw. versendende Zustellsystem, über das die Nachricht zum Anzeigemodul übermittelt wurde, MUSS im `msg:Origin` Element (Definition siehe 3.1.2.45) angegeben sein.

Die PVP-Participant-ID des Zustellsystems, welches Ursprung der Sendung ist, MUSS im Elements `msg:Origin/msg:ParticipantID` (Definition siehe 3.1.2.46) angegeben werden

Über das Element `msg:Subject` (Definition siehe 3.1.2.47) MUSS der Betreff der Nachricht angegeben werden.

Über das Element `msg:GZ` (Definition siehe 3.1.2.48) KANN optional die Geschäftszahl der Zustellung angegeben werden.

Die Angabe der Zustellqualität ist verpflichtend. Es MUSS entweder die behördliche Zustellqualität über das Element `msg:DeliveryQuality` (Definition siehe 3.1.2.49) oder die privatrechtliche Zusendungsqualität über das Element `msg:PrivateMessageQuality` (Definition siehe 3.1.2.50) angegeben werden.

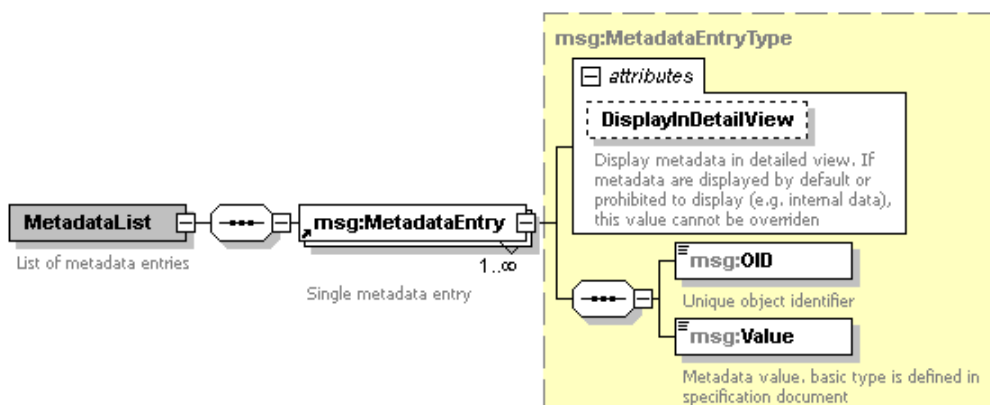
Der Versender KANN eine Liste von alternativen Minderheitensprachen über das das Element `msg:NotificationLanguages` (Definition siehe 3.1.2.51) angegeben. Diese Liste von Minderheitensprachen wird gemeinsam mit den vom Teilnehmer im TNVZ hinterlegten Minderheitensprachen beim Verfassen von Verständigungen berücksichtigt.

Des Weiteren KANN eine Referenz zu einer anderen Nachricht über das Element `msg:Reference/msg:ZSDeliveryID` (Definition siehe 3.1.2.53) angegeben werden.

Jede Nachricht KANN mit Tags bzw. Schlagworten versehen werden. Dies erfolgt über das Element `msg:Tags/msg:Tag` (Definition siehe 3.1.2.56).

Optional KANN eine Liste von verfahrensspezifischen Attributen übergeben werden. Dies MUSS über das Element `msg:MetadataList/msg:MetadataEntry` (Definition siehe 3.1.2.58) erfolgen.

**Abbildung 5 – Struktur des `msg:MetadataList` Elements**



Will ein Versender eigene verfahrensspezifische Attribute in der Detailansicht der Nachricht anzeigen lassen, so muss er diese zuerst beim Anzeigemodul registrieren. Im Zuge der Registrierung erhält der Versender vom Anzeigemodul für jedes einzelne Attribut eine OID, welche bei der Übermittlung angegeben werden muss.

Das Attribut `DisplayInDetailView` gibt dabei an, ob das Metadatum in der Detailanzeige einer Zustellung angezeigt werden soll. Die Angaben zum Metadatum für `OID` (Definition siehe 3.1.2.59) und `Value` (Definition siehe 3.1.2.60) sind gemäß der Definition in Abschnitt 1.2 zu befüllen.

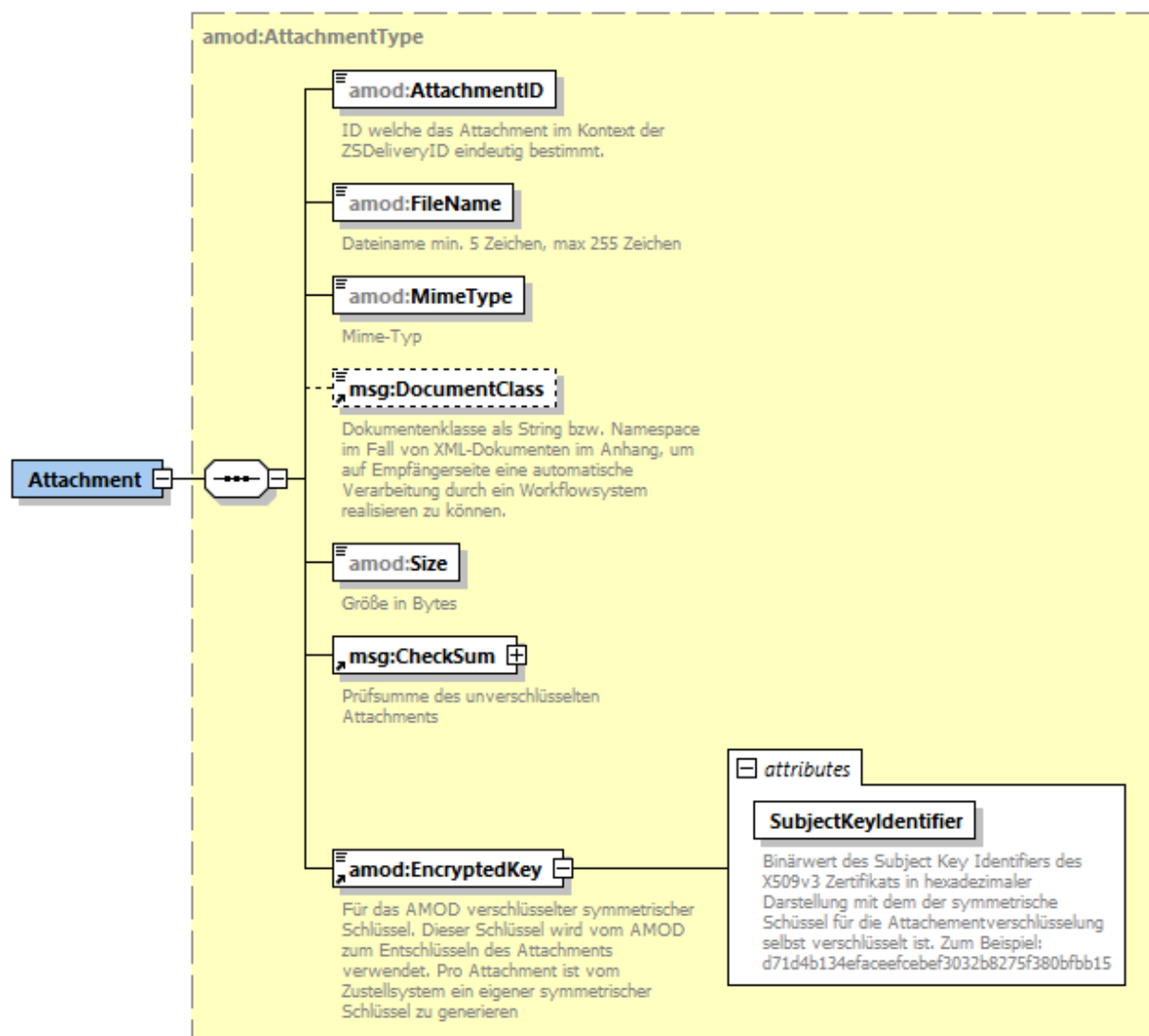
Folgende Liste von MetadataEntry Elemente werden vom Anzeigemodul unterstützt:

- In der gegenständlichen Fassung definiert dieses Dokument keinen zusätzlichen Metadaten

### 3.2.1.2.1.5 Anhänge

Die Metadaten zu jedem einzelnen Attachment werden in die Liste der Attachment-Metadaten (amod:Attachments) des amod:PushMetadataRequests aufgenommen. Der Mailbody einer Nachricht wird zum ersten Attachment. Im Element msg:DocumentClass ist für das erste Attachment jedenfalls der Wert „Mailbody“ einzutragen, um den Mailbody eindeutig aus der Liste der Attachments herausfiltern zu können. Der MIME-Type darf nur text/plain sein. (HTML ist nicht zulässig). Es darf nur ein Attachment geben für das gilt: msg:DocumentClass = „Mailbody“.

Abbildung 6 – Struktur des amod:Attachment Elements



Für jede Nachricht MÜSSEN die Metadaten sämtlicher Anhänge angegeben werden. Pro Attachment sind folgende Metadaten anzugeben (siehe Abbildung 6):

- **AttachmentID** – Eindeutige ID des Attachments innerhalb der Nachricht (Definition siehe 3.1.2.63)
- **FileName** – Dateiname des Attachments (Definition siehe 3.1.2.64)

- **MimeType** – MIME-Typ (Content-Type) des Attachments (Definition siehe 3.1.2.65)
- **DocumentClass** (optional) – Dokumentenklasse des Attachments (Definition siehe 3.1.2.66)
- **Size** – Dateigröße des Attachments (Definition siehe 3.1.2.67)
- **Checksum** – Hashwert des Attachments (Definitionen siehe 3.1.2.69 und 3.1.2.70)
- **EncryptedKey** – Verschlüsselter symmetrischer Sessionkey mit dem das Attachment für das AMOD verschlüsselt wurde. Details zur Verschlüsselung siehe Abschnitt 5.2 *Verschlüsselung von Attachments*
- **SubjectKeyIdentifier** – Der Subject-Key-Identifier mit der OID 2.5.29.14 wird verwendet, um den öffentlichen Schlüssel des X.509 v3 Zertifikats eindeutig identifizieren zu können, mit dem der symmetrische Sessionkey verschlüsselt wurde. Details zur Verschlüsselung siehe Abschnitt 5.2 *Verschlüsselung von Attachments*

### 3.2.1.2.1.6 URL-Action-Links

URL-Action-Links stellen eine Erweiterung der AMOD-Metadaten gemäß „verfahrensspezifische Metadaten“ dar. Hier haben Verfahren die Möglichkeit URLs anzugeben, um direkt aus der Nachricht in die Versender-Applikation zu verlinken.

Wenn die Nachricht ein Attachment enthält, für das gilt:

- MIME-Type = „application/xml“ und
- Dokumentenklasse (`msg:DocumentClass`) = „http://reference.e-government.gv.at/namespace/zustellung/urlaction/20180116#“

dann enthält das Attachment ein XML-File mit URL-Action-Links, welche vom Anzeigemodul interpretiert werden können.

Seitens Anzeigemoduls wird geprüft, ob die URL über eine zugelassene technische Methode (https) anzusprechen ist und ob der angegebene Domainname in der Liste der zugelassenen Domains enthalten ist (Whitelisting der Domainnamen). Aus Sicherheitsgründen müssen die an das Anzeigemodul übermittelten Domainnamen vorab bekannt gegeben werden. Wenn in den URL-Action-Links ein Domainname angegeben ist, der nicht im Anzeigemodul registriert ist (Whitelisting), wird die Nachricht nicht angenommen.

Die Verkettung aller Elemente zur vollständigen URL und Visualisierung im User Interface erfolgt durch das Anzeigemodul.

Werden zusätzliche XML-Metadaten für das AMOD via Attachments übermittelt, müssen diese wie in Kapitel 3.2.1.2.1.5 Anhänge beschrieben, mitgegeben werden. Abhängig von `msg:DocumentClass` Element ist die Dateigröße von Attachments mit zusätzlichen XML-Metadaten für das Anzeigemodul limitiert.

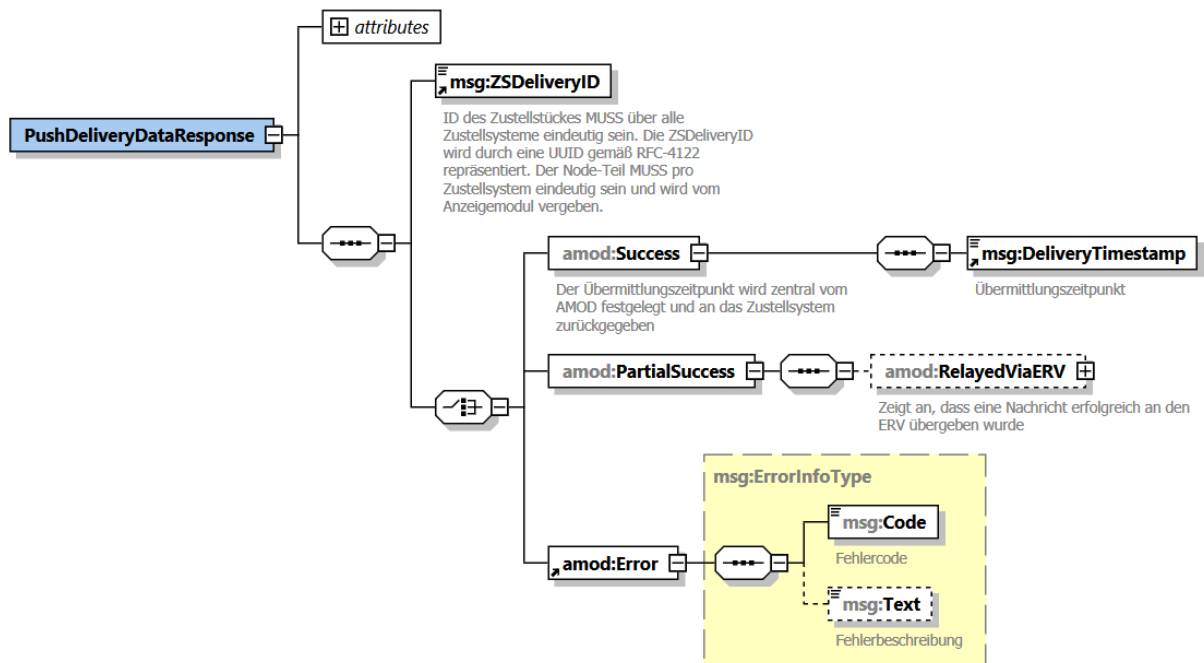
Aktuelle gelten folgende Limits:

DocumentClass	Limit
<code>http://reference.e-government.gv.at/namespace/zustellung/urlaction/20180116#</code>	128kByte

### 3.2.1.2.2 Response

Die Antwort auf einen `amod:PushDeliveryDataRequest` ist über das `amod:PushDeliveryDataResponse` Element definiert (siehe Abbildung 7).

Abbildung 7 – Struktur des `amod:PushDeliveryDataResponse` Elements



Konnten für eine Nachricht die Metadaten erfolgreich übermittelt werden, so wird dies vom Anzeigemodul mit einem `amod:Success` Element bestätigt. Der Zeitpunkt der Übermittlung wird in der Response im `msg:DeliveryTimestamp` Element zurückgegeben.

Wenn die Zustellung in den Elektronischen Rechtsverkehr der Justiz (ERV) weitergeleitet wurde, wird dies dem zuständigen Zustellsystem vom Anzeigemodul mit einem `amod:PartialSuccess\amod:RelayedViaERV` Element angezeigt. In diesem Fall ist die Zustellung noch nicht abgeschlossen. Erst mit der zeitversetzt übermittelten Nachrichtenoperation `amod:ERVConfirmedDelivery` wird der erfolgreiche Abschluss der Zustellung inklusive Zustellzeitpunkt zurückgemeldet.

Im Fehlerfall (`amod:Error`) werden `msg:Code` und `msg:Text` zurückgeliefert, die das Problem bei der Übermittlung der Metadaten einer Nachricht beschreiben. Die anwendbaren Fehler-Codes sind in Tabelle 2 angeführt.

Tabelle 2 – Fehler-Codes im Nichterfolgsfall

Code	Error-Message	Beschreibung
<i>Allgemein</i>		
AM0403_U	Not permitted	Operation ist nicht zulässig
AM0500_R	Internal Server Error	Interner Fehler
<i>Metadaten</i>		

Code	Error-Message	Beschreibung
AM3001_U	Origin incomplete	Wenn Daten zur Bestimmung des Zustellsystems einer Nachricht nicht vollständig sind.
AM3002_U	Unknown origin	Das Zustellsystem, welches Ursprung der Nachricht ist, ist dem Anzeigemodul nicht bekannt
AM3003_U	DeliveryQuality missing	Die Nachrichtenqualität, d.h. entweder die Zustellqualität oder die privatrechtliche Sendungsqualität muss angegeben sein.
AM3004_U	Unknown deliveryQuality	Die angegebene Nachrichtenqualität ist unbekannt
AM3005_U	Portal incomplete	Wenn Daten zur Bestimmung des Portals, für welches die Nachricht bestimmt ist, nicht vollständig sind
AM3006_U	Unknown portal	Das angegebene Portal für das die Nachricht bestimmt oder optimiert ist, ist dem Anzeigemodul unbekannt
AM3007_U	Unknown property datatype	Wenn der in den verfahrensspezifischen Metadaten ( <code>msg:Properties</code> ) verwendete Datentyp nicht unterstützt wird
AM3008_U	Receiver identification missing	Personenkennung des Empfängers ist nicht gesetzt
AM3009_U	Unknown identificationType in receiver	Der angegebene Typ der Personenkennung wird vom Anzeigemodul nicht unterstützt
AM3010_U	Familyname of physicalPerson missing	Der Familienname des Empfängers (oder Versenders) fehlt
AM3011_U	Fullname of corporate body missing	Der volle Name des Unternehmens - entweder Empfängers oder Versender - fehlt
AM3013_U	Invalid careOf	Die Metadaten für die „Zu Handen“-Zustellungen sind ungültig
AM3014_U	Property value missing	Der Wert eines verfahrensspezifischen Metadatums ist ungültig
AM3015_U	DeliveryQuality 'Information' only allowed for authorities	Nur Behörden steht der Sendungsqualität „Information“ zur Verfügung

Code	Error-Message	Beschreibung
AM3018_U	Value validation failed. Invalid fields: <fieldNames_commaseparated>	Die Überprüfung der übermittelten Metadaten ist fehlgeschlagen. Die fehlerhaften Felder werden in der Liste in der Fehlermeldung mitgegeben
AM3019_U	Message with given zsDeliveryID already exists	Nachricht mit der angegebenen Zustellsystem-ID existiert bereits
AM3020_R	The validity period of the ZUSEToken has expired	Das ZUSEToken ist abgelaufen. Das Zustellsystem muss den Webservice-Call QueryAddressability wiederholen
AM3021_U	The request's metadata doesn't match with ZUSEToken data	Die Metadaten im Request stimmen nicht mit den Daten im ZUSEToken überein
AM3022_U	Insufficient ZUSE specification version - expected version number: %1 actual version number: %2	Die vom Zustellsystem implementierte ZUSE-Spezifikationsversion ist veraltet <ul style="list-style-type: none"> <li>Parameter %1: Erwartete Mindest-Versionsnummer</li> <li>Parameter %2: Vom Zustellsystem übermittelte Versionsnummer</li> </ul>
<i>Metadaten zu den Attachments</i>		
AM4001_U	No mailbody attachment given	Es muss ein Mailbody mitgegeben werden
AM4002_U	First attachment not marked as mailbody	Das erste Attachment muss den Mailbody enthalten
AM4003_U	First attachment (mailbody) must be plain text	Der Mailbody muss im Textformat (MIME-Type plain/text) sein
AM4004_U	Metadata-attachment too big	Wenn zu einer Nachricht erweiterte Metadaten mitgeliefert werden, die vom Anzeigemodul interpretiert werden (z.B. URL-Actionlinks), so gilt eine definierte maximale XML-Dateigröße. Wird diese Dateigröße überschritten, wird die gesamte Nachricht mit einer Fehlermeldung abgewiesen.  URL-Actionlinks: max. 128kByte
AM4005_U	Referenced metadata- xml-attachment missing	Das in den Metadaten referenzierte Attachment fehlt

Code	Error-Message	Beschreibung
AM4006_U	Invalid metadata-attachment	Die erweiterten Metadaten für das Anzeigemodul, welche als Attachment mitgeliefert wurden, können nicht korrekt interpretiert werden.
AM4007_U	Invalid file name	Der Filename entspricht nicht den Konventionen
AM4008_U	The submitted MIME-Type %1 is not supported	Der übermittelte MIME-Type wird nicht unterstützt <ul style="list-style-type: none"> <li>Parameter %1: Übermittelter MIME-Type</li> </ul>
<i>URL Action Links</i>		
AM4021_U	Invalid portnumber in urlaction-metadata-attachment	Die Port-Nummer der URL ist entweder keine Nummer oder liegt außerhalb des zulässigen Bereichs
AM4022_U	Given urlaction-domain not allowed	Der in der URL verwendete Domainname muss beim Anzeigemodell registriert werden.  Anderenfalls wird die Annahme der Nachricht verweigert.

### 3.2.1.3 Binding

Für den Datenaustausch MUSS das Netzwerkprotokoll SOAP in der Version 1.2 über das HTTP Binding in [SOAP12] verwendet werden.

Sämtliche Kommunikation muss gesichert gemäß den Anforderungen in Abschnitt 3.2.1.1 erfolgen.

Die entsprechende WSDL-Beschreibung ist als gesonderte Datei der Spezifikation beigelegt.

- zuseamod\_p2.wsdl



## 4 Übermittlung von Nachrichtenoperationen an Zustellsysteme

Im Zuge der Interaktion des Empfängers mit dem Anzeigemodul kann sich der Status von Zustellungen ändern. Dies betrifft sowohl die Interaktion über GUI-basierte Zugänge wie Browser, als auch automatisierte M2M Zugänge über eine automatisierte Abholung. Des Weiteren können auch bestimmte weitere Ereignisse eine Änderung von Zuständen eines Zustellstücks auslösen. Dieser Abschnitt definiert die Übermittlung derartiger Nachrichtenoperationen vom Anzeigemodul an das Zustellsystem.

Bezogen auf den Nachrichtenstatus und die Metadaten ist das Anzeigemodul das führende System.

Eine Nachricht gilt für Versender erst dann als erfolgreich übermittelt, wenn der erfolgreiche Push der Metadaten vom Anzeigemodul bestätigt wurde.

Der Zeitpunkt der Übermittlung wird in der Response zur Übertragung der Metadaten dem zuständigen Zustellsystem übermittelt.

Zustellsysteme müssen damit umgehen können, dass sie vom AMOD mehrfach die GLEICHE Nachrichtenoperation zu einer Nachricht erhalten. Aufgrund von Synchronisationsproblemen kann es vorkommen, dass das AMOD zu einer Nachricht eine Nachrichtenoperation mit der gleichen OperationID mehrfach versendet.

Wenn das Zustellsystem bereits eine MessageOperation mit einer bestimmten OperationID verarbeitet hat, dann ist diese erneute Übermittlung der MessageOperation zu ignorieren. Keinesfalls ist dem AMOD mit einer Fehlermeldung zu antworten.

### 4.1 Nachrichtenoperationen Definitionen

Folgende Ereignisse lösen die Übermittlung einer Nachrichtenoperation an das Zustellsystem aus.

- **Nachweisliche Zustellung angenommen** (`amod:Accepted`): Nur im Falle einer nachweislichen Zustellung, wenn der Empfänger eine Nachricht entweder durch direkte Anmeldung am Anzeigemodul via Web-Browser oder über eine automatisierte Schnittstelle annimmt, ist die Annahme an den zuständigen Zustelldienst zu kommunizieren. Der Zustelldienst hat die Übermittlung der elektronischen Zustellbenachrichtigung mit Zustellnachweis an den Versender zu initiieren.
- **Zustellmangel „Verständigung fehlgeschlagen“** (`amod:DeliveryError(AM0101_U)`): Wenn die Verständigung an einen Empfänger fehlschlägt, ist dieser Mangel an den für die Nachricht zuständigen Zustelldienst zurückzumelden.
- **Zustellhindernis „Verständigung fehlgeschlagen und Abholfrist verstrichen“** (`amod:DeliveryError(AM0102_U)`): Wenn die Verständigung an den Empfänger fehlgeschlagen ist und der Empfänger die nachweisliche Zustellung nicht innerhalb der Abholfrist abholt, liegt ein Zustellhindernis vor und die Zustellung gilt als nicht bewirkt.
- **Ablauf der Abholfrist** (`amod:DeliveryError(AM0100_U)`)<sup>2</sup>: Läuft die Abholfrist gemäß [ZUSTG] ab, MUSS dieses Ereignis dem verantwortlichen Zustelldienst zurückgemeldet werden, damit dieser den Zustellnachweis an den Versender

<sup>2</sup> Diese fachliche Gegebenheit ist in der technischen Spezifikation der Schnittstelle nicht exakt abgebildet, da der Ablauf der Abholfrist streng genommen keinen Fehler darstellt. Denn mit dem Verstreichen der Abholfrist kann die nachweisliche Zustellung dennoch als bewirkt gelten (Zustellfiktion), sofern keine Ausnahmetatbestände des ZUSTG vorliegen.

retourniert. Die nachweisliche Zustellung steht dem Empfänger weiterhin bis zum Ablauf der Vorhaltdauer gemäß [ZUSTG] im AMOD zur Verfügung.

- **Zustellhindernis „Empfänger hat keinen Zugriff auf Postfach“** (amod:Delivery-Error(AM0103\_U)): Wenn der Empfänger auf sein Postfach keinen Zugriff hat, liegt ein Zustellhindernis vor und die Zustellung gilt als nicht bewirkt. Gleichzeitig mit dieser Nachrichtenoperation wird auch die Nachrichtenoperation „Deleted“ an den Zustelldienst übermittelt.
- **Zustellhindernis „Empfänger hat keinen Zugriff auf die beigefügten Dokumente“** (amod:Delivery-Error(AM0104\_U)): Wenn der Empfänger auf beigefügte Dokumente keinen Zugriff hat, liegt ein Zustellhindernis vor und die Zustellung gilt als nicht bewirkt. Gleichzeitig mit dieser Nachrichtenoperation wird auch die Nachrichtenoperation „Deleted“ an den Zustelldienst übermittelt.
- **Weiterleitung in den ERV bestätigt** (amod:ERVConfirmedDelivery): Diese Operation zeigt an, dass eine in den ERV weitergeleitete Nachricht erfolgreich im Verfügungsbereich des Empfängers bzw. ERV-Teilnehmers eingelangt ist und damit als zugestellt gilt.
- **Verständigungsversuche** (amod:NotificationInformation): Die Nachrichtenoperation „NotificationInformation“ stellt keine Zustandsänderung im Zustellprozess dar, vielmehr wird das Zustellsystem 24 Stunden nach dem Eintreffen der Nachricht über den Status bezüglich der Verständigung informiert, falls noch keine andere Nachrichtenoperation ausgeführt wurde.
- **Nachricht gelöscht** (amod:Deleted): löscht ein Benutzer eine Nachricht aus dem Papierkorb oder wird eine Nachricht automatisch vom Anzeigemodul gelöscht, bspw. weil die Vorhaltdauer abgelaufen ist, so MUSS dieser Status an das für die Nachricht zuständige Zustellsystem übermittelt werden. Erst bei positiver Bestätigung durch das Zustellsystem sind die Metadaten am Anzeigemodul unwiderruflich zu löschen, andernfalls muss das Anzeigemodul so lange versuchen das Zustellsystem zu kontaktieren, bis die Statusinformation erfolgreich übertragen werden konnte.
- **Rückmeldung von technischen Problemen:** ist primär für den Ausnahmefall angedacht, wenn es einem Zustelldienst nicht möglich ist, die msg:DeliveryNotification inklusive PDF-Rückschein zu erzeugen. Durch das AMOD-Betriebsteam kann ein amod:MessageOperationRequest mit einem standardisierten Fehlercode und einer Fehlermeldung an den Zustelldienst gesendet werden, die den technischen Fehler mittels msg:DeliveryRequestStatus an den Versender weiterleiten. Anhand des standardisierten Fehlercodes ist der aktuelle Zustellprozessstatus für den Empfänger klar ersichtlich.
  - **Information „TechnicalError AM0300\_U“**  
Ein technisches Problem im Status „Abholfrist verstrichen“ ist aufgetreten.
  - **Information „TechnicalError AM0301\_U“**  
Es ist ein technisches Problem im Status „Verständigung fehlgeschlagen“ aufgetreten.
  - **Information „TechnicalError AM0302\_U“**
  - Es ist ein technisches Problem im Status „Verständigung fehlgeschlagen und Abholfrist verstrichen“ aufgetreten.
  - **Information „TechnicalError AM0310\_U“**  
Es ist ein technisches Problem im Status „Angenommen“ aufgetreten.

Durch folgende Nachrichtenoperationen wird im Fall einer nachweislichen Zustellung eine Zustellbenachrichtigung mit Zustellnachweis (`msg:DeliveryNotification`) ausgelöst:

- **DeliveryError AM0100\_U** - Abholfrist ist verstrichen: Gültige Zustellung, die nicht angenommen wurde
- **DeliveryError AM0101\_U** - Verständigung ist fehlgeschlagen: Stellt einen Zustellmangel dar, über den der Versender informiert werden muss. Dies ist ein temporärer Zustand, da der Empfänger bis zum Verstreichen der Abholfrist noch Kenntnis von der Zustellung erlangen kann („Heilung“)
- **DeliveryError AM0102\_U** - Verständigung fehlgeschlagen und Abholfrist verstrichen: Die Zustellung wurde „nicht bewirkt“
- **DeliveryError AM0103\_U** - Empfänger hat keinen Zugriff auf Postfach: Die Zustellung wurde „nicht bewirkt“
- **DeliveryError AM0104\_U** - Empfänger hat keinen Zugriff auf beigefügte Dokumente: Die Zustellung wurde „nicht bewirkt“
- **Accepted** - Nachricht angenommen
- **ERVConfirmedDelivery** - Nachricht wurde erfolgreich in den ERV zugestellt

## 4.2 Abfolge der Nachrichtenoperationen

Die möglichen und zulässigen Abfolgen von Nachrichtenoperationen werden abhängig von der Zustellqualität und anderer Parameter in den folgenden Abschnitten mittels Zustandsübergangsdiagrammen dargestellt. Jeder Zustand wird durch eine Box repräsentiert. Die Linien stellen die möglichen bzw. zulässigen Zustandsübergänge dar und legen die Reihenfolge fest, in der das AMOD Nachrichtenoperationen zum zuständigen Zustellsystem übermittelt.



Eine einfach gerahmte Box repräsentiert einen Zwischenstatus, d.h. zu dieser Nachricht sendet das AMOD weitere Webservice-Calls „**MessageOperation**“.



Eine doppelt gerahmte Box repräsentiert einen finalen Status. Wird ein finaler Status erreicht, muss das Zustellsystem die Nachricht löschen.



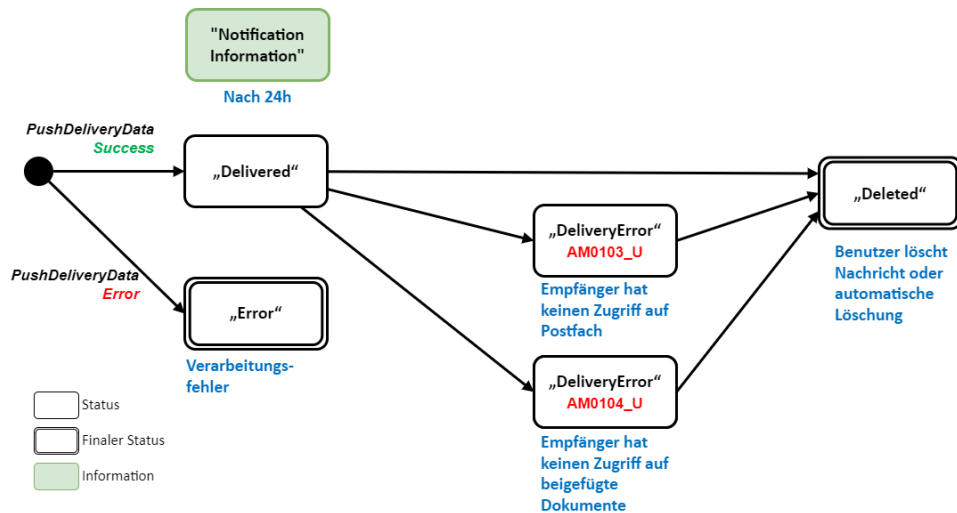
Eine einfach gerahmte Box in der Farbe Grün repräsentiert einen Informationsstatus.

Unter der Bedingung, dass die Nachricht im Vorfeld erfolgreich vom Zustellsystem an das AMOD gepusht wurde, d.h. die Webserviceoperation „**PushDeliveryData**“ vom AMOD mit „**Success**“ beantwortet wurde, fordert das AMOD jedenfalls und explizit das zuständige Zustellsystem mittels der finalen Nachrichtenoperation „**Delete**“ zur endgültigen Löschung einer Nachricht auf.

Endgültige Löschung der Nachricht bedeutet, dass die auslösende Aktion sowie alle Metadaten der Nachricht vom Zustellsystem zu protokollieren sind und alle Attachments der Nachricht unwiderruflich gelöscht werden.

#### 4.2.1 Nachrichtenoperationen, die bei der Zustellqualität „Zustellung bzw. Zusendung ohne Zustellnachweis“ vom AMOD an das Zustellsystem übermittelt werden

Abbildung 8 – Zustandsübergangsdiagramm für Zustellungen bzw. Zusendungen ohne Zustellnachweis



Wird das **PushDeliveryData** für eine nicht-nachweisliche Zustellung oder eine nicht-nachweisliche Sendung mit einem „**Success**“ vom AMOD beantwortet, dann konnte die Nachricht erfolgreich verarbeitet und der Versand der Verständigung erfolgreich angestoßen werden.

Tritt beim **PushDeliveryData** ein Fehler auf, antwortet das AMOD mit einem „**Error**“, die Zustellung gilt als „nicht durchgeführt“. In diesem Fall ist die Nachricht vom Zustellsystem zu löschen.

24 Stunden nach dem Eintreffen der Nachricht sendet das AMOD für nicht-nachweisliche Zustellungen bzw. Sendungen die Nachrichtenoperation „**NotificationInformation**“, falls noch keine andere Nachrichtenoperation ausgeführt wurde. Diese stellt keine Zustandsänderung im Zustellprozess dar, vielmehr wird das Zustellsystem über den Status bezüglich der Verständigung informiert. Betreffend folgender Situationen wird informiert:

- Verständigung ist noch nicht erfolgt oder es ist ein Fehler beim Versenden der Verständigung aufgetreten. In diesem Fall ist das `msg:NotificationsPerformed` Element nicht vorhanden.
- Die erste Verständigung wurde erfolgreich an den E-Mail-Server übergeben. In diesem Fall sind die Elemente `msg:NotificationsPerformed`, `msg:RecipientNotification` und `msg:Timestamp` gesetzt.
- Die erste Verständigung ist fehlgeschlagen (Bounce Message erhalten). In diesem Fall sind die Elemente `msg:NotificationsPerformed`, `msg:RecipientNotification` und `msg:Timestamp` gesetzt und das `msg:Failed` Element ist auf `true` gesetzt.

Wenn die Zustellung durch den Benutzer manuell, oder nach Ablauf der Vorhaltdauer gemäß [ZUSTG] automatisiert gelöscht wird, sendet das AMOD die finale Nachrichtenoperation „**Deleted**“. Die Nachricht muss vom Zustellsystem endgültig gelöscht werden. Der Versender wird von der Löschung nicht informiert.

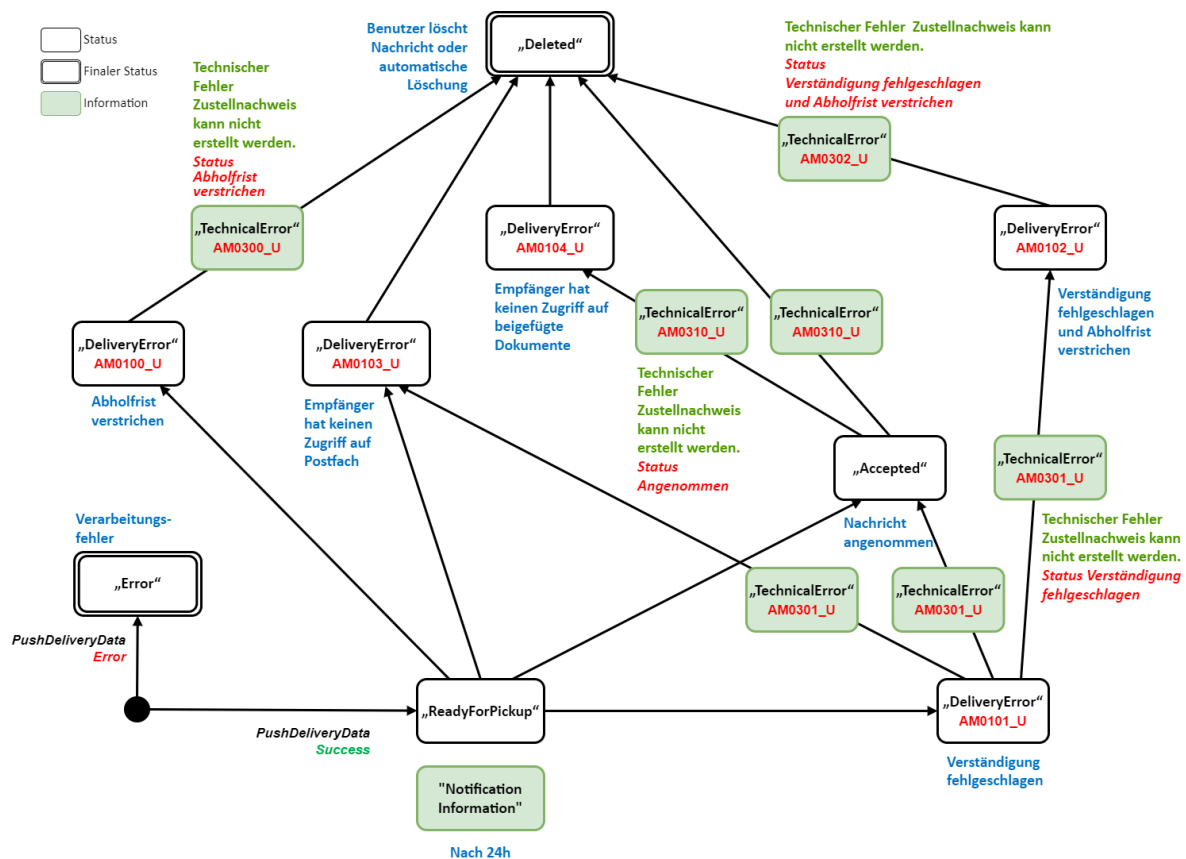
Der Zustellfehler „Empfänger hat keinen Zugriff auf Postfach“ (amod:Delivery-Error(AM0103\_U)) und der Zustellfehler „Empfänger hat keinen Zugriff auf beigefügte Dokumente“ (amod:Delivery-Error(AM0104\_U)) sind tatsächliche Zustellfehler, d.h. die Zustellung ist nicht bewirkt.

Bei diesen beiden Fehlern (amod:Delivery-Error(AM0103\_U) und amod:Delivery-Error(AM0104\_U)) dürfen bei nicht nachweislichen Zustellungen und Zusendungen die Elemente NotificationsPerformed und NotificationAddressList nicht befüllt werden.

Diese Verarbeitung trifft nur für Nachrichten zu, wenn keine ERV Weiterleitung aktiv ist.

#### 4.2.2 Nachrichtenoperationen, die bei der Zustellqualität „Zustellung bzw. Zusendung mit Zustellnachweis“ vom AMOD an den Zustelldienst übermittelt werden

Abbildung 9 – Zustandsübergangsdiagramm für Zustellungen bzw. Zusendungen mit Zustellnachweis



Wird das **PushDeliveryData** für eine nachweisliche Zustellung oder eine nachweisliche Sendung mit einem „**Success**“ vom AMOD beantwortet, dann konnte die Nachricht erfolgreich verarbeitet, die erste Verständigung erfolgreich für den Versand vorbereitet werden und die 14-tägige Abholfrist beginnt zu laufen. Die Nachricht befindet sich im Status „ReadyForPickup“.

Der Zeitpunkt, an dem die erste E-Mail-Verständigung erfolgreich versandt wurde, wird für die Berechnung des Zustellzeitpunkts gemäß [ZUSTG] herangezogen.<sup>3</sup>

<sup>3</sup> Der erfolgreiche Versand einer E-Mail bedeutet lediglich, dass die E-Mail erfolgreich an den Mail-Server des Empfängers übermittelt werden konnte. Die E-Mail ist zu diesem Zeitpunkt noch nicht im E-Mail-Postfach des Empfängers verfügbar, da die weitere Verarbeitung in der Regel asynchron erfolgt.

Tritt beim **PushDeliveryData** ein Fehler auf, antwortet das AMOD mit einem „**Error**“, die Zustellung gilt als „nicht durchgeführt“. In diesem Fall ist die Nachricht vom Zustellsystem zu löschen.

Wenn die Nachricht innerhalb der 14-tägigen Abholfrist angenommen wird, sendet das AMOD die Nachrichtenoperation „**Accepted**“. Es kann in speziellen Fällen vorkommen, dass noch keine erste Verständigung erfolgt ist, was jedoch kein Zustellhindernis darstellt. Sobald die Annahme erfolgt ist, werden keine Verständigungen mehr verschickt.

Wenn die 14-tägige Abholfrist verstrichen ist – ohne dass der Empfänger das Zustellstück angenommen hat – gilt die Zustellung dennoch als bewirkt und das AMOD sendet die Nachrichtenoperation „**DeliveryError (AM0100\_U)**“, um das Verstreichen der Abholfrist anzuzeigen.

Der Empfänger hat für weitere 8 Wochen die Möglichkeit die Nachricht im AMOD zu lesen.

Wenn der Zustellmangel „Verständigung fehlgeschlagen“ auftritt, d.h. die Verständigung des Empfängers per E-Mail fehlgeschlagen ist (Bounce Message), sendet das AMOD die Nachrichtenoperation „**DeliveryError (AM0101\_U)**“. Dies ist ein temporärer Zustand, da der Empfänger mittelbar Kenntnis über die Zustellung erhalten kann („Heilung“).

Wenn das Zustellhindernis „Verständigung fehlgeschlagen und Abholfrist verstrichen“ eintritt, gilt die Zustellung als „nicht bewirkt“ und das AMOD sendet die Nachrichtenoperation „**DeliveryError(AM0102\_U)**“.

Wenn der Zustellmangel „Verständigung fehlgeschlagen“ vorliegt und der Empfänger die Nachricht innerhalb der 14-tägigen Abholfrist abholt, gilt die Nachricht dennoch als angenommen und das AMOD sendet die Nachrichtenoperation „**Accepted**“.

Wenn nach der Übermittlung einer Nachricht der Empfänger bzw. der Vertreter keine Möglichkeit mehr hat, ins AMOD einzusteigen, da von einem zugrundeliegenden Register eine Auflösung bekannt gegeben wurde, sendet das AMOD die Nachrichtenoperation „**DeliveryError (AM0103\_U)**“ zusammen mit der finalen Nachrichtenoperation „**Deleted**“.

Wenn der Empfänger auf die beigefügten Dokumente einer bereits angenommenen Nachricht nicht zugreifen kann, da der verantwortliche Zustelldienst die Dokumente nicht korrekt bereitstellen kann, sendet das AMOD die Nachrichtenoperation „**DeliveryError (AM0104\_U)**“ zusammen mit der finalen Nachrichtenoperation „**Deleted**“.

Wenn die Zustellung durch den Benutzer manuell, oder nach Ablauf der Vorhaltdauer gemäß [ZUSTG] automatisiert gelöscht wird, sendet das AMOD die finale Nachrichtenoperation „**Deleted**“. Die Nachricht muss vom Zustellsystem endgültig gelöscht werden.

24 Stunden nach dem Eintreffen der Nachricht sendet das AMOD für nachweisliche Zustellungen bzw. Sendungen die Nachrichtenoperation „**NotificationInformation**“, falls noch keine andere Nachrichtenoperation ausgeführt wurde. Diese stellt keine Zustandsänderung im Zustellprozess dar, vielmehr wird das Zustellsystem über den Status bezüglich der Verständigung informiert. Betreffend folgende Situationen wird informiert:

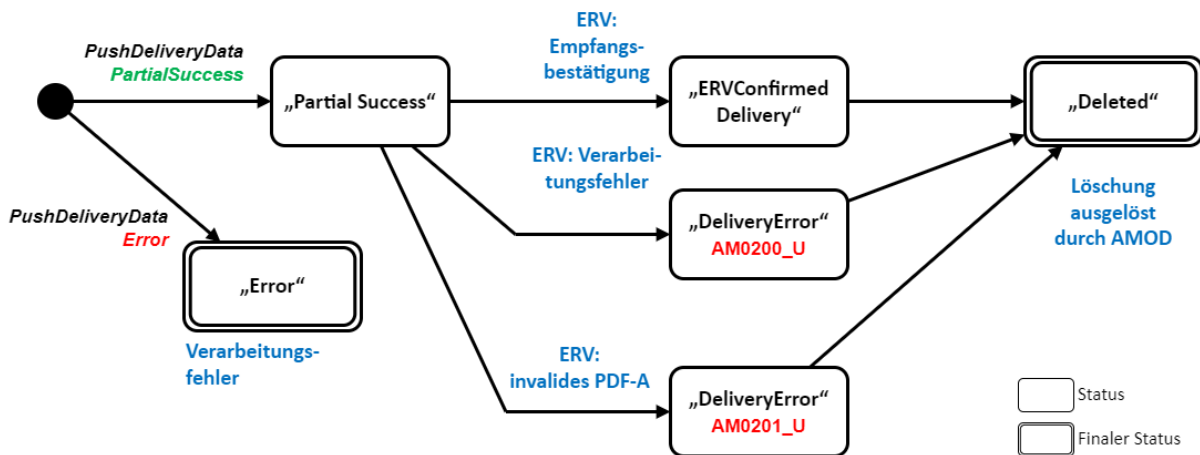
- Die erste Verständigung wurde erfolgreich an den E-Mail-Server übergeben. In diesem Fall sind die Elemente `msg:NotificationsPerformed`, `msg:RecipientNotification` und `msg:Timestamp` gesetzt.
- Die erste Verständigung ist fehlgeschlagen (Bounce Message erhalten). In diesem Fall sind die Elemente `msg:NotificationsPerformed`, `msg:RecipientNotification` und `msg:Timestamp` gesetzt und das `msg:FailedElement` ist auf `true` gesetzt.

Wenn es zu technischen Problemen kommt, besteht für das AMOD-Betriebsteam die Möglichkeit, diese im System zu erfassen und das AMOD sendet einen `amod:MessageOperationRequest` mit einem standardisierten Fehlercode und einer Fehlermeldung an den Zustelldienst.

Diese Verarbeitung trifft nur für Nachrichten zu, wenn keine ERV Weiterleitung aktiv ist.

#### 4.2.3 Nachrichtenoperationen, die bei der Weiterleitung in den ERV an das Zustellsystem übermittelt werden

Abbildung 10 – Zustandsübergangsdiagramm bei Weiterleitung in den ERV



Wenn die Nachricht in den ERV weitergeleitet werden soll, antwortet das AMOD dem Zustellsystem auf das **PushDeliveryData** unmittelbar mit einem „**PartialSuccess**“ ohne Zustellzeitpunkt, jedoch mit dem Hinweis, dass die Nachricht in den ERV weitergeleitet wird. Zu diesem Zeitpunkt ist die Übermittlung noch nicht abgeschlossen.

Wenn beim **PushDeliveryData** bereits im AMOD ein Fehler auftritt, antwortet das AMOD direkt mit einem „**Error**“. In diesem Fall ist die Nachricht vom Zustellsystem zu löschen.

Wenn der ERV asynchron an das AMOD zurückmeldet, dass die Nachricht im Verfügungsbereich des Empfängers eingelangt ist, gilt die Nachricht als zugestellt und das AMOD sendet die Nachrichtenoperation „**ERVConfirmedDelivery**“ an das Zustellsystem.

Zustellsysteme haben dem Versender mittels `msg:DeliveryRequestStatus` eine Übergabebestätigung zu retournieren.

Im Falle einer nachweislichen Zustellung müssen Zustelldienste eine Zustellbenachrichtigung (`msg:DeliveryNotification`) an den Versender übermitteln.

Zeitgleich mit der Nachrichtenoperation „**ERVConfirmedDelivery**“ wird dem Zustellsystem vom AMOD die finale Nachrichtenoperation „**Delete**“ übermittelt. Hiermit wird das Zustellsystem explizit vom AMOD zur endgültigen Löschung der Nachricht aufgefordert.

Die Löschung der Nachricht hat das Zustellsystem im Anschluss an die erfolgreiche Verarbeitung der Nachrichtenoperation „**ERVConfirmedDelivery**“ durchzuführen.

##### Ausnahmebehandlung

Tritt bei der Verarbeitung der Nachricht im ERV ein Fehler auf, wird dieser asynchron an das Zustellsystem mittels Nachrichtenoperation „**DeliveryError**“ zurückgemeldet. Eine fehlgeschlagene Übergabe bedeutet, dass die Zustellung nicht stattgefunden hat und der Versender auf den Fehler reagieren muss.

Hierbei werden zwei Fehlercodes unterscheiden:

- **AM0200\_U**: Allgemeiner ERV Verarbeitungsfehler
- **AM0201\_U**: Zumindest eines der übermittelten PDF-Dokumente entspricht nicht dem PDF/A-Standard

Zeitgleich mit der Nachrichtenoperation „**DeliveryError**“ wird dem Zustellsystem vom AMOD die finale Nachrichtenoperation „**Delete**“ übermittelt. Hiermit wird das Zustellsystem explizit vom AMOD zur endgültigen Löschung der Nachricht aufgefordert.

### 4.3 Nachrichtenoperationen Bindings

Dieser Abschnitt definiert die Schnittstelle(n) für die Übertragung von Informationen zu Nachrichtenoperationen vom Anzeigemodul zum für ein Zustellstück zuständigen Zustellsystem. Grundsätzlich können beliebige Schnittstellenformate zum Einsatz kommen. Im Sinne der Flexibilität, d.h. wenn bspw. neue Nachrichtenoperationen notwendig werden, sowie einer nachhaltigen zukunftsfähigen Schnittstellendefinition, sollen neue Technologien relativ einfach für die Umsetzung dieser Schnittstelle eingesetzt werden können. Folgende Technologien werden im Rahmen dieser Spezifikation aktuell unterstützt:

- Extensible Markup Language (XML)

Jede Technologiespezifikation der Nachrichtenoperationen-Schnittstelle ist unterteilt in die folgenden drei Abschnitte:

- **Authentifizierung** – definiert die beidseitige Authentifizierung zwischen Anzeigemodul und Zustellsystem
- **Format** – legt das technische Format fest, in welchem Nachrichtenoperationen definiert werden
- **Binding** – definiert das Protokoll, über welches die Nachrichtenoperationen im entsprechenden Format nach erfolgreicher Authentifizierung übertragen werden.

#### 4.3.1 XML Format und Binding

Dieser Abschnitt beschreibt Anfragen (Request) bzw. Antworten (Response) für die Übertragung von Nachrichtenoperationen im XML Format.

##### 4.3.1.1 Authentifizierung

Die Authentifizierung des Anzeigemoduls gegenüber dem Anwendungsportal des Zustellsystems MUSS gemäß den Vorgaben aus Abschnitt 2 erfolgen.

Wenn die Authentifizierung über Portalverbundtechnologie (vgl. Kapitel 2.1 Teilnehmer des Portalverbunds) erfolgt, MUSS vom Anzeigemodul folgende Rolle übermittelt werden:

- ZUSE-DISPLAY-SERVICE

Beispiel für die zu setzenden PVP 2.1 Http-Header:

```
POST /abc.qv.at/anwendung2/xyz HTTP/1.1
Host:zustellsystem.at
User-Agent: .JNET 1.1
X-PVP-VERSION: 2.1
X-PVP-BINDING: http
X-PVP-PARTICIPANT-ID: <AMOD>
X-PVP-USERID: <USERID AMOD>
X-PVP-PRINCIPALNAME: <PRINCIPAL NAME AMOD>
X-PVP-SECCLASS: 2
X-PVP-ROLES: ZUSE-DISPLAY-SERVICE
Content-Type: text/xml
Content-Length: 788
```

Wenn die Authentifizierung mittels Zertifikats (vgl. Kapitel 2.2 Nicht Teilnehmer des Portalverbunds) erfolgt, MUSS vom Anzeigemodul nur das Zertifikat übermittelt werden und es DÜRFEN keine PVP 2.1 Http-Header übermittelt werden.

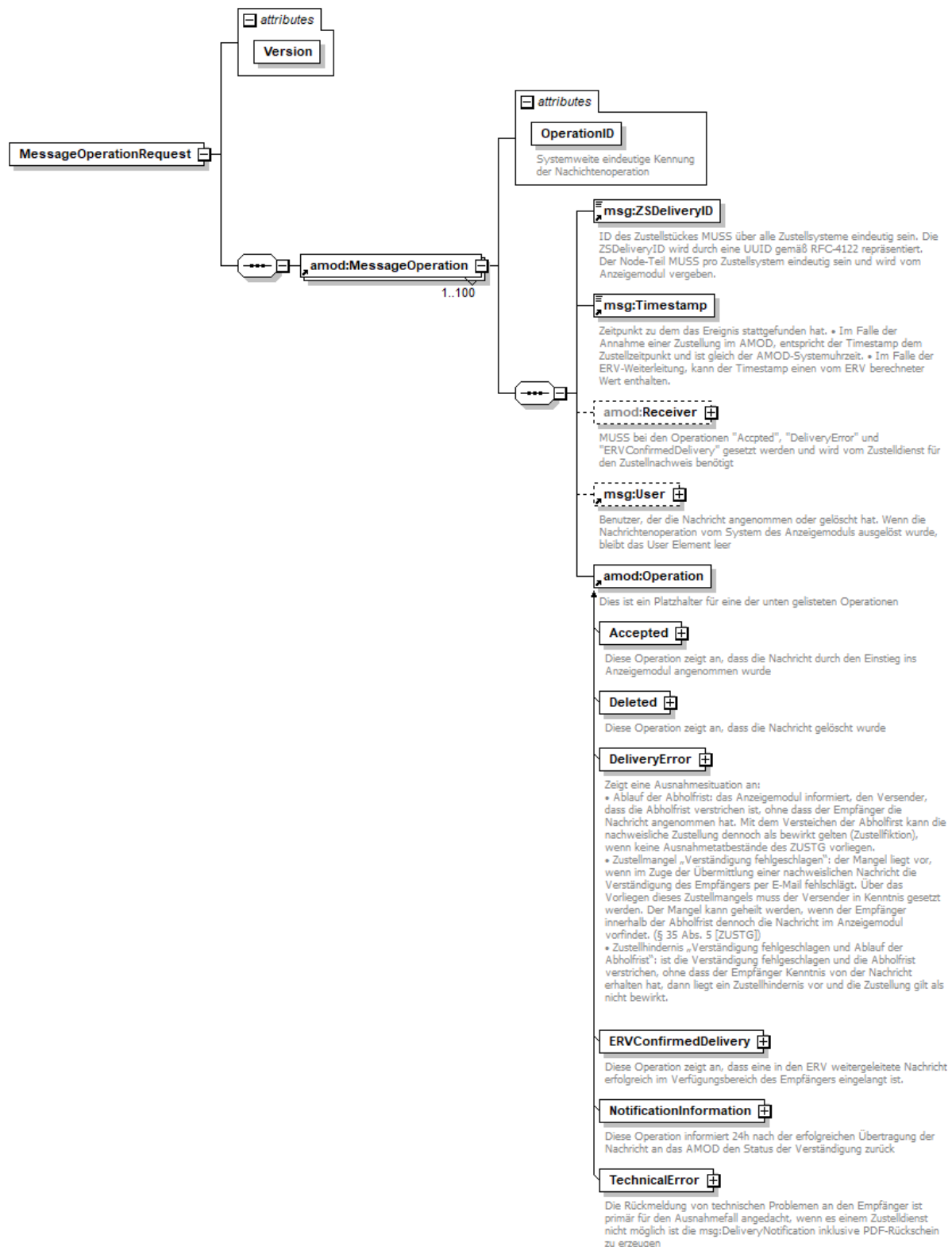
##### 4.3.1.2 Format

###### 4.3.1.2.1 Request



Vom Anzeigemodul an das Zustellsystem zu übertragende Nachrichtenoperationen werden über das `amod:MessageOperationRequest` Element gekapselt (siehe Abbildung 11).

**Abbildung 11 – Struktur des `amod:MessageOperationRequest` Elements**



Pro Request können bis zu 100 Nachrichtenoperationen (Element `amod:MessageOperation`) übermittelt werden. Dies ermöglicht die Übertragung von Nachrichtenoperationen im Bulk.

Das Anzeigemodul MUSS für jede einzelne `amod:MessageOperation` eine systemweite eindeutige `OperationID` erzeugen.

Diese Anforderung ist notwendig, damit sowohl das Anzeigemodul als auch die Zustellsysteme rasch erkennen können, ob eine bestimmte `amod:MessageOperation` bereits korrekt verarbeitet wurde.

Die `OperationID` hat folgenden Aufbau:

- Format: „YYYYMMDDTHH:MI:SS.NANOS-RANDOM\_NR“, 37-stellig
- Datum
  - ◆ Jahr, 4-stellig
  - ◆ Monat, 2-stellig, führende Nullen
  - ◆ Tag, 2-stellig, führende Nullen
- Zeit, Zeitzone=Mitteleuropäische Zeit (CET/MEZ), implizit
  - ◆ „T“
  - ◆ Stunde, 2-stellig, führende Nullen,
  - ◆ Minuten, 2-stellig, führende Nullen
  - ◆ Sekunden, 2-stellig, führende Nullen
  - ◆ Nanosekunden, 9-stellig, führende Nullen
- Bindestrich „-“
- Zufallszahl, 9-stellig, numerisch, führende Nullen
- Beispiel: „20180811T13:42:59.123456789-563985412“

Die `msg:ZSDeliveryID` gibt die systemweit eindeutige Zustell-ID gemäß Definition in Abschnitt 3.1.2.1 an. Details zur Struktur und Erzeugung der UUID sind der zu [ZUSEMSG] entnehmen.

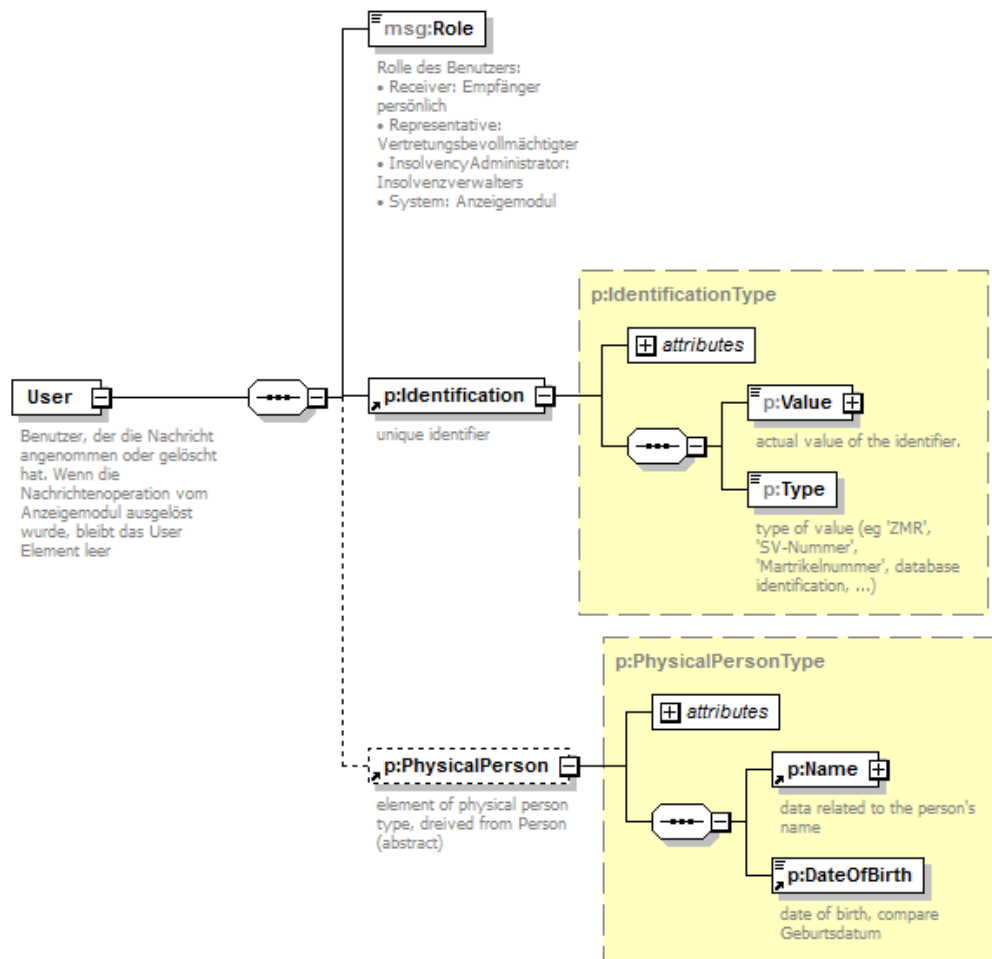
Der `msg:Timestamp` entspricht dem Zeitpunkt, zu dem das fachliche Ereignis eingetreten ist, wie beispielsweise dem Annahmezeitpunkt. Im Falle einer ERV-Weiterleitung enthält der `msg:Timestamp` das vom ERV berechnete Zustelldatum mit der Uhrzeit „00:00:00“.

In Nachrichtenoperationen (`amod:MessageOperation`) dürfen zur eindeutigen Identifikation von natürlichen Personen ausschließlich für das Anzeigemodul verschlüsselte bereichsspezifische Personenkennzeichen des Bereichs „Zustellung“ verwendet werden. Der zugehörige Identifikationstyp ist gleich „**urn:publicid:gv.at:ecdid+ZUSEAMOD+ZU**“.

Das `msg:Receiver` Element MUSS ausgefüllt werden, wenn die Operation vom Typ „Accepted“, „DeliveryError“ oder „ERVConfrimedDelivery“ ist. Bei diesen Operationen benötigt der Zustelldienst die vollständigen Personendaten des Empfängers für die Erstellung des Zustellnachweises.

Im `msg:User` Element werden die Personendaten jenes Benutzers übermittelt, der die Nachrichtenoperation durchgeführt hat. Das `msg:User` Element darf entfallen, wenn die Operation automatisiert vom Anzeigemodul ausgelöst wurde. Zur eindeutigen Identifikation des Benutzers wird das verschlüsselte bPK gemäß dem Identifikationstyp „**urn:publicid:gv.at:ecdid+ZUSEAMOD+ZU**“ angegeben. Nur im Falle von Vertretungsbevollmächtigten einer Behörde ist auch die PVP-Benutzerkennung als eindeutiger Identifikator mit dem Typ „**urn:pvp-userid**“ zulässig.

Abbildung 12 – Struktur des msg:User Elements



Der Benutzer kann eine der folgenden Rollen innehaben, die im msg:Role Element übermittelt wird:

- **Receiver** – Der Empfänger persönlich
- **Representative** – Ein Vertretungsbevollmächtigter des Empfängers
- **InsolvencyAdministrator** – Im Falle einer Postsperre (vgl. [ZUSEORG]) wird der Insolvenzverwalter zum Empfänger

Der Benutzer MUSS immer eine natürliche Person sein, welche eindeutig über ihr vbPK oder im Falle von Behördenmitarbeitern über ihre userid identifiziert werden können MUSS.

In welcher Form das vbPK vom Anzeigemodul zurückgegeben wird, hängt davon ab, ob beim Push der Metadaten im Request das Element am XPath

```
/amod:PushDeliveryDataRequest/amod:Sender/p:CorporateBody/p:Target
```

gesetzt wurde (Definition siehe Abschnitt 3.1.2.10).

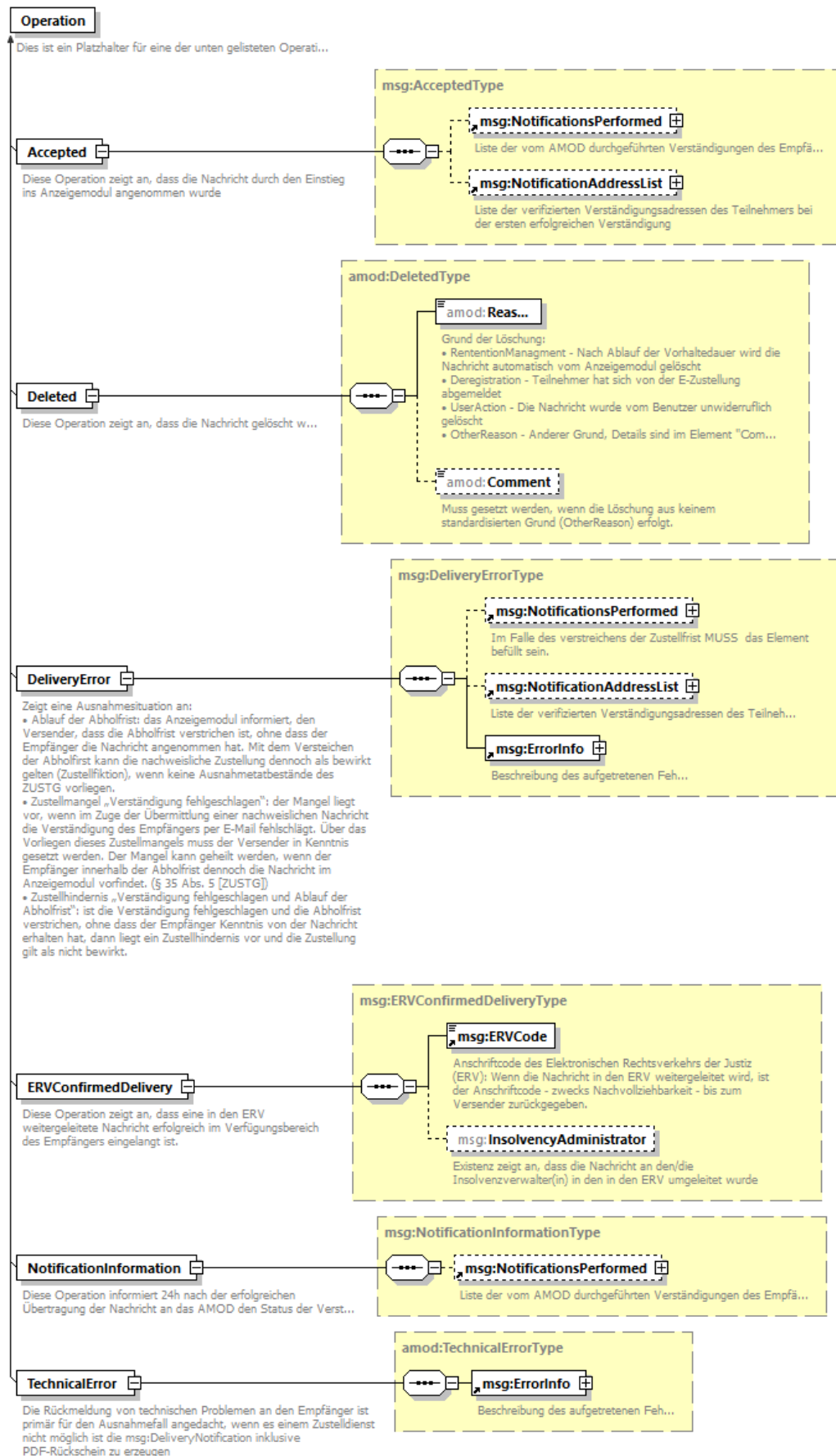
- Wurde das msg:Target Element gesetzt, MUSS es den Bereich und das VKZ - codiert als Identifikationstyp - der versendende Behörde enthalten, welche die gesetzliche Verantwortung für die Aufbewahrung des Zustellnachweis hat. Wenn das Target gesetzt wurde, wird im Rahmen zukünftiger technischer Möglichkeiten das bPK-ZU jenes Benutzers vom AMOD umgeschlüsselt, welcher die Nachricht angenommen hat.

- Wurde das `Target` Element NICHT gesetzt, wird das für das VKZ ZUSEAMOD verschlüsselte bPK-ZU zurückgegeben:  
**urn:publicid:gv.at:ecdid+ZUSEAMOD+ZU**

Im `PhysicalPerson` Element können optional der Name und das Geburtsdatum des Benutzers mitgegeben werden.

Das `Operation` Element gibt die exakte Nachrichtenoperation mit allfälligen weiteren Parametern an.

Abbildung 13 – Struktur des amod:Operation Elements



Gemäß Abschnitt 4.1 sind folgende `amod:Operation` Elemente definiert:

- Nachricht angenommen (Element `amod:Accepted`). Sub-Elemente sind:
  - Das Element `msg:NotificationsPerformed` enthält die Liste der Verständigungszeitpunkte.
  - Das Element `msg:NotificationsAddressList` enthält die Liste der elektronischen Adressen, an die das Anzeigemodul die Verständigung über die Hinterlegung eines Zustellstücks gesandt hat.
    - E-Mail-Adressen (`msg:InternetAddress`) werden als „ungültig“ markiert (`Invalid="true"`), wenn der sendende E-Mail-Server entweder nicht erreichbar war oder mit einer Bounce-Message geantwortet hat.
- Ausnahmesituation „Abholfrist verstrichen“, „Zustellmangel“ oder „Zustellhindernis“ (Element `amod:DeliveryError`). Sub-Elemente sind:
  - `msg:ErrorInfo` mit den Sub-Elementen `msg:Code` und `msg:Text` beschreiben die Ausnahmesituation. Die möglichen Codes sind in Tabelle 3 (bis AM0201\_U) gelistet.
  - Optional enthält Element `msg:NotificationsPerformed` die Liste der Verständigungszeitpunkte.
  - Das Element `msg:NotificationsAddressList` enthält die Liste der elektronischen Adressen, an die das Anzeigemodul die Verständigung über die Hinterlegung eines Zustellstücks gesandt hat.
    - E-Mail-Adressen (`msg:InternetAddress`) werden als „ungültig“ markiert (`Invalid="true"`), wenn der sendende E-Mail-Server entweder nicht erreichbar war oder mit einer Bounce-Message geantwortet hat.
- Nachricht löschen (Element `amod:Delete`)
  - Im `amod:Reason` Element muss einer der vier standardisierten Gründe angegeben werden
    - **RetentionManagement** - Nach Ablauf der Vorhaltdauer (Details siehe [ZUSEORG]) wird die Nachricht automatisch vom Anzeigemodul gelöscht.
    - **Deregistration** - Teilnehmer hat sich von der E-Zustellung abgemeldet
    - **UserAction** - Die Nachricht wurde vom Benutzer unwiderruflich gelöscht
    - **OtherReason** - Anderer Grund, in diesem Fall MÜSSEN der Löschrund im `amod:Comment` Element angegeben werden.
- Weiterleitung in den ERV bestätigt (Element `amod:ERVConfirmedDelivery`)
  - Das `msg:ERVCode` Element enthält den Anschriftcode an den die Nachricht im ERV weitergeleitet wurde
  - Die Existenz des `msg:InsolvencyAdministrator` Elements zeigt an, dass die Zustellung in den ERV an den/die Insolvenzverwalter(in) umgeleitet wurde
- Der Verständigungsversuch (Element `amod:NotificationInformation`) wird bei nicht nachweislichen und nachweislichen Zustellungen und Zusendungen zurückgemeldet

- Das Element `msg:NotificationsPerformed` mit der Liste der Verständigungszeitpunkte enthält den Timestamp des Verständigungsversuchs und die Information, ob die Verständigung erfolgreich war.
- Der technische Fehler (Element `amod:TechnicalError`) wird bei nachweislichen Zustellungen und Zusendungen zurückgemeldet
  - Das Element `msg:ErrorInfo` mit den Sub-Elementen `msg:Code` und `msg:Text` beschreibt den technischen Fehler. Die möglichen Codes sind in Tabelle 3 (ab AM0300\_U) gelistet.

Tabelle 3 – Codes, die das Anzeigemodul zurückmeldet

Code	Meldung	Beschreibung
AM0100_U	Pick up time exceeded	Die Abholfrist ist verstrichen
AM0101_U	Notification failed	Die Verständigung des Empfängers ist fehlgeschlagen
AM0102_U	Notification failed and pick up time exceeded	Die Verständigung des Empfängers ist fehlgeschlagen und die Abholfrist ist verstrichen
AM0103_U	Recipient does not have access to their mailbox	Empfänger hat keinen Zugriff auf Postfach. Die Zustellung wurde „nicht bewirkt“
AM0104_U	Recipient does not have access to the attached documents	Der Empfänger hat keinen Zugriff auf beigefügte Dokumente. Die Zustellung wurde „nicht bewirkt“
AM0200_U	ERV forwarding to Code %1: General Service Error - %2 (%3)	Die Weiterleitung in den ERV wurde mit einem allgemeinen Servicefehler quittiert %1: ERV-Anschriftcode %2: Originale Fehlermeldung des ERV %3: Originaler Fehlercode des ERV
AM0201_U	ERV forwarding to Code %1: PDF file must be conform to the PDF/A standard	Zumindest eines der PDF-Attachments entspricht nicht dem PDF/A Standard %1: ERV-Anschriftcode
AM0300_U	Due to a technical issue, the proof of delivery could not be created. The delivery is in the status "Pick up time exceeded"	Aufgrund technischer Probleme konnte der Zustellnachweis nicht erstellt werden. Die Zustellung befindet sich im Status „Abholfrist verstrichen“
AM0301_U	Due to a technical issue, the proof of delivery could not be created. The delivery is in the status "Notification failed"	Aufgrund technischer Probleme konnte der Zustellnachweis nicht erstellt werden. Die Zustellung befindet sich im Status „Verständigung fehlgeschlagen“

Code	Meldung	Beschreibung
AM0302_U	Due to technical problems, the proof of delivery could not be created. The delivery is in the status "Notification failed and pick up time exceeded"	Aufgrund technischer Probleme konnte der Zustellnachweis nicht erstellt werden.  Die Zustellung befindet sich im Status „Verständigung fehlgeschlagen und Abholfrist verstrichen“
AM0310_U	Due to technical problems, the proof of delivery could not be created. The delivery is in the status "Accepted"	Aufgrund technischer Probleme konnte der Zustellnachweis nicht erstellt werden.  Die Zustellung befindet sich im Status „Angenommen“

### Beispiel einer Nachrichtenoperation „Angenommen“:

```
<?xml version="1.0" encoding="UTF-8"?>
<amod:MessageOperationRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:p="http://reference.e-government.gv.at/namespace/persondata/phase2/20181206#"
  xmlns:msg="http://reference.e-government.gv.at/namespace/zustellung
/msg/phase2/20181206#"
  xmlns:amod="http://reference.e-government.gv.at/namespace/zustellung
/amod/phase2/20181206#"
  Version="2.4.0-003">
  <amod:MessageOperation OperationID="20180811T13:42:59.123456789-563985412">
    <msg:ZSDeliveryID>a95c530a-7af5-3492-a744-99e70578d150</msg:ZSDeliveryID>
    <msg:Timestamp>2001-12-21T09:30:47Z</msg:Timestamp>
    <amod:Receiver>
      <p:Identification>
        <p:Value>
NEK/9Z04cd8fc7006b1e58ee40790448cd3fb4ebb8f80c1187f0567e376e8627cb96f66ef32cd8248b6
94bba632085f2bce84e587053clefe899ec1bb460acf5cf2
        </p:Value>
        <p:Type>urn:publicid:gv.at:ecdid+ZUSEAMOD+ZU</p:Type>
      </p:Identification>
      <p:PhysicalPerson>
        <p:Name>
          <p:GivenName>Max</p:GivenName>
          <p:FamilyName>Mustermann</p:FamilyName>
        </p:Name>
        <p:DateOfBirth>1940-01-01</p:DateOfBirth>
      </p:PhysicalPerson>
    </amod:Receiver>
    <msg:User>
      <msg:Role>Receiver</msg:Role>
      <p:Identification>
        <p:Value>
NEK/9Z04cd8fc7006b1e58ee40790448cd3fb4ebb8f80c1187f0567e376e8627cb96f66ef32cd8248b6
94bba632085f2bce84e587053clefe899ec1bb460acf5cf2
        </p:Value>
        <p:Type>urn:publicid:gv.at:ecdid+ZUSEAMOD+ZU</p:Type>
      </p:Identification>
      <msg:TargetIdentification>
        <p:Value>
16904cd8fc7006b1e58ee40790448cd3fb4ebb8f80c1187f0567e376e8627cb96f66ef32cd8248b694b
ba632085f2bce84e587053clefe899ec1bb460acf5cf2
        </p:Value>
        <p:Type>urn:publicid:gv.at:ecdid+BMF+SA</p:Type>
      </msg:TargetIdentification>
    </p:PhysicalPerson>
    <p:Name>
      <p:GivenName>Max</p:GivenName>
      <p:FamilyName>Mustermann</p:FamilyName>
    </p:Name>
  </amod:MessageOperation>
</amod:MessageOperationRequest>
```



```

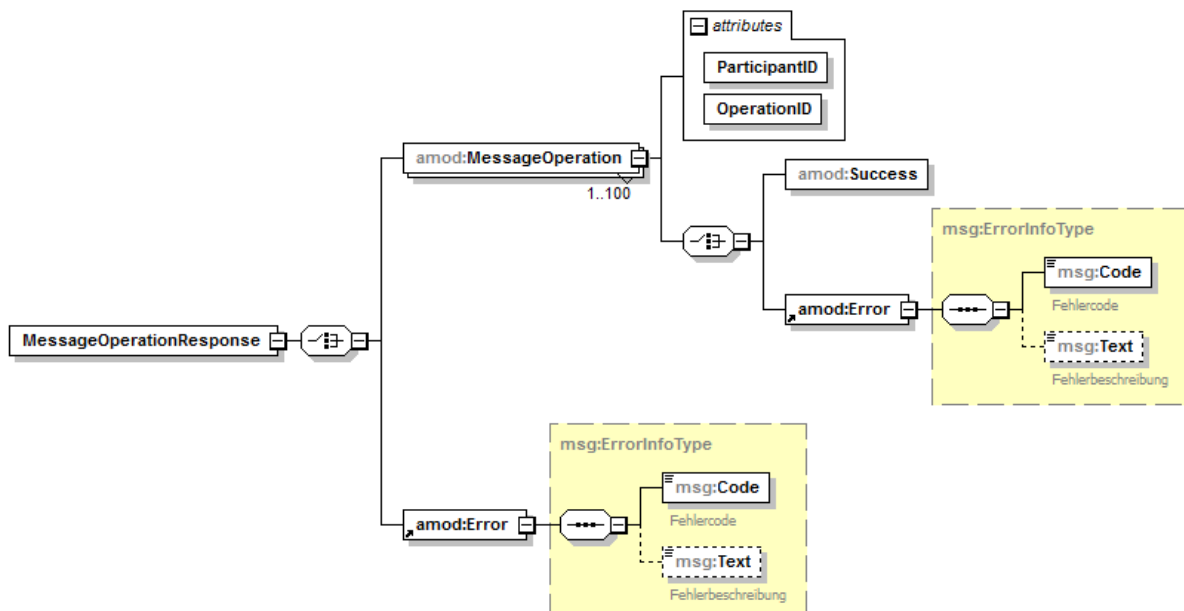
    </p:Name>
    <p:DateOfBirth>1940-01-01</p:DateOfBirth>
  </p:PhysicalPerson>
</msg:User>
<amod:Accepted>
  <msg:NotificationsPerformed>
    <msg:RecipientNotification>
      <msg:Timestamp>2001-12-17T09:30:47Z</msg:Timestamp>
    </msg:RecipientNotification>
    <msg:RecipientNotification>
      <msg:Timestamp>2001-12-19T09:30:47Z</msg:Timestamp>
    </msg:RecipientNotification>
  </msg:NotificationsPerformed>
  <msg:NotificationAddressList>
    <msg:InternetAddress Id="ID1">
      <p:Address>max.mustermann@office.at</p:Address>
    </msg:InternetAddress>
    <msg:InternetAddress Id="ID2">
      <p:Address>max.mustermann@provider.at</p:Address>
    </msg:InternetAddress>
    <msg:InternetAddress Id="ID3" Invalid="true">
      <p:Address>m.mustermann@unbekannt.at</p:Address>
    </msg:InternetAddress>
  </msg:NotificationAddressList>
</amod:Accepted>
</amod:MessageOperation>
</amod:MessageOperationRequest>

```

#### 4.3.1.2.2 Response

Die Antwort auf einen `amod:MessageOperationRequest` ist über das `amod:MessageOperationResponse` Element definiert (siehe Abbildung 14).

Abbildung 14 – Struktur des `amod:MessageOperationResponse` Elements



Für jeden `amod:MessageOperation` Eintrag des Requests gibt es einen entsprechenden `amod:MessageOperation` Eintrag in der Response. Die Reihenfolge der Einträge in der Response muss der Reihenfolge im Request entsprechen. Zur Sicherheit wird auch in der Response jeder Eintrag über ein `OperationID` Attribut gekennzeichnet, das dem Wert des Attributs im Request entsprechen muss.

Konnte eine Operation vom Zustellsystem erfolgreich durchgeführt werden, so wird dies vom Zustellsystem mit einem leeren `amod:Success` Element quittiert. Im Fehlerfall werden `msg:Code` und `msg:Text` zurückgeliefert, die das Problem bei der Durchführung der jeweiligen Nachrichtenoperation beschreiben. Die anwendbaren Fehler-Codes sind in Tabelle 4 angeführt.

**Tabelle 4 – Fehlermeldungen für Message Operations, die das Zustellsystem zurückliefert**

Code	Error-Message	Beschreibung
ZS0001_U	Unknown ZSDeliveryID	Operation wird auf eine Nachricht angewandt, die dem Zustellsystem nicht bekannt ist.
ZS0002_U	Timestamp missing	Zeitpunkt der Durchführung der Benutzeraktion muss mitgegeben werden.
ZS0400_U	Bad Request	Grundsätzlich müssen sich die Zustellsysteme bei der Kommunikation mit dem AMOD tolerant verhalten, z.B. wenn dieselbe Message Operation mehrmals gesendet wird. Wenn jedoch die Message Operation eindeutig im Widerspruch zur aktuellen Verarbeitung der Nachricht steht, MUSS dieser Fehler angezeigt werden.
ZS0403_U	Webservice operation is not permitted	Webserviceoperation ist nicht zulässig.
ZS0404_U	Operation is not supported	Diese Nachrichtenoperation wird vom Anzeigemodul nicht unterstützt.
ZS0500_R	Internal Server Error	

#### 4.3.1.3 Binding

Für den Datenaustausch MUSS das Netzwerkprotokoll SOAP in der Version 1.2 über das HTTP Binding in [SOAP12] verwendet werden.

Sämtliche Kommunikation muss gesichert gemäß den Anforderungen in Abschnitt 3.2.1.1 erfolgen.

Die entsprechende WSDL-Beschreibung ist als gesonderte Datei der Spezifikation beigelegt.

- zuse2amod\_p2.wsdl
- amod2zuse\_p2.wsdl

## 5 Übertragung von Attachments

### 5.1 Authentifizierung

Die Authentifizierung MUSS gemäß den Vorgaben aus Abschnitt 4.3.1.1 erfolgen.

### 5.2 Verschlüsselung von Attachments

#### 5.2.1 Symmetrischer Schlüssel

Für jeden Anhang MUSS ein eigener symmetrischer Schlüssel erstellt werden.

1. Schlüssel dürfen niemals wiederverwendet werden. Schlüssel sind mit sicheren Zufallsgeneratoren, die dem Stand der Technik entsprechen, zu erstellen.
2. Als Algorithmus für den Schlüssel MUSS AES mit einer Schlüssellänge von 256 Bit [AES] verwendet werden.
3. Als Betriebsmodus MUSS der Counter Mode [AES] verwendet werden
4. Ein Padding DARF NICHT verwendet werden

Daraus folgt: es ist die Cipher `AES/CTR/NoPadding` zu verwenden.

#### 5.2.2 Verschlüsselung des symmetrischen Schlüssels

Nach der erfolgreichen Verschlüsselung und Persistierung des Attachments MUSS der symmetrische Schlüssel selbst mit dem asymmetrischen Public Key des AMOD verschlüsselt werden.

Hierzu muss die Cipher `RSA/ECB/OAEPWithSHA-256AndMGF1Padding` verwendet werden.

Der für das AMOD verschlüsselte symmetrische Schlüssel darf persistiert werden. Der unverschlüsselte symmetrische Schlüssel MUSS verworfen werden.

Daraus folgt: das Zustellsystem hat nach Abschluss der Verarbeitung keine Möglichkeit mehr auf den Klartext bzw. Inhalt der Nachricht zuzugreifen.

#### 5.2.3 Subject-Key-Identifier

Das AMOD-Zertifikat, das den asymmetrischen öffentlichen Schlüssel enthält, wird regelmäßig erneuert. Damit der Zertifikatswechsel – auch "Key-Rollover" genannt – reibungslos verläuft, überschneiden sich die Gültigkeitszeiträume des alten und des neuen Zertifikats.

Um eindeutig identifizieren zu können, welches Zertifikat bzw. welcher Schlüssel verwendet wurde, MUSS das `SubjectKeyIdentifier`-Attribut in den Metadaten des Attachments (XPath: `amod:Attachment/amod:EncryptedKey/@SubjectKeyIdentifier`) auf den Wert des ASN.1-Metadatenfeldes des X.509 v3 Zertifikats mit der OID 2.5.29.14 gemäß [RFC5280] gesetzt werden. Der Binärwert ist ohne den ASN.1-Header in hexadezimaler Darstellung auszugeben.

Falls der Subject-Key-Identifier dem AMOD nicht bekannt ist, wird der Validierungsfehler `AM3018_U` retourniert.

### 5.3 Attachment Übertragung

Um Attachments beliebiger Größe verarbeiten zu können, muss der HTTPS-Server des Zustellsystems Range-Requests gemäß [RFC7233] unterstützen.

Beim Download durch das AMOD werden die Attachments stets blockweise mittels Range-Requests angefordert. Dieses Feature wird von jedem Standard-Webserver unterstützt, der

das „Hypertext Transfer Protocol in der Version 1.1 (HTTP/1.1)“ implementiert hat. Ein Beispiel dazu ist im Anhang unter 11.2 angeführt.

### 5.3.1 Request

Die Anforderung zur Übermittlung eines Attachments an das Anzeigemodul erfolgt über eine HTTP GET Anfragemethode [HTTP11] am Zustellsystem. Es sind dabei HTTP 1.1 oder HTTP/2 als Übertragungsprotokolle zulässig. Es ist jene URL für den Aufruf zu verwenden, die am Anzeigemodul für das jeweilige Zustellsystem in der Konfiguration hinterlegt ist. Dem Zustellsystem MÜSSEN dabei die Argumente in Tabelle 5 übergeben werden. Die Angabe weiterer Argumente ist nicht zulässig.

Gemäß [RFC3986] dürfen die Argumente in der URL nicht case-sensitiv sein, da Windows-Server NICHT zwischen Groß- und Kleinschreibung unterscheiden.

**Tabelle 5 – Verpflichtende HTTP Argumente für Abholung eines Attachments**

Argument	Beschreibung
zs_delivery_id	Siehe Definition in Abschnitt 3.1.2.1
identifier_type	Siehe Definition in Abschnitt 3.1.2.24
identifier_value	Siehe Definition in Abschnitt 3.1.2.25
attachment_id	Siehe Definition in Abschnitt 3.1.2.63

Im Request MÜSSEN folgende Header aus Tabelle 6 übergeben werden.

**Tabelle 6 – Verpflichtende HTTP Request Header für Abholung eines Attachments**

Header	Beschreibung
Host	Angabe des DNS Namens des Zustellsystems (dient zur Unterscheidung beim Betrieb von mehreren Diensten in einer virtuellen Host Umgebung)

Die Angabe folgender Header ist optional, MÜSSEN aber gegebenenfalls vom Zustellsystem unterstützt werden: Connection, Date, Range, TE, Transfer-Encoding, Upgrade, User-Agent

Weitere Header werden ignoriert.

Beispiel einer Anfrage:

```
GET /attachment?delivery_id=123456&attachment_id=ATT-123&identifier=ABC&identifier_type=bPK HTTP/1.1
Host: MeinZustellsystem.at
```

### 5.3.2 Response

#### 5.3.2.1 Erfolgsfall

Konnte das Attachment mit der angegebenen Zustell-ID bzw. Attachment-ID erfolgreich in der lokalen Datenbank des Zustellsystems gefunden und dem angegebenen Empfänger zugeordnet werden, so ist vom Zustellsystem eine HTTP GET Response mit dem Code 200

zu erzeugen und das Attachment im Body zu retournieren. Wie das Attachment retourniert wird (binär, komprimiert, etc.), hängt auch von der in HTTP Headern angegebenen Übertragungsmethode ab.

Die Attachments MÜSSEN für das Anzeigemodul verschlüsselt sein. Details zur Verschlüsselung siehe Abschnitt 5.2 *Verschlüsselung von Attachments*.

In der Response MÜSSEN vom Zustellsystem folgende Header aus Tabelle 7 generiert und in der HTTP Response mitübergaben werden.

**Tabelle 7 – Verpflichtende HTTP Response Header für Abholung eines Attachments im Erfolgsfall**

Header	Beschreibung
ZSDeliveryID	Siehe Definition in Abschnitt 3.1.2.1
Date	Siehe RFC 2616 [HTTP11] bzw. [RFC7233]
Content-Type	Siehe RFC 2616 [HTTP11] bzw. [RFC7233]
ChecksumAlgorithm	Siehe Definition in Abschnitt 3.1.2.69
ChecksumValue	Siehe Definition in Abschnitt 3.1.2.70

Die Angabe folgender Header ist optional: Connection, Content-Encoding, Content-Length, Content-Range, Server, Transfer-Encoding

Weitere Header werden nicht ausgewertet bzw. ignoriert.

Beispiel einer erfolgreichen Response:

```
HTTP/1.1 200 OK
ZSDeliveryID: 123456
Date: Thu, 26 Apr 2018 07:45:55 GMT
Server: Apache/1.2.3 (Unix)
Content-Length: 567890
ChecksumAlgorithm: SHA256
ChecksumValue: ABCDEF=
Connection: close
Content-Type: application/pdf
(Inhalt von Bescheid.pdf)
```

### 5.3.2.2 Fehlerfall

Tritt ein Fehler beim Abruf eines Attachments auf, bspw., weil dieses nicht existiert oder einem anderen Empfänger zugeordnet ist, so ist die Anfragen mit einem HTTP 400 (Bad Request) Fehler zu quittieren. Der Content-Type Header ist dabei auf text/plain zu setzen und der Fehlercode samt Beschreibungstext ist als Body getrennt durch einen Strichpunkt zu übermitteln.

In der Response MÜSSEN vom Zustellsystem folgende Header aus Tabelle 8 generiert und in der HTTP Response mitübergaben werden.

**Tabelle 8 – Verpflichtende HTTP Response Header für Abholung eines Attachments im Fehlerfall**

Header	Beschreibung
ZSDeliveryID	Siehe Definition in Abschnitt 3.1.2.1
Date	Siehe RFC 2616 [HTTP11] bzw. [RFC7233]
Content-Type	Siehe RFC 2616 [HTTP11] bzw. [RFC7233]

Die Angabe folgender Header ist optional, MÜSSEN aber gegebenenfalls vom Zustellsystem unterstützt werden: Connection, Content-Encoding, Content-Length, Content-Range, Server, Transfer-Encoding

Weitere Header werden nicht ausgewertet bzw. ignoriert.

Beispiel einer negativen Response:

```
HTTP/1.1 500 Internal Server Error
ZSDeliveryID: 123456
Date: Thu, 26 Apr 2018 07:45:55 GMT
Server: Apache/1.2.3 (Unix)
Content-Length: 567890
Connection: close
Content-Type: text/plain
```

**Tabelle 9 – Fehler-Codes im Nichterfolgsfall**

HTTP-Error-Code	Bedeutung
403	Der Zugriff auf das angeforderte Attachment wurde verweigert. Beispielsweise wenn ein Attachment zu einer Nachricht angefordert wird, welche noch gar nicht gelesen wurde.
404	Das angeforderte Attachment kann nicht gefunden werden. Dieser Fehler wird zurückgegeben, wenn das Attachment nicht bzw. nicht mehr existiert.
500	Interner Serverfehler
503	Das Zustellsystem, bei dem das Attachment gespeichert ist, kann nicht erreicht werden.

## 6 Abholung von Zustellstücken

Die Abholung von Zustellstücken kann über das ein- bzw. angebundene Anzeigemodul durch ein E-Government-Portal bzw. ein Behördenportal erfolgen.

### 6.1 Ein-/Anbindung in Browser durch Internetportale

Das Anzeigemodul wird im Bürgerserviceportal (oesterreich.gv.at) sowie im Unternehmensserviceportal (usp.gv.at) eingebunden. Das bedeutet, dass das Softwaremodul des Anzeigemoduls an das Design des jeweiligen Portals angeglichen wird, sodass für den Benutzer ein einheitliches Design zwischen Anzeigemodul, Bürgerserviceportal bzw. Unternehmensserviceportal gegeben ist.

Weitere E-Government Portale können das Anzeigemodul anbinden, d.h. auf den jeweiligen Webseiten der Portale kann über eine Schaltfläche ein Single-Sign-On Durchstieg auf die Webseite, die das Anzeigemodul bereitstellt, ermöglicht werden.

Behördenportale können für ihre Bediensteten das Anzeigemodul anbinden, d.h. auf den jeweiligen Webseiten der Behörden kann über eine Schaltfläche ein Single-Sign-On Durchstieg auf die Webseite, die das Anzeigemodul bereitstellt, ermöglicht werden.

#### 6.1.1 Authentifizierung

Die Authentifizierung MUSS gemäß den Vorgaben aus Abschnitt 2 erfolgen. Es gelten folgende zusätzliche Anforderungen:

Im Fall von Internetportalen, die das Anzeigemodul ein- oder anbinden, MUSS das PVP-R-Profil [PVP2RPROFIL] implementiert werden. Das Anzeigemodul behält sich vor zukünftig auch das PVP2 S-Profil [PVP2SPROFIL] zu unterstützen.

##### 6.1.1.1 Filtern und setzen von PVP-2.1 HTTP-Headervariablen durch das Internetportal

Das Portal muss alle vom Client gelieferten HTTP-Header, die dem Platzhalter „X-PVP\*“ entsprechen, herausfiltern und alle für die Anbindung erforderlichen X-PVP-Header setzen.

#### 6.1.2 Anbindung durch ein E-Government-Portal für natürliche und juristische Personen

##### 6.1.2.1 Liste der PVP2-Header, die vom AMOD interpretiert werden

Die nachfolgende Liste gibt einen Überblick darüber, welche PVP2-Header bei der Anbindung des Anzeigemoduls durch ein E-Government-Portal für natürliche und juristische Personen gesetzt werden müssen.

Alle hier genannten PVP2-Header müssen vom Portal initialisiert werden, um zu verhindern, dass ein Benutzer manipulierte HTTP-Header bis zum AMOD übermitteln kann.

**Tabelle 10: Liste der PVP2-Header für E-Government-Portale**

Jur. Personen LOW/ E-ID	Nat. Personen LOW/E-ID	PVP 2.1 HTTP Header Name	Bedeutung
		<b>Allgemein</b>	
✓/✓	✓/✓	X-PVP-VERSION	Versionsnummer
✓/✓	✓/✓	X-PVP-PARTICIPANT-ID	Teilnehmerkennung
✓/✓	✓/✓	X-PVP-SECCLASS	Sicherheitsklasse

Jur. Personen LOW/ E-ID	Nat. Personen LOW/E-ID	PVP 2.1 HTTP Header Name		Bedeutung
		Externer Benutzer, der im eigenen Namen (z.B.: über oesterreich.gv.at) oder im Namen einer juristischen Person (z.B.: über usp.gv.at) agiert		
✓/ ✓	opt./ opt.	X-PVP-USERID		Benutzerkennung
✓/ ✓	✓/ ✓	X-PVP-PRINCIPAL-NAME		entweder/oder: <ul style="list-style-type: none"><li>Nachname</li><li>Organisationsname</li><li>Systemname</li></ul>
✓/ ✓	opt./ opt.	X-PVP-OU		Voller Name der Organisation
opt. / ✓	✓ / ✓	X-PVP-GIVEN-NAME		Vorname
opt. / ✓	✓ / ✓	X-PVP-BIRTHDATE		Geburtsdatum
opt. / ✓	✓ / ✓	X-PVP-BPK		Bereichsspezifisches Personenkennzeichen für den Bereich ZU. Dieses Kennzeichen darf nur verwendet werden, wenn die Applikation ausschließlich im Bereich ZU arbeitet.  Es MUSS entweder X-PVP-BPK oder X-PVP-ENC-BPK-LIST gesetzt sein.
opt. / ✓	✓ / ✓	X-PVP-ENC-BPK-LIST		Liste von verschlüsselten bPK's – mit verschlüsselten bPK für ZUSEAMOD-ZU.  Es MUSS entweder X-PVP-BPK oder X-PVP-ENC-BPK-LIST gesetzt sein.
opt. / opt.	opt. / opt.	X-PVP-EID-CITIZEN-QAA-EIDAS-LEVEL		Authentifizierungslevel des Bürgers
✓ / ✓	✓ / ✓	X-PVP-ROLES:ZUSE-DISPLAY-SERVICE(AUTH- LEVEL=E-ID)		Rolle "ZUSE-DISPLAY-SERVICE" mit dem Parameter "AUTH-LEVEL", der eines der drei Werte annehmen kann: <ul style="list-style-type: none"><li>LOW</li><li>FON</li><li>E-ID</li></ul>
		Vertretungsinformationen für externe User		
✓/ ✓		X-PVP-ROLES: MPK_POSTBEVO LLMAECHTIGTER( OU="ORG-NAME", Stammzahl="STAM MZAHL-TYP"- „STAMMZAHL- VALUE")	Rolle "MPK_POSTBEVOLLMAECHTIGTER" mit den Parametern „Organisationseinheit (OU)" und „Stammzahl".  Die „Organisationseinheit (OU)" kann auch entfallen, wenn eine juristische Person vertreten wird. In diesem Fall wird die OU aus dem Header X-PVP-OU verwendet.  z.B. MPK_POSTBEVOLLMAECHTIGTER(OU=ACME GmbH,Stammzahl=XFN-222222a)	
		Vertretene Organisation (Unternehmen/Behörde) Die PVP 2.1 Header zur Abbildung der vertretenen Organisation werden derzeit vom AMOD nicht ausgewertet, sind jedoch vom Portal verpflichtend zu löschen.		
		X-PVP-MANDATOR-LEGAL-PERSON-FULL-NAME		Organisationsname
		X-PVP-MANDATOR-LEGAL-PERSON-SOURCE-PIN- TYPE (deprecated)		Stammzahlentyp
		X-PVP-MANDATOR-LEGAL-PERSON-SOURCE-PIN- TYPE-V2		Stammzahlentyp (ab Version 2.3.0 PVP Attribut-Profil)



Jur. Personen LOW/ E-ID	Nat. Personen LOW/ E-ID	PVP 2.1 HTTP Header Name	Bedeutung
		X-PVP-MANDATOR-LEGAL-PERSON-SOURCE-PIN	Stammzahl
		<b>Vertretene natürliche Person</b>	
	✓ / ✓	X-PVP-MANDATOR-NATURAL-PERSON-FAMILY-NAME	Nachname
	✓ / ✓	X-PVP-MANDATOR-NATURAL-PERSON-GIVEN-NAME	Vorname
	✓ / ✓	X-PVP-MANDATOR-NATURAL-PERSON-BIRTHDATE	Geburtsdatum
	opt. / opt.	X-PVP-MANDATOR-NATURAL-PERSON-BPK	bereichsspezifisches Personenkennzeichen für den Bereich ZU des Vollmachtgebers.  Es MUSS entweder X-PVP- MANDATOR-NATURAL-PERSON- BPK oder X-PVP-MANDATOR- NATURAL-PERSON-ENC-BPK- LIST gesetzt sein.
	opt. / opt.	X-PVP-MANDATOR-NATURAL-PERSON-ENC-BPK-LIST	Liste von vbPKs des Vollmachtgebers - mit verschlüsselten bPK für ZUSEAMOD-ZU.  Es MUSS entweder X-PVP- MANDATOR-NATURAL-PERSON- BPK oder X-PVP-MANDATOR- NATURAL-PERSON-ENC-BPK- LIST gesetzt sein

### 6.1.2.2 Externer Benutzer

Um externe Benutzer, die im eigenen Namen agieren, eindeutig identifizieren zu können, MÜSSEN vom Portal folgende Header übermittelt werden:

- X-PVP-VERSION
- X-PVP-PARTICIPANT-ID
- X-PVP-SECCLASS
- X-PVP-PRINCIPAL-NAME
- X-PVP-GIVEN-NAME
- X-PVP-BIRTHDATE
- X-PVP-BPK **oder** X-PVP-ENC-BPK-LIST
- X-PVP-ROLES

Wenn es sich um eine vertretene natürliche Person handelt, müssen zusätzlich folgende Header übermittelt werden:

- X-PVP-MANDATOR-NATURAL-PERSON-FAMILY-NAME
- X-PVP-MANDATOR-NATURAL-PERSON-GIVEN-NAME
- X-PVP-MANDATOR-NATURAL-PERSON-BIRTHDATE
- X-PVP-MANDATOR-NATURAL-PERSON-BPK **oder** X-PVP-MANDATOR-NATURAL-PERSON-ENC-BPK-LIST

#### 6.1.2.2.1 Übermittlung der Identität des Benutzers entweder auf Basis des bPK-ZU oder des vbPK-ZU

Um den Benutzer eindeutig identifizieren zu können, MUSS vom Portal verpflichtend entweder das unverschlüsselte oder verschlüsselte Personenkennzeichen für den Bereich „ZU“ mitgegeben werden.

1. Das unverschlüsselte Personenkennzeichen des Bereichs „Zustellung (ZU)“ ist die erste Wahl zur eindeutigen Identifizierung des Benutzers
  - Beispiel für ein bPK des Bereichs „**Zustellung (ZU)**“  
X-PVP-BPK: ZU:j/NxdRQhp+tNyE9WhHdBSYuy3hA=
2. Wenn kein Personenkennzeichen für den Bereich „ZU“ zur Verfügung steht, dann MUSS in der Liste der verschlüsselten bPKs (HTTP-Header X-PVP-ENC-BPK-LIST) das bereichsspezifische Personenkennzeichen (vbPK) des Bereichs „ZU“, welches für den Service-Identifizier „ZUSEAMOD“ verschlüsselt ist, hinzugefügt werden
  - Die Liste kann mehrere vbPKs enthalten.
  - Beispiel für den Aufbau einer Liste mit zwei verschlüsselten bereichsspezifischen Personenkennzeichen:  
(<Verwaltungskennzeichen>+<Bereichskennzeichen>|<vbPK>);(<Verwaltungskennzeichen>+<Bereichskennzeichen>|<vbPK>)
  - Beispiel einer Liste mit zwei verschlüsselten bPKs:  
X-PVP-ENC-BPK-LIST: (BMI+T1|c1tWDIrXH3BEbhChZpwKCPSSp9thLzKQI=) ; (ZUSEAMOD+ZU|d1aXRlc1tWDIrXH3BEbhChZpwKzY2=)

#### 6.1.2.3 Externer Benutzer, der im Namen einer juristischen Person agiert

Um externe Benutzer, die im Namen einer juristischen Person agieren, eindeutig identifizieren zu können, MÜSSEN vom Portal folgende Header übermittelt werden, wenn es sich um eine niederschwellige Anmeldung (X-PVP-ROLES:ZUSE-DISPLAY-SERVICE (AUTH-LEVEL=FON) oder X-PVP-ROLES:ZUSE-DISPLAY-SERVICE (AUTH-LEVEL=LOW)) handelt:

- X-PVP-VERSION
- X-PVP-PARTICIPANT-ID
- X-PVP-SECCLASS
- X-PVP-USERID
- X-PVP-PRINCIPAL-NAME
- X-PVP-OU
- X-PVP-ROLES

Handelt es sich um eine höherwertige Anmeldung (X-PVP-ROLES:ZUSE-DISPLAY-SERVICE (AUTH-LEVEL=E-ID)) MÜSSEN auch folgende Header übermittelt werden:

- X-PVP-GIVEN-NAME
- X-PVP-BIRTHDATE
- X-PVP-BPK oder X-PVP-ENC-BPK-LIST

Die Personendaten der juristischen Person, in deren Namen der externe Benutzer tätig ist, wird aus den angegebenen PVP Rollen gemäß folgender Syntax ermittelt:

X-PVP-ROLES: MPK\_POSTBEVOLLMAECHTIGTER (OU="ORG-NAME",  
Stammzahl="STAMMZAHL-TYP"-„STAMMZAHL-VALUE")

ORG-NAME := Name der juristischen Person

STAMMZAHL-TYP := Typ der Stammzahl der juristischen Person

STAMMZAHL-VALUE := Stammzahl der juristischen Person

**Beispiel:** X-PVP-ROLES: MPK\_POSTBEVOLLMAECHTIGTER(OU=BH  
Weiz,Stammzahl=XGLN-1234567890)

### Vollständiger Name der juristischen Person

Der vollständige Name der juristischen Person, für die der Benutzer tätig ist, wird im HTTP-Header „X-PVP-MANDATOR-LEGAL-PERSON-FULL-NAME“ (Organisationseinheit) abgebildet.

**Beispiel:** X-PVP-MANDATOR-LEGAL-PERSON-FULL-NAME: **ACME GmbH**

### Stammzahl der juristischen Person für die der Benutzer tätig ist

Die Stammzahl der juristischen Person, für die der Benutzer tätig ist, wird im HTTP-Header „X-PVP-MANDATOR-LEGAL-PERSON-SOURCE-PIN“ (Stammzahl) abgebildet.

**Beispiel:** X-PVP-MANDATOR-LEGAL-PERSON-SOURCE-PIN: **999999m**

### Stammzahlentyps der juristischen Person, für die der Benutzer tätig ist

Der Typ der Stammzahl der juristischen Person, für die der Benutzer tätig ist, wird im HTTP-Header „X-PVP-MANDATOR-LEGAL-PERSON-SOURCE-PIN-TYPE-V2“ (Typ der Stammzahl) abgebildet.

**Beispiel:** X-PVP-MANDATOR-LEGAL-PERSON-SOURCE-PIN-TYPE-V2:  
urn:publicid:gv.at:baseid+XFN

Mögliche Werte:

- „urn:publicid:gv.at:baseid+XFN“ Firmenbuchnummer
- „urn:publicid:gv.at:baseid+XZVR“ Nummer des Zentralen Vereinsregisters
- „urn:publicid:gv.at:baseid+XGLN“ Global Location Number für andere Register (wie z.B. ERSB, LFR, Steuer, ...)

#### 6.1.2.4 Authentifizierungsmethode

Die Authentifizierungsmethode wird in der HTTP-Header-Variable „X-PVP-ROLES“ in der Rolle „ZUSE-DISPLAY-SERVICE“ mit dem Parameter „AUTH-LEVEL“ übermittelt.

#### Wertebereich des Authentifizierungslevels

Wert	Level	SecClass	Bedeutung
E-ID	3	2	ID Austria oder Handysignatur oder Bürgerkarte
FON	2	1	FON- oder USP-Kennung
LOW	1	1	Niederschwellige Anmeldung mit Benutzerkennung und Passwort

**Beispiel:** X-PVP-ROLES: ZUSE-DISPLAY-SERVICE (AUTH-LEVEL=E-ID)

Wird auch der optionale HTTP-Header „X-PVP-EID-CITIZEN-QAA-EIDAS-LEVEL“ geliefert, so MUSS dieser bei den Werten „LOW“ und „FON“ auf <http://eid.as.europa.eu/LoA/low> gesetzt werden und bei „E-ID“ auf <http://eid.as.europa.eu/LoA/high> gesetzt werden andernfalls kommt es zu einem Fehler.

### 6.1.3 Anbindung durch ein Behördenportal für Behördenmitarbeiter

#### 6.1.3.1 Liste der PVP2-Header, die vom AMOD interpretiert werden

Die nachfolgende Liste gibt einen Überblick darüber, welche PVP2-Header bei der Anbindung des Anzeigemoduls durch ein Behördenportal für Behördenmitarbeiter gesetzt werden müssen.

Alle hier genannten PVP2-Header müssen vom Portal initialisiert werden, um zu verhindern, dass ein Benutzer manipulierte HTTP-Header bis zum AMOD übermitteln kann.

**Tabelle 11: Liste der PVP2-Header für Behördenportale**

Jur. Personen LOW/E-ID	PVP 2.1 HTTP Header Name	Bedeutung
	<b>Allgemein</b>	
✓/ ✓	X-PVP-VERSION	Versionsnummer
✓/ ✓	X-PVP-PARTICIPANT-ID	Teilnehmerkennung
✓/ ✓	X-PVP-SECCLASS	Sicherheitsklasse
	<b>Behördenmitarbeiter</b>	
✓/ ✓	X-PVP-USERID	Benutzerkennung
✓/ ✓	X-PVP-PRINCIPAL-NAME	entweder/oder: <ul style="list-style-type: none"> <li>Nachname</li> <li>Organisationsname</li> <li>Systemname</li> </ul>
✓/ ✓	X-PVP-OU	Voller Name der Organisation
✓/ ✓	X-PVP-GID	Globale Account Kennung
opt. / opt.	X-PVP-BPK	bereichsspezifisches Personenkennzeichen.
opt. / opt.	X-PVP-GIVEN-NAME	Vorname
opt. / opt.	X-PVP-BIRTHDATE	Geburtsdatum
opt. / opt.	X-PVP-EID-CITIZEN-QAA-EIDAS-LEVEL	Verpflichtende Angabe LoA "high" für Anmeldung mit ID Austria/Handy-Signatur/Bürgerkarte für die Registrierung am Anzeigemodul.
	<b>Vertretungsinformationen für Behördenmitarbeiter</b>	
✓ / ✓	X-PVP-ROLES:MPK_POSTBEVOLLMAECHTIGTER(OU=BEHOERDE A, Stammzahl=XGLN-9110000000001)  oder  X-PVP-ROLES:MPK_POSTBEVOLLMAECHTIGTER(SOURCE=XGLN-9110000000001 BEHOERDE A);MPK_POSTBEVOLLMAECHTIGTER(SOURCE=9110000000002 BEHOERDE B)	Rolle "MPK_POSTBEVOLLMAECHTIGTER" mit den Parametern „Organisationseinheit (OU)“ und „Stammzahl“.  oder  Rolle "MPK_POSTBEVOLLMAECHTIGTER" für mehrere juristische Personen, wobei der Parameter „SOURCE“ aus der Stammzahl und der Organisationseinheit (OU) erstellt wird.
opt. / opt.	X-PVP-ROLES:MPK_REGISTRIERUNG(OU=BEHOERDE A, Stammzahl=XGLN-9110000000001)  oder  X-PVP-ROLES:MPK_REGISTRIERUNG(SOURCE=XGLN-9110000000001 BEHOERDE A);MPK_REGISTRIERUNG(SOURCE=9110000000002 BEHOERDE B)	Rolle "MPK_REGISTRIERUNG" für die Registrierung am Anzeigemodul mit den Parametern „Organisationseinheit (OU)“ und „Stammzahl“  oder  Rolle "MPK_REGISTRIERUNG" für mehrerer juristische Person, wobei der Parameter „SOURCE“ aus der Stammzahl und der Organisationseinheit (OU) erstellt wird.

### 6.1.3.2 Behördenmitarbeiter

Um den Behördenmitarbeiter eindeutig identifizieren zu können, müssen vom Portal folgende Header übermittelt werden:

- X-PVP-VERSION
- X-PVP-PARTICIPANT-ID
- X-PVP-SECCLASS
- X-PVP-USERID
- X-PVP-PRINCIPAL-NAME
- X-PVP-OU
- X-PVP-GID
- X-PVP-ROLES

Für die Abholung als Behördenmitarbeiter ist eine Sicherheitsklasse (SecClass) 2 oder höher notwendig.

#### 6.1.3.2.1 Liste der vertretenen Behörden

Die Personendaten der juristische(n) Person(en), in deren Namen der Behördenmitarbeiter tätig ist, wird aus den angegebenen PVP Rollen gemäß folgender Syntax ermittelt:

Vertretung für genau eine juristische Person:

```
X-PVP-ROLES: MPK_POSTBEVOLLMAECHTIGTER(OU="ORG-NAME",
Stammzahl="STAMMZAHL-TYP"-„STAMMZAHL-VALUE")
```

ODER

Vertretung für eine oder mehrere juristische Personen:

```
X-PVP-ROLES: MPK_POSTBEVOLLMAECHTIGTER(SOURCE="STAMMZAHL-TYP"-
„STAMMZAHL-VALUE"|"ORG-NAME" (, SOURCE = "STAMMZAHL-TYP"-„STAMMZAHL-
VALUE"|"ORG-NAME") *)
```

ORG-NAME := Name der juristischen Person

STAMMZAHL-TYP := Typ der Stammzahl der juristischen Person

STAMMZAHL-VALUE := Stammzahl der juristischen Person

Vertretungen für mehrere juristische Personen werden ENTWEDER durch einen Strichpunkt getrennt aufgelistet ODER indem die weiteren Vertretungen durch einen Beistrich getrennt innerhalb der Rolle MPK\_POSTBEVOLLMAECHTIGTER angeführt werden.

Beispiel:

```
X-PVP-ROLES: MPK_POSTBEVOLLMAECHTIGTER(SOURCE=XGLN-1234567890|BH
Weiz);MPK_POSTBEVOLLMAECHTIGTER(SOURCE=XGLN-56789012345|BH Hartberg)
```

Beispiel:

```
X-PVP-ROLES: MPK_POSTBEVOLLMAECHTIGTER(SOURCE=XGLN-1234567890|BH
Weiz, SOURCE=XGLN-56789012345|BH Hartberg)
```

#### 6.1.3.2.2 Registrierung einer Behörde zur elektronischen Zustellung

Möchte der Behördenmitarbeiter eine Behörde für die elektronische Zustellung registrieren, so MUSS sich der Mitarbeiter mit ID Austria/Handy-Signatur/Bürgerkarte am Stammportal anmelden und der sich daraus ergebende Header übermittelt werden:

- X-PVP-EID-CITIZEN-QAA-EIDAS-LEVEL:  
http://eidas.europa.eu/LoA/high

Alternativ kann pro vertretener Behörde die Rolle MPK\_REGISTRIERUNG gesetzt werden.

Beispiel:

Vertretung für genau eine juristische Person:

X-PVP-ROLES: MPK\_REGISTRIERUNG(OU=BH Weiz,Stammzahl=XGLN-1234567890)

Vertretung für eine oder mehrere juristische Personen:

X-PVP-ROLES: MPK\_REGISTRIERUNG(SOURCE=XGLN-1234567890|BH Weiz);MPK\_REGISTRIERUNG(SOURCE=XGLN-56789012345|BH Hartberg)

#### 6.1.4 Fehler

Die vom Portal gelieferten Header werden vom Anzeigemodul verarbeitet und auf Korrektheit überprüft. Sollte bei der Überprüfung einzelner Headerwerte bzw. die Kombination aus Headerwerten fehlerhaft sein, so wird die Anfrage mit einem 403 abgewiesen.

### 6.2 Anzahl der Nachrichten ungelesen und gesamt

Um dem Benutzer im E-Government-Portal vor dem Aufruf des Anzeigemoduls informieren zu können, wie viele Nachrichten insgesamt im Postfach liegen und wie viele davon ungelesen sind, können E-Government-Portale im Benutzerkontext, basierend auf den gesetzten PVP-Headern mittels Webservice Operation `MessageCount` das Anzeigemodul abfragen.

#### 6.2.1 XML Format und Binding

Dieser Abschnitt beschreibt Anfragen (Request) bzw. Antworten (Response) für die Ermittlung der Anzahl von Nachrichten im Postfach

##### 6.2.1.1 Authentifizierung

Die Authentifizierung des E-Government-Portals gegenüber dem Anwendungsportal des Anzeigemoduls MUSS gemäß den Vorgaben aus Abschnitt 6.1 erfolgen.

Beispiel für die zu setzenden PVP 2.1 Http-Header für einen Behördenmitarbeiter:

```
POST /abc.gv.at/anwendung2/xyz HTTP/1.1
Host:zustellsystem.at
User-Agent: .JNET 1.1
X-PVP-VERSION: 2.1
X-PVP-OU: IIII/4
X-PVP-GID: AT:L6:123456
X-PVP-PARTICIPANT-ID: AT:L6
X-PVP-USERID: max.mustermann@usp.gv.at
X-PVP-PRINCIPAL-NAME: Mustermann
X-PVP-SECCLASS: 2
X-PVP-ROLES: MPK POSTBEVOLLMAECHTIGTER(OU=BH Weiz,Stammzahl=XGLN-
1234567890)
Content-Type: text/xml
Content-Length: 788
```

##### 6.2.1.2 Format

Das Anzeigemodul wertet die PVP-Header aus, um festzustellen für welche natürliche oder juristische Person die Anzahl der Nachricht im Postfach ermittelt werden soll.

Die Header müssen den Vorgaben aus den Abschnitten 6.1.2.1 bzw. 6.1.3.1 entsprechen.

#### 6.2.1.2.1 Request

Es ist ein leeres `amod:MessageCountRequest` Element zu übergeben.

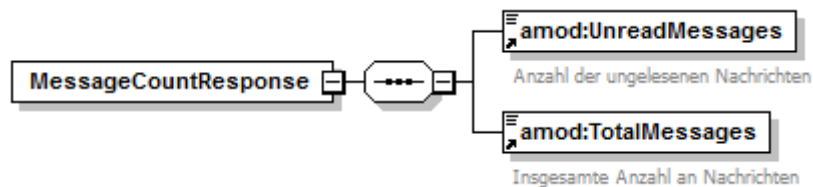
**Abbildung 15 – Struktur des `amod:MessageCountRequest` Elements**



#### 6.2.1.2.2 Response

Im `amod:UnreadMessages` Element wird die Anzahl der ungelesenen Nachrichten und im `amod:TotalMessages` Element wird die Gesamtanzahl der Nachrichten übergeben.

**Abbildung 16 – Struktur des `amod:MessageCountResponse` Elements**



#### 6.2.1.3 Binding

Für den Datenaustausch MUSS das Netzwerkprotokoll SOAP in der Version 1.2 über das HTTP Binding in [SOAP12] verwendet werden.

Sämtliche Kommunikation muss gesichert gemäß den Anforderungen in Abschnitt 3.2.1.1 erfolgen.

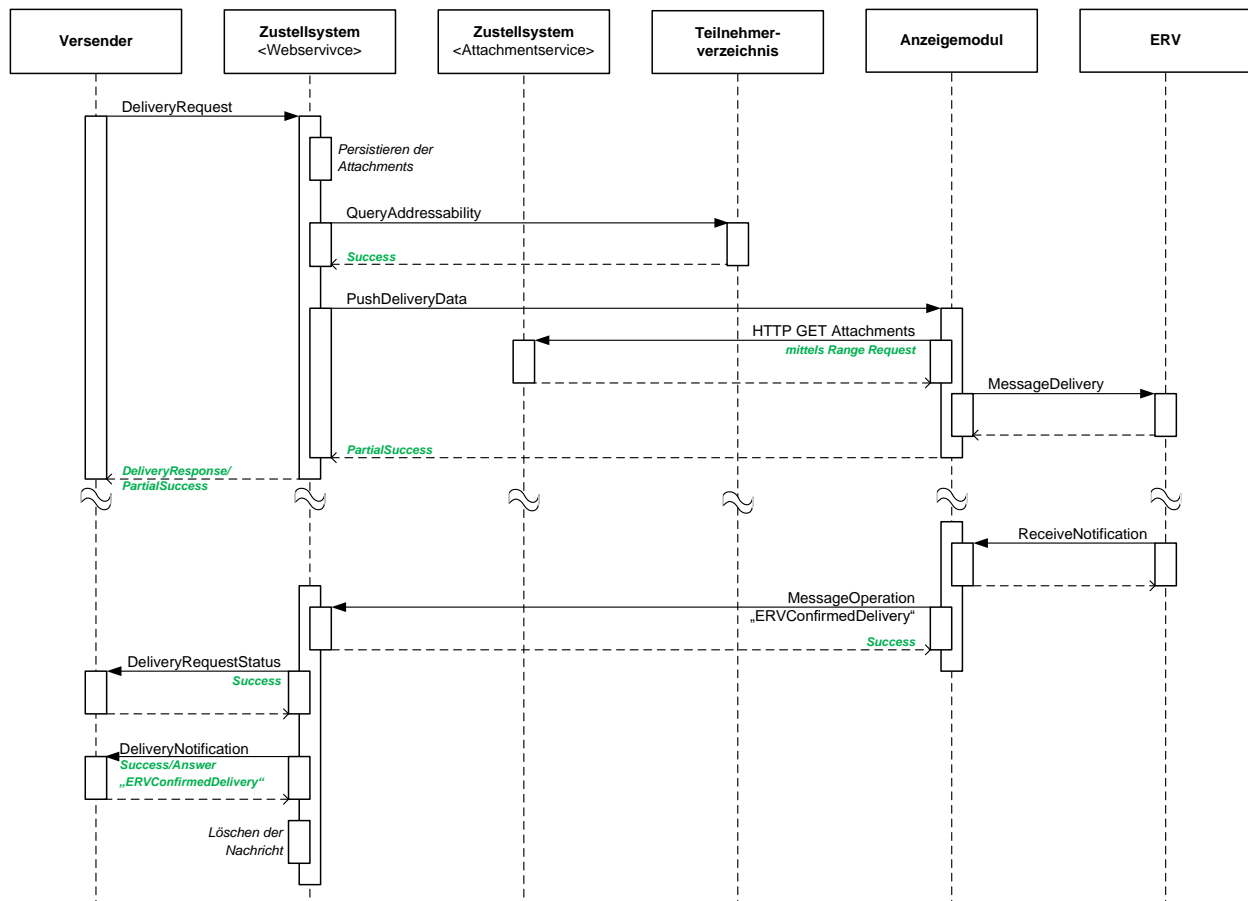
Die entsprechende WSDL-Beschreibung ist als gesonderte Datei der Spezifikation beigelegt.

- `gui2amod_p2.wsdl`

## 7 Weiterleitung der Nachricht in den Elektronischen Rechtsverkehr der Justiz (ERV)

Sofern bei einem im Teilnehmerverzeichnis registrierten Teilnehmer die Weiterleitung in den ERV aktiviert ist, werden ALLE eingehenden Zustellungen und Zusendungen (gemäß Zustellgesetz) des Teilnehmers vom Anzeigemodul in den ERV weitergeleitet.

Abbildung 17 – Weiterleitung einer RSa-Zustellung in den ERV



Im Folgenden sind die Auswirkungen einer aktiven Weiterleitung in den ERV auf den Zustellprozess beschrieben.

Alle Nachrichten an den Teilnehmer werden in den ERV weitergeleitet. Erfüllt eine Nachricht nicht die Voraussetzungen, um vom ERV verarbeitet werden zu können, wird der `msg:DeliveryRequest` mit einem Fehler quittiert.

Der Zustellzeitpunkt wird vom ERV ermittelt bzw. berechnet (Details siehe [ZUSEORG]).

Der Zeitpunkt, zu dem die Zustellung in der jeweiligen Übermittlungsstelle und damit im Verfügungsbereich des Empfängers „angekommen“ ist, d.h. die Zustellung erfolgt ist, ist Basis für die Berechnung des Zustellzeitpunkts gemäß [GOG], welcher „dem nächsten auf die Ankunft in der Übermittlungsstelle folgenden Werktag“ entspricht.

Die Information, dass die Zustellung via ERV und damit nicht nach [ZUSTG] sondern nach [GOG] erfolgt ist, muss über das Zustellsystem an den Versender gemeldet werden. Dieser Umstand MUSS auch am Zustellnachweis ersichtlich sein.

Im Falle der Weiterleitung in den ERV werden keine expliziten Verständigungen generiert, da die Zustellung mit Einlangen in den Verfügungsbereich des Empfängers bei seiner Übermittlungsstelle als zugestellt gilt.



Eine explizite Annahme durch den Empfänger ist im ERV nicht vorgesehen.

## 7.1 Weiterleitung einer Zustellung oder Zusendung

### 7.1.1 Übermittlung der Zustellung

1. Versender übermittelt eine Zustellung oder Zusendung an das Zustellsystem
2. Das Zustellsystem fragt das Teilnehmerverzeichnis ab
3. Teilnehmerverzeichnis gibt im verschlüsselten ZUSEToken die Information mit, dass die Weiterleitung in den ERV aktiviert ist
4. Das Zustellsystem pusht die Metadaten der Nachricht zum Anzeigemodul
5. Das Anzeigemodul holt sich die Attachments vom Zustellsystem
6. Das Anzeigemodul leitet die Nachricht inklusive Attachments asynchron an den ERV weiter und antwortet dem Zustellsystem mit `amod:PartialSuccess` und dem ERV-Code an den weitergeleitet wurde

Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
<amod:PushDeliveryDataResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:msg="http://reference.e-
government.gv.at/namespace/zustellung/msg/phase2/20181206#"
xmlns:amod="http://reference.e-
government.gv.at/namespace/zustellung/amod/phase2/20181206#">
  <msg:ZSDeliveryID>a95c530a-7af5-3492-a744-99e70578d150</msg:ZSDeliveryID>
  <amod:PartialSuccess>
    <msg:RelayedViaERV>
      <msg:ERVCode>Z251212</msg:ERVCode>
    </msg:RelayedViaERV>
  </amod:PartialSuccess>
</amod:PushDeliveryDataResponse>
```

7. Das Zustellsystem antwortet dem Versender unmittelbar mit einem `msg:PartialSuccess` ohne Zustellzeitpunkt jedoch mit Hinweis auf die Weiterleitung in den ERV
  - Das `msg:RelayedViaERV` Element zeigt dem Versender an, dass in den ERV weitergeleitet wurde

Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
<msg:DeliveryResponse Id="DeliveryResponse_99e70578d150"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:msg="http://reference.e-
government.gv.at/namespace/zustellung/msg/phase2/20181206#">
  <msg:PartialSuccess>
    <msg:DeliverySystem>http://zustelldienst.at</msg:DeliverySystem>
    <msg:ZSDeliveryID>a95c530a-7af5-3492-a744-99e70578d150</msg:ZSDeliveryID>
    <msg:AppDeliveryID>appid-23490090456u9</msg:AppDeliveryID>
    <msg:GZ>GZ123456789</msg:GZ>
  </msg:PartialSuccess>
  <msg:RelayedViaERV>
    <msg:ERVCode>Z251212</msg:ERVCode>
  </msg:RelayedViaERV>
  <dsig:Signature>
    <!-- Daten der Signatur des Zustelldienstes über das
         msg:DeliveryResponse Element-->
  </dsig:Signature>
</msg:DeliveryResponse>
```

## 7.1.2 Erfolgreiche Weiterleitung in den ERV

1. Der ERV meldet dem Anzeigemodul asynchron die erfolgreiche Verarbeitung der Nachricht inklusive Zustellzeitpunkt zurück.
2. Bei erfolgreicher Verarbeitung meldet das Anzeigemodul dem Zustellsystem mittels Nachrichtenoperation `amod:ERVConfirmedDelivery` den Zustellzeitpunkt zurück
  - Der Zustellzeitpunkt ist dem `amod:MessageOperation/msg:Timestamp` Element zu entnehmen

Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
<amod:MessageOperationRequest
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:p="http://reference.e-
government.gv.at/namespace/persondata/phase2/20181206#"
  xmlns:msg="http://reference.e-
government.gv.at/namespace/zustellung/msg/phase2/20181206#"
  xmlns:amod="http://reference.e-
government.gv.at/namespace/zustellung/amod/phase2/20181206#"
  Version="2.4.0-003">
  <amod:MessageOperation OperationID="20180811T13:42:59.123456789-563985412">
    <msg:ZSDeliveryID>a95c530a-7af5-3492-a744-99e70578d150</msg:ZSDeliveryID>
    <!-- Zeitpunkt bzw. Datum, zu dem die Zustellung im
      Verfügungsbereich des ERV-Teilnehmers eingelangt ist-->
    <msg:Timestamp>2025-05-02T00:00:00</msg:Timestamp>
    <amod:Receiver>
      <p:Identification>
        <!-- GLN des Bezirksgerichts Krems an der Donau -->
        <p:Value>9110023614250</p:Value>
        <p:Type>urn:publicid:gv.at:baseid+XGLN</p:Type>
      </p:Identification>
      <p:CorporateBody>
        <p:FullName>Bezirksgericht Krems an der Donau</p:FullName>
      </p:CorporateBody>
    </amod:Receiver>
    <amod:ERVConfirmedDelivery/>
    <msg:ERVCode>Z251212</msg:ERVCode>
    <amod:ERVConfirmedDelivery/>
  </amod:MessageOperation>
</amod:MessageOperationRequest>
```

3. Das Zustellsystem meldet dem Versender mittels `msg:DeliveryRequestStatus` den Zustellzeitpunkt und den ERV-Code, an den weitergeleitet wurde, zurück
  - Der vom ERV gemeldete Zustellzeitpunkt (`amod:MessageOperation/msg:Timestamp`) MUSS vom Zustellsystem auf das `msg:DeliveryTimestamp` Element gemappt werden

Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
<msg:DeliveryRequestStatus Id="DeliveryRequestStatus_99e70578d150"
  xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:msg="http://reference.e-
government.gv.at/namespace/zustellung/msg/phase2/20181206#" Version="2.4.0-003">
  <msg:Success>
    <msg:DeliverySystem>http://zustelldienst.at</msg:DeliverySystem>
    <msg:ZSDeliveryID>a95c530a-7af5-3492-a744-99e70578d150</msg:ZSDeliveryID>
    <msg:AppDeliveryID>appid-23490090456u9</msg:AppDeliveryID>
    <msg:GZ>GZ123456789</msg:GZ>
    <msg:DeliveryTimestamp>2025-05-02T00:00:00</msg:DeliveryTimestamp>
  </msg:Success>
  <msg:RelayedViaERV>
    <msg:ERVCode>Z251212</msg:ERVCode>
  </msg:RelayedViaERV>
```

```

    <dsig:Signature>
      <!-- Daten der Signatur des Zustelldienstes über das
            msg:DeliveryRequestStatus Element-->
    </dsig:Signature>
  </msg:DeliveryRequestStatus>

```

4. Mit der erfolgreichen Übertragung des msg:DeliveryRequestStatus/msg:Success ist die Verarbeitung der Zustellung abgeschlossen.
  - Im Falle einer nicht nachweislichen Zustellung bzw. Zusendung erhält der Versender vom Zustellsystem keine weiteren Informationen
  - Im Falle einer nachweislichen Zustellung bzw. Zusendung hat der Zustelldienst einen Zustellnachweis zu erstellen (vgl. Abschnitt 7.2)
5. Die endgültige Löschung der Nachricht wird explizit durch das Anzeigemodul mittels Nachrichtenoperation „Delete“ angefordert.

### 7.1.3 Fehlschlag der Weiterleitung in den ERV

1. Der ERV meldet dem Anzeigemodul asynchron zurück, dass bei der Verarbeitung der Nachricht ein Fehler aufgetreten ist
2. Das Anzeigemodul leitet den Fehler mittels Nachrichtenoperation „DeliveryError“ an das Zustellsystem weiter
  - Wenn zumindest eines der PDF-Attachments nicht dem PDF/A Standard entspricht wird der Fehler AM0201\_U retourniert
  - Wenn ein anderer ERV-Fehler auftritt, wird der generelle Fehler AM0200\_U inklusive der Originalfehlermeldung des ERV retourniert

Beispiel:

```

<?xml version="1.0" encoding="UTF-8"?>
<amod:MessageOperationRequest
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:p="http://reference.e-
government.gv.at/namespace/persondata/phase2/20181206#"
  xmlns:msg="http://reference.e-
government.gv.at/namespace/zustellung/msg/phase2/20181206#"
  xmlns:amod="http://reference.e-
government.gv.at/namespace/zustellung/amod/phase2/20181206#"
  Version="2.4.0-003">
  <amod:MessageOperation OperationID="20180811T13:42:59.123456789-563985412">
    <msg:ZSDeliveryID>a95c530a-7af5-3492-a744-99e70578d150</msg:ZSDeliveryID>
    <msg:Timestamp>2025-05-02T00:15:12</msg:Timestamp>
    <amod:DeliveryError>
      <msg:ErrorInfo>
        <msg:Code>AM0201_U</msg:Code>
        <msg:Text>
          ERV forwarding to Code Z251212: PDF file must be conform
            to PDF/A standard</msg:Text>
        </msg:ErrorInfo>
      </amod:DeliveryError>
    </amod:MessageOperation>
  </amod:MessageOperationRequest>

```

3. Das Zustellsystem meldet dem Versender mittels msg:DeliveryRequestStatus die fehlerhafte Verarbeitung zurück, d.h. die Zustellung hat nicht stattgefunden und wurde nicht bewirkt.

Beispiel:

```

<?xml version="1.0" encoding="UTF-8"?>
<msg:DeliveryRequestStatus Id="DeliveryRequestStatus_99e70578d150"
  xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

```

```

xmlns:msg="http://reference.e-
government.gv.at/namespace/zustellung/msg/phase2/20181206#" Version="2.4.0-003">
  <msg:Error>
    <msg:DeliverySystem>http://zustelldienst.at</msg:DeliverySystem>
    <msg:ZSDeliveryID>a95c530a-7af5-3492-a744-99e70578d150</msg:ZSDeliveryID>
    <msg:AppDeliveryID>appid-23490090456u9</msg:AppDeliveryID>
    <msg:GZ>GZ123456789</msg:GZ>
    <msg:ErrorInfo>
      <msg:Code>524</msg:Code>
      <msg:Text>
        ERV forwarding to Code z251212: PDF file must be conform
        to PDF/A standard</msg:Text>
      </msg:ErrorInfo>
    </msg:Error>
    <dsig:Signature>
      <!-- Daten der Signatur des Zustelldienstes über das
        msg:DeliveryRequestStatus Element-->
    </dsig:Signature>
  </msg:DeliveryRequestStatus>

```

4. Mit der Übertragung des msg:DeliveryRequestStatus/msg:Error ist die Verarbeitung der Zustellung abgeschlossen.
5. Die endgültige Löschung der Nachricht wird explizit durch das Anzeigemodul mittels Nachrichtoperation „Delete“ angefordert.

## 7.2 Weiterleitung einer Zustellung bzw. Zusendung mit Zustellnachweis

Die Weiterleitung einer Zustellung bzw. Zusendung mit Zustellnachweis („RSa-Qualität“) in den ERV erfolgt analog einer nicht nachweislichen Zustellung bzw. Zusendung.

Zusätzlich MUSS der Zustelldienst nach der erfolgreichen Übermittlung des msg:DeliveryRequestStatus einen Zustellnachweis (msg:DeliveryNotification) erzeugen und direkt an die Webservice-URL oder E-Mail-Adresse des Versender übermitteln.

Diesen Schritt sollte der Zustelldienst zeitverzögert durchführen, um dem Versender ausreichend Zeit zu geben die zuvor versendete Übergabebestätigung (msg:DeliveryRequestStatus) abarbeiten zu können.

Der vom ERV bestimmte Zustellzeitpunkt ist dem amod:MessageOperation/msg:Timestamp Element zu entnehmen.

Beispiel:

```

<msg:DeliveryNotification Id="DeliveryNotification_77f70578d150"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:p="http://reference.e-
government.gv.at/namespace/persondata/phase2/20181206#"
xmlns:msg="http://reference.e-
government.gv.at/namespace/zustellung/msg/phase2/20181206#" Version="2.4.0-003">
  <msg:DeliverySystem>http://zustelldienst.at</msg:DeliverySystem>
  <msg:ZSDeliveryID>a95c530a-7af5-3492-a744-99e70578d150</msg:ZSDeliveryID>
  <msg:AppDeliveryID>appid-23490090456u9</msg:AppDeliveryID>
  <msg:GZ>GZ123456789</msg:GZ>
  <msg:SenderDetails>
    <p:Identification>
      <p:Value>9110001234567</p:Value>
      <p:Type>urn:publicid:gv.at:baseid+XGLN</p:Type>
    </p:Identification>
    <p:CorporateBody>
      <p:FullName>Musterbehörde</p:FullName>
      <p:Target>urn:publicid:gv.at:ecdid+BMF+SA</p:Target>
    </p:CorporateBody>
  </msg:SenderDetails>

```

```

<msg:ReceiverDetails>
  <p:Identification>
    <!-- GLN des Bezirksgerichts Krems an der Donau -->
    <p:Value>9110023614250</p:Value>
    <p:Type>urn:publicid:gv.at:baseid+XGLN</p:Type>
  </p:Identification>
  <p:CorporateBody>
    <p:FullName>Bezirksgericht Krems an der Donau</p:FullName>
  </p:CorporateBody>
</msg:ReceiverDetails>
<msg:Timestamp>2025-05-02T00:00:00</msg:Timestamp>
<msg:ERVConfirmedDelivery>
  <msg:ERVCode>Z251212</msg:ERVCode>
</msg:ERVConfirmedDelivery>
<dsig:Signature>
  <!-- Daten der Signatur des Zustelldienstes über das
        msg:DeliveryNotification Element-->
</dsig:Signature>
<msg:AdditionalFormat Type="application/pdf">
JVBERi0xLjQKJcfsj6IKNSAwIG9iago8PC9MZW5ndGggNiAwIFlvdGVyIC9GbGF0ZURlY29kZT4+C
nN0cmVhbQp4nCtUMNAzNFIwAEEYIzmXqxBIwViaWijoGptYminoGiiAabCcfcPC5gks+VyAQAgCAlgxUZW
5kc3RyZWFTcmVuZG9iago2IDAgb2JqCjUyCmVuZG9iago0IDAgb2JqCjw8L1RKKACiigAooooAKKKKAC
iigAooooAKKKKACiigAooooAKKKKACiigAooooAKKKKACiigAooooAKKKKACiigAooooAKKKKACiigAooooAKKKKACi
iigAooooAKKKKACiigAooooAKKKKACiigAooooAKKKKACiigwMDAgbiAKdHJhaWxlco8PCAvU2l6Z
SAXMCAvUm9vdCAxIDAgUiAvSW5mbYAyIDAgUgovSUQgWzxDMDk3RUQ4OTBCRTZBNEM5MUEyMTZBRUU3Mjc
c4Mjk4Rj48QzA5N0VEODkwQkU2QTRDOTFBMjE2QUVFNzI3ODI5OEY+XQo+PgpdZGFydHhyZWYKMjE3Mjc
1CiUlRU9GCg==
</msg:AdditionalFormat>
</msg:DeliveryNotification>

```

## 8 Synchronisation

### 8.1 Definition der Verarbeitungsarten

#### 8.1.1 Synchrone Verarbeitung

Der Terminus „synchron“ bedeutet im Kontext dieses Dokuments, dass ein Webservice-Call direkt als Reaktion auf eine Benutzereingabe ausgeführt wird.

Die Übermittlung einer **MessageOperation** als Reaktion einer Benutzeraktion erfolgt unmittelbar, d.h. der Webservice-Call wird direkt durch die Benutzeraktion ausgelöst. Das GUI wartet jedoch nicht auf die Antwort, stattdessen wird die Abarbeitung des Webservice-Calls in einem eigenständigen Hintergrundprozess ausgeführt.

#### 8.1.2 Asynchrone Verarbeitung

Der Terminus „asynchron“ bedeutet im Kontext dieses Dokuments, dass ein Webservice-Call nicht unmittelbar ausgeführt wird, sondern zeitlich versetzt durch einen Cronjob (Begriffsdefinition siehe unten) ausgelöst wird.

Achtung: Auch bei der asynchronen Webservice-Kommunikation zwischen Zustellsystem und dem Anzeigemodul muss der Aufrufer immer auf eine Webservice-Response warten. Wenn die Antwort nicht eintrifft, war der Webservice-Call nicht erfolgreich und muss wiederholt werden.

Es wird explizit darauf hingewiesen, dass eine „fire-and-forget“-Strategie sowohl im Kontext einer asynchronen als einer synchronen Kommunikation nicht zulässig ist.

#### 8.1.3 Cronjob

Ein Cronjob ist ein Programm, das zeitgesteuert, in definierten periodischen Abständen (z.B. jede Minute) aufgerufen wird, um im Hintergrund automatisch Aufgaben abzuarbeiten.

#### 8.1.4 Retry-Mechanismus

Wenn ein synchroner Webservice-Call auf ein Timeout aufläuft, ohne dass eine Antwort von der Gegenstelle eingetroffen ist, tritt eine Ausnahme- bzw. Fehlersituation ein.

Mittels Cronjob wird der Webservice-Call asynchron so lange wiederholt, bis die Daten erfolgreich zur Gegenstelle übermittelt werden konnten.

Das AMOD hat für die Webservice-Operation **MessageOperation** einen Retry-Mechanismus zu implementieren.

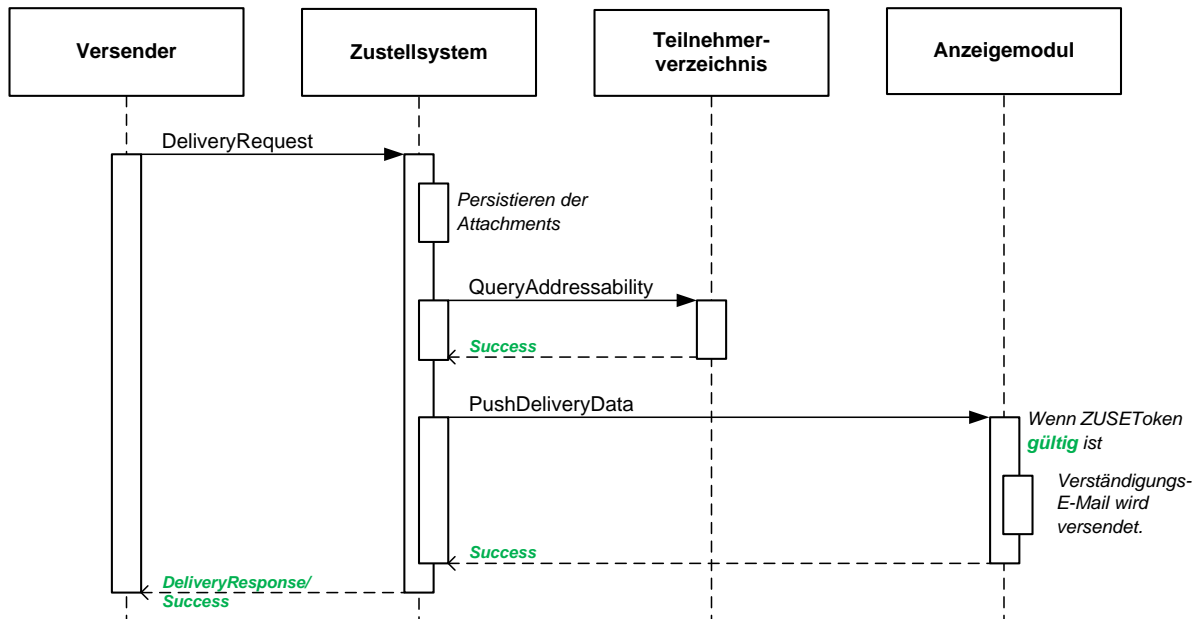
Zustellsysteme haben für die Webservice-Operation **PushDeliveryData** einen Retry-Mechanismus zu implementieren (Details siehe Kapitel 9).

#### 8.1.5 Timeout

Falls bei der Beschreibung der Webservices nicht explizit ein anderer Wert angegeben ist, ist von einem generellen Standardtimeout von **30 Sekunden** auszugehen.

## 8.2 Übermittlung einer Nachricht

Abbildung 18: Sequenzdiagramm zur Übermittlung einer Nachricht

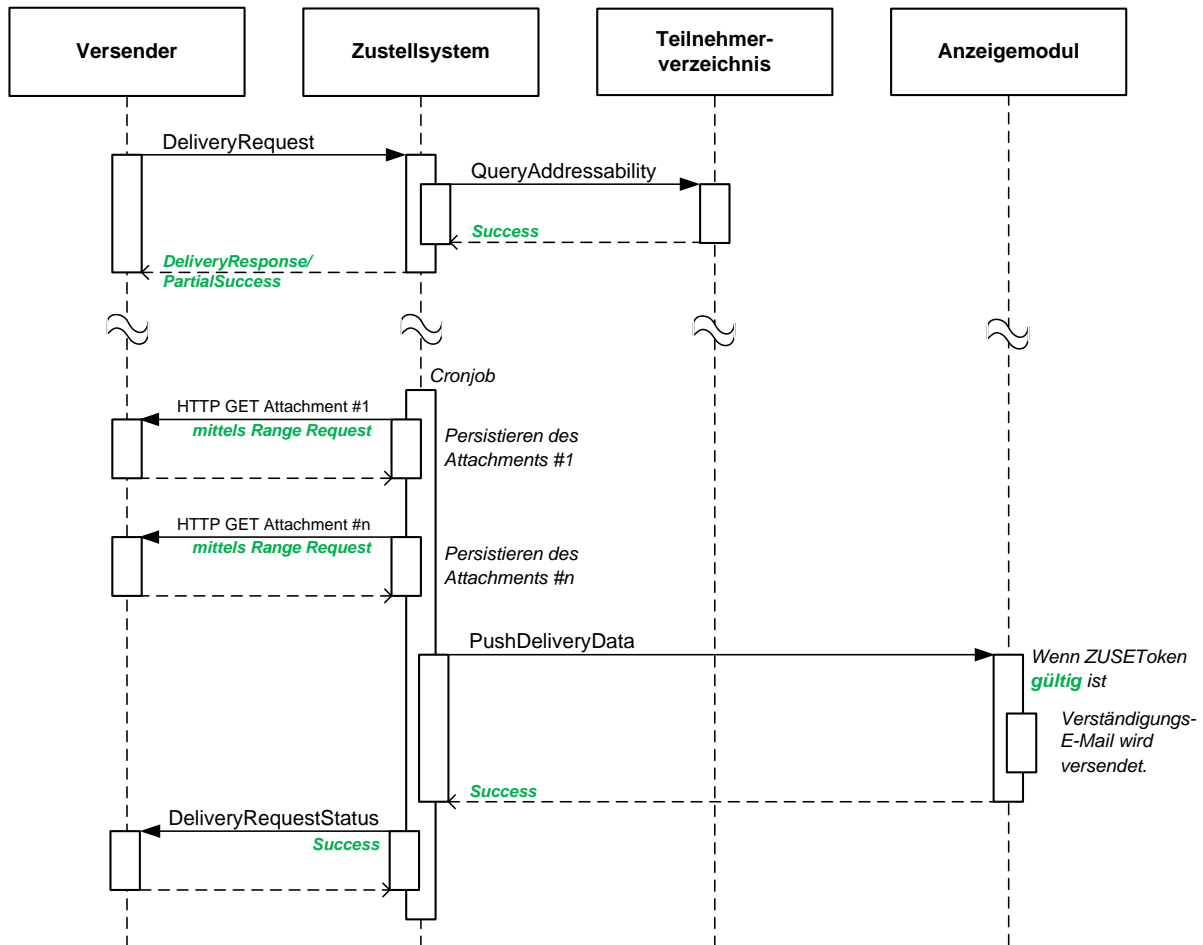


### 8.2.1 Ablauf

1. Der Versender übermittelt die Nachricht inklusive Inline-Attachments mittels **DeliveryRequest** an das Zustellsystem.
2. Das Zustellsystem prüft gemäß Sicherheitsrichtlinie die Attachments auf Schadsoftware und verschlüsselt und persistiert diese für das AMOD.
3. Das Zustellsystem fragt beim TNVZ die Erreichbarkeit des Empfängers mittels **QueryAddressability** ab.
4. Wenn der Empfänger erreichbar ist, meldet das TNVZ den Sucherfolg inklusive verschlüsseltem ZUSEToken an das Zustellsystem zurück.
5. Das Zustellsystem pusht die Metadaten inklusive verschlüsseltem ZUSEToken an das Anzeigemodul (**PushDeliveryData**)
6. Das Anzeigemodul entschlüsselt das ZUSEToken und prüft die Gültigkeit.
7. Wenn das ZUSEToken nicht abgelaufen ist, wird eine E-Mail zur Verständigung des Empfängers versandt.
8. Nach Abschluss der Verarbeitung retourniert das AMOD den **Success** an das Zustellsystem.
9. Das Zustellsystem bestätigt die erfolgreiche Verarbeitung dem Versender.

## 8.3 Asynchrone Übermittlung der Attachments

Abbildung 19: Sequenzdiagramm zur asynchronen Übermittlung der Attachments



### 8.3.1 Ablauf

1. Der Versender übermittelt die Metadaten der Nachricht mittels `DeliveryRequest` an das Zustellsystem
2. Das Zustellsystem fragt beim TNVZ die Erreichbarkeit des Empfängers mittels `QueryAddressability` ab.
3. Wenn der Empfänger erreichbar ist, meldet das TNVZ den Sucherfolg inklusive verschlüsseltem ZUSEToken an das Zustellsystem zurück.
4. Das Zustellsystem gibt dem Versender ein `PartialSuccess` zurück, d.h. es kann zu diesem Zeitpunkt noch nicht bestimmt werden, ob die Nachricht erfolgreich verarbeitet werden kann oder nicht.
5. Asynchron zur Verarbeitung des `DeliveryRequest` via Cronjob holt sich das Zustellsystem mittels HTTP GET unter zur Hilfenahme von Range Requests die einzelnen Attachments vom Versender.
6. Das Zustellsystem prüft gemäß Sicherheitsrichtlinie die Attachments auf Schadsoftware und verschlüsselt und persistiert diese für das AMOD.
7. Das Zustellsystem pusht die Metadaten inklusive verschlüsseltem ZUSEToken an das Anzeigemodul (`PushDeliveryData`).
8. Das Anzeigemodul entschlüsselt das ZUSEToken und prüft die Gültigkeit.

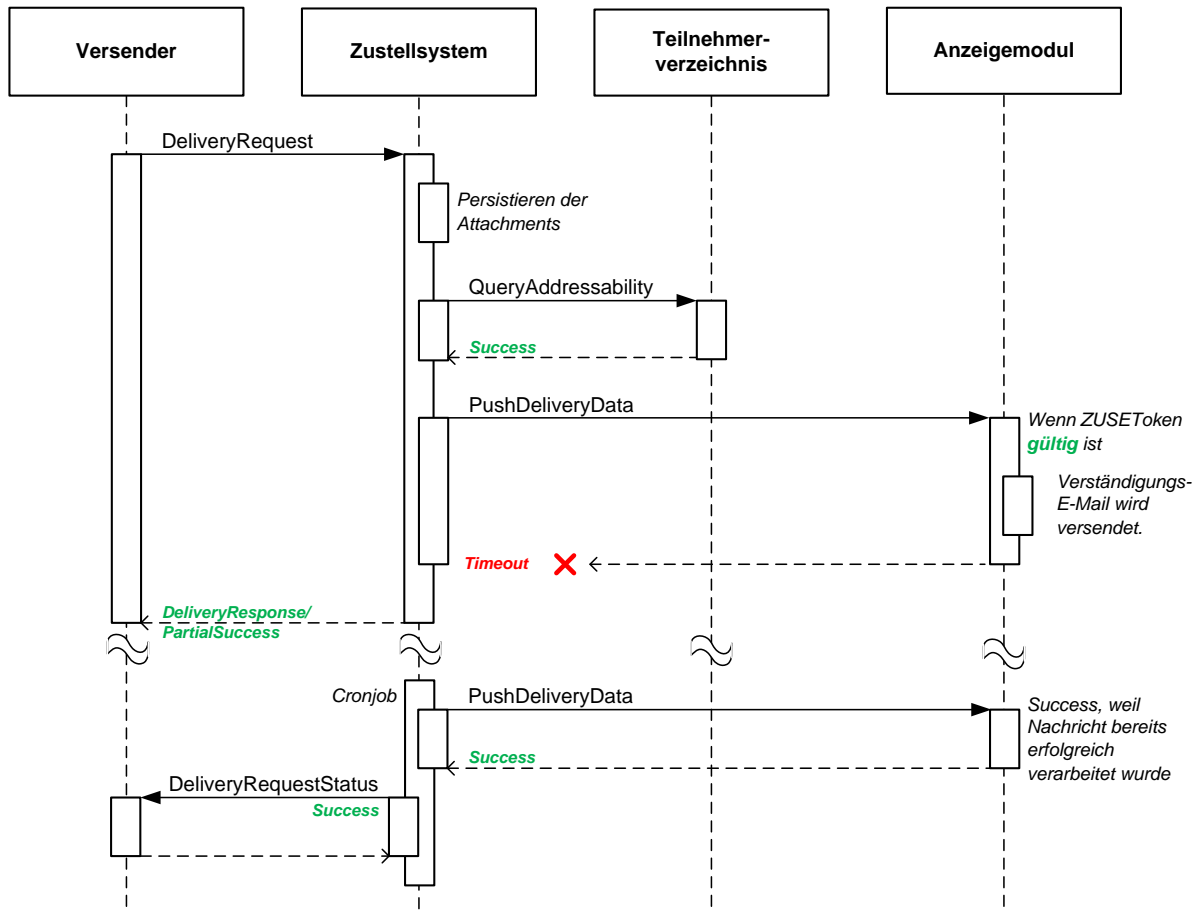


9. Wenn das ZUSEToken nicht abgelaufen ist, wird eine E-Mail zur Verständigung des Empfängers versandt.
10. Nach Abschluss der Verarbeitung retourniert das AMOD den `Success` an das Zustellsystem.
11. Das Zustellsystem ruft mittels `DeliveryRequestStatus` den Versender auf, um diesen die erfolgreiche Verarbeitung zu bestätigen.

## 9 Ausnahmebehandlung

### 9.1 Das Anzeigemodul verarbeitet den Request, der Response erreicht das Zustellsystem nicht

Abbildung 20: Sequenzdiagramm zur Ausnahme „Response erreicht das Zustellsystem nicht“



#### 9.1.1 Ablauf

1. Der Versender übermittelt die Nachricht inklusive Inline-Attachments mittels **DeliveryRequest** an das Zustellsystem.
2. Das Zustellsystem prüft gemäß Sicherheitsrichtlinie die Attachments auf Schadsoftware und verschlüsselt und persistiert diese für das AMOD.
3. Das Zustellsystem fragt beim TNVZ die Erreichbarkeit des Empfängers mittels **QueryAddressability** ab.
4. Wenn der Empfänger erreichbar ist, meldet das TNVZ den Sucherfolg inklusive verschlüsseltem ZUSEToken an das Zustellsystem zurück.
5. Das Zustellsystem pusht die Metadaten inklusive verschlüsseltem ZUSEToken an das Anzeigemodul (**PushDeliveryData**).
6. Das Anzeigemodul entschlüsselt das ZUSEToken und prüft die Gültigkeit.
7. Wenn das ZUSEToken nicht abgelaufen ist, wird eine E-Mail zur Verständigung des Empfängers versandt.
8. Nach Abschluss der Verarbeitung retourniert das AMOD den **Success** an das Zustellsystem.

## Ausnahme

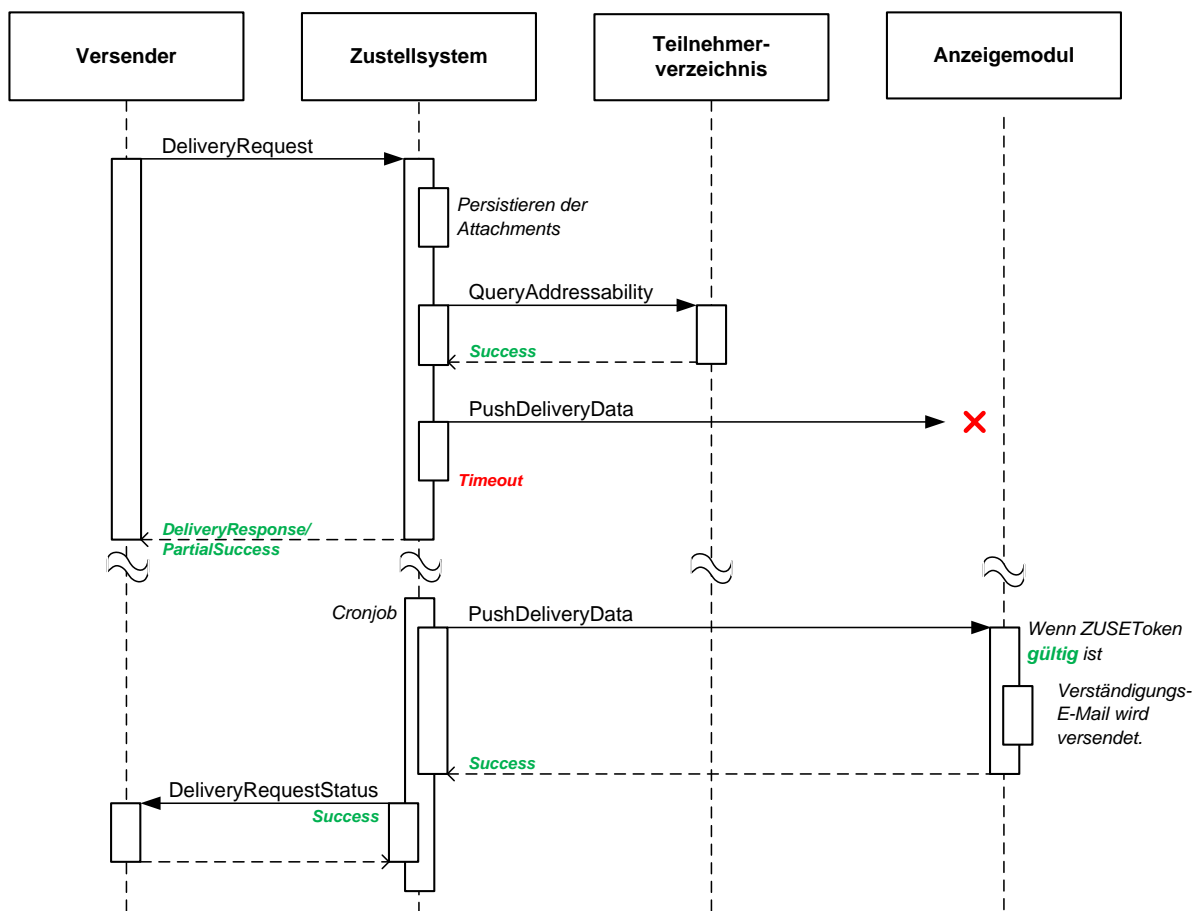
Auf Grund technischer Probleme ist das Zustellsystem temporär nicht mehr erreichbar und erhält die Antwort vom AMOD nicht mehr.

### 9.1.2 Ausnahmebehandlung

1. Nach Wiederanlauf stellt das Zustellsystem fest, dass der Push nicht beantwortet wurde.
2. Das Zustellsystem wiederholt den Push der Metadaten durch Retry des Webservice-Calls `PushDeliveryData`
3. Das AMOD stellt fest, dass es diese Nachricht bereits erfolgreich verarbeitet hat und sendet ohne jede weitere Prüfung einen `Success` zurück.
4. Das Zustellsystem bestätigt die erfolgreiche Verarbeitung dem Versender

## 9.2 Der Request erreicht das Anzeigemodul nicht, der Retry ist erfolgreich

Abbildung 21: Sequenzdiagramm zur Ausnahmebehandlung mit erfolgreichen Retry



### 9.2.1 Ablauf

1. Der Versender übermittelt die Nachricht inklusive Inline-Attachments mittels `DeliveryRequest` an das Zustellsystem.
2. Das Zustellsystem prüft gemäß Sicherheitsrichtlinie die Attachments auf Schadsoftware und verschlüsselt und persistiert diese für das AMOD.
3. Das Zustellsystem fragt beim TNVZ die Erreichbarkeit des Empfängers mittels `QueryAddressability` ab.

4. Wenn der Empfänger erreichbar ist, meldet das TNVZ den Sucherfolg inklusive verschlüsseltem ZUSEToken an das Zustellsystem zurück
5. Das Zustellsystem pusht die Metadaten inklusive verschlüsseltem ZUSEToken an das Anzeigemodul (`PushDeliveryData`)

### **Ausnahme**

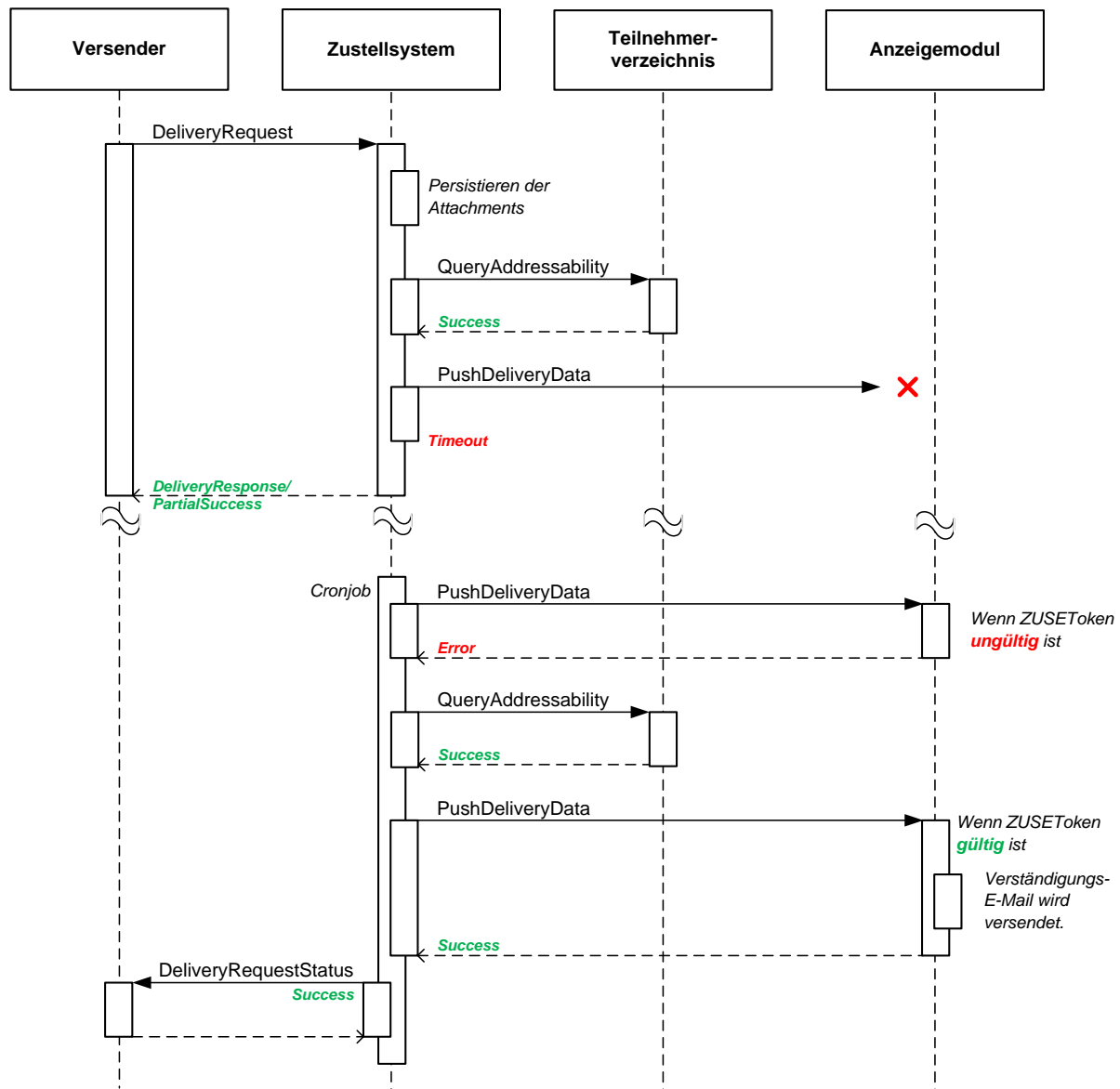
Auf Grund technischer Probleme ist das AMOD temporär nicht erreichbar und der Webservice-Call des Zustellsystems läuft auf ein Timeout.

### **9.2.2 Ausnahmebehandlung**

1. Wenn das Zustellsystem vom AMOD keine Antwort erhält und keine Information darüber hat, ob der Request erfolgreich vom AMOD verarbeitet werden konnte, MUSS es an den Versender einen `PartialSuccess` zurückmelden.
2. Asynchron und in periodischen Abständen MUSS das Zustellsystem via Cronjob den Push der Metadaten an das AMOD so lange wiederholen, bis es eine Antwort vom AMOD erhält.
3. Erreicht es das AMOD wieder und antwortet dieses mit `Success`, ruft das Zustellsystem mittels `DeliveryRequestStatus` den Versender auf, um diesen die erfolgreiche Verarbeitung zu bestätigen.

### 9.3 Der Request erreicht das Anzeigemodul nicht, der Retry inklusive Teilnehmerverzeichnisabfrage sind erfolgreich

Abbildung 22: Sequenzdiagramm zur Ausnahmebehandlung „Empfänger wiederholt erreichbar“



#### 9.3.1 Ablauf

1. Der Versender übermittelt die Nachricht inklusive Inline-Attachments mittels `DeliveryRequest` an das Zustellsystem.
4. Das Zustellsystem prüft gemäß Sicherheitsrichtlinie die Attachments auf Schadsoftware und verschlüsselt und persistiert diese für das AMOD.
5. Das Zustellsystem fragt beim TNVZ die Erreichbarkeit des Empfängers mittels `QueryAddressability` ab.
6. Wenn der Empfänger erreichbar ist, meldet das TNVZ den Sucherfolg inklusive verschlüsseltem ZUSEToken an das Zustellsystem zurück
7. Das Zustellsystem pusht die Metadaten inklusive verschlüsseltem ZUSEToken an das Anzeigemodul (`PushDeliveryData`)

## Ausnahme

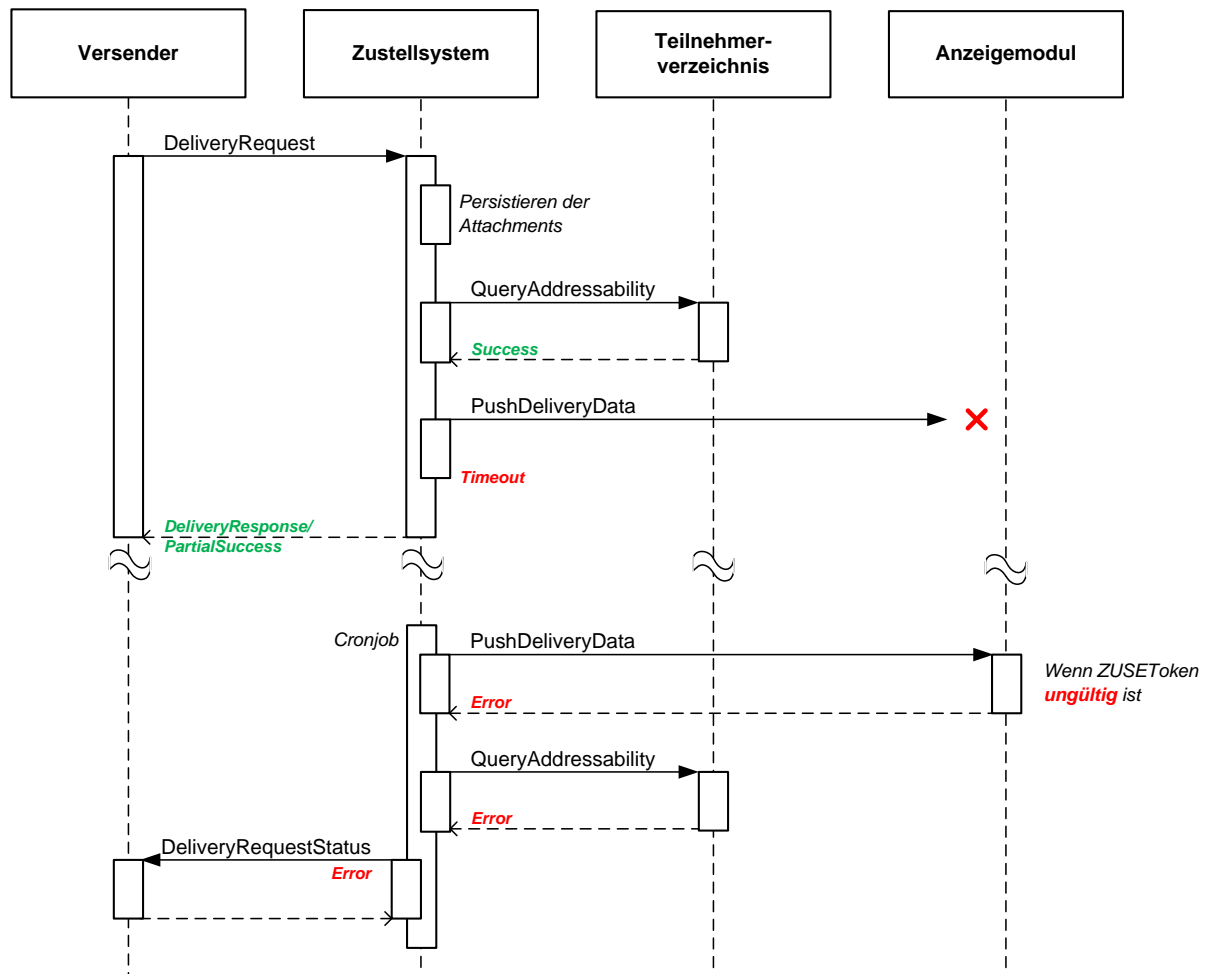
Auf Grund technischer Probleme ist das AMOD temporär nicht erreichbar und der Webservice-Call des Zustellsystems läuft auf ein Timeout.

### 9.3.2 Positive Ausnahmebehandlung

1. Wenn das Zustellsystem vom AMOD keine Antwort erhält und keine Information darüber hat, ob der Request erfolgreich vom AMOD verarbeitet werden konnte, MUSS es an den Versender einen `PartialSuccess` zurückmelden.
2. Asynchron und in periodischen Abständen MUSS das Zustellsystem via Cronjob den Push der Metadaten an das AMOD so lange wiederholen, bis es eine Antwort vom AMOD erhält.
3. Das Zustellsystem kann bei der Wiederholung erfolgreich die Metadaten an das AMOD pushen.
4. Das AMOD kennt die Nachricht nicht und prüft das ZUSEToken.
5. Die Gültigkeit des ZUSEToken ist abgelaufen.
6. Das AMOD gibt eine entsprechende Fehlermeldung an das Zustellsystem zurück.
  - Hinweis: auch wenn dem Zustellsystem klar ist, dass das ZUSEToken nicht mehr gültig sein kann, MUSS es in der Ausnahmesituation zuerst die Gültigkeit vom AMOD prüfen lassen, bevor es ein neues ZUSEToken beim TNVZ anfordert.
7. Das Zustellsystem fragt beim TNVZ erneut die Erreichbarkeit des Empfängers mittels `QueryAddressability` ab.
8. Der Empfänger ist weiterhin mehr erreichbar (keine Abwesenheit oder Abmeldung von der E-Zustellung). Das TNVZ gibt einen Fehler zurück.
9. Wenn der Empfänger weiterhin erreichbar ist, meldet das TNVZ den Sucherfolg inklusive verschlüsseltem ZUSEToken an das Zustellsystem zurück
10. Das Zustellsystem pusht die Metadaten inklusive verschlüsseltem ZUSEToken an das Anzeigemodul (`PushDeliveryData`)
11. Das Anzeigemodul entschlüsselt das ZUSEToken und prüft die Gültigkeit.
12. Wenn das ZUSEToken nicht abgelaufen ist, wird eine E-Mail zur Verständigung des Empfängers versandt.
13. Nach Abschluss der Verarbeitung retourniert das AMOD den `Success` an das Zustellsystem.
14. Das Zustellsystem ruft mittels `DeliveryRequestStatus` den Versender auf, um diesen die erfolgreiche Verarbeitung zu bestätigen.

## 9.4 Der Request erreicht das Anzeigemodul nicht, beim Retry ist der Empfänger nicht mehr erreichbar

Abbildung 23: Sequenzdiagramm zur Ausnahmebehandlung „Empfänger nicht mehr erreichbar“



### 9.4.1 Ablauf

1. Der Versender übermittelt die Nachricht inklusive Inline-Attachments mittels `DeliveryRequest` an das Zustellsystem.
2. Das Zustellsystem prüft gemäß Sicherheitsrichtlinie die Attachments auf Schadsoftware und verschlüsselt und persistiert diese für das AMOD.
3. Das Zustellsystem fragt beim TNVZ die Erreichbarkeit des Empfängers mittels `QueryAddressability` ab.
4. Wenn der Empfänger erreichbar ist, meldet das TNVZ den Sucherfolg inklusive verschlüsseltem ZUSEToken an das Zustellsystem zurück.
5. Das Zustellsystem pusht die Metadaten inklusive verschlüsseltem ZUSEToken an das Anzeigemodul (`PushDeliveryData`).

#### Ausnahme

Auf Grund technischer Probleme ist das AMOD temporär nicht erreichbar und der Webservice-Call des Zustellsystems läuft auf ein Timeout.

### 9.4.2 Negative Ausnahmebehandlung

1. Wenn das Zustellsystem vom AMOD keine Antwort erhält und keine Information darüber hat, ob der Request erfolgreich vom AMOD verarbeitet werden konnte, MUSS es an den Versender einen PartialSuccess zurückmelden.
2. Asynchron und in periodischen Abständen MUSS das Zustellsystem via Cronjob den Push der Metadaten an das AMOD so lange wiederholen, bis es eine Antwort vom AMOD erhält.
3. Das Zustellsystem kann bei der Wiederholung erfolgreich die Metadaten an das AMOD pushen.
4. Das AMOD kennt die Nachricht nicht und prüft das ZUSEToken.
5. Die Gültigkeit des ZUSEToken ist abgelaufen.
6. Das AMOD gibt eine entsprechende Fehlermeldung an das Zustellsystem zurück.
  - Hinweis: auch wenn dem Zustellsystem klar ist, dass das ZUSEToken nicht mehr gültig sein kann, MUSS es in der Ausnahmesituation zuerst die Gültigkeit vom AMOD prüfen lassen, bevor es ein neues ZUSEToken beim TNVZ anfordert.
7. Das Zustellsystem fragt beim TNVZ erneut die Erreichbarkeit des Empfängers mittels `QueryAddressability` ab.
8. Der Empfänger ist nicht mehr erreichbar (Abwesenheit oder Abmeldung von der E-Zustellung). Das TNVZ gibt einen Fehler zurück.
9. Das Zustellsystem ruft mittels `DeliveryRequestStatus` den Versender auf, um diesen über den gescheiterten bzw. fehlerhaften Zustellversuch zu informieren.



## 10 Betriebsüberwachung

Um die geforderte hohe Verfügbarkeit der E-Zustellung sicherstellen zu können, um rasch Ausfälle oder Verbindungsprobleme einzelner Systemkomponenten automatisiert erkennen zu können, haben die Zustellsysteme und das Anzeigemodul die Möglichkeit sich gegenseitig mit Hilfe der Webservice Operationen `IsAlive` bzw. `IsAliveEcho` zu überwachen.

Im Sinne eines 4-Augen-Prinzips ist es das Ziel, dass sich die Betriebsteams der Zustellsysteme und des Anzeigemoduls gegenseitig bei der Betriebsüberwachung unterstützen.

### 10.1 Cronjob `IsAlive` des Anzeigemoduls

Das Anzeigemodul ruft mittels Cronjob in periodischen Abständen „round-robin“ bei allen angeschlossenen Zustellsystemen die Webservice-Operation `IsAlive` auf.

Der Cronjob setzt **jede Minute** pro Zustellsystem einen Webservice-Call `IsAlive` ab (Timeout = **30 Sekunden**) um zu überprüfen, ob das Zustellsystem erreichbar ist.

### 10.2 Cronjob `IsAlive` der Zustellsysteme

Die Zustellsysteme haben einen Cronjob zu implementieren, der periodisch die Webservice-Verbindung zum Anzeigemodul testet.

Bekommt das Zustellsystem keine Antwort vom Anzeigemodul, ist davon auszugehen, dass die Verbindung unterbrochen ist. In diesem Fall MUSS das Zustellsystem den `msg:DeliveryRequests` von seinen Kunden mit einem Fehler quittieren.

Wenn das Anzeigemodul wieder auf die Webservice-Calls `IsAlive` antwortet, ist der Push der Metadaten wieder zu aktivieren.

Der Cronjob setzt **jede Minute** einen Webservice-Call `IsAlive` ab (Timeout = **30 Sekunden**) um zu überprüfen, ob das Anzeigemodul erreichbar ist.

Das `amod:Token` Element DARF NICHT gesetzt werden.

### 10.3 Cronjob `IsAliveEcho`

Mit Hilfe des Cronjob `IsAliveEcho` werden die Webservice-Verbindungen in beide Richtungen durch das Anzeigemodul automatisiert geprüft.

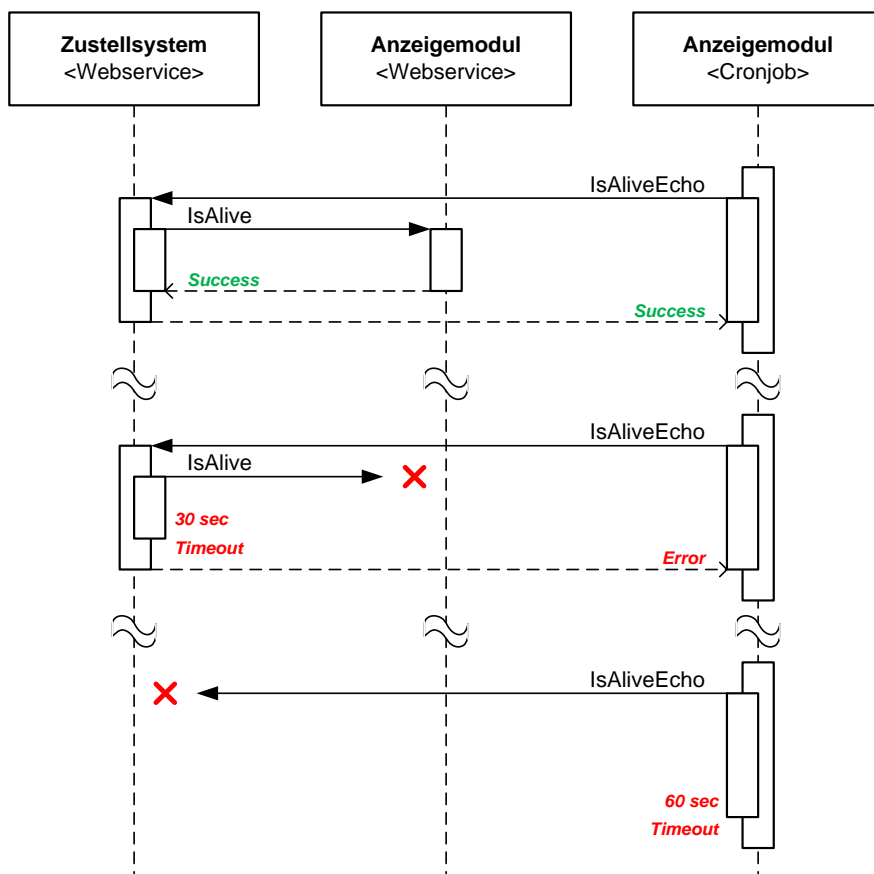
Das Anzeigemodul testet die mittels Webservice-Call `IsAliveEcho` die Verbindung zwischen Anzeigemodul und Zustellsystem.

Wenn das Zustellsystem einen `amod:IsAliveEchoRequest` empfängt, hat es von seiner Seite mittels Webservice-Call `IsAlive` die Verbindung zwischen Zustellsystem und Anzeigemodul zu testen.

Wenn der Webservice-Call `IsAlive` des Zustellsystems auf ein Timeout aufläuft, muss das Zustellsystem einen Fehler an das Anzeigemodul zurückgegeben.

Wenn der Verbindungstest mit `IsAlive` erfolgreich war, wird ein `amod:IsAliveEchoResponse/amod:Success` an das Anzeigemodul zurückgemeldet.

Abbildung 24: Sequenzdiagramm „IsAliveEcho“



## 10.4 XML Format und Binding

Dieser Abschnitt beschreibt Anfragen (Request) bzw. Antworten (Response) für die Betriebsüberwachungsfunktionen IsAlive und IsAliveEcho.

### 10.4.1 Authentifizierung

Die Authentifizierung der Zustellsysteme gegenüber dem Anwendungsportal des Anzeigemoduls muss gemäß den Vorgaben aus Abschnitt 1.2 erfolgen.

Es muss vom Portal des Zustellsystems folgende Rolle übermittelt werden:

- Anzeigemodul: ZUSE-DISPLAY-SERVICE
- Zustellsysteme: ZUSE-DELIVERY-SERVICE

Beispiel für die zu setzenden PVP 2.1 Http-Header eines Zustellsystems:

```

POST /abc.gv.at/anwendung2/xyz HTTP/1.1
Host:zustellsystem.at
User-Agent: .JNET 1.1
X-PVP-VERSION: 2.1
X-PVP-BINDING: http
X-PVP-PARTICIPANT-ID: AT:VKZ:XFN-999999x
X-PVP-USERID: support@zustellsystem.at
X-PVP-PRINCIPALNAME: Zustellsystem GmbH
X-PVP-SECCLASS: 2
X-PVP-ROLES: ZUSE-DELIVERY-SERVICE
Content-Type: text/xml
Content-Length: 788
  
```

### 10.4.2 Format

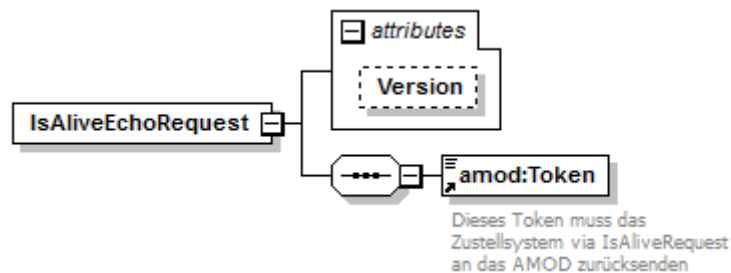
#### 10.4.2.1 Operation IsAliveEcho

Die Webservice Operation `IsAliveEcho` ist nur vom Anzeigemodul zu implementieren und dient dem Verbindungstest zwischen Anzeigemodul und Zustellsystem

#### 10.4.2.1.1 Request

Das Anzeigemodul gibt im Request immer ein `amod:Token` Element mit. Das Zustellsystem muss synchron von seiner Seite mittels Operation `IsAlive` die Verbindung zwischen Zustellsystem und Anzeigemodul testen. Bei diesem Aufruf MUSS das gegenständige Token übergeben werden.

Abbildung 25 – Struktur des `amod:IsAliveEchoRequest` Elements



#### 10.4.2.1.2 Response

Das Zustellsystem wartet auf die Antwort des Webservice-Calls `IsAlive`.

Wenn der Verbindungstest erfolgreich war, retourniert das Anzeigemodul ein `amod:Answer` Element. Dieses `amod:Answer` Element muss das Zustellsystem im `amod:IsAliveEchoResponse/amod:Success` Element wieder zurück an das Anzeigemodul transferieren.

Wenn der Verbindungstest nicht erfolgreich war, weil der Webservice-Call `IsAlive` auf einen Timeout aufgelaufen ist, ist eine Fehlermeldung zu retournieren.

Abbildung 26 – Struktur des `amod:IsAliveEchoResponse` Elements

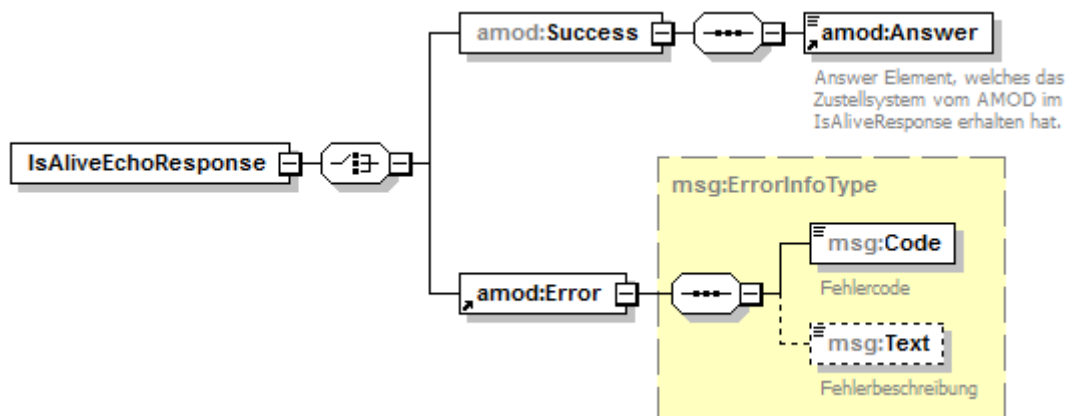


Tabelle 12 – `IsAliveEcho` Fehlercodes vom Zustellsystem

Code	Error-Message	Beschreibung
ZS0403_U	Not permitted	Operation ist nicht zulässig
ZS0500_R	Internal Server Error	Interner Fehler

Code	Error-Message	Beschreibung
ZS0504_R	Gateway Timeout	Das Zustellsystem konnte seine Funktion als Gateway oder Proxy nicht erfüllen, weil es innerhalb einer festgelegten Zeitspanne keine Antwort vom AMOD auf den <code>IsAliveRequest</code> erhalten hat.
ZS1202_U	Propagate error messages "token is invalid"	Die Fehlermeldung des AMOD auf den <code>IsAliveRequest</code> wird weiterpropagiert

#### 10.4.2.2 Operation *IsAlive*

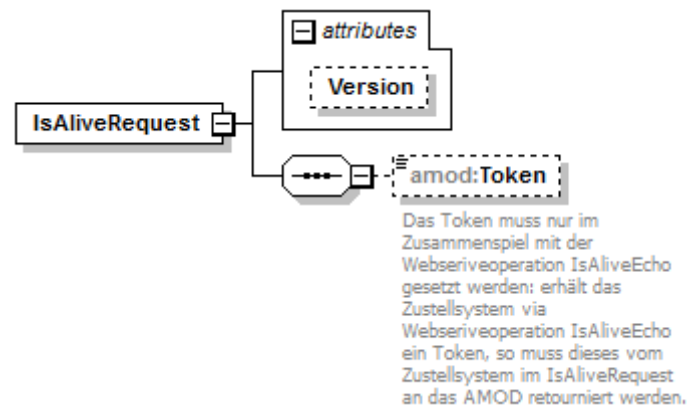
Die Webservice Operation `IsAlive` steht sowohl dem Anzeigemodul als auch allen Zustellsystemen zur Verfügung.

##### 10.4.2.2.1 Request

Wenn das Zustellsystem von sich aus die Verbindung zwischen Zustellsystem und Anzeigemodul testen will, muss kein `amod:Token` Element übergeben werden.

Wenn die Operation `IsAlive` im Zuge der Verarbeitung der Operation `IsAliveEcho` aufgerufen wird, so MUSS das vom Anzeigemodul übermittelte `amod:Token` Element übergeben werden.

Abbildung 27 – Struktur des `amod:IsAliveRequest` Elements



##### 10.4.2.2.2 Response

Wenn im Request das `amod:Token` Element gesetzt war, liefert das Anzeigemodul im `amod:IsAliveResponse/amod:Success` Element ein `amod:Answer` Element zurück.

Konnte das Anzeigemodul das `amod:Token` Element nicht auswerten, wird eine Fehlermeldung retourniert.

Abbildung 28 – Struktur des amod:IsAliveResponse Elements

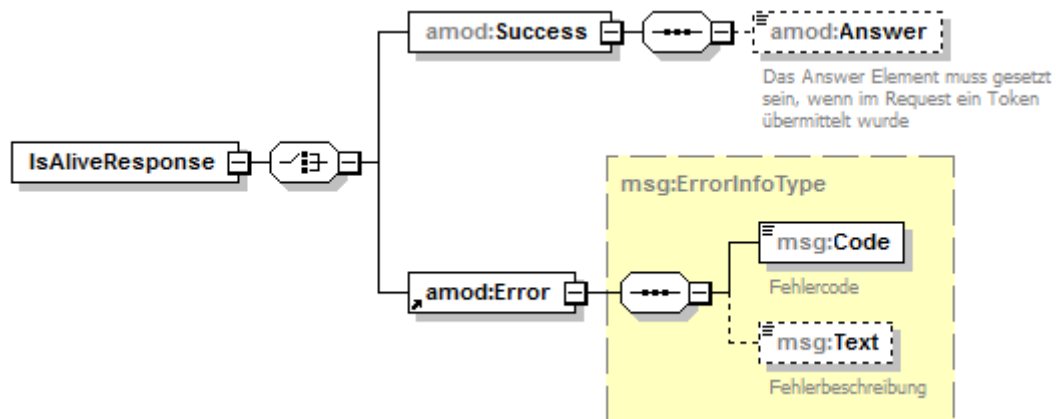


Tabelle 13 – IsAlive Fehlercodes vom Anzeigemodul

Code	Error-Message	Beschreibung
AM0403_U	Not permitted	Operation ist nicht zulässig
AM0500_R	Internal Server Error	Interner Fehler
AM1201_U	Token is invalid	Das vom Zustellsystem übergebene Token ist ungültig

Tabelle 14 – IsAlive Fehlercodes vom Zustellsystem

Code	Error-Message	Beschreibung
ZS0403_U	Not permitted	Operation ist nicht zulässig
ZS0500_R	Internal Server Error	Interner Fehler

### 10.4.3 Binding

#### 10.4.3.1 SOAP

Für den Datenaustausch MUSS das Netzwerkprotokoll SOAP in der Version 1.2 über das HTTP Binding in [SOAP12] verwendet werden.

Sämtliche Kommunikation muss gesichert gemäß den Anforderungen in Abschnitt 3.2.1.1 erfolgen.

Die entsprechende WSDL-Beschreibung ist als gesonderte Datei der Spezifikation beigelegt.

- zuse2amod\_p2.wsdl
- amod2zuse\_p2.wsdl

#### 10.4.3.2 REST

Zusätzlich muss für die IsAlive-Funktion auch eine GET REST Ressource „/is\_alive“ von den Zustellsystemen implementiert werden, damit auch die Erreichbarkeit der HTTP

Schnittstelle für den Attachment Download geprüft werden kann. Hier ist im Erfolgsfall eine leere Response und der Statuscode 204 zu retournieren.

Diese Ressource wird, wie die SOAP-Webservices, periodisch durch einen Cronjob geprüft.

## 11 Protokollierung

### 11.1 *Löschfrist für fachliche Protokollierungsdaten des Anzeige-moduls*

Fachliche Protokollierungsdaten werden nach 3 Jahren gelöscht. Folgende Daten werden protokolliert:

- Adressierungsdaten
  - Personendaten des Senders
  - Personendaten des Empfängers
- Metadaten der Nachricht (u.a.)
  - Nachrichten-IDs
  - Geschäftszahl (GZ)
  - Betreff
- Nachrichtenereignisse
  - „Nachricht eingetroffen“
  - „Zustellhindernis“
  - „Eintritt der Zustellfiktion“
  - etc.
- Zugriffsdaten
  - Eindeutige Benutzerkennung
  - Benutzeraktionen wie beispielsweise „Nachricht angenommen“, „Nachricht gelesen“ oder „Nachricht gelöscht“

Präzisierung der Löszeitpunkte

Nach dem Löschen der Nachricht werden die folgenden fachlichen Protokollierungsdaten 3 Jahre nach dem Einlangen der Nachricht (Zeitpunkt der Übermittlung) gelöscht:

- Adressierungsdaten
- Daten zur Identifizierung der Nachricht
- Nachrichtenereignisse

Zugriffsdaten werden 3 Jahren nach dem Anlegen des Zugriffsprotokolleintrags gelöscht.

## A. Anhang

### 11.2 Beispiel: Blockweise Übertragung von Attachments

Das Anzeigemodul holt Attachments IMMER mit Hilfe von Range-Request beim Zustellsystem ab. Im Folgenden ist die HTTP-Kommunikation zwischen dem Anzeigemodul und dem Zustellsystem für ein Attachment bestehend aus zwei Blöcken skizziert.

Das Anzeigemodul fordert den ersten Block des Attachments an Beispiel eines Requests:

```
GET /attachment?delivery_id=123456&attachment_id=9493b96d-7501-4c87-810e-8d42a64a8c79&identifizier=ABC&identifizier_type=bPK HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
Cache-Control: no-cache
Connection: keep-alive
Cookie: AMODJSESSIONID=AD88E2026B1D7FCD819FBFA1486FB556
Expires: Mon, 1 Jan 1990 00:00:00 GMT
Host: MeinZustellsystem.at
Referer: http://amod.mpk.qv.at/amod-frontend/portal/main/

Pragma: no-cache
Range: bytes=0-500000

uuid: 9493b96d-7501-4c87-810e-8d42a64a8c79
x-pvp-birthdate: 1980-01-01
x-pvp-bpk: ZU:NEK/9ZsnA7e2phK71F/OSdIjwbU=
x-pvp-given-name: Max
x-pvp-ou: Bundesministerium fuer Finanzen
x-pvp-participant-id: AT:B:115-USP
x-pvp-principal-name: Mustermann
x-pvp-roles: ZUSE-DISPLAY-SERVICE (AUTH-LEVEL=E-ID)
x-pvp-secclass: 2
x-pvp-userid: xxxxx.xxxxxx@bmf.gv.at
x-pvp-version: 2.1
```

Beispiel einer erfolgreichen Response:

```
HTTP/1.1 206 Partial Content

Request URL: http://localhost/attachment
Request Method: GET
Status Code: 206 Partial Content
Remote Address: [::1]:80
Referrer Policy: no-referrer-when-downgrade

Accept-Ranges: bytes
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type,
Accept
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-length, Content-Size, Etag, uuid
Access-Control-Request-Methods: GET

Content-Disposition: inline;filename="Bescheid.pdf"
Content-Type: application/pdf
Content-Length: 500001
Content-Range: bytes 0-500000/721682
Content-Size: 721682
Content-Start: 0

Date: Thu, 26 Apr 2018 07:45:55 GMT
ETag: Bescheid.pdf
Expires: Thu, 03 May 2018 07:45:55 GMT
Server: Apache-Coyote/1.1

uuid: 9493b96d-7501-4c87-810e-8d42a64a8c79

ZSDeliveryID: 123456
ChecksumAlgorithm: SHA256
ChecksumValue: ABCDEF=
(Erster Teil des Inhalts von Bescheid.pdf)
```

Das Anzeigemodul fordert den zweiten und letzten Block des Attachments an



**Beispiel eines Requests:**

```

GET /attachment?delivery id=123456&attachment id=9493b96d-7501-4c87-810e-
8d42a64a8c79&identifizier=ABC&identifizier type=bPK HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
Cache-Control: no-cache
Connection: keep-alive
Cookie: AMODJSESSIONID=AD88E2026B1D7FCD819FBFA1486FB556
Expires: Mon, 1 Jan 1990 00:00:00 GMT
Host: MeinZustellsystem.at
Referer: http://amod.mpk.gv.at/amod-frontend/portal/main/

Pragma: no-cache

Range: bytes=500001-721681

uuid: 9493b96d-7501-4c87-810e-8d42a64a8c79

x-pvp-birthdate: 1980-01-01
x-pvp-bpk: ZU:NEK/9ZsnA7e2phK71F/OSdIjwbU=
x-pvp-given-name: Max
x-pvp-ou: Bundesministerium fuer Finanzen
x-pvp-participant-id: AT:B:115-USP
x-pvp-principal-name: Mustermann
x-pvp-roles: ZUSE-DISPLAY-SERVICE (AUTH-LEVEL=E-ID)
x-pvp-secclass: 2
x-pvp-userid: xxxxx.xxxxx@bmf.gv.at
x-pvp-version: 2.1

```

**Beispiel einer erfolgreichen Response:**

```

HTTP/1.1 206 Partial Content

Request URL: http://localhost/attachment
Request Method: GET
Status Code: 206 Partial Content
Remote Address: [::1]:80
Referrer Policy: no-referrer-when-downgrade

Accept-Ranges: bytes
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type,
Accept
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: Content-length, Content-Size, Etag, uuid
Access-Control-Request-Methods: GET

Content-Disposition: inline;filename="Bescheid.pdf"
Content-Type: application/pdf
Content-Range: bytes 500001-721681/721682
Content-Size: 721682
Content-Start: 0

Date: Thu, 26 Apr 2018 07:45:55 GMT
ETag: Bescheid.pdf
Expires: Thu, 03 May 2018 07:45:55 GMT
Server: Apache-Coyote/1.1

uuid: 9493b96d-7501-4c87-810e-8d42a64a8c79

ZSDeliveryID: 123456
ChecksumAlgorithm: SHA256
ChecksumValue: ABCDEF=
(Zweiter und letzter Teil des Inhalts von Bescheid.pdf)

```

## B. Abbildungsverzeichnis

Abbildung 1 – Struktur des <code>amod:PushDeliveryDataRequest</code> Elements .....	53
Abbildung 2 – Struktur des <code>amod:Sender</code> Elements .....	54
Abbildung 3 – Struktur des <code>amod:Receiver</code> Elements .....	55
Abbildung 4 – Struktur des <code>amod:MetaData</code> Elements .....	57
Abbildung 5 – Struktur des <code>msg:MetadataList</code> Elements .....	58
Abbildung 6 – Struktur des <code>amod:Attachment</code> Elements .....	59
Abbildung 7 – Struktur des <code>amod:PushDeliveryDataResponse</code> Elements .....	61
Abbildung 8 – Zustandsübergangsdiagramm für Zustellungen bzw. Zusendungen ohne Zustellnachweis .....	68
Abbildung 9 – Zustandsübergangsdiagramm für Zustellungen bzw. Zusendungen mit Zustellnachweis .....	69
Abbildung 10 – Zustandsübergangsdiagramm bei Weiterleitung in den ERV .....	71
Abbildung 11 – Struktur des <code>amod:MessageOperationRequest</code> Elements .....	73
Abbildung 12 – Struktur des <code>msg:User</code> Elements .....	75
Abbildung 13 – Struktur des <code>amod:Operation</code> Elements .....	77
Abbildung 14 – Struktur des <code>amod:MessageOperationResponse</code> Elements .....	81
Abbildung 15 – Struktur des <code>amod:MessageCountRequest</code> Elements .....	95
Abbildung 16 – Struktur des <code>amod:MessageCountResponse</code> Elements .....	95
Abbildung 17 – Weiterleitung einer RSa-Zustellung in den ERV .....	96
Abbildung 18: Sequenzdiagramm zur Übermittlung einer Nachricht .....	103
Abbildung 19: Sequenzdiagramm zur asynchronen Übermittlung der Attachments .....	104
Abbildung 20: Sequenzdiagramm zur Ausnahme „Response erreicht das Zustellsystem nicht“ .....	106
Abbildung 21: Sequenzdiagramm zur Ausnahmebehandlung mit erfolgreichen Retry .....	107
Abbildung 22: Sequenzdiagramm zur Ausnahmebehandlung „Empfänger wiederholt erreichbar“ .....	109
Abbildung 23: Sequenzdiagramm zur Ausnahmebehandlung „Empfänger nicht mehr erreichbar“ .....	111
Abbildung 24: Sequenzdiagramm „IsAliveEcho“ .....	114
Abbildung 25 – Struktur des <code>amod:IsAliveEchoRequest</code> Elements .....	115
Abbildung 26 – Struktur des <code>amod:IsAliveEchoResponse</code> Elements .....	115
Abbildung 27 – Struktur des <code>amod:IsAliveRequest</code> Elements .....	116
Abbildung 28 – Struktur des <code>amod:IsAliveResponse</code> Elements .....	117

## C. Tabellenverzeichnis

Tabelle 1 - Namespaces.....	10
Tabelle 2 – Fehler-Codes im Nichterfolgsfall .....	61
Tabelle 3 – Codes, die das Anzeigemodul zurückmeldet.....	79
Tabelle 4 – Fehlermeldungen für Message Operations, die das Zustellsystem zurückliefert .....	82
Tabelle 5 – Verpflichtende HTTP Argumente für Abholung eines Attachments .....	84
Tabelle 6 – Verpflichtende HTTP Request Header für Abholung eines Attachments .....	84
Tabelle 7 – Verpflichtende HTTP Response Header für Abholung eines Attachments im Erfolgsfall.....	85
Tabelle 8 – Verpflichtende HTTP Response Header für Abholung eines Attachments im Fehlerfall.....	85
Tabelle 9 – Fehler-Codes im Nichterfolgsfall .....	86
Tabelle 10: Liste der PVP2-Header für E-Government-Portale.....	87
Tabelle 11: Liste der PVP2-Header für Behördenportale .....	92
Tabelle 12 – IsAliveEcho Fehlercodes vom Zustellsystem .....	115
Tabelle 13 – IsAlive Fehlercodes vom Anzeigemodul.....	117
Tabelle 14 – IsAlive Fehlercodes vom Zustellsystem .....	117

## D. Revision History

Version	Datum	Autor(en)	
2.4.0	XX.XX.2024	Tauber A.	<p>Der Begriff „Zielserver“ wurde auf „sendender E-Mail-Server“ umbenannt</p> <p>URL-Action-Links müssen nun wie unter 3.2.1.2.1. Anhänge beschrieben übergeben werden</p> <p>Aufgrund der Aufteilung des Ergänzungsregisters für sonstige Betroffene (ERsB) in vier einzelne Stammregister wurde der neue übergeordnete Stammzahlentyp <b>Global Location Number</b> (urn:publicid:gv.at:baseid+XGLN) etabliert, der die Ordnungsnummer des ERsB (urn:publicid:gv.at:baseid+XERSB) innerhalb der Elektronischen Zustellung ersetzt</p> <p>Im Header X-PVP-ROLES ist eine Anpassung des Präfixes des Stammzahlenwerts erforderlich. Anstelle des bisherigen Präfixes "XERSB-" ist zukünftig das Präfix "XGLN-" zu verwenden. Dies betrifft die beiden Rollenparameter <code>Stammzahl</code> und <code>SOURCE</code>, die in den Rollen <code>MPK_POSTBEVOLLMAECHTIGTER</code> und <code>MPK_REGISTRIERUNG</code> zum Einsatz kommen</p> <p>Im Kapitel 3.2.1.1 und 4.3.1.1 Authentifizierung wurde die Referenz korrigiert und auf die beiden Authentifizierungsvarianten im Detail eingegangen</p> <p>Definition von XML SimpleTypes im Namespace <code>http://reference.e-government.gv.at/namespace/zustellung/types/phase2/20240718#</code>, um die Feldlängen automatisiert prüfen zu können</p> <p>Das als „deprecated“ gekennzeichnete Element <code>msg:ERVDeliveryTimestamp</code> wurde aus dem XML-Schema entfernt</p> <p>Klarstellungen in Formulierungen, Abbildungen und Beispielen, sowie Korrekturen</p> <p>Kennzeichnung des HTTP Response-Headers „Content-Length“ als optional statt verpflichtend (siehe Tabelle 7 und Tabelle 8)</p> <p>Neues <code>SubjectKeyIdentifier</code> Attribut in den Attachment-Metadaten, um den öffentlichen Schlüssel des AMOD X.509 v3 Zertifikats eindeutig identifizieren zu können, mit dem der symmetrische Sessionkey verschlüsselt wurde</p> <p>Neuer Fehlercode <code>ZS0400_U</code> „Bad Request“ für den Fall, dass die Message Operation eindeutig im Widerspruch zur aktuellen Verarbeitung der Nachricht steht</p>
2.3.0	09.11.2023	Tauber A.	<p>E-Mail-Adressen (<code>msg:InternetAddress</code>) in der Liste der elektronischen Verständigungsadressen (<code>msg:NotificationAddressList</code>), werden als „ungültig“ markiert (<code>Invalid="true"</code>), wenn der Zielserver entweder nicht erreichbar war oder mit einer Bounce-Message geantwortet hat</p> <p>Das AMOD retourniert bei nachweislichen und nicht nachweislichen Zustellungen und Zusendungen die Nachrichtenoperation „<i>NotificationInformation</i>“, um das Zustellsystem über erfolgreiche und/oder fehlerhafte elektronische Verständigungen zu informieren</p> <p>Mehr Transparenz in Fehlerfällen, durch zusätzliche Zustellfehler sowie durch die neuen „technischen Fehler“</p> <p>Das <code>msg:Logo</code> Element wurde aus den Metadaten des Versenders entfernt</p> <p>Der Header X-DELIVERY-AUTH-METHOD wird nicht mehr unterstützt. Die Authentifizierungsmethode wird nun im PVP-Header X-PVP-ROLES im Parameter <code>AUTH-LEVEL</code> der Rolle <code>ZUSE-DISPLAY-SERVICE</code> übermittelt.</p> <p>Die PVP-Header X-PVP-OU und X-PVP-USERID sind bei E-Government-Portale für natürliche Personen nur noch optional</p> <p>Um Vertretungen für mehr als eine Behörde PVP-spezifikationskonform abbilden zu können, wurde der neue Rollenparameter <code>SOURCE</code> definiert. Dieser Parameter kann sowohl für die Rolle <code>MPK_POSTBEVOLLMAECHTIGTER</code> als auch die Rolle <code>MPK_REGISTRIERUNG</code> verwendet werden</p>

			Falls ein Zustellsystem über den Portalverbund an das AMOD angebunden wird, MUSS die PVP-Rolle <code>ZUSE-DELIVERY-SERVICE</code> mitgegeben werden
2.2.0	30.03.2021	Tauber A.	<p>Korrektur fehlerhafter Wert bei LoA high aufgrund Verwendung aus intermediate PVP Spec</p> <p>Das Version Attribut im <code>amod:PushDeliveryDataRequest</code> MUSS vom Zustellsystem gesetzt werden.</p> <p>Der Versender KANN zusätzliche Informationen übermitteln, die vom Anzeigemodul in den Verständigungstext eingefügt werden.</p> <p>Das AMOD retourniert in den Nachrichtenoperationen „Accepted“ und „DeliveryError“ zusätzlich die elektronischen Verständigungsadressen, da diese verpflichtenden Bestandteile des Zustellnachweises sind.</p>
2.1.3	31.05.2020	Tauber A.	<p>Präzisierung: nur bei RSa-Zustellungen wird vom AMOD die Nachrichtenoperation „Accepted“ an den zuständigen Zustelldienst versendet</p> <p>Die Zustellsysteme werden vom AMOD jedenfalls und explizit zur endgültigen Löschung einer Nachricht mittel Nachrichtenoperation „Delete“ aufgefordert.</p> <p>Präzisierung: Abfolge der Nachrichtenoperationen bei</p> <ul style="list-style-type: none"> <li>• RSa-Zustellungen</li> <li>• nonRSa-Zustellungen</li> <li>• Weiterleitung in den ERV</li> </ul> <p>Präzisierung: Nachrichtenoperationen bei denen im Falle einer RSa-Zustellung eine Zustellbenachrichtigung vom Zustelldienst an den Versender übermittelt werden muss</p> <p>Das Kapitel „Abholung von Zustellstücken“ wurde überarbeitet.</p> <p>Validierung von E-Mail-Adressen</p>
2.1.2	03.10.2019	Tauber A.	PVP Header
2.1.1	06.08.2019	Tauber A.	Ergänzung um die Weiterleitung in den ERV
2.1.0	09.04.2019	Tauber A.	Anpassungen an neues Zustellgesetz
2.0.0	10.05.2018	Tauber A.	Initialversion

## E. Referenzen

[AES]	National Institute of Standards and Technology, FIPS Pub 197: Advanced Encryption Standard (AES), 26. November 2001
[GOG]	Gerichtsorganisationsgesetz, RGBL. Nr. 217/1896, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 58/2018
[HTTP11]	RFC 2616 - „Hypertext Transfer Protocol -- HTTP/1.1“ <a href="https://www.ietf.org/rfc/rfc2616.txt">https://www.ietf.org/rfc/rfc2616.txt</a>
[ISO639-1]	ISO 639-1 - „Language codes - Part 1“ <a href="https://www.iso.org/iso-639-language-codes.html">https://www.iso.org/iso-639-language-codes.html</a>
[PERSDATA]	Larissa Naber: PersonData Struktur: XML Spezifikation – Dokumentation, E-Government Konvention, Version 2.0.0.
[PKIX]	RFC 5280 - „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“ <a href="https://www.ietf.org/rfc/rfc5280.txt">https://www.ietf.org/rfc/rfc5280.txt</a>
[PVP2EGOVTOKEN]	AG-IZ, Portalverbundprotokoll Version 2, eGovernment Attribute Profile
[PVP2RPROFIL]	AG-IZ, Portalverbundprotokoll Version 2, R-Profil
[PVP2SPROFIL]	AG-IZ, Portalverbundprotokoll Version 2, S-Profil
[PVPSMA]	AG-IZ, Portalverbund Sicherheitsmaßnahmen (Algorithmen)
[RFC822]	RFC822 - „Standard for ARPA Internet Text Messages“ <a href="http://www.ietf.org/rfc/rfc0822.txt">http://www.ietf.org/rfc/rfc0822.txt</a>
[RFC2045]	RFC 2045 - „Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies“ <a href="https://www.ietf.org/rfc/rfc2045.txt">https://www.ietf.org/rfc/rfc2045.txt</a>
[RFC2048]	RFC 2048 - „Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures“ <a href="https://www.ietf.org/rfc/rfc2048.txt">https://www.ietf.org/rfc/rfc2048.txt</a>
[RFC2119]	RFC 2119 - „Key words for use in RFCs to Indicate Requirement Levels“ <a href="https://www.ietf.org/rfc/rfc2119.txt">https://www.ietf.org/rfc/rfc2119.txt</a>

[RFC3986]	RFC 3986 - „Uniform Resource Identifier (URI): Generic Syntax“ <a href="https://www.ietf.org/rfc/rfc3986.txt">https://www.ietf.org/rfc/rfc3986.txt</a>
[RFC4122]	RFC 4122 - „A Universally Unique Identifier (UUID) URN Namespace“ <a href="https://www.ietf.org/rfc/rfc4122.txt">https://www.ietf.org/rfc/rfc4122.txt</a>
[RFC5322]	RFC 5322 - „Internet Message Format – Abschnitt 3.4.1. Addr-Spec Specification“ <a href="https://tools.ietf.org/html/rfc5322#section-3.4.1">https://tools.ietf.org/html/rfc5322#section-3.4.1</a>
[RFC5280]	RFC 5280 - „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – Abschnitt 4.2.1.2. Subject Key Identifier“ <a href="https://www.ietf.org/rfc/rfc5280.txt#section-4.2.1.2">https://www.ietf.org/rfc/rfc5280.txt#section-4.2.1.2</a>
[RFC7233]	RFC 7233 - „Hypertext Transfer Protocol (HTTP/1.1): Range Requests“ <a href="https://www.ietf.org/rfc/rfc7233.txt">https://www.ietf.org/rfc/rfc7233.txt</a>
[SOAP12]	SOAP Version 1.2 Part 2: Adjuncts (Second Edition) <a href="https://www.w3.org/TR/soap12-part2/">https://www.w3.org/TR/soap12-part2/</a>
[XMLDSIG]	Mark Bartel, XML Signature Syntax and Processing. <a href="http://www.w3.org/TR/xmlsig-core/">http://www.w3.org/TR/xmlsig-core/</a> , 2002.
[ZUSEMSG]	Tauber A., Elektronische Zustellung – Message Spezifikation, 2.1.0
[ZUSEORG]	Tauber A., Elektronische Zustellung – Organisatorisches, Modelle und Prozesse, 2.0.3
[ZUSETNVZ]	Tauber A., Elektronische Zustellung – Teilnehmerverzeichnis Spezifikation, 2.1.0
[ZUSTG]	Bundesgesetz über die Zustellung behördlicher Dokumente (Zustellgesetz – ZustG), BGBl. Nr. 200/1982, idF. BGBl. I Nr. 16/2020.