

MailBox X.400

MessageGate für OpenMS V5.7

Benutzerhandbuch

V2.6



Alle Produkte oder Dienstleistungen, die in diesem Handbuch genannt werden, sind durch die Warenzeichen oder eingetragene Warenzeichen der jeweiligen Unternehmen oder Organisationen gekennzeichnet. Die Telekom Deutschland GmbH schließt jegliche Haftung für die Zuordnung der Warenzeichen zu den verschiedenen Unternehmen oder Organisationen aus.

Die Informationen in diesem Benutzerhandbuch können ohne vorherige Ankündigung geändert werden und stellen keinerlei Verpflichtung für die Telekom Deutschland GmbH dar. Die Telekom Deutschland GmbH haftet nicht für Fehler und Mängel in diesem Handbuch. Die Vervielfältigung dieser Dokumentation ist nur im Rahmen eines Lizenzvertrags oder einer Geheimhaltungsvereinbarung gestattet. Ohne die ausdrückliche, schriftliche Genehmigung durch die Telekom Deutschland GmbH darf dieses Handbuch weder inhaltlich verändert noch in andere Sprachen übersetzt werden.

Copyright © 2023

Telekom Deutschland GmbH
BusinessMail X.400
Postfach 107300
68165 Mannheim

Inhaltsverzeichnis

0 VORWORT	1
0.1 Bitte senden Sie Kommentare an folgende E-Mail-Adresse:	1
0.2 Die folgenden Schriftarten werden verwendet:	1
0.3 Die folgenden Abkürzungen werden verwendet:	2
0.4 Neues in V2.6	3
1 EINFÜHRUNG IN MESSAGEGATE FILE INTERFACE	4
1.1 Mit MessageGate File Interface können Sie:	4
1.2 X.400 – ein internationaler Standard	4
1.3 Intention für die Realisierung von MessageGate	4
2 SCHNITTSTELLENBESCHREIBUNG	6
2.1 Übersicht	6
2.2 Das Verzeichnis von MessageGate File Interface	11
2.3 Das Format einer Mitteilung	13
2.3.1 Der Header der Mitteilung	13
2.3.2 Das Format der Adresse	16
2.3.3 Die Nutzdaten der Mitteilung	18
2.3.4 S/MIME gesicherter Inhalt	21
2.4 Kein Weiterleiten von empfangenen Mitteilungen	25
2.5 Das Format der Transmissionsset Datei	25
2.5.1 Die zentrale EDI-Funktion	25
2.5.2 Die Nutzdaten der Transmissionsset Datei	27
2.6 Closed User Group (CUG)	27
2.7 Der Statusreport	28
2.7.1 Allgemein	28
2.7.2 Anfordern eines Statusreports	28
2.7.3 Syntax des Statusreports (strukturierte Form)	30
2.7.4 Syntax des Statusreports (CSV-Format)	35
2.8 Lesebestätigung versenden	37
2.9 Kommunikations-/Partnerschaftsprofile	38
2.9.1 Allgemein	38
2.9.2 X.400 Reports	39
2.9.3 X.400 Headerinformationen	40
2.9.4 X.400 Body Parts	41
2.9.5 Binäre Daten codieren als	41
2.9.6 Ausgabeformat	42
2.9.7 Statusreport abfragen	42
2.9.8 Automatischen Statusreport konfigurieren	42
2.9.9 EDI-Partnerschaft	43
2.9.10 SMTP-Filter	44
2.9.11 Web-Service für WebConfig	45
3 ZUGANG ÜBER SFTP (SSH)	46
3.1 Allgemein	46

3.2	Besonderheiten des Zuganges	46
3.3	Empfohlene SFTP-Kommunikationsmodule	47
3.3.1	Für Microsoft® Windows 32 Bit Betriebssysteme	47
3.3.2	Für Microsoft® Windows 64 Bit Betriebssysteme	53
3.3.3	Für Linux und Unix Betriebssysteme	54
3.3.4	Für Apple Max OS X	54
3.3.5	Für alle anderen Betriebssysteme	55
4	ZUGANG ÜBER HTTPS/WEBDAV	56
4.1	Allgemein	56
4.2	Besonderheiten des Zuganges	57
4.3	Empfohlene WebDAV Kommunikationsmodule	57
4.3.1	Für Microsoft® Windows 32 Bit Betriebssysteme	57
4.3.2	Für Microsoft® Windows 64 Bit Betriebssysteme	65
4.3.3	Für Linux und Unix Betriebssysteme	65
4.3.4	Für Apple iOS	66
4.3.5	Für alle anderen Betriebssysteme	67
5	ZUGANG ÜBER HTTPS/WEB-SERVICES	68
5.1	Allgemein	68
5.2	Besonderheiten des Zuganges	69
5.3	Web-Service API	69
5.3.1	Das Web-Service Profil v1	70
5.3.2	Das Web-Service Profil v2 (v2a)	72
5.3.3	Das Web-Service Profil v3 (v3a)	81
5.4	Getestete REST-Kommunikationsmodule	84
6	AS2 UND MESSAGEGATE	86
6.1	Allgemein	86
6.2	Unterschiede zwischen File Interface und AS2 Nutzern	88
7	SMTP-MTA UND MESSAGEGATE	98
7.1	Allgemein	98
7.2	Unterschiede zwischen File Interface und SMTP MTA Nutzern	98
8	LÖSUNGEN FÜR MESSAGEGATE REALISIEREN	106
8.1	Erste Tests mit Standard-E-Mail-Clients	106
8.1.1	Test mit Outlook Express bei älteren Windows OS	106
8.1.2	Test mit Thunderbird	106
8.1.3	Test mit Microsoft Live Mail bei neueren Windows OS	107
8.2	Lösung gestalten und entwickeln	108
	ANHANG A X.400 ADRESSELEMENTE	110
	ANHANG B: FEHLERCODES	112
B1.	Fehlercodes MessageGate Poller Prozess:	112
B2.	MessageGate Errorcode im Statusreport	113
B3.	MTA Errorcode (Non Delivery) im Statusreport	120
B4.	X.400 User Agent Errorcode (Non Receipt) im Statusreport	125

B5. Umsetzregel bei Fehlercodes DN zu DSN	126
ANHANG C: BEISPIELE FÜR MITTEILUNGEN UND REPORTS	130
C1. Ausgelieferte Mitteilung mit Textanhang	130
C2. Ausgelieferte Mitteilung mit Binäranhang	130
C3. Ausgelieferte Mitteilung mit Multibodypart	131
C4. Ausgelieferte Mitteilung mit Multirecipient	132
C5. Versendete Mitteilung ohne Anforderung Report	132
C6. Versendete Mitteilung mit Anforderung Report	134
C7. Versendete Mitteilung mit Multirecipient	134
C8. Ausgelieferte signierte Mitteilung	135
C9. Ausgelieferte verschlüsselte Mitteilung	136
C10. Transmissionsset mit zwei Interchange	137
C11. Statusreport ohne Historie	139
C12. Statusreport mit Historie	140
C13. Statusreport nur für bestimmte Order-ID	141
C14. Statusreport nur für bestimmte Message-ID	142
C15. Statusreport für abgewiesene Mitteilungen	142
C16. Report für versendete Mitteilung (Multirecipient)	143
ANHANG D: ZEICHENSÄTZE	146

0 Vorwort

Das Produkt

In diesem Handbuch wird das MessageGate File Interface beschrieben, einer Schnittstelle des MailBox Service von *BusinessMail X.400* zum Austausch von Mitteilungen zwischen einem Hostrechner und Teilnehmern von elektronischen Mail-Systemen gemäß dem X.400-Standard.

Der Leser

Dieses Handbuch wendet sich an alle Kunden von BusinessMail X.400, die nicht die standardisierte P7 Remote User Agent Schnittstelle von *BusinessMail X.400* einsetzen können, um Daten und Mitteilungen an Partner zu versenden bzw. von diesen zu empfangen. Die MessageGate Schnittstelle wird zunächst parallel zu dem schon seit Jahren verfügbaren Batch User Agent (BUA) angeboten; soll diesen aber mittelfristig ersetzen.

Weitere Dokumente

- Siehe auch Batch User Agent Reference Guide
- RFC 2822, RFC 1521

Eingetragene Warenzeichen

Microsoft® und Windows TM sind Warenzeichen der Microsoft Corporation.

Weitere Produkt- und Firmennamen, die in diesem Handbuch verwendet werden, dienen nur der Kennzeichnung der Produkte. Es kann sich hierbei um Warenzeichen bzw. eingetragene Warenzeichen der jeweiligen Unternehmen handeln.

0.1 Bitte senden Sie Kommentare an folgende E-Mail-Adresse:

helpdesk.businessmailx400@telekom.de, Betreff: MessageGate Benutzerhandbuch

0.2 Die folgenden Schriftarten werden verwendet:

- | | |
|------------------|---|
| Diese Schriftart | Wird z.B. für Beispiele des Inhalts von Mitteilungen benutzt, die über MessageGate übertragen wurden. |
| Diese Schriftart | Wird für die Parameter der MessageGate Dateischnittstelle bzw. auch deren Werte benutzt. |

0.3 Die folgenden Abkürzungen werden verwendet:

API	Application Programming Interface
AS2	Applicability Statement 2 - Standard (EDIINT) für die B2B Kommunikation über Internet (RFC 4130)
BUA	Batch User Agent – Eine Dateischnittstelle des <i>BusinessMail X.400 MailBox Service</i> , um auf eine Kundenmailbox zugreifen zu können
BP14	Body Part 14 – Bilaterally defined (binary) ITU-T X.400 Standards (1984)
CA	Certificate Authority, Erstellt und signiert digitale Zertifikate
CR	Carriage Return - Wagenrücklauf
CSV	comma-separated values – Ein einfaches, strukturiertes Textformat, um den Inhalt einer Datenbank darzustellen, wobei jeder Eintrag einer Textzeile entspricht.
CUG	Closed User Group, geschlossene Benutzergruppe, bei der ein Datenaustausch nur zwischen den registrierten Benutzern möglich ist.
DDA	Domain Defined Attributes (X.400 Adress-Elemente)
DN / NDN	X.400 Delivery Notification (Report) oder Non-Delivery Notification (Report) wird durch den X.400 MTA erzeugt.
EDI	Electronic Data Interchange, eine Gruppe von Standards zum Austausch von Geschäftsdaten.
EDIFACT	Ein Standard für Electronic Data Interchange – ISO 9735
FTBP	FTAM (File Transfer, Access and Management) Body Part, wird zur Übertragung von binären Inhalten mit zusätzlichen Informationen (z.B. Dateinamen, Typ des Inhalts etc.) verwendet.
FTP	File Transfer Protocol (RFC 959)
GDI	Global Domain Identifier (X.400 Terminologie)
GLN	Global Location Number (registrierte EDI Adresse)
HTTP(S)	Hypertext Transfer Protocol: Protokoll, um Daten über das Internet zu übertragen
ILN	International Location Number (registrierte EDI-Adresse)
ITU-T	International Telecommunication Union - Telecommunication
LF	Line Feed - Zeilenvorschub
MB	Megabyte – 1 000 000 Bytes – Definition empfohlen von International System of Units (SI)
MDN	Message Disposition Notification – Typ von Report benutzt bei SMTP (RFC 3798) und AS2 (RFC 4130)
MIME	Multipurpose Internet Mail Extensions (RFC1521 ff)
MPLS	Multiprotocol Label Switching – IP-Backbone, der einen speziellen Label Mechanismus benutzt, um VPN zu definieren.

MS	(X.400) Message Store
MTA	(X.400) Message Transfer Agent
P2/ P22/ P35	X.400 Mitteilungstypen
P7	Standard-Protokoll bei X.400 für die Kommunikation zwischen X.400 Remote User Agent und Message Store
PEDI	Spezieller X.400 EDI-Mitteilungstyp definiert in X.435 (entspricht P35)
RFC	Request for Comment – Internet Standard
RN / NRN	X.400 Receipt Notification (Report) oder Non Receipt Notification (Report) wird durch den X.400 User Agent (Client) erzeugt
SFTP	Secure File Transfer Protocol (Teil der Secure Shell Protocol Suite, RFC 4259 ff)
S/MIME	Secure/ Multipurpose Internet-Mail Extensions (V3.2, RFC 5751), Security Erweiterung (Signatur/Verschlüsselung) für MIME
SMTP	Simple Mail Transfer Protocol – Internet Mail Protocol Standard (RFC 2822 ff)
TS	Transmission Set (EDIFACT) – Eine Datei, die einen oder mehrere EDIFACT Interchange enthalten kann
UNB	EDIFACT Interchange Kopfzeile
UNZ	EDIFACT Interchange Schlusszeile
VPN	Virtual Private Network (im TCP/IP Umfeld wird hier meist IPSEC eingesetzt)
WebDAV	HTTP Extensions for Distributed Authoring (RFC 2518) – Erweiterung des Befehlssatzes von http (Kopieren, Verschieben)
<i>WebConfig</i>	<i>BusinessMail X.400</i> Management Plattform, über die ein Benutzer seinen X.400 Account (Eintrag) und seine Partnerschaften verwalten kann.
Web-Service	Verschiedene Protokolle und Standards zum Übertragen von Daten zwischen Anwendungen oder Systemen. Oft wird HTTP in Verbindung mit XML, SOAP, WDSL und UDDI verwendet.
X.435	Siehe PEDI

0.4 Neues in V2.6

- Ergänzung im Kapitel 3 wegen Einführung eines neuen SFTP-Servers und bei SFTP-Zugriff mittels WebDrive Next Generation im Kapitel 3.3.2
- Ergänzung bei Konfiguration AS2 Mitteilungsversand im Kapitel 6.2.

1 Einführung in MessageGate File Interface

1.1 Mit MessageGate File Interface können Sie:

- Mitteilungen mit den Benutzern von *MailBox X.400*, mit Benutzern von anderen X.400-Mail-Systemen und mit Internet-Benutzern austauschen. MessageGate unterstützt dabei den X.400 Standard 1984 und 1988/92.
- Mitteilungen an Faxempfänger senden.
- Den Status Ihrer Mitteilung(en) in von Maschinen bearbeitbarer Form abfragen.
- Lesebestätigungen (Receipt Reports) für empfangene Mitteilungen erzeugen.
- Standard-Transportmechanismen des TCP/IP Protokolls (SFTP, HTTPS mit WebDAV Erweiterung oder mittels Web-Service) verwenden, um Mitteilungen/ Nutzdaten zum MailBox Service zu übertragen bzw. von dort abholen.

1.2 X.400 – ein internationaler Standard

X.400 ist der Name eines internationalen Standards (ITU, ISO) zum Austausch von elektronischen Mitteilungen, der die Anforderungen und Empfehlungen für E-Mail-Programme beschreibt. In ihm ist festgelegt, wie eine Mitteilung adressiert werden muss, welche Zeichen bzw. Datentypen zulässig sind und wie die Kommunikation zu erfolgen hat.

Im X.400 Standard sind Auslieferbestätigung (Delivery Notification/Report) und Lesebestätigung (Receipt Notification/Report) definiert, mit denen man den Status seiner Mitteilungen prüfen kann.

Weltweit gibt es eine Vielzahl von Telekommunikationsnetzen mit Diensten, die den Austausch von Mitteilungen gemäß dem X.400-Standard ermöglichen. Einer der größten Vorteile von X.400 besteht darin, dass Mitteilungen auch zwischen Benutzern mit unterschiedlichen Computersystemen über sichere Netzwerkverbindungen ausgetauscht werden können.

1.3 Intention für die Realisierung von MessageGate

BusinessMail X.400 bietet schon seit mehr als 25 Jahren eine Dateischnittstelle für Hostrechner an, die den Namen Batch User Agent (BUA) trägt. Hierbei wird für den Kunden auf Applikationsservern des MailBox Service ein Arbeitsverzeichnis angelegt, in das er üblicherweise mittels aktiven FTP die Nutzdaten und Auftragsdateien überträgt.

In den Auftragsdateien wird definiert, an wen die Nutzdaten versendet oder ob Mitteilungen aus dem Message Store abgeholt werden sollen. Die Nutzdaten dieser abgeholt Mitteilungen werden dann in einer Unterverzeichnisstruktur des Arbeitsverzeichnisses abgelegt und weitere mitteilungsrelevante Daten in der Ergebnisdatei des Auftrags hinterlegt. Der Kunde kann sich diese Daten dann wieder per FTP abholen. Dieser Mechanismus hat sich seit Jahren bewährt, erfordert aber während der Implementierung einen recht hohen Aufwand, da es sich um eine proprietäre Lösung handelt.

Im Rahmen der Implementierung des AS2 Gateway von *BusinessMail X.400* wurde ein neuer Hostprozess entwickelt, der eine Dateischnittstelle bereitstellt, die deutlich einfachere Strukturen aufweist und die als MessageGate File Interface (im weiteren Verlauf des Dokuments wird teilweise auch nur der Name MessageGate benutzt) per SFTP (SSH) oder aber auch mittels HTTPS (mit WebDAV Erweiterung oder Web-Service) angesprochen werden kann. Die Hauptvorteile von MessageGate sind ein SMTP/MIME kompatibles Übergabe-Format und dass Mitteilungen direkt an der Dateischnittstelle ausgeliefert werden. Ein Pollen des Message Store wie beim BUA ist deshalb nicht notwendig und die Nutzdaten stehen somit unmittelbar zur Verfügung. Das Übergabe Format SMTP/MIME wurde gewählt, da es auf dem Markt eine Vielzahl von Bibliotheken und Werkzeuge gibt, um solche Strukturen zu erstellen bzw. zu verarbeiten. MessageGate verhält sich hier konform zu RFC 2822 und zu RFC 1521 und den entsprechend nachfolgenden RFC, die für MIME relevant sind.

2 Schnittstellenbeschreibung

2.1 Übersicht

In diesem Kapitel werden die Funktionen von MessageGate File Interface kurz beschrieben. Die Details zu den einzelnen Punkten finden sich in den nachfolgenden Kapiteln wieder. Im Anhang C: Beispiele für Mitteilungen und Reports werden außerdem weitere Beispiele für Mitteilungen und Reports sowie Fehlercodetabellen beschrieben.

Nutzern von MessageGate wird auf den Applikationsservern des MailBox Service ein Arbeitsverzeichnis eingerichtet. Mittels HTTPS (mit WebDAV Erweiterung oder Web-Service) oder SFTP (SSH) können in dieses Verzeichnis Mitteilungen/Nutzdaten übertragen bzw. daraus Mitteilungen/Nutzdaten abgeholt werden. Anhand der Extension der Dateinamen (.IN → verarbeiten/versenden, .OUT → ausgeliefert) wird unterschieden, ob es sich um Daten handelt, die zum Versand anstehen oder um solche, die ausgeliefert wurden.

Da aber bei Verwendung von SFTP oder HTTPS/WebDAV der Verarbeitungsprozess nicht zweifelsfrei erkennen kann, ob die Dateien komplett durch die Kundenapplikation übertragen wurden, sollten die Daten zunächst mit der Endung „*.TMP“ im Arbeitsverzeichnis abgelegt und erst danach in „*.IN“ umbenannt werden. Beim Ausliefern von Mitteilungen auf die Dateischnittstelle nutzt der MessageGate Prozess beim Kopieren der Daten von den MailBox Hostrechner auf die Applikationsserver einen ähnlichen Mechanismus, nur dass hier die temporären Dateien nicht sichtbar sind.

Versenden von Mitteilungen

Schritt 1: Client → überträgt mittels HTTPS/WebDAV oder SFTP die Datei „M_Auftrags-ID.TMP“ → MessageGate Verzeichnis.

Schritt 2: Client → benennt mittels HTTPS/WebDAV oder SFTP die Datei „M_Auftrags-ID.TMP“ im MessageGate Verzeichnis in „M_Auftrags-ID.IN“ um.

Bei Verwendung von HTTPS/Web-Service entfällt der Schritt 1 und es wird direkt schon die Datei mit Endung „.IN“ übertragen, da der Web-Service sicherstellt, dass nur eine komplett übertragene Datei verarbeitet wird.

Schritt 3: MessageGate verarbeitet die Datei „M_Auftrags-ID.IN“, versendet eine entsprechende X.400 Mitteilung und löscht die Datei.

Ausliefern von Mitteilungen

Schritt 1: MessageGate übernimmt vom X.400 MTA eine Mitteilung, die an den MessageGate Benutzer adressiert wurde und stellt diese als Datei „M_Auftrags-id.OUT“ im MessageGate Verzeichnis ein. Wurde das Leistungsmerkmal Closed User Group aktiviert, wird der Dateiname um die Absender User-ID ergänzt.

Schritt 2: Client → Holt mittels HTTPS (WebDAV/Web-Service) oder SFTP die Datei „M_Auftrags-ID.OUT“ (bzw. „M_Auftrags-ID_User-ID.OUT“ bei CUG) aus dem MessageGate Verzeichnis ab und löscht diese Datei.

MessageGate interpretiert alle Dateien, die mit „M_“ anfangen als Mitteilungen. Die Auftrags-ID darf maximal 26 Zeichen lang sein und es sind nur Zeichen aus dem Alphabet (keine deutschen Sonderzeichen), Ziffern und ausgewählte Sonderzeichen („_“, „-“ und „\$“) erlaubt. **Beachten Sie hierbei auch die im nächsten Kapitel beschriebene Versionsverwaltung von Dateien!**

Üblicherweise erwartet der MessageGate Prozess eine Mitteilungsdatei (bzw. liefert diese auch so aus), in der die Verwaltungsinformationen (Absender, Empfänger, Betreff, Mitteilungsnummer, etc.) und die Nutzdaten (MIME oder S/MIME-Content) in einer SMTP/MIME (Version 1.0) Struktur gegliedert sind. MessageGate akzeptiert kei-

ne Mitteilungen mit leerem Content. Pro Mitteilung können bis zu 50 Empfänger (getestet) angegeben werden.

Auch die Einschränkung, dass bei empfangenen Mitteilungen nur der MessageGate Benutzer adressiert werden darf, wurde nun aufgehoben. Die Einschränkung auf einen Empfänger sowohl in Sende- als auch Empfangsrichtung gilt aber weiterhin für den Fall, dass die Daten signiert und/oder verschlüsselt als S/MIME-Content angeliefert werden.

Beispiel für Format einer ausgelieferten Mitteilung mit mehreren Anhängen

Name: M_5K00AG0HBDM0F2F8.OUT

```
To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE" <49603@viat.de>
From: "G=ipm;S=tester;O=testag;A=viat;C=de" <49637@viat.de>
Message-ID: 614 07/11/13
X-MPDUID: 8B0663A011DCEC4417009682
Date: 13 Nov 2010 13:10:22 +0100
Subject: Test mit 3 Bodyparts
Disposition-Notification-To: "G=ipm;S=tester;O=testag;A=viat;C=de"
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="MG_=_CA610D0211DC91E900007CAD_=_MG"
```

```
--MG_=_CA610D0211DC91E900007CAD_=_MG
Content-Type: text/plain
Content-Transfer-Encoding: 8bit
```

Test äöüÄÖÜß

```
--MG_=_CA610D0211DC91E900007CAD_=_MG
Content-Type: application/octet-stream
Content-Disposition: attachment; filename="4d654d1d.zip"
Content-Transfer-Encoding: binary
```

```
PK      tYr2ÄQa6+    <4d654d1d.0µ"ls£: ...÷Tñ"è¥Ói3xJU/$!|DØb2xgd °1Ø
```

```
      4d654d1d.0PK       8  
--MG_=_CA610D0211DC91E900007CAD_=_MG
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0062)https://securep7.viat-test.de/~0000001045/result/fetch_all.RES -->
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=windows-1252">
<META content="MSHTML 5.50.4930.1700" name=GENERATOR></HEAD>
<BODY><XMP>LOGIN:
.
</XMP></BODY></HTML>
```

```
 
--MG_=_CA610D0211DC91E900007CAD_=_MG—
```

Regeln für versendete Mitteilungen

Pflichtelemente sind: „To:“ und Content-Type/Encoding. Alle anderen Felder sind optional. Ist die Message-ID nicht definiert, wird die Auftrags-ID als X.400 Message-ID verwendet.

Die Adressen bei „To:“, „Cc:“, „Bcc:“ und „From:“ (Groß- oder Kleinschreibung oder Mix ist erlaubt) setzen sich zusammen aus einem Alias, in dem die X.400 Adresse (Adressfelder sind durch Semikolon „;“ getrennt) angegeben werden kann, und der SMTP- Adresse (<x@viat.de> bzw. <User-ID@viat.de>).

Mögliche Adressformen:

```
"c=de;a=viat;P=prmd;o=org;s=Nachname;g=Vorname" <x@viat.de> Externe Adresse ohne User-ID
"" <73237@viat.de> Lokale oder externe Adresse mit User-ID
```

“c=de;a=viat;o=org;s=Nachname:g=Vorname“ <71111@viat.de>

Adresse, wenn MessageGate ausliefert und User-ID bekannt ist

Wird beim Versenden bei „To:“, „Cc:“ oder „Bcc:“ sowohl die X.400 Adresse als auch die User-ID angegeben, nutzt MessageGate die X.400 Adressfelder und verifiziert nicht die angegebene User-ID!

Im Zusammenhang mit der zentralen EDI-Funktion (muss für den MessageGate Nutzer explizit aktiviert werden) ist es auch möglich, einen oder mehrere EDIFACT Interchange in einer sogenannten Transmissionsset-Datei zum Versand zu übergeben bzw. einen von X.400 Partnern gesendeten EDIFACT Interchange in einer solchen Datei als reine Nutzdaten zu erhalten.

Beispiel für Format einer Transmissionsset Datei

Name: T_5K00AG0HBDM0F2F8.OUT

```
UNA:+.? '
UNB+UNOA:2+MGATE1:65+TESTER:65+020508:1413+0709210008'
UNH+EVA0000001+INVOIC:D:95A:UN:ETEIB+++'
.
.
UNT+37+EVA0000001'
UNZ+1+0709210008'
```

Es ist aber nicht mehr notwendig, die zentrale EDI-Funktion aktivieren zu lassen, um die dort integrierte Option Closed User Group (nur bestimmte EDI/EDIFACT Absender können Dokumente anliefern) verwenden zu können. Die CUG kann nun auch für beliebige Mitteilungen aktiviert werden (nur konfigurierte MessageGate Partner können dann Mitteilungen im Verzeichnis ausliefern).

Die Verwaltungsinformationen der Mitteilungsdatei wurden auf ein Minimum begrenzt, um die Schnittstelle so einfach wie möglich zu halten. Umsetzregeln für das Erstellen einer Mitteilung (X.400 Message Typ, Umsetzung MIME-Body in X.400 Body Part, Verfallsdatum, welche Reports sollen angefordert werden etc.) werden in entsprechenden Parametern im Profil des MessageGate Benutzers bzw. in dessen Partnerschaftsprofilen festgelegt. Partnerschaftsprofile müssen aber nicht in jedem Fall angelegt werden, da im Header der Mitteilung auch beliebige X.400 Adressen angegeben werden können und nicht nur bekannte Kommunikationspartner. Partnerschaftsprofile sind dann relevant, wenn sich die Kommunikationsparameter einer Partnerschaft von denen in der Grundeinstellung des MessageGate Benutzers unterscheiden sollen (z.B. andere Reports anfordern oder einen anderen X.400 Mitteilungstyp verwenden).

Parameter bei Grundeinstellung bzw. Partnerschaft

- Umsetzung angeforderter Bestätigung (Disposition-Notification-To:) in X.400 Anforderung Non Delivery Notification (NDN), Delivery Notification (DN) oder Receipt Notification (RN) beim Versenden von Mitteilungen (Default ist DN -> Auslieferbestätigung)
- Durchreichen von Receipt Notification als Disposition-Notification-To: in empfangenen Mitteilungen unterdrücken oder nicht (Default ist nicht unterdrücken)
- Verfallzeitpunkt einer X.400 Mitteilung in Minuten (Default ist 1440 → 24 Stunden)
- Format des Inhalts der X.400 Mitteilung (Default ist IPM88) beim Versenden
- Umsetzung MIME in X.400 Body Part (Default ist Variabel → Umsetzung in adäquaten Body Part) beim Versenden (beim Empfang gelten vergleichbare Regel)
- Ausliefern binäre MIME-Inhalte in „BASE64“ oder „Binary“ (Default ist Binary)
- Ausliefern von EDIFACT Dokumenten in Transmissionsset Datei oder als SMTP-Mailstruktur (nur bei aktivierter zentraler EDI-Funktion und nur in Grundeinstellung → Default ist Transmissionsset Datei)

MessageGate sieht nicht vor, dass neben Mitteilungen auch X.400 Reports an der Dateischnittstelle ausgeliefert werden, da dies einen zusätzlichen Implementierungsaufwand auf Kundenseite bedeuten würde.

Informationen über den Status einer Mitteilung bzw. mehrerer Mitteilungen können über einen Statusreport manuell angefordert bzw. automatisch (Konfiguration im Benutzerprofil) erzeugt werden.

Beispiel für Anforderung eines Statusreports im strukturierten Format

Name: S_040308001.IN

Format: History

Direction: both

Parameter in Anforderung Statusreport (logische Und- Verknüpfung zur Eingrenzung)

Disposition: All, Modified (Default All, alle Einträge, nicht nur die seit letzter Abfrage geänderten)
 Direction: Sent, Received, Both (Default ist Sent)
 Format: History, CSV-C, CSV-S, Actual (Default ist Actual -> aktueller Status und nicht alle Statusänderungen anzeigen)
 Message-ID: Mitteilungsnummer oder Teilstring
 Order-ID: Auftragsnummer oder Teilstring
 Since: dd-mmm-yyyy hh:mm:ss, seit Zeitpunkt Tag, Monat (englische Kurzschreibweise), Jahr Stunde, Minute, Sekunde

Diesen Statusreport stellt MessageGate als strukturierte Datei zur Verfügung, die in abgestuften Detaillierungsgraden genaue Informationen über versendete bzw. empfangene Mitteilungen mit Zuordnung der entsprechenden X.400 Reports liefert. Bei Mitteilungen mit mehreren Empfängern wird pro Empfänger ein Eintrag im Report angezeigt. In diesem Fall sind die Message-ID bzw. die Order-ID nicht eindeutig, sondern es muss auch die Empfängeradresse ausgewertet werden. Bei empfangenen Mitteilungen wird weiterhin nur ein Eintrag für den Absender angezeigt. Die eigentliche Empfängerliste wird dann im RFC2822 Header der Mitteilung ausgegeben.

Beispiel für Statusreport mit Format Actual (S_Auftrags-ID.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:56:23

Filters: Disposition=All, Direction=Both, Format=Actual, Since=13-Nov-2010

From: "G=ipm;S=tester;O=testag;A=viaT;C=de" <49637@viaT.de>

Order-ID: 5K00AG0HBDM0F2F8

Message-ID: 614 07/11/13

MTS-ID: CA610D0211DC91E900007CAD

Status: Read

Date: 13-Nov-2010 14:01:18 +0100

Beispiel für Statusreport mit Format History (S_Auftrags-ID.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:56:22

Filters: Disposition=All, Direction=Both, Format=History

To: "" <49637@viaT.de>

Order-ID: Test_3_Body011

Message-ID: 260002 12/11/25 MGATE Test

MTS-ID: 098FC66111DC91F80000A6BD

Sent: 13-Nov -2010 14:52:21 +0100

Delivered: 13-Nov-2010 14:52:27 +0100

Read: 13-Nov-2010 14:54:00 +0100

Einträge mit Format „Actual“ haben immer eine feste Länge von 6 Zeilen. Beim Format „History“ ist die Anzahl der Zeilen variabel (5-7).

Als Alternative zu diesen gut lesbaren Reports kann man auch über das Format „CSV-S“ (CSV-Format mit Semikolon als Trennzeichen) bzw. „CSV-C“ (mit Komma als Trennzeichen) einen Report auswählen, der für die maschinelle Verarbeitung optimiert ist.

Das automatische Erzeugen eines Statusreports auf Basis von Hostprofilen wird im Kapitel 2.9 Kommunikations-/Partnerschaftsprofile genauer erläutert.

Falls mit dem X.400 Partner vereinbart und von diesem in einer Mitteilung entsprechend angefordert, kann für die empfangene Mitteilung eine Lesebestätigung erzeugt/versendet werden.

Beispiel für das Versenden eines Receipt Reports

Name: R_5K00AG0HBDM0F2F8.IN

Processed → Receipt Report/Notification (RN), positive Lesebestätigung

Failed → Non Receipt Report/Notification (NRN), Verworfen → negative Lesebestätigung

Dateien, die der MessageGate Prozess verarbeitet hat („*.IN“), werden automatisch aus dem Arbeitsverzeichnis gelöscht. Alle anderen Dateien (ausgelieferte Mitteilungen oder Statusreports) werden durch den sogenannten Purger nach einer definierten Verweilzeit aus dem Arbeitsverzeichnis gelöscht. Diese Verweilzeit kann kundenindividuell durch den Betrieb von *BusinessMail X.400* eingerichtet werden. Es wird aber empfohlen, dass die Kundenapplikation das kontrollierte Löschen dieser Dateien übernimmt und somit zeitnah das Verzeichnis geleert wird.

Einen Purger gibt es auch für die Relation in der Datenbank (Trace_Tab), in der die Statusinformationen für die Mitteilung/die Transaktion gespeichert werden. Die Verweilzeit dieser Einträge wird ebenfalls durch den Betrieb von *BusinessMail X.400* eingerichtet, ist aber kundenindividuell einstellbar. Zunächst wird ein Default von 240 Stunden im User Profil in der Datenbank hinterlegt.

MessageGate kennt zwei Klassen von Verarbeitungsfehlern. Zum einen werden die Mitteilungsdateien beim Lesen im Kundenverzeichnis auf Vollständigkeit und Syntax geprüft und werden im Fehlerfall erst gar nicht der weiteren Verarbeitung zugeführt. Die Datei verbleibt dann im Verzeichnis und der Name wird um einen Fehlercode (siehe Anlage B) erweitert und ein Eintrag in der Datenbank vorgenommen, der per Status Report abgefragt werden kann. Tritt der Fehler erst bei der späteren Verarbeitung (z.B. bei Schnittstelle zum MTA) auf, wird nur ein entsprechender Eintrag in der Datenbank vorgenommen.

Es ist auch möglich, MessageGate mit vermindertem Leistungsumfang zu beauftragen. In diesem Fall kann der Benutzer lediglich Mitteilungen empfangen. Das Versenden von Mitteilungen und Lesebestätigung und auch das Anfordern von Status Reports ist nicht möglich. Die automatische Erzeugung von Status Reports konfiguriert in *WebConfig* (Web basierendes Konfigurationstool) ist aber möglich.

In Verbindung mit der zentralen EDI-Funktion wäre bei vermindertem Leistungsumfang eine Lösung realisierbar, bei der mit einem einfachen Webbrowser bereits die Nutzdaten (EDIFACT Dokumente) abgeholt und in eine Anwendung (z.B. ELFE Nachverarbeitung) importiert werden können.

2.2 Das Verzeichnis von MessageGate File Interface

Das Arbeitsverzeichnis von MessageGate File Interface sieht standardmäßig keine Unterverzeichnisstruktur vor. Die Unterscheidung, ob Daten versendet werden sollen oder ob diese zum Abholen bereitstehen, wird nur durch die Extension der Datei festgelegt.

Vom X.400 MTA (Message Transfer Agent) übergebene Mitteilungen liefert der MessageGate Prozess umgehend an der Dateischnittstelle aus.

Der Pollerprozess prüft in regelmässigen Abständen, ob Aufträge („*.IN“, zu versendende Mitteilungen oder Transmissionssets, Statusabfragen, zu versendende Lesebestätigungen) abzuarbeiten sind. Der Intervall dieser Prüfungen wird pro Gruppe festgelegt, wobei momentan nur eine Gruppe (Intervall 1 Minute) konfiguriert ist, der ein Benutzer zugeordnet werden kann. Findet der Prozess eine „*.IN“ Datei, verarbeitet er diese. Der Prozess kann aber nicht in jedem Fall sicherstellen, dass die Datei vollständig ist und somit der Transfer von der Kundenanwendung zum Applikationsserver abgeschlossen wurde.

Zu versendende Daten müssen daher bei SFTP und HTTPS/WebDAV immer zunächst als temporäre Datei („*.TMP“) übertragen und sollten erst nach vollständiger Übertragung umbenannt („*.IN“) werden.

Bitte beachten Sie auch, dass bei den Applikationsservern auf Grund des OpenVMS Betriebssystems neben dem Punkt zur Abgrenzung der Extension keine weiteren Punkte innerhalb des Dateinamens zulässig sind.

Neben der Extension des Dateinamens wird durch den ersten Buchstaben des Namens festgelegt, um welche Art von Datei es sich handelt. Danach folgt, abgetrennt durch einen Unterstrich “_“, die Auftragsnummer (Auftrags-ID) mit maximal 26 Stellen Länge.

Diese Auftragsnummer kann neben Ziffern auch Buchstaben (keine Umlaute oder „ß“) und bestimmte Sonderzeichen enthalten:

Bindestrich “-“

Unterstrich “_“

Dollarzeichen “\$“

Bitte stellen Sie sicher, dass die von Ihrer Anwendung vergebene Auftrags-ID und auch die in der Mitteilung genutzte Message-ID eindeutig sind, damit MessageGate die zu dieser Transaktion gehörenden Quittungen/ Reports korrekt zuordnen kann. Bitte beachten Sie auch die Besonderheit des OpenVMS Betriebssystems, das Dateien mit Versionsnummer hinterlegt. Dies bedeutet, dass Dateien mit gleichem Namen nicht überschrieben werden. Beim Zugriff über HTTPS/WebDAV oder HTTPS/Web-Service ist dies aber nicht erkennbar. Dies gilt dann aber auch für den Zugriff über SFTP, sobald der neue SFTP-Server (OpenSSH) in Betrieb gegangen ist. Beim Zugriff wird immer die neueste (höchste Versionsstand) Datei geöffnet bzw. gelöscht. Nach dem Löschen taucht dann der Dateiname wieder im Verzeichnis auf, wobei hier dann wieder von den verbliebenen Dateien diejenige mit dem höchsten Versionsstand angezeigt wird.

Ist beim MessageGate Account die Closed User Group Funktion aktiviert, so wird der Dateiname einer empfangenen Mitteilung, abgetrennt durch einen Unterstrich “_“, noch um die User-ID des Absenders erweitert. Die User-ID ist dabei immer sechs Stellen lang und es werden bei Bedarf führende Nullen eingefügt.

MessageGate sieht folgende Konventionen für Dateinamen vor:

a) Zu versendende Mitteilungen mit RFC2822 Header:

M_<Auftrags-ID>.IN

b) Zu versendende Transmissionsets (ein oder mehrere EDIFACTInterchange) ohne RFC2822 Header:

T_<Auftrags-ID>.IN

c) Für das Versenden einer Empfangsbestätigung:

R_<Auftrags-ID>.IN

d) Für das Anfordern eines Statusreport:

S_<Auftrags-ID>.IN

e) Für empfangene Mitteilungen mit RFC2822 Header:

M_<Auftrags-ID>.OUT bzw. M_<Auftrags-ID>_<User-ID>.OUT (aktivierte CUG)

f) Für empfangene Transmissionsets (momentan ein Interchange) ohne RFC2822 Header:

T_<Auftrags-ID>.OUT

g) Für bereitgestellte Statusreports:

S_<Auftrags-ID>.OUT

Sie können sowohl große als auch kleine Buchstaben für den Namen der Datei und der Extension benutzen, müssen aber beachten, dass die Filterfunktion bei der Statusabfrage (beim Parameter Order-ID → Auftragsnummer) keysensitiv ist und somit Groß-/Kleinschreibung geprüft wird.

Die Formate der einzelnen Dateien werden in den nachfolgenden Kapiteln im Detail beschrieben.

Sollte der Pollerprozess beim Verarbeiten von Mitteilungsdateien Fehler erkennen (Syntaxfehler, Datei nicht vollständig etc., siehe auch Anlage B), wird die Datei nicht weiter bearbeitet, sondern verbleibt im Verzeichnis und der Dateiname wird mit einem entsprechenden Fehlercode versehen (z.B. M_Auftrags-ID.IN_ERR0005, wenn die Datei noch nicht vollständig übertragen war).

2.3 Das Format einer Mitteilung

Die Mitteilungsdatei besteht aus einem Verwaltungsteil (Header) und den Nutzdaten (MIME bzw. S/MIME-Content). Die Struktur des Nutzdatenteils ist konform zu RFC 1521 und den zugehörigen nachfolgenden RFC bzw. zum RFC 5751 bei S/MIME. Im Verwaltungsteil der Mitteilung, der konform zum RFC 2822 (SMTP) aufgebaut ist, befinden sich Informationen, die sowohl vom Mailsystem als auch vom Empfänger benötigt werden, um die Mitteilung richtig zuordnen zu können. MessageGate nutzt nur die Elemente, die für die Verarbeitung unbedingt notwendig sind und überträgt diese in die X.400 Mitteilung. Wie bei SMTP-Mitteilungen üblich werden andere, unbekannte Elemente ignoriert.

Da der Verwaltungsteil der Mitteilung möglichst einfach strukturiert sein soll, werden viele für die Erzeugung der X.400 Mitteilung relevanten Parameter in Hostprofilen (MessageGate Benutzer bzw. Partnerschaftsprofil) hinterlegt.

Die Nutzdaten können aus einem Dokument/einer Datei bestehen oder aber aus mehreren (Multipart), die auch mit einer Signatur oder durch Verschlüsselung geschützt werden können. MessageGate akzeptiert aber keine Mitteilungen mit leerem Content. Um welchen MIME-Content es sich handelt, muss im Verwaltungsteil der Mitteilung definiert werden. Beispiele finden Sie im Anhang C.

Die maximale Gesamtgröße einer Mitteilung beträgt 100 MByte. Beim Versenden von ungesicherten Inhalten (kein S/MIME) können bis zu 50 Empfänger (getestet) angegeben werden, wobei mindestens ein „To:“ Empfänger enthalten sein muss. Bei S/MIME-Content ist nur ein Empfänger erlaubt. Bei ausgelieferten Mitteilungen werden alle Empfänger im RFC2822 Header angezeigt.

2.3.1 Der Header der Mitteilung

Für MessageGate sind die nachfolgenden Elemente des RFC2822 Header relevant. Die Klassifizierung in obligatorisch und optional gilt dabei nur für zu versendende Mitteilungen (*.IN). Bei Mitteilungen, die MessageGate ausliefert (*.OUT), sind alle Felder enthalten.

From:

Absender der Mitteilung: optional (Format siehe nächstes Kapitel), wenn angegeben, muss die Adresse korrekt sein!

To:

Empfänger der Mitteilung: obligatorisch (Format siehe nächstes Kapitel)
Mindestens ein Empfänger mit To: muss enthalten sein

Cc:

Kopieempfänger der Mitteilung: optional (Format siehe nächstes Kapitel)

Bcc:

Blind Copy Empfänger der Mitteilung: optional (Format siehe nächstes Kapitel)

Message-ID:

Mitteilungsnummer, die in der zu versendenden X.400-Mitteilung verwendet werden soll bzw. aus der empfangenen X.400 Mitteilung übernommen wurde, optional.

Maximal 64 Zeichen, Printable String Zeichensatz. Bitte stellen Sie sicher, dass diese Nummer eindeutig ist, damit der Empfänger diese Mitteilung richtig verarbeiten und eine hierfür angeforderte Lesebestätigung (Receipt Notification) durch den MessageGate Prozess korrekt zugeordnet werden kann.

Wird keine Message-ID angegeben, übernimmt MessageGate die Auftrags-ID als Message-ID.

Beachten Sie bitte, dass das Telefax Gateway von *BusinessMail X.400* nur Mitteilungsnummern mit einer Länge von 16 Zeichen unterstützt und somit auf dem Deckblatt die restlichen Zeichen nicht anzeigt. Wenn Sie also Mitteilungen per Fax versenden wollen, sollten Sie entsprechend kurze Nummern wählen.

Subject:

In der X.400-Mitteilung zu verwendendes bzw. daraus entnommenes Betreff-Feld, optional. Maximal 128 Zeichen (Teletex Zeichensatz T.61)

Beachten Sie bitte, dass der MessageGate Prozess bei Mitteilungen, die er an der Dateischnittstelle ausliefert, abweichend vom Standard RFC 2822 deutsche Sonderzeichen (ä,ö.ü,Ä,Ö,Ü,ß) im Betreff unverändert darstellt. MessageGate akzeptiert aber bei Mitteilungen, die zum Versenden übergeben werden, neben dieser Darstellungsform auch eine standardkonforme Codierung mit ISO8859-1 Zeichensatz → "=?iso-8859-1?x?...txt...?=", wobei x=Q (quoted-printable) oder aber x=B (BASE64) definiert sein kann.

Date:

Datum der versendeten Mitteilung (Standard MIME Format mit Datum und Uhrzeit), optional.

MessageGate übernimmt diesen Wert nicht in die X.400 Mitteilung. Beispiele für Format:

2 Nov 2010 09:31:44 +0100

(Format des Absenzeitpunkts bei ausgelieferter Mitteilung, englische Abkürzung des Monats)

Tue, 2 Nov 2010 09:31:44

Disposition-Notification-To:

Anforderung einer Empfangsbestätigung/ eines Reports, optional. Die Umsetzung in entsprechende X.400 Reports erfolgt abhängig vom im Hostprofil hinterlegten Wert des Parameter „Empfangsbestätigungen Richtung X.400“ wie folgt:

0 → Anforderung Nicht Auslieferbestätigung (NDN, Non Delivery Notification)

1 → Anforderung Auslieferbestätigung (DN, Delivery Notification)

2 → Anforderung Lese- und Auslieferbestätigung (RN, Receipt Notification und DN)

Bitte lesen Sie auch das Kapitel 2.9.2 X.400 Reports, um mehr zu diesem Thema zu erfahren.

MessageGate führt diesen Parameter im RFC2822 Header einer ausgelieferten Mitteilung an, falls der Absender in der X.400 Mitteilung eine Lesebestätigung angefordert hatte und dieses Leistungsmerkmal im Kommunikationsprofil nicht unterdrückt wird. Wenn gewünscht, kann durch die Kundenanwendung der Versand einer Lesebestätigung angestoßen (siehe Kapitel 2.8 Lesebestätigung versenden) werden.

Wenn MessageGate eine Mitteilung ausliefert, wird zwischen den Hochkommata nach dem Parameter "Disposition-Notification-To:" die X.400 Adresse des Absenders eingetragen. Beim Versenden von Mitteilungen muss zwischen den Hochkommata nichts angegeben werden, da MessageGate diese Adresse nicht auswertet.

Bsp.:

Disposition-Notification-To: "" (Minimum beim Versenden)

Disposition-Notification-To: "c=de, a=viat; s=tester; O=testag" (Ausgelieferte Mitteilung)

X-MPDUID:

Mitteilungsnummer, die der X.400 MTA beim Versenden der Mitteilung zuweist (nur bei ausgelieferten Mitteilungen), maximal 32 Zeichen (bei versendeten Mitteilungen kann MPDUID als MTS-ID im Statusreport abgefragt werden)

MIME-Version:

Optional. Default: 1.0 (Es wird auch nur diese Version unterstützt).

Content-Type:

Format (Zeichensatz, Transfer Encoding) der Nutzdaten entsprechend dem MIME Standard (RFC 2045 „Multipurpose Internet Mail Extensions“ und den folgenden relevanten RFC) bzw. S/MIME V3.2 Standard (RFC 5751), obligatorisch.

Beschreibt den Nutzdatenbereich der Mitteilung. Muss zusammen mit „Content-Transfer-Encoding:“ und wenn vorhanden „Content-Disposition:“ immer am Ende des Header stehen, da getrennt durch eine Leerzeile dann der Nutzdatenbereich (Content) der Mitteilung folgt.

Folgende Content-Types werden unterstützt:

Einzelner Textanhang:

text/plain; charset=ISO-8859-1

Einzelner Binäranhang:

application/octet-stream

Mehrere Anhänge:

multipart/mixed; boundary="====_NextPart_Nr."

Signierter Inhalt:

multipart/signed; protocol="application/pkcs7-signature"; micalg=shaxxx;
boundary="====_NextPart_Nr."

(erlaubte Werte für xxx sind 1, 256, 384, 512)

Verschlüsselter (und eventuell signierter) Inhalt:

application/pkcs7-mime; smime-type=enveloped-data; name="smime.p7m"
(unterstützte Cipher Suites DES3, AES128, AES192, AES256)

Weitere Details siehe Kapitel 2.3.3 Die Nutzdaten der Mitteilung bzw. 2.3.4 S/MIME gesicherter Inhalt.

Content-Transfer-Encoding:

Kodierung eines Nutzdatenteils. Obligatorisch

7bit

8bit

quoted-printable

base64

binary

Content-Disposition:

Dateiname, unter dem der Nutzdatenteil abgelegt werden soll, optional.

2.3.2 Das Format der Adresse

Das hier beschriebene Format ist relevant für die Header Elemente „To:“, „Cc:“, „Bcc:“ und „From:“. Eine Adresse besteht aus zwei Teilen, dem Alias und der eigentlichen SMTP-Adresse. Bei MessageGate wird der Alias dazu benutzt, um eine X.400 Adresse zu übergeben. Die eigentliche SMTP-Adresse besteht aus dem Domainnamen „viat.de“ rechts vom @ Zeichen und dem Buchstaben „X“ oder der „User-ID“ (*BusinessMail X.400* interne Kennung) des Partners.

Mögliche Adressierungsformen sind:

- a) Adressieren des Partners über X.400 Adresse im Alias:

"X.400 Adresselemente, getrennt durch ein Semikolon" <x@viat.de>

Diese Adressform sollte benutzt werden, wenn für den Partner keine Partnerschaft und damit keine User-ID eingerichtet wurde oder ein Übergang (z.B. Fax-Gateway) angesprochen wird. Für das Erstellen der X.400 Mitteilung werden dann die im MessageGate User Profil hinterlegten Parameter verwendet. MessageGate nutzt diese Adressform, wenn Mitteilungen von Absendern ausliefert werden, für die in der Datenbank kein Eintrag/keine User-ID eingerichtet wurde.

Bsp. "c=de;a=viat;o=testteam;s=tester;g=erster" <x@viat.de>

Diese Adressform sollte auch benutzt werden, um die Gateway Dienste von *BusinessMail X.400* anzusprechen. Ein Beispiel für einen solchen Fall wäre eine Mitteilung an das Fax Gateway von *BusinessMail X.400*. Hier werden Fax spezifische Parameter in den DDA-Adressfelder übergeben. Die Inhalte der DDA-Felder können sich also je nach Auftrag/Ziel der Fax Mitteilung unterscheiden.

Bsp. "DDA:Service=Fax;DDA:Format=A4;X121=06212946911;A=viaT;C=DE" <x@viat.de>

Wird innerhalb eines Adressfeldes das Zeichen „;“ verwendet, muss dies doppelt angeführt werden, da MessageGate diese sonst als Trennzeichen zwischen den Adressfeldern interpretiert.

- b) Adressieren des Partners über Angabe der User-ID in SMTP-Adresse (Alias ist leer!)

"" <User-ID@viat.de>

Diese Adressform sollte benutzt werden, wenn der Empfänger ein Teilnehmer des MailBox Service von *BusinessMail X.400* ist oder aber wenn einem externen Partner eine User-ID zugeordnet wurde. Dies ist z.B. dann der Fall, wenn eine MessageGate oder eine EDI-Partnerschaft (siehe auch das Kapitel 2.5 Das Format der Transmissionsset Datei für weitere Details) eingerichtet wurde.

Bsp. "" <69365@viat.de>

- c) Adressieren des Partners über X.400 Adresse im Alias und unter Angabe der User-ID in SMTP-Adresse

"X.400 Adresselemente, getrennt durch ein Semikolon" <User-ID@viat.de>

Diese Adressform nutzt der MessageGate Prozess, wenn er Mitteilungen von Absender ausliefert, deren User-ID bekannt ist.

Bsp. "c=de;a=viat;o=testteam;s=tester;g=erster" <99999@viat.de>

Wird diese Adressform beim Versenden von Mitteilungen benutzt, so wertet MessageGate nur den X.400 Adressteil aus und verifiziert nicht die User-ID.

Die maximale Länge der Adresse sind 256 Zeichen (Alias + SMTP-Adressteil). Sollte dies nicht ausreichen, um Ihren Partner eindeutig zu adressieren, empfehlen wir einen Partnerprofileintrag vorzunehmen und diesen Partner dann über die User-ID zu adressieren.

Mögliche X.400 Adresselemente (bei der Bezeichnung der Elemente können sowohl Groß- als auch Kleinbuchstaben gewählt werden), die im Alias der Adresse genutzt werden können, sind:

C=xx;	Country Code (2 Zeichen Printable String, z.B. de)
A=xxxxx;	ADMD-Namen (16 Zeichen Printable String, z.B. viaT)
P=xxxxx;	PRMD-Namen (16 Zeichen Printable String, z.B. MGI)
O=xxxxx;	Organisationsnamen (64 Zeichen Printable oder Teletex String, z.B. Telekom)
OU1=xxxx;	Organisationseinheit 1 (32 Zeichen Printable oder Teletex String)
OU2=xxxx;	Organisationseinheit 2 (32 Zeichen Printable oder Teletex String)
OU3=xxxx;	Organisationseinheit 3 (32 Zeichen Printable oder Teletex String)
OU4=xxxx;	Organisationseinheit 4 (32 Zeichen Printable oder Teletex String)
DDA:xxx=xxxx;	Domain Defined Attributes (Typ mit 8 Zeichen = Wert mit 128 Zeichen, beide Printable oder Teletex String, z.B. service=fax)
S=xxxxx;	Nachname (Surname, 40 Zeichen Printable oder Teletex String)
G=xxxxx;	Vorname (Givenname, 16 Zeichen Printable oder Teletex String)
CN=xxxxx;	Commonname (64 Zeichen Printable oder Teletex String)
N-ID=xxxxx;	Boxkennung (Unique Agent ID, 32 Zeichen Numerisch)
X121=xxxxx;	Netzwerk Kennung (15 Zeichen Numerisch)
T-ID=xxxx;	Terminal Kennung (24 Zeichen Printable String)
I=xx;	Initialen (5 Zeichen Printable String)
Q=xxx;	Generation(qualifier) (3 Zeichen Printable String)

Abhängig von dem im Kommunikationsprofil gewählten „X.400 Content-Type“ (Mittelungstyp) werden bestimmte Adresselemente beim Versenden durch den MessageGate Prozess unterdrückt. So wird z.B. der Commonname nicht in der Absender- und auch der Empfängeradresse berücksichtigt, wenn „X.400 Content Type“ auf den Wert „IPM84“ gesetzt wurde.

Siehe auch die Erläuterung in Kapitel 2.9 Kommunikations-/Partnerschaftsprofile und im Anhang A X.400 Adresselemente.

2.3.3 Die Nutzdaten der Mitteilung

Welches Format die Nutzdaten haben, wird bereits im Header der Mitteilung beim Feld „Content-Type:“ festgelegt. Sie können eine Mitteilung versenden, bei der die Nutzdaten aus einem einzelnen Dokument/einem Anhang bestehen oder aber auch mehrere Dokumente anhängen, die gesichert (signiert und/oder verschlüsselt) oder ungesichert übertragen werden sollen.

Einen mittels S/MIME gesicherten Inhalt (der signiert und /oder verschlüsselt wurde) sendet der MessageGate Prozess immer als einzelnen FTAM Body Part innerhalb der X.400 Mitteilung, wobei bei nur signierten Inhalten als Name „smime.p7s“ und die OID "id-signedData" {1 2 840 113549 1 7 2} verwendet wird und bei verschlüsselten bzw. bei verschlüsselten und signierten Inhalten als Name „smime.p7m“ und die OID "id-signedAndEnvelopedData" {1 2 840 113549 1 7 4} (siehe auch nächstes Kapitel 2.3.4 S/MIME gesicherter Inhalt).

Wollen Sie nur ein einzelnes, ungesichertes Dokument versenden, muss im Verwaltungsteil beim „Content Type:“ der Typ des Anhangs (Text, binär) definiert werden. Im Feld „Content-Transfer-Encoding:“ legen Sie fest, in welchem Format die Daten übergeben werden. Binärdaten können sowohl mit BASE64 (7-Bit-Codierung) oder aber mit Binary (8-Bit-Codierung) an die Dateischnittstelle übergeben werden. Beim Versenden dekodiert dann der MessageGate Prozess die BASE64 codierten Daten und sendet diese in 8-Bit-(Binary)-Codierung.

Über einen Parameter im Hostprofil bzw. im Partnerschaftsprofil wird festgelegt, ob der MessageGate Prozess die Binärdaten in einer an der Dateischnittstelle ausgelieferten (empfangenen) Mitteilung als Binary oder aber BASE64 codiert bereitstellt.

Versenden Sie mehrere ungesicherte Dokumente in einer Mitteilung, muss dieser Inhalt als „multipart/mixed“ definiert und die einzelnen Dokumente dann in diesem Content (abgegrenzt durch Boundery Einträge) eingebunden werden.

Bei der Umsetzung des in der MIME Struktur übergebenen Nutzdatenanteils in die X.400 Mitteilung sind zwei der im Kommunikationsprofils aufgeführten Parameter relevant, „X.400 Content-Type“ und „Bodypart“.

Im „X.400 Content-Type“ wird festgelegt, welches Format beim Versenden der X.400 Mitteilungen genutzt wird. Standardmäßig wird „IPM88“ verwendet, das mehr X.400 Body Part Typen unterstützt und möglichst in der Grundeinstellung nicht geändert werden soll. Nur in Ausnahmen sollte „IPM84“ (z.B. bei Problemen mit Commonname in Adresse) in den Partnerschaftsprofilen eingestellt werden.

Die folgenden Umsetzregeln werden verwendet, um die Nutzdaten einer Mitteilung, die versendet werden soll, in äquivalenten X.400 Body Parts abzubilden. Die Regeln sind nur dann relevant, wenn im Kommunikationsprofil beim Parameter „Bodypart“ der Wert „Variable“ festgelegt wurde und sind auch abhängig vom dem im Kommunikationsprofil festgelegten „X.400 Content Type“ (Mitteilungstyp):

Textanhang:

text/plain; charset=ISO-8859-1

- Content-Transfer-Encoding:
 - 7 Bit
 - 8 Bit
 - quoted-printable
- *Content-Disposition:*
 - *Attachment; Filename=<Dateiname>*

wird umgesetzt in

- General Text Body Part, ISOLATIN1 (ISO 8859-1) Zeichensatz bzw. in IA5 IRV Repertoire, wenn Mitteilungen an externe Systeme ausgeliefert werden, die nur den X.400 Standard 1984 unterstützen. Beim Umsetzen auf 1984er Standard erfolgt dabei keine Zeichensatz-Konvertierung, das höchste Bit wird unverändert übernommen
- Wird ein Dateiname angegeben, erzeugt MessageGate zusammen mit dem Textinhalt einen BP15 FTBP (FTAM Body Part), damit diese Dateiinformation für den X.400 Empfänger erhalten bleibt. Falls der X.400 Empfänger FTBP nicht unterstützt, bitte den Text ohne Dateinamen übertragen oder aber eine Partnerschaft mit dem Mapping „IA5-Text“ bzw. „Iso-Latin-1“ einrichten.

Binäranhang:

application/octet-stream

- Content-Transfer-Encoding:
 - base64
 - binary

wird umgesetzt in

- Body Part 14

application/octet-stream

- Content-Transfer-Encoding:
 - base64
 - binary
- Content-Disposition:
 - Attachment; Filename=<Dateiname>

wird umgesetzt in

- Body Part 15 FTBP (FTAM Body Part), wenn Profil IPM88 eingestellt;
- Body Part 14 (Bilaterally defined Body Part), wenn Profil IPM84 eingestellt → der Dateiname geht verloren

Mehrteilig:

multipart/mixed; boundary="---=_NextPart_xxx....."

Die einzelnen Anhänge werden entsprechend den oben beschriebenen Umsetzregeln als äquivalente X.400 Body Parts in die Mitteilung eingefügt.

Ändern Sie im Kommunikationsprofil den Parameter „Bodypart“ nur dann, wenn Ihr Partner einen bestimmten Body Part Typ zwingend erwartet und Sie dies in Ihrer Anwendung nicht durchgängig abbilden können.

Informationen über diesen Parameter finden Sie auch im Kapitel 2.9 Kommunikations-/Partnerschaftsprofile.

Beispiele für Mitteilungen mit verschiedenen Content Typen sind in Anhang C: Beispiele für Mitteilungen und Reports aufgeführt.

Für Mitteilungen, die MessageGate ausliefert, gibt es feste Regeln, die vom Benutzer nicht geändert werden können.

Textanhang:

- General Text Body Part oder IA5Text
- ISOLATIN1-Zeichensatz oder IA5 Repertoire

wird umgesetzt in

- Content-Type:
 - text/plain
- Content-Transfer-Encoding:
 - 8Bit

Binäranhang:

- Body Part 14 (BP14)

wird umgesetzt in

- Content-Type:
 - application/octet-stream
- Content-Transfer-Encoding:
 - binary/base64 (abhängig von Parameter im Profil)

- Body Part 15 FTBP (FTAM Body Part)

wird umgesetzt in

- Content-Type:
 - application/octet-stream
- Content-Transfer-Encoding:
 - binary/base64 (abhängig von Parameter im Profil)
- Content-Disposition:
 - Attachment; Filename=<Dateiname>

Multibodypart:

wird umgesetzt in

multipart/mixed; boundary="====_NextPart_xxx...."

Die einzelnen Anhänge werden entsprechend den oben beschriebenen Umsetzregeln als MIME-Content Type in die Mitteilung eingefügt.

Folgende Besonderheiten sind zu beachten:

- Ältere X.400 Clients, die keinen BP15 FTBP unterstützen, fügen die Dateiinformation (Namen, Typ) der an eine Mitteilung angehängten Datei als sogenannte CDIF Information (IA5 Text Body Part) vor den eigentlichen Nutzdatenteil, der als Body Part 14 gesendet wird. MessageGate wertet diese CDIF Information aus und erzeugt einen Content Type application/octet-

stream mit Content-Disposition: Attachment; Filename. Dadurch verringert sich die Anzahl der in die SMTP-Mitteilung abgebildeten Body Parts.

- Der X.400 Standard kennt nur eine begrenzte Anzahl von Body Part Typen, während die MIME Spezifikation eine Vielzahl von Content Types enthält. MessageGate versucht anhand von vordefinierten Pattern den Inhalt eines Body Parts zu erkennen und den korrekten Content Type zu setzen. Momentan sind bei dieser DOCMAGIC Funktion Pattern für EDIFACT und PDF hinterlegt.

2.3.4 S/MIME gesicherter Inhalt

Soll der Inhalt einer Mitteilung signiert und/oder verschlüsselt an einem anderen X.400 Empfänger gesendet bzw. von diesem empfangen werden, muss dieser als S/MIME-Content (Struktur) angeliefert werden bzw. er wird entsprechend unverändert (bis auf parametergesteuerte Konvertierung Content Transfer Encoding von Binary in BASE64 bei verschlüsselten Inhalten) aus der X.400 Mitteilung übernommen.

In der X.400 Mitteilung wird der S/MIME-Content aus Kompatibilitätsgründen zu älteren X.400 Clients immer als einzelner BP15/ FTAM Body Part übertragen, der wenn notwendig sogar in einen BP14 konvertiert werden kann, ohne dass sich am Inhalt etwas ändert. Bitte stellen Sie vor Verwendung eines S/MIME-Content sicher, dass die Anwendung Ihres X.400 Partners diesen verarbeiten kann.

Bei den P7 Client Produkten FileWork und UA-FI ist die korrekte Behandlung solcher S/MIME-Content ab der Version 5.2 schon integriert und die Nutzdaten werden ungesichert bereitgestellt. Bei älteren X.400/ P7 Clients muss der S/MIME-Content mit geeigneten Tools, z.B. OpenSSL, bearbeitet werden, um an die Nutzdaten zu gelangen.

Sollten Sie Mitteilungen an einen externen Partner senden, dessen Mailservice mittels SMTP MTA (siehe Kapitel 7 SMTP MTA und MessageGate) angebunden ist, sollten Sie möglichst die in den S/MIME-Content eingebundenen Dokumente schon mit einem passenden Content Transfer Encoding versehen, also z.B. bei Text Anhängen dann Quoted printable und bei binären Anhängen und falls vorhandenen auch bei der Signatur dann BASE64, da weder das File Interface beim Versenden noch der SMTP MTA beim Ausliefern der Mitteilung eine Änderung des Encodings vornehmen kann, da ansonsten die Signatur ungültig wird. Verschlüsselte Inhalte können diese Prozesse mangels privaten Schlüssel ohnehin nicht einsehen.

Nachfolgend werden die entsprechenden Regeln beim Versenden und Empfangen von gesicherten Mitteilungen im Detail beschrieben.

1. Folgende Regel gilt für das Versenden von signierten Inhalten (ein oder mehrere Dokumente mit Signatur inkl. des Zertifikats des Signierenden als eigener MIME Body Part, micalg=SHA1, SHA256, SHA384, SHA512 unterstützt):

Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=shaxxx; boundary=---...

Content-Transfer-Encoding: binary >>> (Nur wenn für signierten MIME-Content als Encoding „Binary“ verwendet wird, ansonsten entfällt Eintrag)

<Leerzeile>

This is a S/MIME signed message

<Leerzeile>

```

boundary=---...
<MIME Content>
Boundary=---...
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: binary/base64 >>> (Auswahl binary oder BASE64)
Content-Disposition: attachment; filename="smime.p7s"
Boundary=---...--

```

>>> wird umgesetzt in

Body Part 15 FTBP (FTAM Body Part)

Name= smime.p7s

OID = "id-signedData" {1 2 840 113549 1 7 2}

>>> Der gesamte S/MIME-Content wird unverändert übernommen, gilt auch für das Content-Transfer-Encoding bei der Signatur

2. Folgende Regel gilt für das Versenden von verschlüsselten Inhalten (ein oder mehrere Dokumente, unterstützte Cipher Suites DES3, AES128, AES192, AES256):

```

Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name="smime.p7m"

```

```

Content-Transfer-Encoding: binary/base64... >>> (Auswahl binary or BASE64)

```

```

Content-Disposition: attachment; filename="smime.p7m"

```

```

<Leerzeile>

```

```

<verschlüsselter MIME-Content>

```

>>> wird umgesetzt in

Body Part 15 FTBP (FTAM Body Part)

Name= smime.p7m

OID = "id-signedAndEnvelopedData" {1 2 840 113549 1 7 4}

>>> Das Content-Transfer-Encoding BASE64 wird dabei in Binary umgesetzt

3. Folgende Regel gilt für das Versenden von signierten und verschlüsselten Inhalten (ein oder mehrere Dokumente mit Signatur inkl. des Zertifikats des Signierenden als eigener MIME Body Part, micalg=SHA1, SHA256, SHA384, SHA512 unterstützt):

```

Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=
shaxxx; boundary=---....

```

```

Content-Transfer-Encoding: binary >>> (Nur wenn für signierten MIME-Content
als Encoding „Binary“ verwendet wird, ansonsten entfällt Eintrag)

```

```

<Leerzeile>

```

```

This is a S/MIME signed message

```

```

<Leerzeile>

```

```

boundary=---...

```

```

<MIME Content>

```

Boundary=---...

Content-Type: application/pkcs7-signature; name="smime.p7s"

Content-Transfer-Encoding: binary/base64 >>> (Auswahl binary oder BASE64)

Content-Disposition: attachment; filename="smime.p7s"

Boundary=---...--

>>> wird eingebettet in

application/pkcs7-mime; smime-type=enveloped-data; name="smime.p7m"

Content-Transfer-Encoding: binary/base64 >>> (Auswahl binary oder BASE64, unterstützte Cipher Suites 3DES, AES128, AES192, AES256)

Content-Disposition: attachment; filename="smime.p7m"

<Leerzeile>

<Verschlüsselter und signierter MIME-Content>

>>> und umgesetzt in

Body Part 15/ FTBP (FTAM Body Part)

Name= smime.p7m

OID = " id-signedAndEnvelopedData" {1 2 840 113549 1 7 4}

>>> Das Content-Transfer-Encoding BASE64 wird in Binary umgesetzt

4. Folgende Regeln gelten beim Empfangen von signierten Inhalten:

Body Part 15/ FTBP (FTAM Body Part)

Name= smime.p7s

OID = "id-signedData" {1 2 840 113549 1 7 2}

>>> wird umgesetzt in

Content-Type: multipart/signed; protocol="application/pkcs7-signature";

micalg=shaxxx; boundary= >>> (mit Signatur inkl. des Zertifikats des Signierenden im separaten MIME Body Part)

Content-Transfer-Encoding: binary >>> (Nur wenn für signierten MIME-Content als Encoding „Binary“ verwendet wird, ansonsten entfällt Eintrag)

<Leerzeile >

This is a S/MIME signed message

<Leerzeile>

boundary=---...

<MIME Content>

Boundary=---...

Content-Type: application/pkcs7-signature; name="smime.p7s"

Content-Transfer-Encoding: binary/base64 >>> (Auswahl binary oder BASE64)

Content-Disposition: attachment; filename="smime.p7s"

Boundary=---...--

5. Folgende Regeln gelten beim Empfangen von verschlüsselten Inhalten:

Body Part 15/ FTBP (FTAM Body Part)

Name= smime.p7m

OID = " id-envelopedData" {1 2 840 113549 1 7 3}

>>> oder

Body Part 15/ FTBP (FTAM Body Part)

Name= smime.p7m

OID = " id-signedAndEnvelopedData" {1 2 840 113549 1 7 4}

>>> wird umgesetzt in

Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name="smimep7m"

Content-Transfer-Encoding: binary/base64 >>> (binary or BASE64 abhängig
vom Parameter in Partnerschaft)

Content-Disposition: attachment; filename="smime.p7m"

<Leerzeile>

<verschlüsselter signierter MIME-Content>

6. Folgende Regeln gelten beim Empfangen von verschlüsselten und signierten Inhalten:

Body Part 15 FTBP (FTAM Body Part)

Name= smime.p7m

OID = " id-signedAndEnvelopedData" {1 2 840 113549 1 7 4}

>>> wird umgesetzt in

Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name="smime.p7m"

Content-Transfer-Encoding: binary/base64 >>> (binary oder BASE64 abhängig
vom Parameter in Partnerschaft)

Content-Disposition: attachment; filename="smime.p7m"

<Leerzeile>

<verschlüsselter signierter MIME-Content>

>>> mit eingebettetem signiertem Inhalt:

Content-Type: multipart/signed; protocol="application/pkcs7-signature"; mi-
calg=shaxxx; boundary=---.... >>> (unterstützte Werte für micalg SHA1,
SHA256, SHA384, SHA512)

Content-Transfer-Encoding: binary >>> (Nur wenn für signierten MIME-Content
als Encoding „Binary“ verwendet wird, ansonsten entfällt Eintrag)

<Leerzeile>

This is a S/MIME signed message

<Leerzeile>

boundary=---...

```
<MIME Content>
Boundary=----...
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: binary/base64 >>> (Auswahl binary or BASE64)
Content-Disposition: attachment; filename="smime.p7s"
Boundary=----...--
```

2.4 Kein Weiterleiten von empfangenen Mitteilungen

Beim MessageGate File Interface ist es nicht vorgesehen, empfangene Mitteilungen weiterzuleiten. Leitet ein Partner eine Mitteilung an einen MessageGate File Interface Benutzer weiter, so werden nur die Nutzdaten durchgereicht. Die Information, dass die Mitteilung weitergeleitet wurde, geht verloren.

2.5 Das Format der Transmissionsset Datei

2.5.1 Die zentrale EDI-Funktion

Neben dem Adressieren von Partnern über die X.400 Adresse im Header einer Mitteilung bietet der MailBox X.400 Service von *BusinessMail X.400* auch die Möglichkeit, über die zentrale EDI-Funktion direkt EDIFACT Interchange (einen oder mehrere) als Nutzdaten (Transmissionsset Datei) zum Versand zu übergeben. Die zugehörige X.400 Empfängeradresse ergänzt das System dabei anhand der vorher in der Datenbank hinterlegten EDI Trading Partnerschaftseinträge. Die zentrale EDI-Funktion unterstützt momentan nur ein EDIFACT Dokument (Interchange) pro Mitteilung, das als Text Body oder aber als binärer Body (BP14 ohne Dateiinformation) gesendet bzw. empfangen werden kann. Somit liefert die zentrale EDI-Funktion auch nur Transmissionsset Dateien an der Dateischnittstelle aus, die einen Interchange enthalten. Da aber diese Beschränkung in einer der nächsten Versionen von MessageGate aufgehoben werden kann, sollten Anwendungen so implementiert werden, dass sie auch empfangene Transmissionsset Dateien verarbeiten können, die mehr als einem Interchange enthalten.

Bitte beachten Sie bei aktivierter zentraler EDI-Funktion, dass aufgrund der Beschränkung auf einen EDIFACT Interchange die Mitteilungen, die Ihr Partner sendet und die mehrere EDIFACT Interchange oder einen EDIFACT Interchange und andere Anhänge enthalten, von der zentralen EDI-Funktion mit der Fehlermeldung „Invalid arguments“ (Reason:1, Diagnostic:11) abgewiesen werden. Wenn Sie den Status von empfangenen Mitteilungen abfragen, werden Sie auch die Einträge für abgewiesene Mitteilungen finden.

Da ja die Transmissionsset Dateien keinen RFC2822 Header enthalten, wird beim Versenden einer X.400 Mitteilung deren Betreff und auch die Message ID aus der Interchange Referenznummer im UNB abgeleitet:

Message ID: <INTERCHANGE CONTROL REFERENCE> (max. 14 Zeichen)

Subject: EDIFACT <INTERCHANGE CONTROL REFERENCE> (max. 22 Zeichen)

Die im nächsten Kapitel beschriebenen Nutzdaten werden auf Basis des im EDI Trading Partnerschaftseintrags hinterlegten Wertes für „Bodypart“ (standardmäßig Text Body Part ISO-Latin-1) an eine zu versendende X.400 Mitteilung gehängt. Sollte Ihr

Partner erwarten, dass die Daten als binärer Anhang (BP14) gesendet werden, müssen Sie für diesen Parameter im Profil den Wert „Bilateral Bodypart 14“ festlegen. Den Content-Type „EDI“ (X.435/ PEDI) sollten Sie nur dann benutzen, wenn der Partner kein anderes Format unterstützt. Bitte beachten Sie dabei, dass auch hier die Beschränkung auf ein EDIFACT Dokument gilt und PEDI-Mitteilungen mit mehr als einem Body Part abgewiesen werden.

Um die zentrale EDI-Funktion nutzen zu können, muss dem MessageGate Benutzer bzw. dessen X.400 Adresse mindestens eine EDI-Kennung zugeordnet werden, die aus einer EDI ID (z.B. ILN/GLN) und einem optionalen EDI Qualifier (z.B. 14 für Handel oder 65 für X.400) besteht. Diese Kennung erwartet MessageGate als EDI-Sender im UNB beim Versenden des Interchange bzw. als EDI-Receiver, wenn ein Partner ein EDIFACT Dokument sendet.

Standardmäßig liefert die zentrale EDI-Funktion dann EDIFACT Dokumente an einen MessageGate Nutzer aus, wenn die Empfängeradresse im UNB diesem Benutzer zugeordnet wurde, unabhängig von der Absenderadresse. Es ist aber auch möglich, sich für jede eigene EDI-Kennung eine Closed User Group (CUG) zu konfigurieren, bei der nur die EDIFACT Dokumente konfigurierter EDI Trading Partner ausgeliefert werden.

Für jeden Geschäftspartner, die der MessageGate Nutzer über die zentrale EDI-Funktion ansprechen (an den er Mitteilungen versendet) will, muss ein EDI Trading Partnerschaftseintrag eingerichtet werden, der ebenfalls aus einer EDI-Kennung und einer zugehörigen X.400 Adresse besteht. Bei dieser Partnerschaft kann das Testflag im UNB mit ausgewertet werden, falls der Partner sowohl über eine Wirkumgebung/ -adresse als auch eine Testumgebung/ -adresse verfügt und für beide Mailboxen dieselbe EDI-Kennung genutzt werden soll. Diese Partnerschaft würde auch herangezogen, wenn wie oben beschrieben, bei einem empfangenen EDIFACT Dokument beim EDI-Empfänger im UNB (eigenen EDI-Kennung) eine geschlossene Benutzergruppe eingerichtet ist.

Gibt es bei aktivierter Testflag-Überprüfung nur eine Partnerschaft, werden nur EDIFACT Dokumente versendet, in denen das Testflag gesetzt wurde (siehe hierzu das EDI Prozess Handbuch, das auf der Service-Seite von *BusinessMail X.400* <https://www.service-viat.de> heruntergeladen werden kann). Diese Partnerschaft kann einer oder auch mehreren EDI-Kennungen des MessageGate Benutzers zugeordnet werden. Für die Erstellung von X.400 Mitteilungen wird auf die Parameter zurückgegriffen, die ebenfalls in der EDI Trading Partnerschaft konfiguriert wurden.

Abhängig von dem im Hostprofil hinterlegten Wert für „Empfangsbestätigungen Richtung X.400“ werden in der X.400 Mitteilung folgende Reports angefordert:

0 → Anforderung Nicht Auslieferbestätigung (NDN, Non Delivery Notification)

1 → Anforderung Auslieferbestätigung (DN, Delivery Notification)

2 → Anforderung Lese- und Auslieferbestätigung (RN, Receipt Notification und DN)

Bitte lesen Sie auch das Kapitel 2.9.2 X.400 Reports, um mehr zu diesem Thema zu erfahren.

Bitte beachten Sie bei der Nutzung der zentralen EDI-Funktion, dass diese zwar den Nutzdatenteil des EDIFACT Dokumentes nicht prüft, jedoch einen Syntaxcheck der Elemente UNA, UNB und UNZ vornimmt. Werden Syntax Fehler erkannt (z.B. fehlende Leerzeichen im UNA oder aber unterschiedliche Referenznummern im UNB und UNZ), wird das Dokument nicht ausgeliefert. Bei empfangenen Mitteilungen erhält der Absender in diesem Fall eine Non Delivery Notification (NDN) mit Diagnostic Code 0x“0B“ (11 dezimal, Invalid Arguments).

Kann das Dokument aufgrund von Syntax Probleme nicht als EDIFACT erkannt werden, wird es als normale Mitteilung ausgeliefert. Bei Interchanges, die versendet werden sollen, wird der Status auf Fehler gesetzt. Gibt der Absender bei empfangenen Mitteilungen eine falsche ILN als Empfänger an oder wurde keine Partnerschaft bei einer CUG konfiguriert, wird die Mitteilung ebenfalls verworfen und der Absender erhält eine NDN mit dem Diagnostic Code 0x"11" (17 dezimal, No bilateral Agreement).

Informationen darüber, ob Mitteilungen zurückgewiesen wurden, können Sie durch Anfordern eines Statusreports erhalten. Bitte geben Sie bei dieser Anforderung an, dass auch die Einträge für empfangene (und damit auch abgewiesene) Mitteilungen (Direction: Both oder Received) aufgelistet werden. Siehe auch Kapitel 2.7 Der Statusreport.

2.5.2 Die Nutzdaten der Transmissionsset Datei

In einer Transmissionsset Datei können mehrere EDIFACT Interchange an die zentrale EDI-Funktion übergeben werden. Leerzeilen zum Separieren der Interchange sind erlaubt, aber nicht unbedingt notwendig.

Die Anzahl der Interchange pro Transmissionsset Datei ist theoretisch nicht limitiert, jedoch empfehlen wir nicht mehr als 100 Interchange pro Transmissionsset Datei vorzusehen. Die Größe der Datei sollte dabei 100 MByte nicht überschreiten.

Eine Transmissionsset Datei, die der MessageGate Prozess an der Dateischnittstelle ausliefert, enthält jedoch Prozesstechnisch bedingt immer nur einen EDIFACT Interchange, da Mitteilungen bzw. deren Inhalt sofort ausgeliefert werden. Diese Beschränkung kann aber in einer späteren Version von MessageGate aufgehoben werden. Wir empfehlen, dass Ihre Anwendung schon darauf vorbereitet wird.

Über einen Parameter im Hostprofil kann außerdem festgelegt werden, ob ein von der zentralen EDI-Funktion über den MessageGate Prozess ausgelieferter EDIFACT Interchange als Transmissionsset Datei oder als Mitteilung mit MIME-Struktur an der Dateischnittstelle abgelegt wird.

Siehe auch Kapitel 2.9 Kommunikations-/Partnerschaftsprofile.

2.6 Closed User Group (CUG)

Unabhängig von der zentralen EDI-Funktion kann auch generell für den MessageGate Account eine Closed User Group aktiviert werden, so dass nur konfigurierte Partner (in WebConfig angelegte Partnerschaft) Dokumente/Mitteilungen ausliefern können. Wie bereits im letzten Kapitel beschrieben, erhält ein nicht konfigurierter Absender dann eine NDN mit dem Diagnostic Code 0x"11" (17 dezimal, No bilateral Agreement). Die Closed User Group kann sogar so weit eingegrenzt werden, dass der konfigurierte Absender nur einen Text Body Part, nur einen binären Body Part oder nur einen beliebigen Body Part anliefern darf, falls die Geschäftsbeziehung bestimmte Inhalte (z.B. bei Übertragung von UTF-8 codierten Inhalten ist binärer Body Part verpflichtend oder bei Web Service Profil v3) voraussetzt. Die Einschränkung auf einen Body Part kann auch ohne Closed User Group aktiviert werden. Bitte stimmen Sie mit der Administration von BusinessMail X.400 ab, ob und in welcher Ausprägung dieses Leistungsmerkmal für Ihren MessageGate Account aktiviert werden soll.

2.7 Der Statusreport

2.7.1 Allgemein

Um die Komplexität der Dateischnittstelle möglichst gering zu halten (nur Übergabe von Mitteilungen bzw. Nutzdaten) wurde darauf verzichtet, Quittierungsmechanismen zu implementieren und X.400 Reports an der Dateischnittstelle auszuliefern. Stattdessen werden die relevanten Statusinformationen von Mitteilungen, die der MessageGate Prozess bearbeitet (versendet oder ausliefert) hat, in einer Datenbankrelation (Trace Tab) befristet gespeichert. Der MessageGate Nutzer kann die Einträge über entsprechende Statusreports abfragen und erhält Informationen, die er seinem Verarbeitungsprozess (z.B. Konverter) und dessen Tracking Mechanismen zuführen kann. Abhängig von dem im Benutzerprofil eingestellten Wert werden die Einträge in dieser Tabelle zu einem bestimmten Zeitpunkt (Purge Time ist standardmäßig 240 Stunden → Einträge müssen mindestens 240 Stunden alt sein, damit diese bei einem Purgerlauf gelöscht werden; ist kundenindividuell änderbar durch Administration von *BusinessMail X.400*) gelöscht.

Wird eine Mitteilung an mehrere Empfänger versendet, so wird pro Empfänger ein Eintrag im Statusreport erzeugt. In diesem Fall sind die Message-ID bzw. die Order-ID nicht eindeutig und es muss nun auch die Empfängeradresse bei der Verarbeitung der Daten berücksichtigt werden.

Beachten Sie dabei, dass die Reihenfolge der Einträge im Statusreport nicht unbedingt der Reihenfolge der Empfänger in der Mitteilung entsprechen muss.

Bei empfangenen Mitteilungen wird immer nur ein Eintrag erzeugt, auch wenn der Absender diese Mitteilung an mehrere Empfänger versendet hatte. Diese zusätzlichen Empfänger werden nur in der ausgelieferten Mitteilung angezeigt.

Im Statusreport wird immer die Adresse angezeigt, die auch im RFC2822 Header der Mail benutzt wurde. Dies gilt auch für die Art der Adressierung. Hier wird aber abweichend von der Mail eine Einheitsschreibweise (erster Buchstabe groß und der Rest klein) verwendet → „To:“, „Cc:“ und „Bcc:“.

2.7.2 Anfordern eines Statusreports

Ein Statusreport kann mit einer entsprechenden Auftragsdatei (S_Auftrags-ID.IN) angefordert oder aber per Benutzerprofil automatisch erzeugt und zugestellt werden. Letzteres ist über *WebConfig* (siehe 2.9.8 Automatischen Statusreport konfigurieren) konfigurierbar. *WebConfig* erlaubt Ihnen auch Statusreports in der Oberfläche anzusehen oder als strukturierte Datei (CSV-Datei) herunterzuladen. Mehr Details finden Sie im Kapitel 2.9.7 Statusreport abfragen.

Bitte beachten Sie, dass es eine individuell durch die MessageGate Administration konfigurierbare Sperrzeit (Default ist zurzeit eine Abfrage alle 5 Minuten) nach einer Statusreportabfrage per Auftragsdatei gibt. Alle in diesem Zeitraum eingestellten Dateien werden mit einem Fehlercode (9999) versehen und es wird keine Reportdatei erzeugt.

Um die Menge der beim Statusreport bereitgestellten Informationen einzugrenzen, können in der Datei Schlüsselwörter angegeben werden, mit denen nur bestimmte Einträge selektiert und deren Ausgabeumfang (nur aktuellen Status der Mitteilung oder gesamte Historie der Transaktion in lesbarer oder vor allem maschinell bearbeitbarer Form) festgelegt wird.

Selektionskriterien sind

- ob der Eintrag seit der letzten Statusabfrage modifiziert wurde
- ob es sich um eine versendete oder empfangene Mitteilung handelt
- nur bestimmte Mitteilungsnummern/-ID
- nur bestimmte Auftragsnummern/-ID
- ab einem bestimmten Datum (versendet bzw. empfangen)

Über einen zusätzlichen Parameter kann festgelegt werden, ob nur der aktuelle Status oder eine komplette Historie (im strukturierten/lesbaren oder im CSV-Format) eines Eintrages ausgegeben wird.

Selektionskriterium:	Erläuterung:
Disposition: all	Selektiert alle Einträge, unabhängig ob sich der Status geändert hat oder nicht (Default) .
Disposition: Modified	Selektiert die Einträge, deren Status sich seit der letzten Abfrage geändert hat (z.B. wurden DN/NDN oder RN/NRN zugeordnet).
Direction: Sent	Selektiert nur versendete Mitteilungen (Default) .
Direction: Received	Selektiert nur empfangene Mitteilungen.
Direction: Both	Selektiert versendete und empfangene Mitteilungen.
Format: Actual	Zeigt nur den aktuellen Status der Mitteilungen mit Zeitstempel der letzten Änderung (Default) in lesbarer Form.
Format: History	Zeigt alle relevanten Statusänderungen der Mitteilungen mit Zeitstempel (Versendet/ Empfangen, Zuordnung von DN/NDN bzw. RN/NRN) in lesbarer Form.
Format: CSV-S	Liefert den Statusreport als CSV-Datei mit Semikolon als Trennzeichen, bei dem alle relevanten Statusänderungen der Mitteilungen (entspricht History) angezeigt werden.
Format: CSV-C	Liefert den Statusreport als CSV-Datei mit Komma als Trennzeichen, bei dem alle relevanten Statusänderungen der Mitteilungen (entspricht History) angezeigt werden.
Message-ID: xxx*	Zeigt nur Einträge, bei denen die Mitteilungs-ID mit dem angegebenen String beginnt. Einen Teilstring immer mit „*“ abschließen. Wird der Parameter nicht angegeben, wird er auch nicht berücksichtigt.
Order-ID: xxx*	Zeigt nur Einträge, bei denen die Auftrags-ID mit dem angegebenen String beginnt. Einen Teilstring immer mit „*“ abschließen. Prozesstechnisch bedingt ist der Wert Case sensitive,

	deshalb beachten Sie die Groß- /Kleinschreibung beim Suchstring. Wird der Parameter nicht angegeben, wird er auch nicht berücksichtigt.
Since: dd-mmm-yyyy hh:mm:ss	Zeigt alle Einträge, die ab einem bestimmten Zeitpunkt in der Datenbanktabelle abgelegt wurden (mmm- englische Kurzschreibweise für Monat). Geben Sie hier nur ein Datum ohne Uhrzeit an, werden alle Einträge, die an diesem Tag erfolgt sind, berücksichtigt. Wird der Parameter nicht angegeben, wird er auch nicht berücksichtigt.

Für die ersten zwei Kriterien und auch für das Ausgabeformat sind Defaults definiert, die MessageGate verwendet, wenn der jeweilige Parameter nicht angegeben wurde. Durch Angabe von mehreren Kriterien kann die Anzahl der im Report angeführten Einträge noch weiter eingeschränkt werden (Logische „Und Verknüpfung“).

Benutzt MessageGate die drei Defaults, werden alle Einträge für versendete Mitteilungen ausgegeben, die in der Datenbanktabelle für diesen MessageGate Benutzer angelegt und noch nicht vom Purger gelöscht wurden. Und dies unabhängig davon, ob der Status seit der letzten Anfrage verändert wurde. Es wird nur eine Information über den aktuellen Status der Mitteilung angezeigt.

2.7.3 Syntax des Statusreports (strukturierte Form)

Hat der MessageGate Prozess eine entsprechende Auftragsdatei (S_Auftrags-ID.IN) verarbeitet, wird er anhand der vorgegebenen Selektionskriterien die Datenbanktabelle nach Einträgen durchsuchen und eine Statusdatei zusammenstellen. Für diese Datei wird er den gleichen Namen wählen, jedoch die Extension durch „.OUT“ ersetzen.

Bitte beachten Sie besonders beim Namen der Auftragsdatei eines Statusreports, dass Sie eine eindeutige Auftragsnummer zuordnen. Das Betriebssystem des Applikationsservers überschreibt bei dem Erstellen der Statusdatei keine vorhandene Datei. Der neuen Datei wird lediglich eine um Eins erhöhte Versionsnummer zugeordnet. Manche SFTP Clients zeigen die entsprechende Versionsnummer (Format: Dateiname.Extension;Versionsnummer) an. Bei HTTPS/WebDAV bzw. HTTPS/Web-Service sieht man die Versionsnummer aber nicht. Dieses Verhalten kann somit bei Ihrer Anwendung zu Problemen führen, falls die Auftragsnummer nicht eindeutig sein sollte.

Der Inhalt der Statusreport Datei besteht aus einem Header und den einzelnen Einträgen. Der Header besteht aus zwei Zeilen, wobei in der ersten die User-ID des MessageGate Benutzers und ein Zeitstempel für das Erstellen des Reports und in der zweiten die berücksichtigten Filterkriterien angegeben werden.

Nach einer Leerzeile (CR/LF) folgen dann die einzelnen Einträge, die dann wieder durch eine Leerzeile voneinander getrennt sind.

Abhängig vom Kriterium „Format“ besteht ein Eintrag immer aus 6 Zeilen (Actual) oder aus 5-7 Zeilen (History). Die Zeilen mit Sender/Empfänger, Auftrags-ID, Message-ID und MTS/MTA ID sind bei beiden Formaten gleich, lediglich der Detaillierungsgrad beim Status unterscheidet sich.

Syntax 1. Zeile Header

Status Report for UserID xxxxx; generated dd-mmm-yyyy hh:mm:ss

Die User-ID ist mindestens 4-stellig, kann aber auch 5 oder 6 Stellen haben.

Beim Datum steht dd für den Tag des Monats (ohne führende Null bei 1-stelligem Tag), mmm für den Monat (englische Kurzschreibweise des Monatsnamens), yyyy für das Jahr (4-stellig), hh für die Stunde (24 Stunden Schreibweise, mit führender 0 bei 1-stelliger Stundenzahl), mm für die Minute (mit führender 0 bei 1-stelliger Minutenzahl) und ss für die Sekunde (mit führender 0 bei 1-stelliger Sekundenzahl). Zeit ist entweder MEZ oder MESZ, siehe auch Syntax Eintrag.

z.B.

Status Report for UserID 4911; generated 13-Sep-2010 13:43:32

Status Report for UserID 23423; generated 7-Sep-2010 07:12:01

Syntax 2. Zeile Header

Filters: Disposition=x, Direction=x, Format=x, Message-ID=x, OrderID=x, Since=dd-mmm-yyyy

Der Wert wird bei jedem Kriterium direkt nach dem „=“ eingefügt, ohne Leerzeichen. Die einzelnen Kriterien sind durch „,“ und einem Leerzeichen getrennt. Nur die Kriterien „Disposition=“, „Direction=“ und „Format=“ werden in der 2. Zeile immer angezeigt, die anderen nur wenn in Statusabfrage (Request) definiert.

- Bei „Disposition=“ können die Werte „All“ oder „Modified“ stehen.
- Bei „Direction=“ können die Werte „Sent“, „Received“ oder „Both“ stehen.
- Bei „Format=“ können die Werte „Actual“ oder „History“ stehen.
- Bei „Message-ID=“ kann entweder ein Suchstring stehen, wenn im Request angegeben oder der Wert wird nicht angezeigt.
- Bei „Order-ID=“ kann entweder ein Suchstring stehen, wenn im Request angegeben oder der Wert wird nicht angezeigt.
- Bei „Since=“ kann entweder ein Datum (dd-mmm-yyyy hh:mm:ss) stehen, wenn im Request angegeben oder der Wert wird nicht angezeigt. Beachten Sie dabei die „Lebensdauer“ von Einträgen in der Datenbank (Purge Time der Trace Tab).

z.B.

Filters: Disposition=All, Direction=Both, Format=Actual, Since=1-Jan-2011

➔ alle Einträge, unabhängig vom Statuswechsel und ob versendet oder empfangen, die seit dem 01.01.2011 00:00:00 in der Tabelle angelegt wurden, mit aktuellem Status ausgeben

Filters: Disposition= Modified, Direction=Received, Format=History

➔ alle Einträge, deren Status sich seit der letzten Abfrage geändert hat und die sich auf empfangene Mitteilungen beziehen, mit allen Statusänderungen ausgeben

Filters: Disposition= Modified, Direction=Sent, Format=History, Order-ID=EDI*

➔ alle Einträge, deren Status sich seit der letzten Abfrage geändert hat und die sich alle versendeten Mitteilungen beziehen und deren Auftrags-ID mit „EDI“ anfängt, mit allen Statusänderungen ausgeben

Syntax Eintrag von versendeter Mitteilung mit Format Actual

Die Zeile besteht immer aus dem Feldnamen, der mit einem Doppelpunkt „:“ abgeschlossen wird, einem Leerzeichen und dem Wert, der wiederum ebenfalls Leerzeichen enthalten kann. Bei der Adresse des Empfängers kann abhängig von der versendeten Mitteilung entweder „To:“, „Cc:“ oder „Bcc:“ stehen.

To:	Adresse des Empfängers laut Mitteilung. Bei einem über die zentrale EDI-Funktion übergebenen EDIFACT Dokument hat die Adresse immer das Format "" <user-id@viat.de>
Cc:	Adresse des Kopie-Empfängers laut Mitteilung.
Bcc:	Adresse des Blind copy Empfängers laut Mitteilung.
Order-ID:	Auftragsnummer aus Dateinamen (maximal 26 Zeichen)
Message-ID:	Mitteilungsnummer laut Mitteilung bzw. bei einem EDIFACT Dokument die Reference ID des Interchange (maximal 64 Zeichen)
MTS-ID:	Die vom MTA beim Versenden der Mitteilung vergebene Kennung.
Status:	Der aktuelle Status der Mitteilung (mögliche Werte finden Sie am Ende des Kapitels)
Date:	Der Zeitpunkt der letzten Statusänderung mit dem Format dd-mmm-yyyy hh:mm:ss +xxxx, wobei dd für den Tag (ohne führende Null bei 1-stelligem Tag), mmm für den Monat (englische Kurzschreibweise), yyyy für das Jahr (4-stellig), hh für die Stunde (mit führender 0 bei 1-stelliger Stundenzahl), mm für die Minute und ss für die Sekunden steht. Der Wert +xxxx zeigt die Korrektur im Vergleich zu UTC/GMZ, also +0100 bei MEZ oder +0200 bei MESZ (Sommerzeit) an

Syntax Eintrag von empfangener Mitteilung mit Format Actual

Die Zeile besteht immer aus dem Feldnamen, der mit einem Doppelpunkt „:“ abgeschlossen wird, einem Leerzeichen und dem Wert, der wiederum ebenfalls Leerzeichen enthalten kann.

From:	Adresse des Absenders
Order-ID:	Durch MessageGate vergebene Auftragsnummer (maximal 26 Zeichen)
Message-ID:	Mitteilungsnummer, die Absender in seiner Mitteilung vorgesehen hat (maximal 64 Zeichen)
MTS-ID:	Die vom Partner MTA beim Versenden der Mitteilung vergebene Kennung (maximal 32 Zeichen). Entspricht dem Wert X-MPDUID im Header der SMTP-Mitteilungsstruktur.
Status:	der aktuelle Status der Mitteilung (mögliche Werte finden Sie am Ende des Kapitels)
Date:	Der Zeitpunkt der letzten Statusänderung mit dem Format dd-mmm-yyyy hh:mm:ss +xxxx, wobei dd für den Tag des Monats (ohne führende Null bei 1-stelligem Tag), mmm für den Monat (englische Kurzschreibweise), yyyy für das Jahr (4-stellig), hh für die Stunde (mit führender 0 bei 1-stelliger Stundenzahl), mm für die Minute und ss für die Sekunde steht. Der Wert +xxxx zeigt die Korrektur im Vergleich zu UTC/GMZ, also +0100 bei MEZ oder +0200 bei MESZ (Sommerzeit) an

Syntax Eintrag von versendeter Mitteilung mit Format History

Die Zeile besteht immer aus dem Feldnamen, der mit einem Doppelpunkt „:“ abgeschlossen wird, einem Leerzeichen und dem Wert, der wiederum ebenfalls Leerzeichen enthalten kann. Bitte beachten Sie bei diesem Eintrag, dass die Anzahl der Statuseinträge variabel ist und aufeinander aufbauen (z.B. „Read:“ setzt voraus, dass bereits der Eintrag für „Sent:“ und „Delivered“ vorhanden ist). Negative Werte schließen die Transaktion ab und es können keine weiteren Statuseinträge folgen. Bei der Adresse des Empfängers kann abhängig von der versendeten Mitteilung entweder „To:“, „Cc:“ oder „Bcc:“ stehen.

- To:** Adresse des Empfängers laut Mitteilung. Bei einem über die zentrale EDI-Funktion übergebenen EDIFACT Dokument hat die Adresse immer das Format "" <user-id@viat.de>
- Cc:** Adresse des Kopie-Empfängers laut Mitteilung.
- Bcc:** Adresse des Blindcopy Empfängers laut Mitteilung.
- Order-ID:** Auftragsnummer aus Dateinamen (maximal 26 Zeichen)
- Message-ID:** Mitteilungsnummer laut Mitteilung bzw. bei einem EDIFACT Dokument die Referenznummer des Interchange (maximal 64 Zeichen)
- MTS-ID:** Die vom MTA beim Versenden der Mitteilung vergebene Kennung (maximal 32 Zeichen).
- Sent:** Zeitpunkt Versendet mit dem Format dd-mmm-yyyy hh:mm:ss +xxxx, wobei dd für den Tag des Monats (ohne führende Null bei 1-stelligem Datum), mmm für den Monat (englische Kurzschreibweise), yyyy für das Jahr (4-stellig), hh für die Stunde (mit führender 0 bei 1-stelliger Stundenzahl), mm für die Minute und ss für die Sekunde steht. Der Wert +xxxx zeigt die Korrektur im Vergleich zu UTC/GMZ, also +0100 bei MEZ oder +0200 bei MESZ (Sommerzeit) an
- Oder**
- Error:** Wenn eine Datei nicht verarbeitet bzw. eine Mitteilung/ ein Dokument nicht versendet werden konnte, wird eine entsprechende Fehlermeldung durch den MessageGate Prozess erzeugt und mit Zeitstempel ausgegeben.
Format:
Error: dd-mmm-yyyy hh:mm:ss +xxxx (Reason: nnnnnnnn, Diagnostic: n)
- Delivered:** Zeitpunkt an dem die Mitteilung in der Mailbox des Empfängers ausgeliefert wurde (Format siehe Sent:)
- Oder**
- Failed:** Mitteilung konnte nicht ausgeliefert werden und der MTA erzeugt eine entsprechende Nicht Auslieferbestätigung (NDN) mit Fehlergrund.
Format:
Failed: dd-mmm-yyyy hh:mm:ss +xxxx (Reason: n, Diagnostic: n)
- Read:** Zeitpunkt an dem der Empfänger auf die Mitteilung zugegriffen (gelesen, verarbeitet) hat (Format siehe Sent:)
- Oder**

Denied: Mitteilung wurde vom Empfänger ungelesen gelöscht/verworfen
 Format:
 Denied: dd-mmm-yyyy hh:mm:ss +xxxx (Reason: n, Diagnostic: n)

Syntax Eintrag von empfangener Mitteilung mit Format History

Zeile besteht immer aus dem Feldnamen, der mit einem Doppelpunkt „:“ abgeschlossen wird, einem Leerzeichen und dem Wert, der wiederum ebenfalls Leerzeichen enthalten kann.

From: Adresse des Absenders
Order-ID: Durch MessageGate vergebene Auftragsnummer (maximal 26 Zeichen)
Message-ID: Mitteilungsnummer, die Absender in seiner Mitteilung vorgesehen hat (maximal 64 Zeichen)
MTS-ID: Die vom Partner MTA beim Versenden der Mitteilung vergebene Kennung (maximal 32 Zeichen). Entspricht dem Wert X-MPDUID im Header der SMTP-Mitteilungsstruktur.
Received: Zeitpunkt Empfangen mit dem Format dd-mmm-yyyy hh:mm:ss +xxxx, wobei dd für den Tag des Monats (ohne führende Null bei 1-stelligem Datum), mmm für den Monat (englische Kurzschreibweise), yyyy für das Jahr (4-stellig), hh für die Stunde (mit führender 0 bei 1-stelliger Stundenzahl), mm für die Minute und ss für die Sekunde steht. Der Wert +xxxx zeigt die Korrektur im Vergleich zu UTC/GMZ, also +0100 bei MEZ oder +0200 bei MESZ (Sommerzeit) an

Oder

Failed: Mitteilung wurde nicht ausgeliefert
 Format:
 Failed: dd-mmm-yyyy hh:mm:ss +xxxx (Reason: n, Diagnostic: n)

Read: Information an Absender, dass die Mitteilung verarbeitet wurde
 Format:
 Read: dd-mmm-yyyy hh:mm:ss +xxxx

Oder

Denied: Information an Absender, dass die Mitteilung verworfen wurde
 Format:
 Denied: dd-mmm-yyyy hh:mm:ss +xxxx (Reason: n, Diagnostic: n)

Mögliche Statuszustände bei versendeten Mitteilungen:

Sent

Error: (Reason: nnnnnnnn, Diagnostic: n)

Delivered

Failed: (Reason: n, Diagnostic: n)

Read

Denied: (Reason: n, Diagnostic: n)

Mögliche Statuszustände bei empfangenen Mitteilungen:

Received

Failed: (Reason: n, Diagnostic: n)

Read

Denied: (Reason: n, Diagnostic: n)

*Beispiele für Statuseinträge sind in Anlage C aufgeführt.***2.7.4 Syntax des Statusreports (CSV-Format)**

Hat der MessageGate Prozess eine entsprechende Auftragsdatei (S_Auftrags-ID.IN) verarbeitet, wird er anhand der vorgegebenen Selektionskriterien die Datenbankta-
belle nach Einträgen durchsuchen und eine Statusdatei zusammenstellen. Für diese
Datei wird er den gleichen Namen wählen, jedoch die Extension durch „.OUT“ erset-
zen. Das CSV-Format ist aber für die maschinelle Verarbeitung optimiert und des-
halb nur sehr schlecht lesbar.

Die Statusdatei im CSV-Format hat ebenfalls einen Header, wobei die beiden ersten
Zeilen dieselben Informationen beinhalten wie das im letzten Kapitel beschriebene
Format. In der ersten Zeile wird die User-ID des MessageGate Benutzers und ein
Zeitstempel für das Erstellen des Reports und in der zweiten die berücksichtigen Fil-
terkriterien angegeben. Durch eine Leerzeile getrennt folgt dann die Definition der
einzelnen Felder, den einzelnen Feldnamen.

Feldname:	Erläuterung:
From	Bei empfangenen Mitteilungen die Adresse des Absenders (Alias/X.400 Adresse + SMTP- Adresse, maximal 256 Zeichen). Da der Alias in Hochkommata gesetzt und dieses Zeichen beim CSV Format aber auch als Begrenzungszeichen für Strings benutzt wird, beginnt das Feld mit drei Hochkommata, nach dem Alias folgen zwei Hochkommata und am Ende der Adresse dann noch ein Hochkommata ("""G=test;S=tester1;O=testag;A=viaT; C=de"" <95344@viaT.de>").
To	Bei versendeten Mitteilungen Adresse des Empfängers (Alias + SMTP- Adresse, maximal 256 Zeichen). Format siehe „From:“. Adressierungstyp (To:, Cc:, Bcc:) siehe Rcpt Type.
Order-ID	Auftragsnummer aus Dateinamen (maximal 26 Zeichen) in Hochkommata.
Message-ID	Mitteilungsnummer laut Mitteilung bzw. bei einem Transmissionsset die Referenznummer des Interchange (maximal 64 Zeichen) in Hochkommata.
MTS-ID	Die vom MTA beim Versenden der Mitteilung vergebene Kennung (=MPDU ID, maximal 32 Zeichen) in Hochkommata.

Received	Zeitpunkt (UTC/GMT), an dem die Mitteilung empfangen wurde (Format des Zeitstempels yyyy/mm/dd hh:mm:ss bei der Dateischnittstelle, dd.mm.yyyy hh:mm in WebConfig) ohne Hochkommata oder aber "Failed", falls die Mitteilung nicht ausgeliefert wurde (Fehlercode siehe Reason und Diagnostic).
Sent	Zeitpunkt (UTC/GMT), an dem die Mitteilung gesendet wurde (Format des Zeitstempels yyyy/mm/dd hh:mm:ss bei der Dateischnittstelle, dd.mm.yyyy hh:mm in WebConfig) ohne Hochkommata oder aber "Error", falls die Mitteilung nicht versendet wurde (Fehlercode siehe Reason und Diagnostic).
Delivered	Zeitpunkt (UTC/GMT), an dem die versendete Mitteilung ausgeliefert wurde (Format des Zeitstempels yyyy/mm/dd hh:mm:ss bei der Dateischnittstelle, dd.mm.yyyy hh:mm in WebConfig) ohne Hochkommata oder aber "Failed", falls die Mitteilung nicht ausgeliefert wurde (Fehlercode siehe Reason und Diagnostic).
Read	Zeitpunkt (UTC/GMT), an dem versendete Mitteilung gelesen/verarbeitet bzw. an dem für empfangene Mitteilung ein entsprechender Report versendet wurde (Format des Zeitstempels yyyy/mm/dd hh:mm:ss bei der Dateischnittstelle, dd.mm.yyyy hh:mm in WebConfig) ohne Hochkommata oder aber "Denied", falls die Mitteilung vom Empfänger verworfen wurde (Fehlercode siehe Reason und Diagnostic).
Reason	Zeigt den Grund für eine fehlgeschlagene Aktion als Fehlercode an (Details siehe Anlage B) ohne Hochkommata.
Diagnostic	Zeigt die Erläuterung für eine fehlgeschlagene Aktion als Fehlercode an (Details siehe Anlage B) ohne Hochkommata.
Errordate	Zeitstempel (UTC/GMT) der fehlgeschlagenen Aktion (Format yyyy/mm/dd hh:mm:ss bei der Dateischnittstelle, dd.mm.yyyy hh:mm in WebConfig) ohne Hochkommata.
Rcpt Type	Adresstyp des Empfängers: To, Cc oder Bcc, bei Versand über zentrale EDI-Funktion ist der Adresstyp EDI (entspricht To)

2.8 Lesebestätigung versenden

Über die Dateischnittstelle von MessageGate kann auch eine Lesebestätigung (positiv oder negativ) für eine empfangene Mitteilung versendet werden, falls der Partner diese angefordert hatte. Die Anforderung dieser Lesebestätigung wird durch das Feld „Disposition-Notification-To: <X.400 Adresse des Absenders>“ im Header der empfangenen Mitteilung definiert.

Es ist jedoch möglich, im Hostprofil festzulegen, dass eine angeforderte Lesebestätigung nicht zur Dateischnittstelle durchgereicht wird, um immer die gleiche Headerstruktur verarbeiten zu können.

Soll für eine Mitteilung eine Lesebestätigung versendet werden, müssen Sie eine Datei erzeugen, in deren Namen sich die Auftrags-ID der empfangenen Mitteilung befindet.

Das Format lautet: „R_<Auftrags-ID der empfangenen Mitteilung>.IN“.

MessageGate setzt die folgenden Werte in der Datei in entsprechende X.400 Reports um:

Processed → Receipt Report/Notification (RN)
Failed → Non Receipt Report/Notification (NRN) mit Reason Code
“0” (Discarded)

Sollten Sie außer diesen erlaubten Werten andere Werte als Dateinhalt des Receipt Report einstellen, wird die Datei von MessageGate mit einem entsprechenden Fehlercode im Dateinamen zurückgewiesen.

Falls Sie MessageGate in Verbindung mit einer aktivierten Closed User Group verwenden, müssen Sie beachten, dass die beim Dateinamen der ausgelieferten Mitteilung ergänzte Absender User-ID nicht zur Auftrags-ID gehört und deshalb bei der „in“-Datei für die Lesebestätigung nicht ergänzt werden darf.

Bitte beachten Sie, dass das Versenden von Receipt Reports bei *BusinessMail X.400* und auch bei anderen X.400 Mailsystemen kostenpflichtig ist (also verbucht bzw. beim Freivolumen angerechnet wird).

2.9 Kommunikations-/Partnerschaftsprofile

2.9.1 Allgemein

Für Benutzer des MessageGate File Interface ist es notwendig, dass zumindest das Benutzer-/Kommunikationsprofil eingerichtet wurde, in dem die Regeln für die Umsetzung von der RFC2822 Mitteilungsinhalte in X.400 Mitteilungen und umgekehrt festgelegt werden.

Sobald dieses Profil Grundeinstellungen eingerichtet ist, kann der MessageGate Benutzer bereits Daten mit anderen X.400 Teilnehmern austauschen und auch die verschiedenen Gateway Services von *BusinessMail X.400* (Telefax- Gateway, Internet-Gateway) nutzen. Für die Erzeugung der Mitteilungen werden dann die im Profil hinterlegten Parameter verwendet.

Wenn für den Partner andere Parameter verwendet werden sollen, ist es notwendig, ein separates Partnerschaftsprofil anzulegen. Dieses Profil kann durch die zentrale Administration von BusinessMail über einen kostenpflichtigen Auftrag eingerichtet werden. Einfacher ist es aber, dies direkt in *WebConfig*, einer Anwendung von *BusinessMail X.400* zur Pflege von Partnerschaftsbeziehungen, vorzunehmen.

Diese Anwendung kann mit einem beliebigen Webbrowser (ActiveX für URL von *WebConfig* freigeben, um alle Funktionen nutzen zu können) unter der Adresse <https://webconfig.viat.de/webconfig> aufgerufen werden. Vor dem erstmaligen Benutzen von *WebConfig* muss aber zunächst auf der Service-Webseite von *BusinessMail X.400* (<https://www.service-viat.de>) ein Clientzertifikat abgeholt werden, um es in der Zertifikatsverwaltung Ihres Rechners/ Browsers zu installieren. Dieses Zertifikat wird beim Verbindungsaufbau zu *WebConfig* abgefragt. Sie müssen dann auch die Verwendung von Cookies freigeben. Zum erstmaligen Einloggen in *WebConfig* müssen dann noch die Zugangsdaten (Benutzername und Passwort) eingegeben werden, die Sie zusammen mit anderen Informationen beim Einrichten Ihres MessageGate Account erhalten. Nach dem ersten Einloggen sollten Sie das WebConfig Passwort ändern oder ein personalisiertes Zertifikat abholen und den Zugriff auf *WebConfig* so abändern, dass Sie sich mit diesem Zertifikat direkt authentifizieren. Holen Sie sich dazu auch das Zertifikat der WebConfig CA auf der Service-Webseite ab, mit dem das personalisierte Zertifikat signiert wurde, und importieren Sie dieses ebenfalls in den Zertifikatsspeicher Ihres Browsers.

Im Hauptmenü von *WebConfig* werden dann abhängig von den beauftragten Leistungsmerkmalen folgende Menüpunkte geboten:

- Benutzerverwaltung für Ändern des *WebConfig* Passwortes, Überprüfung der Änderungen an Partnerschaften und Download von Daten (offizielle Zertifikate, EVN etc.), Grundeinstellungen für *WebConfig* wie Zeitzone, Trennzeichen für CSV- Dateien und Gültigkeitsdauer von Cookies
- Verwaltung von Zertifikaten für den Zugriff über WebDAV oder Web-Service
- Verwaltung von MessageGate Grundeinstellung und Partnerschaften inkl. Verwaltung von Statusreports
- Verwaltung der EDI-Partnerschaften (eigene EDI-Kennungen, EDI-Partnerschaften) bei aktivierter zentralen EDI-Funktion
- Verwaltung der Internet-E-Mail/SMTP Partnern (SMTP-Filter)

- Zugriff auf erweiterte Serviceinformationen

Das nachfolgende Bild zeigt die Menüpunkte eines MessageGate Benutzers, bei dem die zentrale EDI-Funktion aktiviert ist. Mehr Informationen zu *WebConfig* finden Sie auf der Serviceseite von *BusinessMail X.400* (<https://www.service-viat.de>).

· · T · · Systems · Business flexibility



The screenshot shows the 'MessageGate Partnerschaft :: Grundeinstellungen' configuration page. The left navigation menu includes: Benutzerverwaltung, EDI Partnerschaft, MessageGate Partnerschaft, **Grundeinstellungen** (highlighted), Erstellen, Anzeigen/Ändern, Löschen, Status Report, Autom. Status Report, SMTP Filter, Service BusinessMail X.400, and Abmelden (Logout). The main configuration area is titled 'Einstellungen' and contains the following settings:

- Bei X.400 Mitteilungen eine angeforderte Empfangsbestätigung umsetzen in: Auslieferungsbestätigung (DN)
- Bei Mitteilungen von X.400-Absendern werden angeforderte Lesebestätigungen: ignoriert, zugestellt, sobald eine Empfangsbestätigung versendet wird
- Message Expiration: 1440 Minuten
- X.400 Content-Type: IPM84, IPM88
- Bodypart: IA5-Text, Bilateral (Bodypart 14), ISO-Latin-1, Kontextabhängig (variabel)
- Binäre Daten codieren als: binary, base64
- Ausgabeformat: SMTP, TS (TransmissionSet)
- Purge-Zeit: 240 Stunden

Buttons for 'Ok' and 'Abbrechen' are located at the bottom of the configuration area.

Unter Grundeinstellungen werden die Defaults der Kommunikationsparameter des MessageGate Benutzers festgelegt und unter Erstellen, Ändern oder Löschen Partnerschaftsprofile verwaltet. Bis auf das Feld Ausgabeformat werden die Parameter der Grundeinstellungen auch in den Partnerschaftsprofilen angeboten. Die in Grundeinstellungen festgelegten Werte werden als Default beim Einrichten von neuen Partnerschaften vorgegeben. Ändern Sie bestimmte Parameter der Grundeinstellung, werden Sie gefragt, ob diese auch bei den schon bestehenden Partnerschaften geändert werden sollen.

2.9.2 X.400 Reports

Der X.400 Standard bietet mit den Delivery (Ausliefer-) bzw. Receipt (Lese-) Notifications (Bestätigung) die Möglichkeit, den Verbleib einer Mitteilung zu prüfen. Standardmäßig wird für einen MessageGate Benutzereintrag im Profil vorgesehen, dass ein Delivery Notification angefordert wird, wenn der Kunde in seiner SMTP-Mitteilung den Parameter „Disposition-Notification-To:“ angegeben hat. In seinem MessageGate Profil und auch in den Partnerprofilen kann der Benutzer folgende Bestätigungen (Reports) auswählen:

- Non Delivery Notification → Report nur dann senden, wenn die Mitteilung nicht ausgeliefert werden kann
- Delivery Notification → Report dann senden, wenn die Mitteilung in der Mailbox des Empfängers ausgeliefert wurde (schliesst Non-Delivery Notification mit ein!)
- Receipt Notification → Report dann senden, wenn die Mitteilung durch den Empfänger verarbeitet (gelesen/abgeholt) wurde. Es wird immer auch eine Delivery Notification angefordert und deren Empfang im Statusreport angezeigt!

Ist in der Mitteilung der Parameter „Disposition-Notification-To:“ nicht angegeben, wird kein Report angefordert. Dies bedeutet, dass der MessageGate Benutzer auch keine Informationen darüber erhält, falls die Auslieferung fehlgeschlagen ist.

Werden Daten über die zentrale EDI-Funktion versendet, wird immer ein Report in Abhängigkeit von den im Profil angegebenen Werten angefordert.

Ob und welche Reports angefordert werden sollten, hängt von den Daten ab, die der MessageGate Benutzer mit seinem Partner austauscht. Wenn auf Applikationsebene schon ein Bestätigungsmechanismus implementiert wurde, ist eine Überwachung auf Transportebene (X.400) unter Umständen nicht notwendig und es muss auch kein Report angefordert werden. Üblich ist es aber, zumindest die Auslieferung der X.400 Mitteilung in die Mailbox des Partners zu überwachen. Fordern Sie hingegen eine Bearbeitungs- /Lesebestätigung an, sollten Sie dies mit Ihrem Partner abgestimmt haben, da der X.400 Standard dem Empfänger die Wahl lässt, diesen Report zu senden oder auch nicht. Die Zuordnung einer Lesebestätigung zu der versendeten Mitteilung ist nur so lange möglich, wie der Eintrag in der Datenbank (Trace_Tab) nicht durch den Purger gelöscht wurde. Außerdem ist zu beachten, dass beim *BusinessMail X.400 Service* wie auch in anderen X.400 Systemen eine Lesebestätigung kostenpflichtig ist.

Legen Sie deshalb im Auswahlfeld „Bei X.400 Mitteilungen eine angeforderte Empfangsbestätigung umsetzen in“ fest, in welchen X.400 Report der Parameter „Disposition-Notification-To:“ umgesetzt werden soll.

Im Auswahlfeld „Bei Mitteilungen von X.400-Absendern werden angeforderte Lesebestätigungen“ legen Sie fest, ob eine vom Partner angeforderte Bearbeitungs-/Lesebestätigung in der Mitteilungsdatei in ein „Disposition-Notification-To:“ umgesetzt oder ob dies unterdrückt werden soll. Standardmäßig wird diese Information durchgereicht, aber unter Umständen verursacht dieses Feld Probleme bei Ihrer Anwendung und kann deshalb im Profil abgeschaltet werden.

2.9.3 X.400 Headerinformationen

Mit dem Parameter „Message Expiration“ wird definiert, wie lange diese Mitteilung gültig ist und beim Parameter „X.400 Content Type“ wird die Struktur der X.400 Mitteilung festgelegt.

Beim Parameter „Message Expiration“ wird standardmäßig der Wert 1440 (Minuten = 24 Stunden) eingerichtet. Dies bedeutet, dass der MTA einen Tag lang versucht, die Mitteilung an den Empfänger auszuliefern, bevor er eine (angeforderte!) Non Delivery Notification (NDN, Nicht Auslieferbestätigung) erzeugt.

Beim Parameter „X.400 Content Type“ legen Sie fest, in welcher Form (Mitteilungstyp) die Daten an Ihren Partner versendet werden. Erlaubte Werte sind IPM84 und IPM88 (Default).

Bei IPM84 wird eine Mitteilung vom Typ P2 (X.400 Standard 1984) erzeugt und es werden Text Body mit IA5 Zeichensatz und binäre Anhänge als Bilaterally defined Body Part (BP14 → Binärdaten ohne Dateiinformation) unterstützt. Der Commonname (CN) wird in diesem Fall nicht übertragen. Benutzen Sie diese Einstellung nur dann, wenn sich die Mailbox Ihres Partners in einem X.400 System befindet, das nur den 1984er Standard unterstützt, und Kompatibilitätsprobleme aufgetreten sind.

Bei IPM88, dem Default für diesen Parameter, wird eine Mitteilung vom Typ P22 (X.400 Standard 1988/92) erzeugt und zusätzlich der BP15 FTAM Body Part (FTBP) unterstützt, bei dem neben binären Inhalten auch der Dateiname übertragen werden kann. Außerdem wird in der Absenderadresse und bei lokalen Empfängeradressen der Commonname übertragen.

Wenn Sie EDIFACT Dokumente über die zentrale EDI-Funktion versenden, wird der Mitteilungstyp durch die Einstellungen im EDI-Partnerschaftseintrag festgelegt. Die zentrale EDI-Funktion bietet dann auch die Möglichkeit, den Mitteilungstyp PEDI (X.435) zu wählen.

2.9.4 X.400 Body Parts

Mit dem Parameter „Bodypart“ wird definiert, wie der MessageGate Prozess bei zu versendenden Mitteilungen den im Nutzdatenteil angegebenen MIME-Content in entsprechende X.400 Body Parts umsetzt. Hier kann man angeben, dass immer ein bestimmter X.400 Body Part (IA5-Text, Bilateral Body Part 14, ISO-Latin-1) benutzt wird oder aber ein MIME-Content Typ in einen äquivalenten X.400 Body Part (Variabel) umgesetzt wird. Variabel ist als Default vorgesehen. Sie sollten diesen Default nur bei Partnerschaftsprofilen abändern, wenn der Partner immer denselben X.400 Body Part erwartet und Ihre Anwendung nicht immer den passenden MIME-Content erzeugen kann oder wenn Ihre Anwendung einen Text MIME-Content mit Dateinamen anliefert und dieser als X.400 Text Body Part versendet werden soll.

Bitte beachten Sie, dass bei einer Mitteilung an mehrere Empfänger eventuell vorhandene Partnerschaftsprofile durch den MessageGate Prozess nicht ausgewertet werden. Hier werden immer die in der Grundeinstellung hinterlegten Umsetzregeln verwendet.

Wenn Sie die zentrale EDI-Funktion nutzen, wird das Mapping eines EDIFACT Dokumentes in einen X.400 Body Part durch die Einstellungen im EDI-Partnerschaftseintrag festgelegt.

2.9.5 Binäre Daten codieren als

Mit diesem Parameter definieren Sie, ob MessageGate beim Umsetzen von binären X.400 Body Parts (BP14 oder BP15/FTBP) in einen MIME-Content Typ diese mit Content Encoding Binary oder aber mit BASE64 anlegen soll. Letzteres kann dann auch von beliebigen E-Mail-Clients importiert und verarbeitet werden. Dieser Parameter wird auch für verschlüsselte S/MIME-Content herangezogen, bei signierten Inhalten aber ignoriert, da ansonsten die Signatur ungültig wird. Beim Versenden von Mitteilungen akzeptiert MessageGate beide Formen des Content-Encoding.

2.9.6 Ausgabeformat

Ist für den MessageGate Eintrag die zentrale EDI-Funktion aktiviert, so kann über diesen Parameter ausgewählt werden, ob ein vom Partner versendetes EDIFACT Dokument als SMTP-Mitteilung inkl. Header-Informationen oder als Transmissions-set-Datei ohne Header-Informationen ausgeliefert werden soll. Diese Einstellung ist aber nicht Partnerbezogen, sondern gilt generell. Dieser Parameter erscheint deshalb nur beim MessageGate Kommunikationsprofil und nicht bei den Partnerkommunikationsprofilen.

2.9.7 Statusreport abfragen

Im Menüpunkt Status Report ist es möglich, den Status der Transaktionen (Mitteilungen gesendet oder empfangen) entweder direkt in der Oberfläche anzeigen zu lassen oder aber als CSV-Datei herunterzuladen bzw. mit einem passenden Programm (z.B. Microsoft Excel) direkt zu öffnen.

Die Anzahl der dargestellten Einträge kann durch Definieren eines Suchzeitraums, der Option „Nur fehlgeschlagene Nachrichten“ und bei direkter Darstellung durch Angabe eines Suchstrings bei Filter eingeschränkt werden. Welches Trennzeichen bei der CSV-Datei benutzt werden soll, wird unter Benutzerverwaltung festgelegt. Der Default ist Semikolon.



The screenshot shows a web browser window with the address bar displaying 'BusinessMail X.400 :: WebKonfiguration' and the user 'mgate (49603)'. The main content area is titled 'MessageGate Partnerschaft :: Status Report abfragen'. Below the title, there is a text input field for 'Datensätze seit' with a placeholder '(Format: DD-MMM-YYYY hh:mm:ss)'. A checkbox labeled 'Nur fehlgeschlagene Nachrichten' is present. Two buttons are visible: 'Status Report anzeigen' and 'Als CSV-Datei herunterladen'. Below these is a 'Filter:' input field. At the bottom, a status message reads: 'Status Report for UserID 49603; generated 25-Nov-2009 08:01:55' and 'Disposition=all, Direction=Both, Format=History'.

2.9.8 Automatischen Statusreport konfigurieren

Statusreports können entweder mittels eines entsprechenden Auftrages angefordert werden oder Sie können sich automatisch Reports erstellen und an Ihre Anwendung ausliefern lassen.

BusinessMail X.400 :: WebKonfiguration mgatetester (49640)

MessageGate Partnerschaft :: Automatischer Status Report

Automatischen Status Report aktivieren

Einstellungen 

Präfix für Dateiname:

Nur fehlgeschlagene Nachrichten:

Wochentage:

- Montag
- Dienstag
- Mittwoch
- Donnerstag
- Freitag
- Samstag
- Sonntag

Täglicher Beginn: (MEZ/MESZ, Format: hh:mm)

Tägliches Ende: (MEZ/MESZ, Format: hh:mm)

Sendintervall: Minuten (0=Einmalig zum täglichen Beginn), mindestens 30

Disposition:

Direction:

Format:

In diesem Menüpunkt können Sie für den Empfang von Statusreports eine Partnerschaft einrichten, bei der Sie den Zeitraum definieren, in dem die Statusreports erzeugt werden (an welchen Wochentag, der Startzeitpunkt, der Endzeitpunkt) und in welchem Intervall (Minimum ist momentan 30 Minuten). Die Namen der bereitgestellten Status Report Dateien können Sie durch ein Präfix ergänzen. Weiterhin stellt MessageGate die Eindeutigkeit des Dateinamens durch einen Zeitstempel sicher. Sie können den Inhalt des Reports durch entsprechende Selektionskriterien definieren (*siehe auch Kapitel 2.7. Der Statusreport*). Durch Aktivieren der Option „Nur fehlgeschlagene Nachrichten“ können Sie die Anzahl der im Report zurückgelieferten Einträge begrenzen.

2.9.9 EDI-Partnerschaft

Wurde bei Ihrem MessageGate Account die zentrale EDI-Funktion aktiviert, können Sie bei diesem Hauptmenüpunkt eigene EDI-Kennungen und auch EDI-Partnerschaften verwalten. Um die zentrale EDI-Funktion nutzen zu können, muss zumindest eine eigene EDI-Kennung konfiguriert sein. Solange keine Closed User Group (CUG) aktiviert wurde, können beliebige Partner nun EDIFACT Dokumente (ein Dokument pro Mitteilung) an diese EDI-Kennung senden.

BusinessMail X.400 :: WebKonfiguration mgate (49603)

EDI Partnerschaft :: Eigene EDI-Kennung erstellen ?

Eigene EDI-Kennung ?

EDI-ID

EDI-Qualifier

Geschlossene Benutzergruppe (nur bestimmte Absender dürfen Nachrichten an diese EDI-Kennung senden)

Falls Sie beabsichtigen, auch EDIFACT-Dokumente an Partner zu senden, muss aber für jeden Partner eine EDI-Partnerschaft eingerichtet werden, bei der Sie die X.400 Adresse (oder User-ID) einer EDI-Kennung (EDI ID, z.B. ILN/GLN und optional einem EDI Qualifier) zuordnen.

Bei der Partnerschaft können Sie als zusätzliches Zuordnungskriterium auch das Testflag im EDIFACT Header (UNB) verwenden, um z.B. zwischen der Produktions- und der Testmailbox Ihres Partners unterscheiden zu können. Wenn Sie das Feld „EDI-Testflag“ bei einer Partnerschaft aktivieren, ohne dass es eine zweite Partnerschaft gibt, wird verhindert, dass Wirkdaten (ohne Testflag im UNB-Header) an diesen Partner ausgeliefert werden.

EDI Einstellungen

EDI Partnerschaft ?

Eigene EDI-Kennung

Partner EDI-ID

Partner EDI-Qualifier

EDI-Testflag

X.400 Content-Type

Bodypart

Sie können in einem Partnerschaftsprofil auch das Mitteilungsformat und den Typ des X.400 Body Parts definieren.

2.9.10 SMTP-Filter

Standardmäßig können Ihnen beliebige Partner aus dem Internet per SMTP-Mitteilung Informationen zusenden. Falls Sie dies nicht wünschen, können Sie über diesen Menüpunkt entweder alle Mitteilungen, die Ihnen per SMTP-Mitteilungen zuge-

sendet werden, im SMTP-Gateway unterdrücken lassen (blockieren) oder aber nur Mitteilungen von konfigurierten Absendern erlauben (teilweise blockieren).

BusinessMail X.400 :: WebKonfiguration mgate (49603)

SMTP Filter :: Status setzen ?

Filter Status

Das Zustellen von X.400-Nachrichten von SMTP-Absendern

Als Filter können Sie dabei komplette Adressen oder auch nur Teile von Adressen (z.B. eine Domain) angeben. Bei Teiladressen darf kein Wildcard Zeichen angegeben werden.

BusinessMail X.400 :: WebKonfiguration mgate (49603)

SMTP Filter :: Adresse hinzufügen ?

Erlaubte SMTP Absenderadresse

Bitte beachten Sie, dass Sie zwar beliebige Filter konfigurieren (einrichten, ändern oder löschen) können, jedoch werden diese nur bei der Einstellung „teilweise blockieren“ wirksam.

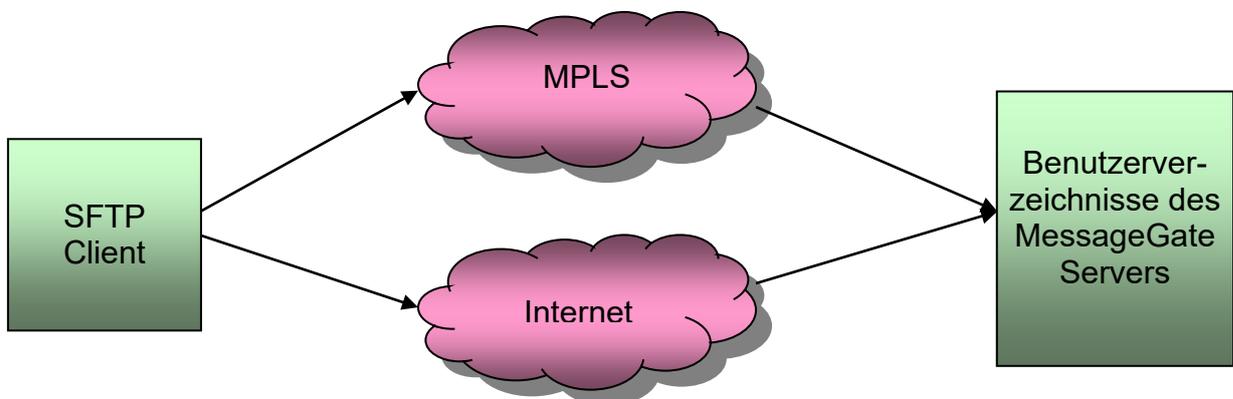
2.9.11 Web-Service für WebConfig

Über den Web-Service für WebConfig können Sie die Werte in der Grundeinstellung des MessageGate Accounts und MessageGate bzw. EDI-Partnerschaften und inzwischen auch eigene EDI-Kennungen aus einer Anwendung heraus verwalten. Die notwendigen Daten sind in einer CSV-Struktur hochzuladen bzw. werden als solche beim Herunterladen angeboten. Details zum Web-Service finden in der Kurzbeschreibung auf der Service Seite von BusinessMail X.400 (<https://www.service-viat.de> im Abschnitt Patches, Download und Handbücher).

3 Zugang über SFTP (SSH)

3.1 Allgemein

Der Transport von Daten über aktives FTP wie beim BUA (alte Dateischnittstelle) wird von vielen Netzwerkadministratoren als zu unsicher und problematisch angesehen, deshalb wird bei MessageGate der Transport über SFTP (als Bestandteil der SSH-Suite) und Port 22 angeboten. Dazu wird auf den Applikationsrechnern von *BusinessMail X.400* ein VMS- Benutzer mit eingeschränkten Rechten eingerichtet. Das benutzerspezifische Übergabe Verzeichnis für MessageGate wird dabei als Login Verzeichnis des VMS- Benutzers konfiguriert. Somit können direkt nach dem Einloggen über SFTP die Daten an den Applikationsrechner übertragen bzw. von dort Daten abgeholt werden.



Der Zugriff auf das *BusinessMail X.400* System kann über das MPLS-Netz der Telekom oder das Internet erfolgen.

Der Zugriff auf das Übergabe-Verzeichnis erfolgt im Internet über die logische Adresse „sftp.viat.de“, bei MPLS über die IP-Adresse 164.31.4.145.

3.2 Besonderheiten des Zuganges

Beim SFTP-Zugang von *BusinessMail X.400* muss sich der Client beim SSH-Server mit dem Benutzernamen und dem privaten Schlüssel (gegen den auf den Applikationsrechner hinterlegten öffentlichen Schlüssel) authentifizieren, während sich der Server gegenüber dem Client mit seinem eigenen Schlüssel authentifiziert. Da sich die von den verschiedenen SFTP-Clients benutzten Schlüsseldateien strukturell stark unterscheiden, muss der Benutzer den öffentlichen Schlüssel (möglichst im SSH2 Format mit Zeilenende-Zeichen LF) seiner Anwendung bzw. des in der Anwendung angelegten Kommunikationsprofils der Administration von *BusinessMail X.400* für die Authentifizierung zur Verfügung stellen. Zum Konvertieren der verschiedenen Formate empfiehlt sich puTTYgen → ist ein Bestandteil der Open Source Software puTTY oder auch von WinSCP. Für das Ändern des Zeilenende-Zeichens sollte bei Bedarf ein geeignetes Tool, wie z.B. Notepad ++ unter Windows, verwendet werden. Der Benutzer kann auch mehrere Schlüsseldateien übergeben. Im Arbeitsverzeichnis von MessageGate wird ein Unterverzeichnis namens SSH2 angelegt, in dem diese Schlüsseldatei(en) zusammen mit der Datei AUTHORIZATION hinterlegt werden. In der Datei AUTHORIZATION werden alle Schlüssel definiert, die der Kunde für das Einloggen in dieses MessageGate Verzeichnis nutzen kann. In diesem Verzeichnis

wird dann auch für den neuen SFTP-Server (OpenSSH) die Datei `authorized_keys` angelegt, in der alle erlaubten Schlüssel verwaltet werden. Für die Kommunikation über SFTP sollten RSA-Schlüssel von mindestens 3072 Bit Länge verwendet werden, der neue SFTP-Server würde dann auch mit ed25519 signierte Schlüssel erlauben. Neue öffentliche Schlüssel können per SFTP direkt in das Unterverzeichnis SSH2 übertragen werden. Die Ergänzung in der Datei `AUTHORIZATION` kann aber nur durch die Administration von *BusinessMail X.400* erfolgen. Dies gilt dann auch für die Einträge in die Datei `authorized_keys` beim neuen SFTP-Server. Bitte hierzu eine Änderung beim Helpdesk beauftragen.

3.3 Empfohlene SFTP-Kommunikationsmodule

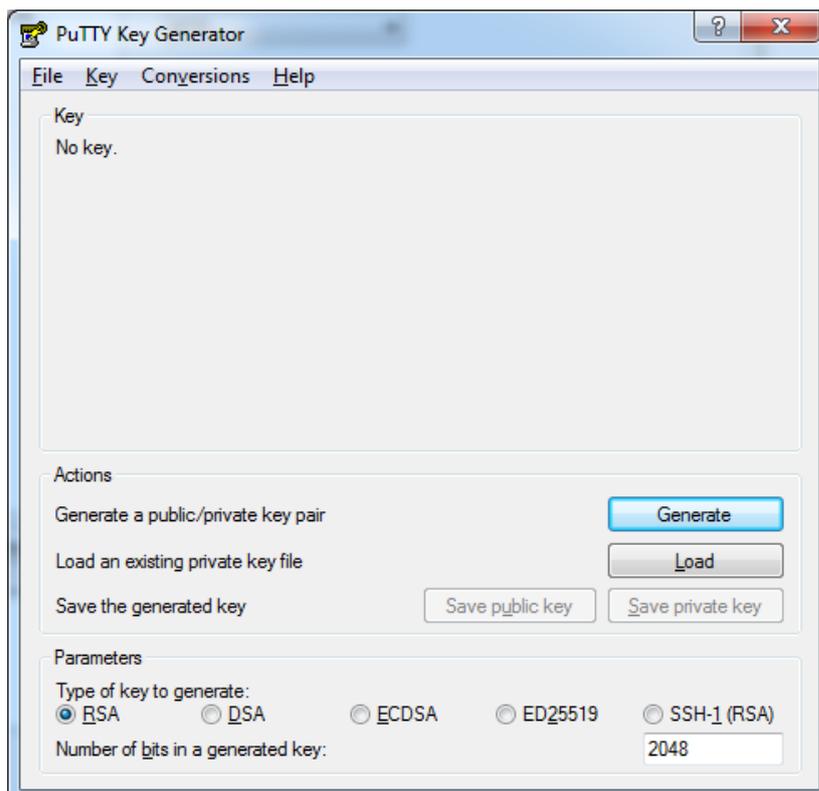
3.3.1 Für Microsoft® Windows 32 Bit Betriebssysteme

▪ WinSCP

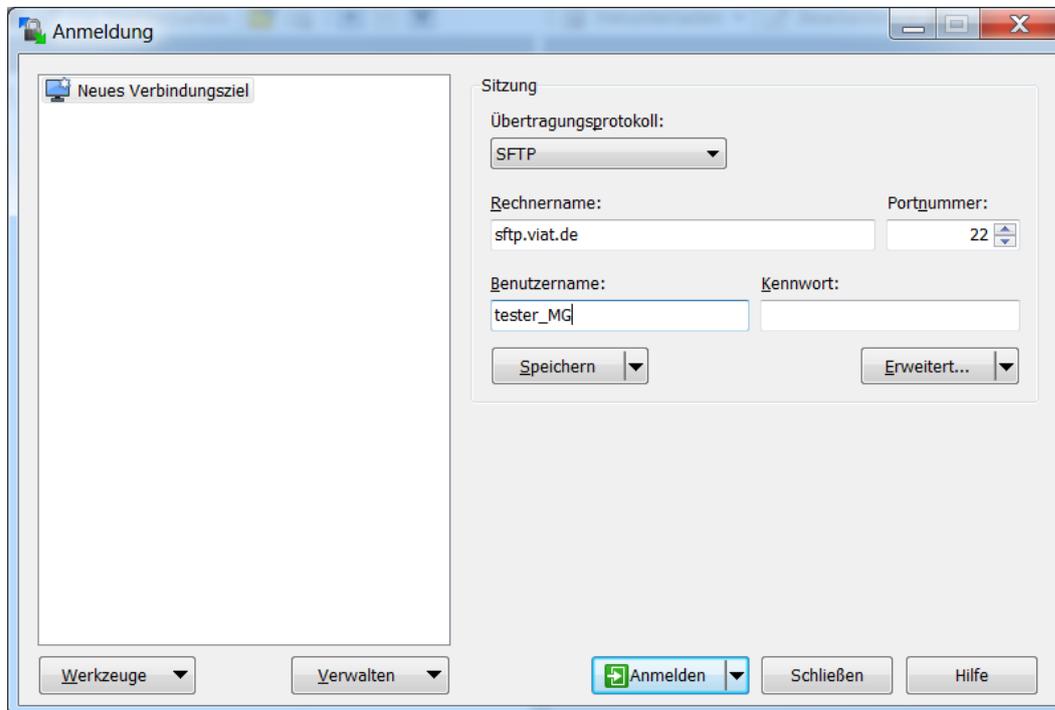
WinSCP ist ein Open Source Client für SFTP (auch für https/WebDAV und FTP) und bietet eine grafische Oberfläche zur Übertragung der Daten vom und zum SSH-Server. *WinSCP* kann aber auch im Batchmodus oder im DOS-Fenster mit einem zum Windows FTP Client vergleichbaren Befehlsumfang betrieben werden, um automatisiert Daten zu übertragen.

Konfiguration:

Zunächst müssen Sie *WinSCP* aufrufen und unter „Werkzeuge“ den Menüpunkt „PuTTYgen ausführen“ auswählen und ein Schlüsselpaar erstellen (Generate) und den öffentlichen Teil des Schlüssels an die Administration von *BusinessMail X.400* senden, damit dieser Schlüssel auf dem Host hinterlegt wird (bitte vorher das Zeilenende-Zeichen mit einem geeigneten Tool, wie z.B. Notepad ++, in LF ändern!). Der private Schlüssel muss lokal gespeichert werden, damit dieser durch *WinSCP* benutzt werden kann.



Nun können Sie in WinSCP ein neues Verbindungsziel anlegen. Wählen Sie als Übertragungsprotokoll „SFTP“ aus. Im Feld „Rechnername“ den logischen Namen des SSH-Servers (über DNS auflösen) oder direkt die IP-Adresse angeben und im Feld „Benutzername“ den zur Verfügung gestellten Benutzernamen. Unter „Erweitert.../Erweitert...“ dann beim Menüpunkt „SSH/Authentifizierung“ im Feld „Datei mit privatem Schlüssel“ die vorher erzeugte Datei mit dem privaten Schlüssel auswählen und nach Verlassen des Menüs „Erweitert...“. dann die Konfiguration speichern.



Nach erfolgter Konfiguration können Sie sich beim SSH-Server anmelden. Beim Verbindungsaufbau fragt *WinSCP* das Passwort des privaten Schlüssels ab (kann im Batchmodus z.B. über eine Datei importiert werden). Beim ersten Verbindungsaufbau sendet der SSH-Server seinen öffentlichen Schlüssel, den Sie akzeptieren müssen.

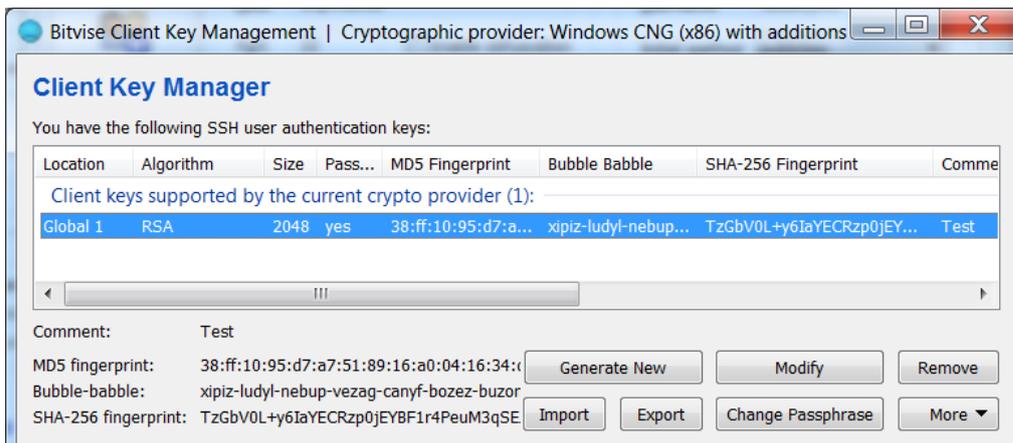
Unter „Erweitert...“ können Sie *WinSCP* an die Erfordernisse Ihrer Anwendung anpassen.

▪ Bitwise SSH Client (ehemals Tunnelier)

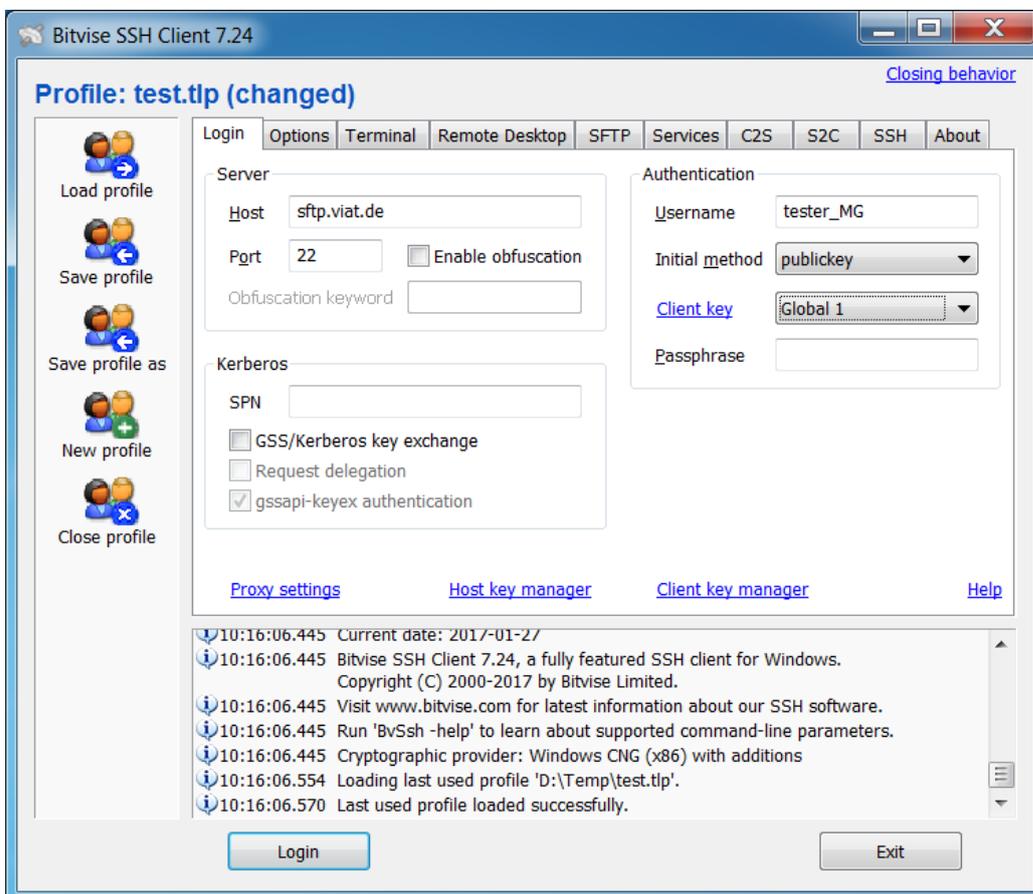
Dies ist ein SSH-Client, der ebenfalls neben einer grafischen Oberfläche einen Batchmodus und einen DOS Command Modus anbietet und von *Bitwise Limited* inzwischen kostenlos angeboten wird.

Konfiguration:

Zunächst müssen Sie mit dem Programm Client Key Manager (kann auch aus der GUI von SSH-Client aufgerufen werden) ein Schlüsselpaar erstellen (Generate New) und den öffentlichen Teil des Schlüssels an die Administration von *BusinessMail X.400* senden, damit dieser Schlüssel auf dem Host hinterlegt wird (bitte vorher das Zeilenende-Zeichen mit einem geeigneten Tool, wie z.B. Notepad ++, in LF ändern!). Bitte beim Erstellen des Schlüsselpaars darauf achten, dass der Wert im Kommentarfeld keine Leerzeichen enthält, da der Client Key Manager den Kommentar ohne Hochkomma in die Datei exportiert. Und dies führt dazu, dass der SFTP-Hostrechner diesen Schlüssel nicht richtig verarbeiten kann.



Dann können Sie *Bitvise* SSH Client starten, um das Kommunikationsprofil zu erstellen. Im Feld „Host“ den logischen Namen des SSH-Servers (wird über DNS auflösen) oder direkt die IP-Adresse angeben, im Feld „Username“ den zur Verfügung gestellten Benutzernamen, bei „Initial method“ den Slot des eingerichteten Schlüssels und bei Passphrase das Passwort des Schlüssels.



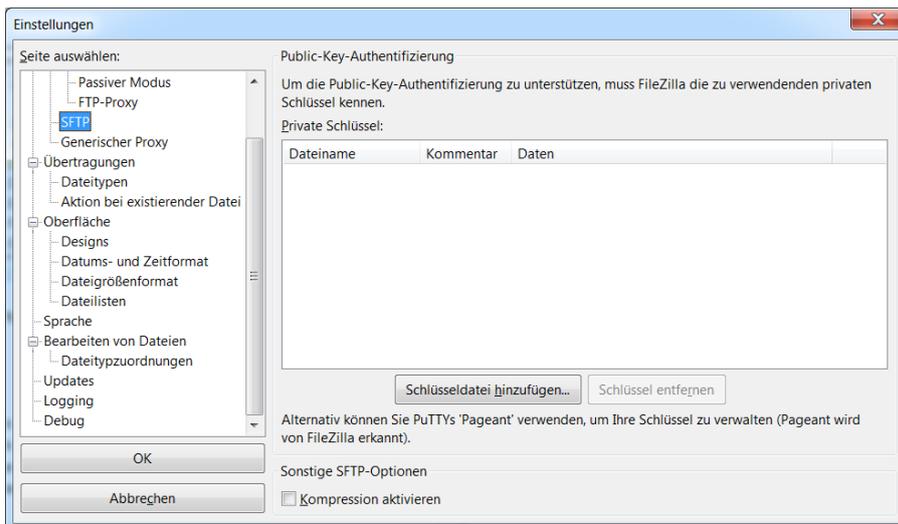
Unter SFTP können Sie das lokale Verzeichnis konfigurieren, das in der grafischen Oberfläche angezeigt wird. Dann können Sie die erste Verbindung aufbauen. Bitte dabei den Schlüssel des Hostrechners akzeptieren.

▪ **FileZilla**

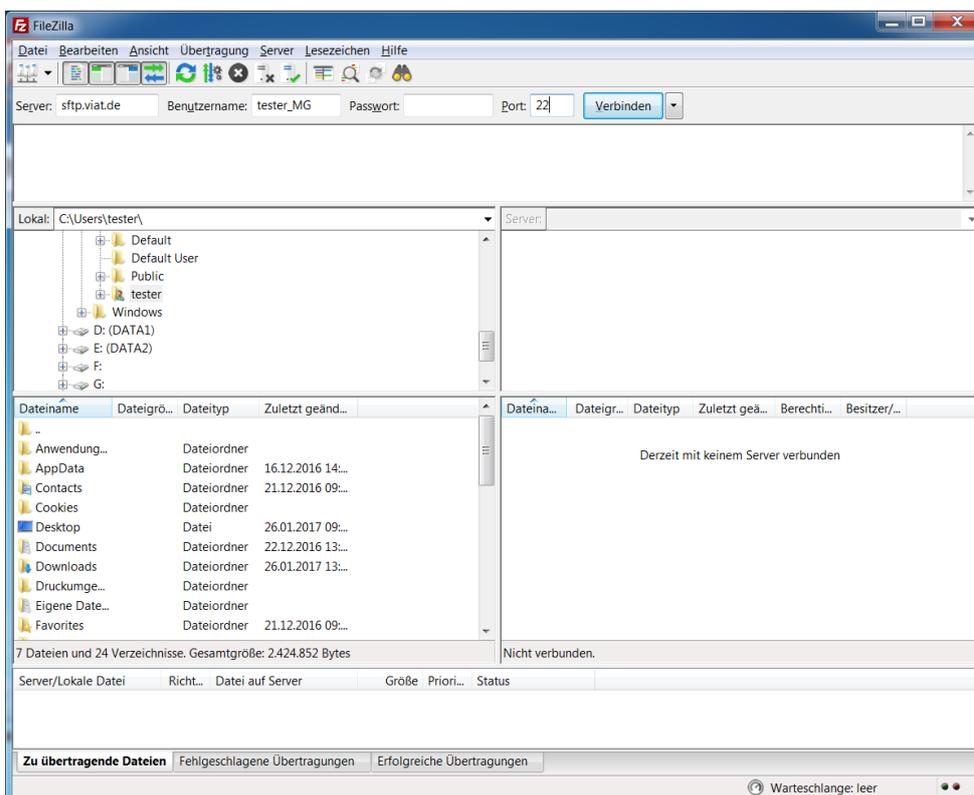
FileZilla ist ein mit WinSCP vergleichbarer Open Source Client für FTP und SFTP.

Konfiguration:

Zunächst müssen Sie mit einem geeigneten Tool (z.B. *puTTYgen*) ein Schlüsselpaar erstellen (Generate) und den öffentlichen Teil des Schlüssels an die Administration von *BusinessMail X.400* senden, damit dieser Schlüssel auf dem Host hinterlegt wird (bitte vorher das Zeilenende-Zeichen mit einem geeigneten Tool, wie z.B. Notepad ++, in LF ändern!). Der private Schlüssel muss lokal (Einstellungen → SFTP) gespeichert werden, damit dieser durch *FileZilla* benutzt werden kann.



Danach können Sie den Zugang zum MessageGate Verzeichnis einrichten. Im Feld „Server“ den logischen Namen des SSH-Servers (über DNS auflösen) oder direkt die IP-Adresse angeben und im Feld „Benutzername“ den zur Verfügung gestellten Benutzernamen.



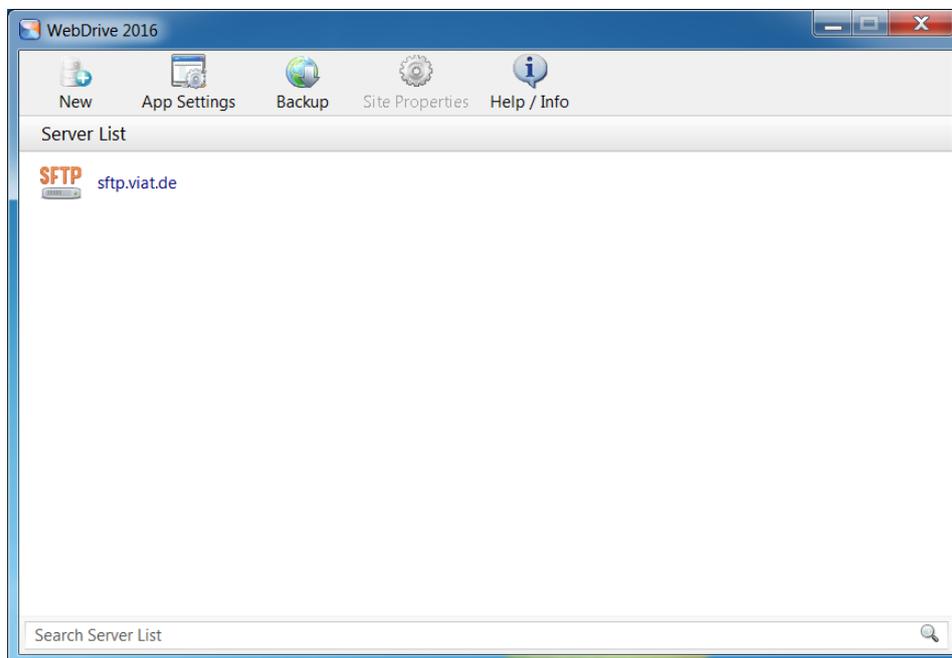
▪ WebDrive von South River Technologies

Erstellen eines Netzwerklaufwerks mit lokalem Laufwerksname über SSH/SFTP (auch über FTP und WebDAV, siehe Kapitel 4 Zugang über HTTPS/WebDAV), so dass das Applikationsverzeichnis wie ein lokales Verzeichnis behandelt werden kann.

Konfiguration (bei WebDrive 10):

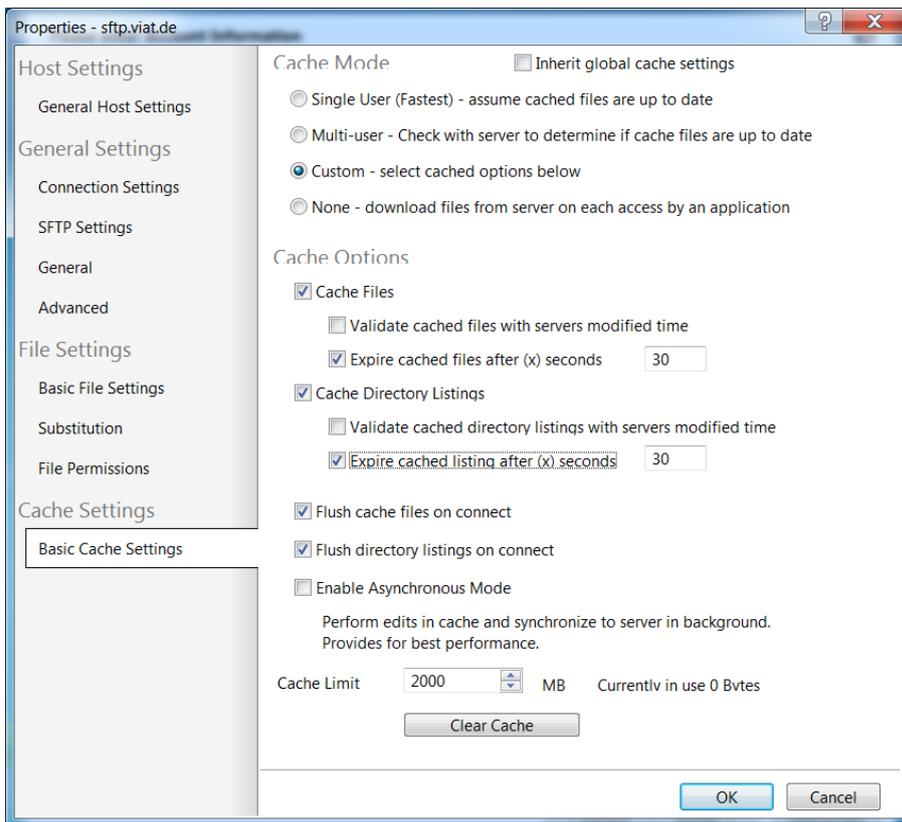
Zunächst unter App Settings → Security im „Host Key Manager“ mittels „Create“ ein Schlüsselpaar z.B. mit RSA 3072 Bit anlegen und den öffentlichen Schlüssel (Public) in eine Datei speichern (bitte dabei Zeilenende-Zeichen LF verwenden!) und diese an die Administration von *BusinessMail X.400* senden, damit dieser Schlüssel auf dem Host hinterlegt wird.

Verbindung einrichten: → New, den Typ „SFTP“ auswählen und dann unter URL/ Adresse den Wert „sftp.viat.de“ angeben und bei „Username“ den Namen des SSH-Accounts (wird bereitgestellt). Ist der Zugriff korrekt eingerichtet, können Sie das ausgewählte Laufwerk wie ein lokales Laufwerk ansprechen.

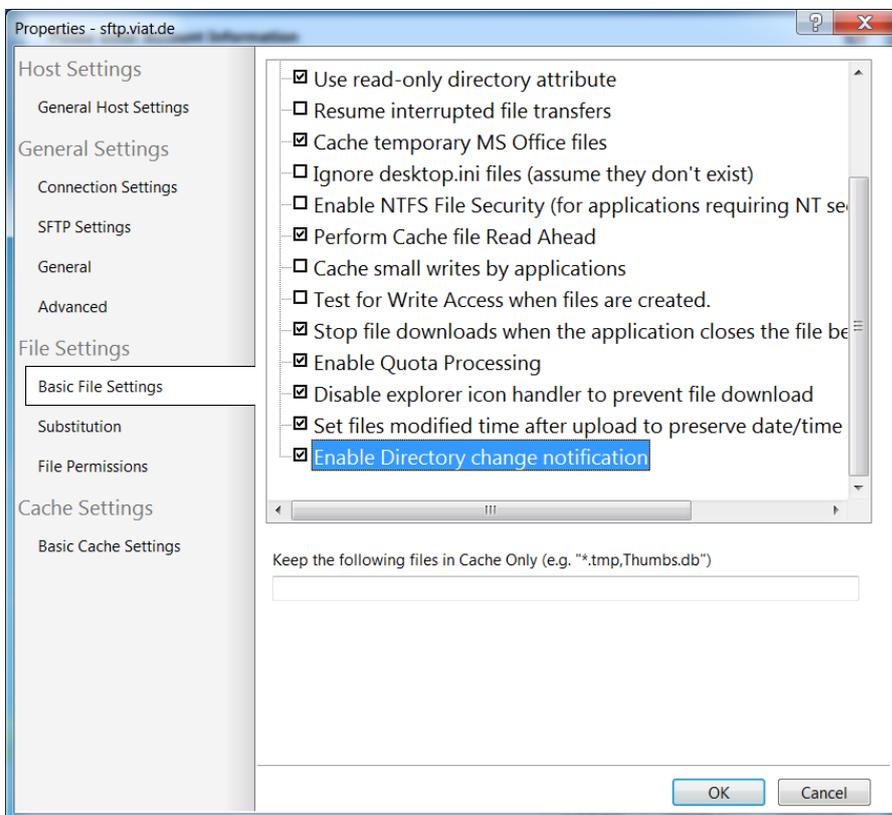


Zuordnen des Zertifikats → Site Properties → SFTP Settings → SFTP HostKey → Client Host Key“ auswählen und Passwort angeben.

Konfiguration Cache → Site Properties → Cache Settings → Basic Cache Settings“ die Parameter “Expire cached files after 30 seconds” und “Expire cached listings after 30 seconds” aktivieren.



Damit der Client die Veränderungen anzeigt, sobald MessageGate Dateien im Verzeichnis eingestellt hat, muss der entsprechende Parameter Site Properties → Cache Settings → Basic Cache Settings „Enable Directory change notification“ aktiviert werden.

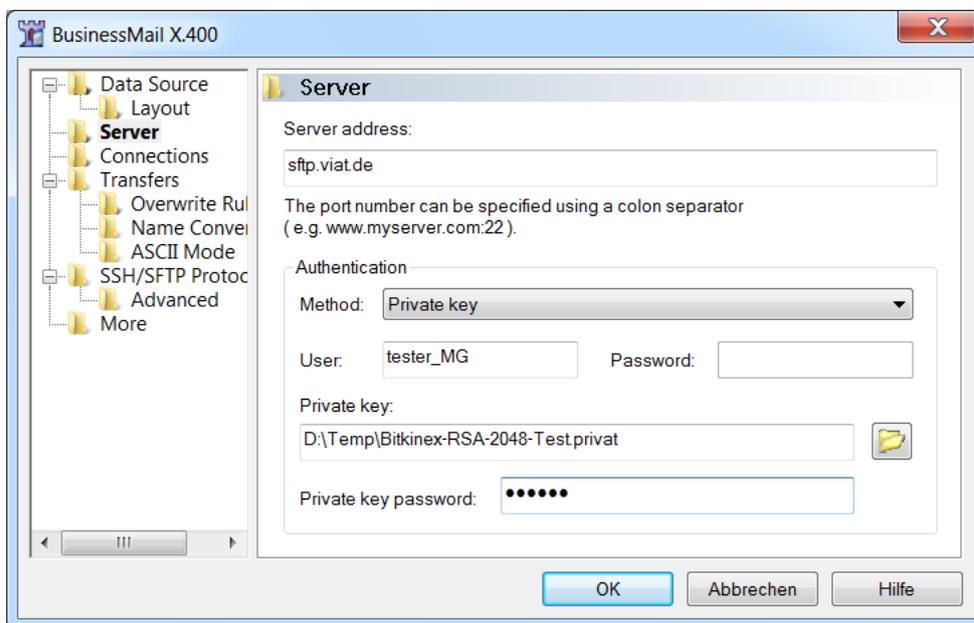


- **BitKinex von BARAD-DUR, LLC**

SFTP (und auch WebDAV) Client mit grafischer Oberfläche und Batchmodus, kann auch als Windows Service laufen

Konfiguration:

Verbindung einrichten: Select SFTP/SSH → Rechte Maustaste oder Data Source → New → SFTP/SSH → Namen zuweisen → Properties → Server



Server address: sftp.viat.de

Authentication Method: Private key

User: Wird von *BusinessMail X.400* bereitgestellt

Private key und Private key password: Mit einem geeigneten Tool (z.B. *puTTYgen*) ein Schlüsselpaar erstellen (Generate) und den öffentlichen Teil des Schlüssels an die Administration von *BusinessMail X.400* senden, damit dieser Schlüssel auf dem Host hinterlegt wird (bitte vorher das Zeilenende-Zeichen mit einem geeigneten Tool, wie z.B. Notepad ++, in LF ändern!). Der private Schlüssel muss lokal gespeichert werden und unter „Private key“ der entsprechende Pfad konfiguriert werden. Falls ein Passwort zugeordnet wurde, dieses bitte unter „Private key password“ angeben.

Durch Doppelklick auf Hosteintrag Fenster von *Bitkinex* Dateimanager öffnen.

Bitkinex bietet auch einen Command Line Modus (ohne Oberfläche) und kann so auch in andere Programme eingebunden werden.

3.3.2 Für Microsoft® Windows 64 Bit Betriebssysteme

Alle im letzten Kapitel aufgeführten Produkte laufen auch unter Windows 64 Bit. South River bietet neuere Versionen von *WebDrive* nur noch als nativ 64 Bit Version an (aktuelle Version *WebDrive NextGen 1.1.16*).

Bitte beachten Sie beim Einsatz von *WebDrive Next Generation* (getestet mit 1.1.13, 1.1.14 und 1.1.16), dass anders als bei den Vorgängerversionen (2019, 2016 usw.) beim Konfigurationspunkt Default directory der Wert „./“ angegeben werden muss (eigentlich sollte dies nicht notwendig sein, da das Login auch das Home Verzeichnis ist). South River versucht dies in einer späteren Version zu korrigieren.

3.3.3 Für Linux und Unix Betriebssysteme

▪ SFTP als Bestandteil des OpenSSH Paketes

Mit dem Programm *ssh-keygen* muss zunächst ein Schlüsselpaar erstellt werden, z.B. *ssh-keygen -t rsa -b 3072* (erzeugt einen 3072 Bit RSA Schlüssel für SSH V2). Das Schlüsselpaar würde dabei im Benutzerverzeichnis im versteckten Unterverzeichnis „*/.ssh*“ mit den Namen *id_rsa* (privater Schlüssel) und *id_rsa.pub* (öffentlicher Schlüssel) angelegt. Der öffentliche Schlüssel muss aber zunächst ins SSH2 Format konvertiert werden, bevor er an die Administration von *BusinessMail X.400* gesendet werden kann:

```
ssh-keygen -e -f ~/.ssh/id_rsa.pub > ~/.ssh/ssh_XXXXX.pub
```

wobei *XXXXX* die *User_ID* des MessageGate Accounts ist. Der Verbindungsaufbau erfolgt dann mit dem Befehl:

SFTP Benutzername@SSH_Host_Name (Benutzername des VMS Account!)

Während der ersten Verbindung müssen Sie den Host Key akzeptieren.

▪ FileZilla

FileZilla ist ein Open Source Client für FTP und SFTP.

Konfiguration:

Die Konfiguration dieses Clients entspricht der unter Windows (siehe Kapitel 3.3.1). Bei neueren Versionen wird das Programm *fzputtygen* mitgeliefert, das zum Erzeugen der notwendigen Schlüsseldateien benutzt werden kann.

3.3.4 Für Apple Max OS X

▪ SFTP aus OpenSSH Paket unter Verwendung des Terminal Programm

Das *OpenSSH* Paket und somit der SFTP-Client kann innerhalb eines Terminalfensters ausgeführt werden. Mit dem Programm *ssh-keygen* muss zunächst ein Schlüsselpaar erstellt werden, z.B. *ssh-keygen -t rsa -b 3072* (erzeugt einen 3072 Bit RSA Schlüssel für SSH V2). Das Schlüsselpaar würde dabei im Benutzerverzeichnis im versteckten Unterverzeichnis „*/.ssh*“ mit den Namen *id_rsa* (privater Schlüssel) und *id_rsa.pub* (öffentlicher Schlüssel) angelegt. Der öffentliche Schlüssel muss aber zunächst ins SSH2 Format konvertiert werden (bitte dabei Zeilenende-Zeichen LF verwenden!), bevor er an die Administration von *BusinessMail X.400* gesendet werden kann:

```
ssh-keygen -e -f ~/.ssh/id_rsa.pub > ~/.ssh/ssh_XXXXX.pub
```

wobei *XXXXX* die *User_ID* des MessageGate Accounts ist). Der Verbindungsaufbau erfolgt dann mit dem Befehl:

SFTP Benutzername@SSH_Host_Name (Benutzername des VMS Account!)

Während der ersten Verbindung müssen Sie den Host Key akzeptieren.

- **FileZilla**

FileZilla ist ein Open Source Client für FTP und SFTP.

Konfiguration:

Die Konfiguration dieses Clients entspricht der unter Windows (siehe Kapitel 3.3.1). Bei neueren Versionen wird das Programm *fzputtygen* mitgeliefert, das zum Erzeugen der notwendigen Schlüsseldateien benutzt werden kann.

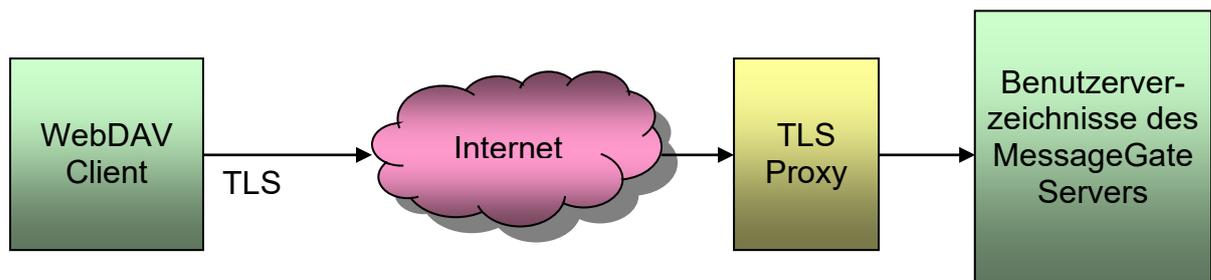
3.3.5 Für alle anderen Betriebssysteme

Auch für viele andere Betriebssysteme, wie z.B. die IBM Betriebssysteme i5/OS bzw. IBM i for Business und zOS gibt es OpenSSH Portierungen, so dass die im Kapitel 3.3.3 Für Linux und Unix Betriebssysteme angegebene Beschreibung auch dort zutreffen sollte. Mangels Testmöglichkeiten wurde dies aber nicht nachgeprüft.

4 Zugang über HTTPS/WebDAV

4.1 Allgemein

Neben dem im vorherigen Kapitel beschriebenen Zugang mittels SFTP wird auch ein Zugang über HTTPS mit WebDAV-Erweiterung angeboten. Dies ist das bevorzugte Protokoll für die Anbindung von Kunden über Internet. Es wird deshalb immer nur eine verschlüsselte (Minimum TLS V1.2 mit mindestens 128 Bit Schlüssel, Server unterstützt auch 256 Bit AES) Verbindung erlaubt. Mit der WebDAV-Erweiterung (RFC 2518 und folgende) bietet HTTP/HTTPS einen zum FTP-Protokoll vergleichbaren Leistungsumfang an, hat aber nicht den Nachteil von FTP, bei dem dann zwei TCP-Verbindungen (Verwaltungs- und Datenverbindung) aufgebaut werden müssen. Der WebDAV Zugang lässt sich deshalb besser in das Sicherheitskonzept (Proxy, Firewall etc.) auf Kundenseite integrieren. Er bietet auch den Vorteil, dass die Applikation auf ein vom WebDAV Server bereitgestelltes Netzwerklaufwerk direkt zugreifen kann, ohne hier ein spezielles Kommunikationsmodul in die Applikation integrieren zu müssen.



Der Zugang erfolgt über die Adresse:

<https://webdav.viat.de/~00000nnnnn/>

wobei nnnnn für die User-ID (*BusinessMail X.400* interne Kennung für Benutzereintrag) steht. Das Zeichen „/“ am Ende der Adresse muss angegeben werden, da ansonsten die Verbindung nicht erfolgreich aufgebaut werden kann.

Voraussetzung für den Aufbau einer TLS-Verbindung zum Applikationsserver ist aber, dass der WebDAV Client auf Aufforderung des TLS-Proxy von *BusinessMail X.400* ein Clientzertifikat sendet. Sie können sich das benötigte Zertifikat mit entsprechendem privaten Schlüssel in *WebConfig* (das CA Zertifikat, mit dem das Zertifikat signiert wurde, kann unter der Service URL: <https://www.service-viat.de> im Bereich „WebConfig & X.400-App“ abgeholt werden) im Menüpunkt „Zertifikatsverwaltung – Erstellen“ generieren lassen und dann im Menüpunkt „Zertifikatsverwaltung – Anzeigen/Download“ als PKCS12 Datei abholen. Bitte beachten Sie, dass dieses Client Zertifikat erst am darauffolgenden Tag beim Proxy aktiviert ist. Falls Ihre Anwendung eine separate Zertifikats- und Schlüsseldatei benötigt, müssen Sie diese mit einem geeigneten Tool (z.B. OpenSSL) aus der PKCS12 Datei extrahieren. Beispiele für OpenSSL:

Export Schlüssel ohne Passortschutz: `openssl pkcs12 -in <name>.p12 -out <name>_key.pem -nodes -nocerts`

Export Schlüssel mit Passortschutz: `openssl pkcs12 -in <name>.p12 -out <name>_key.pem -nocerts`

Export Zertifikat: `openssl pkcs12 -in <name>.p12 -out <name>_key.pem -nodes -nokeys -clcerts`

Falls Ihre Security Policy den Einsatz eines durch eine offizielle CA signierten Zertifikats voraussetzt, wird Ihnen auf Wunsch beim Einrichten Ihres Zuganges dieses bereitgestellt (PKCS12 Datei und separate Zertifikats- und Schlüsseldatei im PEM-Format). Loggen Sie sich dazu mit Ihren Zugangsdaten in *WebConfig* (siehe auch Kapitel 2.9) ein und holen sich das Zertifikat unter dem Menüpunkt „Benutzerverwaltung – Downloads“ als ZIP-Datei ab.

Das abgeholte Zertifikat und den privaten Schlüssel müssen Sie nun noch in Ihren WebDAV-Client importieren. Standardmäßig wird beim Erstellen der P12/PFX Datei, die den privaten Schlüssel und das Zertifikat enthält, ein Passwort zugeordnet, da die meisten Lösungen ein Passwort beim Import erwarten. Sollten Sie eine Lösung einsetzen, bei der ein Passwort aber Probleme bereitet, bitte dies bei der Beauftragung Ihres Accounts angeben. Dann wird eine Datei ohne Passwort bereitgestellt. Beachten Sie, dass nicht alle WebDAV-Lösungen Client Zertifikate unterstützen. Siehe hierzu in Kapitel 4.3 die Beschreibung der Clients, die erfolgreich getestet wurden, bzw. Bibliotheken für WebDAV, die auch Client-Zertifikate unterstützen.

Beim Einrichten des MessageGate Verzeichnisses wird festgelegt, ob das Client Zertifikat auch zur Authentifizierung beim Webserver verwendet oder ob zusätzlich noch ein Benutzername und ein Passwort abgefragt werden soll.

4.2 Besonderheiten des Zuganges

Kunden, die lediglich Mitteilungen erhalten/abholen (z.B. Anwendung für elektronischen Fernmelderechnung), benötigen nicht unbedingt eine WebDAV Lösung, da auch mit einem Webbrowser diese Daten abgeholt werden könnten. Die Mitteilungen/Dokumente würde dann der Purger auf Basis der konfigurierten Verweilzeit im Arbeitsverzeichnis löschen. Sobald aber Daten zum Applikationsserver (Mitteilungen, Lesebestätigungen, Statusabfragen) übertragen werden sollen, ist eine HTTPS Lösung mit WebDAV Erweiterung auf Clientseite notwendig.

Um bei eingeschränkter Funktion zu erkennen, ob Mitteilungen abgelehnt wurden, muss entweder in *WebConfig* ein Status Report abgefragt oder dort die automatische Erzeugung von Status Reports konfiguriert werden. Dann werden diese Reports an der Dateischnittstelle zur automatischen Verarbeitung bereitgestellt.

Bitte beachten Sie beim Upload von Mitteilungsdateien, dass der MessageGate Prozess davon ausgeht, dass diese in ISO-Latin-1/ANSI codiert wurden. Sollte Ihr Betriebssystem diese in UTF-8 (z.B. bei Windows 10 ab Rev. 1903) codiert gespeichert haben, kann es beim Abbilden von Sonderzeichen, z.B. deutscher Umlaute, innerhalb des Betreffs der Mitteilung zu Verfälschungen kommen (in X.400 Mitteilung wird T.61 Zeichensatz verwendet).

Nachfolgend finden Sie einige Kommunikationsmodule bzw. die Bibliotheken, um solche zu erstellen, die in Zusammenhang mit MessageGate getestet wurden.

4.3 Empfohlene WebDAV Kommunikationsmodule

4.3.1 Für Microsoft® Windows 32 Bit Betriebssysteme

- **Microsoft® Windows Explorer (ab Windows 2000)**

Unter Netzwerkumgebung ein neues Netzwerklaufwerk einrichten. Bitte beachten Sie, dass Sie bei Windows 2003 Server und bei Windows Vista (x86) den Patch

KB907306 einspielen müssen, damit die Verbindung aufgebaut wird. Bei Windows 2003 Server muss weiterhin der WebClient Dienst gestartet werden, der standardmäßig auf „Manuell“ steht. Ab Windows 7 kann ein Netzwerklaufwerk nur dann eingerichtet werden, wenn das Client Zertifikat auch zur Authentifizierung beim Webserver verwendet wird. Bitte dies beim Einrichten des WebDAV Accounts entsprechend angeben.

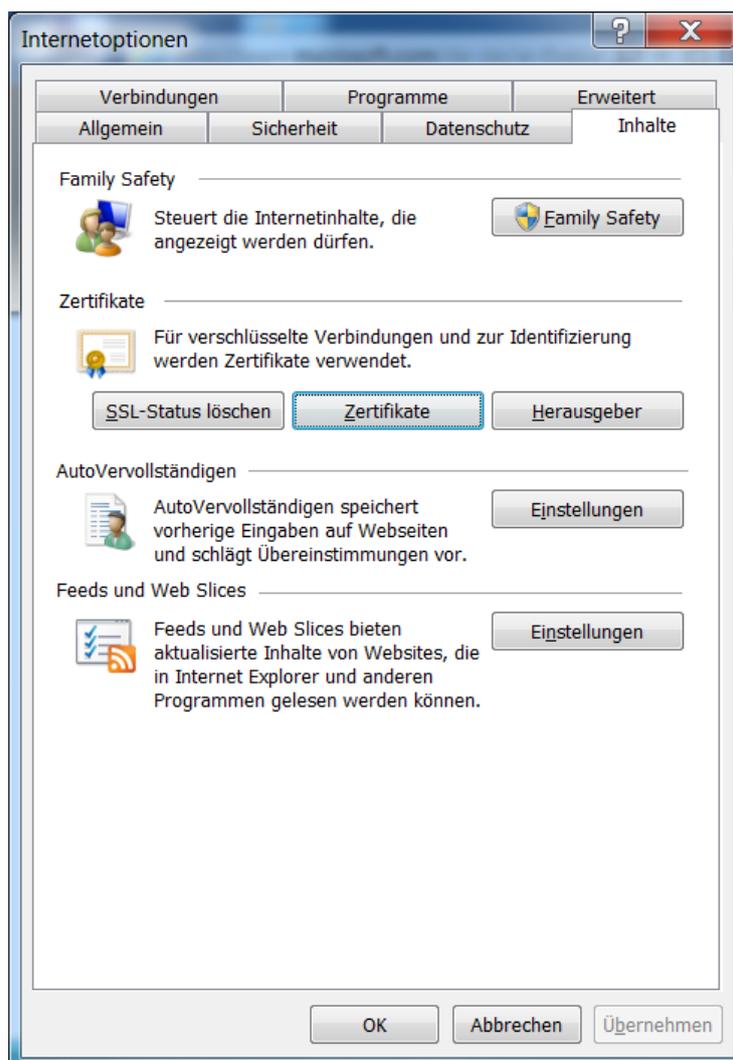
Konfiguration:

Netzwerkumgebung → Netzwerkreisource (bei Windows 2003 Netzwerkumgebung) hinzufügen → https://webdav.viat.de/~00000...

oder bei neuen Windows OS (Windows 7 und neuer):

Netzwerk → Netzwerklaufwerk verbinden → Verbindung mit einer Webseite herstellen... → Eine benutzerdefinierte Netzwerkadresse auswählen → bei Internet – oder Netzwerkadresse „https://webdav.viat.de/~00000...“ eingeben

Voraussetzung ist aber zunächst der Import des Zertifikats mit privaten Schlüssel (*.p12) in den Zertifikatsstore von Windows z.B. durch Doppelklick auf die Zertifikatsdatei, über IE Explorer → Extras → Internetoptionen → Inhalte → Zertifikate → Importieren oder über die MMC (Ausführen MMC.exe) und Snap-Ins hinzufügen → Zertifikate → Eigenes Benutzerkonto (oder Computerkonto) das Snap-In zunächst laden und dann Eigene Zertifikate → Alle Aufgaben → Importieren aufrufen.

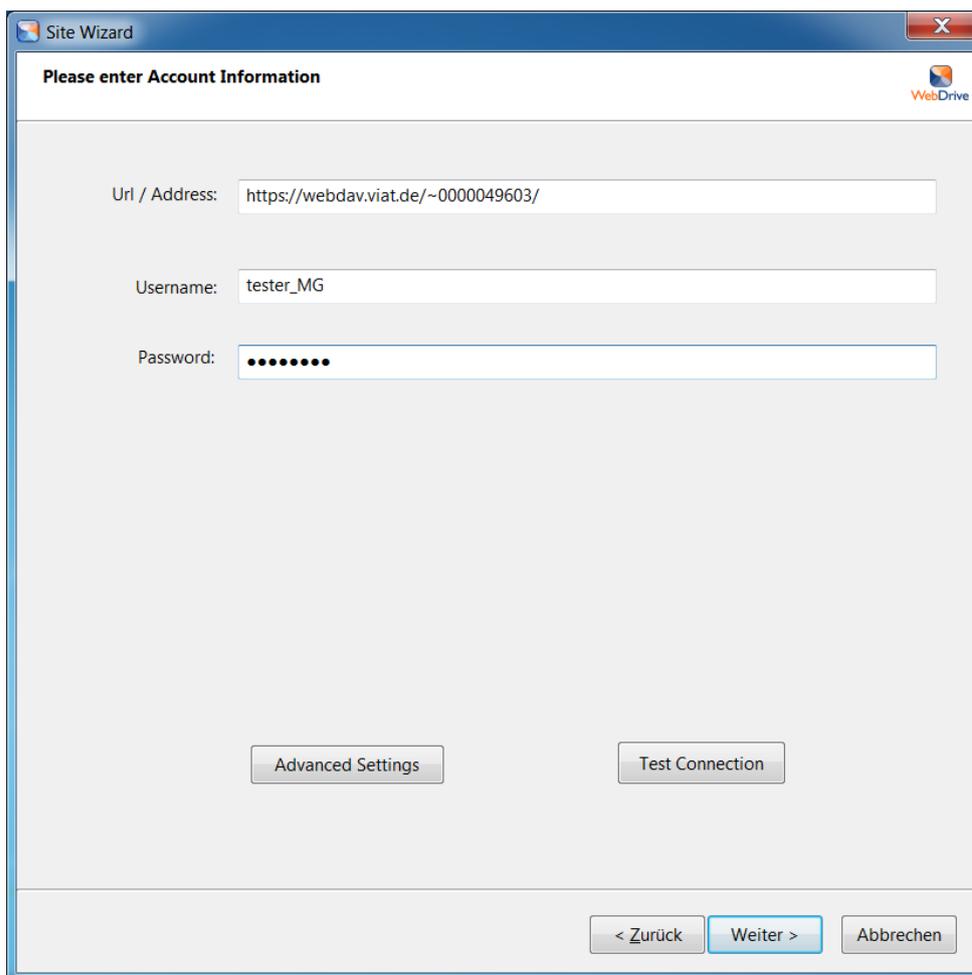


- **WebDrive von South River Technologies**

Erstellen eines Netzwerklaufwerks mit lokalem Laufwerksname über WebDAV (auch über SFTP), so dass das Applikationsverzeichnis wie ein lokales Verzeichnis behandelt werden kann.

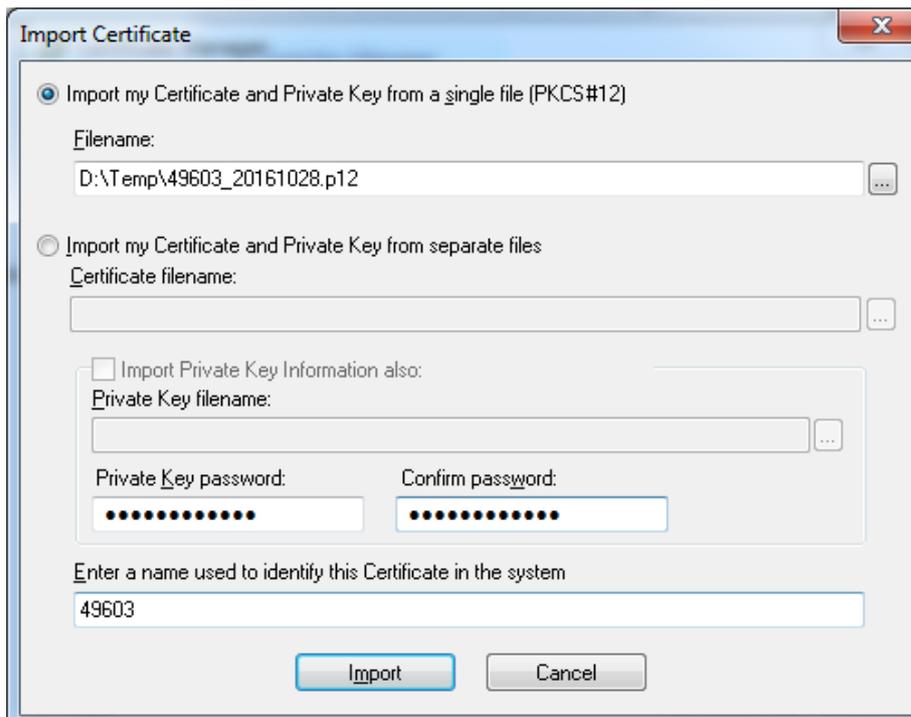
Konfiguration (bei WebDrive 10):

Bei → New den Typ „Secure WebDAV“ auswählen und dann unter URL/Adresse den Wert „https://webdav.viat.de/~00000xxxxx“ (xxxxx ist User-ID) angeben und bei „Username“ und „Password“ die bereitgestellten Daten eintragen

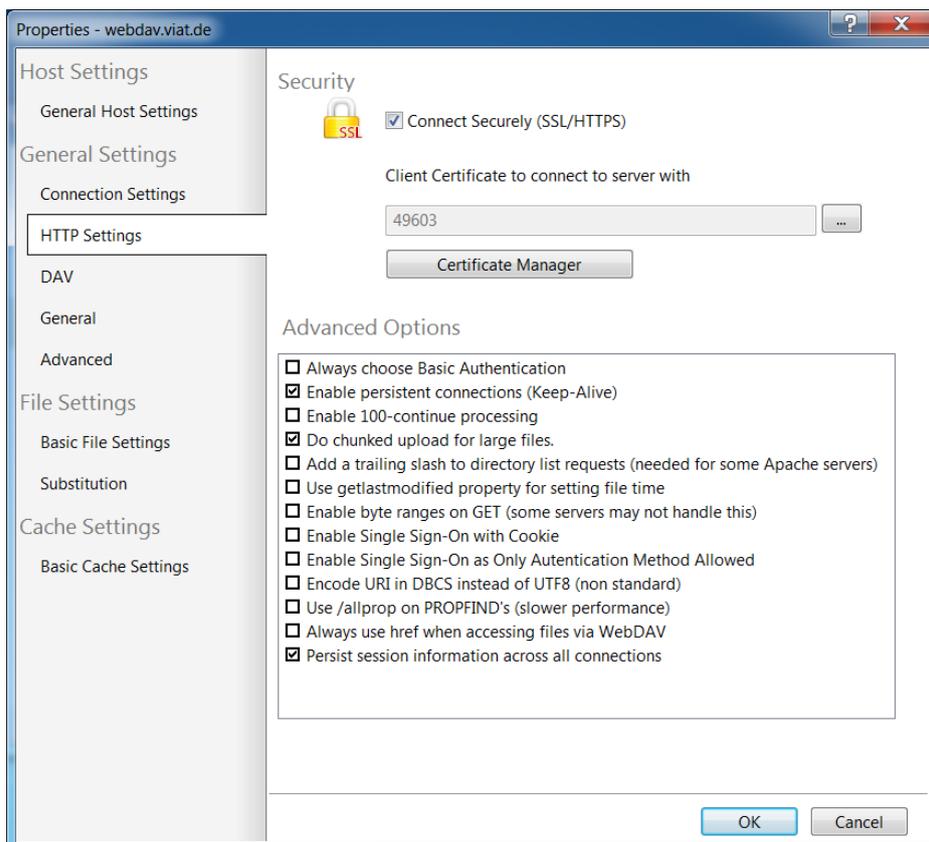


The screenshot shows a 'Site Wizard' dialog box with the title 'Please enter Account Information'. It contains three input fields: 'Url / Address' with the value 'https://webdav.viat.de/~0000049603/', 'Username' with the value 'tester_MG', and 'Password' which is masked with dots. Below the fields are two buttons: 'Advanced Settings' and 'Test Connection'. At the bottom right, there are three navigation buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

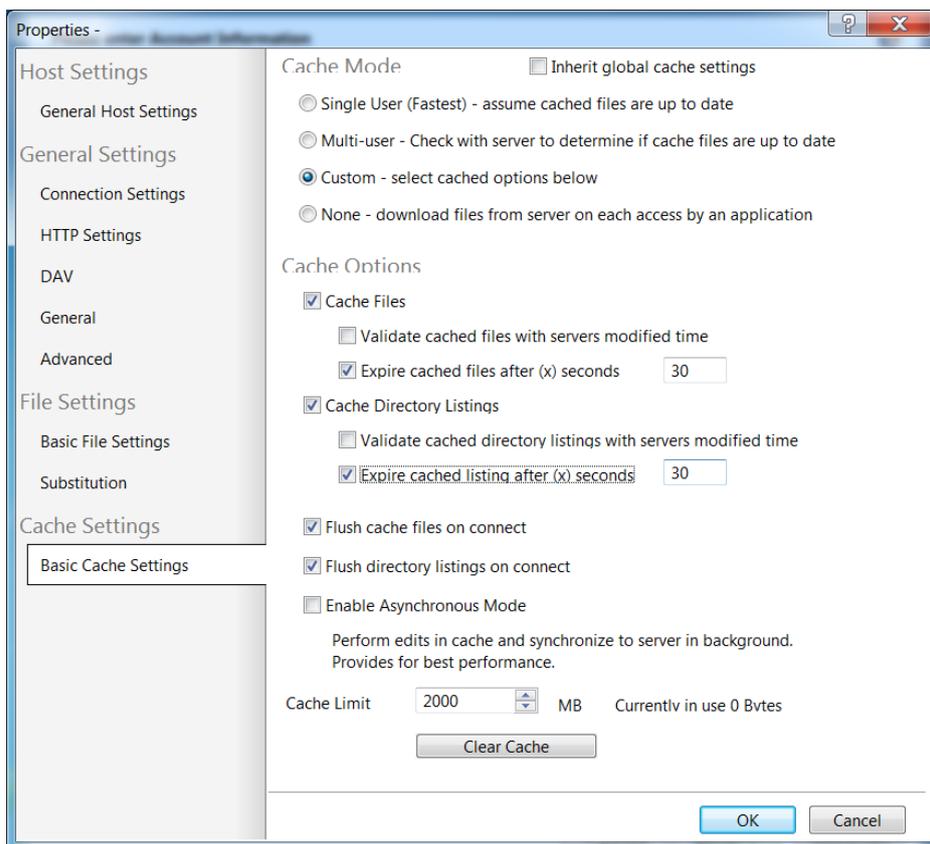
Import des Zertifikats: „→ Advanced Settings → HTTP Settings → Certificate Manager → Import → Import ... from single file (PKCS#12):“ und dann PKCS12 Datei angeben, Passwort angeben und Name zuweisen



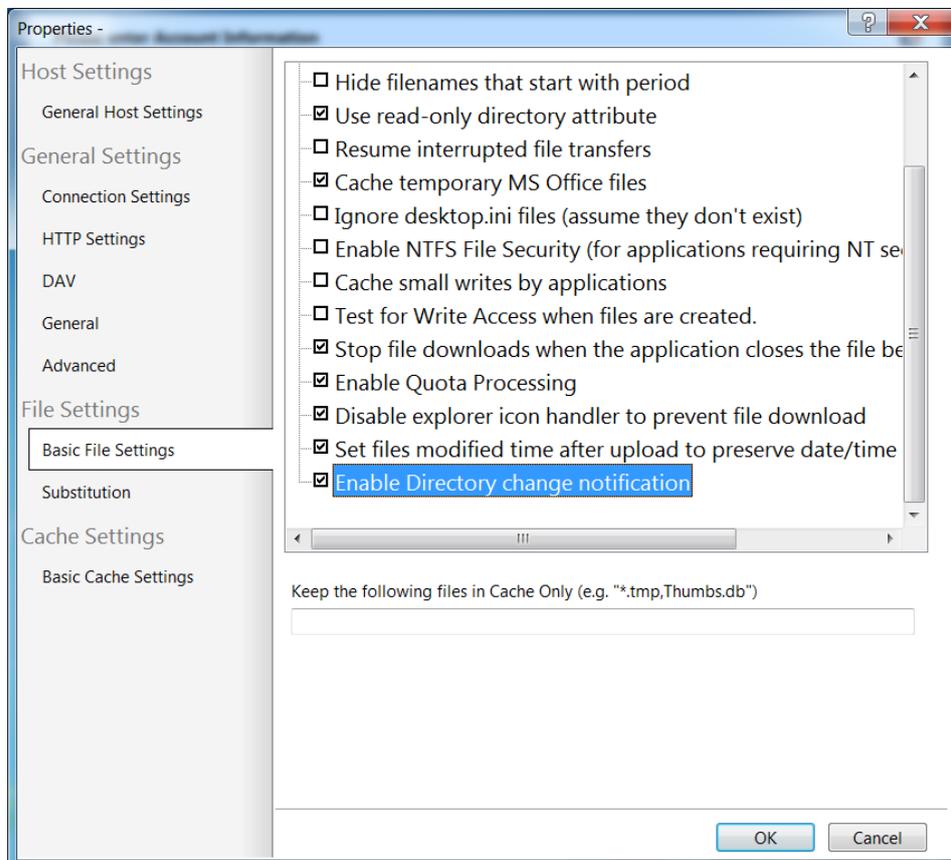
Namen in „Properties of Site“/ HTTP Settings auswählen



Configuration Cache → Program Setting → Cache Settings → Options → Custom →
 Expire cached files after 30 seconds und Expire cached listings after 30 seconds



Damit der Client die Veränderungen anzeigt, sobald MessageGate Dateien im Verzeichnis eingestellt hat, muss der entsprechende Parameter „Enable Directory change notification“ aktiviert werden.

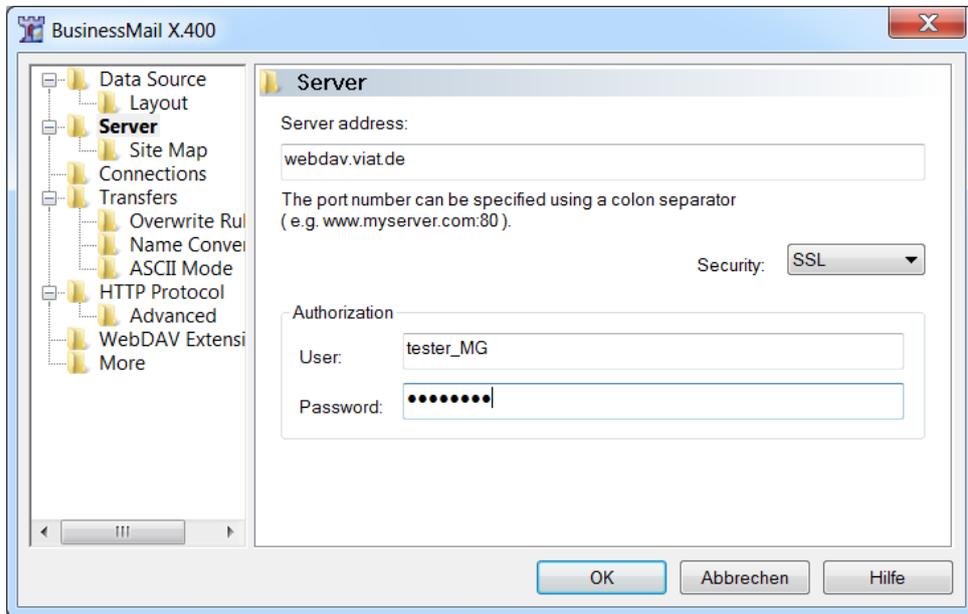


▪ **BitKinex von BARAD-DUR, LLC**

WebDAV (und auch SFTP) Client mit grafischer Oberfläche und Batchmodus, kann auch als Windows Service laufen

Konfiguration:

Verbindung einrichten → Select http → Rechte Maustaste oder Data Source → New → http/webdav → Namen zuweisen → Properties → Server

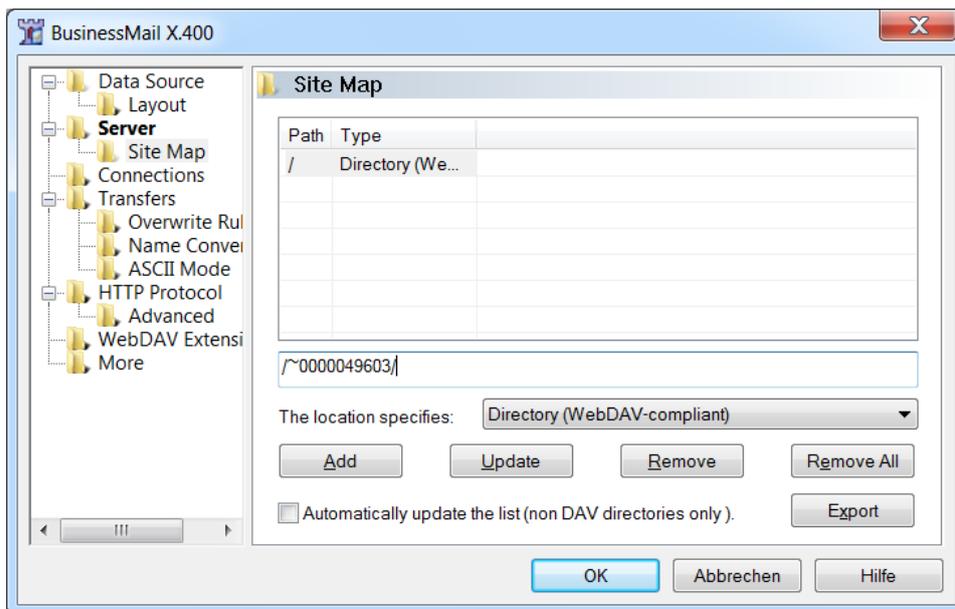


Server address: webdav.viat.de

Security: SSL

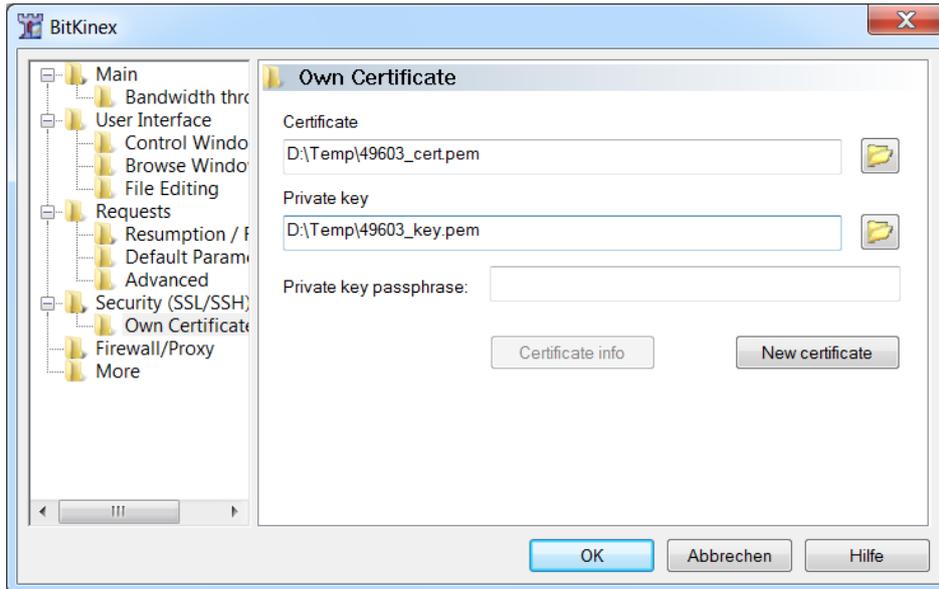
User + Password: Wird von *BusinessMail X.400* bereitgestellt

→ Site Map



Path: /~00000nnnnn/ → (nnnnn ist User-ID)

Zertifikat einrichten → File → Option → Security → Own certificate



Zertifikats- und Schlüsseldatei aus ZIP bzw. PKCS12 Datei extrahieren, Pfad in Oberfläche angeben und Passwort für Schlüssel eintragen.

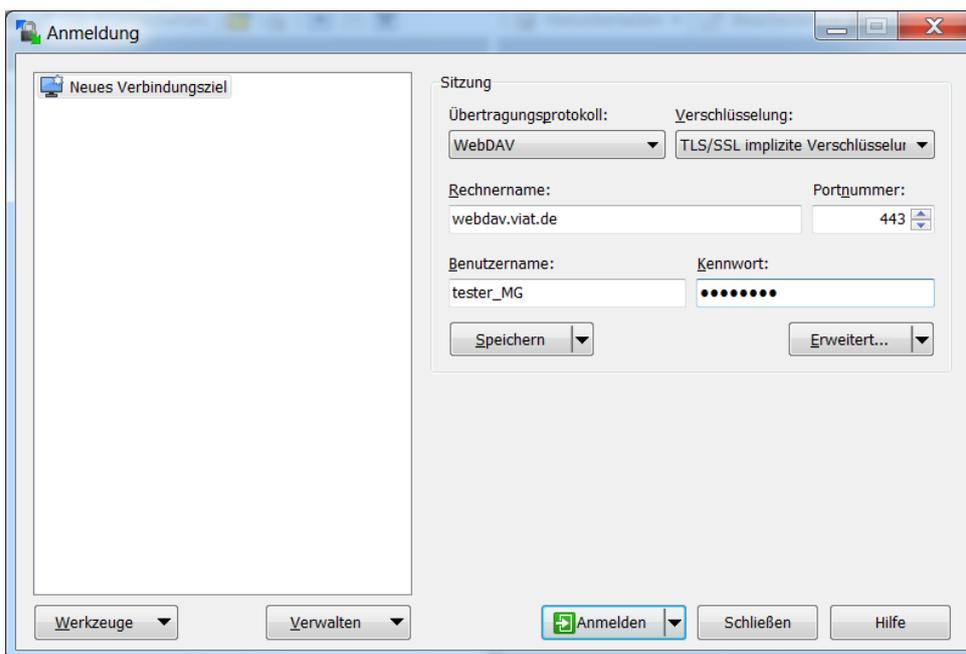
Durch Doppelklick auf Hosteintrag Fenster von *Bitkinex* Dateimanager öffnen

Bitkinex bietet auch einen Command Line Modus (ohne Oberfläche) und kann so auch in andere Programme eingebunden werden.

▪ WinSCP

WinSCP ist ein Open Source Client für SFTP, https/WebDAV und FTP und bietet eine grafische Oberfläche zur Übertragung der Daten vom und zum Webserver.

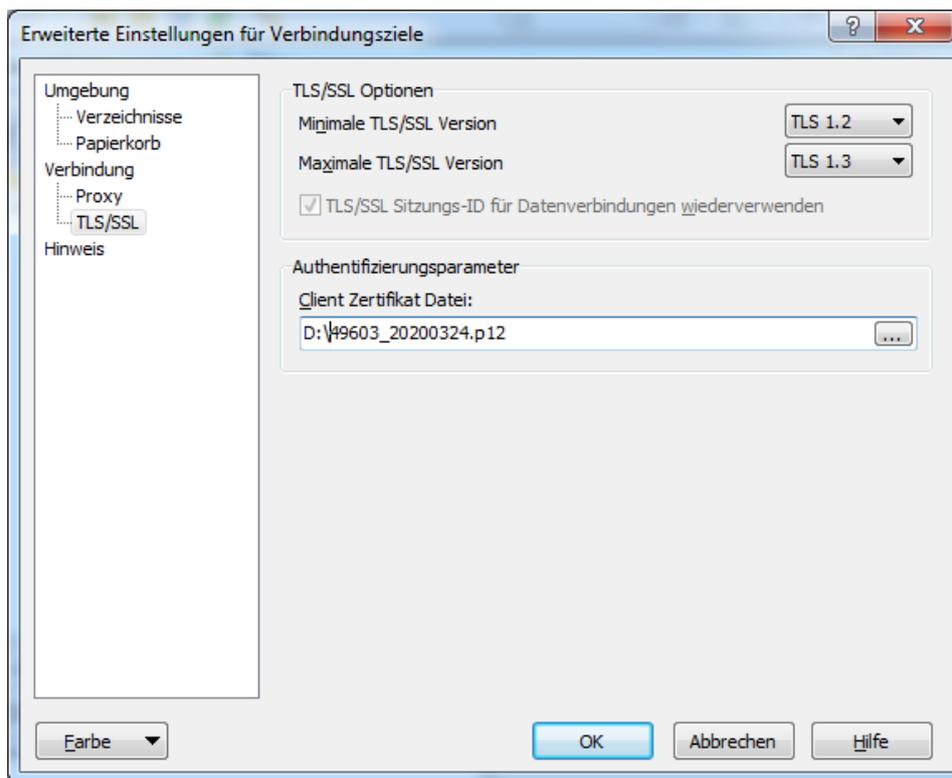
WinSCP kann aber auch im Batchmodus oder im DOS-Fenster mit einem zum Windows FTP Client vergleichbaren Befehlsumfang betrieben werden, um Daten zu übertragen.



Konfiguration:

Sie müssen in WinSCP ein neues Verbindungsziel anlegen. Wählen Sie als Übertragungsprotokoll „WebDAV“ aus. Im Feld „Rechnername“ den logischen Namen des https Servers (über DNS auflösen) oder direkt die IP-Adresse angeben und im Feld „Benutzername“ und „Passwort“ die zur Verfügung gestellten Login Informationen eintragen.

Unter „Erweitert.../Erweitert...“ dann beim Menüpunkt „Verbindung – TLS/SSL“ im Feld „Client Zertifikat Datei“ die bereitgestellte PKCS12 Datei auswählen und nach Verlassen des Menüs „Erweitert...“ dann die Konfiguration speichern.



Nun können Sie sich beim https Server anmelden. Beim Verbindungsaufbau fragt *WinSCP* das Passwort der PKCS12 Datei ab (kann im Batchmodus z.B. über eine Datei importiert werden).

Unter „Erweitert...“ können Sie *WinSCP* an die Erfordernisse Ihrer Anwendung anpassen.

- **Mozilla Firefox für Windows mit Add-on „Open as Webfolder 0.22“**

Für den Webbrowser Mozilla Firefox existiert ein Add-on, das auf die WebDAV Funktion von Windows (des Explorers) zurückgreift und erlaubt, mittels Firefox Dateien an MessageGate zu übergeben und auch Dateien zu löschen. Da das Modul aber nur Windows Funktionen nutzt, die man besser über Explorer eingibt, ist der Einsatz nicht sinnvoll. Unter Linux gibt es für Firefox auch kein Add-on.

- **Onion (WebDAV C++ Library)**

Wird momentan nicht weitergepflegt!

- **Neon (WebDAV C Library, Grundlage für verschiedene WebDAV Clients)**

Bibliothek, letzter Stand September 2021 (siehe <https://notroj.github.io/neon/>).

4.3.2 Für Microsoft® Windows 64 Bit Betriebssysteme

Alle im letzten Kapitel aufgeführten Produkte laufen auch unter Windows 64 Bit.

South River bietet neuere Versionen von *WebDrive* nur noch als nativ 64 Bit Version an (aktuelle Version WebDrive NextGen 1.1.16).

4.3.3 Für Linux und Unix Betriebssysteme

- **Cadaver**

Command Line Client, der vom Befehlsumfang an die FTP Line Clients von Linux und Microsoft® MS-DOS angelehnt ist.

Bei Cadaver muss man zunächst mit dem Befehl "set client-cert Zertifikatsname.p12" das Zertifikat als PKCS12 Datei importieren. Beim Verbindungsaufbau fragt Cadaver das Schlüsselpasswort ab → Zertifikat ohne Passwort beauftragen!

- **Konqueror (Web und Directory Browser für Linux)**

Als Zieladresse „webdavs://webdav.viat.de:443/~xxxxxx“ angeben.

Bei älteren Linux Versionen Probleme mit IPv6 Support, bitte deaktivieren

Konfiguration:

Zunächst muss das Zertifikat unter Einstellungen → Verschlüsselung → Ihre Zertifikate importiert werden. Dann muss unter Authentifizierung dieses Zertifikat als Standardzertifikat mit Option Senden oder aber die Option Nachfragen gewählt werden.

Bei neueren Linux Distributionen kann (z.B. bei open SUSE mittels Konqueror bzw. Dolphin) ein Netzwerk Ordner eingerichtet werden.

Bei open SUSE Netzwerk Browser aufrufen → Netzwerk Ordner hinzufügen → Web-Ordner

- Unter Namen einen beliebigen Namen zuordnen
- Bei User den Benutzernamen Ihres WebDAV Accounts eingeben
- Bei Server „webdav.viat.de“ eingeben
- Bei Port 443 eingeben
- Bei Ordner „~00000nnnnn“ eingeben, wobei nnnnn für die User-ID Ihres MessageGate Eintrags steht
- Verbindung verschlüsseln aktivieren

- **davfs (Dateisystem für das direkte Einbinden eines Netzwerklaufwerks)**

Installation für Debian und Ubuntu, läuft aber auch nach Installation entsprechender Bibliotheken unter open SUSE-Linux

Unter <https://www.service-viat.de> finden Sie eine ausführliche Beschreibung für die Einrichtungen eines Netzwerklaufwerks mittels davfs.

Bitte beachten Sie, das Dateisystem vor dem Herunterfahren des Rechners zu „dismounten“!

- **Sitecopy (Konsolen Programm zum Abgleich zwischen einem lokalen Verzeichnis und dem MessageGate Verzeichnis)**

Ab Version 0.16.3. Die Konfigurationsdatei könnte z.B. so lauten:

```
***
site webdav
server webdav.viat.de
protocol webdav
username <Username>
password <Password>
client-cert </path/to/cert.p12>           #in man-page nicht aufgelistet!
remote /~<User-ID>/
local /<localer/pfad>/
http secure
***
```

- **Onion (WebDAV C++ Library)**

Wird momentan nicht weitergepflegt!

- **Neon (WebDAV C Library, Grundlage für verschiedene WebDAV Clients)**

Bibliothek, letzter Stand September 2021 (siehe <https://notroj.github.io/neon/>).

4.3.4 Für Apple iOS

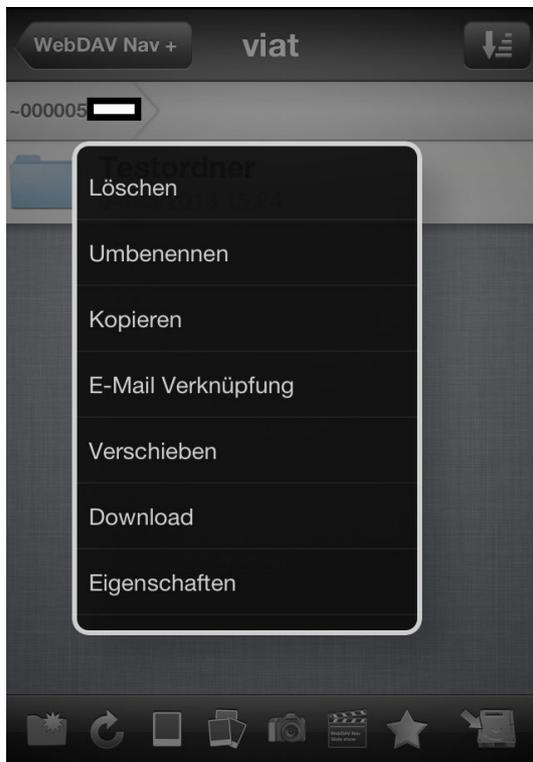
- **WebDAV Nav+ (kostenpflichtige App für Power User, kostenlose Version WebDAV Nav unterstützt kein Client Zertifikat)**

Die App aus dem iPhone App Store herunterladen und installieren. Zunächst müssen Sie ein neues Profil mit den für Ihren MessageGate Account bereitgestellten Zugangsdaten einrichten.



Dann müssen Sie für die Autorisierung beim TLS-Proxy bereitgestellte PKCS12 Datei im Root Verzeichnis (Dokumente) mit dem Namen des Profils ablegen. Also in unserem Beispiel wäre dies der Dateiname „viat.p12“.

Nun können Sie sich in das MessageGate Verzeichnis einloggen und Daten hochladen bzw. abholen. Das nachfolgende Bild zeigt die verfügbaren Optionen.



4.3.5 Für alle anderen Betriebssysteme

- **Neon (WebDAV C Library, Grundlage für verschiedene WebDAV Clients)**
Bibliothek, letzter Stand September 2021 (siehe <https://notroj.github.io/neon/>).
- **Sitecopy (Abgleich von Dokumenten zwischen Client und Host mit WebDAV)**

Ab Version 0.16.3. Die Konfigurationsdatei könnte z.B. so lauten:

```

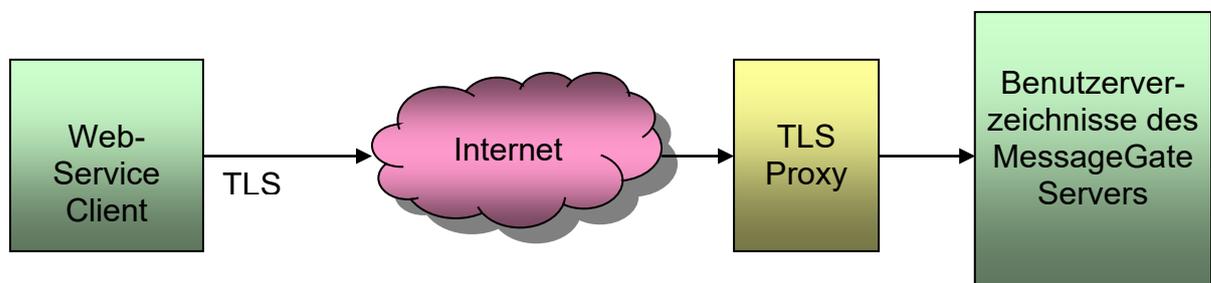
***
site webdav
server webdav.viat.de
protocol webdav
username <Username>
password <Password>
client-cert </path/to/cert.p12>           #in man-page nicht aufgelistet!
remote /~<User-ID>/
local /<localer/pfad>/
http secure
***

```

5 Zugang über HTTPS/Web-Services

5.1 Allgemein

Neben den in den vorherigen Kapiteln beschriebenen Zugängen wird nun auch ein Zugang für das MessageGate File Interface über einen REST basierenden Web-Service (HTTPS) angeboten. HTTPS ist das bevorzugte Protokoll für die Anbindung von Kunden über Internet. Eine verschlüsselte (Minimum TLS V1.2 mit mindestens 128 Bit Schlüssel, Server unterstützt auch 256 Bit AES) Verbindung ist hierbei verpflichtend. Neben den schon im letzten Kapitel erläuterten Vorteil beim Zugang über HTTPS mit WebDAV Erweiterung (bessere Integration in das Netzwerk Sicherheitskonzept) lässt sich ein Web-Service auch besonders gut in eine Applikation integrieren, falls dies gewünscht ist.



Der Zugang erfolgt über die Adresse:

<https://webdav.viat.de/mgate/vn/~00000nnnnn/>

wobei das nnnnn für die User-ID (*BusinessMail X.400* interne Kennung für Benutzer eintrag) und das n bei v für die Nummer des hinterlegten Web-Service Profils steht. Alle Profile unterstützen die Funktionen PUT (Übertragen einer Mitteilungsdatei, einer Transmission Set Datei, einer Lesebestätigungsdatei oder einer Statusabfrage Datei), GET (Abholen einer Dateiliste, einer Mitteilungsdatei, einer Transmission Set Datei oder einer Status Abfrage Datei) und DELETE (Löschen einer Mitteilungsdatei, einer Transmission Set Datei oder einer Status Datei). Das Zeichen „/“ am Ende der Adresse muss angegeben werden, da ansonsten die Verbindung nicht erfolgreich aufgebaut werden kann.

Voraussetzung für den Aufbau einer TLS-Verbindung zum Applikationsserver ist aber, dass der Web-Service Client auf Aufforderung des TLS-Proxy von *BusinessMail X.400* ein Clientzertifikat sendet. Sie können sich das benötigte Zertifikat mit entsprechendem privatem Schlüssel in WebConfig (das CA-Zertifikat, mit dem das Zertifikat signiert wurde, kann unter der Service URL: <https://www.service-viat.de> im Bereich „WebConfig & X.400-App“ abgeholt werden) im Menüpunkt „Zertifikatsverwaltung – Erstellen“ generieren lassen und dann im Menüpunkt „Zertifikatsverwaltung – Anzeigen/Download“ abholen. Bitte beachten Sie, dass dieses Zertifikat erst am darauffolgenden Tag beim Proxy aktiviert ist.

Falls Ihre Security Policy den Einsatz eines durch eine offizielle CA signierten Zertifikats voraussetzt, wird Ihnen auf Wunsch beim Einrichten Ihres Zuganges dieses bereitgestellt (PKCS12 Datei und separate Zertifikats- und Schlüsseldatei im PEM-Format). Loggen Sie sich dazu mit Ihren Zugangsdaten in *WebConfig* (siehe auch

Kapitel 2.9) ein und holen sich das Client Zertifikat unter dem Menüpunkt „Benutzerverwaltung – Downloads“ ab.

Das abgeholte Zertifikat und den privaten Schlüssel müssen Sie nun noch in Ihren Web-Service Client bzw. Ihre Web-Service Anwendung importieren. Standardmäßig wird beim Erstellen der P12/PFX Datei, die den privaten Schlüssel und das Zertifikat enthält, ein Passwort zugeordnet, da die meisten Lösungen ein Passwort beim Import erwarten. Sollten Sie eine Lösung einsetzen, bei der ein Passwort aber Probleme bereitet, bitte dies bei der Beauftragung Ihres Accounts angeben. Dann wird eine Datei ohne Passwort bereitgestellt.

Beim Einrichten des MessageGate Verzeichnisses wird festgelegt, ob das Client Zertifikat auch zur Authentifizierung beim Webserver verwendet (Standard) oder ob zusätzlich noch ein Benutzername und ein Passwort abgefragt werden soll.

5.2 Besonderheiten des Zuganges

Der Web-Service Zugang wurde so konzipiert, dass er mittels Skripts sehr flexibel an die Bedürfnisse der Kunden angepasst werden kann und dass verschiedene Profile hinterlegt werden können. Beim Web-Service stehen zurzeit die Profile 1 (v1) und 2 (v2/v2a) zur Verfügung. Bei v1 wird weitestgehend ein 1:1 Mapping zu den vorhandenen MIME-Strukturen (Content Type) der Dateien im Übergabeverzeichnis vorgenommen, während bei v2 (v2a) die Daten standardmäßig als JSON (Array) Struktur übertragen werden.

Bitte beachten Sie beim Upload von Mitteilungsdateien, dass der MessageGate Prozess davon ausgeht, dass diese in ISO-Latin-1/ANSI codiert wurden. Sollte Ihr Betriebssystem diese in UTF-8 (z.B. bei Windows 10 ab Rev. 1903) codiert gespeichert haben, kann es beim Abbilden von Sonderzeichen, z.B. deutscher Umlaute, innerhalb des Betreffs der Mitteilung zu Verfälschungen kommen (in X.400 Mitteilung wird T.61 Zeichensatz verwendet).

5.3 Web-Service API

Methoden	Request https://webdav.viat.de/mgate/	Beschreibung
Upload file	PUT .../v1/~00000nnnnn/<file name> Content-Type: message/rfc822 PUT .../v1/~00000nnnnn/<file name> Content-Type: text/plain PUT .../v2/~00000nnnnn/<file name> Content-Type: application/json PUT .../v3/~00000nnnnn/<file name> Content-Type: application/json	Hochladen einer Datei: <ul style="list-style-type: none"> • Mitteilung • Transmission Set • Status Report Request • Receipt Notification
List dir	GET .../v1/~00000nnnnn/*.out Content-Type: text/plain GET .../v1/~00000nnnnn/M_* Content-Type: text/plain GET .../v1/~00000nnnnn/*.in Content-Type: text/plain	Liste aller Dateien: <ul style="list-style-type: none"> • mit Endung “.out” • die mit „M_“ beginnen • die mit „.in“ enden

	<pre>GET .../v2/~0000nnnnn/*.out Content-Type: application/json GET .../v2/~0000nnnnn/M_* Content-Type: application/json GET .../v2/~0000nnnnn/*.in Content-Type: application/json GET .../v3/~0000nnnnn/*.out Content-Type: application/json GET .../v3/~0000nnnnn/M_* Content-Type: application/json GET .../v3/~0000nnnnn/*.in Content-Type: application/json</pre>	
Get file	<pre>GET .../v1/~0000nnnnn/<file name> Msg: Content-Type: message/rfc822 TS: Content-Type: text/plain SR: Content-Type: text/plain, text/csv-c, oder text/csv-s GET .../v2/~0000nnnnn/<file name> Msg: Content-Type: application/json TS: Content-Type: application/json SR: Content-Type: application/json GET .../v3/~0000nnnnn/<file name> Msg: Content-Type: application/json TS: Content-Type: application/json SR: Content-Type: application/json</pre>	<p>Abholen Datei:</p> <ul style="list-style-type: none"> • Mitteilung (Msg) • Transmission Set (TS) • Status Report (SR)
Delete file	<pre>DELETE .../v1/~0000nnnnn/<file name> DELETE .../v2/~0000nnnnn/<file name> DELETE .../v3/~0000nnnnn/<file name></pre>	Löschen einer Datei

5.3.1 Das Web-Service Profil v1

Das Profil enthält die folgenden Funktionen:

PUT - Upload einer Datei

Mit der Methode "PUT" wird eine neue Datei im MessageGate Verzeichnis angelegt. PUT erwartet dabei die Datei als Content, wobei der (eindeutige) Dateiname mit einem "M", "T", "R" oder "S" gefolgt von einem Unterstrich "_" beginnen muss. Die Dateierweiterung muss explizit auf ".in" enden oder wenn diese fehlt, wird dann implizit ein ".in" ergänzt. Groß-/Kleinschreibung spielt beim Dateinamen keine Rolle. Sind diese Bedingungen nicht erfüllt, wird der Status "HTTP 404 Not found" mit der erweiterten Information „Invalid filename format" zurückgeliefert.

Wird das Header-Feld "Content-Type" beim PUT mitgeliefert, muss der Wert bei den Dateitypen "T", "R" und "S" mit "text" beginnen. Für den Dateityp "M" muss ein Header-Element "Content-Type" vorhanden sein, das entweder den Wert "message/rfc822" enthält oder mit "application/" (z.B. application/octet-stream) beginnt. Andernfalls wird der Status "HTTP 406 – Not Acceptable" mit der erweiterten Information „Illegal combination of filename and Content-Type" zurückgeliefert.

Bei Übertragung von Daten mit Content-Type "text/..." dürfen keine binären Daten übertragen werden. Ist beim Upload die übertragende Datei noch nicht vorhanden, wird sie neu angelegt und der Status "HTTP 201 Created" zurückgeliefert. Das Header-Feld "Location" enthält als Wert dann die neue URL. Ist beim Upload eine Datei mit dem definierten Namen bereits vorhanden, wird die Übertragung abgelehnt und der Status "HTTP 423- Locked" mit der erweiterten Information „File currently locked" zurückgeliefert. Beim Upload können nur "ganze" Dateien übertragen werden. Die Verwendung des Header-Feld "Content-Range" ist somit unzulässig und wird mit dem Status "HTTP 400 Bad request" mit der erweiterten Information „Content-Range not allowed" quittiert.

Ein Beispiel für das Hochladen einer Message Datei (M_) mit curl:

```
curl https://webdav.viat.de/mgate/v1/~0000049640/ -X PUT -T M_161031_001.in -H "Content-Type: message/rfc822" --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Der abschließende Schrägstrich "/" bei der URL ist erforderlich.

GET - Dateiliste abrufen

Mit der Methode "GET" kann eine Liste der Dateien im Verzeichnis mit dazugehörigem Datum sowie die Dateigröße in Byte angefordert werden. Übergibt man beim GET nur die URL des MessageGate Verzeichnis erhält man als Ergebnis eine Dateistruktur im CSV-C-Format (Felder durch Komma getrennt), die alle Dateien mit Erstellungsdatum (YYYY-MM-DD HH-MM-SS) und Größenangabe in Bytes enthält.

Das Beispiel mit curl:

```
curl https://webdav.viat.de/mgate/v1/~0000049640/ --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

ergibt z.B. die CSV-Struktur:

```
"Filename","Datetime","Filesize"
"m_1610.in_err0007","2016-10-31 15:02:22",6756
"s_161024.out","2016-10-31 15:16:17",7138
"m_d45f427672e345.out", 2016-10-31 15:16:59",204217
```

Wird als Format in CSV-S (Felder durch Semikolon getrennt) gewünscht, ist dies mit dem HTTP-Header "Accept: text/csv-s" anzugeben. Wird eine reine Textdatei ohne Überschriften und anderes Datumsformat (DD MMM YYYY HH-MM-SS, wobei MMM für den abgekürzten englischen Monatsnamen steht) erwartet, muss der HTTP-Header "Accept: text/plain" angegeben werden.

In der Liste werden Unterverzeichnisse nicht berücksichtigt. Der Umfang der bereitgestellten Liste kann explizit durch Ergänzung der URL um ein entsprechendes Selektionskriterium (z.B. „*.out“ oder „*.in“, sofern diese nicht schon vom Poller des MessageGate Prozess verarbeitet wurden) reduziert werden.

Hier ein Beispiel mit curl:

```
curl https://webdav.viat.de/mgate/v1/~0000049640/*.in --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Wildcards („*“) können auch benutzt werden, um die Liste der Dateien auf einen bestimmten Typ (z.B. „m_*.out“) einzuschränken.

GET - Download einer Datei

Mit "GET" kann auch gezielt eine bestimmte Datei durch Ergänzung der URL um den Dateinamen heruntergeladen werden. Hier ein Beispiel mit curl, bei dem eine Message Datei abgeholt und der Default Content Type message/rfc822 verwendet wird:

```
curl https://webdav.viat.de/mgate/v1/~0000049640/m_53786626568.out --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Die Dateiendung ".out" ist bei Downloads optional und wird bei Fehlen implizit verwendet.

Der vom Web-Service zurückgelieferte Content-Type ist abhängig vom Wert bei "Accept" im Request und auch vom Typ (Dateinamen) der Datei, die heruntergeladen werden soll.

Beginnt der Dateiname nicht mit "M_", "T_" oder "S_" oder ist die Dateiendung weder ".out" noch nicht vorhanden, dann wird ein Content-Type "application/octet-stream" bzw. wenn nicht anders möglich "text/plain" verwendet.

Beginnt der Dateiname mit "M_", dann wird ein Content-Type "message/rfc822" bzw. als Notlösung "application/octet-stream" verwendet.

Beginnt der Dateiname mit "T_", dann wird ein Content-Type "text/plain" verwendet.

Beginnt der Dateiname mit "S_", dann wird ein Content-Type "text/csv-c", "text/csv-s" oder "text/plain" verwendet, je nachdem, in welchem Format die Datei tatsächlich vorliegt und was als "Accept" angegeben wurde.

Folgende HTTP Response Codes sind möglich:

200 OK (Anfrage erfolgreich bearbeitet, Datei wird heruntergeladen.)

404 Not found (Die Datei existiert nicht.)

406 Not Acceptable (Der Dateityp passt nicht zum Wert bei "Accept")

423 Locked (Die angeforderte Datei wird gerade anderweitig bearbeitet)

DELETE - Eine Datei löschen

Mit "DELETE" wird eine bestimmte Datei aus dem Verzeichnis gelöscht.

Hier ein Beispiel mit curl:

```
curl https://webdav.viat.de/mgate/v1/~0000049640/s_161031.out -X DELETE --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Die Dateiendung ".out" ist beim Löschen optional und wird implizit ergänzt, sofern eine Datei mit diesem Namen existiert. Im Erfolgsfall wird der Status "HTTP 204 No content" zurückgeliefert. Dies gilt auch dann, wenn die Datei vorher schon nicht mehr existiert hat. Dieser Status bedeutet somit, dass eine Datei mit diesem Namen nach erfolgreicher Anfrage nicht mehr vorhanden ist.

Ist die angegebene Datei noch in Bearbeitung oder anderweitig gesperrt, wird der Status "HTTP 423 Locked" mit der erweiterten Information „File currently locked" zurückgeliefert.

Die Verwendung von Wildcards/Platzhalter im Dateinamen ist nicht erlaubt. Bei solch einem Request wird der Status "HTTP 500 Internal Server Error" zurückgeliefert.

5.3.2 Das Web-Service Profil v2 (v2a)

Bei diesem Profil (bei v2 werden die beim Download bereitgestellten Daten mit CR/LF, Leerzeichen und Tabs zur besseren Lesbarkeit versehen, bei v2a ohne Zusatzzeichen) werden die bisherigen Strukturen (Text, Message RFC2822, CSV usw.) in eine JSON-Struktur umgesetzt. Beim Upload können unabhängig vom Profil v2 oder v2a die Daten mit oder ohne Zusatzzeichen übertragen werden. Die in den ein-

zelen Dateien verwendeten Feldbezeichner und deren Werte innerhalb der JSON Struktur entsprechen dabei weitestgehend denen in den Kapiteln 2.3 (Mitteilung), 2.5 (Transmission Set), 2.7.2 (Anfordern Status Report) und 2.8 (Senden Lesebestätigung).

Da aber das bei den RFC2822 Feldbezeichnern einer Mitteilungsdatei (z.B. Message-ID) verwendete Minus-/Trennzeichen „-“ bei Java Scripts zu Problemen führen kann, werden diese beim Download von Daten durch Unterstrich „_“ ersetzt und auch der Punkt bei X.400 Adresse (X400_Address) entfällt. Außerdem wird bei den Feldbezeichnern eine einheitliche Schreibweise verwendet; das erste Zeichen (auch nach „_“) wird groß, der Rest klein geschrieben. Zusätzliche Ausnahmen werden weiter unten bei den Beispielen beschrieben.

Während der Absender (From:) bei einer Mitteilung nur einmal vorkommen kann, ist es bei MessageGate und damit auch bei diesem Profil möglich, mehrere Empfänger anzugeben. Dazu wird dann jeweils ein Array für To:, Cc: und Bcc: (die beiden letzteren nur falls vorhanden) angegeben, in dem die einzelnen Adressen als Elemente (X400_Address, User_Id) aufgeführt sind. Das Array wird auch verwendet, wenn nur eine Adresse enthalten ist.

Binäre Daten als Anhang einer Mitteilung sollten immer BASE64 codiert übergeben werden. Bitte dies auch bei der Grundeinstellung des MessageGate Accounts in WebConfig definieren, so dass binäre Daten immer BASE64 codiert an der Dateischnittstelle ausgeliefert und somit auch entsprechend abgeholt werden. Bei signierten Mitteilungen den Absender darum bitten, dass die binären Inhalte BASE64 codiert sind.

Beim Anfordern eines Status Reports sollte immer als Format "CSV-C" oder "CSV-S" angegeben werden, damit das Mapping in die JSON-Struktur korrekt funktioniert.

Das Profil enthält die folgenden Funktionen:

PUT - Upload einer Datei

Mit der Methode "PUT" wird eine neue Datei im MessageGate Verzeichnis angelegt. PUT erwartet dabei die Datei als Content, wobei der (eindeutige) Dateiname mit einem "M", "T", "R" oder "S" gefolgt von einem Unterstrich "_" beginnen muss. Die Dateierweiterung muss explizit auf ".in" enden oder wenn diese fehlt, wird dann implizit ein ".in" ergänzt. Groß-/Kleinschreibung spielt beim Dateinamen keine Rolle. Sind diese Bedingungen nicht erfüllt, wird der Status "HTTP 404 Not found" mit der erweiterten Information „Invalid filename format“ zurückgeliefert.

Wird das http Header-Feld "Content-Type" beim PUT mitgeliefert, sollte der Wert bei allen Dateitypen "application/json" lauten. Bei ungültigem Content Type wird der Status "HTTP 406 – Not Acceptable" mit der erweiterten Information „Illegal combination of filename and Content-Type" zurückgeliefert.

Ist beim Upload die übertragende Datei noch nicht vorhanden, wird sie neu angelegt und der Status "HTTP 201 Created" zurückgeliefert. Das Header-Feld "Location" enthält als Wert dann die neue URL. Ist beim Upload eine Datei mit dem definierten Namen bereits vorhanden, wird die Übertragung abgelehnt und der Status "HTTP 423- Locked" mit der erweiterten Information „File currently locked" zurückgeliefert. Beim Upload können nur "ganze" Dateien übertragen werden. Die Verwendung des Header-Feld "Content-Range" ist somit unzulässig und wird mit dem Status "HTTP 400 Bad request" mit der erweiterten Information „Content-Range not allowed" quittiert.

Ein Beispiel für das Hochladen eine Message Datei (M_), die zwei Body Parts (Beispiel mit einem Body Part siehe GET) hat, mit curl:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/ -X PUT -T M_161031_001.in -H "Content-Type:application/json" --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

mit der folgenden JSON-Struktur (mit Zeilenumbrüchen, Leerzeichen und Tabs entsprechend dem Profil v2):

```
{
  "TO": [
    {
      "X400_Address": "G=ipm;S=tester;O=testag;A=viaT;C=de",
      "User_Id": "49637"
    }
  ],
  "From": {
    "X400_Address": "G=MG1;S=MGATE;CN=MG1 MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE",
    "User_ID": "49603"
  },
  "Message_Id": "0001-01-03-2018",
  "Date": "01 Mar 2018 09:11:30 +0100",
  "Subject": "testout",
  "Mime_Version": "1.0",
  "Content_Type": {
    "Mime_Type": "multipart/mixed"
  },
  "Multipart": [
    {
      "Content_Type": {
        "Mime_Type": "text/plain"
      },
      "Content_Transfer_Encoding": "8bit",
      "Data": "Test mit BASE64 encoded file attachment"
    },
    {
      "Content_Type": {
        "Mime_Type": "application/octet-stream"
      },
      "Content_Transfer_Encoding": "base64",
      "Content_Disposition": {
        "Disposition_Type": "attachment",
        "Filename": "webdav.p12"
      },
      "Data": "AQcBMwGCiqSlb3DQEMAYwDgQlzn9gMIQvocscAggAgIIEILQGaNZr0IW6bN6jEdpt
hjnBzmCv8W9ipvE8wmpVxzUEWj5Mh226vHaBp2WtMBaHPSomsXFMPEJJj9JFnF2SgPxDZVjUe5ImUB2EQDA
opQEYLxJSX0YXh8uqnSD5Se4vuex+kunnb6o2nGXT8+Y9m3/uNCD9MEb6CGIA0JExtmWQJXkDeHDZJlYiVC
pclt-
NeMNc7EGH842jRGzS1umfOeSWb8+TcA2/uZtzaE9uIL7lFd7dfJzfo984pFKR8vOxKIADbOn1CpuSQFHHDgCZ
YVy1EHODllmQbml+bJ2GwxUPKdDUGdyK6G45JHZjuj4zDUSRXwfnrRmSHZhUpRQwAPYyQo6zxhdd7NsdXPu
7mDisNE/p6p0DNPTf97/AiPWVMEWz0nsflTqF+4L0NXVKia7Mp8o7Zzrn5XpwJ0/LP+47/+ZyCaClqB/qYtGlbxlgI0
4DFbS6xaoUu7iNh7ZSqnXNMRJREtBx/WVoMChpYHuvVqitPWdsBpawNpUHS5uEXUopa0UlyXOn9ALfLE0t9v5
FP4NE3xSHMGAc5iisH7Fys8g5Z+SGp3n9ynM8Jw97JhZfjKoQMqrFzNL5FIZUBVwNYOtUNXxKJ3L+1WtRXSE
QgmfhptKZicCZKH0GZQ4Z8F4r9sA7wmS9CbLjiNQImWlrvaMWE3fi6dzhrUOFIdu2LE7TI7+1Qmh/AcP3NVIUSU
ZIGJqqGc5l1BUmp3CJPo25xJ7zAek/YECJmQ5p9"
```

```

    }
  ]
}

```

Ein Beispiel für das Hochladen einer Transmission Set Datei (T_) mit curl:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/ -X PUT -T T_181116_0001.in -H "Content-Type:application/json" --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

mit dem folgendem JSON Array Struktur, die zwei Interchanges enthält (das Segment Endezeichen Apostroph „“ wurde in diesem Beispiel „Escaped“, wobei der Web-Service auch ein Apostroph korrekt verarbeiten kann, und zur besseren Lesbarkeit wurden Zeilenumbrüche, Leerzeichen und Tabs entsprechend dem Profil v2 verwendet. Unabhängig von der Anzahl der Interchanges sollte immer ein Array verwendet werden):

```
[
  {
    "Interchange": "UNA:+.? \u0027
    UNB+UNOA:2+MGATE1:65+TESTER:65+020508:1413+0709210008\u0027
    UNH+EVA0000001+INVOIC:D:95A:UN:ETEIB++0\u0027
    ...
    UNT+37+EVA0000001\u0027
    UNZ+1+0709210008\u0027"
  },
  {
    "Interchange":"UNA:+.? \u0027
    UNB+UNOA:2+MGATE1:65+TESTER:65+020508:1413+0709210009\u0027
    UNH+EVA0000001+INVOIC:D:95A:UN:ETEIB++0\u0027
    ...
    UNT+37+EVA0000001\u0027
    UNZ+1+0709210009\u0027"
  }
]
```

Ein Beispiel für das Anfordern eines Status Reports (S_) mit curl:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/ -X PUT -T S_12002.in -H "Content-Type:application/json" --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

mit der folgenden JSON-Struktur (zur besseren Lesbarkeit wurden Zeilenumbrüche, Leerzeichen und Tabs entsprechend dem Profil v2 verwendet):

```
{
  "Since": "13-Nov-2018",
  "Format": "CSV-C",
  "Direction": "both"
}
```

Ein Beispiel für das Versenden einer Lesebestätigung (R_) mit curl:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/ -X PUT -T R_12002.in -H "Content-Type:application/json" --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

mit der folgenden JSON-Struktur (zur besseren Lesbarkeit wurden Zeilenumbrüche, Leerzeichen und Tabs entsprechend dem Profil v2 verwendet):

```
{
  "Status": "Processed"
}
```

Der abschließende Schrägstrich "/" bei der URL ist erforderlich.

GET - Dateiliste abrufen

Mit der Methode "GET" kann eine Liste der Dateien im Verzeichnis mit dazugehörigem Datum sowie die Dateigröße in Byte angefordert werden. Übergibt man beim GET nur die URL des MessageGate Verzeichnis, erhält man als Ergebnis ein JSON-Array, das die einzelnen Einträge der Liste als JSON-Struktur (Felder durch Komma getrennt) beinhaltet und dabei alle Dateien mit Erstellungsdatum (YYYY-MM-DD HH-MM-SS) und Größenangabe in Bytes berücksichtigt.

Hier ein Beispiel mit curl:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/ --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

ergibt z.B. die folgende JSON Array Struktur (zur besseren Lesbarkeit wurde das Profil v2 mit Zeilenumbrüchen, Leerzeichen und Tabs gewählt):

```
[
  {
    "Filename": "m_1610.in_err0007",
    "Datetime": "2016-10-31 15:02:22",
    "Filesize": "6756"
  },
  {
    "Filename": "s_161024.out",
    "Datetime": "2016-10-31 15:16:17",
    "Filesize": "7138"
  },
  {
    "Filename": "m_d45f427672e345.out",
    "Datetime": "2016-10-31 15:16:59",
    "Filesize": "204217"
  }
]
```

In der Liste werden Unterverzeichnisse nicht berücksichtigt. Der Umfang der bereitgestellten Liste kann explizit durch Ergänzung der URL um ein entsprechendes Selektionskriterium (z.B. *.out oder *.in, sofern diese nicht schon vom Poller des MessageGate Prozess verarbeitet wurden) reduziert werden:

Hier ein Beispiel mit curl:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/*.in --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Wildcards („*“) können auch benutzt werden, um die Liste auf einen bestimmten Typ von Datei (z.B. „m_*.out“ oder „*.in_err*“) einzuschränken.

GET - Download einer Datei

Mit "GET" kann auch gezielt eine bestimmte Datei durch Ergänzung der URL um den entsprechenden Dateinamen heruntergeladen werden. Beim Übertragen von EDIFACT Dokumenten im Mitteilungstext oder in einer Transmission Set Datei wird das Segment Endzeichen Apostroph „“ durch „\u0027“ ersetzt, da dieses Zeichen nicht von allen Parsern verarbeitet werden kann.

Hier ein Beispiel mit curl, bei dem eine ungesicherte Message Datei mit einem Body Part abgeholt und der Content Type application/json verwendet wird:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/m_53786626568.out --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

ergibt z.B. die folgende JSON-Struktur (zur besseren Lesbarkeit wurde das Profil v2 mit Zeilenumbrüchen, Leerzeichen und Tabs gewählt, bitte beachten das abweichend vom Profil v1 statt „X-Mpduid“ die Feldbezeichnung „Mts-Id“ entsprechend dem Statusreport verwendet wird):

```
{
  "To": [
    {
      "X400_Address": "G=MG1;S=MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE",
      "User_ID": "49603"
    }
  ],
  "From": {
    "X400_Address": "G=ipm;S=tester;O=testag;A=viat;C=de",
    "User_Id": "49637"
  },
  "Message_Id": "124 01-03-2018",
  "Mts-Id": "16067AF811E8E7211E0018B9",
  "Date": "01 Mar 2018 12:10:59 +0100",
  "Subject": "test001",
  "Mime_Version": "1.0",
  "Content_Type": {
    "Mime_Type": "text/plain"
  },
  "Content_Transfer-Encoding": "8bit",
  "Data": "test ohne Dateianhang"
}
```

Hier ein Beispiel mit curl, bei dem eine verschlüsselte und signierte Message Datei abgeholt und der Content Type application/json verwendet wird:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/m_d7ae2u7s1oh0t3ch.out --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

ergibt z.B. die folgende JSON-Struktur (zur besseren Lesbarkeit wurde das Profil v2 mit Zeilenumbrüchen, Leerzeichen und Tabs gewählt, bitte beachten das abweichend vom Profil v1 statt „X-Mpduid“ die Feldbezeichnung „Mts-Id“ entsprechend dem Statusreport verwendet wird):

```
{
  "To": [
    {
      "X400_Address": "G=MG1;S=MGATE; O=TESTAG;P=MGATE;A=VIAT;C=DE",
      "User_ID": "49603"
    }
  ],
  "From": {
    "X400_Address": "G=ipm;S=tester;O=testag;A=viaT;C=de",
    "User_Id": "49637"
  },
  "Message_Id": "8552 19/03/12",
  "Mts-Id": "0172375E11E944A185D454AE",
  "Date": "12 Mar 2019 08:29:51 +0100",
  "Subject": "test Web-Service mit verschlüsselter Mitteilung",
  "Mime_Version": "1.0",
  "Content_Type": {
    "Mime_Type": "application/pkcs7-mime ",
    "Smime_Type": "enveloped-data",
  }
}
```

```

    "Name": "smime.p7m"
  },
  "Content_Transfer-Encoding": "base64",
  "Content-Disposition": {
    "Disposition_Type": "attachment",
    "Filename": "smime.p7m"
  },
  "Data": "MIAGCSqGSIb3DQEHA6CAMIACAQAxggKSMI...AAAAAANCg"
}

```

Hier ein Beispiel mit curl, bei dem eine signierte Message Datei mit zwei Textanhängen und einem binären Anhang abgeholt und der Content Type application/json verwendet wird:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/m_438233gh1qh0t3pk.out --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

ergibt z.B. die folgende JSON-Struktur (zur besseren Lesbarkeit wurde das Profil v2 mit Zeilenumbrüchen, Leerzeichen und Tabs gewählt, bitte beachten das abweichend vom Profil v1 statt „X-Mpduid“ die Feldbezeichnung „Mts-Id“ entsprechend dem Statusreport verwendet wird):

```

{
  "To": [
    {
      "X400_Address": "G=MG1;S=MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE",
      "User_Id": "49603"
    }
  ],
  "From": {
    "X400_Address": "G=ipm;S=tester;O=testag;A=viaT;C=de",
    "User_Id": "49637"
  },
  "Message_Id": "8553 19/03/25",
  "Mts_Id": "F38BA8C211E94EF185D4DABC",
  "Date": "25 Mar 2019 11:34:29 +0100",
  "Subject": "test Web-Service mit signierter Mitteilung",
  "Disposition_Notification_To": "\"G=ipm;S=tester;O=dtag;A=viaT;C=de\"",
  "Mime_Version": "1.0",
  "Content_Type": {
    "Mime_Type": "multipart/signed",
    "Protocol": "application/pkcs7-signature",
    "Micalg": "sha256"
  },
  "Multipart": [
    {
      "Content_Type": {
        "Mime_Type": "multipart/mixed"
      },
      "Multipart": [
        {
          "Content_Type": {
            "Mime_Type": "text/plain",
            "Charset": "ISO-8859-1"
          },
          "Content_Transfer-Encoding": "quoted-printable",
          "Data": "test"
        }
      ]
    }
  ]
}

```

```

    },
    {
      "Content_Type": {
        "Mime_Type": "text/plain",
        "Charset": "ISO-8859-1"
      },
      "Content_Transfer-Encoding": "quoted-printable",
      "Data": "\r\nC:\\Users\\tester\\Documents>C:\\OpenS....."
    },
    {
      "Content_Type": {
        "Mime_Type": "application/octet-stream"
      },
      "Content_Transfer-Encoding": "base64",
      "Content_Disposition": {
        "Disposition_Type": "attachment",
        "Filename": "Modem_cfos.txt",
        "Modification_Date": "Wed, 02 Sep 2015 09:04:32 +0100"
      },
      "Data": "DQoJICAgICAgeysrfSBkZW5vdGV....."
    },
  ],
},
{
  "Content_Type": {
    "Mime_Type": "application/pkcs7-signature",
    "Name": "smime.p7s"
  },
  "Content_Transfer-Encoding": "base64",
  "Content_Disposition": {
    "Disposition_Type": "attachment",
    "Filename": "smime.p7s"
  },
  "Data": "MIIJ5gYJKoZIhvcNAQcColIJ1zCCCdMCAQExDTALBglg.....CX"
}
]
}

```

Hier ein Beispiel mit curl, bei dem eine Transmission Set Datei abgeholt und der Content Type application/json verwendet wird:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/T_657832112362.out --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

ergibt z.B. die folgende JSON-Array-Struktur (das Segment Ende Zeichen Apostroph wird „Escaped“ und zur besseren Lesbarkeit wurde das Profil v2 mit Zeilenumbrüchen, Leerzeichen und Tabs gewählt, unabhängig von der Anzahl der Interchanges wird ein Array verwendet):

```
[
  {
    "Interchange": "UNA:+.? \u0027
    UNB+UNOA:2+TESTER:65+ MGATE1:65+020508:1413+0709210009\u0027
    UNH+EVA0000001+INVOIC:D:95A:UN:ETEIB++0\u0027
    ...
    UNT+37+EVA0000001\u0027
    UNZ+1+0709210009\u0027"
  }
]
```

```

    }
]

```

Hier ein Beispiel mit curl, bei dem ein Status Report mit einer empfangenen und einer versendeten Mitteilung abgeholt und der Content Type application/json verwendet wird:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/R_10023.out --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

ergibt z.B. die folgende JSON-Struktur (zur besseren Lesbarkeit wurde das Profil v2 mit Zeilenumbrüchen, Leerzeichen und Tabs gewählt, außerdem werden abweichend vom Profil v1, wie bei der Message Struktur, bei den Adressen die Feldbezeichner „X400_Address“ und „User_Id“ verwendet. Falls letzte nicht bekannt, wird "" zurückgeliefert.):

```

{
  "Type": "Status Report",
  "User_Id": "49603",
  "Date": "2019/02/15 08:33:29",
  "Timezone": "GMT",
  "Filter": {
    "Disposition": "All",
    "Direction": "Both",
    "Format": "CSV-C",
    "Since": "15-Feb-2019"
    "Message-Id": "",
    "Order-Id": ""
  },
  "Report": [
    {
      "From": {
        "X400_Address": "G=ipm;S=tester;O=testag;A=viat;C=de",
        "User-ID": "49637"
      },
      "To": {},
      "Order_Id": "657832112376",
      "Message_Id": "126 13-11-2018",
      "Mts_Id": "16067AF777E8E7211E0018B9",
      "Received": "13.11.2018 12:34",
      "Sent": "",
      "Delivered": "",
      "Read": "",
      "Reason": "",
      "Diagnostic": "",
      "Errordate": "",
      "Rcpt_Type": "To"
    },
    {
      "From": {}
      "To": {
        "X400_Address": "G=ipm;S=tester;O=testag;A=viat;C=de",
        "User_Id": "49637"
      },
      "Order_Id": "131118-0001",
      "Message_Id": "131118-0001",
      "Mts_Id": "19127AF777E8E7211E002312",
      "Received": ""
    }
  ]
}

```

```

    "Sent": "13.11.2018 12:36",
    "Delivered": "13.11.2018 12:36",
    "Read": "13.11.2018 12:38",
    "Reason": "",
    "Diagnostic": "",
    "Errordate": "",
    "Rcpt_Type": "To"
  }
]
}

```

Die Dateiendung „.out“ ist bei Downloads optional und wird bei Fehlen implizit verwendet. Der vom Web-Service zurückgelieferte Content-Type ist per Default "application/json".

Folgende HTTP Response Codes sind möglich:

200 OK (Anfrage erfolgreich bearbeitet, Datei wird heruntergeladen.)

404 Not found (Die Datei existiert nicht.)

406 Not Acceptable (Der Dateityp passt nicht zum Wert bei "Accept" oder zum Content Type "application/json")

423 Locked (Die angeforderte Datei wird gerade anderweitig bearbeitet)

DELETE - Eine Datei löschen

Mit "DELETE" wird eine bestimmte Datei aus dem Verzeichnis gelöscht.

Hier ein Beispiel mit curl:

```
curl https://webdav.viat.de/mgate/v2/~0000049640/s_161031.out -X DELETE --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Die Dateiendung „.out“ ist beim Löschen optional und wird implizit ergänzt, sofern eine Datei mit diesem Namen existiert. Im Erfolgsfall wird der Status "HTTP 204 No content" zurückgeliefert. Dies gilt auch dann, wenn die Datei vorher schon nicht mehr existiert hat. Dieser Status bedeutet somit, dass eine Datei mit diesem Namen nach erfolgreicher Anfrage nicht mehr vorhanden ist.

Ist die angegebene Datei noch in Bearbeitung oder anderweitig gesperrt, wird der Status "HTTP 423 Locked" mit der erweiterten Information "File currently locked" zurückgeliefert.

Die Verwendung von Wildcards/Platzhalter im Dateinamen ist nicht erlaubt. Bei solch einem Request wird der Status "HTTP 500 Internal Server Error" zurückgeliefert.

5.3.3 Das Web-Service Profil v3 (v3a)

Dieses Profil entspricht weitestgehend dem Profil v2/v2a (JSON-Struktur, bei v3 werden die beim Download bereitgestellten Daten mit CR/LF, Leerzeichen und Tabs zur besseren Lesbarkeit versehen, bei v3a ohne Zusatzzeichen). Es ist vor allem für den Einsatz bei aktivierter Closed User Group und nur in Verbindung mit dem TEDIS P2 Ansatz bei EDI-Dokumenten (1 Empfänger und ein EDIFACT Dokument versendet als ein Text oder als ein binärer Body Part) vorgesehen. Deshalb sind alle im Kapitel 5.3.2 Das Web-Service Profil v2 (v2a) beschriebenen Befehle auch mit v3 möglich und weitestgehend sind die Ergebnisse auch gleich.

Unterschiede gibt es bei der (minimalisierten) Struktur zum Erzeugen der Mitteilungsdatei (eine Empfänger User-ID, Mitteilungsnummer, Betreff, einen Text oder binären Body Part), die mittels PUT in das MessageGate Verzeichnis hochgeladen wird. Auch der Download, mittels GET abgeholt, erfolgt dann in der minimalisierten

Struktur, wobei hier die Absender User-ID und zusätzlich die Order-ID angezeigt wird. Dies ist deshalb notwendig, da beim Befehl GET für das Abholen von Mitteilungsdateien nun die Option NEXTFILE angeboten wird. Bei dieser Option muss man nicht zuerst den Inhalt des Verzeichnisses auflisten, um den Dateinamen der Mitteilungsdatei für das explizite Abholen zu erhalten. Bei einem GET mit NEXTFILE wird automatisch die älteste im Verzeichnis ausgelieferte Mitteilungsdatei zurückgeliefert. Damit diese nicht immer wieder angeboten wird, verschiebt der Web-Service diese nach dem Abholen in den Unterordner „ARCHIVE“. Dort verbleibt sie so lange, bis der Purger Prozess (entsprechend dem konfigurierten Zeitraum für das Entfernen von älteren Dateien) diese löscht, und kann somit bei Bedarf nochmals abgeholt werden (dann aber zunächst mit GET zum Auflisten des Verzeichnisses und nachfolgend explizites Abholen über GET und Dateinamen). In Verbindung mit der Closed User Group kann man die Option NEXTFILE sogar absenderspezifisch (Absender User-ID in URL ergänzen und älteste von diesem Absender verfügbare Mitteilung anbieten) verwenden und die archivierten Mitteilungen werden in einen absenderspezifischen (User-ID) Unterordner von „ARCHIVE“ verschoben.

PUT - Upload einer Mitteilungsdatei

Mit der Methode "PUT" wird eine neue Mitteilungsdatei im MessageGate Verzeichnis angelegt. PUT erwartet dabei die Datei als Content, wobei der (eindeutige) Dateiname mit einem "M" gefolgt von einem Unterstrich "_" beginnen muss. Die Dateierweiterung muss explizit auf ".in" enden oder wenn diese fehlt, wird dann implizit ein ".in" ergänzt. Groß-/Kleinschreibung spielt beim Dateinamen keine Rolle. Sind diese Bedingungen nicht erfüllt, wird der Status "HTTP 404 Not found" mit der erweiterten Information „Invalid filename format“ zurückgeliefert.

Wird das http Header-Feld "Content-Type" beim PUT mitgeliefert, sollte der Wert "application/json" lauten. Bei ungültigem Content Type wird der Status "HTTP 406 – Not Acceptable" mit der erweiterten Information „Illegal combination of filename and Content-Type" zurückgeliefert.

Ist beim Upload die übertragende Datei noch nicht vorhanden, wird sie neu angelegt und der Status "HTTP 201 Created" zurückgeliefert. Das Header-Feld "Location" enthält als Wert dann die neue URL. Ist beim Upload eine Datei mit dem definierten Namen bereits vorhanden, wird die Übertragung abgelehnt und der Status "HTTP 423- Locked" mit der erweiterten Information „File currently locked" zurückgeliefert. Beim Upload können nur "ganze" Dateien übertragen werden. Die Verwendung des Header-Feldes "Content-Range" ist somit unzulässig und wird mit dem Status "HTTP 400 Bad request" mit der erweiterten Information „Content-Range not allowed" quittiert.

Abweichend vom Profil v2/v2a ist ja nur ein minimaler Header (Empfänger User-ID, Mitteilungsnummer, Betreff) vorgesehen und es wird auch nur ein Body Part (entweder Text als ISO-Latin 1 oder Binär als Body Part 14 ohne Dateinamen) unterstützt.

Ein Beispiel für das Hochladen eine Message Datei (M_), mit einem Text Body Part mit curl (Beispiel mit Binär bei GET):

```
curl https://webdav.viat.de/mgate/v3/~0000049640/ -X PUT -T M_211020_001.in -H "Content-Type:application/json" --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

mit der folgenden JSON-Struktur (mit Zeilenumbrüchen, Leerzeichen und Tabs entsprechend dem Profil v3):

```
{
  "User_Id": "49637",
  "Message_Id": "0001-01-11-2021",
  "Subject": "testin",
```

```
"TEXT": "Test mit BASE64 encoded file attachment"
}
```

GET - Download einer Mitteilungsdatei

Mit "GET" kann gezielt eine bestimmte Datei durch Ergänzung der URL um den entsprechenden Dateinamen heruntergeladen werden.

Hier ein Beispiel mit curl, bei dem eine ungesicherte Message Datei mit einem binären Body Part (Text von Beispiel PUT in BASE64 codiert) abgeholt und der Content Type application/json verwendet wird:

```
curl https://webdav.viat.de/mgate/v3/~0000049640/m_53786626568.out --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

ergibt z.B. die folgende JSON-Struktur (zur besseren Lesbarkeit wurde das Profil v3 mit Zeilenumbrüchen, Leerzeichen und Tabs gewählt):

```
{
  "Order_Id": "53786626568",
  "User_Id": "49637",
  "Message_Id": "0002-01-11-2021",
  "Subject": "testout",
  "DATA": " VGVzdCBtaXQgQkFTRTY0IGVuY29kZWQgZmlsZSBhdHRhY2htZW50"
}
```

Verwendet man statt einem Dateinamen die Option NEXTFILE, so bietet der Web-Service die älteste Mitteilung im MessageGate Verzeichnis als (minimalisierte) JSON-Struktur im http Result an. Hier ein Beispiel:

```
curl https://webdav.viat.de/mgate/v3/~0000049640/NEXTFILE --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Die entsprechende Mitteilungsdatei wird nun in den Unterordner „Archive“ verschoben und könnte somit bei Bedarf nochmals abgerufen werden. Hier ein Beispiel:

```
curl https://webdav.viat.de/mgate/v3/~0000049640/archive/m_53786626569.out --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Beim erstmaligen Verschieben einer Mitteilungsdatei wird dann der Unterordner „ARCHIVE“ automatisch angelegt.

Ist für den MessageGate Account die Closed User Group aktiviert, wird der Name einer ausgelieferten Mitteilungsdatei um die User-ID des Absenders erweitert und dann ist es möglich, in Verbindung mit NEXTFILE die älteste Mitteilung aus dem Verzeichnis abzuholen, die von diesem Absender stammt. Hier ein Beispiel:

```
curl https://webdav.viat.de/mgate/v3/~0000049640/NEXTFILE/042788/ --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Die entsprechende Mitteilungsdatei wird hierbei nicht nur in den bereits beschriebenen Unterordner „ARCHIVE“ verschoben, sondern dort in einen Unterorder mit der entsprechenden Absender User-ID und könnte somit bei Bedarf nochmals abgerufen werden. Hier ein Beispiel:

```
curl https://webdav.viat.de/mgate/v3/~0000049640/archive/042788/m_53786626579_042788.out --cacert ca-bundle.crt --cert tester_cert.pem --key tester_key.pem -v
```

Beim erstmaligen Verschieben einer Mitteilungsdatei wird automatisch der Unterordner mit der entsprechenden Absender User-ID angelegt.

Sollte das v3/v3a Profil ohne Closed User Group verwendet werden, ist es möglich, dass eine von einem Partner gesendete Mitteilung mit mehreren Anhängen ausgeliefert wird. Beim Abholen wird der Multi Part aus der Message Datei 1:1 in die JSON-Datei durchgereicht.

Hier ein Beispiel:

```
{
  "Order_Id": "051B3MQV3UH0W39N",
  "User_Id": "49637",
  "Message_Id": "238 22/03/09",
  "Subject": "test 2xFTAM",
  "Multipart": "--MG_=_D8563E2211EC9FB6DC9C1895_=_MG\r\nContent-Type: application/octet-stream\r\nContent-Disposition: attachment; filename=\"test.zip\"\r\nContent-Transfer-Encoding: base64\r\n\r\nUESDBBQAAAA ... IFydHMNCiAgKD4xTUlpIGZhaWxpbmcuDQo=\r\n--MG_=_D8563E2211EC9FB6DC9C1895_=_MG--\r\n"
}
```

Der Upload einer Mitteilung mit Multi Part wird nicht unterstützt.

5.4 Getestete REST-Kommunikationsmodule

Für die Tests des Web-Service Zugangs wurden die Module:

- curl (siehe <https://curl.haxx.se/download.html>), zum Aufruf auf Kommandozeilenebene und verfügbar für die verschiedensten Betriebssysteme (Windows 32 und 64 Bit, Linux, Unix, Mac OS X, OpenVMS usw.).
- Postman, früher ein Addon für den Webbrowser Google Chrome für Windows, inzwischen eine eigenständige App für Windows, MacOS und Linux (siehe <https://www.postman.com/downloads/>)

verwendet.

Seite ist aus redaktionellen Gründen leer.

6 AS2 und MessageGate

6.1 Allgemein

Die Benutzer des AS2 Gateway kommunizieren nur indirekt mit dem MessageGate Prozess, da die eigentliche AS2 Kommunikation durch ein separates Modul mit dem Namen ComAS2 (wird von der Firma Compinia GmbH & Co. KG als Java Kommunikationsmodul auch für andere Plattformen, wie Windows oder Linux angeboten) erfolgt. Der MessageGate Prozess (MGAS2X) übernimmt die Aufträge von ComAS2 und versendet diese dann als X.400 Mitteilungen. Falls im Partnerschaftsprofil die End-to-End Security nicht aktiviert (Standardeinstellung) ist, extrahiert ComAS2 die Nutzdaten aus den eventuell signierten und /oder verschlüsselten AS2 Mitteilungen, so dass der X.400 Partner diese direkt verarbeiten kann. Bei aktiviertem Leistungsmerkmal reicht ComAS2 die gesicherten Daten als S/MIME-Content in einem Body Part 15/ FTAM Body Part (siehe auch Kapitel 2.3.4 S/MIME gesicherter Inhalt) zum X.400 Partner durch, so dass dieser dann die Extraktion der Nutzdaten übernehmen muss. In der AS2 Lösung des Kunden muss dann zum Verschlüsseln und zum Prüfen der Signatur ein Zertifikat verwendet werden, das der X.400 Partner zur Verfügung gestellt hat und nicht das des AS2 Service von BusinessMail X.400. Vor dem Aktivieren dieses Leistungsmerkmals muss abgeklärt werden, in welcher Form der X.400 Partner die Daten erwartet. Die P7 Clients FileWork und UA-FI ab der V5.2 erwarten z.B., dass in der Signatur das Zertifikat des Signierenden enthalten ist, damit die Nutzdaten direkt bereitgestellt werden können.

X.400 Mitteilungen für einen AS2 Benutzer werden vom MessageGate Prozess direkt an ComAS2 übergeben. ComAS2 übermittelt die Dokumente dann mittels AS2 Protokoll an die konfigurierte IP- Adresse (URL) der Kundenapplikation und ergänzt abhängig von der Einstellung des Parameters „End-to-End Security“ und anderen partnerschaftsspezifischen Parameter die Signatur bzw. verschlüsselt die AS2 Mitteilung. MessageGate übernimmt bei dieser Transaktion auch das Umsetzen zwischen den verschiedenen Reports. Die Umsetzung der AS2 MDN in einen X.400 Report beim Mitteilungsverkehr zwischen X.400 und AS2 Benutzer ist abhängig vom eingestellten Gateway- Modus.

Gateway-Modus „Agent“ oder „Transfer“

Ist der Gateway-Modus „Agent“ eingestellt (Default), so erzeugt der MessageGate Prozess schon beim Ausliefern der Mitteilung an ComAS2 eine X.400 DN (Delivery Notification → Auslieferbestätigung), falls der X.400 Benutzer diese angefordert hat. Die vom AS2 Benutzer zurückgesendete MDN wird nur dann in eine RN (Receipt Notification – Lesebestätigung → Status in Report ist „Read“) umgesetzt, wenn diese vom X.400 Benutzer angefordert und der Versand vom AS2 Benutzer erlaubt wurde. Im „Agent“ Modus kann der AS2 Benutzer auf die besonderen Leistungsmerkmale des Gateways wie Nachrichtenverwaltung und automatischen Statusreport zurückgreifen.

Der Gateway-Modus „Transfer“ sollte dann benutzt werden, wenn der AS2 Partner kein Kunde des *BusinessMail X.400 Service* ist und deshalb auch nicht das Recht hat, *WebConfig* und die anderen Funktionen des AS2 Gateway zu nutzen. In diesem Fall beauftragt der X.400 Benutzer die Anbindung seines Partners, der nur über AS2 kommunizieren kann. Für den X.400 Benutzer ist es wichtig, dass erst dann eine X.400 Delivery Notification (Auslieferbestätigung → Status in Report ist „Delivered“)

versendet wird, wenn der AS2 Partner den Empfang der Mitteilung mit einer MDN quittiert hat. Die Anforderung einer RN wird in diesem Modus ignoriert und auch die Nachrichtenverwaltung ist für den X.400 Benutzer nur eingeschränkt verfügbar. Es greifen hier die vom X.400/F.400 Standard vorgegebenen Timeout Werte und nach Erreichen des Timeouts wird einen NDN mit entsprechendem Fehlercode erzeugt.

Sowohl ComAS2 als auch der MessageGate Prozess unterstützen Dokumente mit MIME-Content „Multipart Mixed“.

Für einen AS2 Benutzer erscheint sein X.400 Partner immer als AS2 Benutzer und für einen X.400 Benutzer sein AS2 Partner als X.400 Benutzer ohne Einschränkung beim jeweiligen Übertragungsprotokoll.

Da EDIINT AS2 (RFC4130) als ein Peer-to-Peer Protokoll definiert ist, muss ein AS2 Benutzer jeden seiner Partner über eine AS2-ID adressieren, die er seinem Partner auch mitteilen muss. Dies gilt auch, wenn der AS2 Benutzer mit einem X.400 Partner kommunizieren will. Diese dem X.400 Partner zugeordnete AS2-ID wird vom AS2 Gateway anhand von Partnerschaftsprofilen in eine X.400 Adresse umgesetzt, welche dann in der X.400 Mitteilung entsprechend verwendet wird.

Es gibt aber hier auch eine Ausnahme. AS2 Benutzer können, wie Benutzer der Dateischnittstelle von MessageGate, die zentrale EDI-Funktion benutzen, um EDIFACT Dokumente an Partner zu senden bzw. von diesen EDIFACT Dokumente zu empfangen. Dazu muss der AS2 Benutzer die zentrale EDI-Funktion als Trading Partner (AS2 Partnerschaft) in seiner Anwendung einrichten und dieser eine AS2-ID zuordnen.

AS2-X.400 Partnerschaft :: Neue Partnerschaft erstellen

Zentrale EDI-Funktion verwenden

AS2 Einstellungen

IDs

AS2-ID: AS2-Partner AS2Tester001

AS2-ID: X.400-Partner 

AS2-ID mit Benutzer-ID des X.400-Partners ergänzen

End-to-End Security aktivieren 

Eigenschaften: X.400 → AS2

default-URL

Altern. URL

Komprimieren

Signieren

Verschlüsseln

MDN anfordern

MDN signieren

MDN Transfer

X.400 Einstellungen

Er kann also über eine AS2-ID mit verschiedenen X.400 Partnern kommunizieren, da die zentrale EDI-Funktion dann über diese AS2-ID nicht nur Dokumente zum Versenden an die Partner entgegennimmt, sondern auch Dokumente von diesen Partnern an den AS2 Benutzer ausliefert. Dies ist vor allem dann interessant, wenn der AS2 Benutzer eine Lösung einsetzt, die nach Anzahl der AS2 Partnerschaften lizenziert ist. Die End-to-End Security wird jedoch bei der zentralen EDI-Funktion nicht unterstützt, da dort der TEDIS P2 Ansatz (eine Mitteilung an einen Empfänger mit einem EDIFACT Interchange als Text oder Binäranhang) verwendet wird.

Bitte beachten Sie auch eine Besonderheit der zentralen EDI-Funktion beim AS2 Gateway im Vergleich zu der bei MessageGate oder bei EDIBOX (spezielle Mailbox). Es können zwar auch innerhalb eines Transmissionssets mehrere Interchange übergeben werden, jedoch kann dann das Gateway die MDN nicht auf Basis einer DN oder RN erzeugen, da ja eine individuelle Zuordnung nicht mehr möglich ist. In diesem Fall erzeugt das AS2 Gateway die MDN, sobald alle Interchange verarbeitet wurden (z.B. X.400 Mitteilungen versendet oder Versand abgelehnt wurde). Um eine korrekte Umsetzung des Reports zu erhalten, sollten Sie also immer nur ein Interchange pro AS2 Mitteilung übergeben.

Mit Einführung von MessageGate als Hostprozess werden nun im AS2 MIME Header bei TO: und FROM: auch die X.400 Adressen übertragen. Diese Felder sind für die AS2 Kommunikation nicht relevant, da hier AS2-TO: und AS2-FROM: ausgewertet werden. Aber vor allem in Verbindung mit der zentralen EDI-Funktion könnte der AS2 Nutzer hiermit überprüfen, wer der X.400 Absender des EDIFACT Dokumentes war.

6.2 Unterschiede zwischen File Interface und AS2 Nutzern

Die nachfolgenden Seiten beschreiben den AS2 Account im „Agent“- Modus, bei dem der AS2 Benutzer Zugriff auf *WebConfig* hat. Viele Punkte gelten auch für den „Transfer“- Modus, jedoch fehlen dort die Menüpunkte EDI Partnerschaft, Nachrichtenverwaltung und automatischer Statusreport bzw. der Zugriff ist eingeschränkt. Üblicherweise ist im „Transfer“ Modus auch nur eine Partnerschaft eingerichtet, und zwar die zwischen dem X.400 Benutzer, der Kunde bei *BusinessMail X.400* ist, und seinem Partner, dessen Anwendung nur das AS2 Protokoll unterstützt und der kein Kunde ist.

Für die Zuordnung von MDN in X.400 Reports und umgekehrt verwendet MessageGate dieselbe Datenbankrelation (Trace_Tab), in der auch die Nutzer des MessageGate File Interface Informationen über den Status der Mitteilungen abfragen können. Auch AS2 Benutzer können mittels *WebConfig* Status Reports abfragen/-holen oder aber sich automatisch Status Reports von einer vorher definierten AS2-ID zusenden lassen (Details zu den Einträgen siehe am Ende des Kapitels).

MessageGate löscht deshalb auch nicht die Einträge für eine Transaktion, sobald diese abgeschlossen ist (X.400 Lesebestätigung wurde auf Basis einer MDN erzeugt bzw. MDN wurde auf Basis eines vorkonfigurierten X.400 Reports erzeugt). Stattdessen verbleiben die Einträge so lange in der Datenbank, bis sie vom sogenannten Purger gelöscht werden. Der Purger, der mehrmals pro Tag die Datenbank überprüft, verifiziert dabei, ob die unter dem Parameter Purge Time definierte Lebensdauer der Einträge (Default ist 240 Stunden, kann kundenindividuell angepasst werden) überschritten ist. Ist dies der Fall, löscht der Purger den Eintrag.

Das Löschen dieses Eintrages bedeutet aber, dass Transaktionen, die noch nicht abgeschlossen werden konnten (z.B., wenn RN noch nicht vom Empfänger zurück-gesendet wurde), auf fehlerhaft gesetzt werden.

Grundeinstellung AS2 Kommunikation

Für den AS2 Account können in *WebConfig* unter dem Menüpunkt „Grundeinstellungen“ folgende Optionen definiert werden.

- Zuordnung der AS2-ID
- bis zu drei Zertifikat Alias für Signatur, Verschlüsselung und TLS (beinhalten jeweils ein bzw. zwei Kundenzertifikate, die in WebConfig im Menü X.509 Zertifikate oder mittels spezieller AS2 Mitteilungen entsprechend dem Certificate Exchange Management CEM verwaltet werden können)
- URL der AS2 Kundenlösung
- Default Einstellung beim Einrichten von neuen AS2 Partnerschaften für das Versenden von X.400 Mitteilungen an AS2 (Daten komprimieren, verschlüsseln mittels 3DES oder AES256-CBC, signieren mittels SHA, SHA2 oder SHA3, ob und in welcher Form MDN anfordern)
- Einstellungen zum Verhalten des AS2 Gateway bei Übertragungsproblemen

BusinessMail X.400 :: [WebKonfiguration](#)
as2tester (49639)
AS2-ID: AS2Tester001

AS2-X.400 Partnerschaft :: Grundeinstellungen

Benutzer

X.400-Adresse cn=as2 tester, g=as2; s=tester; o=testag; n-id=2049639; a=VIAT-AS2; c=DE

Einstellungen des AS2-Benutzers

MTA-Modus	Agent <input type="text"/>
AS2-ID	AS2Tester001 <input type="text"/>
URL	http://as2.testag.de:4080/ <input type="text"/>
Alias Signatur	AS2TESTPC1
Alias Verschlüsselung	AS2TESTPC1_ENC
Alias TLS	AS2TESTPC1_TLS
Email Adresse	as2@testag.de <input type="text"/>
Inaktiv	<input checked="" type="checkbox"/>
AS2-Bypass aktivieren	<input checked="" type="checkbox"/>
Duplikate-Check	<input checked="" type="checkbox"/>
End-to-End Security aktivieren	<input type="checkbox"/>
Purge-Zeit	240 Stunden
Sende Timeout	<input type="text" value="1440"/> Minuten (0-65535, 0=Sendeversuch unbegrenzt)
Sende Timeout MDN	<input type="text" value="1440"/> Minuten (0-65535, 0=Sendeversuch unbegrenzt)
Empfangstimeout MDN	<input type="text" value="0"/> Minuten (0-65535, 0=keine Wiederholung)
Max. Wiederholungsversuche	<input type="text" value="0"/> (0-127, 0=keine Wiederholung)

Default-Eigenschaften: X.400 → AS2

Sende Timeout AS2 Mitteilung

Über den ersten Timeout-Parameter kann man konfigurieren, dass Dokumente nach einer festgelegten Zeit als fehlgeschlagen in der Nachrichtenverwaltung angezeigt werden, falls die Mitteilungen nicht an die AS2 Lösung des Kunden ausgeliefert werden konnten oder direkt dorthin umgeleitet wurden. Auf die Nachrichtenverwaltung kann der Kunde mittels *WebConfig* zugreifen, um die Nutzdaten manuell abzuholen oder die Transaktion zu löschen bzw. neu anzustoßen.

Nachrichtenverwaltung

AS2-X.400 Partnerschaft :: Nachrichtenverwaltung ⓘ

Datensätze seit (Format: DD-MMM-YYYY hh:mm:ss)

Datensätze bis (Format: DD-MMM-YYYY hh:mm:ss)

Filter: ⓘ

Zeit	Nachricht	Status	Download	Aktionen
13.07.2022 10:54:10	04224KMTRRI0W7DI	bypassed	📄	nochmal senden löschen
13.07.2022 10:54:22	14224KMTRRI0W7DI	bypassed	📄	nochmal senden löschen
13.07.2022 13:11:05	24224KMTRRI0W7DL	bypassed	📄	RN senden nochmal senden löschen

```

From: "G=ipm;S=tester;O=testag;A=viat-test;C=de" 49637@viaT.de
Order-ID: 24224KMTRRI0W7DL
Message-ID: 83 22/07/13
MTS-ID: 405B062611ED02ADDC9C87A5
Content-Type: text/plain
Encoding: 8bit
Received: 13-Jul-2022 13:11:05 +0200
AS2-ID: BM400_49637
AS2-Status: bypassed
  
```

Die Einträge in der Nachrichtenverwaltung stehen aber auch nur dann zur Verfügung, solange der Transaktionseintrag in der Datenbank existiert und nicht durch den Purger gelöscht wurde. Wird eine Mitteilung in der Nachrichtenverwaltung für den erneuten Versand markiert, wird diese an ComAS2 übergeben, auch wenn der „AS2 Bypass“ noch aktiviert ist. Die Mitteilung wird erst dann wieder in der Nachrichtenverwaltung verfügbar, wenn der entsprechende Sendetimeout erreicht ist. Wird eine angeforderte RN versendet, ist die Transaktion abgeschlossen und die Mitteilung kann nicht erneut über AS2 versendet werden.

Sende Timeout MDN und Wiederholung Mitteilungsversand

Ein zweiter Timeout-Parameter legt fest, wie lange das AS2 Kommunikationsmodul versuchen soll, asynchrone MDN zu versenden, bevor die Transaktion auf fehlerhaft gesetzt wird.

Die beiden nächsten Parameter definieren, ob das AS2 Gateway eine Mitteilung erneut senden soll, falls die angeforderte asynchrone MDN in der definierten Zeit nicht zurückgesendet wurde und wie oft diese Wiederholung durchgeführt werden soll. Steht der Wert für Wiederholungen auf „0“, so verschiebt das AS2 Gateway die Mitteilungen nach Erreichen des Timeouts direkt als fehlgeschlagen in die Nachrichtenverwaltung. Wird eine Zahl ungleich „0“ eingetragen, so versendet das AS2 Kommunikationsmodul die AS2 Mitteilung entsprechend oft, bevor diese als fehlgeschlagen in die Nachrichtenverwaltung erscheint.

Wir empfehlen aber, in der Konfiguration (siehe Bild unter MDN-Transfer) für den Versand einer AS2 Mitteilung (X.400 ⇒ AS2) eine synchrone MDN anzufordern.

Steuerung AS2 Kommunikation im Problemfall

Mit der Option „Inaktiv“ kann die Auslieferung von Mitteilungen an die AS2 Lösung des Kunden temporär unterdrückt werden (z.B. während eines Zertifikatswechsels). Gibt es bei der AS2 Lösung des Kunden ein größeres Problem, können alle Mitteilungen mit der Option „AS2-Bypass aktivieren“ direkt in die Nachrichtenverwaltung zur manuellen Bearbeitung umgeleitet werden. Weiterhin kann aktiviert werden, ob das AS2 Gateway bei den über das AS2 Protokoll empfangenen Mitteilungen auf Basis der Message-ID einen „Duplicate Check“ durchführen soll.

Konfiguration der Umsetzung AS2 nach X.400 Mitteilung

Für die Konfiguration der Zuordnung zwischen X.400 Reports und MDN gibt es in *WebConfig* ebenfalls entsprechende Einstellungsoptionen bei den Menüpunkten „Grundeinstellung“ und „AS2 – X.400 Partnerschaften“. Neben AS2 spezifischen Abschnitten/ Feldern sind die Parameter für die Umsetzung von AS2 Dokumenten in X.400 Mitteilungen und umgekehrt vergleichbar zu denen bei normalen MessageGate Nutzern.

Default-Eigenschaften: X.400 ⇒ AS2

Komprimieren	<input checked="" type="checkbox"/>
Signieren	SHA256
Verschlüsseln	AES
MDN anfordern	<input checked="" type="checkbox"/>
MDN signieren	SHA256
MDN Transfer	asynchron: HTTP

X.400 Einstellungen

Einstellungen

Vom Benutzer angeforderte asynchrone MDN zurücksenden: Nach Auslieferung Mitteilung (DN)

Bei Mitteilungen von X.400-Absendern werden angeforderte Lesebestätigungen:

ignoriert
 zugestellt, sobald eine Empfangsbestätigung versendet wird

Message Expiration: Minuten

X.400 Content-Type: IPM84
IPM88

Bodypart: IA5-Text
Bilateral (Bodypart 14)
ISO-Latin-1
Kontextabhängig (variabel)

Binäre Daten codieren als: binary
base64

Kommentar:

Ok
Abbrechen

Um den Vorgaben des AS2 Standards zu genügen, gibt es beim Feld „Von AS2 Nutzer angeforderte asynchrone MDN zurücksenden“ vier Alternativen:

- Sofort → asynchrone MDN senden, sobald Dokument MessageGate übergeben wurde
- Nach Versand Mitteilung → asynchrone MDN senden, sobald Mitteilung an X.400 MTA übergeben wurde und dieser eine Mitteilungsnummer (X-MPDUID bzw. MTS ID) erzeugt hat. Diese wird dann in der MDN zum AS2 Nutzer übertragen.
- Nach Auslieferung Mitteilung (DN) → asynchrone MDN senden, sobald die Mitteilung in der Mailbox des Empfängers ausgeliefert wurde. Schliesst Non-Delivery Notification mit ein!
- Nach Verarbeitung Mitteilung (RN) → asynchrone MDN senden, sobald die Mitteilung durch den Empfänger verarbeitet (gelesen/abgeholt) wurde. Schliesst die Anforderung einer Delivery Notification mit ein, jedoch kann deren Empfang nur im Statusreport überprüft werden.

Wird die Alternative „Sofort“ gewählt, erhält der AS2 Nutzer lediglich die Information, dass das AS2 Dokument vom AS2 Gateway angenommen wurde, aber er erkennt nicht, ob es beim X.400 Transfer Probleme gegeben hat.

Achtung: Dies gilt auch, wenn er bei den angelieferten Dokumenten eine synchrone MDN angefordert hat. Das Anfordern von synchronen MDN in Verbindung mit dem AS2 Gateway wird deshalb explizit **nicht** empfohlen! Denn dann kann der AS2 Nutzer nur anhand des Statusreport (z.B. in der WebConfig GUI oder mittels Empfangs eines automatischen Statusreport und unter Verwendung der Option „nur fehlgeschlagen“) ermitteln, ob beim X.400 Transfer ein Fehler aufgetreten ist.

Bei „Nach Versand Mitteilung“ weiß er zwar, dass die Mitteilung vom AS2 Gateway versendet wurde (und erhält die MTA Mitteilungskennung X-MPDUID), aber auch hier erhält er keine Informationen über Probleme beim X.400 Transfer.

Es wird empfohlen, die Alternative „Nach Auslieferung Mitteilung (DN)“ zu wählen. Dann hat man die Bestätigung, dass der Partner auf die Mitteilung zugreifen könnte.

Die Alternative „Nach Verarbeitung Mitteilung (RN)“ liefert zwar auch noch die Information, dass der Partner auf die Mitteilung zugegriffen (abgeholt/ gelesen) hat. Aber es muss sichergestellt sein, dass der Partner auch RN zeitnah erzeugt, da Ihre Anwendung unter Umständen zu lange auf die MDN warten müsste (unnötige Alarmierung oder Wiederholung der Transaktion!).

Nutzung zentrale EDI-Funktion

Wie schon im letzten Kapitel beschrieben, gibt es die Möglichkeit, beim Versand von Mitteilungen über die zentrale EDI-Funktion eine Transmission Set Datei mit mehreren EDIFACT Interchange zu übergeben. In diesem Fall ist es aber nicht möglich, eine asynchrone MDN auf Basis von X.400 Reports zu erzeugen, da ja mehrere Mitteilungen versendet werden. Hier wird, wenn nicht in der oben beschriebenen Option „Sofort“ ausgewählt wurde, immer die MDN versendet, sobald der MTA die Mitteilungen bearbeitet hat. Konnten die Mitteilungen versendet werden, wird in der MDN der jeweiligen EDI Interchange ID eine X.400 MTS ID zugeordnet. Ist ein Versand nicht möglich (falsche Adresse, Syntaxfehler, keine EDI Partnerschaft vorhanden) wird eine entsprechende Erläuterung der Interchange ID zugeordnet.

Bsp. für Text in MDN:

*** IC(s) failed ***

AS2TEST3 0815 :11 NOTEXIST :65 Receiving Partner not found

AS2TEST4 NOTEXIST :11 2001005 :65 Sending Partner not found

*** IC(s) submitted ***

AS2TEST1 0815 :11 2001005 :65 X-MPDUID: C8D72CFB11E17CCE85D40FBA

AS2TEST2 0815 :11 2001005 :65 X-MPDUID: C8EDE94B11E17CCE85D413BA

Falls Sie eine Umsetzung von X.400 Reports in MDN wünschen, bitte immer nur einen Interchange in der Transmission Set Datei übertragen.

Bei Mitteilungen, die ein X.400 Partner an seinen AS2 Partner sendet, erzeugt der MessageGate Prozess bereits bei der Übergabe der Mitteilung an ComAS2 eine Auslieferbestätigung (Delivery Notification DN), wenn der Absender dies angefordert hat. ComAS2 versucht die Mitteilung dann abhängig von den konfigurierten Timern (Sende Timeout, Purge Timer) der AS2 Lösung des Nutzers zuzustellen. Bei Nichterreichbarkeit verlängert sich der Intervall der einzelnen Wiederholversuche kontinuierlich um eine Minute bis letztendlich im Stundenabstand versucht wird, das Dokument zuzustellen. Wenn nicht anders konfiguriert, werden die Wiederholversuche erst durch das Löschen des Eintrags in der Trace_Tab beendet. Dann wird diese Transaktion auf fehlerhaft gesetzt.

Um dem X.400 Partner die Möglichkeit zu geben, die Auslieferung der AS2 Dokumente zu überprüfen, sollte dieser in der X.400 Mitteilung eine Lesebestätigung (Receipt Notification RN) anfordern und im Partnerschaftprofil beim Feld „Bei Mitteilungen von X.400 Absendern werden angeforderte Lesebestätigungen“ die Alternative „Zugestellt“ wählen.

Bitte beachten Sie dabei aber, dass eine RN kostenpflichtig ist (wird bei der Berechnung des übertragenen Volumen berücksichtigt)!

Abweichend vom File Interface, wo ja beim Versenden der X.400 Mitteilung die Message ID und der Betreff aus der UNB-Referenznummer abgebildet wird, übernimmt das AS2 Gateway für die Message ID eine interne Bearbeitungsnummer und für den X.400 Betreff den entsprechenden Betreff (Subject) der AS2 Mitteilung.

Automatischer Statusreport

Wie schon weiter oben erwähnt, kann sich der AS2 Benutzer, wie der Benutzer des MessageGate File Interface, entsprechende Status Reports in *WebConfig* abfragen/ abholen oder dort eine automatische Auslieferung über AS2 konfigurieren.

Für den automatischen Empfang von Status Reports muss bei dem Menüpunkt „Automatischer Status Report“ eine entsprechende AS2 Partnerschaft eingerichtet werden.

Neben den im Kapitel 2.9.8 Automatischen Statusreport konfigurieren beschriebenen Einstellungen muss hierbei dem Reporting Prozess eine AS2-ID zugeordnet werden.

Wie bei den anderen AS2 Partnerschaften können Sie festlegen, ob die Daten dabei komprimiert, signiert und/oder verschlüsselt übertragen werden sollen. Falls von Ihnen gewünscht, kann durch die Administration von BusinessMail X.400 auch für diese Partnerschaft eine alternative URL eingerichtet werden. Eine MDN wird für den Statusreport aber nicht angefordert.

Die ersten Zeilen der Einträge innerhalb eines AS2 Status Reports sind identisch zu denen beim File Interface. Es werden aber zusätzliche, AS2 spezifische, Informationen ergänzt, um den Status der AS2 Transaktionen zu beschreiben.

AS2-X.400 Partnerschaft :: Automatischer Status Report

Automatischen Status Report aktivieren

AS2 Einstellungen

IDs

AS2-ID: AS2-Partner AS2Tester001
 AS2-ID: Status Report

Eigenschaften: X.400 ⇒ AS2

default-URL
 Altern. URL
 Komprimieren
 Signieren
 Verschlüsseln

Automatischer Status Report

Einstellungen

Nur fehlgeschlagene Nachrichten

Wochentage Montag
 Dienstag
 Mittwoch
 Donnerstag
 Freitag
 Samstag
 Sonntag

Täglicher Beginn (MEZ/MESZ, Format: hh:mm)
 Tägliches Ende (MEZ/MESZ, Format: hh:mm)
 Sendeintervall Minuten (0=Einmalig zum täglichen Beginn), mindestens 30
 Disposition
 Direction
 Format

Nachfolgend die Erläuterungen für diese erweiterten Informationen:

AS2-ID: AS2 Kennung des X.400 Partners

AS2-MIC Message Integrity Check, wird im Message Header beim Anfordern von signierten MDN gesendet!

AS2-Status: Mögliche Werte sind:

(MDN) not yet sent → kurzzeitige Status bei Mitteilungen (Transaktion X.400 → AS2) oder asynchronen MDN (Transaktion AS2 → X.400), die MessageGate an ComAS2 übergeben hat, für die aber noch kein Verbindungsversuch erfolgt ist

(MDN) still sending → Mitteilung (Transaktion X.400 → AS2) oder asynchrone MDN (Transaktion AS2 → X.400) liegt in Resend Queue von ComAS2

(async MDN) sent → Mitteilung (Transaktion X.400 → AS2) oder asynchrone MDN (Transaktion AS2 → X.400) gesendet

sync MDN sent → synchrone MDN gesendet (Transaktion AS2 → X.400)

sync MDN received → Mitteilung (Transaktion X.400 → AS2) gesendet und synchrone MDN erhalten

async MDN requested → Mitteilung (Transaktion X.400 → AS2) gesendet und asynchrone MDN angefordert

async MDN received → Mitteilung (Transaktion X.400 → AS2) gesendet und asynchrone MDN erhalten

deleted by order → Mitteilung (Transaktion X.400 → AS2) wurde auf Anforderung in *WebConfig* aus der Nachrichtenverwaltung gelöscht

bypassed → Mitteilung (Transaktion X.400 → AS2) wurde über Schalter in Grundeinstellung direkt in die Nachrichtenverwaltung verschoben

send error – bypassed → Mitteilung (Transaktion X.400 → AS2) nach Timeout beim Versenden in die Nachrichtenverwaltung verschoben

send error – discarded → Mitteilung (Transaktion X.400 → AS2) nach Timeout verworfen (nur im Transfermodus)

async MDN missing - bypassed → Mitteilung (Transaktion X.400 → AS2) konnte zwar per AS2 versendet werden, aber die angeforderte asynchrone MDN ist nicht vor Ablauf des Timers zurückgesendet worden. Die Mitteilung ist deshalb in die Nachrichtenverwaltung verschoben worden. Abhängig vom Parameter Wiederholungen wurde die Mitteilung mehrfach versendet (siehe auch Sentcounter)

async MDN missing - discarded → Mitteilung (Transaktion X.400 → AS2) konnte zwar per AS2 versendet werden, aber die angeforderte asynchrone MDN ist nicht vor Ablauf des Timers zurückgesendet worden. Die Mitteilung wurde deshalb verworfen (gilt nur im Transfermodus). Abhängig vom Parameter Wiederholungen wurde die Mitteilung mehrfach versendet (siehe auch Sentcounter)

send again requested → kurzzeitiger Status, wenn eine in der Nachrichtenverwaltung angezeigte Mitteilung (Transaktion X.400 → AS2) erneut versendet werden soll

error → kurzzeitiger Status, wenn Timer abgelaufen, aber die Mitteilung (Transaktion X.400 → AS2) noch nicht in die Nachrichtenverwaltung verschoben wurde

Message received → Mitteilung wurde über AS2 empfangen, aber es wurde keine MDN angefordert (Transaktion AS2 → X.400)

AS2-Lastsent:	Zeitstempel des letzten Versands Format: dd-mmm-yyyy hh-mm-ss +0100 (+0200 Sommerzeit)
Sentcounter:	Zähler, wie oft die Mitteilung (Transaktion X.400 → AS2) versendet wurde (Retry bei Timeout von angeforderter asynchronen MDN)
MDN_expected	Zeitpunkt, an dem die angeforderte asynchrone MDN erwartet wird Format: dd-mmm-yyyy hh-mm-ss +0100 (+0200 Sommerzeit)

Wurde als Format „CSV-C“ oder „CSV-S“ angegeben, werden neben den im Kapitel 2.7.4 Syntax des Statusreports (CSV-Format) angegebenen Felder noch folgende Werte ausgegeben:

Feldname:	Erläuterung:
AS2-ID	AS2 Kennung des X.400 Partners in Hochkommata
AS2-MIC	Message Integrity Check, in Hochkommata, wird im Message Header beim Anfordern von signierten MDN gesendet!
AS2-Status	Mögliche Werte, siehe oben mit Hochkommata
AS2-Lastsent	Zeitpunkt (UTC/GMT), an dem die AS2 Mitteilung an Ihre AS2 Lösung versendet wurde (dd.mm.yyyy hh:mm) ohne Hochkommata
Sendcounter	Zähler, wie oft Mitteilung versendet wurde, ohne Hochkommata.
MDN_expected	Zeitpunkt (UTC/GMT), zu dem die angeforderte asynchrone MDN erwartet wird (dd.mm.yyyy hh:mm), ohne Hochkommata

Seite ist aus redaktionellen Gründen leer.

7 SMTP-MTA und MessageGate

7.1 Allgemein

Aufgrund der Anfragen von X.400 Domain Betreibern nach einer Anbindung über einen SMTP MTA unter Beibehaltung der vorhandenen X.400 Adressen (Global Domain Identifier ⇒ GDI) bietet der MailGate X.400 Service nun neben dem X.400 MTA auch einen entsprechenden SMTP (RFC 2822 kompatiblen) MTA an.

Die Umsetzung zwischen SMTP (MIME bzw. S/MIME) und X.400 Mitteilungen übernimmt ein modifizierter MessageGate Prozess (MGPMDF), der zum einen über eine API mit dem systeminternen SMTP-MTA und zum anderen über die sogenannte XAPI mit dem X.400 MTA kommuniziert.

Zwar schreibt auch dieser MessageGate Prozess Einträge in den Statusreport, aber dieser Report ist nur für den Administrator des Kundenmailsystems vorgesehen und nicht für die Endbenutzer. Abweichend vom File Interface ist deshalb eine Umsetzung von SMTP-Reports in X.400 Reports und umgekehrt vorgesehen, um auch den Endbenutzern Statusinformationen bereitzustellen.

Als SMTP MTA Engine wird der PMDF MTA der Fa. Process Software eingesetzt, da dieser wie der X.400 MTA (Mailbus 400 der Fa. Hewlett-Packard Enterprise) unter OpenVMS betrieben werden kann.

Bei der aktuellen Version des SMTP MTA werden nicht alle Umsetzregeln zwischen X.400 und RFC 2822 angewendet, die in den RFC 2156/2157 (Mixer) definiert sind. Details hierzu finden Sie im nachfolgenden Kapitel.

7.2 Unterschiede zwischen File Interface und SMTP MTA Nutzern

SMTP MTA Nutzer kommunizieren nur indirekt mit dem MessageGate Prozess, da sie ja einen E-Mail-Client verwenden, um mit den Partnern Daten auszutauschen. Diese Mitteilungen werden mittels SMTP zur BusinessMail X.400 Plattform übertragen. Hier übernimmt der MessageGate Prozess die Umsetzung zwischen RFC 2822 und X.400 Mitteilung und verwaltet diese Transaktion in einer Datenbankrelation (Trace Tab). Dort werden dann auch die einzelnen Reports den Mitteilungen zugeordnet. Anders als beim File Interface, wo man diese Zuordnung nur im Statusreport erkennt, werden aber beim SMTP MTA die entsprechenden SMTP-Reports (DSN bzw. MDN) dann auch an den Absender gesendet.

Empfohlen wird dabei auf SMTP-Seite einen MTA einzusetzen, der DSN (Delivery Status Notification nach RFC 1891 bzw. 3461) unterstützt. Dann könnten X.400 Delivery Notifications (DN) in DSN und X.400 Receipt Notifications (RN) in MDN (Message Disposition Notifications laut RFC 3798) und umgekehrt umgesetzt werden.

Der MessageGate Prozess erlaubt zwar auch die Umsetzung zwischen einer X.400 DN und einer MDN, jedoch ist diese Lösung problematisch, da es dann am E-Mail-Client liegt, eine MDN zu erzeugen und nicht der SMTP MTA des Kunden Mailsystems dies initiieren kann. Im X.400 Standard ist jedoch festgelegt, dass eine angeforderte X.400 DN in jedem Fall erzeugt bzw. eine NDN erzeugt werden muss, falls die Mitteilung nicht zweifelsfrei ausgeliefert wurde. Der MGPMDF wird deshalb eine

NDN mit Fehler „Time expired“ erzeugen, falls die MDN nicht rechtzeitig eintrifft. Eine „verspätete“ MDN wird dann ignoriert.

Auch bei der Umsetzung der Mitteilungsinhalte gibt es Unterschiede. Während man beim File Interface auswählen kann, ob binäre MIME-Contents entweder im Format Binary oder in BASE64 dargestellt werden, wird beim SMTP MTA ausschließlich BASE64 angeboten. Dies ist aber ohnehin das für eine RFC2822 Mail empfohlene Format. In Richtung X.400 werden BASE64 codierte binäre Inhalte decodiert und als BP14 ohne Dateinamen bzw. als BP15 FTAM Body Part übertragen. Dies gilt auch für einen S/MIME-Content, der weitestgehend unverändert wie beim File Interface in einen einzelnen BP15/FTAM Body Part (siehe 2.3.4 S/MIME gesicherter Inhalt) umgesetzt wird. Siehe hierzu auch weiter unten den Abschnitt X.400 Mitteilungsstruktur.

Nachfolgend ein Beispiel für die Grundeinstellung einer Domain mit SMTP MTA und MGPMDF.

MessageGate SMTP Partnerschaft :: Grundeinstellungen ⓘ

Benutzer

X.400-Adresse n-id=2060036; p=PMDF-TEST; a=VIAT-TEST; c=DE

Einstellungen ⓘ

eine in SMTP Mitteilung angeforderte MDN umsetzen in Anforderung einer X.400-Verarbeitungsbestätigung (RN) ▾

eine in X.400 Mitteilung angeforderte DN als DSN in SMTP Mitteilung anfordern ▾

eine in X.400 Mitteilung angeforderte RNNRN als MDN in SMTP Mitteilung anfordern ▾

Message Expiration 1440 Minuten

X.400 Content-Type IPM84
IPM88

Bodypart ⓘ IA5-Text
Bilateral (Bodypart 14)
ISO-Latin-1
Kontextabhängig (variabel, flach)
Kontextabhängig (variabel, geschachtelt)

Abbildung in SMTP Adresse ⓘ X.400 Adress Syntax verwenden
Alle X.400 Adresselemente umsetzen
Nur natürliche Adresse erlaubt

Binäre Daten codieren als base64 ▾

Purge-Zeit ⓘ 120 Stunden

Domäne ⓘ pmdf-test.de

Kommentar

Ok Abbrechen

Neu sind in der SMTP MTA Grundeinstellung die Regeln zur Umsetzung einer X.400 Report Anforderung, die zusätzlichen Regeln beim Mapping in den X.400 Body Part und die Anzeige für das Mapping zwischen X.400 und SMTP-Adresse (Domäne).

Unabhängig von der o.g. Einstellung für die Anforderung eines X.400 Reports setzt der MGPMDF die Anforderung einer SMTP DSN immer in die Anforderung einer X.400 DN um. Und selbst wenn keine DSN angefordert wurde, fordert MGPMDF eine X.400 NDN (Non Delivery Notification) an, so dass im Fehlerfall der E-Mail-End-

nutzer eine DSN mit entsprechendem Fehlercode erhält. Siehe hierzu auch B5. Umsetzregel bei Fehlercodes DN zu DSN.

Bitte beachten Sie auch, dass der X.400 Standard es erlaubt, pro Empfänger einer Mitteilung unterschiedliche Reports anzufordern. Dies lässt sich aber in einer SMTP-Mitteilung nicht abbilden. Wird also eine Mitteilung an mehrere SMTP-Empfänger gesendet und in der X.400 Mitteilungen für einige der Empfänger eine Lesebestätigung angefordert wurde und für andere nicht, wird in der SMTP-Mitteilung keine MDN angefordert, selbst wenn dies im Profil konfiguriert wurde.

Partnerschaftseinträge

Wie beim File Interface gibt es auch beim SMTP-MTA die Möglichkeit, gezielt Partnereinträge mit von den Grundeinstellungen abweichenden Umsetzregeln einzurichten. Diese gelten dann aber für alle SMTP-Benutzer in dieser Domain. Bitte beachten Sie dabei, dass der SMTP MTA abweichende Umsetzregeln in den Partnereinträgen nur dann berücksichtigt, wenn es in der Mitteilung nur einen Empfänger gibt. Hat die Mitteilung mehrere Empfänger, werden immer die in der Grundeinstellung hinterlegten Regeln verwendet.

Adressumsetzung

Bei den SMTP MTA Grundeinstellungen wird auch angezeigt, in welche Domain die X.400 Adresse des Mitteilungsempfängers abgebildet wird. Für die übrigen Adressfelder der RFC2822 Adresse wird das im RFC 2156/2157 (Mixer) definierte Mapping verwendet, bei dem der Vorname und Nachname links vor dem „@“ und Organisation und Organisationseinheit als Domains rechts davon (von rechts nach links) angeordnet werden.

Adressumsetzung bei Domain aus Beispiel

X.400 Adresse: c=de;a=viat-;p=pmdf-test;o=testag;ou1=entwicklung;s=tester; g=erster

SMTP-Adresse: erster.test@entwicklung.testag.pmdf-test.de

MGPMDF erlaubt aber vor allem für Migrationszwecke (Wechsel von X.400 MTA zu einem SMTP MTA) beim Mapping auf einen RFC2822 Domainnamen neben den X.400 GDI-Adressfeldern (Global Domain Identifier: Country, ADMD, PRMD) auch Organisation und Organisationseinheiten zu berücksichtigen. Folgende Umsetzregel wäre somit auch möglich:

X.400 Adressfilter: c=de;a=viat-;p=pmdf-test;o=testag;ou1=entwicklung

SMTP-Domain: entwicklung.de

Die übrigen Adressfelder einer X.400 Adresse würden dann bei der Umsetzung entsprechend vor und nach dem „@“ der RFC2822 Adresse angeordnet.

Erhält der SMTP MTA Endbenutzer eine Mitteilung, würde seine Empfängeradresse somit in dieser „natürlichen“ Adressform dargestellt.

Das Format der Absenderadresse und falls vorhanden, die der anderen Empfänger der Mitteilung, wird über die Konfigurationsoption „Abbildung in die SMTP-Adresse“ in der Grundeinstellung oder dem Partnerprofil festgelegt.

Bei der Defaulteinstellung „X.400 Adress Syntax verwenden“ wird die gesamte X.400 Adresse des Absenders links vom „@“ Zeichen abgebildet, wobei die einzelnen

Adresselemente durch einen Schrägstrich „/“ eingerahmt werden. Enthält eines der Adressfelder Leerzeichen oder Sonderzeichen, wird der Teil vor dem „@“ in Hochkommata gesetzt. Bitte beachten Sie, dass einige E-Mail Clients beim Reply auf eine empfangene Mitteilung die Hochkommata in der Adresse der neuen Mitteilung nicht berücksichtigen, was den Versand (Ablehnung durch eigenen SMTP Server) bzw. die Auslieferung der Mitteilung (Ablehnung durch SMTP MTA) verhindern würde. Bitte dann die Hochkommata vor dem Versand ergänzen (siehe auch Hinweis zu Telefax Gateway weiter unten).

Bsp. für X.400 Adresse links vom @: /G=ipm/S=tester/O=testag/A=viaT/C=de/@ bmx400.de

Als Alternative dazu kann man auch die Einstellung „Alle X.400 Adresselemente umsetzen“ auswählen, bei der der SMTP MTA versucht, die X.400 Adresse(n) in „natürliche“ RFC2822 Adressen umzusetzen. Falls aber die X.400 Adresse Elemente oder Zeichen enthält, die nicht in eine klassische RFC2822 Adresse abgebildet werden können, werden die entsprechenden Elemente als X.400 Felder links vom „@“ Zeichen abgebildet („Mixed“ Adresse). Es gibt z.B. für die X.400 Adressfelder CN (Commonname) oder Generation keine Gegenstücke in der SMTP Adresse oder auch das in einer X.400 Adresse erlaubte „+“ Zeichen kann nicht abgebildet werden. Leerzeichen in X.400 Adresse werden durch ein Tilde Zeichen „~“ in der RFC2822 Adresse ersetzt.

Bsp. für natürliche SMTP-Adresse: ipm.testers@testag.bmx400.de

Bsp. für Adresse mit X.400 Elemente: /CN=ipm~tester/@testag.bmx400.de

Als dritte Option kann man auswählen, dass ausschließlich „natürliche“ RFC2822 Adressen übertragen werden dürfen. Enthält die X.400 Absenderadresse oder die Adresse eventuell vorhandener zusätzlicher Empfänger nicht abbildbare Element oder Zeichen, weist der SMTP MTA diese X.400 Mitteilung mit dem Fehler „Konvertierung nicht möglich“ (Reason Code 2, Diagnostik Code 8) in der NDN zurück.

Bei Mitteilungen von SMTP an X.400 kann man sowohl Adressen mit der X.400 Syntax links vom „@“ Zeichen, „natürliche“ Adressen oder auch „Mixed“ Adressen beim Empfänger verwenden. Bei „natürlichen“ und „Mixed“ Adressen ermittelt der SMTP MTA anhand der in der Datenbank hinterlegten Einträge und Regeln eine entsprechende X.400 Adresse.

Auch SMTP MTA Benutzer können die Gateway Lösungen von BusinessMail X.400 ansprechen. Bei der Adressierung des Telefax Gateway ist aber darauf zu achten, dass der Adressteil vor dem @ Zeichen in jedem Fall in Hochkommata gesetzt wird, da das „:“ Zeichen im DDA Feld sonst zu Problemen führt.

Bsp.: "/X121= 0391580217255/DDA:Service=FAX/A=viat/C=de/"@BMX400.DE

SMTP MTA Benutzer können den RFC2822 Adressen der X.400 Partner auch einen Alias zuordnen. Beim Versand von Mitteilungen nach X.400 werden diese Alias und auch ein Alias bei der Absenderadresse vom SMTP MTA ignoriert. Die Adressen in ausgelieferten SMTP-Mitteilungen enthalten keinen Alias.

In der X.400 Mitteilung, die der Empfänger erhält, wurde durch den MGPMDF bei der Absenderadresse entsprechend den im Domain Profil hinterlegten Umsetzregeln die RFC2822 Adresse in eine eindeutige X.400 Adresse umgesetzt. In das Adressfeld „Freeform Name“ (Teletex Zeichensatz) wird die ursprüngliche SMTP Adresse (die ersten 64 Zeichen) bestehend aus dem Alias und der Mailbox Adresse abgebildet. Abweichend vom Standard wird, wie z.B. auch bei Microsoft Outlook, die Mailbox Adresse in eckige Klammern gesetzt:

Aliasname [vorname.nachname@domain]

um Kompatibilitätsprobleme mit älteren X.400 Clients zu vermeiden.

X.400 Mitteilungsstruktur

Im RFC 2156/2157 (Mixer) werden u.a. die Regeln für die Umsetzung von MIME-Content Type in X.400 Body Parts beschrieben. Diese Umsetzregeln wurden beim SMTP MTA weitestgehend implementiert und der MGPMDF unterstützt somit auch den X.400 Body Part vom Typ Mitteilung.

Mit dem Standard Wert „Variabel/flach“ der Option „Mapping Body Part“ legt man z.B. fest, dass geschachtelte SMTP-Mitteilungsinhalte (Multipart/alternate oder Multipart/related) in der X.400 Mitteilung ohne Verschachtelung abgebildet werden. Die MIME-Contents werden entsprechend ihrer Reihenfolge als X.400 Body Parts in die neue Mitteilung übernommen. Enthält die RFC2822 Mitteilung einen MIME-Content vom Type Multipart/alternate (z.B., wenn der Mitteilungstext sowohl als Text als auch als HTML-Seite übertragen wird), werden die eingebetteten MIME-Contents somit als X.400 Body Parts ohne Hinweis auf den identischen Inhalt abgebildet.

Will man die Informationen über die Verschachtelung innerhalb des MIME-Content in die X.400 Mitteilung durchreichen, muss man die Option „Variabel/geschachtelt“ auswählen. Dann werden die verschachtelten MIME-Content als X.400 Body Part vom Typ Mitteilung in der X.400 Mitteilung dargestellt, die dann auch Informationen über die Art der Verschachtelung im Betreff enthält, z.B. alternative Darstellung Mitteilungstext oder in HTML-Seiten eingebettete Bilder.

Abweichend vom File Interface und AS2 akzeptiert der SMTP MTA neben einem MIME Text Content mit Zeichensatz ISO-Latin-x (x=1-9) und IA5 auch andere Zeichensätze (z.B. ISO-Latin-15, Windows-1252 oder UTF-8). Da es aber keine entsprechenden X.400 Body Parts gibt, wird der Text in einen BP15 General Text ISO-Latin 1 (ISO 8859-1) Body Part abgebildet, wobei ein MIME-Header mit Informationen über den ursprünglichen Zeichensatz dem Text vorangestellt wird.

Werden gesicherte (signierte und/oder verschlüsselte) Inhalte mittels S/MIME-Content in der SMTP-Mitteilung übertragen, setzt der SMTP MTA diesen in der X.400 Mitteilung in einen einzelnen Body Part 15 FTAM Body Part um (siehe auch Kapitel 2.3.4 S/MIME gesicherter Inhalt). Bis auf das Ändern des Transfer Encoding von BASE64 in Binary bei verschlüsselten (enveloped) Inhalten wird der Inhalt beim S/MIME-Content unverändert im FTAM Body Part abgebildet. Auch beim Empfang von X.400 Mitteilungen mit gesicherten Inhalten wird der S/MIME-Content im FTAM Body Part bis auf das Umsetzen des Transfer Encoding von Binary in BASE64 bei verschlüsselten (enveloped) Inhalten unverändert übernommen. Falls Ihre E-Mail-Clients das Content-Transfer-Encoding Binary bei den eingebetteten Dokumenten nicht verarbeiten können, muss der X.400 Partner beim Erzeugen des S/MIME-Content bei den einzelnen Dokumenten schon das geeignete Transfer Encoding (Text dann als Quoted printable und bei binären Anhängen und Signatur dann BASE64) verwenden.

Weitergeleitete Mitteilungen

Unterschiede zum File Interface gibt es auch bei der Behandlung von weitergeleiteten (ungesicherten) Mitteilungen. Während das File Interface diese nicht unterstützt, werden sie beim SMTP MTA wie folgt übertragen:

- a) Eine an einen RFC2822 Empfänger weitergeleitete X.400 Mitteilung (Anhang vom Typ Message) wird als Content-Type `message/rfc822` (siehe RFC 2046) dargestellt. Die Anhänge der weitergeleiteten Mitteilungen sind dann als weitere Content-Types z.B. als `multipart/mixed` eingebettet. Es könnten aber auch weitere Mitteilungen sein, die dann wieder als `message/rfc822` eingebettet werden.
- b) Da es keinen einheitlichen Standard für die Darstellung einer weitergeleiteten Mitteilung in einer RFC2822 Mitteilung gibt, werden beim Weiterleiten von RFC2822 Mitteilungen an einen X.400 Empfänger die entsprechenden MIME-Contents im Mitteilungstext (1. Text Body) der X.400 Mitteilung abgebildet und nicht als Message Body Part angehängt. Nur wenn die weitergeleitete Mitteilung als Content Type `message/rfc822` definiert ist, wird diese bei Einstellung Body Part „Variabel/flach“ oder „Variabel/geschachtelt“ in einen X.400 Mitteilungs Body Part abgebildet. Bei der Einstellung Body Part „IA5-Text“, „Bilateral“ oder „ISO-Latin-1“ wird die MIME Struktur der weitergeleiteten Mitteilung im entsprechenden X.400 Body Part abgebildet. Die Einstellung Body Part „IA5-Text“ kann dabei zu Informationsverlust führen. Dies gilt auch für den X.400 Content-Type „IPM84“.

Mitteilungs-ID

Wenn der MGPMDF empfangene X.400 Mitteilungen in RFC2822 Mitteilungen umsetzt, übernimmt er die X.400 Message ID (P2/P22 Message ID, wird vom X.400 Client erzeugt), die maximal 64 Stellen lang sein kann und ergänzt getrennt durch ein „#“ eine 16 stellige Kennung. Damit ist sichergestellt, dass diese RFC2822 Message ID in jedem Fall eindeutig ist und die von den SMTP Systemen bzw. dem E-Mail Client erzeugten Reports zugeordnet und als X.400 Reports versendet werden können. Falls die X.400 Message ID Leerzeichen enthält, werden diese durch das Unterstrich („_“) Zeichen ersetzt, da Leerzeichen in der Message ID bei einigen E-Mail Clients Probleme verursachen.

Besp.: Message-id: <341_11/11/25#EA4A4CI404G0LBPN@tstmt_pmdf.telebox400.de>

Beim Umsetzen von RFC2822 Mitteilungen in X.400 Mitteilungen übernimmt der MGPMDF die ersten 64 Zeichen der RFC2822 Mitteilungs ID als X.400 Message ID. Es sollte durch den Systemadministrator der Domains sichergestellt werden, dass dieser Wert eindeutig ist, da ansonsten eine angeforderte X.400 Lesebestätigung (Receipt Notification) nicht zugeordnet werden kann.

Statusreport

Um den Administratoren des SMTP-Systems eine bessere Nachverfolgung der übertragenen Mitteilungen zu ermöglichen, werden im Statusreport sowohl die Empfänger- als auch die Absenderadresse für jede Mitteilung ausgegeben. Weiterhin werden die SMTP Message ID (statt Order-ID), die X.400 Message ID (entspricht Message-ID) und die MTS-ID angezeigt. Die übrigen Felder entsprechen denen beim MessageGate File Interface. Bei Mitteilungen von X.400 an SMTP wird deshalb auch nicht der Zeitpunkt des eigentlichen Mitteilungsversands angezeigt, sondern mit „Received:“ der Zeitpunkt, an dem der MGPMDF die Mitteilung zum Weiterversand an den SMTP-Empfänger erhalten hat. Bei Mitteilungen von SMTP an X.400 wird bei

„Sent:“ der Zeitpunkt angegeben, an dem MGPMDF die X.400 Mitteilung versendet hatte.

Bei Einträgen für Mitteilungen, die von SMTP an X.400 übertragen werden, beginnt der Statureintrag mit „To:“, „Cc:“ oder „Bcc:“ und bei Mitteilungen von X.400 an SMTP mit einer „From:“ Adresszeile. Die zusätzlichen Empfänger der Mitteilung werden wie beim File Interface nur im Header der Mitteilung angezeigt, außer es sind mehrere Empfänger in der gleichen Domain. Dann wird für jeden Empfänger ein Eintrag in der Datenbank (Trace Tab) angelegt.

Enthält die SMTP-Adresse einen Alias, wird der eigentliche Adressteil durch spitze Klammern (<>) abgegrenzt. Fehlt der Alias, werden auch keine spitze Klammern angezeigt.

Bsp.

```
To: erster tester </G=erster/S=tester/O=testag/A=viaT/C=de/@bmx400.DE>  
From: test@pmdf-test.de  
SMTP-Msg-ID: <4F1D739B.1070307@pmdf-test.de>  
X400-Msg-ID: 4F1D739B.1070307  
MTS-ID: FE19811D11E145D906005F96  
Sent: 23-Jan-2012 15:50:37 +0100  
Delivered: 23-Jan-2012 15:50:37 +0100
```

Enthält die SMTP-Adresse Leerzeichen, wird diese in Hochkommata dargestellt.

Wird der Statusreport als CSV-Datei heruntergeladen, werden neben der bei MessageGate angeboten Struktur (mit From: und To:) zusätzlich am Ende der Spalte noch die Felder To: und From: angeboten. Somit können sowohl der Absender als auch der Empfänger der SMTP-Mitteilung dargestellt werden, ohne an der „MessageGate Logik“ etwas ändern zu müssen. Bei einer Mitteilung von X.400 nach SMTP wird dann entsprechend der oben beschriebenen besser lesbaren Darstellung ein Wert beim „ersten“ From und ein Wert beim „zweiten“ To eingetragen. Bei einer Mitteilung von SMTP nach X.400 wird ein Wert beim „ersten“ To und ein Wert beim „zweiten“ From eingetragen. Das Feld „Rcpt Type“ definiert dabei in beiden Fällen, um welchen Typ von Empfänger es sich handelt (To:, Cc: oder Bcc:).

Seite ist aus redaktionellen Gründen leer.

8 Lösungen für MessageGate realisieren

8.1 Erste Tests mit Standard-E-Mail-Clients

8.1.1 Test mit Outlook Express bei älteren Windows OS

Outlook Express eignet sich gut, um Mitteilungen für einen ersten Test mit MessageGate zu erstellen bzw. um sich ausgelieferte Mitteilungen und deren Attachements anzuschauen. Grundlage ist dabei, dass Outlook Express erlaubt, Mitteilungen als Textdatei (Endung *.eml) abzuspeichern bzw. diese auch wieder darzustellen.

Legen Sie zunächst ein E-Mail-Konto an und geben Sie im Feld „Angezeigter Name“ Ihre X.400 Adresse ein (Adressfelder durch Semikolon getrennt, Adresse nicht in Hochkommata setzen!) und bei E-Mail-Adresse „User-ID@viat.de“ oder „X@viat.de“, wobei bei User-ID die Nummer Ihres MessageGate Eintrages genutzt werden sollte (als Beispiel 58111@viat.de). Bei SMTP und POP3 Server können Sie „Test“ eintragen, da diese Werte nicht verwendet werden.

Nun können Sie unter Kontakte eine Zieladresse eintragen, wobei Sie beim Nachnamen wieder die X.400 Adresse (Adressfelder durch Semikolon getrennt, Adresse nicht in Hochkommata setzen!) eingeben und bei E-Mail-Adresse entweder User-ID@viat.de (z.B. 58111@viat.de) oder aber x@viat.de angeben. Am besten geben Sie hier die Adresse des eigenen MessageGate Eintrags an, da dann auch schon eine Mitteilung in das MessageGate Verzeichnis ausgeliefert wird.

Als Nächstes können Sie eine Mitteilung erstellen und die Adresse aus dem Adressbuch übernehmen. Bei der Mitteilung bitte Format auf Nur-Text einstellen und beliebige Dateien anhängen. Dann unter „Datei → Speichern unter“ den Namen und den Pfad der Textdatei angeben, in der die Mitteilung gespeichert werden soll. Da Outlook Express im Gegensatz zu Thunderbird (siehe nächstes Kapitel) beim Entwurf noch keine Message-ID erzeugt, sollten Sie den Dateinamen schon gleich mit einer geeigneten Auftragsnummer versehen (z.B. M_test00001.eml), die dann als X.400 Message-ID übernommen wird. Dann kann die Datei in „*.TMP“ umbenannt und per SFTP oder HTTPS in das MessageGate Verzeichnis übertragen werden. Sobald die Datei dort in „*.IN“ umbenannt wurde, wird sie von MessageGate versendet und wenn an eigenen MessageGate Eintrag adressiert, auch als „M_*.OUT“ Datei wieder ausgeliefert.

Nach dem Abholen kann man diese Datei dann in „*.eml“ umbenennen und wieder mit Outlook Express öffnen. In der Mitteilung wird die ursprüngliche Auftragsnummer als Mitteilungsnummer angezeigt. Outlook Express kann übrigens binäre Daten sowohl mit Encoding BASE64 als auch Binary verarbeiten und man muss hier den entsprechenden Parameter im User Profile bzw. Partner Profile nicht anpassen.

8.1.2 Test mit Thunderbird

Auch mit Thunderbird kann eine Mitteilung erzeugt und als Textdatei abgelegt werden. Thunderbird fügt sogar eine Message-ID bei Entwurfsmitteilungen ein. Dafür kann Thunderbird aber die Anhänge von importierten Mitteilungen nicht darstellen, bei denen als Encoding die Einstellung Binary benutzt wurde.

Um eine Mitteilungsdatei zu erhalten, sollte man zunächst ein Konto einrichten, bei dem als E-Mail-Adresse User-ID@viat.de (z.B. 58111@viat.de) oder aber x@viat.de

angeben wird. Bei „Ihr Name:“ dann die X.400 Adresse Ihres MessageGate Eintrags angeben (Adressfelder durch Semikolon getrennt, Adresse nicht in Hochkommata setzen!). Bei POP3 Server können Sie „Test“ eintragen, da dieser Wert nicht verwendet wird.

Nun können Sie im Adressbuch eine Zieladresse eintragen, wobei Sie beim Nachnamen wieder die X.400 Adresse (Adressfelder durch Semikolon getrennt, Adresse nicht in Hochkommata setzen!) eingeben und bei E-Mail-Adresse entweder User-ID@viat.de (z.B. 58111@viat.de) oder aber x@viat.de angeben. Am besten geben Sie hier die Adresse des eigenen MessageGate Eintrags an, da dann nach dem Versenden der ersten Testmitteilung auch schon eine Mitteilung in das MessageGate Verzeichnis ausgeliefert wird.

Als Nächstes können Sie eine Mitteilung erstellen und die Adresse aus dem Adressbuch für „An:“ übernehmen. Bei „Von:“ wählen Sie das neu eingerichtete Konto aus. Beim Betreff und im Mitteilungstext können Sie beliebige Werte angeben und auch zusätzliche Dateien anhängen. Sie sollten aber bei Einstellungen → Format „Nur Reintext“ wählen. Dann sollten Sie die Mitteilung als Entwurf speichern.

Wenn Sie die Mitteilung im Ordner „Entwürfe“ auswählen, können Sie mit der rechten Maustaste die Funktion „Speichern als:“ nutzen, um eine „*.eml“- Datei zu erstellen (bei Wahl des Dateinamens MessageGate Syntax beachten!). Diese „*.eml“- Datei können Sie in „*.TMP“ umbenennen, in Ihr MessageGate Verzeichnis übertragen und dann in „*.IN“ umbenennen. Nun verarbeitet MessageGate diese Datei und liefert auch wieder eine Mitteilungsdatei aus, falls der Empfänger der eigene MessageGate Eintrag war.

Diese Datei kann (nach Umbenennen) wieder in Thunderbird importiert werden. Es muss aber im Host Profile (Benutzer- oder Partnerprofile) festgelegt sein, dass binäre Daten als „BASE64“ ausgeliefert werden, damit Thunderbird die Anhänge richtig verarbeiten kann.

8.1.3 Test mit Microsoft Live Mail bei neueren Windows OS

Bei neueren Windows Betriebssystemen, bei denen Microsoft das Programm Outlook Express nicht mehr anbietet, kann man auch das im optionalen Paket Windows Essentials (wird von Microsoft jedoch nur bis Februar 2017 unterstützt) enthaltene Programm Windows Live Mail 2012 installieren, um Mitteilungen für einen ersten Test mit MessageGate zu erstellen bzw. um sich ausgelieferte Mitteilungen und deren Attachements anzuschauen. Dieses Programm erlaubt wie Outlook Express, Mitteilungen als Textdatei (Endung *.eml) abzuspeichern bzw. diese auch wieder darzustellen.

Legen Sie zunächst ein E-Mail-Konto an und geben Sie bei E-Mail-Adresse „User-ID@viat.de“ oder X@viat.de an, wobei bei User-ID die Nummer Ihres MessageGate Eintrages genutzt werden sollte (als Beispiel 58111@viat.de). Im Feld „Anzeigennamen für Ihre gesendeten Nachrichten“ dann Ihre X.400 Adresse eintragen (Adressfelder durch Semikolon getrennt, Adresse nicht in Hochkommata setzen!). Bei Passwort und bei den Feldern SMTP und POP3 Server (bei aktivierter Option „Servereinstellungen manuell konfigurieren“) können Sie „Test“ eintragen, da diese Werte nicht verwendet werden.

Nun können Sie unter Kontakte im Adressbuch eine Zieladresse eintragen, wobei Sie beim Nachnamen wieder die X.400 Adresse (Adressfelder durch Semikolon getrennt, Adresse nicht in Hochkommata setzen!) eingeben und bei E-Mail (privat) entweder User-ID@viat.de (z.B. 58111@viat.de) oder aber x@viat.de angeben. Am besten

geben Sie hier die Adresse des eigenen MessageGate Eintrags an, da dann auch schon eine Mitteilung in das MessageGate Verzeichnis ausgeliefert wird.

Als Nächstes können Sie eine Mitteilung erstellen und die Adresse aus dem Adressbuchbereich Kontakte übernehmen. Bei der Mitteilung bitte Format auf Nur-Text einstellen und beliebige Dateien anhängen. Dann unter „Datei → Speichern unter“ den Namen und den Pfad der Textdatei angeben, in der die Mitteilung gespeichert werden soll. Da Live Mail wie Outlook Express beim Entwurf noch keine Message-ID erzeugt, sollten Sie den Dateinamen schon gleich mit einer geeigneten Auftragsnummer versehen (z.B. M_test00001.eml), die dann als X.400 Message-ID übernommen wird. Dann kann die Datei in „*.TMP“ umbenannt und per SFTP oder WebDAV in das MessageGate Verzeichnis übertragen werden. Sobald die Datei dort in „*.IN“ umbenannt wurde, wird sie von MessageGate versendet und wenn an eigenen MessageGate Eintrag adressiert, auch als „M_*.OUT“ Datei wieder ausgeliefert.

Nach dem Abholen kann man diese Datei dann in „*.eml“ umbenennen und wieder mit Live Mail öffnen. In der Mitteilung wird als Mitteilungsnummer die ursprüngliche Auftragsnummer angezeigt. Wie Outlook Express kann auch Live Mail binäre Daten sowohl mit Encoding BASE64 als auch Binary verarbeiten und man muss hier den entsprechenden Parameter im User Profile bzw. Partner Profile nicht anpassen.

8.2 Lösung gestalten und entwickeln

Es gibt für die Bearbeitung der SMTP/MIME Syntax eine Vielzahl von Bibliotheken für die verschiedensten Programmiersprachen und Betriebssysteme und dies sowohl für Open Source als auch für kommerzielle Versionen. Das Erstellen von SMTP/MIME Dateien bzw. das Verarbeiten solcher Dateien innerhalb eines Programms sollte somit ohne größere Probleme möglich sein.

Mehr Zeit sollte dagegen für das Design der Lösung verwendet werden, um auch auf fehlgeschlagene Transaktionen reagieren zu können. X.400 bietet hierbei mit den verschiedenen Arten von Bestätigungen/ Reports die Möglichkeit, eine Transaktionsüberwachung zu implementieren. MessageGate liefert diese Information innerhalb des Statusreports zurück.

Wenn schon keine Überwachung von positiven Bestätigungen erfolgt, sollte zumindest die negative Bestätigung (z.B. NDN oder Versandfehler) einer Mitteilung ausgewertet werden und eine Reaktion innerhalb der Anwendung (z.B. Alarmierung oder Ersatzschaltung) auslösen. Dies sollte bei aktivierter EDI-Funktion auch für empfangene Mitteilungen gelten, wobei hier eine manuelle Bearbeitung sinnvoll ist. Durch die Abfrage von Statusreports kann man gut erkennen, ob MessageGate die Auslieferung von EDIFACT Dokumenten verweigert hat und warum.

Für den Zugriff auf das Übergabe-Verzeichnis von MessageGate stehen drei Kommunikationsvarianten zur Verfügung, SFTP, HTTPS/WebDAV und HTTPS/Web-Service. Wird MessageGate mit vermindertem Leistungsumfang beauftragt, ist der Zugriff über HTTPS/WebDAV die optimale Lösung, da zum Abholen der ausgelieferten Mitteilung ein einfacher Browser ausreichen würde. Die ausgelieferten Mitteilungen (und wenn konfiguriert, auch automatisch erzeugte Statusreports) werden ja nach einer definierten Zeit gelöscht, wobei diese Zeit entsprechend dem Verkehrsaufkommen gewählt werden sollte.

Seite ist aus redaktionellen Gründen leer.

Anhang A X.400 Adresselemente

In diesem Anhang finden Sie Liste der X.400 Adresselemente, die im Alias bei „To:“, „Cc:“, „Bcc:“ oder „From:“ verwendet bzw. die bei der X.400 Adresse im Partnerschaftsprofil werden können:

C=	Länderkennung (Country Code, 3 Zeichen Printable String)
A=	Administrative Domain Name (ADMD, 16 Zeichen Printable String)
P=	Private Domain Name (PRMD, 16 Zeichen Printable String)
O=	Organisationsnamen (64 Zeichen Printable oder Teletex String)
OU1=	Organisationseinheit 1 (32 Zeichen Printable oder Teletex String)
OU2=	Organisationseinheit 2 (32 Zeichen Printable oder Teletex String)
OU3=	Organisationseinheit 3 (32 Zeichen Printable oder Teletex String)
OU4=	Organisationseinheit 4 (32 Zeichen Printable oder Teletex String)
S=	Nachname (Surname, 40 Zeichen Printable oder Teletex String)
G=	Vorname (Givenname, 16 Zeichen Printable oder Teletex String)
CN=	Commonname (64 Zeichen Printable oder Teletex String)
N-ID=	Boxkennung (UA-ID, 32 Zeichen Numerisch)
X121=	Netzwerk Kennung (15 Zeichen Numerisch)
T-ID=	Terminal Kennung (24 Zeichen Printable String)
I=	Initialen (Initials, 5 Zeichen Printable String)
Q=	Generation (Generation Qualifier, 3 Zeichen Printable String)
DDA:Typ=Wert	Domain Defined Attributes (Typ mit 8 Zeichen = Wert mit 128 Zeichen, beide Printable oder Teletex String , z.B. dda:service=fax)

Die möglichen Werte bei Printable String sind im Anhang D angeführt.

Bei einer X.400 Adresse sind folgende Regeln zu beachten:

1. Neben dem GDI (Global Domain Identifier), der sich aus Country Name, ADMD-Namen und PRMD-Namen zusammensetzt und somit einen Mailservice/ein Mailsystem definieren, muss mindesten ein zusätzliches Adressfeld angegeben werden, dass den Empfänger/ die Mailbox eindeutig definiert. Üblicherweise ist dies der Nachname (Surname S), der Commonname (CN) oder aber die Boxkennung (Unique Agent ID → UA-ID).
2. Die Boxkennung definiert eine Mailbox eindeutig und kann deshalb alternativ zu einer mnemonischen Adresse, die aus Namen und Organisationselementen besteht, genutzt werden.
3. Bei mnemonischen Adressen müssen unter Umständen mehrere Adressfelder angegeben werden, um den Empfänger eindeutig zu adressieren
4. Surname, Givenname, Initials und Generation Qualifier werden auch unter der Bezeichnung Personal Name (PN) zusammengefasst. Dieser Personal Name wird vor allem beim SMTP-Gateway eingesetzt, wenn dieses X.400 Adressen in SMTP-Mitteilungen abbilden muss.

Besonderheiten bei den Adressen des MailBox Service von *BusinessMail X.400*

1. Im Gegensatz zu anderen X.400 Systemen muss beim MailBox Service die Empfängeradresse nur eindeutig sein, damit die Mitteilung ausgeliefert wird. Es müssen nicht alle Adressfelder angegeben werden, die der Mailbox des Empfängers in der Datenbank zugeordnet wurden. Die Nutzung einer verkürzten Adresse ist aber mit dem Risiko versehen, dass durch das Einrichten einer neuen Mailbox die Eindeutigkeit verloren geht und Mitteilungen somit zurückgewiesen werden. Es ist zu empfehlen, immer die vollständigen Adressen zu nutzen oder aber Benutzer des MailBox Service direkt über die User-ID (MessageGate übernimmt die aktuelle Adresse aus der Datenbank) oder die Unique Agent-ID (Boxkennung in X.400 Adresse) zu adressieren, da diese Adresse immer eindeutig ist.

2. Wenn ein Partner im Internet adressiert werden soll, der nur SMTP-Mailtransfer unterstützt, muss die Mitteilung über das Internet Gateway versendet werden. Dieser Gateway Service wird über die GDI „c=de“ und „a= viat-smtp“ angesprochen. Um die Regeln von X.400 nicht zu verletzen, muss der Nachname des Empfängers im Feld „S=“ (Surname) und falls vorhanden auch der Vorname im Feld „G=“ (Givenname) eingetragen werden. Die eigentliche Internet-Adresse wird aber in einem DDA-Feld übergeben. Der Typ des Feldes lautet „rfc-822“ und der Wert beinhaltet die Internet-Adresse. Zu beachten ist, dass das „@“ kein gültiges Zeichen beim Printable String ist und deshalb durch „(a)“ ersetzt werden muss.

Bsp.

```
"c=de; a=viat-smtp; g=hans; s=meier; DDA:rfc-822=hans.meier(a)telekom.de" <x@viat.de>
```

3. Wenn an einen Partner ein Telefax versendet werden soll, muss die Mitteilung über das Telefax Gateway versendet werden. Dieser Gateway Service wird über die GDI „c=de“ und „a=viat“ angesprochen. Die Faxrufnummer muss im Feld „X121=“ übergeben werden und im DDA-Feld muss bei Typ „Service“ und bei Wert „Fax“ angegeben werden.

Bsp.

```
"c=de;a=viaT;X121=061519992725;DDA:service=fax" <x@viat.de>
```

Weitere Informationen zum Telefax Gateway können Sie über <https://www.service-viat.de> abrufen.

Anhang B: Fehlercodes

B1. Fehlercodes MessageGate Poller Prozess:

Reasoncode	Fehlertext	Beschreibung
0001	Invalid arguments	Ungültige Parameter oder Wert in verarbeiteter Datei
0002	Cannot separate sender ID	Interner Verarbeitungsfehler, bitte an Helpdesk wenden
0003	Invalid file name	Ungültiger Dateiname (muss mit M, R, S oder T anfangen)
0004	File-OrderID too long	Auftrags ID ist länger als 26 Zeichen und kann nicht verarbeitet werden
0005	Cannot open file	Datei ist noch vom Übertragungsprozess blockiert, bitte zunächst Datei immer mit Extension "*.tmp" vollständig übertragen und dann erst umbenennen
0006	Cannot create file	Interner Verarbeitungsfehler, bitte an Helpdesk wenden
0007	Invalid HDR in file	Interner Verarbeitungsfehler, bitte an Helpdesk wenden
0008	Error writing bodypart file	Interner Verarbeitungsfehler, bitte an Helpdesk wenden
0009	Error writing header file	Interner Verarbeitungsfehler, bitte an Helpdesk wenden
0010	Cannot move	Interner Verarbeitungsfehler, bitte an Helpdesk wenden
0011	Wrong parameter specified	Datei enthält unzulässige Werte
0012	Empty file	Datei ist leer. Bitte Datei immer mit Extension "*.tmp" vollständig übertragen und dann erst umbenennen
0013	Invalid content in status request file	Abfrage für Statusreport enthält unzulässige Werte
0014	Invalid msg type	Ungültige Syntax bei Mitteilungsdtei
0015	Missing header element To:	Pflichtfeld Empfänger fehlt
0016	Invalid SMTP address	Adresse bei TO: oder FROM: ist fehlerhaft oder nicht vollständig (Alias fehlt oder SMTP-Adressteil fehlt)
0017	Missing header element Content-Type:	Pflichtfeld Definition Nutzdaten fehlt
0018	Missing header element Content-Transfer-Encoding:	Pflichtfeld Definition Encoding Nutzdaten fehlt

9999	Status report request ignored	Anforderung Status Report wurde verworfen, da innerhalb der konfigurierten Sperrfrist eingestellt.
------	-------------------------------	--

B2. MessageGate Errorcode im Statusreport

Errorcode	Internal Textsymbol	Beschreibung
134250499	SHM_EXISTS	shared memory already exists>
134250500	SHM_NOT_EXISTS	shared memory does not exist>
134250501	PRC_DULPNAM	process name %s already exists>
134250505	ATTRIB_INVALID	invalid or unsupported attribute>
134250506	BUFFER_EMPTY	buffer is empty>
134250507	BUFFER_OVERFLOW	buffer overflow>
134250508	BUFFER_TOO_SMALL	buffer too small for primitive>
134250509	NO_BUFFER	no buffer>
134250510	CHECKSUM_INVALID	invalid checksum: %s>
134250511	CLASS_EMPTY	pom_class holds no elements>
134250512	CLASS_END	end of class reached>
134250513	CLASSCTX_NULL	internal error: class context is null>
134250514	CLASSCTX_INVALID	internal error: invalid class context>
134250515	DESCR_NOT_FOUND	descriptor %s not found>
134250516	NO_DEVICE	no device available>
134250517	DIR_CREATE	cannot create directory %s>
134250518	DIR_NAME_INVALID	directory name invalid %s>
134250519	DIR_NOT_FOUND	directory not found %s>
134250520	DIR_NO_ACCESS	no access to directory %s>
134250521	DISK_FULL	disk is full %s>
134250522	DISK_NAME_INVALID	invalid disk name %s>
134250523	DISK_NOT_FOUND	disk not found %s>
134250524	DISK_NO_ACCESS	no access to disk %s>
134250525	DS_INIT	DS API function ds_init failed>
134250526	DS_SHUT	DS API function ds_shut failed>
134250527	DS_BIND	DS API function ds_bind failed>
134250528	DS_UNBIND	DS API function ds_unbind failed>
134250529	DS_ADD_ENTRY	DS API function ds_add_entry failed>
134250530	DS_MODIFY_ENTRY	DS API function ds_modify_entry failed>
134250531	DS_REMOVE_ENTRY	DS API function ds_remove_entry failed>
134250532	DS_SEARCH	DS API function ds_search failed>
134250533	ELEM_LENGTH_MISS	tried pom_write on an element created without length>
134250534	ELEM_NOT_FOUND	cannot find element of specified type %s>
134250535	ELEM_READONLY	tried to modify readonly element %s>
134250536	ELEM_NOT_PRESENT	element not present>
134250537	ELEM_MULTI_VALUED	element is multi-valued>
134250538	ENCOD_ANY	ANY syntax found in %s>
134250539	ENCOD_END	end of encoding; %s>

134250540	ENCOD_EXCEEDED	encoding exceeds 4 bytes length>
134250541	ENCOD_INVALID	invalid encoding; %s>
134250542	ENCOD_EOC_EXPECTED	expected EOC; %s>
134250543	ENCOD_INCOMPLETE	incompleted decode; %s>
134250544	ENCOD_LENGTH	element length exceeded; %s>
134250545	ENCOD_EMPTY	tried to encode an empty primitive; %s>
134250546	ENCOD_MANDATORY	missing mandatory element; %s>
134250547	ENCOD_LIMIT	limit exceeded; %s>
134250548	UNSUP_EXTID	ExtensionId %s is not supported>
134250549	ENTITY_ACCESS	invalid access method for entity>
134250550	ENTITY_ATTR	invalid type %s of entity attribute>
134250551	ENTITY_TYPE	invalid entity type>
134250552	ENTITY_SLOT_INV	invalid slot number %s for entity>
134250553	ENTITY_SLOT_NOFR	no slot free for entity>
134250554	ENTITY_TYPE_ATTR	expected attribute TYPE>
134250555	ENTITY_CMD_NOTSUPP	command not supported>
134250556	ENTITY_RESTART	can not restart entity %s>
134250557	ENTITY_ATTR_TAB	attribute description not found>
134250558	ENTITY_DUPLNAM	name for entity already exists>
134250559	ENTITY_MGMT	Master not active>
134250560	ENTITY_NOT_EXIST	entity not exist>
134250561	ENTITY_WILDCARD	wildcard not supported>
134250562	ENTITY_CREATE	can not create entity %s>
134250563	ENTITY_LIMIT	Entity %s exceeds restarting limit>
134250564	MGMT_SHUTDOWN	OMS system is down>
134250565	ENTITY_NORESTART	restarting not allowed>
134250566	ENTITY_ABNORMAL	Entity %s terminated abnormally>
134250567	ENTITY_ERROR	Entity %s terminated due to an er- ror>
134250568	ENTRY_NOT_FOUND	found no or no more entry>
134250569	ENTRY_IGNORE	ignore this entry>
134250570	ENTRY_EXISTS	entry already exists>
134250571	ENTRY_ISCHILD	cannot delete child-entry without its parent>
134250572	ENTRY_SELECT	entry selected by MSK>
134250573	ENV_LOG	environment/logical %s not set>
134250574	EXPR_EMPTY	%s-expression is empty>
134250575	FEAT_NOT_SUPP_YET	feature not supported yet>
134250576	FILE_CONNECT	cannot connect to record access block of file %s>
134250577	FILE_CREATE	cannot create file %s>
134250578	FILE_DELETE	cannot delete file %s>
134250579	FILE_END	end of file detected %s>
134250580	FILE_BEGIN	beginning of file detected %s>
134250581	FILE_FREE	cannot release lock (possibly not set), file: %s>
134250582	FILE_LENGTH	attempt to read past end of file %s>
134250583	FILE_LOCK	cannot lock file %s>
134250584	FILE_NAME_INVALID	invalid filename %s>

134250585	FILE_NO_SUCH	no such file: %s>
134250586	FILE_OPEN	cannot open file %s>
134250587	FILE_READ	error reading on file %s>
134250588	FILE_SEEK	cannot seek to file position, file: %s>
134250589	FILE_TRUNCATE	cannot truncate file %s>
134250590	FILE_WRITE	error writing to file %s>
134250591	FILE_PARTIAL	cannot read as many bytes as asked for>
134250592	FUNC_NOT_IMPLM	function %s not implemented>
134250593	FUNC_SDS_NOT_EXIST	this function will never exist>
134250594	FUNC_SEQUENCE	invalid sequence of function-calls>
134250595	IPC_KEY	invalid key name %s>
134250596	IPC_LOCK_NOT_GRANT	lock not granted>
134250597	IPC_MBX_REMOVED	message queue is removed>
134250598	IPC_CREATION	process creation error (%s)>
134250599	IPC_MBX	message queue error (%s)>
134250600	IPC_LOCK	locking error (%s)>
134250601	IPC_SHM	shared memory error (%s)>
134250602	IPC_LNM	logical name error (%s)>
134250603	IPC_NO_LOGTAB	logical name table %s for mailbox does not exist>
134250604	IPC_NO_PRIV	insufficient privilege for IPC operation>
134250605	IPC_USRQUOTA	quota of user %s failed (%s)>
134250606	IPC_USER_UNKNOWN	user %s unknown>
134250607	IPC_LOGNAM	error on logical name passed through VMS funtion>
134250608	LOCSUBM_VIOLATED	non local submission>
134250609	MATCH_INAPPR	inappropriate matching>
134250610	MEMORY_INSUFF	no memory>
134250611	MODE_LOCK_UNKNOWN	unknown locking mode %s>
134250612	MODE_OPER_UNKNOWN	got unknown operation mode %s>
134250613	MSG_CONTENT_LONG	content too long>
134250614	MSG_CONTENT_MULTI	more than one content>
134250615	MSG_CONTENT_NONE	content missing>
134250616	MSG_ENV_MISS	envelope missing>
134250617	MSG_ENV_WHAT	unknown element in envelope>
134250618	MSG_IFC_NONE	child entry without IFC entry encountered>
134250619	MSG_MISSING	message missing>
134250620	MSG_NOT_REC	no message received>
134250621	MSG_NOT_SEND	no message sent>
134250622	MSG_ORIGIN_MULTI	more than one originator>
134250623	MSG_ORIGIN_NONE	originator missing>
134250624	MSG_ORR_MULTI	more than one originator report requested>
134250625	MSG_ORR_NONE	no originator report requested>
134250626	MSG_RECIP_NONE	recipient missing>
134250627	MSG_RECNAME_MULTI	more than one recipient name>
134250628	MSG_RECNAME_NONE	no recipient name>
134250629	MSG_REPORT_WHAT	unknown element in report>

134250630	MSG_ORIGIN_INVALID	invalid message originator>
134250631	MTA_CANCEL	MTA function ma_cancel failed,%s>
134250632	MTA_CLOSE	MTA function ma_close failed,%s>
134250633	MTA_FINISH_DEL	MTA function ma_finish_delivery failed,%s>
134250634	MTA_NOT_AVAIL	MTA not available>
134250635	MTA_NO_MPDU	MTA has not MPDU %s>
134250636	MTA_OPEN	MTA function ma_open failed,%s>
134250637	MTA_START_DEL	MTA function ma_start delivery failed,%s>
134250638	MTA_SUBMIT	MTA function ma_submit failed,%s>
134250639	MTA_WAIT	MTA function ma_wait failed,%s>
134250640	MTA_AGENTNAME	MTA agent name invalid>
134250641	OCOM_PORT_INVALID	Invalid port number>
134250642	OCOM_FREE	The osak has queued the request. There is free block>
134250643	OCOM_QUEUED	The osak has queued the request>
134250644	OCOM_DISRUPTED	A disruptive event has occurred>
134250645	OCOM_INVAEI	The application entity invocation is invalid>
134250646	OCOM_INVDEFCTXT	The default context response is invalid>
134250647	OCOM_INVFUNC	The call is invalid>
134250648	OCOM_INVFUS	The functional units are invalid>
134250649	OCOM_INVID	The activity identifier is too long>
134250650	OCOM_INVPCTXT	The presentation context list is invalid>
134250651	OCOM_INVSYNCPNT	The synchronization point serial number is invalid>
134250652	OCOM_NOPROCINFO	The is no process-id and no process-name>
134250653	OCOM_NOSYNCPNT	The synchronization point serial number is missing>
134250654	OCOM_TRANSERR	There is error in transport provider>
134250655	OCOM_NOEVENT	There is no event>
134250656	OCOM_INCPCI	The PCI is not complete>
134250657	OCOM_INSFWS	There is not enough workspace in the parameter block>
134250658	OCOM_NOBUFFERS	There are not enough user data buffers>
134250659	OCOM_OVERFLOW	Too much user data has been sent for session v-1>
134250660	OCOM_INVTOKEN	The token setting is invalid>
134250661	OCOM_INVEVENT	There is invalid event>
134250662	OM_CREATE	Object Management function om_create failed,%s>
134250663	OM_DELETE	Object Management function om_delete failed,%s>
134250664	OM_GET	Object Management function om_get failed,%s>
134250665	OM_INSTANCE	Object Management function

		om_instance failed,%s>
134250666	OM_PUT	Object Management function om_put failed,%s>
134250667	OM_READ	Object Management function om_read failed,%s>
134250668	OM_WRITE	Object Management function om_write failed,%s>
134250669	OPER_UNKNOWN	Operation %s is unknown>
134250670	PARAM_INVALID	invalid parameter %s>
134250671	PARAM_NULL	parameter %s was a NULL pointer>
134250672	LENGTH_INVALID	invalid length %s>
134250673	PORT_INVALID	invalid port %s>
134250674	PRIV_MISSES	process misses privilege>
134250675	PVERS_INVALID	protocol version invalid>
134250676	QUEUE_EMPTY	empty queue>
134250677	QUOTA_EXHAUSTED	process quota exhausted>
134250678	RANGE_REVERSED	range reversed>
134250679	RANGE_NOTVALID	range out of bounds>
134250680	RESTR_EXCEEDED	restrictions exceeded>
134250681	RULE_UNKNOWN	rule %s is unknown>
134250682	SERVER_BUSY	server is busy>
134250683	SERVER_DOWN	server is down>
134250684	SIGNAL_NOT_SUPP	Signal (interrupt) is not supported: %s>
134250685	SQL_ERROR	SQL error: %s>
134250686	STATE_INVALID	current facility state does not allow this operation>
134250687	STATUS_NEW_DEL	tried to delete a NEW-message>
134250688	STATUS_CHANGE	change from actual status to given is not supported>
134250689	STATUS_UNKNOWN	status %s is not known>
134250690	STRUCT_USER_ERROR	got wrong structures from user agent>
134250691	SYNTAX_DIFFERENT	different OM_syntax between pom_add and pom_write>
134250692	SYNTAX_UNKNOWN	given OM_syntax %s is unknown>
134250693	SYNTAX_ERROR	syntax error>
134250694	TABLE_FULL	table overflow>
134250695	TABLE_UNKNOWN	tried to lock an unknown MDB-table %s>
134250696	TAG_TOO_BIG	tag too big .gt. 4 bytes>
134250697	TRANSACTION_INACTIVE	Transaction %s inactive>
134250698	TRANSACTION_ACTIVE	Transaction %s active>
134250699	TRANSACTIONID_WRONG	Transaction Id %s wrong>
134250700	TYPE_DIFFERENT	different OM_type between pom_add and pom_write>
134250701	USER_AMBIGUOUS	user name is ambiguous>
134250702	USER_NEW_NOT_SPEC	existing user name has same elements plus some other>
134250703	USER_OLD_NOT_SPEC	existing user name has same elements but fewer>

134250704	USER_PWD_INVALID	invalid password given by user>
134250705	USER_UNKNOWN	user name is unknown>
134250706	USER_DOUBLE_LOGIN	user is already logged in %s>
134250707	USER_ACTIV_NOT_DEL	cannot delete user with status ACTIVE>
134250708	USER_NAME_NOT_MOD	orname elements modify only single user>
134250709	USER_PWD_EXPIRED	user password expired>
134250710	USER_SRVC_EXPIRED	user service expired>
134250711	USER EDI_DENIED	no agreement between EDI sender and receiver>
134250712	USER EDI_NO_SND	Sending Partner not found>
134250713	USER EDI_NO_REC	Receiving Partner not found>
134250714	USER EDI_NO_AGROP	Agreement for open receiver not found>
134250715	USER EDI_NO_AGRCL	Agreement for closed receiver not found>
134250716	USER_MAX_LOGIN_FAILS	maximum login fails reached>
134250717	DOMAIN_AMBIGUOUS	domain name is ambiguous>
134250718	ORNAME_INVALID	no valid addressing form specified>
134250719	USER EDI_NO_RUT	Routing Partner not found!>
134250720	USER_DISCONNECT_NOT_DEL	cannot delete user with status DISCONNECTED>
134250721	VERSION_INVALID	version invalid>
134250722	VALUE_TOO_BIG	value too long>
134250723	WRONG_VALUE	wrong values: %s>
134250724	WRONG_VALUE_TYPE	value type is unknown: %s>
134250725	WRONG_VALUE_LENGTH	value length is incorrect>
134250726	WRONG_VALUE_NUMBER	digits in value is not a number>
134250727	WRONG_VALUE_MAKEUP	make-up of value is wrong>
134250728	WRONG_VALUE_RANGE	value out of range>
134250729	WRONG_VALUE_SYNTAX	wrong value syntax>
134250730	WILDCARD_INVALID	wildcard not allowed>
134250731	DECODE_END	end of decoding>
134250732	NO_SUCH_SND	no such sender>
134250733	NO_SUCH_REC	no such recipient>
134250734	TP_AMBIGUOUS	trading partner is ambiguous>
134250735	NO_SUCH_RUT	no such router>
134250736	NO_DEFAULT_VALIDFOR	no default validfor-entry available>
134250737	HAVE_SPECIAL_VALIDFOR	special validfor-entries still exist>
134250738	LOGONNAME_AMBIGUOUS	logonname is ambiguous>
134250739	MANDATORY_ATTRIBUTE	mandatory attribute missing>
134250740	MANDATORY_SECTION	mandatory section missing>
134250741	MANDATORY_TABLE	mandatory table missing>
134250742	BCKP_PURG	Backup/Purger/Repair cannot run parallel>
134250743	TIME_RELATIVE	cannot convert relative time into UTC format>
134250744	CFG_TOKEN_UNKNOWN	found unknown token in config file>
134250745	CFG_TOKEN_AMBIGUOUS	found ambiguous token in config

		file>
134250746	CFG_SYNTAX	found token without '=' in config file>
134250747	CFG_VALUE_UNKNOWN	value not found in conversion table>
134250748	CFG_VALUE_AMBIGUOUS	value has ambiguous conversion>
134250749	CFG_VALUE_SYNTAX	syntax error in config file>
134250750	CFG_VALUE_NOTMULTI	config value is not multi valued>
134250751	CFG_TABLE_SYNTAX	error in conversion table>
134250752	EDPRS_INVIC	invalid interchange syntax>
134250753	EDPRS_INVTRAIL	invalid interchange trailer>
134250754	EDPRS_INVHEAD	invalid interchange header>
134250755	EDPRS_RUBBISH	too many useless characters>
134250756	EDPRS_CTRLREF	control reference mismatch>
134250757	EDPRS_TAGLONG	found too long EDI tag>
134250758	EDPRS_ELEMLONG	found too long EDI element>
134250759	EDPRS_TOOMANYIC	too many Interchanges>
134250760	PARSE_BREAK	break current parsing>
134250761	UTL_LOCK_CREATE	Lock create failed>
134250762	UTL_LOCK_DESTROY	Lock destroy failed>
134250763	UTL_LOCK	Locking failed>
134250764	UTL_UNLOCK	Unlocking failed>
134250765	POMSORT_IGNORED	pom type %s ignored (reflist: %s)>
134250766	STOP_RESOURCE	out of resources>
134250767	ADDINFO	Additional info: %s>
134250768	RSC_NOT_FOUND	Resource information not found>
<p>Unter bestimmten Umständen wird statt des MessageGate Fehlers auch der von anderen Modulen der Hostapplikation angezeigt (nachfolgende Beispiel). Bitte diesen Fehlercode zur Analyse an den Helpdesk melden.</p>		
159416462		MTA function ma_submit failed,%s

B3. MTA Errorcode (Non Delivery) im Statusreport

Fehlercode bei NDN:

Reasoncode	X.400 Standard	Beschreibung
0	Transfer-failure	Probleme bei MTA-Interkommunikation
1	Unable-to-transfer	Probleme bei der Behandlung der Mitteilung durch zuständigen MTA
2	Conversion-not-performed	Konvertierung konnte nicht durchgeführt werden
3	Physical-rendition-not-performed	Anlieferung über das Gateway zum Briefdienst nicht möglich
4	Physical-delivery-not-performed	Auslieferung an das Gateway zum Briefdienst nicht möglich
5	Restricted-delivery	Eingeschränkte Auslieferung
6	Directory-operation-unsuccessful	X.500 Verzeichnisabfrage nicht erfolgreich
7	deferred-delivery-not-performed	Verzögerte Auslieferung nicht möglich
8	transfer-failure-for-security-reason	Übertragung aus Sicherheitsgründen nicht möglich
99	MessageGate Poller Error (non-standard)	Kein Wert aus X.400 Standard: Fehler bei Bearbeitung einer Datei (.in) durch MessageGate Poller. Beim Diagnostic Code wird dann der Poller Fehlercode (siehe B1.) angezeigt

Beschreibung für die Ursache der Nichtauslieferung bei NDN

Diagnostic Code	X.400 Standard	Beschreibung
0	Unrecognized-OR-name	Adresse unbekannt
1	Ambiguous-OR-name	Adresse nicht eindeutig
2	MTS-congestion	Überlastung des Message Transfer Systems
3	Loop-detected	Schleife im Message Transfer System entdeckt
4	Recipient-unavailable	Empfänger (-mailbox) ist nicht erreichbar
5	Maximum-time-expired	Maximale Auslieferzeit überschritten
6	Encoded-Information-	Mitteilungsdefinitionen nicht un-

	Types-unsupported	terstützt
7	Content-too-long	Mitteilung ist zu groß
8	Conversion-impractical	Notwendige Konvertierung unmöglich
9	Implicit-conversion-prohibited	Notwendige Konvertierung durch Absender verboten
10	Implicit-conversion-not-subscribed	Notwendige Konvertierung ist für diesen Empfänger nicht vereinbart
11	Invalid-arguments	Ungültiger Inhalt bzw. ungültige Parameter
12	Content-Syntax-error	Syntax Fehler in Mitteilung
13	Size-constraint-violation	Länge eines oder mehrerer Parameter überschreitet die in der Empfehlung angegebenen Werte
14	Protocol-violation	Notwendiger Parameter nicht vorhanden
15	Content-type-not-supported	Typ von Anhang nicht unterstützt
16	Too-many-recipients	Zu viele Empfänger angegeben
17	No-bilateral-agreement	Notwendige Vereinbarung für die Auslieferung der Mitteilung nicht vorhanden
18	Unsupported-critical-function	Für den Transfer der Mitteilung notwendige Funktion wird nicht unterstützt
19	Conversion-with-loss-prohibited	Notwendige Konvertierung wurde durch Absender verboten, da Inhalt verändert würde
20	Line-too-long	Informationsverfälschung, da Zeile zu lang
21	Page-split	Informationsverfälschung, da Textinhalte auf Seiten aufgeteilt werden müssten
22	Pictorial-symbol-loss	Informationsverfälschung, da ein oder mehrere Bildsymbole verloren gehen
23	Punctuation-symbol-loss	Informationsverfälschung, da ein oder mehrere Satzzeichen verloren gehen
24	Alphabetic-character-loss	Informationsverfälschung, da ein oder mehrere Schriftzeichen verloren gehen
25	Multiple-information-loss	Informationsverfälschung
26	Recipient-reassignment-	Mitteilung konnte nicht ausgeliefert werden, da der Absender

	prohibited	das Umleiten an einen alternativen Empfänger verboten hatte
27	Redirection-loop-prohibited	Mitteilung konnte nicht ausgeliefert werden, da das Umleiten an einen alternativen Empfänger zu einer Schleife geführt hat
28	DI-expansion-prohibited	Mitteilung konnte nicht ausgeliefert werden, da der Absender das Aufgliedern der Empfänger anhand einer Verteilerliste verboten hatte
29	No-dl-submit-permission	Mitteilung konnte nicht ausgeliefert werden, da der Absender nicht das Recht hat, Verteilerlisten zu adressieren
30	DI-expansion-failure	Fehler beim Aufgliedern einer Verteilerliste
31	Physical-rendition-attributes-not-supported	Gateway zum Briefdienst unterstützt die angeforderten Leistungsmerkmale nicht
32	Undeliverable-mail-physical-delivery-address-incorrect	Gateway zum Briefdienst meldet ungültige Empfängeradresse
33	Undeliverable-mail-physical-delivery-office-incorrect-or-invalid	Gateway zum Briefdienst meldet ungültige Auslieferstelle
34	Undeliverable-mail-physical-delivery-address-incomplete	Gateway zum Briefdienst meldet unvollständige Empfängeradresse
35	Undeliverable-mail-recipient-unknown	Gateway zum Briefdienst meldet unbekannte Empfängeradresse
36	Undeliverable-mail-recipient-deceased	Gateway zum Briefdienst meldet Empfänger verstorben
37	Undeliverable-mail-organisation-expired	Gateway zum Briefdienst meldet Empfänger nicht mehr vorhanden
38	Undeliverable-mail-recipient-refused-to-accept	Gateway zum Briefdienst meldet Empfänger hat Annahme verweigert
39	Undeliverable-mail-recipient-did-not-claim	Gateway zum Briefdienst meldet Empfänger hat Mitteilung nicht abgeholt
40	Undeliverable-mail-recipient-changed-address-permanently	Gateway zum Briefdienst meldet Empfänger hat Adresse dauerhaft geändert und Weiterleiten ist nicht möglich
41	Undeliverable-mail-	Gateway zum Briefdienst meldet

	recipient-changed-address-temporarily	Empfänger hat Adresse zeitlich begrenzt geändert und Weiterleiten ist nicht möglich
42	Undeliverable-mail-recipient-changed-temporary-address	Gateway zum Briefdienst meldet Empfänger hat zeitlich begrenzte Adresse aufgegeben und Weiterleiten ist nicht möglich
43	Undeliverable-mail-new-address-unknown	Gateway zum Briefdienst meldet Empfänger ist umgezogen und neue Adresse unbekannt
44	Undeliverable-mail-recipient-did-not-want-forwarding	Gateway zum Briefdienst meldet Empfänger hat ein notwendiges Weiterleiten untersagt
45	Undeliverable-mail-originator-prohibited-forwarding	Gateway zum Briefdienst meldet Absender hat notwendiges Weiterleiten untersagt
46	Secure-messaging-error	Mitteilung kann nicht ausgeliefert werden, da dies die Sicherheitsrichtlinien verletzt
47	Unable-to-downgrade	Mitteilung kann nicht ausgeliefert werden, da Konvertierung auf älteren Standard nicht möglich
48	Unable-to-complete-transfer	Übertragung konnte nicht abgeschlossen werden (z.B., weil die Mitteilung zu groß ist)
49	Transfer-attempts-limit-reached	Maximale Anzahl der Verbindungsversuche für den Mitteilungstransfer ist überschritten
50	Incorrect-notification-type	In Mitteilung definierter Reporttyp stimmt nicht mit dem Inhalt der Mitteilung überein
51	DI-expansion-prohibited-by-security-policy	Mitteilung konnte nicht ausgeliefert werden, da das Aufgliedern der Empfänger anhand einer Verteilerliste durch eine Sicherheitsregel verboten wurde
52	Forbidden-alternate-recipient	Mitteilung konnte nicht ausgeliefert werden, da das Umleiten an einen alternativen Empfänger durch eine Sicherheitsregel verboten wurde
53	Security-policy-violation	Verletzung einer Sicherheitsregel
54	Security-services-refusal	Die angeforderten Sicherheitsmerkmale sind nicht verfügbar
55	Unauthorised-dl-member	Mitteilung konnte nicht ausgeliefert werden, da ein Empfänger der Verteilerliste nicht adressiert

		werden darf
56	Unauthorised-dl-name	Mitteilung konnte nicht ausgeliefert werden, da der Absender die Verteilerliste nicht adressieren darf
57	Unauthorised-originally-intended-recipient-name	Weiterleitung oder Verteilung innerhalb einer DL ist für diese Empfängeradresse nicht erlaubt
58	Unauthorised-originator-name	Der Absender ist nicht autorisiert, die Mitteilung auszuliefern
59	Unauthorised-recipient-name	Der Empfänger ist nicht autorisiert, diese Mitteilung zu erhalten
60	Unreliable-system	Weiterleitung an ein System, das Sicherheitsmerkmale nicht unterstützt, wurde abgelehnt
61	Authentication-failure-on-subject-message	Integrität der Mitteilung nicht sichergestellt
62	Decryption-failed	Inhalt der Mitteilung konnte nicht entschlüsselt werden
63	Decryption-key-unobtainable	Kein Schlüssel zum Entschlüsseln der Mitteilung vorhanden
64	Double-envelope-creation-failure	Der MTA konnte die Mitteilung nicht gesichert übertragen
65	Double-enveloping-message-restoring-failure	Der MTA konnte die ursprüngliche Mitteilung nicht wiederherstellen
66	Failure-of-proof-of-message	Fehler beim Bearbeiten der Proof-of Sicherheitsmerkmale
67	Integrity-failure-on-subject-message	Fehler beim Bearbeiten der Integritätscheck Sicherheitselemente
68	Invalid-security-label	Ungültiges Sicherheitsmerkmal
69	Key-failure	Der notwendige Schlüssel ist nicht vorhanden
70	Mandatory-parameter-absence	Notwendiges Sicherheitselement nicht vorhanden
71	Operation-security-failure	Übertragung oder Auslieferung der Mitteilung aus Sicherheitsgründen nicht möglich
72	Repudiation-failure-of-message	Mitteilung wurde nicht mit einer qualifizierten Signatur versehen
73	Security-context-failure	Benutzte Sicherheitsmerkmale sind nicht kompatibel zu den Sicherheitsregeln
74	Token-decryption-failed	Token konnte nicht entschlüsselt

		werden
75	Token-error	Fehler beim Zugriff auf das Token
76	Unknown-security-label	Unbekannte Sicherheitsmerkmale
77	Unsupported-algorithm-identifier	Zum Sichern der Mitteilung verwendeter Algorithmus wird nicht unterstützt
78	Unsupported-security-policy	Angeforderte Sicherheitsmerkmale werden nicht unterstützt
-1	No Diagnostic code in NDN	Dieser Wert wird vom MTA zurückgeliefert, wenn die NDN entgegen den Vorgaben des Standards keinen Diagnostic code enthält

B4. X.400 User Agent Errorcode (Non Receipt) im Statusreport

Fehlercode bei NRN:

Codenummer	X.400 Standard	Beschreibung
0	IPM-discarded	Mitteilung wurde verworfen
1	IPM-auto-forwarded	Mitteilung wurde automatisch weitergeleitet und eine Verarbeitung ist nicht sichergestellt

Grund für das Verwerfen von Mitteilungen:

Codenummer	X.400 Standard	Beschreibung
0	IPM-expired	Mitteilung ist abgelaufen
1	IPM-obsolete	Mitteilung ist ungültig
2	User-subscription-terminated	Vertragsverhältnis mit Empfänger ist gekündigt

B5. Umsetzregel bei Fehlercodes DN zu DSN

X.400 Reason code	X.400 Diagnostic Code	X.400 Standard	SMTP Action
6	0	Unrecognized-OR-name	5.1.1
6	1	Ambiguous-OR-name	5.1.4
0	2	MTS-congestion	5.4.5
0	3	Loop-detected	5.4.6.
0	4	Recipient-unavailable	5.2.1
0	5	Maximum-time-expired	5.4.7
2	6	Encoded-Information-Types-unsupported	5.6.1
1	7	Content-too-long	5.3.4
2	8	Conversion-impractical	5.6.3
2	9	Implicit-conversion-prohibited	5.6.2
2	10	Implicit-conversion-not-subscribed	5.6.5
1	11	Invalid-arguments	5.5.4
1	12	Content-Syntax-error	5.5.2
1	13	Size-constraint-violation	5.5.0
1	14	Protocol-violation	5.5.0
1	15	Content-type-not-supported	5.6.1
1	16	Too-many-recipients	5.5.3
1	17	No-bilateral-agreement	5.7.1
1	18	Unsupported-critical-function	5.5.1
2	19	Conversion-with-loss-prohibited	5.6.5
2	20	Line-too-long	5.6.5
2	21	Page-split	5.6.5
2	22	Pictorial-symbol-loss	5.6.5
2	23	Punctuation-symbol-loss	5.6.5
2	24	Alphabetic-character-loss	5.6.5
2	25	Multiple-information-loss	5.6.5
1	26	Recipient-reassignment-prohibited	5.4.0
1	27	Redirection-loop-prohibited	5.4.0
1	28	DI-expansion-prohibited	5.7.2
1	29	No-dl-submit-permission	5.7.2
1	30	DI-expansion-failure	5.2.4
3	31	Physical-rendition-attributes-not-supported	5.0.0

4	32	Undeliverable-mail-physical-delivery-address-incorrect	5.0.0
4	33	Undeliverable-mail-physical-delivery-office-incorrect-or-invalid	5.0.0
4	34	Undeliverable-mail-physical-delivery-address-incomplete	5.0.0
4	35	Undeliverable-mail-recipient-unknown	5.0.0
4	36	Undeliverable-mail-recipient-deceased	5.0.0
4	37	Undeliverable-mail-organization-expired	5.0.0
4	38	Undeliverable-mail-recipient-refused-to-accept	5.0.0
4	39	Undeliverable-mail-recipient-did-not-claim	5.0.0
4	40	Undeliverable-mail-recipient-changed-address-permanently	5.0.0
4	41	Undeliverable-mail-recipient-changed-address-temporarily	5.0.0
4	42	Undeliverable-mail-recipient-changed-temporary-address	5.0.0
4	43	Undeliverable-mail-new-address-unknown	5.0.0
4	44	Undeliverable-mail-recipient-did-not-want-forwarding	5.0.0
4	45	Undeliverable-mail-originator-prohibited-forwarding	5.0.0
8	46	Secure-messaging-error	5.7.0
1	47	Unable-to-downgrade	5.6.5
0	48	Unable-to-complete-transfer	5.5.0
0	49	Transfer-attempts-limit-reached	5.4.0
1	50	Incorrect-notification-type	5.6.0
8	51	DI-expansion-prohibited-by-security-policy	5.7.2
8	52	Forbidden-alternate-recipient	5.7.0
8	53	Security-policy-violation	5.7.0
8	54	Security-services-refusal	5.7.0
8	55	Unauthorized-dl-member	5.7.0
8	56	Unauthorized-dl-name	5.7.2
8	57	Unauthorized-originally-intended-recipient-name	5.7.0
8	58	Unauthorized-originator-name	5.7.1

8	59	Unauthorised-recipient-name	5.7.0
8	60	Unreliable-system	5.7.3
8	61	Authentication-failure-on-subject-message	5.7.7
8	62	Decryption-failed	5.7.5
8	63	Decryption-key-unobtainable	5.7.5
8	64	Double-envelope-creation-failure	5.7.0
8	65	Double-enveloping-message-restoring-failure	5.7.0
8	66	Failure-of-proof-of-message	5.7.0
8	67	Integrity-failure-on-subject-message	5.7.0
8	68	Invalid-security-label	5.7.0
8	69	Key-failure	5.7.5
8	70	Mandatory-parameter-absence	5.7.0
8	71	Operation-security-failure	5.7.0
8	72	Repudiation-failure-of-message	5.7.0
8	73	Security-context-failure	5.7.0
8	74	Token-decryption-failed	5.7.5
8	75	Token-error	5.7.0
8	76	Unknown-security-label	5.7.0
8	77	Unsupported-algorithm-identifier	5.7.4
8	78	Unsupported-security-policy	5.7.4

Seite ist aus redaktionellen Gründen leer.

Anhang C: Beispiele für Mitteilungen und Reports

C1. Ausgelieferte Mitteilung mit Textanhang

Empfangene Mitteilung (M_5K00AG0HBDM0F2F9.OUT)

To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE" <49603@viaT.de>
 From: "G=ipm;S=tester;O=testag;A=viaT;C=de" <49637@viaT.de>
 Message-ID: 615 10/11/13
 X-MPDUID: 3D23437A11DCEC31170084BF
 Date: 13-Nov-2010 13:10:22 +0100
 Subject: Test mit Textbodypart
 Disposition-Notification-To: "G=ipm;S=tester;O=testag;A=viaT;C=de"
 MIME-Version: 1.0
 Content-Type: text/plain
 Content-Transfer-Encoding: 8bit

Test
 äöüÄÖÜß1234567890123456789012345678901234567890123456789012345678901
 234567890123456789012345678901234567890123456789012345678901234567890
 123456789012345678901234567890123456789012345678901234567890123456789
 01234567890123456789012345678901234567890

In dieser Mitteilung (Dateiname M_5K00AG0HBDM0F2F9.OUT) wurde eine Lesebestätigung angefordert, jedoch wurde keine Lesebestätigung versendet (siehe nachfolgende Beispiele für Reports).

C2. Ausgelieferte Mitteilung mit Binäranhang

Empfangene Mitteilung (M_5K00AG0HBDM0F2FA.OUT)

To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE" <49603@viaT.de>
 From: "G=ipm;S=tester;O=testag;A=viaT;C=de" <49637@viaT.de>
 Message-ID: 616 10/11/13
 X-MPDUID: 575BCBFB11DCEB9F1700C184
 Date: 13-Nov-2010 13:10:22 +0100
 Subject: Test mit Binäranhang
 Disposition-Notification-To: " G=ipm;S=tester;O=testag;A=viaT;C=de "
 MIME-Version: 1.0
 Content-Type: application/octet-stream
 Content-Disposition: attachment; filename="4d654d1d.zip"
 Content-Transfer-Encoding: binary

PK      tYr2ÄQa6÷   
 .
 .
 .
     4d654d1d.0PK       8  

In dieser Mitteilung (Dateiname M_5K00AG0HBDM0F2FA.OUT) wurde eine Lesebestätigung angefordert und es wurde eine Nicht Lesebestätigung versendet (siehe nachfolgende Beispiele für Reports).

C3. Ausgelieferte Mitteilung mit Multibodypart

Empfangene Mitteilung (M_5K00AG0HBDM0F2F8.OUT)

To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE" <49603@viaT.de>
 From: "G=ipm;S=tester;O=testag;A=viaT;C=de" <49637@viaT.de>
 Message-ID: 614 10/11/13
 X-MPDUID: 8B0663A011DCEC4417009682
 Date: 13-Nov-2010 13:10:22 +0100
 Subject: Test mit 3 Bodyparts
 Disposition-Notification-To: "G=ipm;S=tester;O=testag;A=viaT;C=de"
 MIME-Version: 1.0
 Content-Type: multipart/mixed; boundary="MG_=_CA610D0211DC91E900007CAD_=_MG"

--MG_=_CA610D0211DC91E900007CAD_=_MG
 Content-Type: text/plain
 Content-Transfer-Encoding: 8bit

Test äöüÄÖÜß

--MG_=_CA610D0211DC91E900007CAD_=_MG
 Content-Type: application/octet-stream
 Content-Disposition: attachment; filename="4d654d1d.zip"
 Content-Transfer-Encoding: binary

PK      tYr2ÄQa6÷   4d654d1d.0 "ls£: ...÷Tñ"ê¥Ói3xJU/\$!;DØb2xgd °1Ø

    4d654d1d.0PK       8  
 --MG_=_CA610D0211DC91E900007CAD_=_MG
 Content-Type: application/octet-stream
 Content-Transfer-Encoding: binary

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0062)https://securep7.viat-test.de/~0000001045/result/fetch_all.RES -->
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=windows-1252">
<META content="MSHTML 5.50.4930.1700" name=GENERATOR></HEAD>
<BODY><XMP>LOGIN::
.
.
.
</XMP></BODY></HTML>
```

 
 --MG_=_CA610D0211DC91E900007CAD_=_MG—

In dieser Mitteilung (Dateiname M_5K00AG0HBDM0F2F8.OUT) wurde eine Lesebestätigung angefordert und es wurde eine Lesebestätigung versendet (siehe nachfolgende Beispiele für Reports).

C4. Ausgelieferte Mitteilung mit Multirecipient

To: "G=edi;S=tester;O=testag;A=viat;C=de" <49638@viaT.de>
 To: "G=ipm;S=tester;CN=ipm tester;O=TESTAG;A=viat;C=DE" <49637@viaT.de>
 Cc: "G=ipm;S=testmiv;O=testag;A=viat;C=de" <23998@viaT.de>
 Cc: "G=EDI;S=TESTMIV;CN=EDI TESTMIV;O=TESTAG;A=VIAT;C=DE" <23999@viaT.de>
 Cc: "S=murxer;O=murx;A=viat;C=de" <X@viaT.de>
 Bcc: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE" <49603@viaT.de>
 From: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE" <49603@viaT.de>
 Message-ID: MGATE 0001 11/03
 X-MPDUID: 5758CA1B11E0498E00005292
 Date: 8 Mar 2011 14:14:12 +0100
 Subject: test Multi Recipients
 MIME-Version: 1.0
 Content-Type: text/plain
 Content-Transfer-Encoding: 8bit

test

Die Mitteilung wurde an sieben Empfänger versendet, wobei der eigene MessageGate Account dabei als Bcc: Empfänger adressiert wurde.

C5. Versendete Mitteilung ohne Anforderung Report

Versendende Mitteilung (M_Test_3_Body010.IN)

To: "" <49637@viat.de>
 Subject: test 3 ohne Leerzeile Bodyparts
 Message-Id: 260001 12/11/10 MGATE Test
 Date: Tue, 12 Nov 2010 13:16:24 +0100
 MIME-Version: 1.0
 Content-Type: multipart/mixed;
 boundary="-----_NextPart_000_0007_01C7E331.7A0CA460"
 Content-Transfer-Encoding: binary

-----_NextPart_000_0007_01C7E331.7A0CA460
 Content-Type: text/plain;
 charset="iso-8859-1"
 Content-Transfer-Encoding: 7bit

-----_NextPart_000_0007_01C7E331.7A0CA460
 Content-Type: application/x-pkcs12;
 name="hpm-webdav.p12"
 Content-Transfer-Encoding: base64
 Content-Disposition: attachment;
 filename="hpm-webdav.p12"

MIIKAQBAzCCCcGCSqGSIb3DQEHAaCCCbGEGgm0MIJSDCCBGcGCSqGSIb3DQEHBqCCBFgwggrU
 AgEAMIIETQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQlZnN9gMIQvocscAggAgIIILQGaNZr
 0IW6bN6jEdphtjnBzmCv8W9ipvE8wmpVxzUEwj5Mh226vHaBp2WtMBaHPSomsXFMPPEJJ9JFnF2S
 gPxDZVjUe5ImUB2EQDAopQEYLXJSX0YXh8uqnSD5Se4vuex+kunnb6o2nGXT8+Y9m3/uNCD9MEb6
 CGIA0JExtmWQJXkDeHDZjLjYiVcPcltNeMnc7EGH842jRGzS1umfOeSWb8+TcA2/uZtzaE9uIL7I
 LfD7dfIjz/4uawC+LstCfO984pFKR8vOxKIADBOn1CpuSIQFHHdgCZYVv1EHOdlmQbml+bJ2Gwx
 UPKDdUGdyK6G45JHZjuj4zDUSRXwfnrRmSUHAMZhUpRQwApPYyQo6zxdhd7NsdXpU7mDisNE/p6p
 0DNPTf97j/AiPWVMEwz0nsfITqF+4LONXVKia7Mp8o7Zzrn5XpwJ0/LP+47/+ZyCaClqB/qYtGlb
 xlgI04DFbS6xaoUu7iNh7ZSqnXNMRJREtBx/WVomChpYHuvVqitPWdsBpawNpUHs5uEXUopa0Uly
 XOn9ALfLE0t9v5FP4NE3xSHMPGSAc5iisH7Fys8g5Z+SGp3n9ynM8Jw97JhZfjKoQMqrMFzNL5FI
 ZUBVwNYOtUNXxKJ3L+1WtRXSEQgmfhptKZicCZKHozGZQ4Z8F4r9sA7wmS9CbljiNqImWlrvaMWE3
 fi6dzhrUOFIdu2LE7TI7+1Qmh/AcP3NVIUSUZIGJqqGc5i1BUmp3CJPo25xJ7zAek/YECJmQ5p9
 I+c2Ja60suKAlt6VfBcd747nIEQXdxYvi8cXQuezhVmvbBrX12Hg4ISioyEg5XFsd4DutZaxTuw
 gReDf8Hw/rMQfE6fhHilS7YirkqJt+q53uILMuN4sdV6u+nFsaoRYT84vTJZ30B5Wsh3Zs4T47r1

rTCn/BpQoQ8N62QF9zAPPL5AfctnDw/oZahJUqnQUNW7H86dLJ1ZkPJEICQ9quQSVjcMWZviliyr
 lnyeW0JE53V5N/38me3xV89f6iUkNvWg3catzHTH5Bay1E1NGVi9cYfuNJ+qsHMxegcu5h9UGiVX
 Z6AFQ5TOWPrObyOunVjUsGT8yIlcpHEBwilPFP4GXq30gt3H7S2sDZSbrrDUYeWgJBgwmJaEjo/z
 Pl67psBqnh4HKZoXAKSrfcF2JK2nt6q442tpIREVpkTXFGF6p7nqVvnP4RBD2LbFD/uzBxpchjR3
 62l6LZ75qjSf4hZHnAVCD7BtfPx3j3mg8flCp7ZyGRgSARpaLrYoMzbMXgIPFYUOqf8rug/AoCqB
 SD6OvMtvRfn5c3JceC9lZQ3/LGaqx7RGaUHYJaSXHPfCiozxtt2slw5nhWIFF1fgfJqVf2L41E2
 8f7pRyHPEjTBK1tozyHaWvsTm7kFm8FlIDCCBUEGCSqGSIb3DQEHAaCCBTIEggUuMIIKJCCBSYG
 CyqGSIb3DQEMCgECollE7jCCBOowHAYKKoZlhvcNAQwBAZAObAiZFPkQkLYL2wICCAAEGgTlcJfj
 y/4rcNs13Bxzac5e9bbDPqW6l6Cng7jB6vXjSPBNMMLL+7BcVKeSIWupmsQeQkvZGhdcbY7Najsk
 KE0EmaVVUPo1lgACKvZ2dc6nAVEeHbA14N1Zl2gCrvKZb1WHWj6NJ9e1xAKYzahVb5dkFNQIO8Y8
 dQXGyHJF6davx+nFdhnoo8wnOA8ntwpJggGJAw5xM7GLIV2Xy0wahfoKG53Jxwgsz/OiLX/uh/Vk
 c/kO+nKF4/au5igH9e18M6/l7A6kP854eXuMDWPXQHE35xAXrvt3gQd1D1n2wMGt/RyCDA1h4mNr
 Xwheql3nPScmwRRsC6JSxZ1dx3kr4Zrw7yRR9HJT7oCn5VjonsdMfEATqY1GLDKOw4LE30Za3bW
 kVSI3VzLxZx80WLcdiL9R1tn1FMbh/YJF52OCF1MqnZdKq/fEP6yUK260PI6mZCS1FLTHI00vN3
 +WPY8itoVb5qqPEHNC1Li3mCHHv7hLS9t6p+JM4+/y2G6MD8pPp/dnUxSidpbgIPV9/DQAMcx9P
 PgHX01HnF8b8r61sKZX0KzixjdxTSdur/A5ZVDtZBzM2etFcEt17O08tko31UmAC/XWe9p2mja1
 ft2NAM3Yqyjf03zT7jw4uLskwcnipcd0snbvlUY7prvn/7oBuTzklqmtvf9nfziyhNjByelytJyc
 qqE8Q+MplrbbWoUnQ2S1cg9zz38EVBIA6WGYvgsKeDAt1x1Zyol2InaCs4cXnZRR9HLZXL2hTW
 aPZ7BVRtYohdme/18XtJgzySggdAMqxOG3I+JiqXXa4M3a38TrndEjNzY9pHLA6Pi1R3liBZ4ZiB
 Ayo2Z42HiU83ZAsDxYTPbb2oYHgzijbvCQ7WomhefhTTV/q5S89FOEtIabYrjBdPliI+Q4GiPYin
 Aw/BgDTHhKx5FXZz8L8WTTwnlvZ0OXq6tQ9ZfiNblZJYth/C/pjSf2kLUH/bj8X8RHeXv3DfaOkn
 bryqx401gwIPx2JSpqcxX7kHroVxF+IYEHpfeEaTJ/650V3yUXmKAwL/CNxoHEqIj6QlppPRAzb7
 kqDFFX1Y/cVtKyQG7s7tHMVFFiEvn93MVri0hIReDxTEIhOQ6a/8D/laitiNO9nF4zATVI7nulxkg
 l2NU3iJMqrXNlpgnh63Z8phS74Q6RW5O8DtVXFDBVnviFiMUvBYxdt8bPLi/c9ZrXFjTr5ozSn2h
 4WSKCiRpdFZGU+u9a4Tr+sU8GZyrDf8QnOB0sUo6aqF3Bjbb2jUHqRgVX1UgmeDGuTZSW2qZY2DQ
 HIJMC7E1BjmVsyPlodJLFRN8hBZCseJwuQ/6dtDoITsrbPtFTNN2kvtpgly6voQYoiDWTyWxFCB8
 NE3hyhkeTtVB92VQ3hxPGvgAp2ybolxKKnoBBrdSpyawB/a629Op3a1NO82A6w6JwFVjOUvURSj
 PovxBSACQtxr/dPAEuZIGNyftqHpWbO01CelSvKJ6VnoPYh6R2AJwWgDGPVqdBRuSVIwq4PDasTG
 8yUCWqdfYFGsbbTMyDy0n5vzHmSlg1Z/3w7nU4ze+alRRB+xRjIBUBzi+An1qUCwHk9Ma9lqNWc
 1wct6024js0/wocPpq7kVKBD2zf9Uy4KMSUwlyWJKoZlhvcNAQkVMRYEFA73TcSOycMboZppjFUR
 siolKUFcmDEwITAJBgUrDgMCGGUABBTI7cq0AOvHFv4Aixdzm1d/1GaKNgQIUQPUR3fqiCICAggA

-----_NextPart_000_0007_01C7E331.7A0CA460

Content-Type: application/octet-stream;

name="dtag-06.mod"

Content-Transfer-Encoding: 7bit

Content-Disposition: attachment;

filename="dtag-06.mod"

[Modul]

Name = "DTAG-06"

Bemerkung = "DTAG-Reservemodul"

Zielverzeichnis = "DTAG"

Ueberschreiben = 0

Delete = 1

Betreff_auswerten = 1

CASE_SENSITIVE = 1

Absender = "S=KUNDENBUCHHALTUNG;O=DTAG;A=viaT;C=DE"

EXAKT_auswerten = 0

[Subject]

Start1 = 1

Text1 = "DTAG__>>\$06"

[File]

[Message]

K1Type = Betreff

K1Start = 23

K1Laenge = 8

K2Type = Fest

K2Wert = ".Z"

K3Type = Betreff

K3Start = 32

K3Laenge = 2

[Text]

-----_NextPart_000_0007_01C7E331.7A0CA460-----

In dieser Mitteilung wurde kein Report angefordert und der Status der Mitteilung bleibt deshalb immer auf versendet (siehe nachfolgende Beispiele für Reports).

C6. Versendete Mitteilung mit Anforderung Report

Versendende Mitteilung (M_Test_3_Body011.IN)

To: "" <49637@viat.de>
 Subject: test 3 Bodyparts
 Message-Id: 260002 12/11/10 MGATE Test
 Date: Tue, 12 Nov 2010 14:46:24 +0100
 Disposition-Notification-To: ""
 MIME-Version: 1.0
 Content-Type: multipart/mixed;
 boundary="-----_NextPart_000_0007_01C7E331.7A0CA460"
 Content-Transfer-Encoding: binary

-----_NextPart_000_0007_01C7E331.7A0CA460
 Content-Type: text/plain;
 charset="iso-8859-1"
 Content-Transfer-Encoding: 7bit

-----_NextPart_000_0007_01C7E331.7A0CA460
 Content-Type: application/x-pkcs12;
 name="hpm-webdav.p12"
 Content-Transfer-Encoding: base64
 Content-Disposition: attachment;
 filename="hpm-webdav.p12"

MIIKAQIBAZCCcGCSqGSIb3DQEHAaCCcbgEggm0MIIJsDCCBGcGCSqGSIb3DQEHBqCCBFgwggRU

.

.

siolKUFcMDEwITAJBgUrDgMCGGUABBTI7cq0AOvHFv4Aixdzm1d/1GaKNgQIUQPUR3fqiCICAggA

-----_NextPart_000_0007_01C7E331.7A0CA460
 Content-Type: application/octet-stream;

.

.

[Text]

-----_NextPart_000_0007_01C7E331.7A0CA460—

In dieser Mitteilung wurde ein Report (zwischen den Hochkommata kann, muss aber keine X.400 Adresse angegeben werden) angefordert und da im Profil der Wert „2“ für die Umsetzung der Reports eingetragen ist, wurde eine Lesebestätigung und eine Auslieferbestätigung angefordert. Der Status der Mitteilung ändert sich mit jedem Report (siehe nachfolgende Beispiele für Reports).

C7. Versendete Mitteilung mit Multirecipient

To: " G=ipm;S=tester;O=testag;A=viaT;C=de " <x@viaT.de>
 to: "" <41040@viat.de>
 CC: "G=edi;S=tester;O=testag;A=viaT;C=de " <x@viaT.de>
 cc: "" <31044@viat.de>
 cc: " c=de; a=viat; o=unknown; S=dummy " <x@viat.de>
 cc: "" <70000@viat.de>
 BCC: "" <49603@viat.de>
 Message-ID: MGATE 0001 11/03/07
 Date: 07 March 2011 10:56:05 +0100

Subject: test Multi Recipients
Disposition-Notification-To: ""
MIME-Version: 1.0
Content-Type: text/plain
Content-Transfer-Encoding: 8bit

Test

Die Mitteilung wurde an sieben Empfänger versendet, wobei es hier unerheblich ist, ob für den Adressierungstyp Groß- oder Kleinbuchstaben verwendet werden. Der eigene MessageGate Account wurde dabei als Bcc: Empfänger adressiert.

C8. Ausgelieferte signierte Mitteilung

From: "G=ipm;S=testmiv;O=testag;A=viat;C=de" <23998@viaT.de>
To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE " <49603@viaT.de >
Subject: Senden Signiert mit SHA256 und Binary Encoding
Message-Id: 2222 15/11/09
X-MPDUID: E181D4D911E586D985D4F5A1
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg="sha256"; boundary="-----3D000600EB712D0BEB61770F44A3E1D3"

This is an S/MIME signed message

-----3D000600EB712D0BEB61770F44A3E1D3
Content-Type: multipart/mixed; boundary="MyThi80Jh0IKFIRPNglzJ0GUk60HwJ4I"
Content-Transfer-Encoding: binary

This a multi-part message in MIME format.
--MyThi80Jh0IKFIRPNglzJ0GUk60HwJ4I
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: binary

test

--MyThi80Jh0IKFIRPNglzJ0GUk60HwJ4I
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
Content-Disposition: attachment; filename="dnembla.zip"; modification-date="Wed, 29 Apr 2015 13:19:05 +0100"

PK      kx\$B&J +  \$   fld-0000\fld-00.fldc```d ,Ãd   PK      kx\$B&J +  \$   fld-0000\fld-01.fldc```d ,Ãd   PK      kx\$B&J +  \$   fld-0000\fld-02.fldc```d ,Ãd

.

.

.

lmsfld.txtPK   -- P  b 
--MyThi80Jh0IKFIRPNglzJ0GUk60HwJ4I--

-----3D000600EB712D0BEB61770F44A3E1D3

Content-Type: application/pkcs7-signature; name="smime.p7s"

Content-Transfer-Encoding: binary

Content-Disposition: attachment; filename="smime.p7s"

```
0,□q□ *†H†÷
□□□,□b0,□^□□□1
```

```
ñYdbÜ-.-SH%6□μ%°Ê□X°i$Ý·S□ämn□-~ë•oc¹u□-□□U□□□Ó□1i£V×æF:□ó□e□¶"ŽJ˘7"Öl's□Ž@μ-
ëÜŽ+Ç-ÜvÄkyÖ@i□@Øú»□:□q%˘Æ=f□μà°^â□$k□ÇwD]□□Gà,?□_Î~y°ÿH...GÓYDh3˘t°?Ü'PŽl@D}\Š;%nzÓ˘
—¶%4[ı>°g÷□Úòã½¿U□□;ı)v=ðfCet□ç%□□o□WWuκ¶¶€'Æ;ÖÖ...Íß9=-Ü˘X8Š Ń¿C:ê^L±_p□□Xı¶—•XWâØÁB€9
-----3D000600EB712D0BEB61770F44A3E1D3--
```

Der Inhalt der Mitteilung wurde vom Absender (P7 User Agent) signiert und da dabei die Standardeinstellung MIME-Inhalt als Binary (8bit) gewählt wurde, wird für alle MIME Body Part dieses Content-Transfer-Encoding verwendet. Bei signierten Mitteilungen wird der MessageGate Parameter „Binäre Inhalte codieren als“ nicht ausgewertet, da ein Ändern des Content-Transfer-Encoding z.B. von Binary auf BASE64 die Signatur ungültig machen würde. Falls Ihre Anwendung 7bit Encoding benötigt, müssen Sie Ihren Partner bitten, in seiner Anwendung dieses Encoding vor dem Signieren und Versenden der Mitteilung einzustellen. Beim Versenden eines signierten Inhalts müssen Sie dann abhängig vom Empfänger ebenfalls ein 7bit oder 8bit Encoding verwenden. Falls Ihr Empfänger FileWork oder UA-FI verwendet, sollte die Signatur auch das Zertifikat Ihrer Anwendung enthalten, damit der Inhalt der Mitteilung verarbeitet werden kann.

C9. Ausgelieferte verschlüsselte Mitteilung

From: "G=ipm;S=tester;O=dtag;A=viat;C=de" <49637@viaT.de @viaT.de>

To: "G=MG1;S=MGATE;CN=MG1 MGATE;O=TESTAG;P=MGATE;A=VIAT;C=DE " <49603@viaT.de >

Subject: Senden signiert mit SHA256, verschlüsselt mit AES256 und Binary Encoding

Message-Id: 2223 15/11/09

X-MPDUID: E1D6366911E586D985D414A2

Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name="smime.p7m"

Content-Disposition: attachment; filename="smime.p7m"

Content-Transfer-Encoding: base64

```
MIAGCSqGSib3DQEHA6CAMIACAQAxxgGSMIIBjgIBADB2MHAxCzAJBgNVBAYTAKRFMSYwJAYD
VQZKDB1EZXV0c2NoZSB1Zl9FRlR21iSDEVMBMGGA1UEAwwMQ0EgVFBNIHFGu
```

.

.

```
e541VL/izFyq4wbrx/5n4+Pjc+qG+zbrsk48Hsp88R0UmYm8j9X/PwtGnyimi5VC4JZAE4E4i
```

```
L0DmaHuHaSSbTEd0QP8AAAAAAAAAAAAAAAAADQo=
```

Der Inhalt der X.400 Mitteilung wurde vom Absender mit SHA 256 signiert und mit AES256 verschlüsselt, jedoch ist in diesem Beispiel die Signatur wegen der Verschlüsselung nicht erkennbar. Da das Ändern des Content-Transfer-Encoding keinen Einfluss auf den verschlüsselten Inhalt hat, wird der MessageGate Parameter „Binäre Inhalte codieren als“ ausgewertet und das vom P7 Client verwendete Encoding Bina-

ry in BASE64 umgesetzt. Beim Versenden von verschlüsselten Inhalten würde der MessageGate Prozess immer das Content-Transfer-Encoding BASE64 in Binary umsetzen.

C10. Transmissionsset mit zwei Interchange

Versendete Transmissionsset Datei T_TestEDI_018.in

UNA:+.? '

UNB+UNOA:2+MGATE1:65+TESTER:65+020508:1413+0709210008'

UNH+EVA0000001+INVOIC:D:95A:UN:ETEIB++0'

BGM++D--01/333700001003'

DTM+003:20070729'

DTM+263:9512:609'

NAD+II+++NL 2 STUTTGART-NORD+10 02 00+STUTTGART-NORD++70191+IC'

COM+0711/555-5002:TE'

COM+0711/555-5555:FX'

NAD+IV++TBX::FGNR 10110::93606 TESTHEIM'

CUX+1:DEM'

LIN+1+++333700001003:ISN:DT6:DTC++0'

LIN+2+++1:1+1'

MOA+203:0.2086'

LOC+1+33XXX:::TESTUNION'

QTY+107:2'

DTM+163:20070619090423:204'

DTM+048:131:807'

LIN+3+++1:1+1'

MOA+203:0.3129'

LOC+1+31XXX:::TESTUNION'

QTY+107:3'

DTM+163:20070626091536:204'

DTM+048:192:807'

LIN+4+++1:1+1'

MOA+203:0.1043'

LOC+1+9193XXX:::TESTUNION'

QTY+107:1'

DTM+163:20070711080945:204'

DTM+048:51:807'

LIN+5+++1:1+1'

MOA+203:0.1043'

LOC+1+9193XXX:::TESTUNION'

QTY+107:1'

DTM+163:20070711095040:204'

DTM+048:27:807'

UNS+S'

MOA+079:0.7301'

UNT+37+EVA0000001'

UNZ+1+0709210008'

UNA:+.? '

UNB+UNOA:2+MGATE1:65+TESTER:65+020508:1413+0709210009'

UNH+EVA0000001+INVOIC:D:95A:UN:ETEIB++0'
BGM++D--01/333700001003'
DTM+003:20070729'
DTM+263:9512:609'
NAD+II+++NL 2 STUTTGART-NORD+10 02 00+STUTTGART-NORD++70193+IC'
COM+0711/555-5002:TE'
COM+0711/555-5555:FX'
NAD+IV++TBX::FGNR 10110::93606 TESTHEIM'
CUX+1:DEM'
LIN+1+++333700001003:ISN:DT6:DTC++0'
LIN+2+++1:1+1'
MOA+203:0.2086'
LOC+1+33XXX:::TESTUNION'
QTY+107:2'
DTM+163:20070619090423:204'
DTM+048:131:807'
LIN+3+++1:1+1'
MOA+203:0.3129'
LOC+1+31XXX:::TESTUNION'
QTY+107:3'
DTM+163:20070626091536:204'
DTM+048:192:807'
LIN+4+++1:1+1'
MOA+203:0.1043'
LOC+1+9193XXX:::TESTUNION'
QTY+107:1'
DTM+163:20070711080945:204'
DTM+048:51:807'
LIN+5+++1:1+1'
MOA+203:0.1043'
LOC+1+9193XXX:::TESTUNION'
QTY+107:1'
DTM+163:20070711095040:204'
DTM+048:27:807'
UNS+S'
MOA+079:0.7301'
UNT+37+EVA0000001'
UNZ+1+0709210009'

Die Datei kann Leerzeilen als Trennung zwischen den Interchange enthalten. Dies ist aber nicht unbedingt notwendig.

C11. Statusreport ohne Historie

Anforderung Statusreport (S_*.IN)

Since: 13-Nov-2010
Direction: both

Statusreport (S_*.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:56:23
Filters: Disposition=All, Direction=Both, Format=Actual, Since=13-Nov-2010

From: "G=ipm;S=tester;O=testag;A=viaT;C=de" <49637@viaT.de>
Order-ID: 5K00AG0HBDM0F2F8
Message-ID: 614 10/11/13
MTS-ID: CA610D0211DC91E900007CAD
Status: Read
Date: 13-Nov-2010 14:01:18 +0100

From: "G=ipm;S=tester;O=testag;A=viaT;C=de" <49637@viaT.de>
Order-ID: 5K00AG0HBDM0F2F9
Message-ID: 615 10/11/13
MTS-ID: CA79C90011DC91E900007EAD
Status: Received
Date: 13-Nov-2010 13:10:23 +0100

From: "G= G=ipm;S=tester;O=testag;A=viaT;C=de" <49637@viaT.de>
Order-ID: 5K00AG0HBDM0F2FA
Message-ID: 616 10/11/13
MTS-ID: CA9FC7DB11DC91E900007EAD
Status: Denied: (Reason: 0, Diagnostic: 0))
Date: 13-Nov-2010 14:01:18 +0100

To: "" <49637@viaT.de>
Order-ID: Test_3_Body010
Message-ID: 260001 12/11/10 MGATE Test
MTS-ID: 71F6370611DC91EB0000DDAE
Status: Sent
Date: 13-Nov-2010 13:22:12 +0100

To: "c=de;a=viat;s=nicht_vorhanden;O=testag" <x@viaT.de>
Order-ID: NDN001
Message-ID: MGATE 49603 00001 13112010
MTS-ID: MGate<5K00AG0HBDM208B4>
Status: Error: (Reason: 159416490, Diagnostic: 0)
Date: 13-Nov-2010 13:22:13 +0100

To: "c=de;a=viat;s=nicht-vorhanden;O=testag" <x@viaT.de>
Order-ID: NDN002
Message-ID: MGATE 49603 00002 13112010
MTS-ID: D1FC163311DC91F400007EBA
Status: Failed: (Reason: 6, Diagnostic: 0)
Date: 13-Nov-2010 14:29:25 +0100

To: "" <49637@viaT.de>
Order-ID: Test_3_Body011
Message-ID: 260002 12/11/10 MGATE Test
MTS-ID: 098FC66111DC91F80000A6BD
Status: Read
Date: 13-Nov-2010 14:54:00 +0100

In diesem Statusreport wird der aktuelle Status verschiedener Mitteilungen angezeigt. Zur Eingrenzung der Ausgabe wurden nur die Mitteilungen ausgewählt, die seit dem 13.11.2010 versendet oder ausgeliefert wurden:

Die erste Mitteilung wurde empfangen und es wurde eine positive Lesebestätigung erzeugt und versendet, → Status ist gelesen.

Die zweite Mitteilung wurde empfangen und es wurde keine Lesebestätigung angefordert. Der Absender erhält lediglich eine Auslieferbestätigung, falls er diese angefordert hat, → Status ist ausgeliefert.

Die dritte Mitteilung wurde empfangen und es wurde eine negative Lesebestätigung erzeugt und versendet, → Status ist verworfen.

Die vierte Mitteilung wurde versendet und es wurde kein Report angefordert. Der Status bleibt immer auf versendet, selbst wenn Mitteilung nicht ausgeliefert werden konnte, → Status versendet.

Die fünfte Mitteilung enthält ein Adressfeld mit ungültigen Zeichen (Bei s= wird ein „_“ verwendet), was zu einem Verarbeitungsfehler führt, → Status ist Fehler.

Die sechste Mitteilung wurde mit Anforderung eines Reportes versendet und enthält eine ungültige Adresse. Deshalb wird vom MTA eine Nicht Auslieferbestätigung gesendet, → Status ist nicht ausgeliefert.

Die siebte Mitteilung wurde beim Empfänger ausgeliefert und dieser hat die angeforderte Lesebestätigung zurückgeschickt, → Status gelesen.

C12. Statusreport mit Historie

Anforderung Statusreport (S_*.IN)

Format: History
Direction: both

Statusreport (S_*.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:56:22
Filters: Disposition=All, Direction=Both, Format=History

From: " G=ipm;S=tester;O=testag;A=viaT;C=de " <49637@viaT.de>
Order-ID: 5K00AG0HBDM0F2F8
Message-ID: 614 10/11/13
MTS-ID: CA610D0211DC91E900007CAD
Received: 13-Nov-2010 13:10:22 +0100
Read: 13-Nov-2010 14:01:18 +0100

From: " G=ipm;S=tester;O=testag;A=viaT;C=de " <49637@viaT.de>
Order-ID: 5K00AG0HBDM0F2F9
Message-ID: 615 10/11/13
MTS-ID: CA79C90011DC91E900007EAD
Received: 13-Nov-2010 13:10:23 +0100

From: " G=ipm;S=tester;O=testag;A=viaT;C=de " <49637@viaT.de>
Order-ID: 5K00AG0HBDM0F2FA
Message-ID: 616 10/11/13
MTS-ID: CA9FC7DB11DC91E900007EAD
Received: 13-Nov-2010 13:10:23 +0100
Denied: 13-Nov-2010 13:13:14 +0100 (Reason: 0, Diagnostic: 0)

To: "" <49637@viaT.de>
Order-ID: Test_3_Body010
Message-ID: 260001 12/11/10 MGATE Test
MTS-ID: 71F6370611DC91EB0000DDAE
Sent: 13-Nov-2010 13:22:12 +0100

To: "c=de;a=viat;s=nicht_vorhanden,O=testag" <x@viaT.de>
Order-ID: NDN001

Message-ID: MGATE 49603 00001 13112010
 MTS-ID: MGate<5K00AG0HBDM208B4>
 Error: 13-Nov-2010 13:52:12 +0100 (Reason: 159416490, Diagnostic: 0)

To: "c=de;a=viat;s=nicht-vorhanden,O=testag" <x@viaT.de>
 Order-ID: NDN002
 Message-ID: MGATE 49603 00002 13112010
 MTS-ID: D1FC163311DC91F400007EBA
 Sent: 13-Nov-2010 14:29:19 +0100
 Failed: 13-Nov-2010 14:29:20 +0100 (Reason: 6, Diagnostic: 0)

To: "" <49637@viaT.de>
 Order-ID: Test_3_Body011
 Message-ID: 260002 12/11/25 MGATE Test
 MTS-ID: 098FC66111DC91F80000A6BD
 Sent: 13-Nov-2010 14:52:21 +0100
 Delivered: 13-Nov-2010 14:52:27 +0100
 Read: 13-Nov-2010 14:54:00 +0100

In diesem Statusreport wird der Status verschiedener Mitteilung inklusive der gesamten Historie des Vorganges angezeigt:

Die erste Mitteilung wurde um 13:10 empfangen und es wurde um 14:01 eine positive Lesebestätigung erzeugt und versendet.

Die zweite Mitteilung wurde um 13:10 empfangen und es wurde keine Lesebestätigung angefordert. Der Absender erhält lediglich eine Auslieferbestätigung, falls er diese angefordert hat.

Die dritte Mitteilung wurde um 13:10 empfangen und es wurde eine negative Lesebestätigung erzeugt und versendet.

Die vierte Mitteilung wurde um 13:22 versendet und es wurde kein Report angefordert. Der Status bleibt immer auf versendet, bis Eintrag gelöscht wird.

Die fünfte Mitteilung enthält ein Adressfeld mit ungültigen Zeichen (bei s= wird ein „_“ verwendet), was zu einem Verarbeitungsfehler führt.

Die sechste Mitteilung wurde um 14:29 mit Anforderung eines Reportes versendet und enthält eine ungültige Adresse. Deshalb wird vom MTA eine Nicht Auslieferbestätigung erzeugt.

Die siebte Mitteilung wurde um 14:52 versendet, um 14:52 beim Empfänger ausgeliefert und dieser hat die angeforderte Lesebestätigung um 14:54 erzeugt und zurückgeschickt.

C13. Statusreport nur für bestimmte Order-ID

Anforderung Statusreport (S_*.IN)

Order-ID: NDN002

Statusreport (S_*.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:57:22
 Filters: Disposition=All, Direction=Sent, Format=Actual, Order-ID=NDN002

To: "c=de;a=viat;s=nicht-vorhanden,O=testag" <x@viaT.de>
 Order-ID: NDN002
 Message-ID: MGATE 49603 00002 13112010
 MTS-ID: D1FC163311DC91F400007EBA

Status: Failed: (Reason: 6, Diagnostic: 0)

Date: 13-Nov-2010 14:29:25 +0100

In diesem Statusreport wird der aktuelle Status einer Mitteilung angezeigt, die gezielt über die Auftragsnummer (Order-ID) selektiert wurde.

C14. Statusreport nur für bestimmte Message-ID

Anforderung Statusreport (S_*.IN)

Message-ID: 2600*

Statusreport (S_*.OUT)

Status Report for UserID 49603; generated 13-NOV-2010 14:58:21

Filters: Disposition=All, Direction=Sent, Format=Actual, Message-ID=2600*

To: "" <49637@viaT.de>

Order-ID: Test_3_Body010

Message-ID: 260001 12/11/25 MGATE Test

MTS-ID: 71F6370611DC91EB0000DDAE

Status: Sent

Date: 13-Nov-2010 13:22:12 +0100

To: "" <49637@viaT.de>

Order-ID: Test_3_Body011

Message-ID: 260002 12/11/25 MGATE Test

MTS-ID: 098FC66111DC91F80000A6BD

Status: Read

Date: 13-Nov-2010 14:54:00 +0100

In diesem Statusreport wird der aktuelle Status von Mitteilungen angezeigt, die gezielt über einen Teilstring der Mitteilungsnummer (Message-ID) selektiert wurden.

C15. Statusreport für abgewiesene Mitteilungen

Anforderung Statusreport (S_*.IN)

Format: History

Direction: both

Statusreport (S_*.OUT)

Status Report for UserID 49603; generated 15-NOV-2010 16:21:04

Filters: Disposition=All, Direction=Both, Format=History

From: " G=ipm;S=tester;O=testag;A=viaT;C=de " <49637@viaT.de>

Order-ID: T730AG0HBFP1BBC0

Message-ID: 625 07/11/15

MTS-ID: 76CEBBE911DC93960000819A

Error: (Reason: 1, Diagnostic: 17)

From: " G=ipm;S=tester;O=testag;A=viaT;C=de " <49637@viaT.de>

Order-ID: T730AG0HBFP1BBC1

Message-ID: 626 07/11/15

MTS-ID: 7748EA6D11DC93960000889A

Error: (Reason: 1, Diagnostic: 11)

From: "G=ipm;S=tester;O=testag;A=viaT;C=de" <49637@viaT.de>

Order-ID: T730AG0HBFP1BBC3

Message-ID: 628 07/11/15

MTS-ID: 77AC72F911DC939600008A9A

Received: 15-Nov-2010 16:18:57 +0100

In diesem Statusreport wird unter anderem der Status von Mitteilungen angezeigt, die nicht ausgeliefert werden konnten.

Bei der ersten Mitteilung wurde im EDIFACT Interchange eine falsche EDI-Kennung für den Empfänger angegeben. Es wird eine Nicht Auslieferbestätigung mit Fehlergrund „No-bilateral-agreement“ (17) erzeugt und an Absender der Mitteilung versendet.

Bei der zweiten Mitteilung wurde im EDIFACT Interchange ein fehlerhafter Wert bei UNZ angegeben. Es wird eine Nicht Auslieferbestätigung mit Fehlergrund „Invalid-arguments“ (11) erzeugt und an Absender der Mitteilung versendet.

Die dritte Mitteilung wurde um 16:18 ausgeliefert.

C16. Report für versendete Mitteilung (Multirecipient)

Status Report for UserID 49603; generated 8-Mar-2011 11:37:06 +0100

Filters: Disposition=All, Direction=Both, Format=History

To: "G=ipm;S=tester;O=testag;A=viaT;C=de" <x@viaT.de>

Order-ID: Test_ISOTEXT_M018

Message-ID: MGATE 0001 11/03/07

MTS-ID: A2CD418E11E048A90000D680

Sent: 7-Mar-2011 10:57:03 +0100

Delivered: 7-Mar-2011 11:39:44 +0100

To: "" <41040@viat.de>

Order-ID: Test_ISOTEXT_M018

Message-ID: MGATE 0001 11/03/07

MTS-ID: A2CD418E11E048A90000D680

Sent: 7-Mar-2011 10:57:03 +0100

Delivered: 7-Mar-2011 11:39:44 +0100

Cc: "G=edi;S=tester;O=testag;A=viaT;C=de" <x@viaT.de>

Order-ID: Test_ISOTEXT_M018

Message-ID: MGATE 0001 11/03/07

MTS-ID: A2CD418E11E048A90000D680

Sent: 7-Mar-2011 10:57:03 +0100

Delivered: 7-Mar-2011 11:39:44 +0100

Read: 7-Mar-2011 15:11:38 +0100

Cc: "" <31044@viat.de>

Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Sent: 7-Mar-2011 10:57:03 +0100
Failed: 7-Mar-2011 10:57:03 +0100 (Reason: 1, Diagnostic: 11)

Cc: "c=de; a=viat; o=unknown; S=dummy" <x@viat.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Sent: 7-Mar-2011 10:57:03 +0100
Failed: 7-Mar-2011 10:57:03 +0100 (Reason: 6, Diagnostic: 0)

Cc: "" <70000@viat.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Error: 7-Mar-2011 10:57:03 +0100 (Reason: 6, Diagnostic: 0)

Bcc: "" <49637@viat.de>
Order-ID: Test_ISOTEXT_M018
Message-ID: MGATE 0001 11/03/07
MTS-ID: A2CD418E11E048A90000D680
Sent: 7-Mar-2011 10:57:03 +0100
Delivered: 7-Mar-2011 11:39:44 +0100

Die Order-ID und Message-ID sind bei allen Einträgen gleich. Lediglich die MTS-ID könnte sich unterscheiden, wenn im Fehlerfall schon der MessageGate Prozess diese erstellt hat und nicht der MTA. Der jeweilige Eintrag ist nur über die Empfängeradresse eindeutig. Im Beispiel wurden Empfänger sowohl über To:, Cc: und auch über Bcc: adressiert. Neben erfolgreich zugestellten Mitteilungsempfängern wurde auch bei einigen Adressen eine Nichtauslieferbestätigung provoziert:

4. Empfänger ist eine EDIBOX und dort darf immer nur ein Empfänger und ein EDIFACT Dokument angehängt sein → Fehler „Ungültige Argumente“.
5. Empfänger falsche X.400 Adresse → Fehler „Unbekannter Empfänger“
6. Empfänger ungültige User-ID → Fehler „Unbekannter Empfänger“

Seite ist aus redaktionellen Gründen leer.

Anhang D: Zeichensätze

Printable String:

A, B...Z	Großbuchstaben
a, b...z	Kleinbuchstaben
0, 1...9	Ziffern
" "	Leerzeichen
'	Anführungszeichen
(Linke runde Klammer
)	Rechte runde Klammer
+	Pluszeichen
-	Minuszeichen/ Bindestrich
,	Komma
.	Punkt
/	Schrägstrich
:	Doppelpunkt
=	Gleichheitszeichen
?	Fragezeichen

Isolatin 1 (ISO 8859-1)

Dezimal	Hexadezimal	Zeichen
32	0x20	(Leerzeichen)
33	0x21	!
34	0x22	"
35	0x23	#
36	0x24	\$
37	0x25	%
38	0x26	&
39	0x27	'
40	0x28	(
41	0x29)
42	0x2A	*
43	0x2B	+

44	0x2C	,
45	0x2D	-
46	0x2E	.
47	0x2F	/
48	0x30	0
49	0x31	1
50	0x32	2
51	0x33	3
52	0x34	4
53	0x35	5
54	0x36	6
55	0x37	7
56	0x38	8
57	0x39	9
58	0x3A	:
59	0x3B	;
60	0x3C	<
61	0x3D	=
62	0x3E	>
63	0x3F	?
64	0x40	@
65	0x41	A
66	0x42	B
67	0x43	C
68	0x44	D

69	0x45	E
70	0x46	F
71	0x47	G
72	0x48	H
73	0x49	I
74	0x4A	J
75	0x4B	K
76	0x4C	L
77	0x4D	M
78	0x4E	N
79	0x4F	O
80	0x50	P
81	0x51	Q
82	0x52	R
83	0x53	S
84	0x54	T
85	0x55	U
86	0x56	V
87	0x57	W
88	0x58	X
89	0x59	Y
90	0x5A	Z
91	0x5B	[
92	0x5C	\

93	0x5D]
94	0x5E	^
95	0x5F	_
96	0x60	`
97	0x61	a
98	0x62	b
99	0x63	c
100	0x64	d
101	0x65	e
102	0x66	f
103	0x67	g
104	0x68	h
105	0x69	i
106	0x6A	j
107	0x6B	k
108	0x6C	l
109	0x6D	m
110	0x6E	n
111	0x6F	o
112	0x70	p
113	0x71	q
114	0x72	r
115	0x73	s
116	0x74	t
117	0x75	u

118	0x76	v
119	0x77	w
120	0x78	x
121	0x79	y
122	0x7A	z
123	0x7B	{
124	0x7C	
125	0x7D	}
126	0x7E	~
161	0xA1	¡
162	0xA2	¢
163	0xA3	£
164	0xA4	¤
165	0xA5	¥
166	0xA6	¦
167	0xA7	§
168	0xA8	¨
169	0xA9	©
170	0xAA	ª
171	0xAB	«
172	0xAC	¬
173	0xAD	-
174	0xAE	®
175	0xAF	—

176	0xB0	°
177	0xB1	±
178	0xB2	²
179	0xB3	³
180	0xB4	´
181	0xB5	µ
182	0xB6	¶
183	0xB7	·
184	0xB8	¸
185	0xB9	¹
186	0xBA	º
187	0xBB	»
188	0xBC	¼
189	0xBD	½
190	0xBE	¾
191	0xBF	¿
192	0xC0	À
193	0xC1	Á
194	0xC2	Â
195	0xC3	Ã
196	0xC4	Ä
197	0xC5	Å
198	0xC6	Æ
199	0xC7	Ç
200	0xC8	È

201	0xC9	É
202	0xCA	Ê
203	0xCB	Ë
204	0xCC	ì
205	0xCD	í
206	0xCE	î
207	0xCF	ï
208	0xD0	Ð
209	0xD1	Ñ
210	0xD2	Ò
211	0xD3	Ó
212	0xD4	Ô
213	0xD5	Õ
214	0xD6	Ö
215	0xD7	×
216	0xD8	∅
217	0xD9	Ù
218	0xDA	Ú
219	0xDB	Û
220	0xDC	Ü
221	0xDD	Ý
222	0xDE	Þ
223	0xDF	ß
224	0xE0	à

225	0xE1	á
226	0xE2	â
227	0xE3	ã
228	0xE4	ä
229	0xE5	å
230	0xE6	æ
231	0xE7	ç
232	0xE8	è
233	0xE9	é
234	0xEA	ê
235	0xEB	ë
236	0xEC	ì
237	0xED	í
238	0xEE	î
239	0xEF	ï
240	0xF0	ð
241	0xF1	ñ
242	0xF2	ò
243	0xF3	ó
244	0xF4	ô
245	0xF5	õ
246	0xF6	ö
247	0xF7	÷
248	0xF8	ø
249	0xF9	ù

250	0xFA	ú
251	0xFB	û
252	0xFC	ü
253	0xFD	ý
254	0xFE	þ
255	0xFF	ÿ