



Logius
*Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties*

Koppelvlakbeschrijving Digipoort
Berichtuitwisseling - SMTP-MTA
(server-to-server)

Versie 2.1.2

Datum	1 juni 2015
Status	Definitief

Colofon

Projectnaam	Digipoort
Versienummer	2.1.2
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Bijlage(n)	0

Inhoud

Colofon	2
Inhoud	3
Inleiding	4
<i>Doel en doelgroep</i>	<i>4</i>
<i>Leeswijzer</i>	<i>4</i>
<i>Status</i>	<i>4</i>
1 Interactie via het koppelvlak	5
1.1 <i>Transport</i>	<i>5</i>
1.2 <i>Inhoud</i>	<i>5</i>
1.2.1 SMTP Envelope	5
1.2.2 SMTP Headers	6
1.2.3 SMTP Body	6
1.2.4 Delivery Status Notifications (DSN's)	8
1.2.5 Adressering	8
1.3 <i>Beveiliging</i>	<i>8</i>
1.3.1 Onweerlegbaarheid	8
1.3.2 Authenticiteit	8
1.3.3 Vertrouwelijkheid	8
1.3.4 Integriteit	9
1.4 <i>Voorbeelden</i>	<i>9</i>
1.4.1 Inkomend SMTP-bericht	9
1.4.2 Uitgaand SMTP-bericht	9
1.4.3 Delivery report	10
2 Algemene afspraken	12
2.1 <i>Standaarden</i>	<i>12</i>
2.1.1 Normatieve RFCs voor berichttransport	12
2.1.2 Normatieve RFCs voor berichtinhoud	12
2.2 <i>Randvoorwaarden</i>	<i>12</i>
2.3 <i>Foutmeldingen</i>	<i>12</i>
2.4 <i>Adressen</i>	<i>13</i>
2.5 <i>Limieten</i>	<i>13</i>
2.6 <i>Ondersteuning</i>	<i>13</i>

Inleiding

Doel en doelgroep

Digipoort (voorheen Overheidstransactiepoort) heeft als doel het realiseren van een generieke elektronische toegangsdienst waarmee het bedrijfsleven de gehele overheid kan bereiken.

Het succesvol functioneren van Digipoort valt en staat met een goede beschrijving van de koppelvlakken waarop de overheid, het bedrijfsleven en burgers moeten (kunnen) aansluiten.

Digipoort biedt het bedrijfsleven en de overheid diverse koppelvlakken. Voor elk koppelvlak is een aparte specificatie beschikbaar. Dit document geeft invulling aan één van deze koppelvlakken, namelijk het SMTP (Simple Mail Transfer Protocol) koppelvlak voor uitwisseling van mailverkeer tussen mailservers (MTAs). Deze koppelvlakspecificatie beschrijft niet de uitwisseling van mailverkeer tussen een mailclient en Digipoort. Hiervoor bestaan afzonderlijke koppelvlakbeschrijvingen: SMTP-MSA en POP3.

Dit document is primair bestemd voor ontwikkelaars van systeem-naar-systeemkoppelingen.

Leeswijzer

Het document is als volgt opgebouwd. Het eerste hoofdstuk bevat algemene informatie. Het tweede hoofdstuk bevat de beschrijving van de werking van het aanleveren. Het derde hoofdstuk geeft een meer gedetailleerde inzicht in de technische werking van het koppelvlak. Het document wordt besloten met een overzicht van alle algemeen van toepassing zijnde standaarden en afspraken.

Status

Dit document is een aangevulde en herschreven versie van de koppelvlakspecificaties Digipoort SMTP-MTA versie 2.1 ten behoeve van het migreren van de Overheidstransactiepoort.

Dit document beschrijft de huidige situatie voor wat betreft het koppelvlak. Ten opzichte van versie 2.1 is de werking van het koppelvlak niet veranderd.

1 Interactie via het koppelvlak

1.1 Transport

Op de volgende manieren kan er verbinding gemaakt worden met Digipoort:

1. Internet
 - a. VPN door middel van IPsec
2. Diginetwerk (voorheen Koppelnet Publieke Sector; alleen voor overheden)

Voor dit koppelvlak is er geen verbinding via SSL/TLS over TCP/IP mogelijk. Dit is wel mogelijk voor de SMTP-MSA en POP3 koppelvlakken.

Het SMTP protocol is een algemeen gebruikt bericht transport protocol. In dit document zal dit protocol globaal worden beschreven, waarbij de nadruk ligt op het beschrijven van uitzonderingen en/of beperkingen ten aanzien van de geldende standaarden. Voor een overzicht van de standaarden zie paragraaf 2.1

Voor SMTP-MTA is het een eis dat de aanleverende partij de beschikking heeft over een volledig functionerende SMTP server: een SMTP server die SMTP berichten kan verzenden, ontvangen én de RFC's ondersteunt die in paragraaf 2.1 worden genoemd.

1.2 Inhoud

Digipoort biedt een basisdienstverlening waar bedrijven en overheden gebruik van kunnen maken. Het SMTP koppelvlak is dusdanig opgezet dat deze een basis biedt voor het verzenden van berichten naar overheidsinstanties. De koppelvlakspecificatie geeft aan van welke specificaties gebruik wordt gemaakt voor het inzenden van berichten en welke standaarden gebruikt worden voor de opbouw van berichten.

In deze koppelvlakspecificatie wordt geen uitspraak gedaan over de werkelijke inhoud van het bericht dat via SMTP wordt verstuurd. Dit betreffen specifieke keten-afspraken, die moeten worden beschreven in de definities die worden opgesteld door de verschillende ketenpartners.

Een SMTP bericht dat wordt uitgewisseld tussen mail servers (MTAs) is opgebouwd uit de volgende onderdelen:

- SMTP Envelope
- Het eigenlijke bericht dat is opgebouwd uit een SMTP Header en uit een SMTP Body

Hieronder worden de onderdelen verder uitgelegd. Voor details wordt verwezen naar de RFCs die zijn opgenomen in paragraaf 2.1

1.2.1 SMTP Envelope

De envelop bevat de gegevens die nodig zijn voor het routeren van SMTP verkeer tussen mailservers (MTAs). Digipoort routeert berichten uitsluitend op basis van de envelop-gegevens.

De envelop omvat de volgende elementen (verbs):

Element	Omschrijving
MAIL FROM <originator address> {ENVID <envelope ID>}	De verzender van de mail (originator address). Elke mail heeft precies 1 verzender. Als een ontvangstbevestiging wordt gevraagd moet een uniek ID worden meegegeven (envelope id)
RCPT TO <recipient address> NOTIFY SUCCESS, FAILURE	De ontvanger van de mail (recipient address). Elke mail heeft precies 1 ontvanger. Door middel van de NOTIFY-optie wordt aangegeven dat ontvangstbevestigingen (of berichten van geen ontvangst) worden verstuurd door de ontvanger. Zie 1.2.4 voor verdere uitleg over de ontvangstbevestigingen.
DATA	De berichtinhoud (SMTP headers en body).

1.2.2

SMTP Headers

De headers bevatten informatie over de berichtinhoud: van wie is het afkomstig, voor wie is het bestemd, wat is het onderwerp etc. De volgende elementen komen voor (alleen de meest gebruikte zijn weergegeven):

Element	Uitleg
from	Adres van de verzender van het bericht
to	Adres van de ontvanger van het bericht.
message-id	Een unieke identificatie van het bericht. De verzender kan deze invullen mits deze uniek is. Indien een message-id ontbreekt voegt Digipoort een eigen message-id toe.
subject	Een beschrijving van het onderwerp van het bericht. Dit element wordt meegegeven aan de ontvanger van het bericht.
date	De door de verzender aangegeven verzenddatum van het bericht.

In de RFC genoemde headerelementen die in de SMTP-header kunnen voorkomen, maar die hierboven niet genoemd zijn, worden door Digipoort niet overgenomen. Digipoort vertaalt tevens de adresheaders van/naar logische Digipoort-adressen. Digipoort kent aan elk uitgaand bericht een eigen message-identificer toe.

1.2.3

SMTP Body

Digipoort kan berichten ontvangen als singlepart MIME, of als multipart MIME.

Digipoort stuurt berichten altijd door als singlepart.

Primair is het SMTP protocol bedoeld voor berichtuitwisseling tussen personen. In het kader van het Digipoort koppelvlak is er sprake van berichtuitwisseling tussen applicaties (systeem-systeem koppeling). Dit betekent dat ten aanzien van de MIME RFC's er een aantal beperkingen gelden. Deze beperkingen zijn nodig om berichtconversie van en naar andere koppelvlakken mogelijk te maken:

Bij gebruik van multipart MIME is het content-type altijd 'multipart/mixed' en gelden de volgende beperkingen:

- Er is ofwel precies één part aanwezig, met daarin dezelfde informatie als in een singlepart
- ofwel er zijn precies twee parts waarvan het eerste content-type text/plain heeft en verder leeg is, en het tweede dezelfde informatie bevat als in een singlepart

Er is dus altijd precies één betekenisvol part aanwezig. Voor dit part gelden de volgende content-parameters:

Parameter	Waarde	Toelichting
Content-Type	text/plain; charset=us-ascii	Voorkeurswaarde voor text-gebaseerde berichten. Andere waarden voor charset zijn toegestaan ¹ . Bij ontbreken van een waarde wordt us-ascii aangenomen. Het is niet toegestaan om te refereren aan Windows Code Pages (CPxxxx). Deze zijn op niet Windows-systemen niet te interpreteren.
	application/edifact	alternatief voor berichten in edifact formaat.
	application/octet-stream	application/octet-stream dient te worden gebruikt voor het verzenden van binary-bestanden.
Content-Transfer-Encoding	base64	voorkeurswaarde
	quoted-printable	alternatief voor base64;
	7bit	Toegestaan, maar wordt afgeraden. Is niet geschikt voor binaire data en tekst met ascii-waardes boven 127. CR/LF-details kunnen verloren gaan bij conversie naar base64. Indien de parameter Content-Transfer-Encoding ontbreekt of de waarde niet is ingevuld, wordt deze altijd als '7bit' geïnterpreteerd.

¹ In ieder geval de volgende character sets worden ondersteund: "us-ascii", "UTF-8", "ISO-8859-1" (Latin1, West European), "ISO-8859-2" (Latin2, East European), "ISO-8859-5" (Cyrillic), "ISO-8859-6" (Arabic), "ISO-8859-7 (Greek), "ISO-8859-8" (Hebrew), "ISO-8859-9" (Latin5, Turkish), "ISO-8859-10" (Latin6, Lappish/Nordic/Eskimo), "ISO-8859-13 (Latin7, Baltic Rim), "ISO-8859-14 (Latin8, Celtic), "ISO-8859-15" (Latin9, saner West european + euro), "ISO-8859-16" (Latin10, South-Eastern European)

Content- Disposition	attachment Filename=<bestandsnaam>. <extensie>	Digipoort vervangt de bestandsnaam altijd door een uniek ID. Indien de parameter ontbreekt of de waarde niet is ingevuld, genereert Digipoort een unieke bestandsnaam met extensie .txt. NB: Ook bij de parameter Content-Type kan een 'name' worden ingevuld. Gebruik van dat veld wordt afgeraden per RFC 2183.
-------------------------	--	---

1.2.4 *Delivery Status Notifications (DSN's)*

De inzendende partij krijgt een DSN bericht terug (opgesteld conform RFC 1891) waarin staat dat het bericht wel of niet correct is afgeleverd

Door middel van de NOTIFY-optie wordt aan de ontvanger gevraagd om een DSN terug te sturen die de status van ontvangst van het bericht aangeeft.

Succes en mislukking worden respectievelijk aangegeven met de parameterwaarden NOTIFY = SUCCESS en NOTIFY = FAILURE.

Digipoort dwingt bij alle partijen het gebruik van de SUCCESS en FAILURE als notify-opties af.

1.2.5 *Adressering*

Digipoort routeert op basis van logische adressen. Dat wil zeggen dat een bedrijf nooit direct een bericht aan een overheidspartij stuurt, maar dat in plaats daarvan het bedrijf een bericht aan een adres in het Digipoort-domein stuurt (en omgekeerd). Ook als Digipoort een bericht verstuurt komt daar nooit het eigenlijke adres van de afzender in voor, maar een logisch Digipoort-adres.

Een logisch adres wordt in Digipoort als een-op-een representatie van een fysiek adres (vertaalregel) gebruikt.

1.3 **Beveiliging**

Sessies worden beveiligd op het niveau van de verbinding.

1.3.1 *Onweerlegbaarheid*

Digipoort legt altijd vast welk pad een bericht van verzender naar ontvanger heeft gevolgd, tezamen met het tijdstip van verwerking. Daarbij wordt ook vastgelegd dat de server van de ontvanger (bedrijf of overheid) een bericht succesvol heeft aangenomen ('SMTP OK').

1.3.2 *Authenticiteit*

Authenticering van verzender en ontvanger wordt voor dit koppelvlak op transportniveau afgehandeld.

1.3.3 *Vertrouwelijkheid*

Berichtencryptie is niet op koppelvlakniveau ingericht. Aangezien Digipoort van de inhoud van een bericht afblijft kan payloadversleuteling een afspraak zijn tussen de stroomeigenaar en aanleveraars. Wel roept dit vragen op met betrekking tot de herbruikbaarheid van data: als berichten voor overheidspartij X versleuteld zijn, kunnen deze niet zonder meer worden hergebruikt door overheidspartij Y.


```
X-Env-Sender: dinv1234@mail.otpnet.nl
X-Env-Recipient: sagittainvoer@nl.defg.net NOTIFY=10
X-DSN-RET: 2
X-DSN-ENVID: P1B61H10314668A1
X-End-of-Envelope:
X-Mailer: OtpTransfer v1.083
Message-ID: <2009082716212002*/OU=DOUANE-INV-
PROD/O=CENTRAAL/PRMD=BELASTINGDIENST/ADMD=400NET/C=NL/@MHS>
From: <dinv1234@mail.otpnet.nl>
To: <sagittainvoer@nl.defg.net>
Subject: //2009082716212002/1GT4H700/
Date: Thu, 27 Aug 2009 16:21:20 +0100
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII; name="dinv1020-20090827-
142122.164-P1B61H10314668A1.txt"
Content-Disposition: attachment; filename="dinv1020-20090827-
142122.164-P1B61H10314668A1.txt"
Content-Transfer-Encoding: base64

TG9yZW0gaXBzdW0gZG9sb3Igc2l0IGFtZXQsIGNvbmluY3RldHVyIGFkaXBpc2ljaW5n
IGVsaXQs
IHNlZCBkbyBlaXVzbW9kIHRlbXBvcjBpbmNpZGlkdW50IHV0IGxhYm9yZSBldCBkb2xv
cmUgbWFn
bmEgYWxpcXVhLiBVdCB1bmltIGFkIGlpbmltIHZlbmlhbSwgcXVpcyBub3N0cnVkJGV4
ZXJjaXRh
dGlvbiB1bGxhbWVnIGxhYm9yaXMgbmlzaSBldCBhbGlxdWlwIGV4IGVhIGNvbWlvZG8g
Y29uc2Vx
dWF0LiBEdWlzIGFldGUgaXJlcmUgZG9sb3IgaW4gcmVwcmVozW5kZXJpdCBpbiB2b2x1
cHRhdGUg
dmVsaXQgZXRzZSBjaWxsZW0gZG9sb3JlIGVlIGZlZ2lhdCBudWxsYSBwYXJpYXR1ci4g
RXhjZXB0
ZXVyIHNpbnQgb2NjYWVjYXQgY3VwaWRhdGF0IG5vbiBwcm9pZGVudCwgc3VudCBpbiBj
dWxwYSBx
dWkgb2ZmaWNpYSBkZXNlcnVudCBtb2xsaXQgYW5pbSBpZCB1c3QgbGFib3JlbS4=
```

1.4.3

Delivery report

Onderstaand voorbeeld geeft een Delivery Status Notification weer (positieve transportbevestiging).

Return-Path: <>
Received: from kslv023.esn.kpn.com (10.30.2.23) by
kslv019.esn.kpn.com (8.5.113)
id 4A7BE27F00000012 for ton@bedrijven.test.otp.nl; Tue, 25
Aug 2009 18:19:56 +0200
Received: by kslv023.esn.kpn.com (8.5.113) id 4A8576E70000001C for
ton@bedrijven.test.otp.nl; Tue, 25 Aug 2009 18:19:56 +0200
X-Mailer: OtpTransfer vl.084
From: <postmaster@mail.test.otp.nl>
To: <ton@bedrijven.test.otp.nl>
Message-ID: <M23767e418b9e0b474e6e00f314c10cd3@mail.test.otp.nl>
Date: Tue, 25 Aug 2009 18:19:54 +0200
Subject: Delivery Status Notification (success) for
tonox0005@mail.test.otp.nl
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;
boundary=B6169063283556c1ed30730512e863d00

This multi-part MIME message contains a Delivery Status
Notification.
If you can see this text, your mail client may not be able to
understand MIME
formatted messages or DSNs (see RFC 2045 through 2049 for general
MIME
information and RFC 1891 through 1894 for DSN specific information).

--B6169063283556c1ed30730512e863d00
Content-Type: text/plain; charset=US-ASCII

Your message (id Envy) was successfully delivered to
<tonox0005@mail.test.otp.nl>.

--B6169063283556c1ed30730512e863d00
Content-Type: message/delivery-status

Reporting-MTA: dns;mail.test.otp.nl
Original-Envelope-ID: Envy

Final-Recipient: rfc822;tonox0005@mail.test.otp.nl
Action: delivered
Status: 2.0.0

--B6169063283556c1ed30730512e863d00
Content-Type: Text/RFC822-headers

Received: from kslv027.esn.kpn.com (10.30.2.27) by
kslv023.esn.kpn.com (8.5.113)
id 4A8576E70000001B for tonox0005@mail.test.otp.nl; Tue, 25
Aug 2009 18:19:52 +0200
Received: from localhost.localdomain (10.30.2.16) by
kslv027.esn.kpn.com (8.5.113) (authenticated as
ton@bedrijven.test.otp.nl)
id 4A939F2200000006 for tonox0005@mail.test.otp.nl; Tue, 25
Aug 2009 18:19:52 +0200
From: "Neil Armstrong" <ton@bedrijven.test.otp.nl>
To: "Target" <tonox0005@mail.test.otp.nl>
Message-ID: <fool12@the.dude>
Date: Tue, 12 Mar 18:30:06 2002 +0200
Subject: Zo simpel
MIME-Version: 1.0
Content-Type: text/plain
Content-Transfer-Encoding: base64

--B6169063283556c1ed30730512e863d00--

2 Algemene afspraken

2.1 Standaarden

2.1.1 Normatieve RFCs voor berichttransport

Standaard	Referentie
Simple Mail Transfer Protocol	ftp://ftp.rfc-editor.org/in-notes/rfc2821.txt
Mail Routing and the domain system	ftp://ftp.rfc-editor.org/in-notes/rfc974.txt
SMTP Service Extension for Delivery Status Notification	ftp://ftp.rfc-editor.org/in-notes/rfc1891.txt
SMTP Service Extension for Remote Message Queue Starting	ftp://ftp.rfc-editor.org/in-notes/rfc1985.txt

2.1.2 Normatieve RFCs voor berichtinhoud

Standaard	Referentie
Internet Message Format	ftp://ftp.rfc-editor.org/in-notes/rfc2822.txt
MIME part 1 – Format of Internet Message Bodies	ftp://ftp.rfc-editor.org/in-notes/rfc2045.txt
MIME part 2 – Media Types	ftp://ftp.rfc-editor.org/in-notes/rfc2046.txt
MIME part 3 – Message Header Extensions for non-ASCII text	ftp://ftp.rfc-editor.org/in-notes/rfc2047.txt
MIME part 4 – Registration Procedures	ftp://ftp.rfc-editor.org/in-notes/rfc2048.txt
MIME part 5 – Conformance Criteria and Examples	ftp://ftp.rfc-editor.org/in-notes/rfc2049.txt
MIXER (MIME Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME	ftp://ftp.rfc-editor.org/in-notes/rfc2156.txt
Mapping between X.400 and RFC 822/MIME Message Bodies	ftp://ftp.rfc-editor.org/in-notes/rfc2157.txt
Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field	ftp://ftp.rfc-editor.org/in-notes/rfc2183.txt

2.2 Randvoorwaarden

Deze zijn beschreven in de protocolstandaarden.

2.3 Foutmeldingen

Deze zijn beschreven in de protocolstandaarden voor wat betreft de interactie tussen MTA's.

Logische fouten die leiden tot afkeuren van berichten en versturen van negatieve Delivery Status Notifications (DSNs) zijn onder meer:

- Kan bekende SMTP headers niet parsen

- Niet ondersteund Content-Type
- Geen body parts aanwezig
- Meer dan 1 body part aanwezig
- Ongeldige Base64, quoted printable
- High ascii in een 7-bit bericht
- Onbekende content-transfer-encoding
- Multipart mime parts zijn niet te parsen
- Mailadressen (in welke vertaalde header dan ook) zijn onbekend bij Digipoort
- Ongeautoriseerde koppeling (voorbeeld: bedrijven naar bedrijven).
- Logisch adres is nog niet geactiveerd.

2.4 Adressen

Deze worden verstrekt na het aanvragen van een account.

2.5 Limieten

Deze worden verstrekt na het aanvragen van een account.

2.6 Ondersteuning

Ondersteuning bij aansluiten en gebruik wordt gegeven door het Servicecentrum Logius. Zie het colofon voor contactgegevens.