Douane
Belastingdienst

Koppelvlakbeschrijving HTG SMTP-MSA en POP3

Versie 1.1

Datum: 24-08-2020
Status: Definitief

Colofon

Titel	Koppelvlakbeschrijving HTG SMTP-MSA en POP3
Organisatie	Nationale Helpdesk Douane T 088 156 66 55 nhd.apeldoorn@belastingdienst.nl

Inhoud

1 Inleiding

1.1 Beschikbare koppelvlakken

De Handel en Transport Gateway (HTG) (voorheen Digipoort Handel & Transport) is een generieke elektronische toegangsdienst waarmee het bedrijfsleven, werkzaam in het domein Handel en Transport, met de overheid elektronische informatie kan uitwisselen. Het succesvol functioneren van de HTG staat of valt met een goede beschrijving van de koppelvlakken waarop de overheid en het bedrijfsleven moeten kunnen aansluiten.

HTG biedt het bedrijfsleven en de overheid koppelvlakken op basis van mail-berichten:

- SMTP-MTA (server-to-server)
- SMTP-MSA en POP3.

Voor elk koppelvlak is een specificatie beschikbaar. Dit document geeft invulling aan twee van deze koppelvlakken, namelijk het SMTP-MSA koppelvlak en het POP3 koppelvlak.

De volgende tabel geeft aan welke koppelvlakbeschrijvingen voor welke berichtstromen gelden.

Berichtstroom	Type koppelvlak	Document
Logistieke berichtstromen voor Douane en voor NVWA	SMTP-MTA	Koppelvlakbeschrijving HTG SMTP-MTA
	SMTP-MSA/POP3	Koppelvlakbeschrijving HTG SMTP-MSA en POP3
Single Window berichtstroom voor Rijkswaterstaat/NCA SSN, Grensbewaking (KMar/ Zeehavenpolitie) en Douane	SMTP-MTA	Koppelvlakbeschrijving HTG Single Window in aanvulling op Koppelvlakbeschrijving HTG SMTP-MTA
	SMTP-MSA/POP3	Koppelvlakbeschrijving HTG Single Window in aanvulling op Koppelvlakbeschrijving HTG SMTP-MSA en POP3
Logistieke berichtstromen met een extra bijlage	SMTP-MTA	Koppelvlakbeschrijving HTG Bericht met extra bijlage in aanvulling op Koppelvlakbeschrijving HTG SMTP-MTA
	SMTP-MSA/POP3	Koppelvlakbeschrijving HTG Bericht met extra bijlage in aanvulling op Koppelvlakbeschrijving HTG SMTP-MSA en POP3

Tabel 1: Berichtstromen en koppelvlakbeschrijvingen

1.2 Doelgroep

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

1.3 SMTP-MSA en POP3

Deze koppelvlakken zijn bedoeld voor laagfrequente interactie tussen bedrijfsleven en HTG (dat wil zeggen niet meer dan 1 interactie per aansluiting per minuut) en wordt ad-hoc over een TCP/IP (internet) verbinding benaderd. Zodra de transacties met het koppelvlak voltooid zijn wordt de verbinding weer verbroken. Voor hoogfrequente interactie moet het koppelvlak SMTP-MTA worden gebruikt. Vooralsnog zal het koppelvlak geen beperkingen opleggen aan de frequentie van het gebruik.

Op basis van de koppelvlakken SMTP-MSA en POP3 kunnen berichten met behulp van een mailclient bij HTG worden aangeleverd, respectievelijk worden opgehaald. Het SMTP-MSA

koppelvlak is bedoeld voor berichten van het bedrijfsleven naar de overheid. Voor berichtenverkeer in omgekeerde richting is het POP3 koppelvlak beschikbaar.

Het SMTP-MSA en POP3 koppelvlak bieden samen een alternatief voor het SMTP-MTA (server-to-server) koppelvlak. Voor server-to-server koppelingen is het opzetten van een Virtual Private Network (VPN) noodzakelijk. De last van het opzetten van een dergelijke verbinding is voor sommige bedrijven te hoog. Het SMTP-MSA koppelvlak en POP3 koppelvlak bieden samen een alternatief waarbij geen VPN vereist is. Het uitgangspunt van dit koppelvlak blijft echter laagfrequente interactie.

1.4 Ondersteuning

Ondersteuning bij aansluiten en gebruik wordt gegeven door de Nationale Helpdesk Douane (NHD).

1.5 Leeswijzer

Dit document is als volgt opgebouwd. Hoofdstuk 1 bevat algemene informatie. Hoofdstuk 2 bevat een globale procesbeschrijving. Hoofdstuk 3 bevat de beschrijving van het SMTP-MSA koppelvlak voor het aanleveren van berichten door het bedrijfsleven naar de overheid. Hoofdstuk 4 bevat de beschrijving van de werking van het POP3 koppelvlak, de beschrijving van de werking van het ophalen van berichten door het bedrijfsleven. Hoofdstuk 5 bevat een beschrijving van de opbouw van het SMTP-bericht. Het document wordt afgesloten met een lijst van afkortingen in hoofdstuk 6.

1.6 Versiehistorie

Versie	Datum	Veranderingen (concept/definitief)
1.0	14-11-2019	Definitieve versie.
1.01	06-12-2019	Fout hersteld in hoofdstuk 5, adres van de ontvanger.
1.02	10-12-2019	Wijziging titelblad.
1.1	24-08-2020	Paragraaf 1.1 Beschikbare koppelvlakken aangevuld vanwege mogelijkheid extra bijlage.

2 Procesbeschrijving

2.1 Algemeen

Elektronische berichten in de logistieke keten Handel en Transport worden door marktpartijen naar overheden verstuurd of van overheden naar marktpartijen. Hiervoor is de voorziening "Handel en Transport Gateway" (HTG) beschikbaar (met daarbinnen het domein htpoort.nl). Deze beschrijving is van belang voor marktpartijen die zelf aansluiten op de HTG. Een marktpartij kan met meerdere e-mailadressen op dezelfde berichtstroom zijn aangesloten. De elektronische berichtuitwisseling tussen overheidspartijen onderling gebeurt via andere koppelvlakken.

Binnen de voorziening HTG vindt, naast controle op de koppelvlakbeschrijving, geen validatie plaats op de inhoud van het bericht (dat wil zeggen geen syntaxcontrole en geen semantiekcontrole).

Binnen HTG worden meerdere berichtstromen onderscheiden voor een aantal overheidspartijen. Een overzicht van de berichtstromen is opgenomen in Tabel 2.

Berichtstroom	Overheidspartijen
Aangiftebehandeling (AGS)	Douane
Aangiftebehandeling convenant partners (AGSC)	Douane
Aangiftebehandeling (DMS)	Douane
Aangiftebehandeling convenant partners (DMSC)	Douane
EMCS	Douane
NCTS / Transit	Douane
CID Informatieverstrekking	Douane
Single Window (voor maritiem en lucht) [1]	Rijkswaterstaat, Douane en Grensbewaking
Vooraanmelding import dierlijke producten	NVWA
Vooraanmelding import plantaardige producten	NVWA
E-logboek visvaartuigen	NVWA

Tabel 2: Berichtstromen op HTG die via SMTP kunnen worden aangeleverd

2.2 Berichtverwerking

HTG conformeert zich bij de berichtverwerking aan de SMTP standaarden, zoals vastgelegd door de IETF. De berichtverwerking door HTG begint met het aanleveren van een bericht. Hierop wordt door HTG binnen dit koppelvlak gereageerd conform de SMTP standaarden.

2.2.1 Aanleveren

Bij het aanleveren van een bericht wordt door HTG vastgesteld of het, in het kader van de betrouwbare werking van HTG, verantwoord is een aangeleverd bericht technisch te accepteren. HTG voert hiertoe de essentiële technische controles uit, zoals een geldige autorisatie, correcte adressering en maximale berichtgrootte.

2.2.2 Ontvangstbevestiging

HTG implementeert de terugkoppeling van acceptatie en weigering van een bericht conform de SMTP standaarden. Dat betekent dat het bericht door de overheid technisch is geaccepteerd zodra de SMTP-server een "250 Ok" response heeft gegeven op het SMTP DATA commando. Het is voor het bedrijfsleven aanvullend mogelijk om tijdens het aanleveren van een bericht te verzoeken om een Delivery Status Notification (DSN). Als in het SMTP RCPT commandogeen NOTIFY-waarden

1 Single Window maakt voor het berichttransport gebruik van de SMTP-MTA of SMTP-MSA en POP3 koppelvlakken, maar kent daarnaast nog aanvullende eisen. Daarom is voor Single Window een aparte aanvullende koppelvlakbeschrijving beschikbaar.

worden meegegeven, wordt standaard alleen bij weigering van het bericht een (negatieve) DSN teruggestuurd. Als een bedrijf bij acceptatie ook een (positieve) DSN wil ontvangen, dan dient dit expliciet te worden aangegeven door middel van het SMTP RCPT commando, waarde NOTIFY (SUCCESS,FAILURE).

HTG accepteert DSN's die worden gestuurd door een marktpartij, maar verplicht het gebruik ervan niet.

2.2.3 Afleveren

HTG verzorgt de aflevering van berichten. Als een bericht moet worden afgeleverd aan een overheidspartij, dan zet HTG een verbinding op met de server van de overheidspartij en na verificatie en het uitvoeren van controles wordt het bericht afgeleverd. Als het bericht moet worden afgeleverd bij een marktpartij met een berichtopslag (POP3 postbus) dan plaatst HTG het bericht in de berichtopslag. De marktpartij moet daarna zelf periodiek het initiatief nemen om via POP3 een verbinding te maken met HTG om het bericht op te halen uit de berichtopslag.

2.3 Koppelvlak

HTG biedt een basisdienstverlening waarvan bedrijven en overheden gebruik kunnen maken. Het koppelvlak SMTP-MSA/POP3 is dusdanig opgezet dat deze de basis biedt voor het uitwisselen van berichten met HTG. Deze koppelvlakbeschrijving geeft aan welke specificaties (RFC's) gelden voor het inzenden en ophalen van berichten en welke specificaties gelden voor de opbouw van berichten.

In deze koppelvlakbeschrijving wordt geen uitspraak gedaan over de werkelijke inhoud van het bericht dat via het koppelvlak wordt verstuurd. Die berichtspecificaties zijn in aparte MIG's vastgelegd door de betrokken overheden.

De koppelvlakbeschrijving wordt in de volgende hoofdstukken verder uitgewerkt.

3 Interactie via SMTP-MSA koppelvlak (aanleveren van berichten)

3.1 Gebruik van Message Submission for Mail

Voor het aanleveren van SMTP-verkeer wordt normaliter een Message Transfer Agent (MTA) ingezet. Deze MTA's zijn voor het afgeven van een bericht benaderbaar op 25/tcp (TCP/IP protocol via poort 25). Er zijn echter veel Internet Service Providers (ISP's) die deze poort van binnenuit blokkeren, waardoor het voor een gebruiker van een gehuurde internetverbinding niet mogelijk is om SMTP-verkeer te onderhouden met een andere partij. Providers bieden een standaardoplossing door alle verkeer via hun eigen MTA te leiden.

Hierdoor is het moeilijk om een beveiligde server-to-server verbinding op te zetten tussen een bedrijf en HTG. Daarom biedt HTG een Message Submission Agent (MSA) in plaats van een standaard MTA. Bedrijven sturen daarmee hun berichten rechtstreeks naar HTG in plaats van hun eigen MTA of de doorgifte van de ISP te gebruiken. De MSA is te bereiken via 587/tcp.

3.1.1 Principe van MSA

Het principe van de MSA wordt beschreven in "Message Submission for Mail" – Request for Comments (RFC) 6409. De insteek van de RFC is als volgt:

> het scheiden van het aannemen en doorgeven van berichten, waardoor de verschillende diensten kunnen werken volgens eigen regels (voor beveiliging, beleid, etc.).

De rol die HTG vervult aan de grens van het overheidsdomein maakt het noodzakelijk om aan zaken als beveiliging en beleid een eigen invulling te geven. Het SMTP-MSA-koppelvlak biedt bedrijven een mogelijkheid voor het aanbieden van berichten bij HTG.

3.1.2 IANA overwegingen ten aanzien van SMTP-MSA

Een groot voordeel van het gebruik van SMTP-MSA is dat deze een door de Internet Assigned Numbers Authority (IANA) toegekende TCP poort gebruikt anders dan 25/tcp, te weten 587/tcp.

3.1.3 Authenticatie

Authenticatie op sessieniveau dient plaats te vinden op basis van SMTP Service Extension for Authentication (SMTP-AUTH). In hoofdstuk 4.3 van RFC 6409 wordt voorgeschreven dat de MSA standaard een foutcode teruggeeft als het MAIL commando wordt gegeven en de sessie nog niet geauthenticeerd is. Dit wordt verder uitgewerkt in paragraaf 3.3.2 van dit document.

3.2 Inhoud

De inhoud van de aan de MSA aangeboden berichten moet zich conformeren aan de in dit document beschreven beperkingen.

3.3 Beveiliging

De beveiliging van het koppelvlak richt zich op de bescherming van de data tussen verzender en ontvanger. Authenticiteit en integriteit van het verzonden bericht worden niet gewaarborgd. Authenticiteit van de verzender van het bericht wordt echter wel in zekere mate gewaarborgd doordat toegangsautorisatie wordt verleend.

3.3.1 Vertrouwelijkheid van transport

Het transport tussen client en server naar het koppelvlak wordt beveiligd door gebruik te maken van zogeheten 1-weg Transport Layer Security (TLS). Alleen het TLS certificaat van de HTG server wordt gebruikt om een beveiligde verbinding op te zetten. Na het initiëren van de verbinding moet direct een TLS verbinding worden opgezet (met het STARTTLS commando) waarover het verdere SMTP verkeer wordt uitgewisseld. Dit principe wordt voor SMTP beschreven in RFC 3207: ”SMTP Service Extension for Secure SMTP over TLS”. Pas na het opzetten van de TLS verbinding is het mogelijk om te authenticeren.

3.3.2 Authenticatie en autorisatie van client

De client moet zich na het opzetten van een TLS verbinding authenticeren voordat deze geautoriseerd is om berichten aan te leveren. Authenticatie geschiedt door middel van gebruikersnaam en wachtwoord.

Het koppelvlak maakt gebruik van SMTP-AUTH en Simple Authentication and Security Layer (SASL) – RFC 4422. Deze twee standaarden tezamen bieden een raamwerk voor implementaties van diverse authenticatiemethoden, waaronder gebruikersnaam en wachtwoord. Telkens als hieronder over SASL wordt gesproken wordt de combinatie SMTP-AUTH/SASL bedoeld.

Het koppelvlak ondersteunt de SASL-mechanismen PLAIN en LOGIN[2]. Doordat het opzetten van de TLS verbinding voor authenticatie verplicht is, is het wachtwoord voldoende beschermd.

3.3.3 Onderkende risico’s en maatregelen

Geen van de bestaande SASL mechanismen is onfeilbaar en alle waarschuwen voor meerdere typen aanvallen. De inrichting van het koppelvlak vraagt extra aandacht voor de volgende risico’s:

Risico	**Maatregel**
Alle door de client gegeven commando’s die voorafgaan aan het STARTTLS commando zijn in “plain text” en voor rekening en verantwoording van de client. Het is aan de client om het STARTTLS commando te geven. Als de client dit achterwege laat is de verbinding niet beveiligd. Dit risico geldt in het bijzonder bij gebruik van de SASL-mechanismen ‘PLAIN’ en ‘LOGIN’.	De MSA server mag voordat het STARTTLS commando volledig en goed is afgewerkt geen enkel gegeven commando honoreren behalve NOOP, EHLO, QUIT en STARTTLS zelf. De server moet alle andere commando’s beantwoorden met een foutcode 5xx.
Een Man-In-The-Middle (MITM) aanval is mogelijk door het fingeren van het antwoord van het STARTTLS commando door de client. De client denkt nu dat TLS niet mogelijk is en zal het afleveren van mail doorzetten in een plain text variant waardoor de bericht inhoud voor de MITM leesbaar is.	MITM aanvallen op SASL zijn vrijwel onmogelijk als de TLS verbinding goed tot stand is gekomen. Voorwaarde is wel dat de client het door de server verstrekte certificaat daadwerkelijk controleert op geldigheid en authenticiteit.

2 Het HTG koppelvlak ondersteunt SASL-mechanisme DIGEST-MD5 niet. Voor de ondersteuning van dit mechanisme moet de SMTP-server kunnen beschikken over het originele wachtwoord, dat dan moet worden opgeslagen. De server van HTG slaat de originele wachtwoorden niet op, maar uitsluitend een *one way hash* van het wachtwoord. Hierdoor is het niet mogelijk om DIGEST-MD5 te ondersteunen. Los daarvan is DIGEST-MD5 door IETF als verouderd bestempeld (zie Moving DIGEST-MD5 to Historic – RFC 6331).

3.4 Voorbeeld

Het onderstaande voorbeeld geeft de interactie tussen client en server weer bij het opbouwen van een sessie en het verzenden van een bericht.

```
<server (S) wacht op een TCP connectie op poort 587>
<client (C) opent een TCP connectie op poort 587>
S: 220 msa-smtp.htpoort.nl ESMTP
C: EHLO mijnbedrijf.nl
S: 250-msa-smtp.htpoort.nl
   250-STARTTLS
C: STARTTLS
S: 220 Ready to start TLS
S & C: <TLS verbinding tussen client en server wordt opgezet>
C: AUTH PLAIN
S & C: <Het PLAIN authenticatie scenario wordt uitgevoerd>
C: MAIL FROM:<ik@mijnbedrijf.nl>
S: 250 2.1.0 Ok
C: RCPT TO:<douaneproces@htpoort.nl>
S: 250 2.1.5 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: <Voert SMTP headers en MIME bericht in>
C: .
S: 250 2.0.0 Ok: queued as AE73753501E        <-- [3]
C: QUIT
<server sluit verbinding>
```

3.5 Standaarden

Standaard	Referentie
TCP/IP	https://tools.ietf.org/html/rfc793 https://tools.ietf.org/html/rfc1122 https://tools.ietf.org/html/rfc1958
Simple Message Transfer Protocol (SMTP)	https://tools.ietf.org/html/rfc5321
Message Submission for Mail (MSA)	https://tools.ietf.org/html/rfc6409
SMTP Service Extension for Authentication (SMTP-AUTH)	https://tools.ietf.org/html/rfc4954
Simple Authentication and Security Layer (SASL)	https://tools.ietf.org/html/rfc4422
Transport Layer Security v1.2 (TLS)	https://tools.ietf.org/html/rfc5246
PLAIN SASL Mechanism	https://tools.ietf.org/html/rfc4616
SMTP Service Extension for Secure SMTP over TLS	https://tools.ietf.org/html/rfc3207

3.6 Randvoorwaarden en afspraken

Alle van toepassing zijnde randvoorwaarden en foutmeldingen zijn reeds beschreven in de normatieve RFC's en deze koppelvlakbeschrijving.

RFC 6409 staat het een MSA toe om e-mail adressen te herschrijven. HTG verwacht bij aanbieding volledige adressen, en herschrijft adressen niet.

3.7 Adressen, gebruikersnaam en wachtwoord

E-mail adressen worden verstrekt na het aanvragen van een account.

3 Met deze "250 OK" accepteert de SMTP-MSA de verantwoordelijkheid om het bericht af te leveren, of om door middel van een DSN te melden dat aflevering niet mogelijk is.

De gebruikersnaam en het wachtwoord worden ook verstrekt na het aanvragen van een account. De gebruikersnaam is de volledige postbusnaam, dus inclusief domein. Het aanvragen van een nieuw wachtwoord is mogelijk door contact op te nemen met de Nationale Helpdesk Douane.

3.8 Limieten en beperkingen

Technische beperkingen van het koppelvlak worden verstrekt na het aanvragen van een account.

4 Interactie via POP3 koppelvlak (ophalen van berichten)

4.1 Gebruik van POP3

Het principe van POP3 wordt beschreven in "Post Office Protocol 3" - RFC 1939. POP3 is bedoeld als toegang tot een berichtenopslag[4]. Deze berichtenopslag bevat alle berichten die bestemd zijn voor een bepaalde gebruiker. Zodra een gebruiker zich heeft geauthenticeerd en toegang heeft gekregen tot zijn berichtenopslag kunnen berichten worden opgehaald.

4.1.1 Drie fasen van een POP3 transactie

Het POP3 protocol kent drie fases waarin het actief is: AUTHORIZATION, TRANSACTION en UPDATE. Tijdens de AUTHORIZATION fase kan een client alleen de mogelijkheden van de server bevragen en zich aanmelden. In de TRANSACTION fase kunnen berichten van de gebruiker worden opgehaald en/of verwijderd. Na de TRANSACTION fase gaat de server automatisch over in de UPDATE fase.

AUTHORIZATION fase
In deze fase moet de client zich authenticeren en daarmee autorisatie krijgen voor het benaderen van de berichtopslag. Dit gebeurt door een combinatie van het USER en PASS commando. De client kan met het CAPA commando de mogelijkheden van de server opvragen. Zodra de autorisatie is verleend begint de TRANSACTION fase.
Als de client hier een QUIT commando geeft, worden de volgende fasen overgeslagen en wordt de verbinding gesloten.

TRANSACTION fase
Als een client autorisatie heeft verkregen voor een berichtopslag komt de server in deze fase. Hier kunnen berichten worden opgehaald en verwijderd. Hiervoor worden respectievelijk de commando's RETR en DELE gebruikt. Het daadwerkelijk verwijderen gebeurt niet in deze fase maar in de UPDATE fase. Zodra de client hier een QUIT commando ingeeft wordt de TRANSACTION fase afgesloten en de UPDATE fase opgestart.

Van een client wordt verwacht dat, na een RETR commando en succesvolle verwerking van het bericht, ook een verwijdering van het bericht volgt door middel van een DELE commando. Het is dus expliciet niet de bedoeling om verwerkte berichten langdurig in de berichtopslag te laten staan.

UPDATE fase
In de UPDATE fase voert de server de gevraagde verwijderingen door.

4.1.2 IANA overwegingen

POP3 opereert op een door de Internet Assigned Numbers Authority (IANA) toegekende TCP poort te weten 110/tcp.

4.2 Inhoud

De inhoud van de uit de POP3-postbus opgehaalde berichten conformeren zich aan de in dit document beschreven beperkingen.

4.3 Beveiliging

De beveiliging van het koppelvlak houdt zich bezig met de bescherming van de data tussen verzender en ontvanger.

4 In het spraakgebruik wordt een berichtenopslag vaak postbus genoemd.

4.3.1 Vertrouwelijkheid van transport

Het transport tussen client en server naar het koppelvlak wordt beveiligd door gebruik te maken van zogeheten 1-weg Transport Layer Security (TLS). Alleen het TLS certificaat van de server wordt gebruikt om een symmetrisch beveiligde verbinding op te zetten.
Na het initiëren van de TCP verbinding moet direct een TLS verbinding worden opgezet (met het STLS commando) waarover het verdere POP3 verkeer wordt uitgewisseld. Dit principe wordt beschreven in RFC 2595: ”Using TLS with IMAP, POP3 and ACAP”. Pas na het opzetten van de TLS verbinding is het mogelijk om te authenticeren.

4.3.2 Authenticatie en autorisatie van client

De client moet zich na het opzetten van een TLS verbinding authenticeren voordat deze geautoriseerd is om berichten op te halen. Authenticatie geschiedt door middel van gebruikersnaam en wachtwoord.

Het koppelvlak maakt gebruikt van de Simple Authentication and Security Layer (SASL) – RFC 4422. Deze standaard biedt een raamwerk voor implementaties van diverse authenticatie-methoden, waaronder gebruikersnaam en wachtwoord.

Het koppelvlak ondersteunt de SASL-mechanismen PLAIN en LOGIN[5]. Doordat het opzetten van de TLS verbinding voor authenticatie verplicht is, is het wachtwoord voldoende beschermd.

4.3.3 Onderkende risico’s en maatregelen

Geen van de bestaande SASL mechanismen is onfeilbaar en alle waarschuwen voor meerdere typen aanvallen. De inrichting van het koppelvlak vraagt extra aandacht voor de volgende risico’s:

Risico	**Maatregel**
Alle door de client gegeven commando’s die voorafgaan aan het STLS commando zijn in “plain text” en voor rekening en verantwoording van de client. Het is aan de client om het STLS commando te geven. Als de client dit achterwege laat is de verbinding niet beveiligd. Dit risico geldt in het bijzonder bij gebruik van de SASL-mechanismen ‘PLAIN’ en ‘LOGIN’.	De POP3 server mag voordat het STLS commando volledig en goed is afgewerkt geen enkel gegeven commando honoreren behalve QUIT en STLS zelf. De POP3-server mag de AUTHORIZATION state niet verlaten voordat het STLS-commando is gegeven en een goede TLS-verbinding tot stand is gekomen.
Een Man-In-The-Middle (MITM) aanval is mogelijk door het fingeren van het antwoord van het STLS commando door de client. De client denkt nu dat TLS niet mogelijk is en zal het afleveren van mail doorzetten in een plain text variant waardoor de bericht inhoud voor de MITM leesbaar is.	MITM aanvallen op SASL zijn vrijwel onmogelijk als de TLS verbinding goed tot stand is gekomen. Voorwaarde is wel dat de client het door de server verstrekte certificaat daadwerkelijk controleert op geldigheid en authenticiteit.

5 Ook voor het POP3 koppelvlak geldt dat HTG het SASL-mechanisme DIGEST-MD5 niet ondersteunt. Zie paragraaf 3.3.2.

4.4 Voorbeeld

Het onderstaande voorbeeld geeft de interactie tussen client en server weer bij het opbouwen van een sessie en het verzenden van een bericht.

```
<server (S) wacht op een TCP connectie op poort 110>
<client (C) opent een TCP connectie op poort 110>
S: +OK Hello there.
C: CAPA
S: +OK Here's what I can do
TOP
STLS
C: STLS
S: +OK Begin TLS negotiation
S & C: <TLS-verbinding tussen client en server wordt opgezet>
C: AUTH PLAIN
S & C: <Het PLAIN authenticatie scenario wordt uitgevoerd>
S: +OK Maildrop locked and ready
C: LIST
S: +OK
1 12288
2 31048713
C: RETR 1
S: +OK 12288 octets follow
<geeft het MIME bericht met ID 1 terug>
C: DELE 1
S: +OK Message 1 deleted
C: QUIT
<server verwijdert bericht met ID 1 en sluit verbinding>
```

4.5 Standaarden

Standaard	Referentie
TCP/IP	https://tools.ietf.org/html/rfc793 https://tools.ietf.org/html/rfc1122 https://tools.ietf.org/html/rfc1958
Post Office Protocol – Version 3 (POP3)	https://tools.ietf.org/html/rfc1939
Simple Authentication and Security Layer (SASL)	https://tools.ietf.org/html/rfc4422
Transport Layer Security v1.2 (TLS)	https://tools.ietf.org/html/rfc5246
Using TLS with IMAP, POP3 and ACAP	https://tools.ietf.org/html/rfc2595
POP3 SASL Authentication Mechanism	https://tools.ietf.org/html/rfc5034
PLAIN SASL Mechanism	https://tools.ietf.org/html/rfc4616

4.6 Randvoorwaarden en afspraken

Alle van toepassing zijnde randvoorwaarden en foutmeldingen zijn reeds beschreven in de normatieve RFC's.

4.7 Adressen, gebruikersnaam en wachtwoord

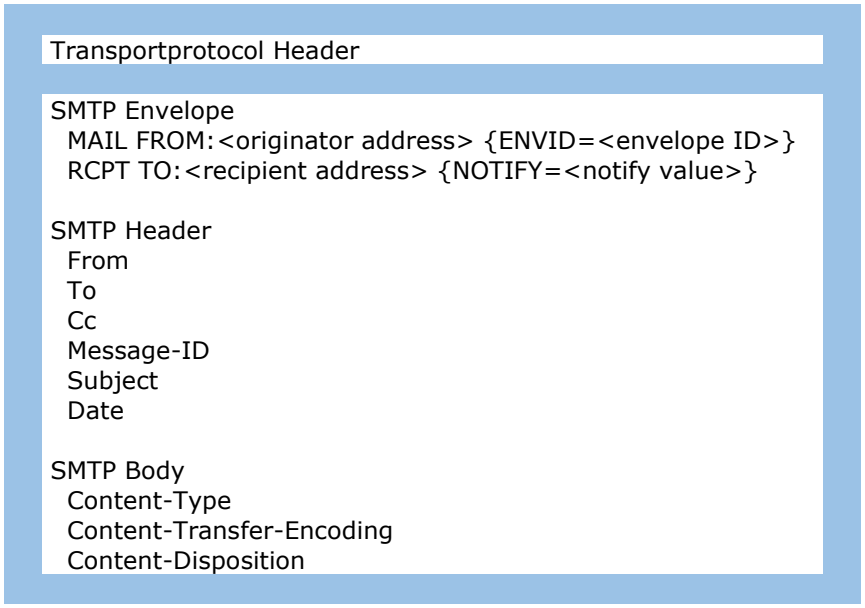
E-mail adressen worden verstrekt na het aanvragen van een account.

De gebruikersnaam en het wachtwoord worden ook verstrekt na het aanvragen van een account. De gebruikersnaam is de volledige postbusnaam, dus inclusief domein. Het aanvragen van een nieuw wachtwoord is mogelijk door contact op te nemen met de Nationale Helpdesk Douane.

4.8 Limieten en beperkingen

Technische beperkingen van het koppelvlak worden verstrekt na het aanvragen van een account.

5 Berichtstroom specificaties



Element	**Specificatie**
MAIL FROM:<originator address> {ENVID=<envelope ID>}	De verzender van de mail (originator address). Elke mail heeft precies één verzender. Als een ontvangstbevestiging wordt gevraagd moet een uniek ID worden meegegeven (envelope ID).
RCPT TO:<recipient address> {NOTIFY=SUCCCESS,FAILURE}	De ontvanger van de mail (recipient address). Elke mail heeft precies één ontvanger. Met de NOTIFY-optie kan worden aangegeven welke afleverbevestigingen (of berichten van geen aflevering) worden verstuurd door de MSA. Afhankelijk van de HTG omgeving waar naar verzonden wordt kan gekozen worden uit: <berichtsoort>@msa-smtp.htpoort.nl <berichtsoort>@msa-smtp.preprod.htpoort.nl
DATA [6]	De berichtinhoud (SMTP headers en body).

Tabel 3: SMTP Envelope

6 Zie Tabel 4 en Tabel 5 voor de invulling van SMTP headers en body.

Element	Specificatie
From	Adres van de verzender van het bericht.
To	Adres van de ontvanger van het bericht. Afhankelijk van de HTG omgeving waar naar verzonden wordt, kan gekozen worden uit: <berichtsoort>@htpoort.nl <berichtsoort>@preprod.htpoort.nl
(Cc)	Aangezien een mail slechts één ontvanger heeft, is het gebruik van Cc (en Bcc) niet toegestaan.
Message-ID	Een unieke identificatie van het bericht. De verzender kan deze invullen mits deze uniek is. Indien een message-ID ontbreekt voegt HTG 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.

Tabel 4: SMTP Headers

Element	Waarde	Toelichting
Content-Type	text/plain; charset=us-ascii	Voorkeurswaarde voor tekst-gebaseerde berichten. Andere waarden voor charset zijn toegestaan[7]. Bij ontbreken van een waarde wordt us-ascii aangenomen. De hier vermelde toegestane waarden gelden voor het SMTP-MSA en POP3 koppelvlak. In de berichtspecificatie (MIG) van de betreffende berichtstroom kunnen voor de inhoudelijke berichten andere eisen worden gesteld aan de te gebruiken tekenset. 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/xml	Alternatief voor berichten in XML 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-waarden 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.
Content-Disposition	attachment filename=<bestandsnaam>.<extensie>	HTG vervangt de bestandsnaam altijd door een uniek ID. Indien de parameter ontbreekt of de waarde niet is ingevuld, genereert HTG een unieke bestandsnaam met extensie .txt.

Tabel 5: SMTP Body

7 In elk geval worden de volgende character sets ondersteund: "us-ascii", "UTF-8", "ISO-8859-1" (Latin1, West European), "ISO-8859-15" (Latin9, West European + Euro).

6 Afkortingen

Afkorting	Betekenis
AGS	Aangiftesysteem van Douane
CID	Comfort Informatie Douane, zekerheidsinformatie, BTW en verlegging controleren
DMS	Douaneaangiften Management Systeem, doorontwikkeling van AGS
DSN	Delivery Status Notification, melding van afleveringsstatus van een e-mail
EMCS	Excise Movement and Control System, systeem voor accijnsgoederen
HTG	Handel en Transport Gateway
IANA	Internet Assigned Numbers Authority, beheersorganisatie voor allerlei Internetcodes
IETF	Internet Engineering Task Force, internationale gemeenschap voor internet evolutie
IP	Internet Protocol
KMar	Koninklijke Marechaussee
MIG	Message Implementation Guide, berichtspecificatie
MSA	Message Submission Agent, ontvangt e-mail van een client
MTA	Mail Transfer Agent, transporteert e-mail van verzender richting ontvanger
NCA SSN	National Competent Authority SafeSeaNet
NCTS	New Computerised Transit System, Douane systeem voor goederenvervoer
NHD	Nationale Helpdesk Douane
NVWA	Nederlandse Voedsel- en Warenautoriteit
POP3	Post Office Protocol - Version 3
RFC	Request for Comments, technische en organisatorische notities over internet
SASL	Simple Authentication and Security Layer, authenticatie framework
SMTP	Simple Mail Transfer Protocol
SW	Single Window, om enkelvoudig meldingen te doen aan meerdere partijen
TCP	Transmission Control Protocol, een internetprotocol
TLS	Transport Layer Security, een netwerkprotocol
VPN	Virtual Private Network, manier om een vertrouwelijk netwerk te maken