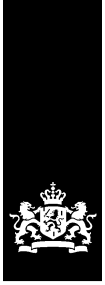

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakbeschrijving Digipoort Berichtuitwisseling - SMTP-MSA

Versie 1.1.1

Datum 2 juni 2015
Status Concept

Colofon

Projectnaam	Digipoort
Versienummer	1.1.1
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Bijlage(n)	`0

Inhoud

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 staat of valt met een goede beschrijving van de koppelvlakken waarop de overheid en het bedrijfsleven 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-MSA-koppelvlak. Op basis van dit koppelvlak kunnen berichten met behulp van een mailclient bij Digipoort worden afgeleverd.. Dit koppelvlak is bedoeld voor berichten van het bedrijfsleven naar de overheid. Voor de bijbehorende retourberichten is het POP3-koppelvlak beschikbaar.

Dit koppelvlak beschrijft niet de standaard voor uitwisseling van berichten tussen mailservers (MTAs). Hiervoor wordt verwezen naar het document "Koppelvlakbeschrijving Digipoort; Berichtuitwisseling - SMTP-MTA (server-to-server)".

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 inkijk in de technische werking van het koppelvlak. Het document wordt besloten met een overzicht van alle algemeen van toepassing zijnde standaarden en afspraken.

Voor meer details over de structuur van SMTP-berichten kunt u de berichstroomspecificaties lezen en de voorbeeldberichten bekijken.

Status
Het SMTP-MSA koppelvlak is ontstaan uit een noodzaak een alternatief te bieden voor de aansluiting van bedrijven die informatie verstrekken aan de Douane en dit nu doen door middel van X.400 P7-postbussen.

Digipoort voorzag voor de totstandkoming van de SMTP-MSA/POP3-koppelvlakken echter alleen in vaste aansluitingen door middel van huurlijnen en VPN's. De last van het opzetten van een dergelijke verbinding is te hoog voor zowel de bedrijven als de beheerder van Digipoort. Samen met het eveneens nieuwe POP3-koppelvlak biedt SMTP-MSA een alternatief waarbij huurlijnen en VPNs niet vereist zijn.

De verwachting is dat de gebruikte open standaarden zich de komende jaren verder zullen ontwikkelen en dat de communicatiebehoefte ook aan verandering onderhevig zal zijn. Het gevolg hiervan is dat de komende

jaren nieuwe releases van Digipoort in gebruik zullen worden genomen. Dat kan gevolgen hebben voor de koppelvlakken.

1 Interactie via het koppelvlak

1.1 Transport

Dit koppelvlak is bedoeld voor laagfrequente interactie (minder dan 1 interactie per bedrijf per minuut) en word ad-hoc over een TCP/IP (internet) verbinding benaderd. Zodra de transacties met het koppelvlak voltooid zijn word de verbinding weer verbroken. Voor hoogfrequente interactie wordt het koppelvlak SMTP-MTA gebruikt. Vooralsnog zal het koppelvlak geen beperkingen opleggen aan de frequentie van het gebruik.

1.2 Gebruik van Message Submission for Mail in plaats van een standaard MTA

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[1]. Echter; veel Internet Service Providers (ISP's) blokkeren deze poort van binnenuit waardoor het voor een gebruiker van een gehuurde internetverbinding niet mogelijk is om SMTP-verkeer te onderhouden met een andere partij. Providers bieden een standaard-oplossing door alle verkeer door een berichtdoorgaafketen te leiden.

Hierdoor is het moeilijk om een beveiligde server-to-serververbinding op te zetten tussen een bedrijf en Digipoort. Vandaar dat Digipoort zich opwerpt als een Message Submission Agent (MSA) voor de overheid. Bedrijven injecteren daarmee hun berichten rechtstreeks in Digipoort in plaats van hun eigen MTA of de doorgaaf van de ISP te gebruiken.

1.2.1 Principe van MSA

Het principe van de MSA word volledig beschreven in *"Message Submission for Mail"* – Request for Comments (RFC) 4409. De insteek van de RFC is als volgt:

Het scheiden van berichtinjectie en berichtdoorgaaf waardoor de verschillende diensten zich toe kunnen spitsen op eigen regels. (voor beveiliging, beleid, etc.).

De rol die Digipoort vervult aan de grens van het overheidsdomein maakt het noodzakelijk om aan zaken als beveiliging en beleid een eigen invulling te geven die afwijkt van een door een provider geboden berichtdoorgaafketen. Het SMTP-MSA-koppelvlak biedt een mogelijkheid voor berichtinjectie bij Digipoort door bedrijven.

1.2.2 IANA overwegingen ten aanzien van MSA

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

1.2.3 Authenticatie

Authenticatie op sessieniveau dient plaats te vinden op basis van SMTP Service Extension for Authentication (SMTP-AUTH). In hoofdstuk 4.3 van de RFC wordt voorgeschreven dat de MSA standaard een foutcode

[1] *25/tcp betekent zoveel als TCP/IP poort no. 25*

teruggeeft als het MAIL commando wordt gegeven en de sessie nog niet geauthenticeerd is. Dit wordt verder uitgewerkt in paragraaf 1.4.2 van dit document.

Figuur 1: Interactie met de MSA-server bij gebruik van SASL

1.3 Inhoud

De inhoud van de in de MSA geïnjecteerde berichten moet zich conformeren aan de in het document Berichtstroom Specificaties - SMTP-MSAPOP3 Logistieke Stromen beschreven beperkingen.

1.4 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.

1.4.1 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. Bij het initiëren van de verbinding kan direct een TLS verbinding worden opgezet waarover het SMTP verkeer wordt uitgewisseld.

Als alternatief kan er een onbeveiligde verbinding worden opgezet waarna het STARTTLS commando wordt gegeven door de client om de TLS te initiëren. Dit principe wordt beschreven in RFC 2487: *"SMTP Service Extension for Secure SMTP over TLS".* Deze optie verdient vanuit het oogpunt van vertrouwelijkheid niet de voorkeur en zou indien mogelijk niet gebruikt moeten worden (zie 1.4.3).

1.4.2 Authenticatie en autorisatie van client

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

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

Een lijst van de beschikbare methoden wordt bijgehouden door het IANA en is in te zien op http://www.iana.org/assignments/sasl-mechanisms.

Het koppelvlak ondersteunt de SASL-mechanismen DIGEST-MD5, PLAIN en LOGIN.

1.4.3 Onderkende risico's en maatregelen

Geen van de bestaande SASL mechanismen is onfeilbaar en allen 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 code 530 (Must issue a STARTTLS command First).
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.

1.4.4 Mogelijke opschaling

Het is mogelijk om de beveiliging op te schalen door authenticatie en autorisatie aan te passen. Hiertoe moet worden overgegaan op 2-weg TLS. Dit houdt in dat ook de client een certificaat aanlevert om de

beveiligde verbinding op te zetten. Vooralsnog is dit bij dit koppelvlak nog niet aan de orde.

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

```
<server (S) wacht op een TCP connectie op poort
587>
<client (C) opent een TCP connectie op poort
587>
  S: 220 msa.overheidstransactiepoort.nl ESMTP
  C: EHLO mijnbedrijf.nl
  S: 250-msa.overheidstransactiepoort.nl
     250-PIPELINING
     250-SIZE 52428800
     250-STARTTLS
     250-8BITMIME
     250-AUTH DIGEST-MD5
  C: STARTTLS
  S: 220 Ready to start TLS
  S & C: <TLS verbinding tussen client en server
wordt opgezet>
  C: AUTH DIGEST-MD5
  S & C: <Het Digest authenticatie scenario
wordt uitgespeeld>
  C: MAIL FROM:<ik@mijnbedrijf.nl>
  S: 250 2.1.0 Ok
  C: RCPT TO:<belastingdienst@overheid.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>
  S: 250 2.0.0 Ok: queued as EA37575310A
  C: QUIT
<server sluit verbinding>
```

2 Algemene afspraken

2.1 Standaarden

Standaard	Referentie
TCP & TCP/IP	http://www.rfcsearch.org/rfcview/RFC/675.html, http://www.rfcsearch.org/rfcview/RFC/1958.html, http://www.rfcsearch.org/rfcview/RFC/1122.html
Simple Message Transfer Protocol (SMTP)	http://www.rfcsearch.org/rfcview/RFC/2821.html
Message Submission for Mail (MSA)	http://www.rfcsearch.org/rfcview/RFC/4409.html
SMTP Service Extension for Authentication (SMTP-AUTH)	http://www.rfcsearch.org/rfcview/RFC/2554.html
Simple Authentication and Security Layer (SASL)	http://www.rfcsearch.org/rfcview/RFC/4422.html
Transport Layer Security v1.1 (TLS)	http://www.rfcsearch.org/rfcview/RFC/4346.html
Digest Authentication for SASL (Digest-MD5)	http://www.rfcsearch.org/rfcview/RFC/2831.html
SMTP Service Extension for Secure SMTP over TLS	http://www.rfcsearch.org/rfcview/RFC/2487.html

2.2 Randvoorwaarden & Foutmeldingen

Alle van toepassing zijnde randvoorwaarden en foutmeldingen zijn reeds beschreven in de normatieve RFC's en de 'Koppelvlakspecificatie-document SMTP-MTA'.
RFC 4409 stelt ondermeer voor om berichten die in de MSA worden geïnjecteerd te vervolmaken, voor zover mogelijk, als dit niet is gedaan door de Mail User Agent (MUA). Het gaat hier dan vooral om het voltooien van e-mail adressen met het (local) domain part en het herschrijven van From adressen. De Digipoort MSA verwacht bij injectie volledige adressen, en ondersteunt voltooien en herschrijven van adressen niet.[2]

2.3 Adressen

Deze worden verstrekt na het aanvragen van een account.

2.4 Limieten en beperkingen

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

2.5 Ondersteuning

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

[2] *Overigens worden adressen door de Digipoort kernfunctionaliteit wél herschreven: van een logisch adres (xyz@otpnet.nl) wordt een vertaling gedaan naar het werkelijke adres (abc@xyz.nl) en omgekeerd.*