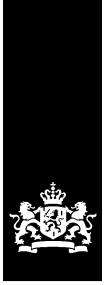


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakbeschrijving Digipoort Berichtuitwisseling - POP3

Versie 1.1.1

Datum 2 juni 2015
Status Definitief

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 (OTP)) 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 POP3-koppelvlak. Op basis van dit koppelvlak kunnen berichten met behulp van een mailclient bij Digipoort worden opgehaald. Dit koppelvlak is bedoeld voor berichten van de overheid naar het bedrijfsleven. Voor berichtverkeer in omgekeerde richting is het SMTP-MSA-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 POP3-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 SMTP-MSA-koppelvlak biedt POP3 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

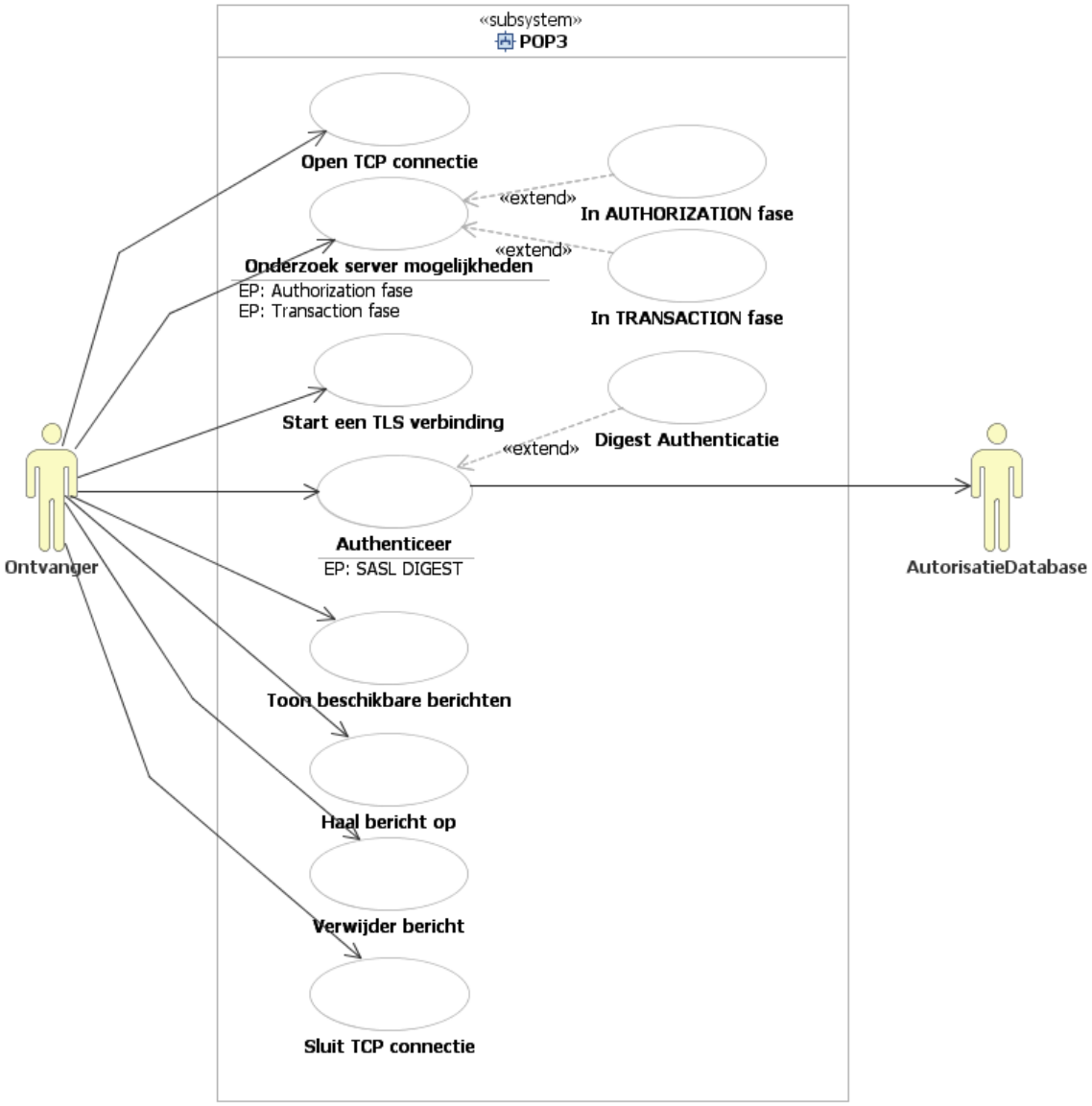
Dit koppelvlak is bedoeld voor laag frequente interactie (minder dan 1 interactie per gebruiker per minuut) en word ad-hoc over een TCP/IP (internet) verbinding benaderd. Zodra de transacties met het koppelvlak voltooid zijn word de verbinding weer verbroken.
Voor hoogfrequente interactie wordt het koppelvlak SMTP-MTA gebruikt.

1.2 Gebruik van POP3

Het principe van POP3 wordt beschreven in *"Post Office Protocol 3"* - RFC 1939.
POP3 is bedoeld als toegang tot een berichtenopslag. 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 wordt deze door de POP3-server op slot gezet. Zolang de POP3-server actief is voor een berichtenopslag kunnen er in deze berichtenopslag geen berichten worden afgeleverd. Ook kunnen er geen berichten worden opgehaald door een andere instantie van de POP3-server.

1.2.1 3 fasen van een POP3 transactie

Het POP3 protocol kent drie fasen 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. Figuur 1 geeft een overzicht van de verschillende fasen.



Figuur 1: Interactie tussen gebruiker er POP3-server bij gebruik van SASL

1.2.1.1 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 word de berichtopslag op slot gezet voor verdere bewerking.
Als de client hier een QUIT commando ingeeft worden de volgende fasen overgeslagen en wordt de verbinding gesloten.

1.2.1.2 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 verwijderen gebeurt niet daadwerkelijk 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.

1.2.1.3 UPDATE fase
In de UPDATE fase voert de server de gevraagde verwijderingen door en ontgrendelt de berichtopslag.

1.2.2 IANA overwegingen
POP3 opereert op een door de Internet Assigned Numbers Authority (IANA) toegekende TCP poort te weten 110/tcp.
NB: TCP poort 995/ssl-pop wordt niet gebruikt. Deze poort wordt 'discouraged' in RFC 2595.

1.3 Inhoud

De inhoud van de uit de POP3-postbus opgehaalde 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 houdt zich alleen bezig met de bescherming van de data tussen verzender en ontvanger.

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 STLS-commando is gegeven door de client. Dit principe wordt beschreven in RFC 2595: *"Using TLS with IMAP, POP3 and ACAP".* 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 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, onder andere, gebruiksnaam en wachtwoord authenticatiemethoden.

Een lijst van de beschikbare methoden wordt bijgehouden door de 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 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.

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.

1.5 Voorbeeld

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

```
<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
     SASL DIGEST-MD5
     TOP
     PIPELINING
     STLS
  C: STLS
  S: +OK Begin TLS negotiation
  S & C: <TLS-verbinding tussen client en server
wordt opgezet>
```

```
  C: AUTH DIGEST-MD5
  S & C: <Het digest authenticatie scenario
wordt uitgespeeld>
  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>
```

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
Post Office Protocol – Version 3 (POP3)	http://www.rfcsearch.org/rfcview/RFC/1939.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
Using TLS with IMAP, POP3 and ACAP	http://www.rfcsearch.org/rfcview/RFC/2595.html
POP3 SASL Authentication Mechanism	http://www.rfcsearch.org/rfcview/RFC/5034.html
Digest Authentication for SASL (Digest-MD5)	http://www.rfcsearch.org/rfcview/RFC/2831.html

2.2 Randvoorwaarden & Foutmeldingen

Alle van toepassing zijnde randvoorwaarden en foutmeldingen zijn reeds beschreven in bovenstaande standaarden.

2.3 Adressen

Deze worden verstrekt na het aanvragen van een account.

2.4 Limieten

Deze 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.