Procesbeschrijving SMTP Single Window

4-11-2016

Inhoud

Inleiding 2
Koppelvlak SMTP MTA 3
Beveiliging 3
Samenhang koppelvlak SMTP MSA en POP3 3
Koppelvlak SMTP MSA 3
Koppelvlak POP3 4
AUTHORIZATION fase 4
TRANSACTION fase 4
UPDATE fase 4
Berichtverwerking 5
Adressering 5
Afleveren 5
Delivery Status Notifications (DSN's) 5
Control-bericht 6

Inleiding

Single Window is een berichten-uitwisselplatform tussen bedrijven en overheidsinstanties. Aan beide "zijden" voorziet het platform in een aantal koppelvlakken waarmee aangesloten kan worden op het platform. Aan bedrijvenzijde kan op de berichtstroom worden aangesloten door gebruik te maken van de SMTP koppelvlakken. Er zijn twee SMTP koppelvlakken, MTA en MSA/POP3. Meer informatie over de SMTP koppelvlakken kunt u vinden op de website van Logius.

Het SMTP MTA koppelvlak voorziet in de uitwisseling van mailverkeer tussen mailservers. Dit maakt het koppelvlak geschikt voor het uitwisselen van grote hoeveelheden mailverkeer.

Het koppelvlak SMTP MSA/POP3 voorziet in de communicatie tussen een mailclient en Single Window. Dit koppelvlak is bedoeld voor laagfrequente interactie (minder dan 1 interactie per bedrijf 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.

Single Window 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 Single Window. 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 het koppelvlak wordt verstuurd. Dit betreffen specifieke ketenafspraken, die zijn beschreven in SW MIG.

Naast de diverse koppelvlakonderdelen bestaat het platform uit een kern-functionaliteit die zorg draagt voor:

- Autorisatie en authenticatie
- Adresvertaling
- Routering
- Protocolconversie
- Logging
- Berichtformaatconversie (Edifact/XML)

Koppelvlak SMTP MTA

Om verbinding met Single Window te kunnen maken moet er een VPN tunnel middels IPSec opgezet worden. Dit is een beveiligde verbinding waarover via poort 25 mailverkeer kan plaatsvinden. Het gebruik van SSL/TLS is bij dit koppelvlak technisch niet mogelijk. De technische gegevens die nodig zijn voor het opzetten van een VPN IPSec tunnel zijn te vinden in het Technische Gegevensformulier.

Het SMTP protocol is een algemeen gebruikt bericht transportprotocol. 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 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 aanleveren en afleveren.

Beveiliging

Sessies worden beveiligd op het niveau van de IPSec verbinding. Ook de authenticatie van verzender en ontvanger wordt voor dit koppelvlak op transportniveau afgehandeld.

Samenhang koppelvlak SMTP MSA en POP3

Het SMTP MSA koppelvlak wordt gebruikt om berichtenverkeer te initiëren naar Single Window. SMTP MSA kan uitsluitend gebuikt voor het aanleveren van berichten. Voor het afleveren van berichten door Single Window is POP3 noodzakelijk. De koppelvlakken SMTP MSA en POP3 moeten beiden worden gebruikt. Beide koppelvlakken voorzien in de communicatie tussen een mail cliënt en Single Window.

Om gebruik te kunnen maken van MSA/POP3 moet u geautoriseerd zijn. Autorisatie geschiedt door de verstrekking van een gebruikersnaam en wachtwoord.

Koppelvlak SMTP MSA

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.

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.

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) – Request for Comments (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.

Koppelvlak 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 authenticeerd 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.

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.

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.

TRANSACTION fase

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

UPDATE fase

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

Berichtverwerking

Het starten van de berichtverwerking door Single Window begint met het aanleveren van het bericht (Edifact of XML). Vervolgens wordt het bericht door Single Window bij de juiste overheidspartij(en) afgeleverd (XML). Omgekeerd kunnen overheidspartijen via antwoordberichten ("declaration responses") op aangeleverde declaratieberichten van bedrijven reageren. Ook kunnen overheidspartijen retourberichten voortkomend uit het toezicht proces ("processresponses") naar aangesloten bedrijven sturen. Meer informatie vindt u in de Single Window Message Implementation Guide (Single Window MIG).

Adressering

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

Aanleveren

Bij het aanleveren wordt door Single Window vastgesteld of het, in het kader van de betrouwbare werking van Single Window, verantwoord is een aangeleverd bericht technisch te accepteren. Single Window voert hiertoe de eerste essentiële technische controles uit. Indien de controles succesvol voltooid worden, initieert het Single Window het afleveren bij een overheidspartij die het declaratiebericht dient te ontvangen.

Afleveren

Nadat een bericht succesvol is aangeleverd aan Single Window moet het bericht afgeleverd worden bij een of meerdere overheidsinstellingen. Single Window verzorgt de aflevering van berichten bij de overheidsinstellingen die de gegevens dienen te ontvangen. Er wordt een verbinding met de uitvragende partij opgezet en na verificatie en het uitvoeren van controles, wordt het bericht afgeleverd. Overheidsinstellingen kunnen ook berichten aanleveren aan Single Window, process responses. Single Window zal deze responseberichten vervolgens afleveren bij de betreffende marktpartij.

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

De redenen voor een DNS Failure kunnen zijn:

- Niet ondersteund Content-Type
- Geen body part 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 Single Window
- Ongeautoriseerde koppeling (voorbeeld: bedrijven naar bedrijven).
- Logisch adres is nog niet geactiveerd

De inzendende partij krijgt een DSN bericht terug waarin staat dat het bericht wel of niet correct is afgeleverd bij Single Window. In de map *SMTP Voorbeeldberichten* is een voorbeeld te vinden van een DSN Delivered en een DSN Failed.

Control-bericht

Single Window valideert het ingezonden bericht tegen de MIG taxonomie. Wanneer deze validatie één of meerdere fouten in het bericht detecteert, zal het bericht niet verder verwerkt worden. Het bericht wordt dan ook niet doorgestuurd naar een overheidsinstantie. In plaats daarvan wordt er een control-bericht verstuurd naar de verzender van het bericht. In het control-bericht staat aangegeven wat in het bericht onjuist is. In de map SMTP Voorbeeldberichten is een voorbeeld te vinden van een control-bericht.