



Logius
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Koppelvlakbeschrijving Digipoort Bestandsuitwisseling - FTP

Koppelvlak versie: 1.6.1
Document versie: 04-10-2018

Datum 04 October 2018
Status Definitief

Colofon

Projectnaam	Digipoort
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Bijlage(n)	Schema metabestand (metabestand.xsd) Aansluitdetails

Wijzigingshistorie

Datum	Auteur	Koppelvlak versie	Document versie	Omschrijving
04-10-2018	Logius	1.6.1	04-10-2018	- Tekstuele aanpassingen ivm de exclusiviteit van de TLS1.2 layer.
13-01-2015	Logius	1.6.1	13-01-2015	- Tekstuele aanpassingen ivm tcp port gedaan.
22-12-2015	Logius	1.6.1	22-12-2015	- Tekstuele aanpassingen gedaan en verwijzingen naar documenten aangepast
26-2-2015	Curtly Inesia	1.6.1	26-2-2015	- Toevoeging verwijs naar Client FTPs met cURL document - Logius sjabloon toegevoegd
6-6-2012	Tom Breuker	1.6.1	6-6-2012	Bijlage met aansluitdetails toegevoegd.
26-3-2012	Tom Breuker	1.6.1	26-3-2012	- Wijzigingshistorie toegevoegd. - Verduidelijking naamgeving databestand en metabestand. - Toelichting te gebruiken poorten voor data overdracht. - Verschil tussen Koppelvlakversie en Documentversie toegevoegd. Niet iedere nieuwe document versie moet worden gezien als een wijziging van het koppelvlak. Andersom is dit natuurlijk wel het geval.
8-8-2011	Logius	1.6.1	8-8-2011	Basis versie

Inhoud

<i>Colofon</i>	2
Wijzigingshistorie	3
Inhoud	4
Inleiding	5
1 Interactie via het koppelvlak	7
1.1 <i>Transport</i>	7
1.2 <i>Inhoud</i>	7
1.2.1 Passive modus (PASV of EPSV).....	7
1.2.2 Data type	7
1.2.3 Inrichting per gebruiker.....	8
1.2.4 Databestand	8
1.2.5 Metabestand	8
1.2.6 Aanlevering van bestanden	9
1.2.7 Hervatten van afgebroken uploads	9
1.2.8 Ontvangstbevestiging	9
1.2.9 Foutmelding.....	10
1.2.10 Ophalen van bestanden.....	10
1.3 <i>Beveiliging</i>	11
1.3.1 Transportbeveiliging.....	11
1.3.2 Vertrouwelijkheid	11
1.3.3 Authenticatie en autorisatie van de client	11
1.3.4 Onderkende risico's en maatregelen.....	12
1.4 <i>Voorbeelden</i>	12
1.4.1 Opzetten van een TLS verbinding	12
1.4.2 Plaatsen van bestanden	13
2 Algemene afspraken	14
2.1 <i>Standaarden</i>	14
2.2 <i>Randvoorwaarden</i>	14
2.3 <i>Foutmeldingen</i>	14
2.4 <i>Adressen en parameters</i>	14
2.5 <i>Limieten en beperkingen</i>	15

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 dat voor berichten via het File Transfer Protocol (FTP) protocol.

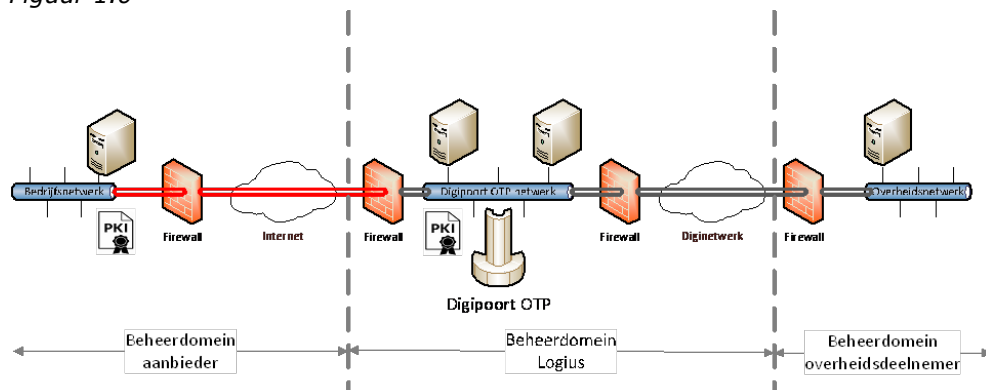
Specifiek betreft dit document het koppelvlak 'Bestandsuitwisseling FTP – 1.6.1'. Dit koppelvlak is bedoeld voor uitwisseling van bestanden tussen bedrijfsleven en overheid.

Logius biedt tevens het koppelvlak 'Grote Berichten FTP' aan. Dit is een apart koppelvlak welke hier niet wordt beschreven.

Dit document is primair bestemd voor ontwikkelaars van systeem-naar- systeem koppelingen tussen bedrijven en Digipoort. Het opzetten van de verbinding tot aan de firewall van Digipoort, het beheerdomein van de aanbieder zoals afgebeeld in Figuur 1.0, dient door de aanbieder te worden gerealiseerd. Van u wordt verwacht dat u beschikt over kennis van FTPs. Ter ondersteuning levert Logius de volgende documenten:

- Berichtstroomspecificaties FTPS v1.6.1 Metabestand
- Metabestand XSD en voorbeeldberichten
- Koppelvlakbeschrijving FTP_v1.6.1
- Procesbeschrijving FTPS V.1.6.1
- Aansluitformulier technische gegevens - FTPS v1.6.1

Figuur 1.0



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.

Status

Het FTP-koppelvlak is ontstaan uit een noodzaak voor de aansluiting van banken en verzekeraars die dermate grote bestanden aan moeten leveren aan, in eerste instantie, de Belastingdienst, dat andere, reeds bestaande, Digipoort-koppelvlakken niet toereikend waren.

In een gezamenlijk pilotproject van banken en Belastingdienst is hiervoor een versie 1.0 van deze koppelvlakspecificaties tot stand gekomen. Deze versie is verder uitgebouwd naar versie 1.6 van de koppelvlakspecificaties. Alle oplossingen maken gebruik van het FTP-protocol met transportlaagbeveiliging door middel van TLS (ook wel FTPs genoemd).

Met dit koppelvlak is het mogelijk om berichten uit te wisselen tussen bedrijven en overheden. Het uitwisselen van berichten tussen overheden of bedrijven onderling wordt niet ondersteund.

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

Het koppelvlak kan worden benaderd via een TCP/IP-verbinding. In alle gevallen wordt voor interactie met het koppelvlak ad hoc een beveiligde verbinding opgebouwd. Na voltooiing van de transacties over het koppelvlak wordt de verbinding weer verbroken. Het koppelvlak staat overdracht van meerdere bestanden in een sessie toe.

Voor FTP zijn twee connecties (verbindingen) nodig. Een controleconnectie welke wordt gebruikt om de commando's en de antwoorden daarop uit te wisselen en een dataconnectie welke wordt gebruikt om de gegevens uit te wisselen.

De te gebruiken poort(reeksen) voor de controle- en dataconnectie zijn opgenomen in het *Aansluitformulier technische gegevens - FTPS v1.6.1*

1.2 Inhoud

Het principe van het FTP protocol wordt beschreven in "File Transfer Protocol" – Request for Comments (RFC) 959.

Berichten die ingestuurd worden bestaan uit het bestand dat word verstuurd aan de afnemer (het databestand) en een bestand met metagegevens betreffende het verstuurd bestand (het metabestand). De metagegevens zijn nodig om de databestanden als bericht te kunnen routeren, en de integriteit en authenticiteit van het bericht te kunnen waarborgen. Bij het andere door Digipoort OTP ondersteunde koppelvlak (SMTP) zijn dergelijke metagegevens onderdeel van het bericht.

1.2.1 *Passive modus (PASV of EPSV)*

Voor het FTP koppelvlak wordt gebruik gemaakt van een passieve modus. De server heeft geen initiatief in het opzetten van een data verbinding maar vertelt de client op welke poort deze een verbinding kan openen voor het insturen van bestanden. Dit wordt gedaan om de beheerlast op firewalls van de gebruikers zo klein mogelijk te houden. De client dwingt dit af door het PASV commando of het EPSV commando. De server geeft als response het te gebruiken IP adres en de bijbehorende data poort in een serie van 6 komma's gescheiden getallen.

Voorbeeld: 192,168,2,1,34,12

De eerste vier getallen geven ieder een byte van het IP adres weer. Dit word dan 192.168.2.1

De laatste twee getallen uit de serie vormen samen het poort nummer. Hierbij wordt het eerste getal vermenigvuldigd met 256 en wordt het tweede getal daarbij opgeteld.

Dit leidt dan tot $34 * 256 + 12 = 8716$.

Dit wordt gedaan om er zeker van te zijn dat het poortnummer in een 8- bits byte past.

1.2.2 *Data type*

FTP start standaard met datatype 'ascii'. Voordat een upload (STOR) of download (RETR) wordt gestart moet(!) worden gewitcht naar datatype 'image'

(binary) met het FTP-commando TYPE I. Hierdoor wordt voorkomen dat checksums op verschillende byte-reeksen worden uitgevoerd (bijvoorbeeld doordat verschillende besturingssystemen anders omgaan met end-of-line characters e.d.).

1.2.3 *Inrichting per gebruiker*

Iedere gebruiker¹ van het FTP koppelvlak krijgt een eigen gebruikersdirectory. Geen enkele andere gebruiker heeft toegang tot deze directory.

De gebruikersdirectory heeft twee subdirectories:

- in – hier kunnen bestanden en metabestanden worden geplaatst die door de Digipoort moeten worden doorgestuurd naar een andere gebruiker.
- out – hier kunnen bestanden en metabestanden worden opgehaald die door Digipoort zijn afgeleverd ten behoeve van de gebruiker. Digipoort plaatst in deze directory ook ontvangstbevestigingen en foutmeldingen.

Gebruikers hebben in elke directory beperkte rechten: opvragen van een lijst bestanden (alle directories), plaatsen van bestanden (in), opvragen en verwijderen van bestanden (out² en in).

1.2.4 *Databestand*

De inhoud van het databestand is volgens afspraak tussen bedrijf en overheidspartij.

Voor bestandsnamen gelden de volgende beperkingen:

- De extensies .meta en .error zijn gereserveerd. Een door een gebruiker aangeleverd databestand mag nooit een van deze extensies hebben.
- Bestandsnamen dienen te voldoen aan een aantal criteria³:
 - o ze bestaan uit alleen maar de tekens a-z,A-Z,0-9,_,., en -
 - o ze beginnen met 1 van de tekens a-z,A-Z,_,.
 - o ze hebben een lengte van minimaal 1 en maximaal 100 tekens, inclusief extensies

1.2.5 *Metabestand*

Het metabestand bevat onderstaande elementen. Het metabestand komt zowel bij inkomende als uitgaande berichten voor, maar kan afhankelijk van de richting verschillende vulling hebben. Zie voor de specificaties omtrent dit bestand de bijgevoegde *Berichtstroomspecificaties FTPS v1.6.1 Metabestand*

Alle elementen komen maximaal eenmaal voor.

De definitie van het metabestand is vastgelegd in het XML-schema *metabestand.xsd*, dat als bijlage bij deze koppelvlakspecificaties is gevoegd.

Voor bestandsnamen gelden dezelfde beperkingen als voor het databestand, met de volgende aanvulling: Een door een gebruiker aangeleverd metabestand

¹ NB: Met gebruiker wordt in de context van deze koppelvlakspecificaties zowel een bedrijf als een overheids-partij bedoeld.

² In de praktijk kan alleen een incorrect geplaatst databestand worden verwijderd. Een geplaatst metabestand zal vrijwel direct leiden tot verwerking van databestand en metabestand.

³ Dit komt overeen met de volgende notatie als extended regular expression:
`/^[a-zA-Z_][a-zA-Z0-9_.-]{0,99}(?!\\.meta\\.error)\\z/`

moet altijd de extensie .meta hebben⁴, voorgaand met de bestandsnaam van het databestand inclusief de extensie.

Zie voor voorbeelden de bijgevoegde voorbeeldberichten.

1.2.6 *Aanlevering van bestanden*

Eerst wordt het databestand volledig aangeleverd (met het STOR commando), en daarna het metabestand. Pas als het metabestand volledig is aangeleverd (herkenbaar aan de eindtag) en het databestand voldoet aan de in het metabestand meegegeven metadata (digest, data- reference id en size) wordt verwerking van het bericht gestart en zal het afgeleverd worden bij de geadresseerde ontvanger. Het databestand zal in de gebruikersdirectory blijven staan tot het bijbehorende metabestand wordt geplaatst en correct wordt bevonden. Op dat moment worden beide uit de gebruikersdirectory van de verzender verwijderd. Dit wordt bevestigd met een ontvangstbevestiging (zie 1.2.8). Bij niet succesvolle aflevering wordt een foutmelding gegeven (zie 1.2.9).

1.2.7 *Hervatten van afgebroken uploads*

Het FTP koppelvlak staat herstel van een eerder afgebroken upload toe door gebruik te maken van het REST (restart) commando.

1.2.8 *Ontvangstbevestiging*

Zodra is vastgesteld dat de aangeleverde bestanden voldoen aan de koppelvlakspecificaties wordt er een ontvangstbevestiging geplaatst in de "out" directory van de verzender.

De ontvangstbevestiging bestaat uit een kopie van het metabestand aangevuld met het element 'received' met het tijdstempel van het moment dat het bericht is aangeleverd.

De naam van de ontvangstbevestiging is als volgt opgebouwd:
{data-reference id verzender}_{data-reference id Digipoort}.ok

Voorbeeld:

```
RENSAGEG_20081231_Ambobank_Amstelhoven.xml_Digipoort_018b0112- 8171-4fed-b360-aa509ba1c6a9.ok
```

⁴ Dit komt overeen met de volgende notatie als extended regular expression:
/^[a-zA-Z_][a-zA-Z0-9_-]{0,99}(?<\.meta)\z/

Als deze filenaam langer wordt dan de maximaal toegestane lengte wordt de "data-reference id verzender" afgekapt.

1.2.9 *Foutmelding*

Wanneer Digipoort de aangeboden combinatie metabestand en databestand niet kan verwerken wordt een foutmelding geplaatst in de "in"-directory van de verzender⁵.

De naam van de file waarin de foutboodschap is opgenomen is als volgt opgebouwd:

```
{data-reference id verzender}_{data-reference id Digipoort}.error
```

Voorbeeld:

```
RENSAGEG_20081231_Ambobank_Amstelhoven.xml_Digipoort_018b011 2-8171-4fed-  
b360-aa509ba1c6a9.error
```

1.2.10 *Ophalen van bestanden*

Digipoort levert eerst het databestand, daarna het metabestand af. Ophalen van bestanden (met het RETR commando) kan beginnen zodra het metabestand zichtbaar is. Na succesvol downloaden mogen de bestanden worden verwijderd door de gebruiker (met het DELE commando)⁶. Als deze filenaam langer wordt dan de toegestane lengte wordt de "data-reference_id verzender" afgekapt.

⁵ Het is mogelijk de verwerking van het bericht te herstarten door een gecorrigeerd metabestand te plaatsen, zonder het databestand opnieuw te hoeven uploaden.

⁶ Het koppelvlak gaat ervan uit dat de gebruiker pas een delete geeft als hij zich ervan vergewist heeft dat het ophalen van het bestand goed gelukt is. Na delete is het bestand niet meer terug te halen

1.3 Beveiliging

1.3.1 *Transportbeveiliging*

Voor de beveiliging van het transport wordt Transport Layer Security (TLS) ingezet. Zowel het certificaat van de server als het certificaat van de client worden gebruikt om een symmetrisch beveiligde verbinding op te zetten. Het principe van TLS verbindingen voor het FTP-protocol wordt beschreven in "Securing FTP with TLS" - RFC 4217.

Om de TLS-verbinding succesvol tot stand te brengen moet gebruik gemaakt worden van een PKIo-certificaat, waarbij het certificaat:

- geldig is
- niet voorkomt op een Certificate Revocation List
- geregistreerd is bij Logius

De data connectie moet altijd met het Protect (PROT) commando worden beveiligd op beveiligingsniveau Private (P). De server staat geen commando's toe die gebruik maken van de data connectie voordat het PROT commando is gegeven en het niveau is gezet op P. Als het PROT commando nog niet is gegeven is het antwoord van de server op commando's die de data connectie gebruiken altijd een foutcode.

Door middel van het Clear Command Channel (CCC) commando kan de controleconnectie weer teruggebracht worden in een plain text staat. De server weigert het CCC commando omdat dit een opening voor Man- In-The-Middle (MITM) aanvallen laat en beantwoordt het verzoek altijd met een foutcode zoals gespecificeerd in RFC 4217.

Door het gebruik van TLS is het Protection Buffer Size (PBSZ) commando nog wel verplicht maar moet altijd een waarde van '0' worden opgegeven waarmee aangegeven wordt dat het hier een streaming verbinding betreft.

1.3.2 *Vetrouwelijkheid*

Vertrouwelijkheid wordt bewerkstelligd door de beperkingen die worden opgelegd aan de gebruiker en aan de verschillende directories. Eén gebruiker krijgt slechts toegang tot één directory. Ook overheidsinstellingen krijgen geen toegang tot de directory van een bedrijf. Berichten worden alleen afgeleverd bij de overheid waaraan ze geadresseerd zijn.

1.3.3 *Authenticatie en autorisatie van de client*

De client moet zich authenticeren door middel van een gebruikersnaam en een wachtwoord alvorens autorisatie word verleend voor de toegang tot de eigen directory.

De server toetst de gebruikersnaam aan het clientcertificaat dat gebruikt is bij het tot stand komen van de TLS-verbinding (zie 3.3.1). De toegang wordt ontzegd als de gebruikersnaam niet overeenkomt met het certificaat.

1.3.4

Onderkende risico's en maatregelen

Onderstaande tabel geeft een overzicht van algemeen onderkende risico's bij gebruik van het FTP-protocol, en de maatregelen die genomen worden om deze risico's weg te nemen.

Risico	Maatregel
Alle commando's die worden ingegeven door de client voordat het AUTH TLS commando is gegeven zijn in plain text en voor rekening en verantwoordelijkheid van de gebruiker. Autorisatiepogingen op een onbeveiligde verbinding laten gebruikersnamen en wachtwoorden leesbaar voor derden.	Een client mag, zolang er nog geen adequaat beveiligde verbinding is opgezet, hoogstens de commando's HELP, FEAT en AUTH ingeven.
Het gebruik van de standaard FTP gebruiker (anonymous) laat mogelijkheden voor ongeautoriseerde clients om bestanden op te halen die voor anderen bedoeld zijn.	Het gebruik van de anonymous gebruiker wordt niet toegestaan.
De FTP server van GBO te plaatsen en er later weer vanaf te halen.	
Het gebruik van de voorgestelde digest geeft geen garanties voor de integriteit van het bestand, het zou gecompromitteerd kunnen zijn zonder dat dit voor de ontvanger waarneembaar is.	Digipoort voldoet aan een groot aantal informatiebeveiligingsmaatregelen die de mogelijkheden tot compromitteren van bestanden tot een minimum beperken. Deze beveiligingsmaatregelen worden jaarlijks in een onafhankelijke audit geverifieerd. Indien volledige zekerheid over de integriteit (en authenticiteit) gewenst is kunnen de zender en ontvanger afspreken om een signed-digest of encryptie toe te passen op het bestand.

1.4

Voorbeelden

NB De gebruikte ipadressen en portnummers kunnen in de praktijk afwijken.

1.4.1

Opzetten van een TLS verbinding

```
<server wacht op een tcp connectie op port 21>
<client opent een verbinding op tcp/21>
S: 220 ftp.procesinfrastructuur.nl ready
C: AUTH TLS
S & C: <TLS verbinding word onderhandeld en opgezet>
S: 234 Security data exchange complete
C: PBSZ 0
```

```
S: 200 Protection Buffer Size set to streaming
C: PROT P
S: 200 Data connection is private
C: USER bank
S: 331 Username      OK, need password for login
C: PASS "het wachtwoord van de bank"
S: 230 User logged in, proceed.
C: QUIT
<server sluit verbinding>
```

1.4.2 *Plaatsen van bestanden*

```
<server en client hebben een TLS verbinding tot stand gebracht, client is
ingelogd>
S: 230 User logged in, proceed.
C: EPSV
S: 227 Entering passive mode (144,43,253,65,82,8)
C: TYPE I
S: 200
C: STOR RENSAGEG_20081231_Ambobank_Amstelhoven.xml
C: <Opent een TCP connectie op 144.43.253.65 poort 21000>
S: 150 Opening BINARY mode SSL data connection for

RENSAGEG_20081231_Ambobank_Amstelhoven.xml.
C: <TLS handshake en versleuteld versturen van de data.>
S: 226 Transfer complete.
C: <herhaalt de stappen vanaf STOR voor alle te plaatsen
bestanden>
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
File Transfer Protocol	http://www.rfcsearch.org/rfcview/RFC/959.html
Transport Layer Security v1.2 (TLS)	http://www.rfcsearch.org/rfcview/RFC/5246.html
Securing FTP with TLS	http://www.rfcsearch.org/rfcview/RFC/4217.html

2.2 Randvoorwaarden

De voor het opzetten van de beveiligde verbinding te gebruiken clientcertificaten zijn PKI.Overheid-certificaten voor gebruik door services (zie <http://www.pkioverheid.nl/voor-certificaatverleners/programma-van-eisen/>; deel 3b).

De gebruiker dient zelf zorg te dragen voor aanschaf van een client- certificaat bij een van de door PKI.Overheid aangewezen serviceproviders.

2.3 Foutmeldingen

Alle van toepassing zijnde foutmeldingen voor het opzetten van de FTP-verbinding en de uitwisseling van bestanden met FTP zijn beschreven in de hierboven genoemde standaarden.

Logische fouten die leiden tot afkeuren van bestanden zijn onder meer:

- Ontbreken van een databestand waarvoor wel een metabestand aanwezig is
- Metabestand kan niet worden gelezen, of heeft incorrecte structuur
- Ontbreken van verplichte elementen in het metabestand
- Sender onbekend in het inkomende metabestand
- Receiver onbekend in het inkomende metabestand
- Bestandsgrootte van het databestand komt niet overeen met filesize in het metabestand
- Digest van het databestand komt niet overeen met digest-waarde in het metabestand
- Bestandsnaam van databestand of metabestand is ongeldig (voldoet niet aan de bestandsnaamconventies)

2.4 Adressen en parameters

Deze worden verstrekt na het aanvragen van een account.

2.5 Limieten en beperkingen

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