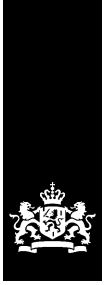


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Koppelvlakbeschrijving Digipoort Grote Berichten 3.0

Koppelvlakversie 1.3

Versie	1.3
Datum	04 oktober 2018
Status	Definitief

Colofon

Projectnaam	Digipoort
Versienummer	1.3
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Bijlage(n)	Servicebeschrijving Digipoort Grote Berichten 3.0 Aanleveren
	Servicebeschrijving Digipoort Grote Berichten 3.0 Aanleveren Addendum Loonheffing
	Servicebeschrijving Digipoort Grote Berichten 3.0 Statusinformatie
	Servicebeschrijving Digipoort Grote Berichten 3.0 Afleveren
	Servicebeschrijving Digipoort Grote Berichten 3.0 Statusupdate

Inhoud

Inleiding

Doel en doelgroep
Dit document beschrijft de afspraken met betrekking tot het elektronische berichtenverkeer bij de overheid via het FTP communicatiekanaal voor Grote Berichten 3.0 van Digipoort.

Dit document is bestemd voor ontwikkelaars van programmatuur voor het aanleveren en opvragen van berichten aan en van de overheid via deze infrastructuur.

Leeswijzer
Deze koppelvlakbeschrijving vormt de basis van een reeks servicebeschrijvingen die inzicht geven in het gebruik van de services van Digipoort. Dit document is als volgt opgebouwd:

- Het eerste hoofdstuk bevat een globale beschrijving van de werking van het koppelvlak 'Grote Berichten 3.0' en de betrokken services;
- Het tweede hoofdstuk geeft een globale omschrijving van het berichtenverkeer over het koppelvlak;
- Het derde hoofdstuk geeft de specificatie voor het gebruik van het koppelvlak Grote Berichten 3.0.;
- Het vierde hoofdstuk geeft een overzicht van alle algemeen van toepassing zijnde standaarden en afspraken.

Deze koppelvlakbeschrijving is onderdeel van een grotere set documenten die de dienstverlening van Digipoort beschrijft.

Status
Dit document beschrijft de afspraken met betrekking tot het koppelvlak 'Grote Berichten 3.0' van Digipoort. 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 het koppelvlak. Logius streeft ernaar om nieuwe releases in nauw overleg met de markt te realiseren. Om het voor marktpartijen snel en eenvoudig mogelijk te maken om gebruik te maken van Digipoort, is er voor gekozen zoveel mogelijk open standaarden en bestaande voorzieningen te gebruiken. Voorbeelden daarvan zijn het gebruik van het FTP-protocol en de toepassing van PKIoverheid-certificaten.

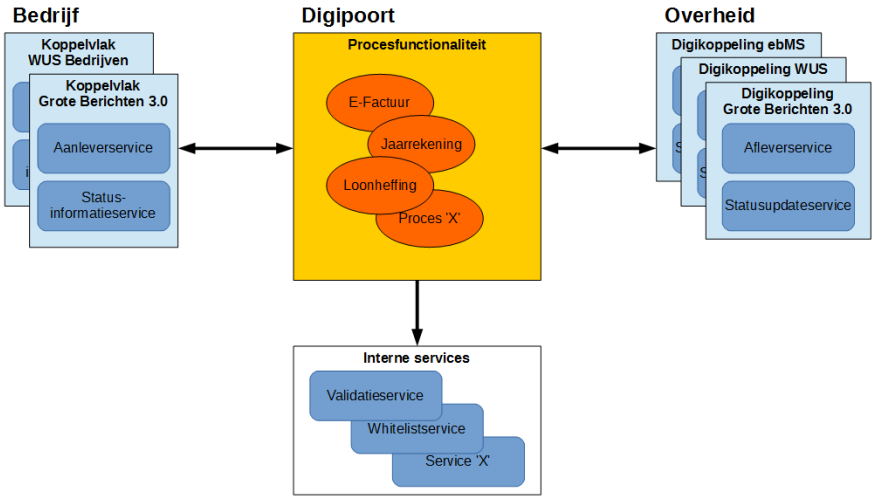
Ondersteuning
Informatie met betrekking tot ondersteuning bij het gebruik van de services van Digipoort is beschikbaar op de website: www.logius.nl/producten/gegevensuitwisseling/digipoort.

1 Berichtenverkeer

1.1 Inleiding

Digipoort kent services gericht op bedrijven en services gericht op de overheid. Daarnaast zijn er services die ondersteunend zijn bij de uitvoering van de verwerkingsprocessen, zoals de blacklistservice en de validatieservice.

In onderstaande afbeelding zijn de services schematisch weergegeven.



Figuur 1: Services binnen Digipoort

Deze koppelvlakbeschrijving vormt de basis voor de services die Digipoort biedt aan bedrijven en overheden. Deze services zijn de Aanleveservice en de Statusinformatieservice voor bedrijven en de Afleverservice en Statusupdateservice voor overheden.

De details van elke service zijn opgenomen in de afzonderlijke service-beschrijvingen.

Het koppelvlak kan worden uitgebreid met nieuwe services. Deze voldoen dan altijd aan deze koppelvlakbeschrijving.

1.2 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 berichten in een transportsessie toe.

Voor de overdracht van berichten via het koppelvlak Grote Berichten 3.0 wordt gebruik gemaakt van het FTP protocol. Het principe van het FTP protocol wordt beschreven in “File Transfer protocol” –RFC 959.

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(reeks) is opgenomen in de specificatie van de verschillende berichtstromen.

1.3 Beveiliging

1.3.1 Transportniveau

De authenticiteit van systemen in Digipoort en van de gebruikers van een service moet door alle deelnemende partijen vastgesteld kunnen worden voordat een datacommunicatiesessie wordt gestart. De authenticiteit van systemen wordt met behulp van PKIoverheid-certificaten gecontroleerd.

Voor een productieaansluiting op Digipoort bent u verplicht gebruik te maken van een PKIoverheid-certificaat (X.509). Dit certificaat waarborgt de veiligheid en betrouwbaarheid van de verbinding tussen uw systeem en Digipoort. Let wel, het PKIoverheid-certificaat is alleen verplicht op de productieomgeving. In de preproductieomgeving is het ook mogelijk om gebruik te maken van self-signed testcertificaten, geleverd door Logius. U kunt een PKIoverheid-certificaat aanvragen via een Certificate Service Provider (CSP). Een overzicht van de huidige CSP's is te vinden op de website van Logius (http://www.logius.nl/producten/toegang/pkioverheid/aansluiten/toetreden-tot-pkioverheid/, onder Toegetreden CSP's). Wegens de doorlooptijd van de aanvraag, adviseren wij u een PKIoverheid-certificaat vroegtijdig aan te vragen. Voor een testcertificaat kunt u zich richten tot het Service Centrum van Logius

Feitelijk wordt de authenticiteit van bedrijven bepaald aan de hand van het PKIOverheid-clientcertificaat dat zich op het cliëntsysteem bevindt. Met behulp van dit certificaat opent de client een verbinding volgens het TLS-protocol (zie het overzicht in figuur 2). Dit protocol biedt naast authenticatie ook encryptie op transportniveau. Het TLS-protocol wordt beschreven in "The TLS Protocol Version 1.2" –RFC 5246.

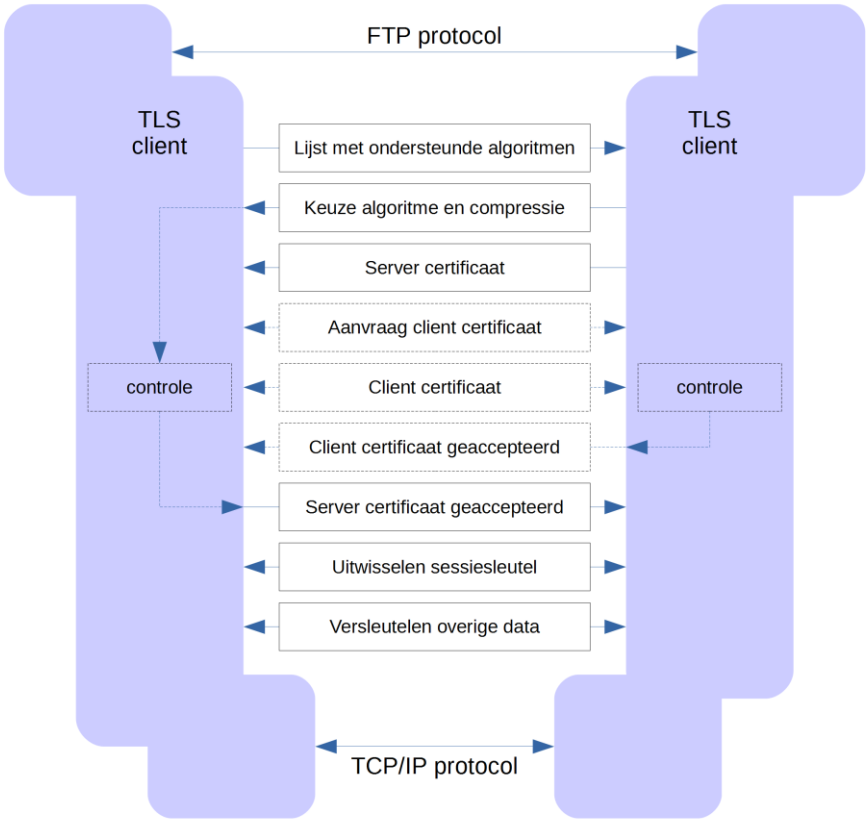
Voor het maken van een verbinding met een Digipoort FTP server zijn (in ieder geval) de volgende zaken vereist:

- Geldig PKIoverheid-certificaat;
- Digipoort FTP account;
- FTP client met ondersteuning voor dubbelzijdige TLS.

De geldigheid van het clientcertificaat wordt aan de hand van de gegevens in het certificaat op de volgende punten gecontroleerd:

- Betreft het een geldig PKIoverheid-certificaat;
- Is het gesigneerd door een Certificate Authority;
- Valt het moment van aanlevering binnen de geldigheidsdata van het certificaat.
- Tegen de Certificate Revocation List (CRL) wordt gecontroleerd of het certificaat niet is ingetrokken.

Op het gebruik van TLS binnen het FTP protocol wordt nader ingegaan in paragraaf 3.2.



Figuur 2: TLS Communicatie

Op transportniveau is de partij die wordt geauthenticeerd de partij waarmee de TLS-verbinding tot stand komt. Dit kan ook een intermediair zijn die voor een of meerdere bedrijven de verbinding met Digipoort verzorgt. Op transportniveau is het dus niet noodzakelijkerwijs de 'eigenaar' van de berichten (het bedrijf namens wie de factuur e.d. wordt verstuurd) wiens identiteit wordt gecontroleerd.

1.3.2 Berichtniveau

Op berichtniveau wordt in het koppelvlak Grote Berichten 3.0 geen beveiliging toegepast.

In het latere verwerkingsproces vindt de controle van de identiteit (die door het certificaat wordt gerepresenteerd) en de autorisatie van de betreffende partij plaats. Tijdens het sturen van een bericht worden alleen de geldigheid van het certificaat en van de handtekening gecontroleerd.

2 Sessieverloop

Een FTP client van een bedrijf maakt een met TLS beveiligde verbinding met een FTP service van Digipoort. Over deze verbinding wordt een bestand met een bericht verzonden, conform de servicespecificatie. Dit bericht bevat een verzoek en eventueel service-afhankelijke inhoud.

Als het bericht niet voldoet aan de eisen gesteld in de koppelvlak-specificatie, wordt er (conform de servicebeschrijving) een foutmelding gegenereerd voor de gebruiker. Ook in het geval dat het bericht niet voldoet aan service specifieke eisen, wordt er een foutmelding gegenereerd. Als het bericht voldoet aan de koppelvlak- en service-eisen, dan wordt een respons gegenereerd. Indien het de aanlevering van een bedrijfsdocument betreft, wordt er een verwerkingsproces voor het bericht opgestart.

Elke service bestaat tenminste uit de volgende onderdelen:

- Controleren verzoek
- Ontvangen (van het gecontroleerde) verzoek
- Verzenden antwoord

Naast bovengenoemde onderdelen kunnen per service andere onderdelen zijn opgenomen. Deze zijn uitgewerkt in de servicebeschrijving.

2.1 Controleren verzoek

Berichten die aan het FTP communicatiekanaal voor Grote Berichten 3.0 van Digipoort worden aangeboden, en berichten die via dit kanaal aan een bedrijf worden aangeboden, zijn opgemaakt conform een vooraf gedefinieerde structuur. Afhankelijk van de service is deze structuur gebaseerd op een MIME multipart bericht (bevattende XML) of puur XML. De structuur is vastgelegd in de betreffende servicebeschrijving. Voor berichten met XML structuur is een XML Schema (XSD) gedefinieerd.

Nadat een verzoek (in de vorm van een bestand) door Digipoort of door het bedrijf is ontvangen, dienen de volgende zaken gecontroleerd te worden:

Controle	**Toelichting**
Is een element aanwezig?	Hierbij wordt gecontroleerd of alle verplichte elementen zoals beschreven in de koppelvlak- en servicespecificaties voorkomen in het verzoek.
Is er geen onbekend element aanwezig?	Hierbij wordt gecontroleerd of in het verzoek geen elementen voorkomen, die niet in de koppelvlak- of servicespecificaties zijn beschreven.

Bevat het element een waarde?	Hierbij wordt gecontroleerd of alle verplichte elementen ook daadwerkelijk een waarde bevatten.
Betreft het een toegestane waarde?	Hierbij wordt gecontroleerd of alle elementen toegestane waarden bevatten.
Is de lengte van de waarde juist?	Hierbij wordt gecontroleerd of de waarde van de elementen niet langer is dan de lengte zoals beschreven in de koppelvlak- of servicespecificaties.

2.2 Ontvangen verzoek

Elk verzoek aan een service van Digipoort wordt vastgelegd in de berichtenadministratie. De berichtenadministratie fungeert binnen Digipoort als audittrail. Op dezelfde wijze kan het bedrijf verzoeken van Digipoort vastleggen in een eigen berichtenadministratie.

2.3 Versturen antwoord

Wanneer het verzoek voldoet aan alle gestelde eisen, wordt het antwoord verstuurd.

Elk antwoord naar Digipoort wordt vastgelegd in de berichtenadministratie. Het bedrijf kan ook antwoorden van Digipoort in een eigen berichtenadministratie vastleggen.

De elementen van het antwoord worden beschreven in de servicebeschrijving van de desbetreffende service.

3 Digipoort FTP server

3.1 Inhoud

Het principe van het FTP protocol wordt beschreven in RFC 959 - "File Transfer Protocol". Het gebruik van TLS voor authenticatie en encryptie op transport niveau voor het FTP protocol wordt beschreven in RFC 4217 - "Securing FTP with TLS" en RFC 2228 - "FTP Security Extensions". Daarnaast worden om het gebruik van een beveiligde verbinding via FTP achter een NAT of firewall mogelijk te maken, de uitbreidingen op het FTP protocol beschreven in RFC 2428 - "FTP Extensions for IPv6 and NATs" ondersteund.

Berichten die ingestuurd worden bestaan uit een bestand dat data bevat dat bij de afnemer afgeleverd moet worden. Daarnaast bevat het bestand metagegevens die nodig zijn om het bericht te kunnen routeren, en de integriteit en authenticiteit van het bericht te kunnen waarborgen. Ook bij andere door Digipoort ondersteunde koppelvlakken (WUS) zijn dergelijke metagegevens onderdeel van het bericht.

3.1.1 Passieve modus (EPSV)

Voor het FTP koppelvlak wordt gebruik gemaakt van een extended passieve modus conform de specificatie van RFC 2428. De server heeft geen initiatief in het opzetten van een dataverbinding, maar vertelt de client op verzoek op welke poort deze een verbinding kan openen voor het insturen van bestanden. Hiermee wordt de beheerlast op firewalls van de gebruikers zo klein mogelijk te houden.

De client dient door gebruik van het EPSV commando de server te verzoeken te luisteren op een datapoort en te wachten op een inkomende verbinding. De server geeft als respons aan de client het poortnummer op waarmee deze dient te verbinden. Het IP-adres voor de dataverbinding dient afgeleid te worden (is gelijk aan) het IP-adres van de controleverbinding.

3.1.2 Data type

Het standaard datatype voor FTP is 'ASCII'. De verzoeken voor Digipoort hebben echter UTF-8 als karakterset. Daarnaast dienen de verzoeken in verband met de aanwezigheid van hashes in de metadata op bit-niveau door de overdracht of opslag naar een ander systeem niet te veranderen. Om dit te bereiken dient de FTP client voor het starten van een upload (STOR) of download (RETR) te switchen naar het datatype 'image' (binair), door middel van het FTP commando TYPE I.

3.1.3 Inrichting per gebruiker

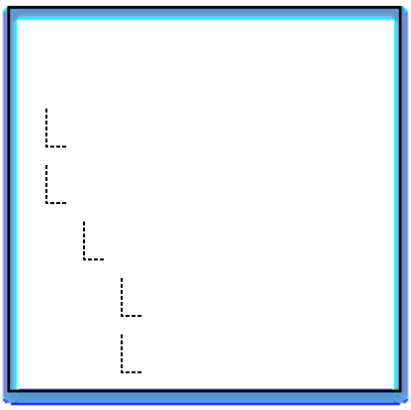
Iedere gebruiker van het FTP koppelvlak krijgt een eigen gebruikersmap op de Digipoort FTP server. Geen enkele andere gebruiker heeft toegang tot deze map.

De gebruikersmap heeft twee submappen:

- *in* – hier kunnen bestanden worden opgehaald die door Digipoort zijn geplaatst ten behoeve van de gebruiker. Digipoort plaatst in deze directory ook ontvangstbevestigingen en foutmeldingen.
- *out* – hier kunnen bestanden worden geplaatst die verwerkt moeten worden door koppelvlakservices van Digipoort.

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

Onder de 'in' en 'out' map zijn aanvullende submappen waarmee onderscheid gemaakt wordt: naar koppelvlak(versie) en service waarmee gecommuniceerd wordt (figuur 3). In de berichtstroomspecificatie zijn per berichtstroom de te gebruiken mappen gedefinieerd.



Figuur 3: Generieke mappenstructuur FTP-server.

Voor het afleveren van berichten en de statusupdate dient de aangesloten partij tevens over een eigen FTP server te beschikken, waar Digipoort verzoeken en antwoorden kan plaatsen. Voor deze servers wordt per berichtstroom de te hanteren mappenstructuur gespecificeerd. In onderstaande tabellen is een overzicht opgenomen van de locaties waar de bestanden geplaatst worden.

Bedrijven	**Locatie verzoeken**	**Locatie antwoorden**
Aanleverservice	Digipoort	Digipoort
Statusinformatieservice	Digipoort	Digipoort

Overheden	**Locatie verzoeken**	**Locatie antwoorden**
Afleverservice	Overheid	Digipoort
Statusupdateservice	Digipoort	Overheid

3.1.4 Bestand

De inhoud en structuur van de bestanden zijn vastgelegd in de servicebeschrijvingen. Daarnaast gelden voor het koppelvlak Grote Berichten 3.0 in ieder geval de volgende beperkingen:

- De maximale bestandsgrootte is 6 GiB, al kan deze voor een specifieke berichtstroom minder zijn.
- De bestandsnaam dient aan de volgende criteria te voldoen:
    - Alleen de tekens a-z, A-Z, 0-9, _ en – zijn toegestaan.
    - De maximale lengte van de bestandsnaam is 80 tekens.
- Per postbus moet de bestandnaam uniek zijn, en niet eerder voor een succesvol aangeleverd bestand gebruikt zijn.

3.1.5 Aanlevering van bestanden

Het bestand wordt aangeleverd door het te plaatsen in de in gebruikersdirectory met het STOR commando. Het bestand wordt na succesvolle aflevering uit de gebruikersdirectory verwijderd. Dit wordt bevestigd met een ontvangstbevestiging. Bij niet succesvolle aflevering wordt een foutmelding gegeven.

3.1.6 Verzoek, respons en foutmelding

De services op het koppelvlak Grote Berichten 3.0 hanteren een verzoek – antwoord mechanisme. Bij het succesvol plaatsen van een bestand zal Digipoort een respons, danwel een foutmelding, plaatsen als een apart bestand in de submap van de betreffende service in de *in* map van de gebruiker. Dit is een asynchroon proces. De inhoud en structuur van de respons, danwel foutmelding, is gedefinieerd in de servicebeschrijving van de aangesproken service.

3.1.7 Ophalen van bestanden

Het ophalen van bestanden bij de FTP server van Digipoort kan beginnen zodra deze zichtbaar voor hem zijn. Hiervoor wordt gebruik gemaakt van het RETR commando. Na het succesvol downloaden van het bestand wordt het bestand automatisch door Digipoort verwijderd. Nadat het bestand verwijderd is kan het niet meer teruggehaald worden.

3.2 Beveiliging

3.2.1 TLS specifieke FTP implementatie

De volgende zaken worden door de Digipoort FTP server afgedwongen voor het (veilig) gebruik van TLS in combinatie met het FTP protocol.

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 biedt 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. Dit is conform de specificatie van RFC 4217.

3.2.2 Vertrouwelijkheid

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. Digipoort verwerkt het bestand na aanlevering en draagt zorg voor het afleveren van het bestand bij ontvanger waarvoor deze bestemd is.

3.2.3 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. Een gebruikersnaam en wachtwoord voor de Digipoort FTP server wordt verkregen d.m.v. de accountaanvraagprocedure van Logius.

De server toetst de gebruikersnaam aan het clientcertificaat dat gebruikt is bij het tot stand komen van de TLS-verbinding (zie 1.3.1). De toegang wordt ontzegd als de gebruikersnaam niet overeenkomt met het geregistreerde certificaat.

3.2.4 Overige beperkingen

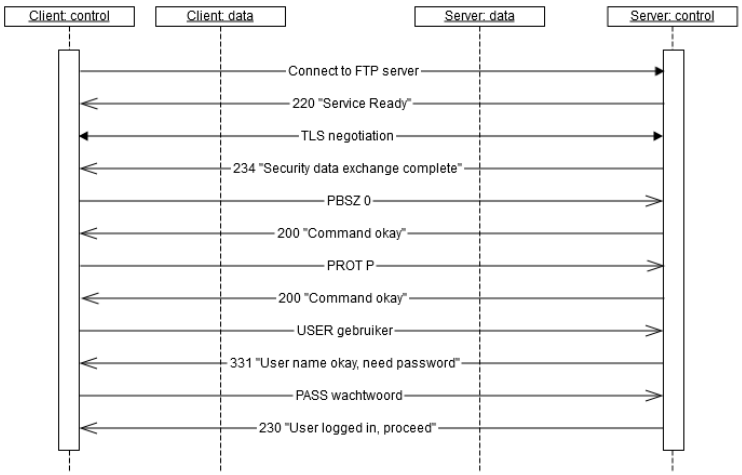
Voor de Digipoort FTP server zijn vanuit het oogpunt van beveiliging de volgende overige beperkingen van kracht:

- Een client mag, zolang er geen beveiligde TLS verbinding is opgezet, alleen de FTP commando's HELP, FEAT en AUTH gebruiken.
- De standaard FTP gebruiker (anonymous) is niet toegestaan.

3.3 Sequencediagrammen

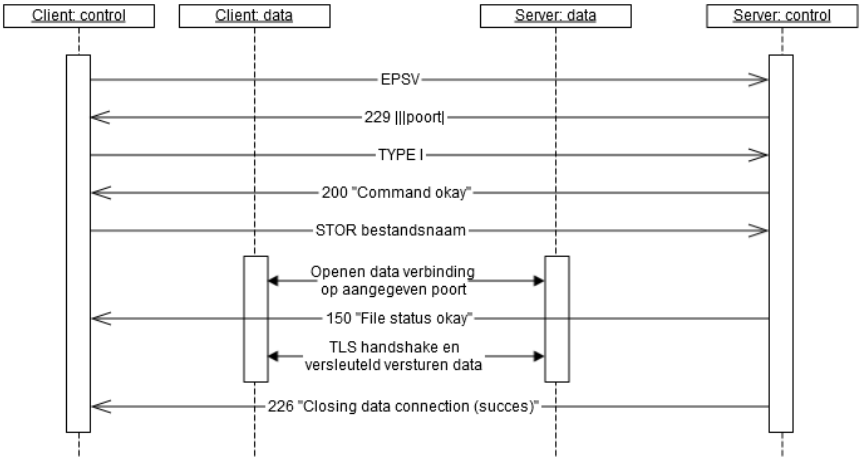
De volgende diagrammen geven een standaardscenario voor de beschreven functionaliteit.

3.3.1 Opzetten van een TLS verbinding



3.3.2 Plaatsen van bestanden

Preconditie: server en client hebben een TLS verbinding tot stand gebracht en de gebruiker is ingelogd.



4 Algemene afspraken

4.1 Communicatiestandaarden

De communicatie tussen webservice client en de webservice verloopt over een aantal lagen. Per laag gelden standaarden. Samengevat gaat het om de volgende standaarden:

Laag	**Standaard**	**Referentie**
Applicatielaag	XML	http://www.w3.org/TR/xml/
	MIME Multipart/Related	http://tools.ietf.org/html/rfc2045 http://tools.ietf.org/html/rfc2046 http://tools.ietf.org/html/rfc2387
Sessielaag	FTP	http://www.ietf.org/rfc/rfc959.txt http://tools.ietf.org/html/rfc3659 http://tools.ietf.org/html/rfc2228
	TLS over FTP	http://tools.ietf.org/html/rfc4217
Transportlaag	TCP	
	TLS v1.2	http://tools.ietf.org/html/rfc5246
Netwerklaag	IP	

4.2 Randvoorwaarden

De voor het opzetten van de beveiligde verbinding te gebruiken clientcertificaten zijn PKIoverheid-certificaten voor gebruik door services (https://www.logius.nl/diensten/pkioverheid/).

De gebruiker dient zelf zorg te dragen voor aanschaf van een clientcertificaat bij een van de door PKIoverheid aangewezen serviceproviders.

4.3 Karaktercodering en karakterset

De ondersteunde karakterset voor de bestanden is UTF-8.