Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Handleiding Aansluiten op Digipoort t.b.v. DigiInkoop/E-Factureren (voor Bedrijven)

Versie 1.7

Datum december 2017
Status Definitief

Colofon

Projectnaam	DigiInkoop en E-facturatie
Versienummer	1.7
Contactpersoon	Servicecentrum Logius
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Bijlage(n)	1

Wijzigingen

Februari 2017	• Aanpassing URL's n.a.v. aanpassing website Logius
December 2017	• Bijlage 2 verwijderd, M-Factuur is uitgefaseerd

Inhoud

Lijst van gebruikte afkortingen

CSP	Certification Service Provider (organisatie die namens een Certification Authority certificaten verstrekt)
HR-XML	Human Resources XML (de op XML gebaseerde standaard die wordt gebruikt voor gestructureerd berichtenverkeer tussen onder meer uitzendorganisaties en overheid.
UBL	Universal Business Language (de op XML gebaseerde standaard die wordt gebruikt voor het versturen van elektronische business documenten, zoals offertes, orders en facturen.
WUS	Middels deze afkorting wordt het op webservices gebaseerde koppelvlak voor bedrijven aangegeven.

1 Inleiding

1.1 Doel

Deze handleiding leidt u door het proces om aan te sluiten op Digipoort voor DigiInkoop/E-Factureren. Het gaat hierbij om het aansluitproces voor *bedrijven*. Hieronder verstaan wij zowel bedrijven die zelf inkoop- en/of factuurgegevens met de overheid willen uitwisselen als 'intermediairs' die dit namens hen doen.

DigiInkoop en E-factureren.

Bij uitwisseling van factuur- en/of inkoopgegevens worden de twee volgende varianten onderscheiden:

1. Uitsluitend elektronisch *factureren* (ook wel E-Factureren genoemd);
2. Geautomatiseerd ondersteunen van het inkoop- en factureringsproces (DigiInkoop).

Het in deze handleiding beschreven aansluitproces richt zich op het inrichten van het *berichtenverkeer* tussen bedrijf en Digipoort. Het indienen van facturen via het (toekomstige) DigiInkoop Leveranciers-portaal blijft hier buiten beschouwing.

Voor **overheden** is een aparte Aansluithandleiding beschikbaar (zie onder https://www.logius.nl/ondersteuning/digiinkoop-voor-rijksdienst-via-digipoort/).

De handleiding geeft u een totaaloverzicht van alle stappen die bij het aansluiten komen kijken. Een succesvolle aansluiting wil zeggen dat uw bedrijf in staat is om bijvoorbeeld digitale facturen via Digipoort naar de beoogde overheid/overheden te versturen en/of inkoopopdrachten en dergelijke van een overheid te ontvangen.

Dit document beschrijft deze stappen vanuit het perspectief van de projectleider die met de realisatie van de aansluiting is belast. De handleiding geeft dan ook in de eerste plaats een totaaloverzicht van de handelingen die uw bedrijf dient uit te voeren. Voor technische details wordt meestal doorverwezen naar additionele documentatie. Sommige technische aspecten zijn echter belangrijk genoeg om al in dit document onder de aandacht te brengen.

Bij elke stap is uitgelegd:

- waarom u deze dient uit te voeren;
- wat de randvoorwaarden zijn voor uitvoering van deze stap;
- welke hulpmiddelen (documenten en tools) hiervoor beschikbaar zijn;
- wat het beoogde resultaat is, en,
- hoe dit resultaat kunt verifiëren.

Waar van toepassing wordt verwezen naar additionele documentatie die voor een bepaalde stap of activiteit beschikbaar is. Tevens wordt dan de vindplaats (website) van deze documentatie aangegeven.

1.2 Fasering aansluitproces

Het aansluitproces dat in dit document wordt beschreven, bestaat uit activiteiten die deels door de aansluitende partij moeten worden uitgevoerd en deels door Logius.

De hierbij gebruikte fasering wordt vanaf hoofdstuk 4 van dit document nader toegelicht:

1. Voorbereiding: o.a. verzamelen van benodigde informatie (documentatie), bepalen van de impact op uw eigen organisatie, aanvragen van PKIoverheid-certificaat en in het geval van DigiInkoop het aanmelden van de beoogde aansluiting bij Logius;
2. Inrichten netwerkconnectiviteit: ervoor zorgen dat het bedrijf via het netwerk (internet) verbinding kan maken met Digipoort;
3. Inrichten koppelvlak: implementeren van de benodigde services en inrichten van de *certificate stores*;
4. Inhoudelijk bericht vormgeven en/of verwerken: ervoor zorgen dat het inhoudelijk bericht (factuur, etc.) in de juiste vorm (conform de gebruikte standaarden, UBL of HR-XML) wordt opgemaakt om te worden verstuurd aan Digipoort c.q. kan worden verwerkt door de eigen systemen;
5. Technische test tegen Digipoort: testen van de koppelvlak-implementatie ter voorbereiding van de ketentest. Deze test wordt uitgevoerd middels een operationele verbinding met de preproductieomgeving van Digipoort;
6. Preproductie (ketentest): uitvoeren ketentest met de beoogde ontvangende overheidsorganisatie over de preproductieverbinding;
7. Productiegang: In overleg met overheidsorganisatie een 'testrun' over de productieverbinding met Digipoort gevolgd door inproductiename van de aansluiting.

1.3 Doelgroep

Deze handleiding richt zich op bedrijven die zelf een aansluiting op Digipoort willen realiseren voor DigiInkoop/E-Factureren, of die een dergelijke aansluiting voor andere bedrijven willen realiseren. In het laatste geval spreken we van intermediairs.

De handleiding richt zich daarbij in de eerste plaats op de projectleider die voor het bedrijf belast is met het realiseren van de aansluiting. De informatie in deze handleiding helpt de projectleider bij het maken van een realistische aansluitplanning en bij het bepalen van de resources die in elke fase van het aansluittraject benodigd zijn.

Voor overheidsorganisaties is een aparte Aansluithandleiding voorhanden (zie https://www.logius.nl/ondersteuning/digiinkoop-voor-rijksdienst-via-digipoort/).

1.4 Leeswijzer

Hoofdstuk 2 geeft algemene informatie over Digipoort en daarmee een beschrijving van de context waarbinnen een aansluiting op DigiInkoop plaatsvindt.

Een globale toelichting op het aansluitproces volgt in hoofdstuk 3.

Vanaf hoofdstuk 4 volgt een gedetailleerde beschrijving van de stappen en bijbehorende activiteiten die binnen het aansluitproces worden onderscheiden. Aan aspecten die van grote invloed kunnen zijn op de doorlooptijd of anderszins van speciaal belang zijn, wordt nadrukkelijk aandacht gegeven.

1.5 Suggesties

Logius vindt het belangrijk dat u snel en zonder problemen van DigiInkoop gebruik kunt maken. Deze handleiding helpt u daarbij. Heeft u suggesties om dit proces verder te verbeteren? Stuur die dan op naar Servicecentrum Logius.

1.6 Begeleiding bij aansluiten

E-facturatie kan zelfstandig door een partij worden geïmplementeerd. Voor DigiInkoop zal Logius de berichtenstromen die u ontvangt moeten configureren in Digipoort.

Heeft u vragen of problemen in de voorbereiding of gedurende het aansluiten dan is het Servicecentrum van Logius uw eerste aanspreekpunt.

Telefoon	0900 555 45 55 (10 ct. p/m)
E-mail	servicecentrum@logius.nl

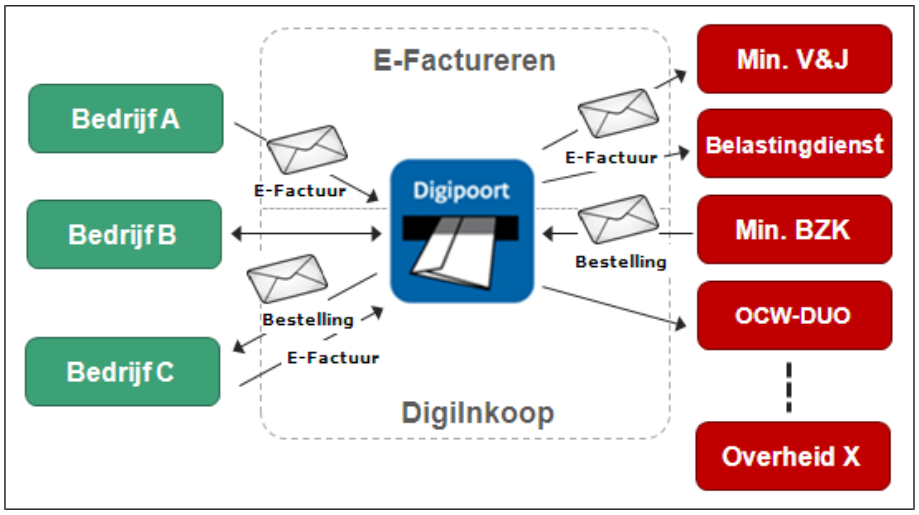
Op de website van Logius vindt u alle documenten die u voor het aansluiten nodig heeft: https://www.logius.nl/ondersteuning/digiinkoop-voor-leveranciers-via-digipoort/.

2 Algemene informatie over Digipoort

DigiInkoop geeft bedrijven de mogelijkheid om factuur- en/of inkoopinformatie met de overheid uit te wisselen met elektronisch berichtenverkeer via Digipoort.

2.1 Digipoort: berichtenverkeer

Digipoort is de centrale infrastructuur waarmee bedrijven digitale informatie kunnen uitwisselen met de overheid. Deze uitwisseling verloopt via berichten. Zo'n bericht kan een e-factuur zijn die een bedrijf aan een overheidsorganisatie verzendt of bijvoorbeeld een tijdkaart met de gewerkte uren of bestelling van de overheidsorganisatie naar het bedrijf.



Figuur 1: overzicht DigiInkoop

Via Digipoort kan een bedrijf berichten uitwisselen met alle op Digipoort aangesloten overheden. Bedrijven hoeven dus niet met iedere overheid een aparte koppeling te realiseren.

2.1.1 Koppelvlakken

Een koppelvlak is een beschrijving van alle afspraken die benodigd zijn om 'betekenisvolle' gegevensuitwisseling tussen twee verschillende informatiesystemen mogelijk te maken.
Digipoort biedt verschillende koppelvlakken voor bedrijven enerzijds en overheden anderzijds, waaronder FTP, SMTP, WUS en ebMS. Via deze koppelvlakken worden diverse berichtstromen van en naar de overheid mogelijk gemaakt, zoals ziekmeldingen, statistiekberichten, facturen, bestellingen, etc.

Voor berichtenverkeer van DigiInkoop moeten bedrijven gebruik maken van het koppelvlak 'WUS 2.0 voor Bedrijven'.

- *Documentatie*: Koppelvlakbeschrijving 'WUS 2.0 voor bedrijven', te vinden in het zip-bestand ("Laatste stabiele versie") op https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-bedrijven/.

2.1.2 Services

Ieder Digipoort-koppelvlak biedt meerdere services. In het geval van het 'WUS 2.0 voor Bedrijven'-koppelvlak gaat het hier om zogenoemde webservices, die voorzien in functionaliteit om elektronische berichten aan te leveren (bijvoorbeeld een factuur gericht aan een overheidsorganisatie) of elektronische berichten te ontvangen (bijvoorbeeld een inkooporder van een overheidsorganisatie).

Deze services zijn generiek van opzet. Dat wil zeggen dat middels deze services inhoudelijk heel verschillende berichten kunnen worden verstuurd. Een bedrijf kan via dezelfde service bijvoorbeeld zowel bestelbevestigingen als facturen als bijvoorbeeld SBR rapportages aan de overheid sturen. Een implementatie van deze services voor DigiInkoop kan in de toekomst dus mogelijk worden hergebruikt voor andere toepassingen.

Meer informatie over de services is te vinden in paragraaf 6.1.6.

- *Documentatie:* servicebeschrijvingen van de afzonderlijke services, te vinden in het zip-bestand ("Laatste stabiele versie") op https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-bedrijven/.

2.1.3 Berichtstroom/verwerkingsproces

Berichten worden met Digipoort uitgewisseld binnen een specifieke 'berichtstroom' of 'verwerkingsproces'. Deze berichtstromen zijn binnen Digipoort gespecificeerd. Een service kan verschillende berichtstromen ondersteunen. Op de envelop van het bericht kunt u aangegeven welke berichtstroom Digipoort moet gebruiken.

2.1.4 Berichten

Vergelijkbaar met een poststuk bestaat een bericht uit een envelop en de berichtinhoud. Op de envelop staat de informatie die nodig is voor adressering, routering en beveiliging van het bericht en geeft aan om welke berichtsoort het gaat. De berichtinhoud bevat de inhoudelijke gegevens die de verzender naar de ontvanger wil sturen (de factuur, inkooporder, etc., in digitale vorm). De vorm en inhoud van de envelop zijn vastgelegd in de koppelvlakspecificatie. In de documentatie (servicebeschrijvingen, zie paragraaf 2.1.2) zijn voorbeelden van de envelop ('SOAP-berichten') te vinden.

Op de inhoud zijn aparte afspraken van toepassing, vastgelegd in inhoudelijk-berichtspecificaties, namelijk in de standaarden UBL en HR-XML. UBL heeft betrekking op levering van producten en diensten en HR-XML betreft Human Resource inkoopstromen.

- *Documentatie:* berichtenstandaard UBL, te vinden onder https://www.logius.nl/ondersteuning/gegevensuitwisseling/ubl-ohnl/ , en berichtenstandaard HR-XML, te vinden onder https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl/.

  De berichtenstandaarden zijn gepubliceerd als zip-bestand. In deze zip-bestanden is binnen de submap 'doc' een lees- of implementatiewijzer te vinden, die een uitgebreide toelichting op de overige documentatie in het zip-bestand geeft.

Digipoort valideert zowel envelop als inhoud tegen de bijbehorende specificaties.

2.2 Digipoort Portaal

Digipoort biedt een internetportaal waarmee via de browser afzonderlijke berichten kunnen worden aangeleverd aan Digipoort. Het Digipoort Portaal kent twee versies: een versie die toegang biedt tot de preproductieomgeving van Digipoort en een versie die toegang biedt tot de productieomgeving.

Het Digipoort Portaal is een generieke voorziening die wordt geboden door Digipoort. Via dit Portaal kunnen berichten worden ingeschoten voor diverse diensten die onder Digipoort worden aangeboden. Hieronder vallen DigiInkoop/E-Factureren, maar ook andere diensten die met DigiInkoop niets van doen hebben.

Het Digipoort Portaal moet niet worden verward met de portaalvoorzieningen die specifiek voor DigiInkoop/E-Factureren worden aangeboden, zoals het Factuurportalen in de markt of het DigiInkoop en E-facturatie leverancierspportaal van Logius.

Vooral het Portaal dat toegang biedt tot de preproductieomgeving kan handig zijn voor bedrijven:

- Het kan in de ontwikkelfase worden gebruikt om statusinformatie uit te vragen voor aangeleverde berichten, zolang u de Statusinformatieservice niet heeft geïmplementeerd;
- Het kan worden gebruikt om de inhoudelijke berichten te testen, die door uw systeem zijn gegenereerd, bijvoorbeeld wanneer de Aanleverservice nog niet operationeel is. Uit de teruggegeven statusinformatie valt onder meer af te lezen of het bericht door Digipoort succesvol is gevalideerd.

❖ *Documentatie:* de Handleiding Digipoort Portaal, te vinden onder : https://www.logius.nl/ondersteuning/digiinkoop-voor-leveranciers-via-digipoort/. Hierin zijn ook de adressen opgenomen waarmee u het Portaal kunt bereiken.

3 Algemene informatie over het aansluitproces

Door een aansluiting op Digipoort kan een bedrijf elektronische berichten uitwisselen met de overheid. In het geval van DigiInkoop gaat het bij deze berichten om gegevens rond elektronisch inkopen en/of factureren.

Binnen DigiInkoop onderscheiden we de twee volgende mogelijkheden:

1. Uitsluitend elektronisch *factureren* (ook wel E-factureren genoemd);
2. Geautomatiseerd ondersteunen van het inkoop- en factureringsproces (DigiInkoop).

Een succesvolle aansluiting betekent dat uw bedrijf in staat is om de gegevens die horen bij de gekozen optie elektronisch te verzenden naar dan wel te ontvangen van de overheid.

Organisatie

Het inrichten van elektronisch berichtenverkeer middels Digipoort is niet alleen een technische exercitie maar kent ook een belangrijk organisatorisch aspect. Niet alleen moeten uw systemen geschikt worden gemaakt voor het verzenden en ontvangen van de berichten, ook de organisatie zal klaar moeten zijn om met deze nieuwe invulling van de informatievoorziening te kunnen werken.

Hierbij kunt u bijvoorbeeld denken aan het volgende: indien E-Factureren of DigiInkoop binnen het bedrijf wordt geïmplementeerd:

- Wat is dan het effect op de bedrijfsprocessen?
- Welke aanpassingen zijn vereist in procedures ter ondersteuning van deze bedrijfsprocessen?
- Wie van het personeel krijgt hier mee te maken (in welke gevallen is sprake van een significant effect op de werkzaamheden)?
- Welke aanvullende maatregelen moeten worden genomen (training/educatie, functieomschrijving/werkinhoudelijk, etc.)
- Etc.

Uw berichten kunnen succesvol afgeleverd worden bij een overheidsorganisatie, maar er zijn ook foutsituaties mogelijk. Zijn systemen en organisatie in staat om deze fouten tijdig te signaleren en hier effectief op te reageren?

Het aansluitproces beschrijft alle handelingen die moeten worden uitgevoerd om met succes op DigiInkoop aan te sluiten. Een deel van deze handelingen moet door uw bedrijf worden uitgevoerd, een ander deel door Logius.

Alle handelingen zijn beschreven in het planningsdocument dat Logius voor aansluitingen heeft ontwikkeld. Deze handelingen zijn voorzien van een gemiddelde doorlooptijd, waarmee u ook een prognose kunt maken van het gehele aansluittraject.

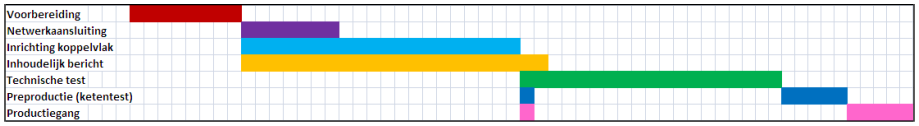
Het planningsdocument is hier te vinden:

❖ https://www.logius.nl/ondersteuning/digiinkoop-voor-leveranciers-via-digipoort/

De afzonderlijke stappen en de activiteiten die daaronder moeten worden uitgevoerd, worden in de volgende hoofdstukken beschreven.

3.1 Doorlooptijd

De doorlooptijd van de aansluiting is mede afhankelijk van de organisatie en de wijze waarop het aansluittraject wordt ingericht. De afzonderlijke stappen hoeven bijvoorbeeld niet allemaal sequentieel te worden uitgevoerd (eventuele afhankelijkheden zijn aangegeven in het planningsdocument). Afhankelijk van de beschikbare capaciteit kunnen ze deels parallel worden uitgevoerd, wat tot een verkorting van de doorlooptijd leidt. Onderstaande figuur toont een voorbeeld van het verloop van de doorlooptijd:



Figuur 2: voorbeeld verloop doorlooptijd

Daarnaast hangt de doorlooptijd van het aansluitproces van een aantal andere zaken af, waaronder:

- technische complexiteit van uw IT-organisatie
- beschikbare kennis en capaciteit binnen uw bedrijf over uw systemen en over de gebruikte standaarden en technologie (zie ook paragraaf 4.2).

3.2 Documentatie

❖ U vindt alle documenten die u voor het aansluiten nodig heeft op : https://www.logius.nl/ondersteuning/digiinkoop-voor-leveranciers-via-digipoort/.

In de navolgende hoofdstukken worden de stappen van het aansluitproces beschreven:

1. Voorbereiding
2. Netwerkaansluiting
3. Inrichting koppelvlak
4. Inhoudelijk bericht genereren en verwerken
5. Technische test tegen Digipoort
6. Preproductie (ketentest)
7. Productiegang

4 Stap 1: voorbereiding

Een aansluiting op Digipoort begint met een voorbereidingsfase waarin alle voorbereidingen worden getroffen om de aansluiting zo soepel mogelijk te laten verlopen. Het gaat in deze fase vooral om het verkrijgen van alle benodigde informatie, het regelen van de benodigde technische capaciteit en het indienen van het aansluitformulier.

Logius verwacht van een bedrijf dat wil aansluiten dat het:

- checkt bij uw sofware leverancier dat uw software geschikt is of gemaakt kan worden;
- de voor het aansluiten benodigde informatie verzamelt en doorneemt;
- ervoor zorgt dat het beschikt over de benodigde technische expertise;
- een projectplan maakt (indien de eigen organisatie dat wenst) waar het document "Planning aansluiten Digipoort PI voor bedrijven voor DigiInkoop/E-Factureren" als leidraad kan dienen.
- aanmelden van uw aansluiting bij Servicecentrum Logius, ga voor het formulier naar https://www.logius.nl/contact/formulieren/aanvraagformulier-digipoort/

Voor DigiInkoop zal Logius op basis van de aanvraag Digipoort inrichten. Voor E-facturatie is dit niet nodig en kan het bedrijf zelfstandig aansluiten. De handelingen, die voor de voorbereiding door bedrijf en Logius moeten worden uitgevoerd, worden hieronder verder toegelicht.

4.1 Informatie verkrijgen

Op de Logius-website kunt u informatie vinden met betrekking tot Digipoort en DigiInkoop/E-Factureren en het aansluiten daarop (DigiInkoop: https://www.logius.nl/diensten/digiinkoop/ en E-factureren: https://www.logius.nl/diensten/e-factureren/). Ook is technische documentatie beschikbaar, waaronder beschrijvingen van de beschikbare services, de verschillende berichttypen en de gebruikte standaarden, zoals UBL en HR-XML. Deze technische informatie is vooral van belang voor architecten, ontwerpers en ontwikkelaars die zijn betrokken bij de realisatie van de koppeling met Digipoort.

Het is van groot belang gebleken om voorafgaand aan het feitelijke aansluittraject een gedegen beeld te krijgen van de activiteiten die moeten worden uitgevoerd en de kennis die daarbij is benodigd, zodat een realistische planning kan worden opgesteld en vastgesteld kan worden of het bedrijf beschikt over de benodigde technische expertise.

Deze Handleiding kan natuurlijk zelf worden gebruikt om een eerste overzicht te verkrijgen.

4.2 Technische expertise in huis halen

Om berichtenverkeer met Digipoort mogelijk te maken, moet een bedrijf een aantal services implementeren volgens het koppelvlak "WUS 2.0 voor

bedrijven". Het koppelvlak is ingericht op basis van internationale standaarden met betrekking tot routering en beveiliging van berichten, etc. Om services conform dit koppelvlak te realiseren, is de nodige technische expertise vereist.

Om vast te stellen in hoeverre uw bedrijf over deze technische expertise beschikt, kan met name naar de volgende aspecten worden gekeken:

- webservices-standaarden (o.a. SOAP, WSDL, WS-Addressing);
- beveiligd transport via dubbelzijdig TLS/SSL (denk hierbij aan het inrichten van de benodigde *certificate stores*);
- WS-Security (digitaal ondertekenen van berichten en kunnen verwerken van ontvangen berichten die op hun beurt digitaal ondertekend zijn);
- Berichtenstandaarden UBL en/of HR-XML: minimaal vereist is gedegen kennis van XML en XSD's voor begrip van UBL/HR-XML.

Niet alle bedrijven beschikken 'in huis' over de vereiste kennis en ervaring. In de markt zijn er verschillende leveranciers actief die de aansluiting voor uw bedrijf kunnen uitvoeren of een deel van de werkzaamheden voor hun rekening kunnen nemen. Check ook bij de leverancier van uw financiële software zij hebben misschien eerder de aansluiting gerealiseerd en kunnen u helpen.

4.3 Inrichten Digipoort door Logius voor DigiInkooppartijen

Indien uw bedrijf wil aansluiten op Digipoort in het kader van DigiInkoop, dient u contact op te nemen met Servicecentrum Logius. Logius kan de Digipoort voor u inrichten in preproductie en de productieomgeving.

4.4 Ketentestpartij

Het technisch testen van uw aansluiting kan in de preproductie omgeving van Digipoort. Hier kunt u testen of uw aansluiting functioneert en of de berichten technisch valide zijn. Maar voor het functioneel testen van de aansluiting heeft u een ketentestpartij nodig. Zij kunnen zien of de factuur ook functioneel aan alle eisen voldoet opdat ze deze in hun omgeving goed kunnen verwerken.

4.5 Aansluitformulier

Middels het 'Aansluitformulier' kunt u een formeel verzoek tot aansluiting op Digipoort indienen. Op het Aansluitformulier kunt u aangeven dat u gebruik wilt maken van berichtstroom DigiInkoop of E-Factureren. Tevens geeft u via dit formulier de benodigde contactgegevens door.

Op het Aansluitformulier geeft u tevens aan dat u akkoord gaat met de Gebruiksvoorwaarden Digipoort.

- *Het aanvraagformulier en de gebruiksvoorwaarden* Digipoort zijn te vinden onder https://www.logius.nl/ondersteuning/e-factureren-voor-leveranciers-via-digipoort/.

Het Aansluitformulier wordt opgestuurd naar Servicecentrum Logius (zie de contactgegevens op pag. 2).

4.6 Projectplan

Het projectplan beschrijft aanpak, planning en benodigde resources (mensen en middelen) voor het realiseren van de verbinding tussen bedrijf en Digipoort voor DigiInkoop/E-Factureren.

Het projectplan is enkel bedoeld als leidraad voor het bedrijf. Logius hoeft hierin geen inzage te hebben.

4.7 Planningsdocument

De planning kan worden gebaseerd op het planningsdocument:

- *Planning aansluiten Digipoort voor bedrijven*, te vinden onder https://www.logius.nl/ondersteuning/e-factureren-voor-leveranciers-via-digipoort/

In het planningsdocument zijn alle aansluithandelingen opgenomen en de partij die voor de betreffende handeling verantwoordelijk is (Logius of bedrijf). In het document is tevens een indicatie van de doorlooptijd per handeling aangegeven, alsmede de mogelijke afhankelijkheden die een handeling met andere handelingen heeft.

4.8 Start aansluittraject

Voor E-facturatie heeft Logius geen acties, omdat Digipoort niet hoeft worden geconfigureerd. U kunt zelfstandig met de documentatie en de testvoorzieningen aansluiten. Zorg wel dat u ook de statusinformatie service implementeert. Dit is een eis voor het gebruik van Digipoort voor E-facturatie.

5 Stap 2: netwerkaansluiting

Netwerkconnectiviteit is randvoorwaardelijk voor een aansluiting op Digipoort. Zonder netwerkconnectiviteit is immers geen berichtenverkeer mogelijk.

Voor bedrijven wordt netwerkconnectiviteit ingericht op basis van internet (beveiligde verbinding over HTTPS).

De server via welke de verbinding met Digipoort wordt opgezet, zal dan ook toegang tot internet moeten hebben. In de regel moeten hiervoor instellingen worden aangepast op de firewall van uw bedrijf. Berichtenverkeer met Digipoort voor DigiInkoop/E-Factureren betreft altijd inkomend en uitgaand verkeer, de firewall zal derhalve voor beide richtingen moeten worden geconfigureerd.

Wanneer de benodigde aanpassingen zijn gedaan, dient de netwerkverbinding te worden getest vanaf de host waarop de software (service-implementatie, zie stap 3) wordt geïnstalleerd. Met behulp van telnet of een vergelijkbare utility kan worden geprobeerd om verbinding met Digipoort te maken.

Zodra het bedrijf beschikt over de benodigde certificaten, kan ook de beveiliging (TLS/SSL) worden getest. De beveiligde verbinding zal later ook vanuit Digipoort worden getest (zie verder onder Hoofdstuk 8). Beveiligd berichtenverkeer is pas mogelijk wanneer beide kanten succesvol een TLS/SSL-verbinding tussen elkaars servers kunnen opzetten. **NB:** in dit stadium is het voldoende als er een TCP/IP-verbinding met Digipoort kan worden gemaakt, er hoeft nog geen beveiligde verbinding te worden opgezet.

Firewall
Aangezien er gebruik wordt gemaakt van het HTTPS-protocol (beveiligde verbinding), moet er verkeer mogelijk zijn over TCP/IP-poort 443 (de firewall moet uitgaand verkeer richting deze poort toelaten). Verkeer vanuit Digipoort naar het bedrijf loopt via hetzelfde protocol, dus ook inkomend verkeer (vanaf Digipoort-endpoint en poort 443) moet worden toegelaten.

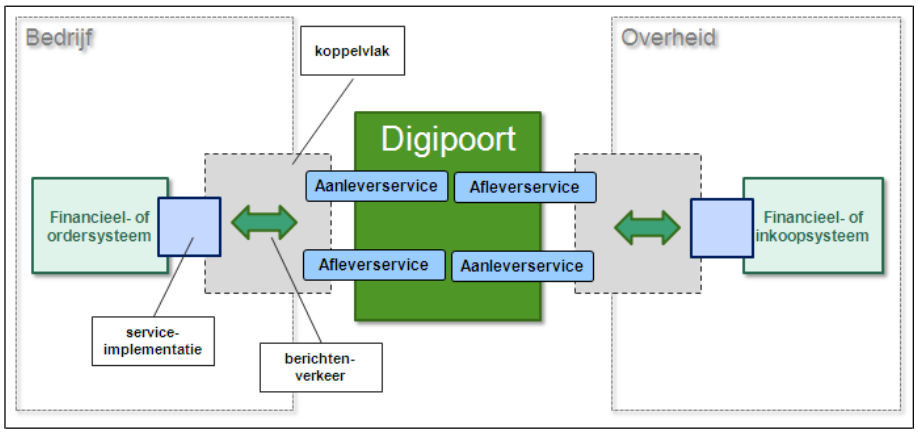
- Opmerking: de bij de Digipoort-endpoints behorende IP-adressen zijn te achterhalen via een 'lookup' van de DNS-namen.

5.1 Mijlpaal netwerkaansluiting

Indien het bedrijf in staat is om vanaf de 'DigiInkoop-host' een TCP/IP-verbinding te maken met Digipoort, is de mijlpaal "netwerkaansluiting gereed" bereikt.

6 Stap 3: realiseren koppelvlak

Het doel van deze stap is om de technische koppeling tussen bedrijf en Digipoort gerealiseerd te krijgen, zodat via deze koppeling een ketentest kan worden uitgevoerd (stap 6) zodra ook de inhoudelijke bericht-verwerking is gerealiseerd (stap 4) en de geïmplementeerde services tegen Digipoort zijn getest (stap 5). De ketentest bestrijkt het gehele proces van gegevensuitwisseling vanuit (bijvoorbeeld) uw financiële- of verkoopsysteem via Digipoort naar de beoogde overheidsorganisatie. Deze keten wordt in onderstaande figuur geïllustreerd:



Figuur 3: overzicht van de keten

In deze stap doorloopt u de volgende stappen:

- Aanvragen van certificaten[1] en inrichten van 'certificate stores';
- Implementeren van de benodigde services.

De software die de implementatie van het koppelvlak (services) vormt, wordt ook wel 'adapter' genoemd. De adapter vormt de softwarematige schakel tussen uw bedrijfssysteem en Digipoort.

Preproductie- en productieomgeving

Berichtenverkeer met Digipoort zal normaliter plaatsvinden via de *productieverbinding*, de 'ingang' voor productieverkeer.

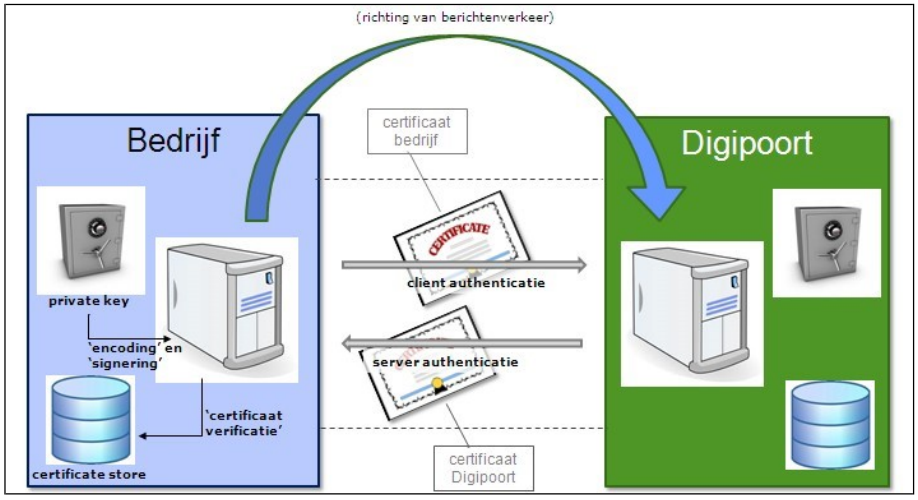
Voor het *testen* van berichtenverkeer biedt Digipoort ook een *preproductieomgeving*. Bedrijven zullen in eerste instantie hun berichtenverkeer inrichten in deze omgeving en pas nadat het testtraject succesvol is afgesloten, kunnen overgaan naar de productieomgeving.

[1] *Vanwege de verwachte levertijd kunnen PKIoverheid-certificaten al eerder zijn aangevraagd.*

6.1 Certificaten

6.1.1 Beveiliging: transportbeveiliging en berichtbeveiliging

Certificaten worden gebruikt bij het opzetten van een beveiligde verbinding tussen bedrijf en Digipoort en bij het digitaal ondertekenen ('signering') van de uitgewisselde berichten.



Figuur 4: overzicht gebruik van certificaten

Het gebruik van een beveiligde verbinding (op basis van tweezijdig TLS/SSL) en het ondertekenen van berichten zijn beide verplicht onder het koppelvlak 'WUS 2.0 voor bedrijven' (zie voor meer informatie *Koppelvlakbeschrijving WUS 2.0 Bedrijven*)[2]. De beveiligde verbinding, waarbinnen beide communicatiepartners zijn geauthenticeerd, zorgt voor versleuteld verkeer tussen bedrijf en Digipoort. Het ondertekenen van een bericht zorgt ervoor dat te allen tijde kan worden geverifieerd van wie het bericht afkomstig is en dat het bericht 'onderweg' niet is gewijzigd.

6.1.2 Productie- en testcertificaten

Voor de *productieverbinding* tussen bedrijf en Digipoort worden PKIoverheid-certificaten gebruikt. Dit zijn certificaten waarvan de echtheid wordt gegarandeerd door een officiële certificaatverstrekker (*Certification Service Provider, CSP*). Deze certificaten worden door zowel bedrijf als Digipoort gebruikt voor wederzijdse identificatie/authenticatie.

Voor de *preproductieverbinding* kunnen testcertificaten worden gebruikt maar ook PKIoverheid productiecertificaten worden geaccepteerd.

Productiecertificaten

PKIoverheid-certificaten zijn certificaten waaraan speciale eisen worden gesteld. Niet alle CSP's verstrekken PKIoverheid-certificaten, en niet alle door CSP's verstrekte certificaten zijn PKIoverheid-certificaten.

Uitsluitend PKIoverheid-certificaten kunnen worden gebruikt voor productieverkeer met Digipoort. Mocht uw bedrijf al beschikken over een beveiligde verbinding op

[2] *Te vinden in het zip-bestand ("Laatste stabiele versie") op https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-bedrijven/*

basis van een *niet*-PKIoverheid-certificaat, dan kan deze verbinding niet ook worden gebruikt voor productieverkeer met Digipoort. Aan een 'endpoint' kan namelijk maar één certificaat worden gekoppeld. Voor communicatie met Digipoort zal in dit geval een aparte server moeten worden ingericht, zodat correcte authenticatie op basis van een PKIoverheid-certificaat kan plaatsvinden.

PKIoverheid-certificaten: belangrijke terminologie

CSP's leveren in de regel verschillende PKIoverheid-certificaten. Voor het beveiligen van de transportverbinding met Digipoort is een zogenoemd *services certificaat* nodig. Dit certificaat wordt gebruikt als *client certificaat* wanneer uw bedrijf een verbinding met Digipoort initieert (oftewel: wanneer namens uw bedrijf een bericht naar Digipoort wordt verstuurd). Hetzelfde certificaat wordt in de regel ook gebruikt als *server certificaat*, waarmee uw server zich identificeert wanneer de verbinding door Digipoort wordt geïnitieerd.

De certificaten bevatten de zogenoemde *publieke sleutel* (.cer formaat), die samen met de bijbehorende *private sleutel* een uniek sleutelpaar vormt. Certificaten worden uitgewisseld met communicatiepartners, terwijl de private sleutel strikt geheim dient te worden gehouden. Soms zit het publieke deel van het certificaat als onderdeel van de certificaat hierarchie in een .crt of .pem bestand.

Certificaten worden door een certificaatverstrekker geleverd op basis van een Certificate Signing Request (CSR), in wezen het verzoek aan een certificaatverstrekker om een certificaat aan te maken op basis van door het bedrijf aangeleverde gegevens. U bent in de meeste gevallen zelf verantwoordelijk voor het creëren van deze CSR. In de regel zal dit gebeuren door de persoon die binnen of namens uw bedrijf acteert als *certificaatbeheerder*. De certificaatbeheerder genereert de CSR nadat hij eerst het private/publieke sleutelpaar heeft aangemaakt.

De geheime private sleutel wordt meestal opgeslagen in een .p12-bestand of .pfx-bestand. Dit bestand is beveiligd met een wachtwoord.

Het gebruikelijke bestandsformaat waarin certificaten door een CSP worden geleverd, is .p7b. In dat laatste geval bevat het bestand ook de 'intermediaire certificaten' die onderdeel uitmaken van de *certificaathiërarchie* op basis waarvan het certificaat wordt vertrouwd.

6.1.3 Aanvragen van PKIoverheid-certificaten

PKIoverheid-certificaten worden aangevraagd bij een CSP waarmee het bedrijf een overeenkomst heeft gesloten. Deze certificaten moeten worden aangevraagd door de persoon die binnen of namens het bedrijf als *certificaatbeheerder* bij de CSP is geregistreerd.

Meer informatie vindt u hier:
https://www.logius.nl/diensten/pkioverheid/aanschaffen/ (onder 'Aanschaffen').

U vindt hier ook een overzicht van CSP's die PKIoverheid-certificaten leveren.

6.1.4 Aanvragen van testcertificaten

De CSP's bieden testcertificaten maar voor het gebruik van Digipoort preprodutie kunt u gratis PKI testcertificaten aanvragen bij het Logius Servicecentrum. Deze kunt u gebruiken voor het testen van de verbinding met Digipoort of het ondertekenen van berichten. Het Logius testcertificaat heeft geen gekoppelde revocationlist. Wilt u uw aansluiting testen met deze functionaliteit dan dient u een testcertificaat bij de CSP aan te schaffen.

Stuur hiervoor een e-mail naar servicecentrum@logius.nl en geef daarbij de volgende informatie:

1. dat u het testcertificaat wilt gebruiken voor Digipoort,
2. de naam van uw organisatie,
3. de naam van de server waar u het testcertificaat op gaat gebruiken,
4. het KvK-nummer van uw bedrijf.

Ad. 2.
Geef de naam op van uw bedrijf waarmee u wilt aansluiten op Digipoort. Bent u een intermediair, dan kunt u uw eigen organisatienaam gebruiken.

Voorbeeld bedrijfsnaam: "PostNL", of "KPN"

Ad. 3.
Geef het URL-adres op van de server, waaronder deze geregistreerd is in de DNS-server. Bijvoorbeeld "testserver.mijnbedrijf.nl". Dit hoeft alleen als u gebruik maakt van een webserver waarvoor u ook werkelijk een voor DNS-naam geregistreerd heeft.

Maakt u geen gebruik van DNS registratie, dan kunt u hier de hostnaam zetten, die de systeembeheerder heeft toegewezen aan de server, of het algemene internetadres van uw bedrijf of organisatie. Bijvoorbeeld: "SERVER234", of "www.mijnbedrijf.nl". Als u als bedrijf alleen berichten aanlevert, dan is een DNS-registratie meestal niet nodig en is het opgeven van het algemene internetadres voldoende.

Voorbeeld DNS-naam: "testserver.mijnbedrijf.nl"
Voorbeeld hostnaam: "SERVER234"
Voorbeeld internetadres: "www.minbzk.nl"

Ad. 4.
Geef dan uw 8-cijferige KvK-nummer op.

Voorbeeld KvK-nr: "30053172"

NB: voor het aanvragen van een testcertificaat bij Logius is het niet nodig om een CSR aan te leveren (zie kader). Logius levert zowel het certificaat als de bijbehorende private sleutel. De private sleutel dient uiteraard zorgvuldig binnen uw bedrijf te worden bewaard en niet te worden uitgewisseld met andere partijen.

6.1.5 Installeren van certificaten

Om een beveiligde netwerkverbinding tussen uw bedrijf en Digipoort op te zetten en de hierover verzonder berichten digitaal te ondertekenen, moeten certificaten en bijbehorende private sleutels toegankelijk zijn voor de software die voor beveiliging en ondertekening zorg draagt. Certificaten en sleutels worden daartoe geïmporteerd in een of meer *certificate stores* (zie ook Bijlage 1).

Wat moet er worden geïnstalleerd?

- Preproductie:
  - eigen testcertificaat (of PKIoverheid-certificaat) en private sleutel, inclusief bijbehorende (test-)certificaathiërarchie;
  - hiërarchie behorend bij het Digipoort-testcertificaat (**NB:** Digipoort gebruikt een 'G1-certificaat'. Vanaf 1 januari 2011 worden 'G2-certificaten' verstrekt. Uw bedrijf heeft waarschijnlijk ook zo'n G2-testcertificaat ontvangen. Deze nieuwe certificaten kennen een eigen certificaathiërarchie, die afwijkt van de G1-hiërarchie. De G1-hiërarchie zal, naast de G2-hiërarchie, door uw systeem moeten worden vertrouwd en moet derhalve worden opgenomen in de verzameling vertrouwde certificaten.

- Productie:
  - eigen PKIoverheid-certificaat en private sleutel, inclusief bijbehorende hiërarchie;
  - hiërarchie behorend bij het Digipoort-certificaat.

    NB: indien het PKIo-certificaat door de CSP in .p7b-formaat is aangeleverd, bevat het normaliter ook al de bijbehorende 'intermediaire certificaten'. Het kan dan nog steeds nodig zijn om het 'stamcertificaat' - het 'Staat der Nederlanden root CA'-certificaat – apart te installeren, aangezien dat niet wordt opgenomen in het .p7b-bestand.

Meer informatie over PKIoverheid-certificaten vind u hier:
https://www.logius.nl/diensten/pkioverheid/

Informatie over stamcertificaat en andere (intermediaire) certificaten in de PKIOoverheid-certificaathiërarchie vindt u hier:
https://www.logius.nl/ondersteuning/pkioverheid/stamcertificaat-installeren/.

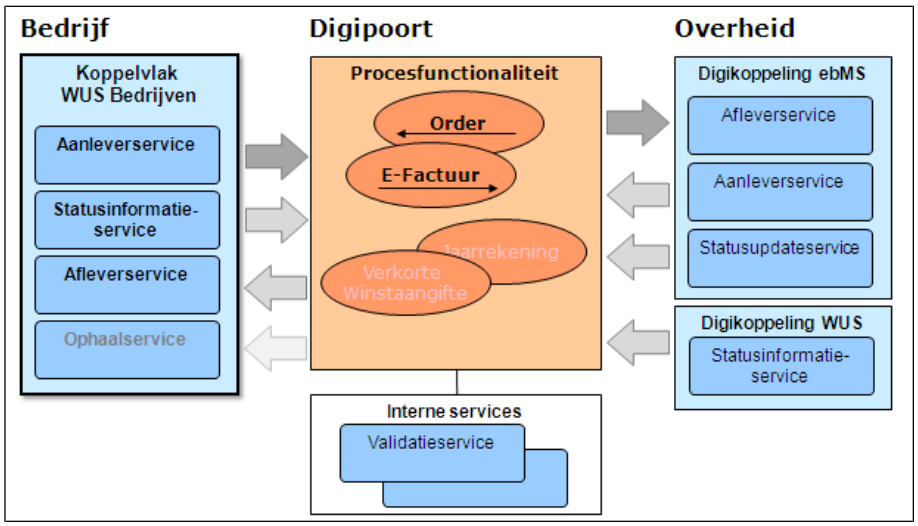
Onder deze laatste link kunt u het stamcertificaat en de intermediaire certificaten desgewenst downloaden.

6.1.6 Implementatie van services

Het Digipoort-koppelvlak specificeert een aantal services voor de gegevensuitwisseling tussen bedrijf en Digipoort.

Er wordt een onderscheid gemaakt tussen services voor bedrijven, services voor overheden en interne services.

Figuur 5 geeft een overzicht van de services onder versie 1.2 van het koppelvlak:



Figuur 5: overzicht Digipoort-services (getoond worden de services onder koppelvlak 1.2)

Als bedrijf heeft u vooral te maken met de services die Digipoort biedt voor bedrijven. Voor de huidige versie van het 'WUS voor Bedrijven'-koppelvlak zijn dat:

- Aanleverservice: de service op Digipoort waarmee u berichten kunt aanleveren voor aflevering aan een overheidsorganisatie;
- Statusinformatieservice: de service op Digipoort waarmee u kunt controleren of uw berichten ook daadwerkelijk zijn afgeleverd bij de overheidsorganisatie. Deze service dient u altijd in combinatie met de Aanleverservice te implementeren;
- Afleverservice: de service op uw adapter waarop Digipoort berichten kan afleveren die voor uw bedrijf bestemd zijn;
- Ophaalservice: de service waarmee u berichten die voor uw bedrijf bestemd zijn kunt ophalen bij Digipoort. Deze service wordt **niet** gebruikt voor DigiInkoop/E-Factureren.

De details van deze services zijn apart beschreven in een Servicebeschrijving. Deze beschrijvingen zijn te vinden in het zip-bestand ("Laatste stabiele versie") op https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-bedrijven/.

Wilt u als bedrijf berichten versturen aan een overheidsorganisatie, zoals e-facturen, dan dient u software te implementeren waarmee u deze berichten kunt aanleveren aan de aanleverservice en waarmee u tevens de statusinformatieservice kunt raadplegen. De aanleverservice en de statusinformatieservice dient u altijd in combinatie te implementeren.

Controleren verzending

Als verzender bent u er verantwoordelijk voor het bericht conform de koppelvlakspecificaties bij Digipoort aan te leveren en vervolgens de status te monitoren totdat u kunt vaststellen dat het bericht succesvol is afgeleverd bij de uiteindelijke ontvanger. Digipoort biedt betrouwbare aflevering, wat betekent dat Digipoort een aangeleverd bericht aflevert bij de ontvanger of aangeeft waarom het bericht niet afgeleverd kon worden.

Uw dient daarom na het aanleveren van het bericht aan de aanleverservice periodiek te controleren of het bericht succesvol is afgeleverd door Digipoort. Dit doet u met de Statusinformatieservice. Het advies is hiervoor een monitor te implementeren die uitzonderingen snel signaleert, zodat u hier op kunt handelen.

In de koppelvlakspecificaties is een document opgenomen over de statussen van Digipoort. Hierin staat beschreven welke actie u dient te ondernemen bij iedere uitzonderingssituatie.

Wilt u als bedrijf berichten ontvangen van een overheidsorganisatie, zoals bestellingen, dan dient u de afleverservice in uw software, zodat Digipoort berichten bij u kan afleveren.

Controleren op dubbele berichten

Het is mogelijk dat u vanuit Digipoort dubbele berichten ontvangt. Hier dient u als ontvanger alert op te zijn en maatregelen voor te nemen. Er kan namelijk een probleem optreden in het verzendproces waardoor Digipoort of de verzender zelf een herzending start. Hierdoor kunt u bijvoorbeeld dezelfde bestelling twee keer binnen krijgen. Dit kan zowel in een identieke envelop (herzending Digipoort) als in een aparte envelop (herzending verzender).

Het advies is de inhoudelijke berichten te controleren en waar nodig te ontdubbelen. Dit kan in de adapter met Digipoort of in het bedrijfssysteem dat de berichten uiteindelijk verwerkt.

6.1.7 Services implementeren

Een service is in wezen een gestandaardiseerde interface naar een achterliggend systeem. Middels de service is het mogelijk om op gestandaardiseerde wijze gegevens uit te wisselen tussen systemen. Het koppelvlak 'WUS voor Bedrijven' maakt gebruik van zogenoemde webservices. De gegevens die met de service kunnen worden uitgewisseld worden beschreven in een XML-document dat WSDL wordt genoemd.

Wanneer uw bedrijf zo'n service wil gebruiken (ook wel 'consumeren' genoemd) moet uw software zijn ingericht voor berichtenverkeer met de service. Met andere woorden, de service moet worden geïmplementeerd binnen uw software. De WSDL vormt daarbij de leidraad of het contract op basis waarvan deze implementatie moet plaatsvinden. De software, middels welke de services (ofwel het koppelvlak) worden geïmplementeerd, wordt ook wel 'adapter' genoemd.

6.1.8 WSDL en XSD (transportspecificatie)

Een webservice wordt technisch beschreven in een WSDL-document. Dit document beschrijft onder meer de berichten die door de service kunnen

worden ontvangen, het adres waarnaar de berichten moeten worden verstuurd en beveiligingsmaatregelen waaraan moet worden voldaan. De WSDL wordt daarom ook wel 'servicecontract' genoemd.

Webservices wisselen gegevens uit in de vorm van zogenoemde SOAP-berichten, waarvan de structuur is gespecificeerd in een XSD (XML Schema) waarnaar in de WSDL wordt verwezen. De feitelijke inhoudelijke gegevens (e-factuur, etc.) zijn zelf als XML-document opgenomen in het SOAP-bericht.
WSDL is een internationaal geaccepteerde standaard. Hierbinnen kan weer van een aantal gerelateerde standaarden gebruik worden gemaakt. Het WUS-koppelvlak maakt expliciet gebruik van twee van deze standaarden: WS-Addressing en WS-Security. Een en ander wordt in meer detail beschreven in de *Koppelvlakbeschrijving WUS voor bedrijven*.

Voor de services die berichtenverkeer van bedrijf naar Digipoort mogelijk maken (bijv. Aanleverservice, Statusinformatieservice) moet door uw bedrijf een 'aanroep' van de service worden geïmplementeerd. Voor de services die berichtenverkeer vanuit Digipoort naar het bedrijf mogelijk maken (bijv. Afleverservice) geldt dat de webservice zelf binnen uw bedrijf moet worden geïmplementeerd. Dit moet gebeuren op basis van de WSDL zoals die binnen de koppelvlakdocumentatie wordt aangeboden.

De koppelvlakdocumentatie bevat de volgende documenten:

- Koppelvlakbeschrijving;
- Overzicht van fouten en statussen (teruggegeven door Digipoort);
- Servicebeschrijvingen van alle services onder het koppelvlak;
- WSDL- en XSD (preproductie en productie)
- Voorbeelden van request- en responseberichten (SOAP-berichten).

6.1.9 Berichtstroomspecificaties

De services die door het koppelvlak 'WUS voor Bedrijven' worden geboden, zijn generiek van aard. Ze worden niet alleen voor DigiInkoop gebruikt, maar ook voor andere processen. De berichten die middels deze services worden uitgewisseld, zijn opgebouwd uit verplichte en optionele elementen. De specificatie van deze berichten is vastgelegd in een (generieke) XSD.

Vanuit een specifiek proces (ook 'berichtstroom' genoemd) kunnen echter aanvullende (specifieke) eisen worden gesteld. Als gevolg hiervan kan een optioneel element binnen een specifieke berichtstroom toch verplicht worden. Ook kunnen aan elementen specifieke eisen worden gesteld met betrekking tot de waarde die aan het element kan of moet worden toegekend. Dergelijke aanvullende eisen zijn van toepassing op de Aanleverservice.

Deze aanvullende eisen kunnen niet worden vastgelegd in de XSD, die immers generiek van aard is. De eisen staan daarom beschreven in een aparte berichtstroomspecificatie. In dit document staat beschreven welke elementen verplicht zijn en welke waarden de aanbieder moet gebruiken om de Aanleverservice goed aan te spreken.

- Documentatie: *Toelichting Digipoort koppelvlakspecificaties bedrijven:* https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-bedrijven/

Digipoort en berichtverwerking

Berichten die aan Digipoort worden aangeboden worden eerst door Digipoort gevalideerd voordat zij kunnen worden doorgezet voor verdere verwerking.

Validatie vindt plaats in twee stappen. Ten eerste worden de gegevens die zijn opgenomen in de envelop gevalideerd: zijn bijvoorbeeld identificatienummers en berichtsoort gevuld volgens het juiste 'format'?

Na een succesvolle validatie van de envelopgegevens wordt het inhoudelijk bericht (factuur, bestelling, etc.) gevalideerd. De inhoud is 'Base 64'-gecodeerd en dient eerst door Digipoort te worden gedecodeerd. Na succesvolle validatie wordt de inhoud opnieuw 'Base 64'-gecodeerd en wordt het bericht door Digipoort getransformeerd conform het koppelvlak met de ontvangende partij en bij deze partij afgeleverd.

Een 'Aflevering' wordt door Digipoort pas als succesvol beschouwd indien de ontvangende partij de verwachte afleverrespons terug heeft gestuurd. Indien een bericht niet direct succesvol kan worden afgeleverd, blijft Digipoort gedurende een vastgestelde periode proberen het bericht alsnog af te leveren. Indien succes ook na herhaald aanbieden uitblijft, wordt een fout op afleveren vastgesteld. De beoogde ontvanger ontvangt hierover een mail van Digipoort.

Elke Digipoort-actie resulteert in een bijbehorende status of, in geval van fouten, foutmelding. Statussen en foutmeldingen zijn door de aanleverende partij op te vragen via de Statusinformatieservice.

6.1.10 Testberichten (inhoudelijk)

In de documentatiesets van UBL en HR-XML zijn voorbeelden te vinden van inhoudelijke berichten die als inhoudelijk testbericht kunnen worden opgenomen in het SOAP-bericht. Het inhoudelijk bericht moet 'Base64'-gecodeerd worden opgenomen in het SOAP-bericht.

6.2 Technische test (services)

Alvorens te testen tegen Digipoort (stap 5) is het zaak om zelf een technische test van de service-implementaties uit te voeren, aangezien vanuit Digipoort-support slechts beperkte technische feedback mogelijk is. Tools als SOAP-UI kunnen helpen voor het testen van service-implementaties.

Aandachtspunten bij implementatie en test:

- WS-Addressing (zijn de verplichte Addressing-elementen correct in de SOAP-berichten opgenomen?);
- WS-Security (worden alle verplichte elementen in een uitgaand bericht correct ondertekend; kan de digitale handtekening onder een binnenkomend bericht correct worden geverifieerd?;
- kunnen voor alle geïmplementeerde services alle bijbehorende berichten (requests) correct worden gegenereerd en de responses correct worden verwerkt?

NB: het gaat in deze stap in de eerste plaats om het testen van het koppelvlak en nog niet om het testen van de inhoudelijke berichten die in de SOAP-berichten worden opgenomen. Desgewenst kunnen berichten uit de UBL- of HR-XML-documentatiesets als voorbeeld in het SOAP-bericht worden opgenomen.

6.3 Mijlpaal: software voor aansluiting gereed

Wanneer certificate stores correct zijn ingericht en alle benodigde services correct zijn geïmplementeerd, is de mijlpaal bereikt. In de volgende stap wordt de implementatie van het koppelvlak getest tegen Digipoort. Na succesvolle afronding van deze test kan vervolgens een ketentest worden uitgevoerd met een ketenpartner (overheidsorganisatie met wie berichten worden uitgewisseld).

7 Stap 4: inhoudelijk bericht genereren/verwerken

In deze stap kijken we naar het feitelijke inhoudelijke bericht (bijv. e-factuur, orderbevestiging, etc.) dat door het bedrijf via Digipoort aan een overheidsorganisatie wordt verzonden of via Digipoort vanuit een overheidsorganisatie wordt ontvangen.

Stap 4 kent een aantal aparte handelingen, die in onderstaande paragrafen verder worden toegelicht.

7.1.1 Bepalen welke berichten gegenereerd/verwerkt moeten kunnen worden

Inhoudelijke berichten worden opgemaakt conform de UBL-standaard of, wanneer het de inhuur van tijdelijk personeel betreft, conform de HR-XML-standaard. Voor meer informatie over deze standaarden, waaronder de beschikbare documentatie,zie

- UBL: https://www.logius.nl/ondersteuning/gegevensuitwisseling/ubl-ohnl/.
- HRXML: https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl/

Digipoort onderscheidt een aantal verschillende berichtsoorten, die gekoppeld zijn aan specifieke 'processen' die onder Digipoort worden onderkend. In de Implementatiewijzer bij de verschillende versies van de berichtenstandaarden zijn de processen met de bijbehorende berichtsoorten en berichttypen beschreven.

Stem met uw ketenpartner af welke stromen gewenst/geëist zijn. In het geval van DigiInkoop wordt vaak begonnen met een beperkt aantal berichtsoorten en wordt dit aantal in een volgende fase uitgebreid.

7.1.2 Berichten kunnen genereren en verwerken

De gegevens die in het inhoudelijk bericht worden opgenomen, zullen in de regel worden aangeleverd vanuit uw financieel- of ordersysteem. Sommige pakketten bieden 'out-of-the-box'-ondersteuning voor de vertaling naar het vereiste berichtenformat; in andere gevallen is maatwerksoftware benodigd. Na de transformatie moet het bericht worden 'opgepakt' door de software die zorgt voor de aanroep van Digipoort's Aanleverservice (de 'adapter'-software). Een correct aangeleverd bericht wordt eerst door Digipoort gevalideerd; alleen inhoudelijk correcte berichten worden afgeleverd bij de beoogde ontvanger (in andere gevallen ontvangt de afzender een foutmelding).

Omgekeerd moeten door Digipoort aangeleverde berichten correct kunnen worden verwerkt door uw ontvangende software (adapter) en achterliggend systeem. De adapter is tevens verantwoordelijk voor het verzenden van een responsbericht naar Digipoort (de werking hiervan zou reeds getest moeten zijn onder stap 3). Alleen na succesvolle ontvangst van een correct responsbericht wordt door Digipoort aan het proces een status 'succesvol' toegekend. Aan het responsbericht worden specifieke eisen gesteld met betrekking tot inhoud en beveiliging (zie voor details de betreffende servicebeschrijving).

7.1.3 Controle van berichten (validatie)

Hieronder wordt verstaan:

❖ controleren of het systeem valide inhoudelijke berichten genereert (conform de gebruikte UBL- en/of HR-XML-specificatie);

Gegenereerde inhoudelijke berichten kunnen 'off-line' worden gevalideerd met behulp van de 'Validatievoorziening' die Logius aanbiedt op http://nlvalidatie.nl/.
Opmerking: de site valideert alleen inhoudelijke berichten, geen SOAP-berichten (m.a.w.: de inhoudelijke berichten moeten worden aangeboden als zelfstandig XML-document, niet verpakt in een SOAP-envelop).

7.1.4 Interne gebruikersacceptatietest

Doel van de interne gebruikersacceptatietest is testen of de interne verwerking van de inhoudelijke berichten correct verloopt:

- controleren of het systeem binnenkomende valide berichten correct verwerkt, en
- controleren of het systeem binnenkomende invalide berichten correct afwijst (inclusief bijbehorende foutafhandeling).

Logius stelt geen specifieke eisen aan deze interne controle.

Wanneer verwerking niet kan plaats vinden omdat matching- en/of verwerkingsinformatie wordt gemist, zal tussen ontvangende- en verzendende partij afstemming plaats moeten vinden om dit te verhelpen.

7.2 Mijlpaal: interne berichtverwerking gereed

Na een succesvolle gebruikersacceptatietest is de mijlpaal bereikt.

8 Stap 5: technische test tegen Digipoort

Wanneer het koppelvlak correct is geïmplementeerd (stap 3) en ook de interne berichtenstroom voor elkaar is (stap 4), is het bedrijf in staat om berichten vanuit de eigen systemen via de 'adapter software' door te sturen naar Digipoort (en te ontvangen vanuit Digipoort). Correcte (gevalideerde) berichten worden door Digipoort afgeleverd bij de beoogde overheidspartij.

Voorafgaand aan de ketentest, waarbij het berichtenverkeer over de hele keten 'bedrijf – Digipoort – overheid' wordt getest, wordt een technische test uitgevoerd. Hierbij wordt gecontroleerd of het koppelvlak correct is geïmplementeerd en succesvol berichtenverkeer met Digipoort mogelijk is.

De technische gegevens die zijn benodigd voor de configuratie van Digipoort voor uw aansluiting worden middels een formulier aan de het aansluitteam verstrekt (zie de volgende paragraaf).

8.1 Aansluitformulier Technische Gegevens

Voor de configuratie van Digipoort in het geval van DigiInkoop voor het uitwisselen van berichten met uw bedrijf, wordt gebruik gemaakt van het *Aansluitformulier Technische Gegevens*. Dit formulier verkrijgt u na aanmelding van uw aansluiting vanuit ons aansluitteam.

In dit formulier kunt u de volgende gegevens invullen:

- Contactgegevens bedrijf en technisch contactpersoon;
- Berichtsoorten waarvan gebruik gaat worden gemaakt;
- Technische gegevens m.b.t. de preproductieomgeving (o.a. netwerkadressen, endpoint voor communicatie vanuit Digipoort), en
- Technische gegevens m.b.t. de productieomgeving.

NB: indien er alleen sprake is van het sturen van e-facturen naar Digipoort, hoeven niet alle technische gegevens te worden aangeleverd.

8.2 Connectiviteitstest

Om berichten uit te kunnen wisselen met Digipoort is het zaak dat er een dubbelzijdig beveiligde verbinding tussen bedrijf en Digipoort wordt opgezet (zie paragraaf 6.1.1). De hiertoe benodigde inrichting (met name het installeren van de benodigde certificaten) is in de voorgaande stappen gerealiseerd en kan nu tegen Digipoort worden getest.

Hier wordt dus onder andere bekeken of de firewalls aan beide kanten het verkeer toelaten en geverifieerd dat de certificate stores aan beide zijden correct zijn ingericht.

De connectiviteitstest kan succesvol worden genoemd als aan het volgende is voldaan:

- het bedrijf kan netwerkverbinding maken met Digipoort (preproductie-endpoint) op poort 443, en
- Digipoort kan netwerkverbinding maken met het bedrijf (preproductie-endpoint) op poort 443.

8.3 Test services (goed/foutstromen)

De service-implementaties die onder stap 3 zijn ontwikkeld, kunnen nu worden getest tegen Digipoort. Hierbij wordt een onderscheid gemaakt tussen het testen van de 'berichtenvelop' (zoals die onder het WUS-koppelvlak is gespecificeerd) en het testen van het inhoudelijke bericht dat hierin wordt meegestuurd (de e-factuur, inkooporder, etc.).

8.3.1 Testen koppelvlak

Vanuit de ontwikkelde software worden berichten naar Digipoort gestuurd en vice versa. Hierbij wordt gekeken of de berichten voldoen aan de koppelvlakspecificaties. Speciaal aandachtspunt hierbij is de correcte digitale ondertekening van de berichten.

Afleverresponse

Digipoort kan berichten afleveren bij een bedrijf indien dat bedrijf de Afleverservice heeft geïmplementeerd. Indien een bericht correct wordt afgeleverd, dient het bedrijf een Afleverresponse aan Digipoort terug te geven.

In de praktijk is gebleken dat het implementeren van deze Afleverresponse vaak technische ondersteuning behoeft, met name wanneer de verstuurde Afleverresponse door Digipoort wordt afgekeurd. Uw bedrijf kan voor deze ondersteuning een beroep doen op het aansluitteam.

Fouten en statussen die door Digipoort kunnen worden teruggegeven, zijn terug te vinden in het volgende document:

- *Documentatie: Foutmeldingen en statusmeldingen Digipoort*, te vinden in het zip-bestand ("Laatste stabiele versie") op https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-bedrijven/.

8.3.2 Testen inhoudelijke berichten

Wanneer is geverifieerd dat het koppelvlak conform specificaties is geïmplementeerd, volgen de tests van de inhoudelijke berichten. Het is hierbij zaak om te verifiëren dat valide berichten correct worden verstuurd naar Digipoort en dat vanuit Digipoort ontvangen berichten correct kunnen worden verwerkt. Tevens moet worden getest dat berichten waarin fouten worden geconstateerd op correcte wijze worden afgevangen (foutafhandeling is dan correct in de software geïmplementeerd).

8.4 Mijlpaal: technische test gereed

Wanneer van alle services is geconstateerd dat ze correct werken (correcte request- en responseberichten, correcte foutafhandeling), is de mijlpaal bereikt. Nu kan worden gestart met de ketentest over de preproductieverbinding (stap 6).

9 Stap 6: ketentest (preproductie)

In de vorige stap is het koppelvlak technisch getest. Een succesvolle test betekent dat alle geïmplementeerde services operationeel zijn bevonden en succesvol berichten kunnen verzenden naar en/of ontvangen vanuit Digipoort.

De functionaliteit moet uiteraard ook zorgvuldig worden getest binnen een opstelling waaraan alle betrokken partijen deelnemen. De stap 'ketentest' beschrijft de activiteiten die daarvoor moeten worden uitgevoerd.

Het doel van deze stap is: het valideren van het berichtenverkeer over de hele keten. Bijvoorbeeld: kan uw financieel systeem e-facturen genereren die via Digipoort bij de beoogde overheidsorganisatie kunnen worden afgeleverd en hier succesvol worden verwerkt?

Om de ketentest uit te kunnen voeren, moet aan een aantal voorwaarden zijn voldaan:

1. de netwerkverbinding met Digipoort is geregeld;
2. alle benodigde services zijn correct geïmplementeerd;
3. alle certificaten/sleutels zijn correct 'geïnstalleerd';
4. Voor DigiInkoop moet het 'Aansluitformulier Technische Gegevens' zijn aangeleverd en Digipoort geconfigureerd;
5. afspraken met de ketenpartner (overheid) zijn gemaakt.

Voorwaarden 1, 2, 3 en 4 zijn al ingevuld onder stap 2, 3 of 4 en getest onder stap 5. Voorwaarde 5 wordt onder de huidige stap ingevuld.

9.1 Uitvoeren ketentest (preproductie)

De ketentest wordt uitgevoerd in overleg met de overheidsorganisatie die als ketenpartner fungeert. De rol van Logius is hier beperkt tot technische ondersteuning met betrekking tot Digipoort; de inhoudelijke afstemming van de berichten ligt in de eerste plaats bij de ketenpartners zelf.

Binnen de ketentest ligt de focus vooral op de inhoudelijke berichten: zijn de partners in staat om elkaars berichten op correcte wijze te verwerken?

Een succesvol afgesloten ketentest maakt de weg vrij naar de laatste stap in het aansluittraject, inproductiename.

Load- en performancetest

Aan de preproductieomgeving worden niet dezelfde eisen gesteld met betrekking tot o.a. performance en schaalbaarheid als aan de productieomgeving. De preproductieomgeving is dan ook niet geschikt voor het uitvoeren van load- en performancetests.

9.2 Mijlpaal: aansluiting in preproductie afgerond

Wanneer Logius zich akkoord heeft verklaard met de resultaten zoals u die heeft gerapporteerd is de aansluiting op preproductie een feit.

10 Stap 7: productiegang

Wanneer de ketentest in stap 6 succesvol is uitgevoerd (de resultaten zijn dan door alle betrokken partijen geaccordeerd: bedrijf, Logius en ketenpartner) kan een feitelijke productiegang worden ingepland.

De activiteiten die onder stap 6 zijn uitgevoerd, worden daarbij nogmaals herhaald om te controleren of de productieverbinding aan alle gestelde eisen voldoet.

10.1 Aansluitformulier Technische Gegevens (productie)

In geval van DigiInkoop kunt u het onder stap 5 reeds gedeeltelijk ingevulde Aansluitformulier aanvullen met de technische gegevens behorend bij de productie- omgeving voor zover u dat niet in eerste instantie heeft gedaan. Op basis van deze gegevens wordt de configuratie van Digipoort aangevuld voor verkeer over de productieverbinding.

10.2 Connectiviteitstest

Ook voor de productieverbinding is het zaak om eerst een connectiviteitstest uit te voeren, om te controleren of het bedrijf succesvol een beveiligde verbinding kan opzetten naar het productieadres van Digipoort en vice versa.

De connectiviteitstest kan succesvol worden genoemd als aan het volgende is voldaan:

- het bedrijf kan netwerkverbinding maken met Digipoort (productie-endpoint) op poort 443, en
- Digipoort kan netwerkverbinding maken met het bedrijf (productie-endpoint) op poort 443.

10.3 Test services (goed/foutstromen)

De service-implementaties zijn reeds getest onder de preproductieverbinding (stap 6). In het algemeen volstaat het hier om de tests nogmaals kort te doorlopen, zodat er absolute zekerheid bestaat dat de services ook in deze omgeving/via deze verbinding het juiste resultaat leveren.

10.4 Uitvoeren ketentest of gecontroleerde productierun (productie)

In overleg met uw ketenpartij kunt u verder de in productiename inrichten met bijvoorbeeld, nog een ketentest over de productieverbinding. Aangezien het hier de productieomgeving betreft, dient u er zorg voor te dragen dat de testberichten niet tot verstoringen leiden in zowel uw productiesystemen als in de productiesystemen van de ketenpartner. Stem dit goed af alvorens 'test'-berichten in te schieten!

Bij de eerste productierun levert uw bedrijf daadwerkelijke bijv. facturen aan over de productieverbinding voor verwerking door de overheidsorganisatie. Hierbij wordt nogmaals nadrukkelijk gekeken naar correcte verwerking van de gegevens. Het volume van de berichtenstroom

tijdens deze run is representatief voor het volume dat tijdens reguliere berichtuitwisseling mag worden verwacht.

Na een correct uitgevoerde eerste productierun mag ervan worden uitgegaan dat de aansluiting volledig operationeel is.

10.5 Inbeheername

Wanneer de eerste productierun correct is uitgevoerd, is de aansluiting in feite gereed en kan deze door Logius in beheer worden genomen.

Uw bedrijf kan door Logius worden opgenomen in het overzicht van aangesloten partijen op de Logius website.

DigiInkoop partijen hebben nog recht op twee weken nazorg. Het aansluitteam blijft gedurende die twee weken beschikbaar om te assisteren bij het oplossen van issues die zich onverhoopt voordoen.

Na afloop van deze twee weken gaat de beheerfase formeel in.

10.6 Mijlpaal: aansluiting in productie

De afronding van deze fase representeert het voltooien van de aansluiting van uw bedrijf op Digipoort.

Bijlage 1: certificaten en certificaathiërarchieën

Wat is een certificaathiërarchie en waarvoor wordt deze gebruikt?

Een certificaat is een elektronisch document dat wordt gebruikt voor het vaststellen van een digitale identiteit. Middels een certificaat wordt gegarandeerd dat een bepaalde *publieke sleutel* daadwerkelijk behoort bij de identiteit aan wie de sleutel is toegekend. De garantie is gelegen in het feit dat het certificaat is ondertekend door een *Certification Service Provider (CSP),* een partij die formeel certificaten verstrekt waarvoor een *Certification Authority CA)* ultiem garant staat.

Het certificaat kan worden gebruikt voor onder meer identificatie- en authenticatiedoeleinden. Een certificaat is in beginsel publiek beschikbaar. Middels de publieke sleutel in het certificaat kan bijvoorbeeld worden geverifieerd of een (TLS-)verbinding is gecodeerd met de bijbehorende *private sleutel*. Publieke- en private sleutel zijn onlosmakelijk met elkaar verbonden, maar de private sleutel wordt, in tegenstelling tot de publieke, zorgvuldig geheim gehouden.

Certificaten die door een CSP worden verstrekt, worden gegarandeerd door de CSP, oftewel: de CSP staat garant voor de identiteit die door het certificaat wordt gerepresenteerd.

Een certificaat wordt geverifieerd middels een *chain of trust*. Aan de basis hiervan staat het *stamcertificaat* of *root certificate*. Het stamcertificaat vormt het ankerpunt voor een hiërarchie van certificaten. Het eerste certificaat onder het stamcertificaat, het *domeincertificaat*, is getekend met de geheime private sleutel van het stamcertificaat. Dit kan worden geverifieerd middels de bijbehorende publieke sleutel, die is opgenomen in het stamcertificaat zelf.

Ieder onderliggend certificaat in de hiërarchie is steeds getekend met de sleutel uit het bovenliggende certificaat. Een certificaat kan dus steeds worden geverifieerd met behulp van het bovenliggende certificaat. De betrouwbaarheid van een door een CSP uitgegeven certificaat is uiteindelijk terug te voeren op het stamcertificaat. De partij die dit stamcertificaat heeft uitgegeven geldt als de ultieme Certification Authority. Alle onderliggende verstrekkers, inclusief de CSP, kunnen worden vertrouwd op basis van het vertrouwen in de Certificate Authority. In het geval van PKIoverheid-certificaten vervult de Staat der Nederlanden deze rol.

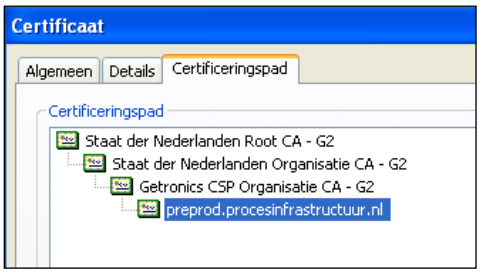
Certificate stores
Om deze verificatie mogelijk te maken, wordt de certificaathiërarchie (stamcertificaat en tussenliggende certificaten) opgenomen in een zogenoemde *certificate trust store*. Een certificaat van een partij die zich hiermee identificeert, kan dan worden geverifieerd tegen de hiërarchie in de trust store (met het stamcertificaat voor 'ultieme verificatie').

Certificate stores die op servers worden ingericht, moeten veelal expliciet worden voorzien van gebruikte certificaathiërarchieën, terwijl die in bijvoorbeeld browsers vaak standaard zijn opgenomen.

Ook het eigen certificaat (het certificaat dat wordt gebruikt voor eigen identificatie of ondertekening van berichten) moet in een certificate store worden opgenomen: de *certificate key store*. Beter gezegd: de private sleutel die hoort bij het certificaat moet in de key store worden opgenomen. Het is immers de private sleutel waarmee wordt ondertekend, etc.; de publieke sleutel in het certificaat dient ter verificatie door de communicatiepartner. Deze key store dient uiteraard afdoende te worden beveiligd, private sleutels dienen immers voor de buitenwereld strikt geheim gehouden te worden.

De hiërarchie van PKIoverheid-certificaten

Ook PKIoverheid-certificaten kennen een certificaathiërarchie. De figuur hiernaast toont een voorbeeld van deze hiërarchie.



In de figuur is te zien dat het voor 'preprod-dgp.procesinfrastructuur.nl' uitgegeven PKIoverheid-certificaat een bovenliggende hiërarchie kent, waarin drie certificaten zijn opgenomen:

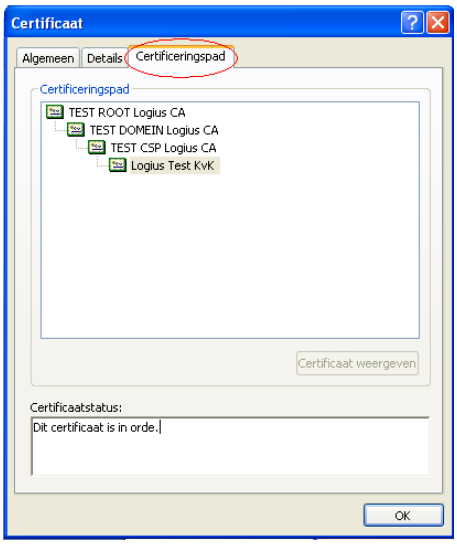
- 'Getronics CSP Organisatie CA – G2'-certificaat;
- 'Staat der Nederlanden Organisatie CA – G2'-certificaat, en
- 'Staat der Nederlanden Root CA – G2'-certificaat.

Het laatstgenoemde certificaat is het stamcertificaat. De overige twee zijn voorbeeldn van de tussenliggende 'domein-' en 'CSP'-certificaten

Alle PKIoverheids-certificaten kennen een dergelijke hiërarchie. *Opmerking:* het 'CSP'-certificaat wordt uitgegeven door een specifieke CSP. Het certificaat zoals dat in de hiërarchie van uw certificaat wordt getoond, kan afwijken van bovenstaand voorbeeld.

Testcertificaten

De door Logius uitgegeven testcertificaten kennen een vergelijkbare hiërarchie. Een voorbeeld wordt hiernaast weergegeven.



Het grote verschil met PKIoverheid-certificaten is, dat het 'stamcertificaat' in dit geval niet is uitgegeven door een 'echte' CA. Het certificaat en de gebruikte hiërarchie bieden dus geen feitelijke garantie voor de identiteit die door het certificaat wordt gerepresenteerd. Ze kunnen daarom uitsluitend voor testdoeleinden worden gebruikt. Wel is de technologie die wordt gebruikt voor het 'verifiëren' van deze certificaten dezelfde als in het geval van PKIoverheid-certificaten. Daarom kunnen met testcertificaten vergelijkbare beveiligingsmaatregelen worden ingericht, zoals het opzetten van een dubbelzijdige TLS-verbinding of het digitaal ondertekenen van berichten.

Om testcertificaten te kunnen gebruiken moet, analoog aan wat hierboven voor PKIoverheid-certificaten is beschreven, de bijbehorende testhiërarchie beschikbaar worden gemaakt. De hiërarchie moet worden opgenomen in de *certificate trust store*. De private sleutel van het eigen certificaat moet worden opgenomen in de *certificate key store*.