Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

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

Versie 1.6

Datum 9 maart 2020
Status Definitief

Colofon

Projectnaam	DigiInkoop
Versienummer	1.6
Contactpersoon	Servicecentrum Logius
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl
Bijlage(n)	1

Inhoud

Lijst van gebruikte afkortingen

CPA	XML-document om een ebMS-adapter te configureren voor berichtenverkeer met een specifieke partner. Voluit: Collaboration Protocol Agreement.
CSP	Certification Service Provider (ook wel Certificate Service Provider genoemd): organisatie die namens een Certification Authority certificaten verstrekt.
ebMS	ebXML Messaging Service, het protocol waarop de Digikoppeling Koppelvlakstandaard ebMS is gebaseerd. Via het Digikoppeling ebMS-koppelvlak vindt asynchrone communicatie met Digipoort plaats. Dit type verkeer wordt ook wel *melding* of *transactie* genoemd.
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 is de op XML gebaseerde standaard voor het versturen van elektronische business documenten, zoals offertes, orders en facturen.
WUS	De op webservices gebaseerde Digikoppeling Koppelvlakstandaard voor overheden. Via het Digikoppeling WUS-koppelvlak vindt synchrone (request-response) communicatie met Digipoort plaats. Dit type verkeer wordt ook wel *bevraging* genoemd.

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 *overheden*. Hieronder verstaan wij zowel overheden die zelf inkoop- en/of factuurgegevens met het bedrijfsleven willen uitwisselen als 'shared services organisaties' of ICT-leveranciers 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 (van offerteaanvraag tot aan factuur) (DigiInkoop).

Het in deze handleiding beschreven aansluitproces richt zich op het inrichten van het *berichtenverkeer tussen overheid en Digipoort*. Het verkeer tussen leveranciers en Digipoort via een factuurportaal, een intermediair of een directe koppeling blijft hier buiten beschouwing. Voor **bedrijven** is een aparte Aansluithandleiding beschikbaar (zie: https://www.logius.nl/ondersteuning/e-factureren-voor-overheden-via-digipoort/)

Deze handleiding geeft u een totaaloverzicht van alle stappen die bij het aansluiten komen kijken. Een succesvolle aansluiting betekent dat uw organisatie in staat is om berichten via Digipoort te ontvangen (E-facturatie) en te verzenden (DigiInkoop) en de status van de verzonden berichten op te halen.

Deze handleiding biedt een overzicht van de stappen die een overheidsorganisatie moet nemen om aan te sluiten op Digipoort. Bij elke stap is uitgelegd:

- waarom deze moet worden uitgevoerd;
- 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 kan worden geverifieerd.

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 op Digipoort bestaat uit de volgende stappen:

1. **Voorbereiding**: o.a. verzamelen van benodigde informatie (documentatie), bepalen van de impact op uw eigen organisatie, aanvragen van PKIoverheid-certificaat, aanmelden van de beoogde aansluiting bij Logius en planningsdocument invullen;
2. Inrichten **netwerkconnectiviteit**: ervoor zorgen dat de overheidsorganisatie via het netwerk (Diginetwerk of internet) verbinding kan maken met Digipoort;
3. Inrichten **koppelvlak**: implementeren van de benodigde services (conform de Digikoppeling-standaarden) 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 of 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. **Ketentest in preproductie**: uitvoeren ketentest met de beoogde ketenpartner (bedrijf) over de preproductieverbinding;
7. **Productiegang**: 'testrun' over de productieverbinding met Digipoort, gevolgd door inproductiename van deaansluiting.

1.3 Doelgroep

Deze handleiding richt zich op overheidsorganisaties die zelf een aansluiting op Digipoort willen realiseren voor DigiInkoop/E-Factureren, of (overheden of leveranciers) die een dergelijke aansluiting voor andere overheidsorganisaties willen realiseren. In het laatste geval spreken we van *shared services organisaties*.

De handleiding richt zich daarbij in de eerste plaats op de projectleider die voor de organisatie 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 bedrijven is een aparte Aansluithandleiding voorhanden (zie https://www.logius.nl/ondersteuning/e-factureren-voor-leveranciers-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: servicecentrum@logius.nl.

1.6 Begeleiding bij aansluiten

Gedurende de voorbereiding is het Servicecentrum van Logius uw eerste aanspreekpunt. Tijdens het feitelijke aansluitproces wordt u vanuit Logius begeleidt door een aansluitcoördinator, die u tijdens de voorbereidingsfase toegewezen krijgt.

In geval van tussentijdse en aanvullende vragen kunt u contact opnemen met Servicecentrum Logius. Wij helpen u graag verder.

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:

Voor E-Factureren:

- https://www.logius.nl/ondersteuning/e-factureren-voor-overheden-via-digipoort/

Voor DigiInkoop:

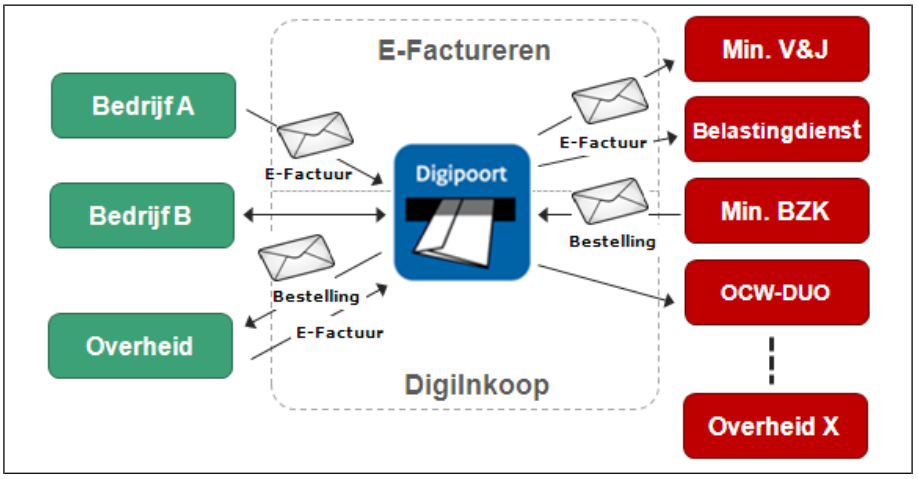
- https://www.logius.nl/ondersteuning/digiinkoop-voor-rijksdienst-via-digipoort/

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 offerte, maar ook een bestelling van een overheid bij een bedrijf of een afwijzing van een offerte.



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. In brede zin specificeert een koppelvlak alle afspraken van bedrijfsproces tot de fysieke netwerkverbinding (zie figuur 2 voor een overzicht).

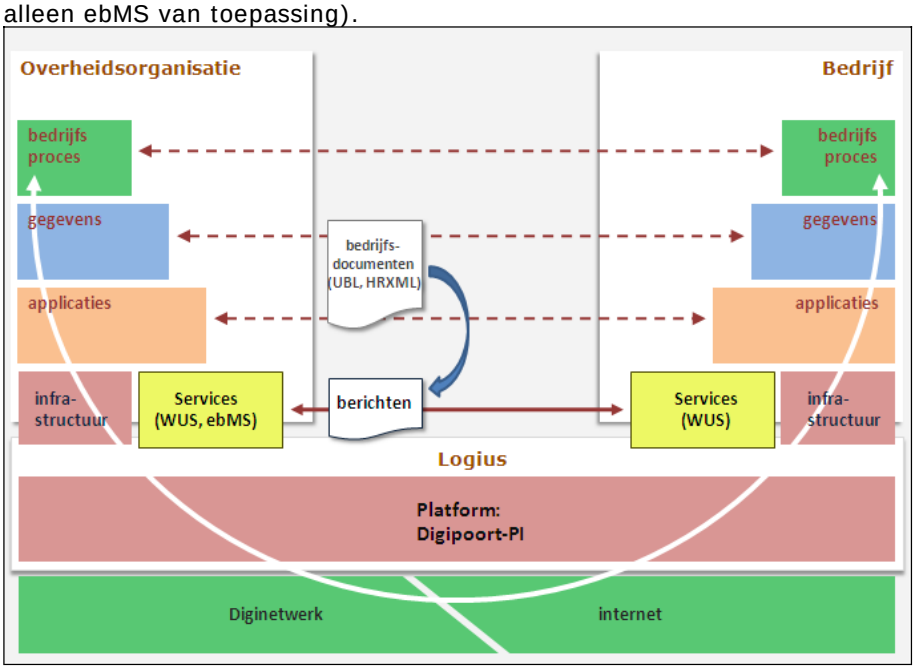
Logius/Digipoort levert koppelvlakspecificaties voor de samenstelling van berichten en het 'niveau' waarop deze berichten worden uitgewisseld (zie figuur 2). Bij dit 'niveau' gaat het om de specificaties van de services waarmee berichten worden uitgewisseld.

Daarnaast stelt Digipoort specifieke eisen aan de onderliggende netwerkverbinding.

Voor berichtuitwisseling biedt Digipoort verschillende koppelvlakken, voor bedrijven enerzijds en overheden anderzijds, waaronder FTP, SOAP, WUS en ebMS. Via deze koppelvlakken worden diverse berichtstromen van en

naar de overheid mogelijk gemaakt, zoals ziekmeldingen, statistiekberichten, facturen, bestellingen, etc.

Voor berichtenverkeer voor DigiInkoop moeten overheidsorganisaties gebruik maken van de koppelvlakken die zijn ingericht conform de Digikoppeling Koppelvlakstandaarden WUS en ebMS (op E-Factureren is alleen ebMS van toepassing).



Figuur 2: Digipoort koppelvlak t.b.v. DigiInkoop/E-Factureren

Digikoppeling Koppelvlakstandaarden WUS en ebMS

WUS en ebMS worden gebruikt voor respectievelijk bevragingen en meldingen (of transacties).

In het geval van bevragingen wordt direct een antwoord op de gestelde vraag verwacht. Op WUS gebaseerde webservices bieden standaard de gewenste functionaliteit voor dit uitwisselingspatroon.

In het geval van meldingen is er sprake van berichten waarop vaak niet direct een antwoord kan worden gegeven, omdat daarvoor aan de kant van de ontvanger eerst een (geautomatiseerd of handmatig uitgevoerd) proces plaats moet vinden. Om de verzender toch de zekerheid te verschaffen over correcte aflevering van het bericht, is het nodig om deze een ontvangstbevestiging te sturen (er wordt gegarandeerd dat een bericht *once-and-once-only* wordt afgeleverd). Deze functionaliteit wordt standaard geboden door het ebMS-protocol.

- *Documentatie en beschrijvingen*:
  WUS Koppelvlakstandaard, zie
  https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-overheden/
  ebMS Koppelvlakstandaard, zie
  https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-ebms-overheden/

2.1.2 Services

Ieder Digipoort-koppelvlak biedt meerdere services. In het geval van Digikoppeling WUS en ebMS gaat het om zogenoemde webservices, die voorzien in functionaliteit om elektronische berichten aan te leveren (bijvoorbeeld een bestelling gericht aan een leverancier) of elektronische berichten te ontvangen (bijvoorbeeld een offerte of een E-factuur).

Onder de koppelvlakken die voor DigiInkoop/E-Factureren aan overheidsorganisaties worden aangeboden, zijn services gespecificeerd als WUS-service of als ebMS-service. Implementatie van de service door de overheidspartij vindt dus plaats conform respectievelijk de WUS- of ebMS-koppelvlakspecificaties.

De services zijn generiek van opzet. Dat wil zeggen dat middels deze services inhoudelijk heel verschillende berichten kunnen worden verstuurd. Een overheidsorganisatie kan via dezelfde service bijvoorbeeld zowel offertes als facturen als bepaalde rapportages ontvangen. Een implementatie van deze services voor DigiInkoop kan in de toekomst dus mogelijk worden hergebruikt voor andere toepassingen die voor hun berichtenverkeer van dezelfde services gebruik maken.

Meer informatie over de services is te vinden in paragraaf 6.2.

- *Documentatie:* servicebeschrijvingen van de afzonderlijke services, te vinden onder:
  - WUS: https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-overheden/
  - ebMS: https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-ebms-overheden/

  De Servicebeschrijvingen zijn terug te vinden in het zip-bestand met de documentatie van WUS- resp. ebMS-services onder het kopje ‘Laatste stabiele versie’.

  De documenten zijn ook terug te vinden in het Digikoppeling Service Register onder de betreffende ebMS-of WUS-service.

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 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). 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’, ‘ebMS-berichten’) te vinden.

Op de inhoud zijn aparte afspraken van toepassing, vastgelegd in inhoudelijk-berichtspecificaties (UBL, HR-XML).

- *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; .xsd en schematron validatie. Er wordt binnen Digipoort alleen niet gevalideerd op de generieke codelijsten (landcodes, valuta, etc).

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 preproductie-omgeving van Digipoort en een versie die toegang biedt tot de productie-omgeving.

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 DigiInkoop leveranciers- en deelnemersportaal.

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

- De services parallel te ontwikkelen en te testen.
  - De statussen van met het Portaal ingeschoten berichten kunnen (mits hetzelfde certificaat wordt gebruikt) worden opgehaald met de System to System koppeling
  - Van de System to System ingeschoten berichten kan via het Portaal de statusinformatie worden uitgevraagd;
- Het kan in de ontwikkelfase worden gebruikt om testberichten aan te leveren (die door Digipoort bij de geadresseerde overheidsdeelnemer worden afgeleverd);
- Het kan worden gebruikt om de inhoudelijke berichten te testen. 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 bij de aansluitdocumentatie op de Logius website. 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 overheidsorganisatie elektronische berichten uitwisselen met bedrijven. In het geval van DigiInkoop gaat het bij deze berichten om gegevens rond elektronisch inkopen en/of factureren.

Binnen DigiInkoop/E-Factureren onderscheiden we de twee volgende mogelijkheden:

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

Optie 1 is beschikbaar voor alle overheden in Nederland. Optie 2 is nu alleen beschikbaar voor de rijksdienst.

Een succesvolle aansluiting betekent dat uw organisatie in staat is om de gegevens die horen bij de gekozen optie elektronisch te verzenden naar dan wel te ontvangen van een of meer bedrijven.

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 uw organisatie 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.

Berichtstromen kunnen resulteren in een geslaagde aflevering, maar er zijn ook foutsituaties mogelijk. Zijn systemen en organisatie in staat om hier effectief op te reageren?

Check bij Logius voor mogelijke ondersteuning bij het doorvoeren van de benodigde organisatieverandering. Er zijn hiervoor diverse hulpmiddelen beschikbaar.

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

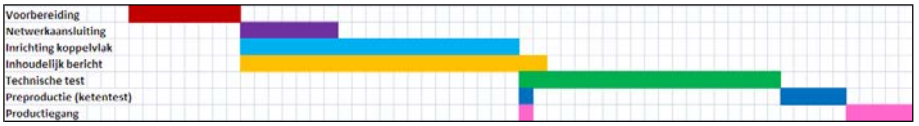
Alle handelingen zijn beschreven in het planningsdocument dat Logius voor aansluitingen heeft ontwikkeld. Deze handelingen zijn voorzien van een gemiddelde doorlooptijd, waarmee u ook een prognose kunt maken van het gehele aansluittraject.

Het planningsdocument is te vinden bij de andere aansluitdocumenten op de Logius website.

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 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 3: voorbeeld verloop doorlooptijd (relatief)

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

- beschikbare kennis binnen uw organisatie over uw systemen en over de gebruikte standaarden en technologie (zie ook paragraaf 4.2);
- Doorlooptijd als gevolg van zaken die ingekocht moeten worden door uw organisatie om de aansluiting te kunnen realiseren;
- Beschikbare aansluitcapaciteit bij Logius.

3.2 Documentatie

❖ U vindt alle documenten die u voor het aansluiten nodig heeft

voor E-Factureren onder:
https://www.logius.nl/ondersteuning/e-factureren-voor-overheden-via-digipoort/

voor DigiInkoop onder:
https://www.logius.nl/ondersteuning/digiinkoop-voor-rijksdienst-via-digipoort/

In de navolgende hoofdstukken worden de stappen van het aansluitproces beschreven. Wij hebben de volgende stappen gedefinieerd:

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, het afstemmen van de planning met Logius en het indienen van het aansluitformulier.

Logius verwacht van een overheidsorganisatie die wil aansluiten dat deze:

- de beoogde aansluiting via e-mail aanmeldt bij Servicecentrum Logius (servicecentrum@logius.nl);
- de voor het aansluiten benodigde informatie verzamelt en doorneemt;
- ervoor zorgt dat het beschikt over de benodigde technische expertise;
- een projectplan en planning, zie als input het document *Planning aansluiten Digipoort PI voor overheden voor DigiInkoop/E-Factureren*.
- De aansluiting met Logius afstemt

Logius zal ervoor zorgen dat het ingediende formulier en planningsdocument worden verwerkt. Zodra dit is gebeurd, krijgt u door Logius een aansluitcoördinator toegewezen die u tijdens het aansluitproces zal begeleiden.

De voorbereidende stappen zijn hieronder verder toegelicht.

4.1 Informatie verkrijgen

Op de Logius-website kunt u informatie vinden over Digipoort en DigiInkoop/E-Factureren. Ook is technische documentatie beschikbaar, waaronder achtergrondinformatie over Diginetwerk en Digikoppeling, 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 de organisatie beschikt over de benodigde technische expertise.

Ook deze handleiding kan worden gebruikt om een eerste overzicht te verkrijgen. Het advies is om de handleiding door te nemen voordat een mogelijk intakegesprek met Logius (zie paragraaf 4.3) plaatsvindt.

4.2 Technische expertise in huis halen

Om berichtenverkeer met Digipoort mogelijk te maken, moet een overheidsorganisatie een aantal services implementeren volgens de koppelvlakken Digikoppeling ebMS en (in het geval van DigiInkoop) Digikoppeling WUS. Beide koppelvlakken zijn ingericht op basis van

internationale standaarden voor routering en beveiliging van berichten. Om services conform dit koppelvlak te realiseren, is de nodige technische expertise vereist.

De uiteindelijke technische implementatie kan meer of minder complex zijn. Dit is onder meer afhankelijk van onderstaande punten:

1. Gaat het alleen om E-Factureren (ontvangen van elektronische facturen) of om DigiInkoop in bredere zin (waarbij ook andere berichtsoorten (bestelling, etc.) worden geïmplementeerd)? Indien alleen berichten worden *ontvangen*, zoals bij E-Factureren, volstaat implementatie van het ebMS-koppelvlak (Afleverservice). Indien ook berichten worden *verzonden* (aanleveren van bijv. bestellingen via de Aanleverservice), dient ook de Status-informatieservice te worden geïmplementeerd, en daarmee het WUS-koppelvlak;

2. Overheden kunnen ervoor kiezen om bij berichtenverkeer met Digipoort al dan niet gebruik te maken van digitale ondertekening van de berichten. Digitale ondertekening verhoogt het betrouwbaarheidsniveau van het berichtenverkeer, maar brengt ook additionele complexiteit met zich mee.

   Het advies is om alleen berichtondertekening te implementeren indien daar vanuit bijv. de eigen architectuur expliciet de noodzaak voor wordt aangegeven. In alle andere gevallen kan gebruik worden gemaakt van het profiel 'zonder ondertekening'. Beveiliging is in de regel afdoende gewaarborgd doordat gebruik wordt gemaakt van beveiliging op transportniveau (dubbelzijdig TLS/SSL) (Digikoppeling). Daarnaast kan gebruik worden gemaakt van verkeer via besloten overheidsnetwerken (Diginetwerk), waarmee naast extra beveiliging ook beschikbaarheid is gegarandeerd;

3. De Afleverservice kent een variant waarbij het volstaat om een ebMS-bevestigingsbericht (*acknowledgement*) terug te sturen en een oudere variant waarbij aanvullend een expliciet respons-bericht naar Digipoort moet worden teruggestuurd.

   De variant met expliciete respons is technisch wat lastiger te implementeren. Bovendien ondersteunen niet alle ebMS-adapters de mogelijkheid voor een expliciet responsbericht. Het advies is dan ook om de variant zonder expliciete afleverrespons te implementeren.

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

- ebMS (waaronder het gebruiken van zogenoemde CPA's);
- Beveiligd transport via dubbelzijdig TLS/SSL (denk hierbij aan het inrichten van de benodigde *certificate stores*);
- Berichtenstandaarden UBL en/of HR-XML: minimaal vereist is gedegen kennis van XML en XSD voor begrip van UBL/HR-XML.

Indien ook het WUS-koppelvlak moet worden geïmplementeerd (Statusinformatieservice):

- webservices-standaarden (o.a. SOAP, WSDL, WS-Addressing);

Indien is gekozen voor additionele beveiliging middels bericht-ondertekening:

- WS-Security/XML-DSig (digitaal ondertekenen van berichten en kunnen verwerken van ontvangen berichten die op hun beurt digitaal ondertekend zijn).

Niet alle overheidsorganisaties beschikken 'in huis' over de vereiste kennis en ervaring. In de markt zijn er verschillende leveranciers actief die de aansluiting voor uw organisatie kunnen uitvoeren of een deel van de werkzaamheden voor hun rekening kunnen nemen. Zie voor een overzicht de lijst met 'Intermediairs' op https://www.logius.nl/ondersteuning/gegevensuitwisseling/welke-leveranciers-doen-mee/ .

4.3 Intakegesprek met Logius

Indien uw organisatie wil aansluiten op Digipoort/DigiInkoop, kunt u via e-mail contact opnemen met Servicecentrum Logius. Het Servicecentrum kan in overleg met u een intakegesprek in met een DigiInkoop medewerker regelen. Tijdens dit gesprek komen de volgende zaken aan bod:

- Is er voldoende technische kennis beschikbaar? (Haalbaarheid doornemen resulterend in advies: aansluiting zelf realiseren of uitbesteden);
- Is de organisatie reeds aangesloten op Digipoort en zo niet, beschikt hij over het Aanvraagformulier Digipoort en is hij bekend met de Aansluitvoorwaarden?
- Is het Planningsdocument ingevuld?
- Wat is het verwachte volume (hoeveel berichten verwacht men te versturen per maand)?
- Zijn de verwachtingen helder (wat kan de klant van Logius verwachten en andersom)?
- Keuze: aansluiting zelf realiseren of uitbesteden aan een externe leverancier.

4.4 Aanvraagformulier Digipoort / E-Factureren

De dienst E-Factureren is beschikbaar voor alle overheidsorganisaties (DigiInkoop is alleen beschikbaar voor de Rijksdienst). Indien uw organisatie geen onderdeel van de Rijksdienst uitmaakt, is deze mogelijk nog niet aangesloten op Digipoort. Dit zal het geval zijn als de organisatie nog geen gebruik maakt van andere berichtstromen die via Digipoort worden aangeboden.

Voor aansluiting op E-Factureren dient u een aanvraagformulier in te dienen:

- *Aanvraagformulier aansluiting e-factureren voor overheden*, te vinden onder https://www.logius.nl/ondersteuning/digiinkoop-voor-rijksdienst-via-digipoort/ .

Op het Aanvraagformulier geeft u tevens aan dat u akkoord gaat met de Aansluitvoorwaarden Digikoppeling, Aansluitvoorwaarden Digipoort

(koppelvlakken SOAP, ebMS en WUS) en met het Addendum Aansluitvoorwaarden elektronisch factureren.

- *Aansluitvoorwaarden Digikoppeling*, te vinden onder https://www.logius.nl/diensten/digikoppeling/ (bijondersteuning)
- *Aansluitvoorwaarden Digipoort*, te vinden onder https://www.logius.nl/diensten/digipoort/
- Het Addendum voor E-Factureren is hier te vinden: https://www.logius.nl/ondersteuning/e-factureren-voor-overheden-via-digipoort/
- Voor als DigiNetwerk wordt gebruikt, dan zij de voorwaarden hiervoor te vinden bij: https://www.logius.nl/ondersteuning/diginetwerk/

Het Aanvraagformulier kunt u opsturen naar Servicecentrum Logius (zie de contactgegevens op pag. 2).

4.5 Aansluitformulier DigiInkoop

DigiInkoop is momenteel alleen beschikbaar voor de Rijksdienst. Als Rijksdienst-organisatie hoeft u geen apart aanvraagformulier voor DigiInkoop in te dienen.

Wel dient u na te gaan of uw organisatie reeds is aangemeld voor Digikoppeling. Is dat niet het geval, dan vindt u hier de benodigde informatie voor aanmelding:

- Aanmelden voor Digikoppeling: https://www.logius.nl/diensten/digikoppeling/

4.6 Projectplan

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

Het projectplan is enkel bedoeld als leidraad voor de organisatie zelf. Logius hoeft hierin geen inzage te hebben. Afstemming tussen overheidsdeelnemer en Logius vindt met name plaats op basis van het planningsdocument dat in de volgende paragraaf wordt toegelicht.

4.7 Planningsdocument

De planning wordt gebaseerd op het planningsdocument dat door de overheidsdeelnemer moet worden ingevuld, mogelijk in overleg met Logius (zie 4.3):

Planning aansluiten Digipoort voor overheden, te vinden onder

voor E-Factureren: https://www.logius.nl/ondersteuning/e-factureren-voor-overheden-via-digipoort/

voor DigiInkoop: https://www.logius.nl/ondersteuning/digiinkoop-voor-rijksdienst-via-digipoort/

In het planningsdocument zijn alle aansluithandelingen opgenomen en de partij die voor de betreffende handeling verantwoordelijk is (Logius of

overheidsdeelnemer). In het document is tevens een indicatie van de doorlooptijd per handeling aangegeven, alsmede de mogelijke afhankelijkheden die een handeling met andere handelingen heeft. Dit document kan u helpen met het opstellen van uw projectplan.

4.8 Start aansluittraject

Pas nadat het aanvraagformulier (indien benodigd) is ontvangen en er een goed plan van aanpak is, start voor Logius formeel het aansluittraject en zal een aansluitcoördinator worden toegewezen die u bij het verdere aansluittraject vanuit Logius begeleidt.

Het aansluittraject start in de regel met een gezamenlijk overleg tussen aansluitcoördinator, projectleider vanuit de klant en de persoon die voor de klant tijdens het traject als primair technisch aanspreekpunt fungeert. Tijdens deze 'kick-off' worden alle aansluitstappen doorlopen met het oog op de wederzijds uit te voeren werkzaamheden. U kunt tijdens dit overleg alle technisch-inhoudelijke vragen voorleggen.

4.9 Overzicht van deliverables

Aan het einde van deze stap levert u de volgende deliverables op:

In het geval van een aansluiting voor E-Factureren:

1. Ingevuld planningsdocument: *Planning aansluiten Digipoort PI voor overheden voor DigiInkoop/E-Factureren*;
2. *Aanvraagformulier aansluiting e-factureren voor Overheden*.

In het geval van een aansluiting voor DigiInkoop:

1. Ingevuld planningsdocument: *Planning aansluiten Digipoort PI voor overheden voor DigiInkoop/E-Factureren*.

5 Stap 2: inrichten netwerkconnectiviteit

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

5.1 Mogelijkheden voor netwerkverbinding

Overheidsorganisaties sluiten bij voorkeur op Digipoort aan via Diginetwerk. Aangezien er onder DigiInkoop/E-Factureren geen departementaal-vertrouwelijke gegevens worden uitgewisseld en een Diginetwerk-verbinding niet voor alle overheden eenvoudig te realiseren is, is voor berichtenverkeer ook een aansluiting via internet toegestaan. Merk op dat beveiliging van het berichtenverkeer reeds is gewaarborgd onder Digikoppeling: gebruik van dubbelzijdige authenticatie (TLS/SSL) en, optioneel, het ondertekenen en/of versleutelen van de berichtinhoud zelf.

5.2 Aansluiten op Diginetwerk

Diginetwerk verbindt besloten overheidsnetwerken met elkaar, zodat er virtueel één besloten netwerk ontstaat. Daarbinnen kunt u veilig gegevens uitwisselen met andere overheden en overheidsvoorzieningen zoals Digipoort.

De besloten netwerken worden ‘koppelnetwerken’ genoemd. Deze koppelnetwerken zijn met elkaar verbonden via een centrale voorziening: het BasisKoppelNetwerk.

Voor een aansluiting op Diginetwerk moet een overheidsorganisatie over een aansluiting op een van de koppelnetwerken beschikken of deze aansluiting realiseren.

Een actueel overzicht van de huidige koppelnetwerken en de organisatie die deze netwerken beheert is te vinden op de Logius website:

https://www.logius.nl/diensten/diginetwerk/hoe-werkt-het

Indien uw organisatie nog niet beschikt over een aansluiting op een van deze koppelnetwerken, moet eerst een dergelijke aansluiting worden gerealiseerd. Logius kan assisteren bij het selecteren van het netwerk en bij het indienen van de aanvraag.

Diginetwerk: aansluiten via koppelnetwerk

Indien uw organisatie nog niet beschikt over een aansluiting op een van genoemde koppelnetwerken, dient allereerst deze aansluiting te worden geregeld. Het realiseren van deze netwerkverbinding kan geruime tijd in beslag nemen.

Opmerking: een aansluiting op een van de koppelnetwerken betekent *niet automatisch* een aansluiting op Diginetwerk! Voor een aansluiting op Diginetwerk moet een apart aansluittraject worden doorlopen. Feitelijk wordt hierbij een reeks

van IP-adressen toegekend die binnen het koppelnetwerk is gereserveerd voor gebruik door Diginetwerk. U kunt hiervoor via Servicecentrum Logius contact opnemen met de Diginetwerk-medewerkers van Logius.

De Aansluitvoorwaarden Diginetwerk zijn hier te vinden:
- https://www.logius.nl/ondersteuning/diginetwerk/

Aanvullende informatie over Diginetwerk is te vinden op https://www.logius.nl/diensten/diginetwerk/. Een aansluiting verloopt via Logius, indien het gekozen koppelnetwerk onder beheer van Logius valt, of via een van de andere beheerders, die hiervoor een offerte zullen uitbrengen.

5.3 Netwerkverbinding realiseren

Om vanuit uw organisatie berichtenverkeer met Digipoort mogelijk te maken, moet uw systeem een netwerkverbinding hebben met Digipoort. Er wordt een onderscheid gemaakt tussen een verbinding met de Digipoort preproductieomgeving, die wordt gebruikt voor testdoeleinden, en een verbinding met de productieomgeving.

Netwerk in kaart brengen

Bij het ontwerp van de netwerkverbinding is een netwerkdiagram onontbeerlijk. In dit diagram wordt de volledige netwerkverbinding in kaart gebracht van Digipoort-omgeving (preproductie- en productieomgeving) naar de bijbehorende endpoints binnen de infrastructuur van uw organisatie. Het is daarbij zaak om met name de koppeling vanuit de infrastructuur en de betrokken koppelnetwerken in kaart te brengen.

Bij een verbinding via *Diginetwerk* zijn mogelijk meerdere koppelnetwerken betrokken. Digipoort zelf is aan Diginetwerk gekoppeld via SUWInet en de Haagse Ring (OSB-VPN). Uw eigen organisatie kan ook aan Diginetwerk gekoppeld zijn via een ander koppelnetwerk. De wijze waarop de verbinding wordt gerealiseerd kan consequenties hebben voor de instellingen van firewalls en dergelijke.

Alle plaatsen waar (mogelijk) wijzigingen moeten worden aangebracht om de verbinding operationeel te krijgen, dienen in het netwerkdiagram te worden opgenomen. Zo kunnen alle betrokken partijen te allen tijde beschikken over een eenduidig overzicht van de netwerkconfiguratie.

In geval van een aansluiting via Diginetwerk moeten uw server(s), via welke het berichtenverkeer met Digipoort gaat lopen, een IP-adres uit de aan uw organisatie toegewezen Diginetwerk-reeks krijgen.

In de regel zullen instellingen moeten worden aangepast op de firewall van uw organisatie. Berichtenverkeer met Digipoort voor DigiInkoop/E-Factureren betreft altijd inkomend en uitgaand verkeer, de firewall zal derhalve voor beide richtingen moeten worden geconfigureerd.

Berichtenverkeer met Digipoort loopt, conform de Digikoppeling-koppelvlakstandaarden, over het beveiligde HTTP-protocol (HTTPS). Digipoort accepteert alleen verkeer over de standaard HTTPS-poort (poort 443).

De DNS-namen die aan uw servers worden toegekend, moeten worden gepubliceerd in uw publieke DNS zodat zij door Digipoort kunnen worden vertaald naar de onderliggende IP-adressen.

5.4 Netwerkverbinding testen

Wanneer alle benodigde aanpassingen aan firewalls e.d. zijn uitgevoerd, dient de netwerkverbinding te worden getest. Met behulp van telnet of een vergelijkbare utility kan worden geprobeerd om verbinding met Digipoort te maken. De netwerkspecialisten van Logius kunnen u desgewenst helpen met deze tests, met name indien de verbinding is ingericht via Diginetwerk.

In die gevallen waarin het testen van de netwerkverbinding niet succesvol is, is het advies om de volgende punten na te gaan:

- Worden de juiste source- en target-adressen gehanteerd?
- Is (intern) de juiste NAT-translatie doorgevoerd?
- Is de firewall van uw organisatie correct geconfigureerd voor inkomend en uitgaand verkeer van/naar de Digipoort-adressen?

Wanneer u beschikt over de benodigde certificaten, kan ook de HTTPS-verbinding (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.

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

5.5 Mijlpaal netwerkaansluiting en deliverables

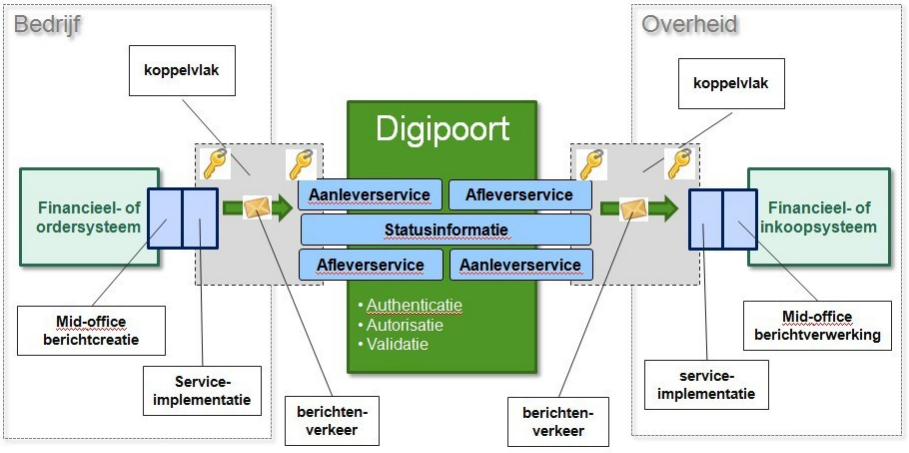
Indien uw organisatie in staat is om succesvol een TCP/IP-verbinding te maken met Digipoort, is de mijlpaal “netwerkaansluiting gereed” bereikt.

Aan het einde van deze stap levert u de volgende deliverables op:

1. Netwerkdiagram, waarin de gerealiseerde netwerkverbinding tussen organisatie en Digipoort is weergegeven. Dit diagram moet worden overhandigd aan uw aansluitcoördinator zodat het kan worden opgenomen in het aansluitdossier;
2. Succesvolle TCP/IP-verbinding tussen Digipoort en het endpoint van uw organisatie over poort 443.

6 Stap 3: realiseren koppelvlak (Digikoppeling)

Het doel van deze stap is om de technische koppeling tussen overheidsdeelnemer en Digipoort gerealiseerd te krijgen, zodat via deze koppeling een ketentest kan worden uitgevoerd (stap 6) zodra ook de inhoudelijke berichtverwerking 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 inkoopsysteem via Digipoort naar het beoogde bedrijf of vanuit het bedrijf naar uw systeem. Deze keten wordt in onderstaande figuur geïllustreerd:



Figuur 4: overzicht van de keten

In deze stap wordt het volgende gedaan:

- Aanvragen van certificaten[1] en inrichten van 'certificate stores';
- Implementatie van de benodigde services (ebMS en mogelijk ook WUS).

Preproductie- en productieomgeving

Berichtenverkeer met Digipoort zal normaliter plaatsvinden via het *productie-koppelvlak*, de 'ingang' voor productieverkeer.

Voor het *testen* van berichtenverkeer biedt Digipoort ook een *preproductie-koppelvlak*. Via dit koppelvlak is dezelfde functionaliteit beschikbaar (maar het kent niet dezelfde performance). Overheden zullen in eerste instantie hun berichtenverkeer inrichten op basis van dit koppelvlak en pas nadat het testtraject succesvol is afgesloten, kunnen overgaan op het productie-koppelvlak.

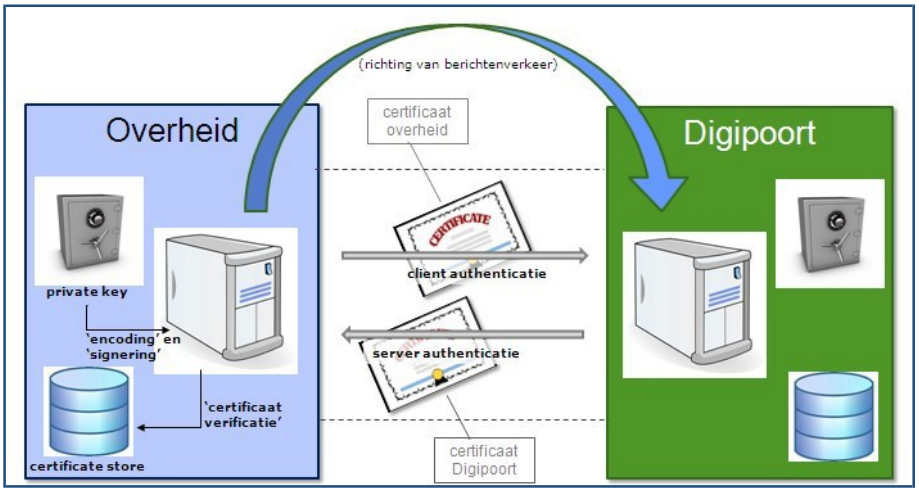
De software die de implementatie van het koppelvlak (services) vormt, wordt ook wel 'adapter' genoemd. De adapter vormt de softwarematige schakel tussen het overheidssysteem en Digipoort. Vaak worden voor ebMS en WUS verschillende adapters (softwareoplossingen) gebruikt.

[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 overheid en Digipoort en bij het digitaal ondertekenen van de uitgewisselde berichten ((‘signering’)).



Figuur 5: overzicht gebruik van certificaten

Het gebruik van een beveiligde verbinding (op basis van tweezijdig TLS/SSL) is verplicht onder Digikoppeling (zie voor meer informatie *Koppelvlakbeschrijving WUS 2.0* en *Koppelvlakbeschrijving ebMS 2.0*)[2]. De beveiligde verbinding, waarbinnen beide communicatiepartners zijn geauthenticeerd, zorgt voor versleuteld verkeer tussen overheids-deelnemer en Digipoort.

Het ondertekenen van berichten is optioneel voor verkeer tussen Digipoort en overheden. Ondertekening 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 overheid 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 overheids-deelnemer als Digipoort gebruikt voor wederzijdse identificatie/authenticatie.

Voor de *preproductieverbinding* kunnen naast PKIoverheid en PKItrial-certificaten ook door Logius verstrekte testcertificaten worden gebruikt.

[2] *Te vinden in de zip-bestande met documentatie op www.logius.nl/producten/gegevensuitwisseling/digipoort/koppelvlakken/wus-20-voor-overheden/ en www.logius.nl/producten/gegevensuitwisseling/digipoort/koppelvlakken/ebms-20-voor-overheden /(onder “Laatst stabiele versie”)*

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 organisatie al beschikken over een beveiligde verbinding op 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 (of minimaal een apart IP-adres op een bestaande server), 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 organisatie een verbinding met Digipoort initieert (oftewel: wanneer namens uw organisatie 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*, 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.

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 de aanvrager aangeleverde gegevens. U bent zelf verantwoordelijk voor het creëren van deze CSR. In de regel zal dit gebeuren door de persoon die binnen of namens uw organisatie 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 .cer of .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. Merk op dat het root-certificaat Staat der Nederlanden niet wordt meegeleverd. Dit root-certificaat kan worden gedownload vanaf de Logius website.

6.1.3 *Aanvragen van PKIoverheid-certificaten*

PKIoverheid-certificaten worden aangevraagd bij een CSP waarmee uw organisatie een overeenkomst heeft gesloten. Deze certificaten moeten

worden aangevraagd door de persoon die binnen of namens de organisatie als *certificaatbeheerder* bij de CSP is geregistreerd.

Meer informatie vindt u hier:

- https://www.logius.nl/diensten/pkioverheid/

Hier is eveneens een overzicht te vinden van CSP's die PKIoverheid-certificaten leveren.

PKItrial-certificaten kunnen binnen de preproductieomgeving worden gebruikt voor berichtondertekening. Deze trial-certificaten kunnen momeneel worden aangevraagd bij een beperkt aantal CSP's.

6.1.4 Aanvragen van Logius testcertificaten

U kunt 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.

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 OIN van uw overheidsorganisatie.

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

Voorbeeld overheid: "Ministerie van Binnenlandse Zaken"

Ad. 3.
Geef het URL-adres op van de server, waaronder deze geregistreerd is in de DNS-server. Bijvoorbeeld "testserver.mijnoverheid.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.mijnoverheid.nl". Als u als bedrijf alleen berichten aanlevert, of als u als overheidsorganisatie gebruik maakt van Diginetwerk, dan is een DNS-registratie meestal niet nodig en is het opgeven van het algemene internetadres voldoende.

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

Ad. 4.
Geef dan uw 20-cijfige overheidsidentificatienummer (OIN) op.

Voorbeeld OIN: "00000001812483297000"

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

6.1.5 Installeren van certificaten

Om een beveiligde netwerkverbinding tussen uw organisatie en Digipoort op te zetten en eventueel de hierover verzonden berichten digitaal te ondertekenen, moeten certificaten en bijbehorende private sleutels toegankelijk zijn voor de software die voor transportbeveiliging 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/PKItrial-certificaat) en private sleutel, inclusief bijbehorende (test-)certificaat-hiërarchie;
  - hiërarchie behorend bij het Digipoort-testcertificaat (**NB:** Digipoort gebruikt op sommige endpoints nog een 'G1-certificaat'. Vanaf 1 januari 2011 worden 'G2-certificaten' verstrekt. Uw organisatie heeft waarschijnlijk ook zo'n G2-testcertificaat ontvangen. Deze nieuwe certificaten kennen een eigen certificaathiërarchie, die afwijkt van de G1-hiërarchie. Wanneer er verbinding wordt gemaakt met een Digipoort-endpoint waarop een G1-certificaat wordt gebruikt, moeten zowel de G1-hiërarchie als de G2-hiërarchie door uw systeem worden vertrouwd. Beide moeten in dat geval 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/

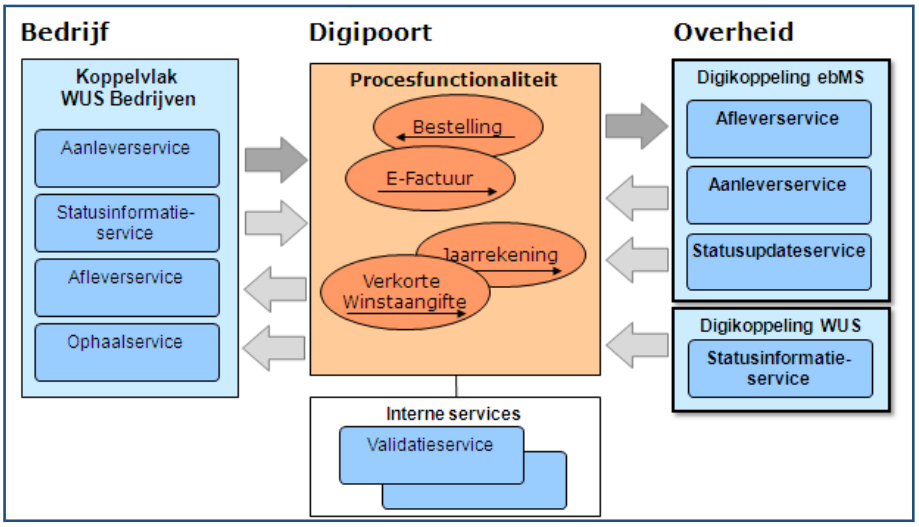
Onder deze laatste link kunt u het stamcertificaat en de intermediaire certificaten desgewenst downloaden.

6.2 Implementatie van services

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

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

Figuur 6 geeft een overzicht van de services onder versie 1.2 van het koppelvlak:



Figuur 6: overzicht Digipoort-services (getoond worden de services onder koppelvlak 1.2)

Als overheidsdeelnemer heeft u vooral te maken met de services die Digipoort biedt aan overheden. Voor de huidige versie van het koppelvlak zijn dat:

- ☐ Aanleverservice (ebMS): de service op Digipoort waarmee u berichten kunt aanleveren voor aflevering aan een leverancier;
- ☐ Statusinformatieservice (WUS): de service op Digipoort waarmee u kunt controleren of uw berichten ook daadwerkelijk zijn afgeleverd bij de leverancier. Deze service dient u altijd in combinatie met de Aanleverservice te implementeren;
- ☐ Afleverservice (ebMS): de service op uw adapter waarop Digipoort berichten kan afleveren die voor uw overheidsorganisatie bestemd zijn;
- ☐ Statusupdateservice (ebMS): aanvullende statusinformatie aanleveren. Deze service wordt niet gebruikt voor DigiInkoop/E-factureren.

Al deze services zijn apart beschreven in de Servicebeschrijvingen. Deze beschrijvingen zijn te vinden in de zip-bestanden (“WUS-services” en “ebMS-services”) op

- ❖ WUS: https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-wus-overheden/

- ebMS: https://www.logius.nl/ondersteuning/gegevensuitwisseling/koppelvlak-ebms-overheden/.

Wilt u als overheidsorganisatie berichten versturen aan een bedrijf (of aan DigiInkoop), zoals bestellingen, 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. Zie ook het document Grip op Digitaal verzenden met hierin beschreven welke actie u dient te ondernemen bij iedere uitzonderingssituatie.

Wilt u als overheidsorganisatie berichten ontvangen van een bedrijf (of van DigiInkoop), zoals e-facturen, 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.

6.2.1 WUS- en ebMS-services

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 ‘Digikoppeling WUS’ maakt gebruik van zogenoemde webservices conform de WS*-standaarden. De gegevens die met de service kunnen worden uitgewisseld worden beschreven in een XML-document dat WSDL wordt genoemd.

Services die worden aangeboden onder het koppelvlak 'Digikoppeling ebMS' worden beschreven in een XML-document dat CPA wordt genoemd. In tegenstelling tot de WSDL die bij WUS-services wordt gebruikt, bevat de CPA gegevens van beide partijen die bij het berichtenverkeer zijn betrokken.

Wanneer uw organisatie een 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 of CPA vormen 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.

Alle informatie die nodig is om de service te implementeren, is terug te vinden in de koppelvlakdocumentatie (zie paragraaf 6.2).

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).

6.2.2 *WUS: WSDL, SOAP en XSD (transportspecificatie)*

Een WUS-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. Een SOAP-bericht is een XML-document met een vaste structuur (Envelope met daarbinnen een optioneel Header- en verplicht Body-element). De semantiek van de Body is gespecificeerd in een XSD (XML Schema) waarnaar in de WSDL wordt verwezen. De feitelijke inhoudelijke gegevens (e-factuur, etc.), ook wel *payload* genoemd, zijn zelf als XML-document opgenomen in de Body van 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 overheden*.

Voor de WUS-service die berichtenverkeer van overheidsorganisatie naar Digipoort mogelijk maakt (Statusinformatieservice) moet door uw organisatie een 'aanroep' van de service worden geïmplementeerd. Veelal gebeurt dit door de WSDL te 'importeren' binnen de adaptersoftware, waardoor de benodigde 'aanroepcode' wordt gegenereerd. Soms gaat dit niet probleemloos, zie voor meer informatie de FAQ's op de website.

6.2.3 *ebMS: CPA en XSD (transportspecificatie)*

In een CPA worden de gegevens opgenomen van de partijen die met elkaar berichten gaan uitwisselen (in dit geval Digipoort en uw overheidsorganisatie). De CPA bevat informatie over de respectievelijke

partijen (naam, OIN), de te hanteren adressen (endpoints), de berichttypen die kunnen worden uitgewisseld en, anders dan in de WSDL, informatie over de certificaten die bij transport- en berichtbeveiliging worden gebruikt.

De CPA moet door beide partijen in hun ebMS-adapter worden geïmporteerd. De adapter weet daarmee welke berichten met welke organisaties onder welke condities kunnen worden uitgewisseld.

Ook in geval van ebMS worden gegevens uitgewisseld in de vorm van SOAP-berichten, waarvan de structuur is gespecificeerd in een XSD. De relatie tussen de berichttypen uit de CPA en hun specificatie in de XSD, wordt in de ebMS-adapter geconfigureerd.

Logius maakt de CPA aan op basis van het technisch aansluitformulier.

6.2.4 Berichtstroomspecificaties

De services die onder de Digikoppeling-koppelvlakken 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 aan 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 overheden*

Voor E-Factureren:

- https://www.logius.nl/ondersteuning/e-factureren-voor-overheden-via-digipoort/

Voor DigiInkoop:

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

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 (SOAP header en body) 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, op te vragen door de Aanleveraar via de Statusinformatieservice. Middels de Statusinformatieservice kan de Aanleveraar altijd nagaan of een bericht succesvol is afgeleverd.

6.2.5 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.

6.3 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.

In de toekomst wordt vanuit Digipoort een 'Aansluit Suite' beschikbaar gesteld, waartegen kan worden getest. Zolang die niet beschikbaar is, bieden tools als SOAP-UI een alternatief 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.

6.4 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. bestelling, etc.) dat door de overheidsorganisatie via Digipoort aan een bedrijf wordt verzonden of via Digipoort vanuit een bedrijf wordt ontvangen (bijv. e-factuur, order, etc.).

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/,

HR-XML:
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.

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 inkoopsysteem. 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 Digipoorts 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). Validatiefouten worden door Digipoort ook geregistreerd als statusmelding. Deze is door de aanleveraar op te vragen middels de Statusinformatieservice.

Omgekeerd moeten door Digipoort aangeleverde berichten correct kunnen worden verwerkt door uw ontvangende software (adapter) en achterliggend systeem. Uw 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 over de 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 OHNL 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 uw organisatie in staat om berichten middels de eigen systemen via de 'adapter software' te ontvangen van en te versturen richting Digipoort. Overigens worden alleen correcte (gevalideerde) berichten door Digipoort doorgestuurd naar/afgeleverd bij de beoogde ontvanger.

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.

Bij deze stap wordt u direct begeleid door de leverancier bij wie het technisch beheer van Digipoort belegd is. U dient tijdig bij uw aansluitcoördinator aan te geven wanneer u deze technische test wilt gaan uitvoeren (conform planningsdocument), zodat hij ervoor kan zorgen dat bij de leverancier de benodigde resources worden vrijgemaakt. De technische gegevens die zijn benodigd voor de configuratie van Digipoort voor uw aansluiting worden middels een formulier aan de leverancier verstrekt (zie de volgende paragraaf).

8.1 Aansluitformulier Technische Gegevens

Voor de configuratie van Digipoort voor het uitwisselen van berichten met uw organisatie, wordt gebruik gemaakt van het *Aansluitformulier Technische Gegevens*. Dit formulier verkrijgt u via uw aansluitcoördinator.

In dit formulier kunt u de volgende gegevens invullen:

- Contactgegevens overheidsorganisatie 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.

Het Aansluitformulier wordt via de aansluitcoördinator doorgegeven aan de Digipoort-leverancier.

8.2 Connectiviteitstest

Om berichten uit te kunnen wisselen met Digipoort is het zaak dat er een dubbelzijdig beveiligde verbinding tussen overheidsorganisatie 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:

- De overheidsorganisatie kan een dubbelzijdig geauthenticeerde netwerkverbinding tot stand brengen met Digipoort (preproductie-endpoint) op poort 443, en
- Digipoort kan een dubbelzijdig geauthenticeerde netwerkverbinding tot stand brengen met de overheidsorganisatie (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 ebMS- of 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 (indien van profiel "digitale ondertekening" gebruik wordt gemaakt).

Aangeleverde SOAP-berichten worden door Digipoort gevalideerd. Merk op dat deze validatie generiek van aard is (de Digipoort-services zijn immers generiek opgezet). Een dienst of berichtstroom, zoals DigiInkoop of E-Factureren, die van zo'n service gebruik maakt, kan aanvullende eisen aan de berichtinhoud stellen. Voor DigiInkoop/E-Factureren zijn deze aanvullende eisen vastgelegd in *berichtstroomspecificaties* (zie paragraaf 6.2.4). Deze aanvullende eisen worden niet in alle gevallen door Digipoort gevalideerd ('afgedwongen'). Het is dan ook zaak om bij de test te verifiëren dat de berichten ook conform berichtstroomspecificatie zijn opgebouwd.

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 van de koppelvlakken.
- *Zie ook het document "Grip op digitaal versturen"* bij koppelvlak documentatie op de Logius website.

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. Er wordt geverifieerd dat berichten die door het bedrijf zijn verzonden ook daadwerkelijk correct door Digipoort worden afgeleverd en (in het geval van DigiInkoop) visa versa. Bovendien wordt geverifieerd dat de inhoudelijke berichten conform de afspraken zijn die u met de aanleverende bedrijven hebt gemaakt.

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. het 'Aansluitformulier Technische Gegevens' is aangeleverd voor configuratie van Digipoort;
5. afspraken met de ketenpartner (bedrijf) 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 een of meer bedrijven die als ketenpartner fungeren. De rol van Logius is hier beperkt tot technische ondersteuning van 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?

Resultaten van de ketentest kunt u vastleggen in een document dat door uw aansluitcoördinator aan u verstrekt zal worden. Dit document dient te worden geretourneerd aan Logius na afronding van de ketentest. Logius bepaalt mede op basis van de resultaten in het document of akkoord voor productiegang kan worden gegeven.

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

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 overheidsorganisatie) 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)

U kunt het onder stap 5 reeds gedeeltelijk ingevulde Aansluitformulier aanvullen met de technische gegevens behorend bij de productie-omgeving (voor zover dat nog niet is gedaan). Op basis van deze gegevens wordt de configuratie van Digipoort aangevuld voor verkeer over de productieverbinding.

Het Aansluitformulier wordt via de Logius-aansluitcoördinator doorgegeven aan Digipoort.

10.2 Connectiviteitstest

Ook voor de productieverbinding is het zaak om eerst een connectiviteitstest uit te voeren, om te controleren of uw organisatie 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:

- de overheidsorganisatie kan netwerkverbinding maken met Digipoort (productie-endpoint) op poort 443, en
- Digipoort kan netwerkverbinding maken met de overheidsorganisatie (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 (productie)

De ketentest wordt nogmaals uitgevoerd, ditmaal 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!

Ook de resultaten van deze ketentest kunt u vastleggen in het eerder hiertoe verstrekte document (zie paragraaf 9.1). Dit document dient te worden geretourneerd aan Logius na afronding van de ketentest. Logius

bepaalt mede op basis van de gerapporteerde resultaten of akkoord voor in productie name (te beginnen met eerste gecontroleerde productierun, zie paragraaf 10.5) kan worden gegeven.

Na een succesvol afgesloten ketentest over de productieverbinding kan een gecontroleerde eerste productierun worden uitgevoerd.

10.5 Uitvoeren eerste gecontroleerde productierun

Bij de eerste productierun ontvangt uw organisatie daadwerkelijke facturen etc. over de productieverbinding voor verdere verwerking door uw financieel- of inkoopsysteem. 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.

10.6 Inbeheername

Wanneer de eerste productierun correct is uitgevoerd, is de aansluiting in feite gereed en kan deze door Logius in beheer worden genomen. Voor deze in beheer name verstrekt Logius u de benodigde informatie, waaronder een checklist en een overzicht van de procedures rond beheer.

Uw organisatie wordt door Logius opgenomen in het overzicht van aangesloten partijen op de Logius website.

Vanaf dit moment heeft uw organisatie nog recht op twee weken nazorg. De aansluitcoördinator 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 en zijn de Serviceniveau-overeenkomsten (SNO) van toepassing

10.7 Mijlpaal: aansluiting in productie

De afronding van deze fase representeert het voltooien van de aansluiting van uw organisatie 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 geheimgehouden.

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.

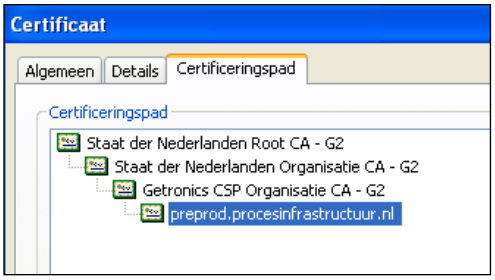
Certificate stores
Om deze verificatie mogelijk te maken, wordt de certificaathiërarchie (stamcertificaat en tussenliggende certificaten) opgenomen in een zogenoemde *certificate trust store*. Een certificaat van een partij die zich hiermee identificeert, kan dan worden geverifieerd tegen de hiërarchie 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 aan 'preprod-dgp.procesinfrastructuur.nl' uitgegeven PKIoverheid-certificaat een bovenliggende hiërarchie kent, waarin drie certificaten zijn opgenomen:

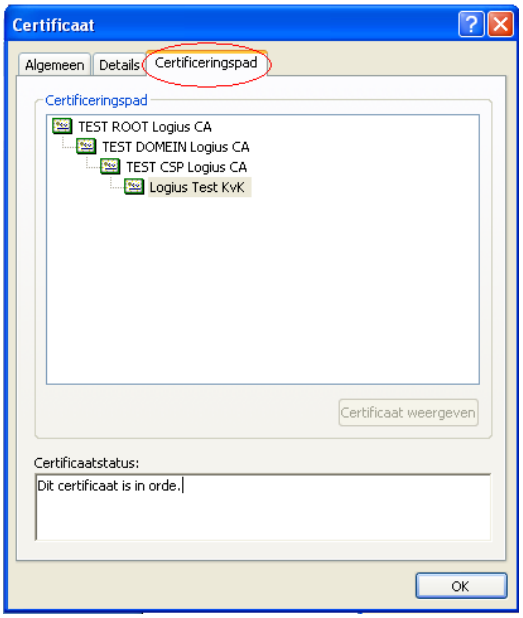
- 'Getronics CSP Organisatie CA – G2'-certificaat;
- 'Staat der Nederlanden Organisatie CA – G2'-certificaat,en
- 'Staat der Nederlanden Root CA – G2'-certificaat.

Het laatstgenoemde certificaat is het stamcertificaat. De overige twee zijn voorbeelden 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*.

Digipoort certificaten

Houdt u er rekening mee dat ook Digipoort elke 3 jaar van certificaat zal veranderen. Dit kan dan tot een actie bij u leiden omdat u bijvoorbeeld het publieke deel van het Digipoort certificaat in uw omgeving op zou moeten nemen.