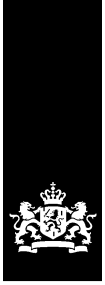


Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DigiD Handreiking, voor Pensioenuitvoerders

Versie 1

Datum oktober 2011
Status Definitief

Colofon

Projectnaam	DigiD
Versienummer	1
Organisatie	Pensioenfederatie ism Logius

•

Inhoud

1 Inleiding

1.1 Doel

Deze handreiking leidt Pensioenfondsen / Pensioenuitvoerders door het gehele traject om aan te kunnen sluiten op DigiD.

1.2 Doelgroep

Deze handreiking is bedoeld voor Pensioenfondsen / Pensioenuitvoerders die gebruik willen maken van DigiD.

1.3 Leeswijzer

Dit document is door de Pensioenfederatie samengesteld voor Pensioenfondsen / Pensioenuitvoerders die willen aansluiten op DigiD. Het is ontleend aan de Handreiking DigiD (versie 2.4 dd 21 oktober 2010). Voor de actuele informatie wordt verwezen naar de website van Logius. De documentatie is te vinden op www.logius.nl/digid onder documentatie.

In de tekst worden “Pensioenfondsen / Pensioenuitvoerders” verder aangeduid met de term “Pensioenuitvoerders”.

1.4 Documentatie

Door de Aansluitvoorwaarden te ondertekenen gaat u akkoord met het product DigiD en de diensten van Logius. Onder de diensten wordt de documentatie en het Servicecentrum bedoeld.

2 Over DigiD

2.1 Wat is DigiD?

DigiD (spreek uit: 'die-gie-dee') staat voor digitale identiteit. DigiD is dé gemeenschappelijke authenticatievoorziening van de overheid, waarmee elektronische diensten in het publieke domein in staat worden gesteld, gebruik te maken van door Logius beschikbaar gestelde authenticatiemiddelen. DigiD is daarmee een voorziening die gebruikers en afnemende overheidsorganisaties met elkaar verbindt. DigiD voorkomt dat overheidsorganisaties eigen authenticatiesystemen moeten gaan ontwikkelen en beheren, en dat gebruikers worden geconfronteerd met een 'digitale sleutelbos'.

DigiD opereert in een omgeving waarbinnen verschillende overheidsorganisaties elektronische diensten aanbieden aan burgers. Enkele voorbeelden van dergelijke diensten zijn het elektronisch aanvragen van een subsidie, inzage in persoonlijke elektronische dossiers en het elektronisch aangifte doen van belasting. Dergelijke elektronische diensten worden in dit document "webdiensten" genoemd.

DigiD hanteert drie zekerheidsniveaus: Basis, Midden en Hoog. DigiD biedt voor burgers gebruikersnaam/wachtwoord (niveau basis) en gebruikersnaam/wachtwoord + sms-code (niveau midden) aan. Meer hierover in hoofdstuk 3. DigiD vervult zelf de rol van authenticatie-instantie. Het authenticatiemiddel is gekoppeld aan een uniek persoonsidentificerend nummer, zoals het burgerservicenummer (BSN)[1] of het zogeheten A-nummer (Administratief Nummer). Het A-nummer is alleen beschikbaar voor gemeenten.

2.2 Wettelijk kader

DigiD mag worden gebruikt door:

- overheidsorganisaties en organisaties met een publiekrechtelijke taak die gebruik willen maken van DigiD als authenticatiemiddel;
- leveranciers die webdiensten ontwikkelen voor overheidsorganisaties en gebruik willen maken van de DigiD preproductie-omgeving.

In die context mag DigiD ook door Pensioenfondsen of door Pensioenuitvoerders namens die Pensioenfondsen worden gebruikt, zolang DigiD uitsluitend wordt toegepast in relatie tot de eerste en tweede pijler producten. Pensioenuitvoerders zullen zelf toezien op juist gebruik van DigiD.

2.3 Financieel

Behalve de relatief beperkte kosten voor de veiligheidscertificaten worden door Logius vooralsnog geen kosten in rekening gebracht voor gebruik van DigiD.
Het is mogelijk dat dit in de toekomst verandert. Er kan op dit mopment geen uitspraak worden gedaan over het kostenniveau en de structuur van die kosten.

[1] *In uitzonderingsgevallen kan gebruik worden gemaakt van het sofinummer*

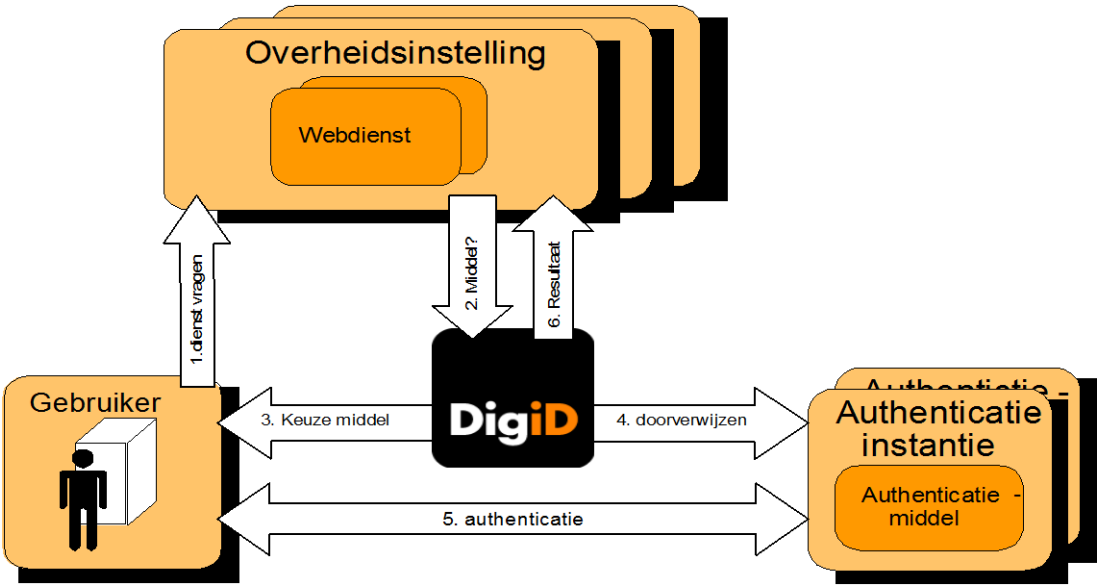
2.4 Praktisch nut voor Pensioenuitvoerders

Gebruik van DigiD heeft voor Pensioenuitvoerders de volgende voordelen:

- Gebruik van DigiD raakt meer en meer ingeburgerd als een vertrouwd inlogmechanisme;
- DigiD heeft vanaf beveiligingsniveau "middel" status van een juridisch getoetste digitale handtekening;
- Onderhoud op eigen inlogmechanisme kan op den duur vervallen (als uitsluitend DigiD wordt gebruikt).

2.5 Werking van DigiD in het kort

Na een aanvraag (1) voor een webdienst op de website van een overheidsorganisatie wordt de gebruiker naar DigiD doorgeleid(2).



Figuur 1: relatie tussen gebruiker, DigiD, de authenticatie-instantie en de overheidsorganisatie (webdienst)

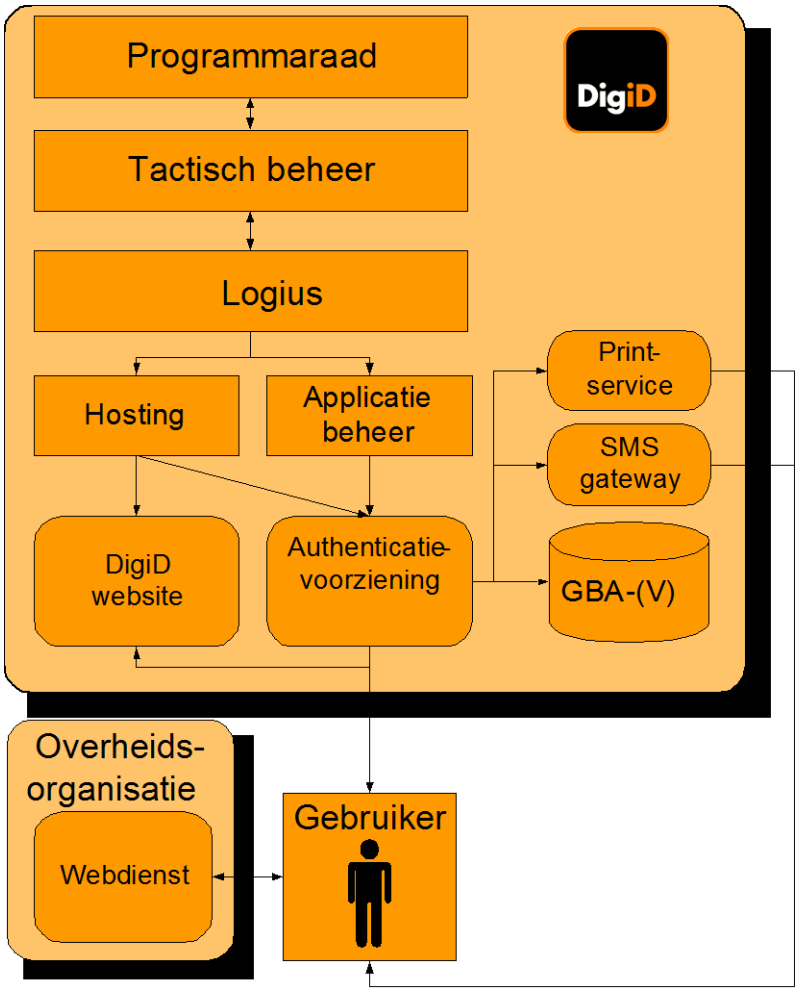
Op basis van het unieke applicatie-ID en op basis van het gebruikte SSL client-certificaat van de webdienst stelt DigiD het gewenste ***minimale*** zekerheidsniveau vast (opgegeven bij registratie van de webdienst). Indien van toepassing ziet de gebruiker vervolgens een keuzescherm met verschillende authenticatiemiddelen waaruit hij kan kiezen (3). Na selectie van een middel wordt de gebruiker doorgeleid naar de betreffende authenticatie-instantie (4). Hier wordt de gebruiker geauthenticeerd (5). Na het uitvoeren van de authenticatie verifieert DigiD het resultaat van de authenticatie (6).

Bij een succesvolle verificatie koppelt DigiD de volgende elementen terug aan de webdienst:

- Het persoonsnummer, bijvoorbeeld het BSN of het A-nummer.
- Het zekerheidsniveau van de authenticatie.

2.6 Rollen en actoren

De gehele infrastructuur van DigiD onderscheidt de volgende actoren (zie figuur 3):



Figuur 3: DigiD actoren

- Programmaraad Logius: verantwoordelijk voor het beleid van DigiD – eindverantwoordelijk is de staatssecretaris van het Ministerie van Binnenlandse Zaken (BZK);
- Tactisch Beheer: uitgevoerd door de afdeling Servicemanagement van Logius;
- Logius: het Servicecentrum van Logius begeleidt u tijdens het aansluitproces en beantwoordt uw vragen die betrekking hebben op het aansluittraject. Zij zijn het eerste aanspreekpunt voor al uw vragen. Verder doet Logius:
  - hosting (beheer infrastructuur van DigiD);
  - applicatiebeheer.
- Authenticatievoorziening (AV): de infrastructuur die rondom een authenticatiemiddel is ingericht om online authenticatie tot stand te kunnen brengen. De authenticatievoorziening is eigendom van een authenticatie-instantie;

- Overheidsorganisatie: proceseigenaar van de webdienst en klant van DigiD diensten;
- Webdienst: de webdienst van een overheidsorganisatie die via DigiD toegang aan de gebruikers verleent;
- Gebruiker: de eindgebruiker van DigiD. Voor DigiD voor burgers is dit een burger.
- Printservice: externe partij die de brief met activeringscode aanmaakt en verstuurt naar de gebruiker;
- SMS-gateway: de applicatie die sms-transactiecodes verstuurt naar gebruikers voor het zekerheidsniveau Midden (alleen voor DigiD voor burgers);
- GBA - GBA-V: Gemeentelijke Basisadministratie Persoonsgegevens Verstrekkingen (GBA-V) van de Gemeentelijke Basisadministratie Persoonsgegevens (GBA) die DigiD raadpleegt ter verificatie van de aanvraaggegevens van de burger.

2.7 Betrouwbaarheid

DigiD is een belangrijke schakel in de elektronische dienstverlening van overheidsorganisaties. Dankzij DigiD weet de overheidsorganisatie wat de identiteit is van de burger is die inlogt bij de webdienst. DigiD vervult hiermee de functie van vertrouwde intermediair tussen gebruiker en overheidsorganisatie/klant.

2.7.1 Zekerheidsniveaus

DigiD definieert verschillende zekerheidsniveaus, want niet voor iedere transactie is maximale zekerheid nodig. De zekerheidsniveaus kenmerken zich door de mate waarin zekerheid kan worden verschaft over de identiteit van een burger. Bij de definiëring van de zekerheidsniveaus is aansluiting gezocht bij vergelijkbare internationale voorzieningen en door het CBP[2] onderkende risicoklassen van persoonsgegevens.

Hierop wordt in het volgende hoofdstuk verder op ingegaan.

2.7.2 Privacy

Om de privacy van de gebruiker te waarborgen, verstrekt DigiD geen naam, adres of woonplaats (NAW) gegevens van de gebruiker aan derden, dus ook niet aan aangesloten organisaties. DigiD gebruikt de NAW-gegevens van burgers uit de GBA-V alleen voor het verzenden van de brief met activeringscode. DigiD bewaart geen NAW-gegevens in haar database. Om sms-authenticatie mogelijk te maken, bewaart DigiD wel het door de gebruiker opgegeven mobiele nummer. De gebruiker heeft de keuze om een e-mailadres op te geven, dit is niet verplicht. Indien de gebruiker hiervoor kiest, kan het e-mailadres ook worden gebruikt voor wachtwoordherstel en het versturen van een herinneringsmail.

2.7.3 Burgerservicenummer

Het burgerservicenummer (BSN) is een uniek identificerend persoonsnummer dat iedereen krijgt die ingeschreven staat in de Gemeentelijke Basisadministratie Persoonsgegevens (GBA) of de nog te vormen registratie niet-ingezetenen (RNI). Met een geheel nieuw wettelijk regime onderscheidt het BSN zich van het sofinummer door een breder gebruik toe te staan en het stelsel te voorzien van de nodige waarborgen op het gebied van privacy. Overheidsorganisaties gebruiken het BSN voor

[2] *College Bescherming Persoonsgegevens*

de communicatie met de burger en voor de uitwisseling van persoonsgegevens tussen (overheids)organisaties onderling.

Met inwerkingtreding van de wet algemene bepalingen burgerservicenummer meldt DigiD in beginsel het BSN of het A-nummer terug. In uitzonderingsgevallen zal DigiD het sofinummer terugmelden aan u. In dat geval treden partijen met elkaar in overleg. Naar verwachting zal op langere termijn het A-nummer niet meer worden gebruikt en/of worden teruggemeld. Een organisatie die het BSN mag gebruiken, zal het veelal moeten gebruiken. Het gebruik is echter niet verplicht wanneer voor de gegevensverwerking bij of krachtens de wet het gebruik van een ander persoonsnummer is voorgeschreven. De inschatting is dat vooralsnog een beperkt aantal sectoren gebruik (gaan) maken van een eigen sectornummer/persoonsnummer. Meer informatie hierover kunt u vinden op www.burgerservicenummer.nl.

2.7.4 Informatiebeveiliging

Informatiebeveiliging is voor DigiD cruciaal. Een aantal redenen op een rij:

- Met behulp van de functionaliteit van DigiD is het voor gebruikers mogelijk zich te authenticeren bij overheidsorganisaties. Omdat aangesloten klanten vertrouwen op de controle die door DigiD plaatsvindt, mogen hierin geen fouten ontstaan.
- De voortgang van bedrijfsprocessen van aangesloten overheidsorganisaties is afhankelijk van de beschikbaarheid van DigiD.
- De functionaliteit van DigiD bestaat grotendeels uit vertrouwelijke elektronische gegevensuitwisseling over het publieke internet.
- De gegevens die binnen DigiD worden gebruikt en uitgewisseld, bevatten informatie over de identiteit van personen. Deze gegevens mogen niet ongeautoriseerd aan derden ter beschikking komen.
- DigiD moet voldoen aan de wetgeving voor privacy en informatiebeveiliging, al dan niet ondersteund door richtinggevende, gerechtelijke en andere uitspraken en/of voorschriften.

Het stelsel van beveiligingsmaatregelen rondom DigiD richt zich op de beschikbaarheid, integriteit en exclusiviteit van DigiD. Deze drie aspecten zijn als volgt gedefinieerd:

- *Beschikbaarheid.* De belangrijkste informatie van DigiD moet op de juiste momenten beschikbaar zijn voor burgers, bedrijven en overheidsorganisaties.
- *Integriteit.* De informatie binnen de systemen van DigiD die wordt uitgewisseld met klanten en authenticatiesystemen moet juist, volledig en tijdig zijn en de programmatuur van DigiD moet volgens de gestelde specificaties werken.
- *Exclusiviteit.* Alleen bevoegden mogen gegevens van DigiD inzien.

Hieronder een voorbeeld voor elk van de aspecten:

- Met betrekking tot beschikbaarheid biedt DigiD bepaalde garanties. Deze garanties zijn opgenomen in de Aansluitvoorwaarden die u als klant accepteert. Maatregelen in onder meer de infrastructuur zorgen ervoor dat DigiD zo goed als continu beschikbaar is (7x24 uur) met uitzondering van onderhoudswindows.

- Als een gebruiker de inlogprocedure bij DigiD start, genereert DigiD een uniek nummer (sessie-ID) voor deze inlogsessie. In elke vervolgstap van het proces van authenticatie (elke communicatie tussen de browser van de gebruiker, de webdienst en DigiD) controleert DigiD deze sessie-ID. Zo kan DigiD de integriteit garanderen. Bovendien wordt aan het eind van het proces, het resultaat nog een keer gecontroleerd door de webdienst bij DigiD. Zo weet men zeker dat de uiteindelijke authenticatie van DigiD afkomstig is.
- De verbindingen tussen browser, webdienst, authenticatievoorziening en DigiD zijn beveiligd met een PKIoverheid services certificaat (SSL). Dit protocol voorkomt dat er wordt ingebroken op het authenticatieproces of dat het berichtenverkeer wordt afgeluisterd of onderschept. Hierdoor is de exclusiviteit gewaarborgd. Voor de functionaliteit Eenmalig inloggen en de WSDL-koppeling met DigiD wordt er gebruik gemaakt van een dubbelzijdig PKIoverheid Certificaat. Het gebruik van een dubbelzijdig certificaat verhoogt de zekerheid van de identiteit van de webdienst bij DigiD.

2.8 Communicatie

Het Servicecentrum Logius zorgt voor de begeleiding van uw aansluiting op DigiD. Hier kunt u ook terecht voor vragen die betrekking hebben op het aansluittraject.

DigiD biedt aangesloten organisaties de mogelijkheid gebruik te maken van kant-en-klaar communicatiemateriaal. Het basismateriaal vindt u onder meer in de Toolkit Communicatie.

2.8.1 www.logius.nl/digid

Communicatie

Met deze toepassing kunnen pensioenuitvoerders naar eigen behoefte communicatiemateriaal samenstellen met hun eigen logo en boodschap. Dit materiaal kunt u gebruiken voor de communicatie naar uw deelnemers over uw aansluiting op DigiD. Ook kunt u specifieke diensten die u via DigiD aanbiedt, promoten. Het digitale promotiemateriaal is gratis. De kosten voor reproductie (drukwerk), mediaplaatsingskosten, uitzendkosten en uitzendkopieën (televisie) zijn voor eigen rekening en risico.

Aansluitinformatie en formulieren

Hier kunt u de meest recente handreiking en bijlagen vinden. Ook vindt u hier de formulieren die u nodig heeft voor het aansluiten van de webdienst(en) op DigiD.

Contact

Hier vindt u de contactgegevens van Logius.

2.9 Veel gestelde vragen

Antwoorden op veelgestelde algemene burger vragen vindt u op de website van DigiD.

2.10 Opmerkingen & klachten

Mocht u klachten en/of opmerkingen hebben dan kunt u deze mailen naar servicecentrum@logius.nl.

3 Zekerheidsniveaus

DigiD hanteert drie gestandaardiseerde zekerheidsniveaus waarin authenticatiemiddelen zijn in te delen, namelijk Basis, Midden en Hoog. Het is de verantwoordelijkheid van u met welk zekerheidsniveau burgers diensten kunnen afnemen.

3.1 Basis

De dienstverlening verschaft een beperkte mate van zekerheid over de authenticiteit van de actie van de gebruiker. Door middel van gebruikersnaam en wachtwoord authenticeert de gebruiker zich bij de webdienst. Een gebruikersnaam/wachtwoord-combinatie is gebaseerd op het principe van een gedeeld geheim. Het door de gebruiker gehanteerde wachtwoord dient bij de ontvanger bekend te zijn zodat DigiD het kan verifiëren.

Dit niveau kunt u gebruiken voor diensten waarbij de aangeboden informatie voornamelijk van betekenis is voor de specifieke aanvrager.

De Pensioenfederatie adviseert dit veiligheidsniveau te hanteren indien de deelnemers uitsluitend raadpleegrechten krijgen.

3.2 Midden

De dienstverlening verschaft een redelijke mate van zekerheid over de authenticiteit van de actie van de gebruiker. Dit niveau kunt u hanteren als u uw gebruikers diensten wilt aanbieden waarvoor u een zwaarder authenticatiemiddel noodzakelijk acht. Zekerheidsniveau Midden maakt gebruik van gebruikersnaam, wachtwoord en een sms-code.

De Pensioenfederatie adviseert dit veiligheidsniveau te hanteren indien de deelnemers de mogelijkheid krijgen om via internet gemaakte keuzes of banknummers door te geven aan de Pensioenuitvoerders.

Met het zekerheidsniveau Midden kunnen uw gebruikers bijvoorbeeld persoonsgerelateerde diensten afnemen via het internet.

Een webdienst vereist het zekerheidsniveau Midden als er een risico is op:

- Leed en ongemak
  Een vertraging van de dienstverlening resulteert in ongemak of additionele inspanningen voor de betrokken partijen. Betrokken partijen kunnen zijn de aanbieder van de webdienst en de gebruiker (burger, bedrijf of overheidsinstantie) die gebruik maakt van de webdienst.
- Financiële verliezen
  Financiële verliezen voor de webdienst zijn onterechte uitkeringen aan gebruikers of verstrekking van diensten voor niets, terwijl hiervoor zou moeten worden betaald. Betrokken partijen kunnen zijn de aanbieder van de webdienst en de gebruiker (burger, bedrijf of overheidsinstantie) die gebruik maakt van de webdienst.
- Reputatieschade
  Problemen met of binnen uw organisatie hebben nieuwswaarde. Reputatieschade resulteert in een lagere bereidheid binnen de

beoogde doelgroep om van de webdienst gebruik te maken of slechte beeldvorming in het algemeen van de webdienst.
- Productieverlies
  Verlies van productiviteit resulteert in onnodige inzet van personeel aan de kant van de dienstaanbieder. Voor de gebruiker kan dit bestaan uit vertraging in de afhandeling of het zich alsnog melden bij een fysiek loket.
- Vrijgave van vertrouwelijke informatie
  Voorbeelden van vertrouwelijke (persoons)gegevens zijn bankrekeningnummers op naam van de gebruiker, burgerservicenummers, inkomensgegevens en medische data.
- Schending van wettelijke voorschriften
  Zijn er bijvoorbeeld wettelijke termijnen aanwezig waarbinnen de dienst moet worden geleverd? Een schending van dergelijke eisen kan bijvoorbeeld leiden tot een berisping, boete, beschikking of veroordeling.
- Persoonlijk letsel
  Met persoonlijk letsel wordt bedoeld fysieke dan wel psychische schade bij de gebruiker.

3.3 Hoog

De dienstverlening verschaft een hoge mate van zekerheid over de authenticiteit van de actie van de gebruiker. Dit niveau gebruikt u als u uw klanten diensten wilt aanbieden waarvoor u het hoogste zekerheidsniveau noodzakelijk acht. Het zekerheidsniveau Hoog is gebaseerd op het zekerheidsniveau zoals wordt voorgeschreven voor gekwalificeerde elektronische handtekeningen vanuit de Wet elektronische handtekeningen.

Op dit moment kan zekerheidsniveau Hoog nog niet geleverd worden binnen DigiD.

4 Voorwaarden voor deelname aan DigiD

4.1 Randvoorwaarden aansluiten op DigiD

Om aan te sluiten op DigiD zijn de voorwaarden als volgt:

- de organisatie is een publiekrechtelijke organisatie of een privaatrechtelijke organisatie die op basis van een wettelijke grondslag belast is met de uitvoering van een publieke taak;
- de organisatie mag op basis van een wettelijke grondslag over het BSN beschikken;
- de taak waarvoor DigiD wordt gebruikt is een publieke taak.

Pensioenuitvoerders voldoen aan de voorwaarden, zolang uitsluitend de eerste en tweede pijler producten worden geraakt.

4.2 Toelichting Aansluitvoorwaarden Preproductie-omgeving

Het Servicecentrum Logius stelt een preproductie-omgeving beschikbaar aan u. U kan deze omgeving gebruiken tijdens het ontwikkelen en testen van de aansluiting van u op DigiD. Het testen van de aansluiting is verplicht. Op de preproductie-omgeving kan geen performancetest uitgevoerd worden.

In de Aansluitvoorwaarden staan de afspraken, die klant en Logius aangaan voor de periode waarin u op de DigiD preproductie-omgeving is aangesloten. Door ondertekening van het Aansluitformulier Preproductie-omgeving verklaart u zich te houden aan de Aansluitvoorwaarden Preproductie-omgeving. U geeft hiermee tevens aan dat hij zorgvuldig met de door de Logius verstrekte informatie om gaat.

U tekent het Aansluitformulier Preproductie-omgeving voordat hij wordt toegelaten tot de DigiD preproductie-omgeving. Het document Aansluitvoorwaarden Pre-productie is opgenomen op www.logius.nl/digid onder documentatie.

N.B. Leveranciers zijn eveneens als klanten gerechtigd om gebruik te maken van de preproductie-omgeving en doorlopen dezelfde procedures als klanten. Leveranciers mogen echter niet aansluiten op de productieomgeving.

4.3 Toelichting Aansluitvoorwaarden Productieomgeving

U moet de Aansluitvoorwaarden Productieomgeving accepteren voordat een webdienst kan aansluiten op de DigiD productieomgeving. Door ondertekening van het Aansluitformulier Productieomgeving verklaart u zich te houden aan de Aansluitvoorwaarden Productieomgeving. Het document Aansluitvoorwaarden Productieomgeving is te vinden op www.logius.nl/digid onder documentatie.

4.3.1 Contactpersonen

U bent zelf verantwoordelijk dat bij het Servicecentrum de juiste contactpersonen bekend zijn. Deze personen kunnen alleen aanpassingen aanvragen met betrekking tot de DigiD aansluiting.

4.4 Serviceniveau DigiD voor Afnemers

In deze bijlage van de Handreiking vindt u het niveau van dienstverlening van de service DigiD en de DigiD website. Het niveau van dienstverlening van de service DigiD en DigiD website is gebaseerd op de gemaakte afspraken tussen de tactisch beheerder van DigiD en de operationeel beheerder. Het Serviceniveau DigiD gaat onder meer in op de servicewindows van de 1e en 2e-lijns ondersteuning, het onderhoudswindow en de performance-indicatoren van DigiD waar u op mag rekenen. Deze zijn beschreven op het gebied van beschikbaarheid, capaciteit en performance, incidentbeheer, calamiteitenbeheer, wijzigingenbeheer en betrouwbaarheid- en integriteitbeheer.

4.5 Verantwoordelijkheden klant versus DigiD

4.5.1 Betrouwbaarheid van dienstverlening

Hieronder vindt u een opsomming van uitgangspunten inzake de betrouwbaarheid van de dienstverlening. Deze lijst is richtinggevend en niet uitputtend.

- U bepaalt zelf het zekerheidsniveau dat is vereist voor het afnemen van een dienst. Zie hoofdstuk 3.
- U dient zelf een risicoanalyse uit te voeren waarmee de eindverantwoordelijke binnen de organisatie van u akkoord is gegaan. In de risicoanalyse wordt het vereiste zekerheidsniveau van de diensten beschreven. Dit niveau is in overeenstemming met het zekerheidsniveau van de authenticatiedienst die bij DigiD wordt afgenomen.
- Een klant is na de eerste aansluiting verplicht elke nieuwe aansluiting van een webdienst op DigiD vooraf te melden aan het Servicecentrum Logius.
- Een klant moet een wijziging die betrekking heeft op de door DigiD ontsloten webdienst afstemmen met het Servicecentrum Logius. Het Servicecentrum Logius beslist of er opnieuw getest moet worden.
- U dient maatregelen te nemen om de netwerkverbinding tussen u en het Servicecentrum Logius te vrijwaren van misbruik. Dit kan bijvoorbeeld door het plaatsen van een firewall en het installeren van antivirus software.
- Het Servicecentrum Logius verwacht dat klanten aangesloten blijven op de preproductie-omgeving, ook na het 'live' gaan van de webdienst. De aansluiting op de preproductie-omgeving is noodzakelijk om wijzigingen en nieuwe webdiensten (ook in de toekomst) te kunnen testen.
- De authenticiteit van u en de vertrouwelijkheid van communicatie tussen u en DigiD wordt gewaarborgd door gebruik te maken van een SSL verbinding. U bent verantwoordelijk voor het verkrijgen van een geldig services certificaat (SSL) conform PKIoverheid. Zie bijlage SSL certificaat.
- Het Servicecentrum Logius adviseert klanten om haar gebruikers te informeren over bestaande risico's en gebruikersverantwoordelijkheden die passen bij elektronische dienstverlening. Denk aan:
    - De mogelijkheid om een certificaat te controleren en uit te kijken voor 'phishing' aanvallen (bij een phishingaanval worden gebruikers omgeleid naar een nagemaakte website alwaar gegevens worden 'gestolen'(ontfutseld));

    - De noodzaak voor gebruikers om zorgvuldig om te gaan met hun DigiD gebruikersnaam met wachtwoord.
- DigiD verifieert de identiteit van gebruikers voor u. DigiD draagt echter geen verantwoordelijkheid voor autorisaties van gebruikers. DigiD koppelt dus alleen een uniek nummer (BSN of A-nummer) terug aan de webdienst, toegang tot delen van de website worden door de webdienst afgedwongen. U dient na een authenticatie van een gebruiker door DigiD zelf te bepalen waartoe deze gebruiker wordt geautoriseerd.
- Om een Denial-of-Service aanval (DoS attack) te voorkomen, raadt het Servicecentrum Logius u aan passende aandacht te besteden aan de preventie en detectie van dergelijke aanvallen en een opvolgingsproces te implementeren.
- U houdt bij wanneer de gebruikte SSL client- en server certificaten verlopen. Certificaten uitgegeven door PKIoverheid gaan maximaal drie jaar mee. Voor de continuïteit van de dienst is het belangrijk dat u tijdig zijn certificaten vernieuwt.

5 Aansluitprocedure

In dit hoofdstuk wordt ingegaan op de aansluitprocedure. Alle benodigde documentatie om aan te sluiten kunt u vinden op www.logius.nl/digid onder documentatie.

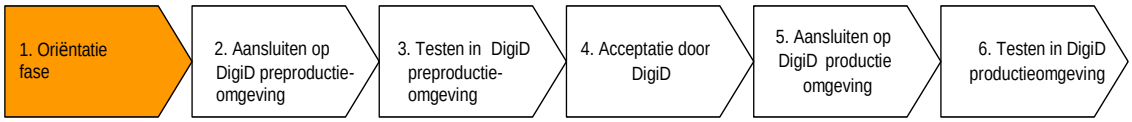
De doorlooptijd van het aansluittraject is afhankelijk van een aantal aspecten:

- u en/of leverancier zelf,
- de aanvraag van het PKIoverheid-certificaten,
- TNT post,
- drukte bij het Servicecentrum Logius.

Als de preproductie-omgeving klaar staat om door Logius getest te worden, duurt het maximaal 5 werkdagen voordat u/leverancier een terugkoppeling krijgt in de vorm van een testrapport.
Als alles goed staat in de preproductie-omgeving, kan u/leverancier door naar de productieomgeving. Hiervoor is een ingevuld Aansluitformulier Productieomgeving nodig, de originele versie moet per post worden geretourneerd aan het Servicecentrum Logius.

Vragen?
Bij vragen over het aansluiten op de DigiD omgeving kan u contact opnemen met het Servicecentrum Logius.

5.1 STAP 1: Oriëntatie fase



5.1.1 Bepalen zekerheidsniveau

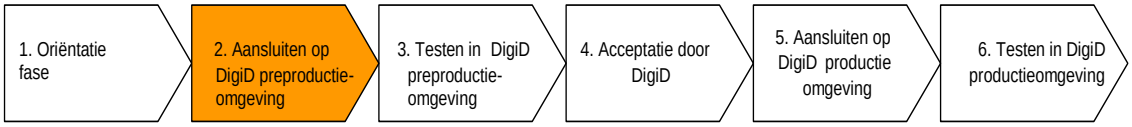
Bepalen wat het gewenste zekerheidsniveau van de authenticatie moet zijn. Zie hiervoor hoofdstuk 3.

5.1.2 PKIoverheid-certificaten aanvragen

Bepaal of er PKIoverheid-certificaten bij een certificaatuitgever aangevraagd moeten worden of controleer of bestaande PKIoverheid-certificaten hergebruikt kunnen worden. Via http://www.pkioverheid.nl kunt u informatie vinden over het PKIoverheid-certificaat.

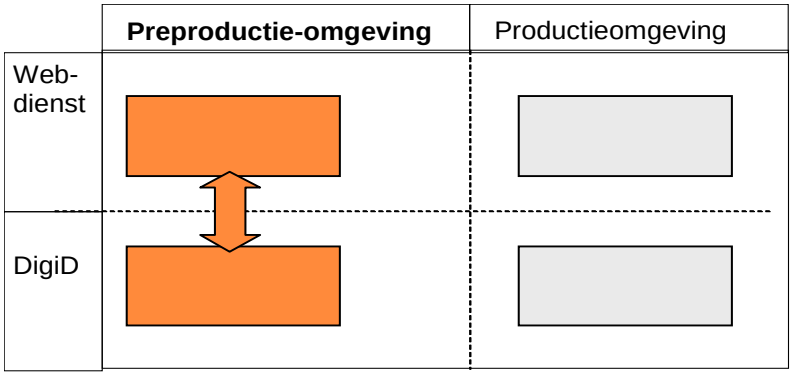
Het is wenselijk om deze activiteit zo vroeg mogelijk in het implementatieproces te starten. Dit is omdat de initiële registratie als abonnee een aantal weken kan duren. Als uw organisatie al abonnee is van een PKIoverheid certificaat verstrekker zal uitgifte veel sneller verlopen.

5.2 STAP 2: Aansluiten op DigiD preproductie-omgeving



Logius stelt een preproductie-omgeving aan u beschikbaar om de koppeling met DigiD te kunnen ontwikkelen en testen. Er is dus een separate preproductie-omgeving voor DigiD.

Logius gaat ervan uit dat u voor zijn webdienst – net als de Logius – naast de productieomgeving een aparte ontwikkel-/preproductie-omgeving heeft gerealiseerd (zie figuur 4).



Figuur 4: Aansluiten op DigiD preproductie-omgeving

In deze stap van de aansluitprocedure test u de koppeling tussen de gerealiseerde preproductie-omgeving van de webdienst en de preproductie-omgeving van DigiD (zie figuur 4).

Voor de preproductie-omgeving kunt u een services certificaat (SSL) van uw webdienst installeren op uw webserver.
Voor het gebruik van de WSDL-koppeling dient u ook een client-certificaat (SSL) te gebruiken voor tweezijdige authenticatie.

N.B. Bij het aansluiten op de DigiD productieomgeving bent u verplicht een SSL-certificaat op basis van PKIoverheid te gebruiken! Houd rekening met de doorlooptijd van de bestelprocedure van de SSL-certificaten.

5.2.1 *Aanvraagformulier Preproductie-omgeving insturen*

Voor u toegang kunt krijgen tot de preproductie-omgeving van DigiD moet u het Aansluitformulier preproductie-omgeving invullen en opsturen naar het Servicecentrum Logius. Deze is te vinden op www.logius.nl/digid onder documentatie. De tijdsduur tussen de ontvangst van het Aansluitformulier preproductie-omgeving en uw ontvangst van het Testpakket door u bedraagt maximaal 5 werkdagen.

Het Aansluitformulier preproductie-omgeving wordt door het Servicecentrum Logius gecontroleerd op juistheid en volledigheid. Is aan deze eisen niet voldaan, dan koppelt het Servicecentrum Logius aan u terug welke gegevens ontbreken of onjuist zijn. Indien het formulier correct en volledig is ingevuld, ontvangt u het DigiD Testpakket. Dit pakket bevat de technische gegevens om aan te kunnen sluiten en u ontvangt daarbij de Application Programming Interface (API).

Technische aansluiting

U kunt nu uw webdienst gaan ontwikkelen. Gebruik daarbij:

1. Application Programming Interface (API);
2. Checklist Testen;

3. Toolkit Communicatie .

Ad 1) De Application Programming Interface (API) geeft technische informatie waarmee authenticatie van de webdienst bij DigiD kan worden gerealiseerd.

Ad 2) De Checklist Testen bevat alle technische en functionele criteria die door DigiD worden vereist. U moet zich ervan verzekeren, dat de webdienst aan alle criteria voldoet. Dit omdat DigiD uw aansluiting zal testen aan de hand van de criteria uit de Checklist Testen. Indien niet wordt voldaan moet de webdienst alsnog worden aangepast conform de criteria. Alleen als de test 100% goed is doorlopen mag de webdienst op de productie-omgeving van DigiD worden aangesloten.
Klanten die niet direct voldoen aan de criteria van de Checklist Testen vertragen daarmee zelf hun aansluitproces.

Logius raadt u sterk aan om de controles in de Checklist Testen volledig en zorgvuldig uit te voeren. Hiermee wordt namelijk de kans op een succesvolle aansluiting op de productieomgeving zonder vertraging aanzienlijk vergroot. U bent zelf verantwoordelijk voor het uitvoeren van de controles.

Let op dat zaken als firewalls, proxies, DNS, IP-ranges goed zijn ingesteld. Let ook op dat proxies en firewalls geschikt zijn voor verkeer met tweezijdige PKIauthenticatie als er gebruik gemaakt wordt van Eenmalig inloggen en DigiD met de WSDL koppeling.

Ad 3) Voor verwijzingen op uw webdienst naar DigiD en teksten waarin wordt gesproken over DigiD, dient u gebruik te maken van teksten uit de Toolkit Communicatie. Het Servicecentrum Logius beoordeelt in stap 4 de gehele website (openbaar gedeelte) van u, dus niet alleen het gedeelte van waaruit de gebruiker naar DigiD wordt doorverwezen. De benodigde tijd voor het testen door u, hangt sterk af van de complexiteit van de situatie en de ervaring die u heeft met de materie.

5.2.2 Eenmalig inloggen

Indien u gebruik maakt van Eenmalig inloggen zijn de volgende stappen noodzakelijk.

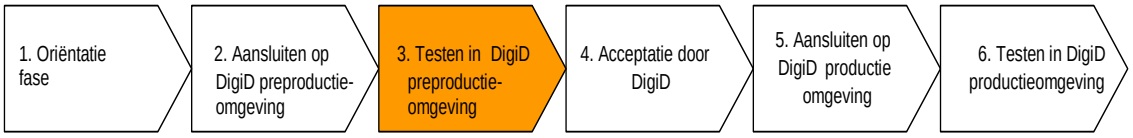
Voor Eenmalig inloggen wordt de technologie SAML 2.0 gebruikt. U kan kiezen hoe u SAML 2.0 technologie aanschaft:

- Selecteer een softwaresysteem uit de markt dat een conformiteitsverklaring voor SAML2.0 heeft. Als het systeem nog geen conformiteitstoets doorlopen heeft, ga dan na of en wanneer dit gaat gebeuren.
- Ontwikkel zelf een software systeem en doorloop daarmee de conformiteitstoets van de Eenmalig inloggen Federatie beheerorganisatie.

Advies van DigiD is om verschillende leveranciers hun product aan u te laten demonstreren.

Eenmaal tot een keuze gekomen, plaatst u de ingekochte of zelf ontwikkelde software binnen uw eigen omgeving en integreert het met de bestaande applicaties.

5.3 STAP 3: Testen door u in DigiD preproductie-omgeving



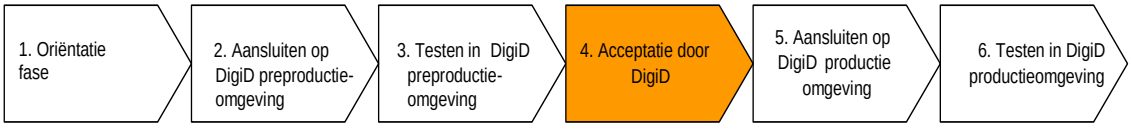
Logius gaat er vanuit dat u tijdens het testen gebruik maakt van een preproductie-omgeving, die **gelijk** is aan de toekomstige productieomgeving van de webdienst.

Eenmalig inloggen: Toegangstest op netwerkniveau
De testkoppeling van de DigiD Eenmalig inloggen Federatie is te vinden op: **test.federatie.overheid.nl**. Al het verkeer dat niet afkomstig is van een IP-adres dat toegelaten wordt door de firewall wordt geblokkeerd. Aandachtspunt hierbij is om te controleren of het IP-adres van uw systeem en dus een verbinding mogelijk is, kunt u gebruik maken van het "ping" commando.

Toegangstest met het PKIoverheid-certificaat
Het PKIoverheid-certificaat dat u van de certificaatverstrekker heeft ontvangen, bevat een publiek deel met de identificerende gegevens van uw organisatie. Om toegang te krijgen tot de SSO Federatie dient u eenmalig deze identificerende gegevens (het publieke deel) via metadata te verstrekken aan de federatie.

Toegangstest met de WSDL-koppeling
Indien u gebruik wilt maken van de WSDL-koppeling met DigiD, dient u dit publieke deel te verstrekken aan Logius. Voor de koppeling met de preproductie-omgeving mag ook gebruikt gemaakt worden van een self-signed certificaat.

5.4 STAP 4: Acceptatie door DigiD



U zorgt ervoor dat hij zijn webdienst in zijn preproductie-omgeving brengt en meldt dit aan Logius. U dient tijdig te zorgen voor een preproductie-omgeving van waaruit naar buiten kan worden gecommuniceerd. En welke vanuit operationeel beheer benaderbaar is.

5.4.1 Testen

U kunt een test aanvragen door een e-mail te sturen of telefonisch contact op te nemen met het Servicecentrum. Daarbij dient u de te testen URL, webdiensten en inloggegevens te verstrekken, zo kan het Servicecentrum Logius op basis van de criteria in de Checklist Testen beoordelen of de webdienst daadwerkelijk aan alle voorwaarden voldoet om aangesloten te mogen worden op de productieomgeving van DigiD.

Voorwaarden

- Logius gaat ervan uit dat uw webdienst, die door Logius in deze stap wordt beoordeeld, daadwerkelijk productierijp is en qua technische, functionele en communicatieve criteria niet afwijkt van de definitieve webdienst. De aansluiting van uw webdienst op

DigiD kan ernstige vertraging oplopen als u uw webdienst ter beoordeling aanbiedt, terwijl de definitieve versie mogelijk niet gaat voldoen aan de gestelde criteria.
- U zorgt ervoor dat het gedeelte van de webdienst, van waaruit wordt doorverwezen naar DigiD, niet toegankelijk is voor gebruikers van de webdienst of dat er duidelijk is aangegeven dat het een testsite betreft.
- U dient uw medewerking te verlenen aan Logius om het testen mogelijk te maken. Hiervoor kan het zijn dat er aanpassingen noodzakelijk zijn aan uw technische infrastructuur om Logius toegang te bieden tot uw acceptatieomgeving, bijvoorbeeld firewall instellingen.

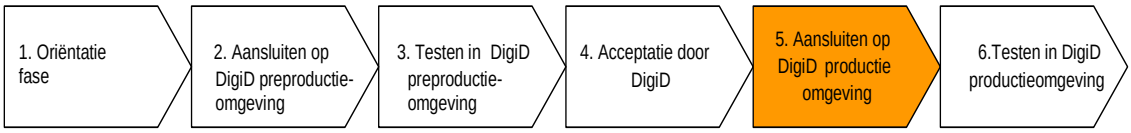
5.4.2 Terugkoppelen testen

Het Servicecentrum Logius koppelt eventuele tekortkomingen van de webdienst terug aan u, door middel van een testrapport. De doorlooptijd van het testen bedraagt maximaal 5 werkdagen. Nadat de tekortkomingen eerst door u worden opgelost volgt opnieuw een volledige test aan de hand van Checklist Testen. Deze wordt tevens teruggekoppeld per mail.

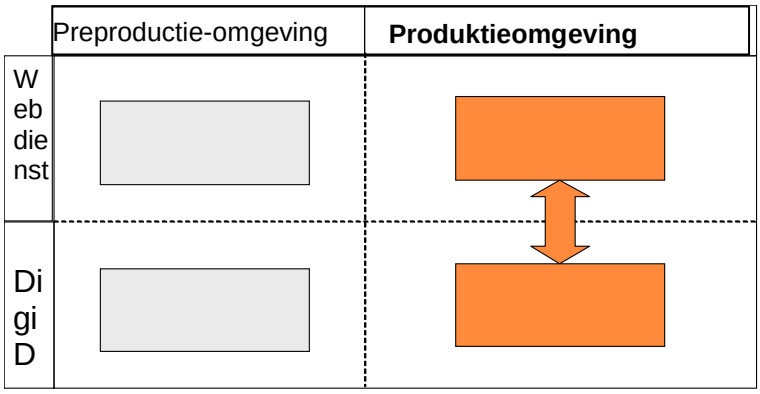
5.4.3 Aansluitformulier productieomgeving

Indien alle punten uit de Checklist Testen goed zijn bevonden krijgt u per mail het Aansluitformulier Productie en de Aansluitvoorwaarden Productieomgeving. Dan moet het ingevulde Aansluitformulier Productieomgeving worden verstuurd naar het Servicecentrum Logius.

5.5 STAP 5: Aansluiten op DigiD productieomgeving



Indien DigiD heeft vastgesteld dat de webdienst aan alle criteria voldoet kan u op de gewenste datum worden aansluiten.



Figuur 5: Aansluiten op DigiD productieomgeving

5.5.1 Aansluitpakket Productieomgeving

U dient in uw productieomgeving, via de nieuw verstrekte URL, te verwijzen naar de DigiD productieomgeving. De nieuwe URL, maar ook

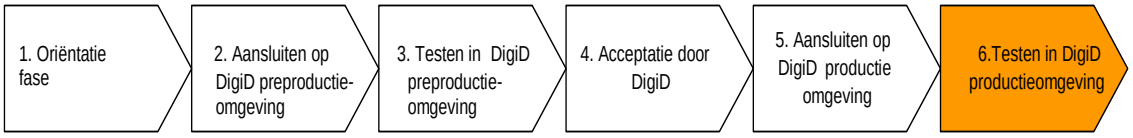
andere nieuwe gegevens die u voor de aansluiting nodig hebt, ontvangt u in het Aansluitpakket Productieomgeving.

Als de gegevens voor de productieomgeving zijn verstuurd, kunt u beginnen met het omzetten van de preproductie-omgeving naar de productieomgeving. Als er contact gemaakt moet worden met de DigiD server ontvangt u resultcode 0099. Dit betekent dat de webdienst nog niet geactiveerd is. Neemt u dan contact op met het Servicecentrum Logius. Het Servicecentrum Logius activeert de webdienst. Op dat moment is voor DigiD de webdienst live.

5.5.2 Eenmalig inloggen: Bevestigingsbrief Productieomgeving

Na het invullen en versturen van het Aansluitformulier Productieomgeving ontvangt u een bevestigingsbrief van het Servicecentrum Logius. Indien u heeft aangegeven dat een bestaande aansluiting DigiD wordt vervangen door de aansluiting op Eenmalig inloggen staat de aansluiting die wordt gedeactiveerd nogmaals vernoemd.

5.6 STAP 6: Testen in DigiD Productieomgeving



Het Servicecentrum Logius beoordeelt vervolgens, aan de hand van de Checklist Testen, nogmaals of de productieomgeving van de webdienst voldoet aan de functionele en communicatiecriteria.

N.B. Indien de webdienst in functioneel opzicht verschilt met de webdienst, die DigiD in stap 4 heeft geaccepteerd, moet de beoordeling door het Servicecentrum Logius van de webdienst opnieuw plaatsvinden. De aansluiting van uw webdienst op DigiD kan hierdoor ernstige vertraging oplopen.

Het Servicecentrum Logius verstuurt haar bevindingen naar u. Het Servicecentrum Logius meldt u of de webdienst communicatieve of functionele tekortkomingen heeft die u eerst moet oplossen. Indien niet is voldaan aan alle criteria, koppelt Logius de webdienst af van de DigiD productieomgeving. Logius stelt u hiervan op de hoogte. Indien de webdienst aan alle criteria voldoet, blijft de productieomgeving van de webdienst op de DigiD productieomgeving aangesloten.

U zorgt ervoor dat het gedeelte van de webdienst, van waaruit is doorverwezen naar DigiD, toegankelijk wordt voor gebruikers van de webdienst. De webdienst is hiermee live gegaan in de DigiD productieomgeving.

Het Servicecentrum Logius verwacht dat u ook aangesloten blijft op de preproductie-omgeving, ook na het activeren van de webdienst. De aansluiting op de preproductie-omgeving is noodzakelijk om wijzigingen en nieuwe webdiensten in de toekomst te kunnen testen.

6 Operationeel

6.1 Monitoring

Nadat een klant is aangesloten op DigiD, bewaakt het Servicecentrum Logius continu de status van de aansluiting van webdiensten op DigiD.

Steekproefsgewijs worden de websites van klanten bezocht, om te onderzoeken of deze nog voldoen aan de technische, functionele en communicatiecriteria zoals gesteld in de Checklist Testen. Indien blijkt dat dit niet het geval is, kan Logius besluiten om de webdienst te ontkoppelen. Verder kan tijdens het hertesten blijken dat een webdienst onveilig functioneert (bijv. schade kan toebrengen aan vertrouwelijke informatie). Dit kan bijvoorbeeld blijken uit beveiligingsincidenten die over een webdienst worden gemeld. Indien de webdienst onveilig functioneert wordt de webdienst ontkoppeld. Zie hoofdstuk 7 Ontkoppelen webdienst van DigiD.

6.2 Wijzigingsbeheer

6.2.1 Wijzigingen aan bestaande webdienst

Afnemers dienen wijzigingen aan hun webdiensten te melden bij het Servicecentrum Logius. Indien de wijziging aanzienlijke invloed zou kunnen hebben op de dienstverlening (denk aan sterke verhoging aantallen gebruikers, hoge eenmalige piekmomenten), dient dit vooraf met het Servicecentrum Logius te worden afgestemd. Bij ontvangst van een melding van een wijziging wordt door het Servicecentrum Logius opnieuw getest om vast te stellen of de kwaliteit en veiligheid van de gewijzigde webdienst in orde zijn.

6.2.2 Nieuwe webdienst bij reeds aangesloten klant

Indien een klant, die al één of meerdere webdiensten op één van de domeinen heeft aangesloten, een nieuwe webdienst wil aansluiten op hetzelfde domein, dient deze klant de aansluitprocedure vanaf stap 3 opnieuw te doorlopen.

Neem hiervoor contact op met het Servicecentrum Logius.

7 Ontkoppelen webdienst van DigiD

Er kunnen situaties ontstaan waardoor de webdienst wordt afgesloten van DigiD. Er kunnen drie redenen zijn waarom een klant wordt afgesloten van DigiD:

1. U besluit geen gebruik meer te maken van DigiD; u meldt aan het Servicecentrum Logius dat u voornemens bent om geen gebruik meer te maken van DigiD. Het Servicecentrum Logius informeert de accountmanager. Logius sluit vervolgens de webdienst af van DigiD. U zorgt ervoor dat alle communicatiemiddelen t.n.v. DigiD van haar website worden gehaald.

2. Als naar aanleiding van een testrapport in de productie omgeving blijkt dat de webdienst niet voldoet aan de eisen, wordt dit door het Servicecentrum Logius gemeld aan u. Het Servicecentrum Logius komt met u een aantal maatregelen overeen, waardoor u wel voldoet aan de Aansluitvoorwaarden. Het Servicecentrum Logius informeert de accountmanager.
   U treft maatregelen en neemt contact op met het Servicecentrum Logius over de genomen maatregelen. Het Servicecentrum Logius stemt met DigiD Tactisch Beheer af of de genomen maatregelen voldoende zijn. Indien de genomen maatregelen niet volstaan, wordt overgegaan tot het afsluiten van de webdienst en wordt u hiervan op de hoogte gesteld. Het Servicecentrum Logius informeert de accountmanager.

3. Het Servicecentrum Logius constateert een acuut beveiligingsincident en sluit de webdienst van DigiD af. U en de accountmanager worden hiervan door het Servicecentrum Logius direct op de hoogte gesteld.
   Het Servicecentrum Logius brengt DigiD Tactisch Beheer op de hoogte van het beveiligingsincident. Het Servicecentrum Logius stemt met DigiD Tactisch Beheer af welke maatregelen door u moeten worden uitgevoerd, om weer te worden aangesloten. Tevens bespreekt het Servicecentrum Logius met u welke maatregelen moeten worden getroffen om herhaling te voorkomen.
   U treft de overeengekomen maatregelen en neemt contact op met het Servicecentrum Logius over de genomen maatregelen. Het Servicecentrum Logius stemt met DigiD Tactisch Beheer af of de genomen maatregelen voldoende zijn. Indien de genomen maatregelen volstaan, wordt overgegaan tot het weer aansluiten van de webdienst en wordt u hiervan op de hoogte gesteld. Het Servicecentrum Logius informeert uw accountmanager.