Ministerie van Volksgezondheid,
Welzijn en Sport

# Digitale toegang in de Zorg

## Factsheet DigiD-assessments

Verder

# Waarom een (meervoudig) DigiD-assessment ?

## Het (DigiD) assessment

Aan een aansluiting op DigiD zijn beveiligingseisen verbonden, bedoeld om de integriteit van de bestaande infrastructuur te kunnen blijven garanderen. Via een jaarlijkse audit, ook wel assessment genoemd, toont u aan te voldoen aan de gestelde eisen. Deze verplichting is opgenomen in de aansluitvoorwaarden van DigiD en maakt ook onderdeel uit van de Wet digitale overheid. Nadat deze in werking is getreden geldt de auditplicht voor het gehele eID-stelsel. Voor de duidelijkheid refereren we naar het assessment als 'DigiD-assessment'.

De uitvoering van een assessment vraagt samenwerking tussen zorgaanbieder en ICT-leverancier en moet uitgevoerd worden door een gekwalificeerde en onafhankelijke IT-auditor (RE). We adviseren daarom altijd om even contact met elkaar te hebben en acties af te stemmen.

**Belangrijk:**
Ongeacht het type aansluiting DigiD blijft de zorgaanbieder er altijd verantwoordelijk voor dat het assessment tijdig plaatsvindt. De uitvoering daarvan kan – afhankelijk van het type aansluiting – gedelegeerd worden aan de ICT-leverancier.

Het assessment vindt pas plaats als de DigiD-aansluiting is geactiveerd ('in productie genomen') maar moet binnen twee maanden na activatie zijn afgerond.

## Typen DigiD-aansluitingen

Een zorgaanbieder kan voor een aansluiting op DigiD kiezen uit verschillende opties:

- Een directe aansluiting.
- Een clusteraansluiting.

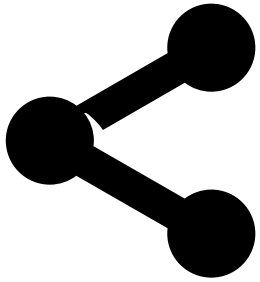
Afhankelijk van de keuze van aansluiting is het de zorgaanbieder *of* de ICT-leverancier die de verschillende stappen in het aansluitproces doorloopt. Ook op gebied van het assessment kan die taakverdeling er per variant anders uitzien. Om duidelijkheid te bieden in wat er moet gebeuren en wie dat moet doen, zijn de stappen per DigiD-aansluiting uitgewerkt.

Behalve de *zorgaanbieder* en de *ICT-leverancier* spelen twee andere partijen een rol: *Logius* is, als onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de beheerder van de DigiD-infrastructuur en functionaliteit. Ook houdt Logius toezicht op de aangesloten organisaties en beoordeelt zij de rapporten die naar aanleiding van de (meervoudige) assessments zijn afgegeven door de auditor.

*DICTU* is de aanbieder van de routeringsdienst TVS (ToegangverleningService). Een aansluiting op TVS betekent tevens een aansluiting op DigiD. Zie voor verdere informatie de factsheet TVS.

# *Flow (meervoudig) assessment*

*Klik op een knop voor meer info!*



***Directe aansluiting***

Hiervoor geldt een enkelvoudig assessment

***Clusteraansluiting***

Hiervoor geldt het meervoudig assessment

Kies, afhankelijk van de DigiD-aansluiting die u voor ogen heeft, het bij behorende stappenplan voor een assessment:

**Directe aansluiting**: enkelvoudig assessment

**Clusteraansluiting**: meervoudig assessment (onder voorwaarden)

# Directe aansluiting

Een directe aansluiting op DigiD vraagt om een enkelvoudig assessment. In onderstaand schema ziet u welke stappen moeten worden doorlopen en wie deze moet zetten: de zorgaanbieder of de ICT-leverancier. Om u goed op het DigiD-assessment voor te bereiden is er de mogelijkheid om u in de materie te verdiepen aan de hand van (online) bijeenkomsten en de beschikbare documentatie.

De verantwoordelijkheid voor het (tijdig) laten uitvoeren van dit assessment ligt altijd bij de zorgaanbieder. Afhankelijk van de wensen kunnen de stappen 2, 3 en 4 gedelegeerd worden aan de ICT-leverancier.

Klik op een knop voor meer info!

**Zorgaanbieder**

**Stap 1**
kennisnemen van eisen

**Stap 3**
Laten uitvoeren DigiD-assessment

**Stap 5**
Laten uitvoeren penetratietest

**Stap 7**
Indienen auditrapportage

**Leverancier**

**Stap 2**
Voorbereiden op DigiD-assessment

**Stap 4**
Meewerken aan DigiD-assessment

**Stap 6**
Meewerken aan penetratietest

# Stap 1

## Kennisnemen van eisen enkelvoudig assessment

### De eisen waar uw eigen organisatie en die van de ICT - leverancier aan moeten voldoen

Als zorgaanbieder wilt u aansluiten op DigiD. Uw organisatie dient daarvoor aan een aantal voorwaarden te voldoen. Afhankelijk van de vraag of en in welke mate u gebruik maakt van een serviceorganisatie of ICT- leverancier (software-oplossing, hosting, netwerkinfrastructuur), zal ook deze door u in meer of mindere mate betrokken moeten worden bij het DigiD-assessment. Neem tijdig kennis van de aspecten die tijdens het DigiD-assessment worden getoetst en ga na of aan alle normen wordt voldaan. Dit geldt ook voor de serviceorganisatie of ICT- leverancier waarvan u diensten afneemt.

Het advies is om in overleg met de ICT- leverancier en de geselecteerde IT-auditor een pre-assessment uit te laten voeren. Hiermee voorkomt u verrassingen tijdens het eigenlijke assessment.

- *Het normenkader en de verdere voorwaarden zijn gedetailleerd beschreven en terug te lezen op de website van Logius.*
- *Het document 'Handreiking DigiD-assessment 2.0 (testaanpak update 2020) versie 1.0' is te vinden op de website van NOREA.*
- *Een gekwalificeerde IT-auditor (RE) vindt u hier.*

### Actiepunten

- Ga in overleg met de auditor na of je leverancier beschikt over een Third Party Memo (TPM). Als dat het geval is, dan hoeft de leverancier mogelijk niet alle stappen uit het stappenplan te doorlopen. Dat scheelt wellicht niet alleen tijd maar ook kosten!
- Een IT-auditor (RE) selecteren in overleg met de ICT-leverancier.
- Voer een gap-analyse uit t.o.v. de normen zoals opgenomen in de handreiking.
- Vaststellen van de scope van het assessment (met de auditor en de ICT-leverancier).
- Plan met de auditor een pre-assessment en laat deze uitvoeren.

*Let op: u bent als zorgaanbieder zelf verantwoordelijk voor de uitvoering van het assessment en voor het eventueel nemen van maatregelen op basis van het resultaat uit het assessment. U dient er zelf voor te zorgen dat uw leverancier hieraan meewerkt.*

# Stap 2

## Voorbereiden op meewerken DigiD-assessment

**Vaststellen welke eisen in het kader van het enkelvoudig assessment worden gesteld aan uw organisatie (contractueel, procedureel en technisch).**

Eén van uw klanten (zorgaanbieder) heeft het voornemen aan te sluiten op DigiD. De zorgaanbieder gebruikt uw software-oplossing en/of ict-infrastructuur. Het uit te voeren DigiD-assessment richt zich daarom (deels) op uw organisatie. Overleg met de door de zorgaanbieder geselecteerde auditor of een pre-assessment noodzakelijk is. Dit is vooral relevant als in uw organisatie niet eerder een DigiD-assessment is uitgevoerd. Wij adviseren tijdig een pre-assessment te plannen. Dit levert een goed beeld op dat behulpzaam is bij het vaststellen van de mate waarin uw softwareoplossing en/of ict-infrastructuur al voldoet aan de eisen van het DigiD-assessment . Daarvóór is het raadzaam al een gap-analyse uit te voeren; dit doet u op basis van de eisen Enkelvoudig DigiD-assessment zoals vastgelegd in de 'Handreiking DigiD-assessment 2.0 (testaanpak update 2020) versie 1.0.'

- *Het proces en de voorwaarden zijn gedetailleerd beschreven en terug te lezen op de website van Logius.*
- *Het document 'Handreiking DigiD-assessment 2.0 (testaanpak update 2020) versie 1.0' is te vinden op de website van NOREA.*

**Actiepunten**

- Op verzoek van de zorgaanbieder kennisnemen van de eisen enkelvoudig DigiD-assessment.
- Opstellen van een gap-analyse.
- Plan, indien van toepassing, een pre-assessment en laat deze uitvoeren.
- Opstellen van een actieplan om op basis van de gap-analyse en de resultaten van de pre-audit eventuele tekortkomingen op te heffen.

*Directe aansluiting* *Clusteraansluiting*

# Stap 3

## Laten uitvoeren DigiD-assessment

**U toont aan dat wordt voldaan aan de gestelde technische beveiligingseisen.**
U laat een penetratietest uitvoeren om aan te tonen dat de organisatie technisch (qua infrastructuur en applicatie) voldoet aan de gestelde eisen. De penetratietest richt zich op de daadwerkelijke aanwezigheid en juiste instelling van een aantal technische beveiligingseisen in de infrastructuur en applicatie(s). De uitkomsten worden door de IT-auditor betrokken in het assessment.

De scope van de penetratietest omvat tenminste de webapplicatie en de infrastructuur voor het netwerksegment met de webapplicatie van de algemene routeringsvoorziening (zoals bijvoorbeeld TVS). Het DigiD-assessment kent specifieke eisen voor de uitvoering van de penetratietest. Kijk op *de website van NOREA* voor meer informatie.

**Actiepunten**
- Verzoek je leverancier om een penetratietest uit te laten voeren.
- Zie er op toe dat de benodigde activiteiten worden uitgevoerd.

Directe aansluiting

Clusteraansluiting

# Stap 4

## Meewerken aan DigiD-assessment

**Vaststellen of vereiste beveiligingsinstellingen in de ICT-infrastructuur aanwezig - en juist geconfigureerd zijn.**

Voorafgaand aan het DigiD-assessment wordt door een gespecialiseerde partij een penetratietest uitgevoerd, die zich richt op de daadwerkelijke aanwezigheid en de juiste instellingen van een aantal technische vereisten in de infrastructuur. De scope van de penetratietest omvat tenminste de webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie.

**Actiepunten**

- Selecteer een gespecialiseerde partij om de penetratietest uit te voeren desgewenst in overleg met de auditor.
- Op verzoek van de zorgaanbieder een penetratietest plannen en deze laten uitvoeren.
- Opstellen van een actieplan om eventuele tekortkomingen op te heffen.

*Directe aansluiting* *Clusteraansluiting*

# Stap 5

## Laten uitvoeren penetratietest

**U toont aan dat uw organisatie en die van uw leverancier(s) voldoen aan de beveiligingseisen die worden gesteld om op de algemene routeringsvoorziening (bijv. TVS)/DigiD te mogen aansluiten.**
Door het laten uitvoeren van een DigiD-assessment door een gekwalificeerde en onafhankelijke auditor (RE) toont u aan dat uw organisatie en die van de ICT-leverancier waarvan u gebruik maakt, voldoen aan de technische en procedurele eisen die hier conform de Handreiking DigiD-assessment aan worden gesteld.

**Let op:** Het assessment kan pas plaatsvinden ***nadat*** de DigiD - aansluiting(en) geactiveerd zijn (in 'productie') en moet zijn afgerond **binnen twee maanden nadat** de aansluitingen zijn geactiveerd.

**Actiepunten**
- Verzoek uw leverancier om mee te werken aan het DigiD-assessment.
- Zie er op toe dat de benodigde activiteiten worden uitgevoerd.

# Stap 6

## Meewerken aan penetratietest

**U toont aan dat de softwareoplossing en de ICT-infrastructuur waarvan deze gebruik maakt, voldoen aan de daaraan gestelde eisen.**

De IT-auditor voert namens de zorgaanbieder het DigiD-assessment (deels) binnen uw organisatie uit. Op basis van het concept-assessmentrapport en in overleg met de auditor stelt u een plan op om eventuele bevindingen te adresseren.
Het definitieve rapport met het verbeterplan stuurt de zorgaanbieder naar Logius.
Let op: Als uw organisatie in het bezit is van een relevante, eerder opgestelde Third Party Mededeling (TPM) die betrekking heeft op (onderdelen van) het DigiD-assessment, dan kan deze verklaring - in overleg met de auditor - worden gebruikt om aan te tonen dat aan die eisen van het assessment wordt voldaan.

**Let op**: Het assessment kan pas plaatsvinden ***nadat*** de DigiD - aansluiting(en) geactiveerd zijn (in 'productie') en moet zijn afgerond **binnen twee maanden nadat** de aansluitingen zijn geactiveerd.

### Actiepunten

- Faciliteer het enkelvoudig DigiD-assessment dat namens de zorgaanbieder wordt uitgevoerd of lever een geldige TPM aan met betrekking tot de softwareoplossing die de zorgaanbieder af neemt.
- Stel indien nodig in overleg met de auditor een verbeterplan op.

Directe aansluiting Clusteraansluiting

# Stap 7

## Indienen auditrapportage

**Door het inzenden van het auditrapport stelt u Logius op de hoogte van het feit dat een DigiD-assessment heeft plaatsgevonden.**

Uiterlijk twee maanden nadat de aansluiting in productie geactiveerd is, dient het auditrapport bij Logius te zijn ingediend. Hiermee is Logius op de hoogte van het feit dat de audit heeft plaatsgevonden en wat de eventuele geconstateerde afwijkingen t.o.v. de normen zijn. Een planning voor het herstel van deze tekortkomingen dient te worden bijgevoegd.
Het auditrapport kan per e-mail of per post worden ingezonden.

*Zie de webpagina IT-auditrapportage voor DigiD: indienen en vervolgstappen? | Logius voor de adressen en voorwaarden.*

**Actiepunten**

- Zend het definitieve auditrapport naar Logius; dit kan per e-mail of per post.
- Stel aan de hand van een planning vast dat uw organisatie en/of die van de leverancier de gerapporteerde tekortkomingen binnen twee maanden kan herstellen.
- Informeer Logius tijdig, ook in het geval dat de termijn van twee maanden overschreden dreigt te worden.

Directe aansluiting

Clusteraansluiting

# Meer informatie over enkelvoudige assessments

**Relevante documenten en informatie over enkelvoudige assessments**

Meer informatie en relevante documenten zijn is gepubliceerd op de website van Logius.

U vindt hier onder andere:
- Norm ICT beveiligingsassessments DigiD
- Handleiding uitvoering ICT beveiligingsassessment

Ook NOREA heeft verschillende handreikingen opgesteld over het DigiD-assessment.

# Clusteraansluiting

## Meervoudig DigiD-assessment

Klik op een knop voor meer info!

In onderstaand schema ziet u op hoofdlijnen hoe de voorbereiding op en het doen uitvoeren van een meervoudig DigiD-assessment in zijn werk gaat. De dienstverlener selecteert - eventueel in overleg met u - een auditpartij. Om uw organisatie goed op het DigiD-assessment voor te bereiden is er gedetailleerde informatie beschikbaar op de website van Logius (zie link onder 'Stap 1'). Ook de IT-auditor (RE) kan u tijdens de voorbereidingen adviseren.

Bij een clusteraansluiting op DigiD is bijna altijd sprake van sprake van een meervoudig assessment. Dat betekent dat de handelingen om het assessment en de pentest uit te (laten) voeren door de ICT leverancier worden geïnitieerd. Als zorgaanbieder bent en blijft u altijd wel 'de aansluithouder' en daarmee formeel aansprakelijk voor het naleven van de gestelde eisen en het voor juiste gebruik van de aansluiting.

**Zorgaanbieder**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | **Stap 5** Ondertekenen aangepast contract | **Stap 7** Ondertekenen akkoord-verklaring | **Stap 9** Vaststellen uitkomst assessment |

**Leverancier**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Stap 1** Check randvoor-waarden meervou-dig DigiD-assessment | **Stap 2** Zelfverklaring (accreditatie) bij Logius aanvragen | **Stap 3** Voorbereiden DigiD-assessment | **Stap 4** Contract met zorgaanbieder | **Stap 6** Akkoord-verklaring | **Stap 8** DigiD-assessment en penetratietest | **Stap 9** Indienen audit-rapportage | |

# Stap 1

## Check randvoorwaarden meervoudig DigiD-assessment

**Om er zeker van te zijn dat u in aanmerking komt voor een meervoudig DigiD-assessment is het van belang vooraf vast te stellen dat u voldoet aan de gestelde randvoorwaarden.**

De clusteraansluiting voor DigiD kent aanvullende voorwaarden ten opzichte van een enkelvoudige aansluiting.
Dit komt vooral omdat u als leverancier bepaalde verantwoordelijkheden van de zorgaanbieder op zich neemt. Zo vindt het DigiD-assessment geheel bij de leverancier plaats en dient deze zich ervan te overtuigen dat de handelingen van de zorgaanbieders de veiligheid van de aansluiting niet in gevaar (zullen) brengen. Tussen u als leverancier en bij u aangesloten zorgaanbieders dient daarom het vertrouwen te bestaan dat u enerzijds namens de zorgaanbieders de juiste zaken regelt en in stand houdt en anderzijds dat de zorgaanbieder zich aan de afspraken houdt waar het gaat om het juiste gebruik van de aansluiting.

Logius is toezichthouder op het correct gebruik van DigiD en heeft daarom de volgende voorwaarden gesteld aan het mogen uitvoeren van een meervoudig DigiD-assessment:

- De beoogde (SaaS -) softwareoplossing levert standaard functionaliteit die voor alle aan te sluiten zorgaanbieders op dezelfde wijze beschikbaar is. Er is dus geen maatwerk per zorgaanbieder.
- Het assessment dient op één centrale locatie uitgevoerd te kunnen worden.
- Er moeten twee zorgaanbieders via de ICT-leverancier worden aangesloten op DigiD bij aanvang van het meervoudig DigiD-assessment. Op die manier kan de meervoudigheid van de aansluiting worden aangetoond.
- Voor het aansluiten van zorgaanbieders is een standaard werkwijze ingericht.

*De voorwaarden zijn gedetailleerd beschreven en terug te lezen op de website van Logius.*
*Hier zijn ook de benodigde documenten gepubliceerd.*

### Actiepunten

- Vaststellen dat de beoogde (SaaS -) softwareoplossing standaard functionaliteiten levert en centraal (bij u als leverancier) beoordeeld kan worden.
- Zorgdragen dat twee zorgaanbieders bij activatie in productie willen aansluiten (op TVS) voor het testen in (pre)productie en het uitvoeren van het meervoudig assessment.

# Stap 2

## Zelfverklaring (accreditatie) bij Logius aanvragen

**Met de ondertekening van het standaardcontract met Logius verklaart u te voldoen aan de voorwaarden om het meervoudig assessment te mogen toepassen.**

Zoals gesteld bij de vorige stap zijn aan het toepassen van het meervoudig assessment voorwaarden verbonden. In een standaardcontract tussen u als leverancier en Logius worden deze voorwaarden formeel overeengekomen; dit noemen we ook wel de 'accreditatie'. We raden aan hier goed kennis van te nemen om -waar nodig in overleg met de zorgaanbieders - tot een besluit komen over de toepasbaarheid van een clusteraansluiting voor DigiD aansluiting.
Het standaardcontract ('zelfverklaring' of accreditatie) kan vervolgens meteen aan het begin van het aansluitproces bij Logius worden aangevraagd door de leverancier.

In het standaardcontract tussen Logius en de leverancier (*Overeenkomst Logius - Leverancier DigiD*) staan in hoofdstuk 4 'Verplichtingen Leverancier' aan welke zaken de leverancier moet voldoen.

### Actiepunten

**Zelfverklaring (Accreditatie) bij Logius aanvragen**

- U kunt het standaardcontract aanvragen middels het e-mailformat
- Zend de aanvraag vervolgens naar DigiDassessment@Logius.nl
- Laat het door Logius opgestuurde standaardcontract rechtsgeldig ondertekenen (let op de juiste inschrijving bij het KvK van de ondertekenaar).
- Retourneer het ondertekende standaardcontract aan Logius.
- Ontvang het door Logius ondertekende standaardcontract retour.

# Stap 3

## Voorbereiden op het meervoudig DigiD-assessment

**Om er zeker van te zijn dat het meervoudig assessment en het opleveren van de rapportage binnen de geldende termijn (twee maanden na activatie van de productie koppeling) kunnen worden afgerond zijn goede voorbereiding nodig.**

Vanaf het moment dat de eerste twee zorgaanbieder in productie zijn aangesloten, heeft u twee maanden de tijd om het meervoudig assessment te laten uitvoeren en de auditrapportage bij Logius in te dienen. Het advies is om een pre-audit uit te laten voeren. Op die manier kunnen eventuele (grote) tekortkomingen tijdig worden verholpen. Indien u al eerder bij een enkelvoudige DigiD-assessment was betrokken, kan de pre-audit vooral worden gericht op de aanvullende zaken m.b.t. de clusteraansluiting aansluiting. Overleg al deze aspecten met de door u geselecteerde auditor.

*Beschikbare auditors (RE's) zijn te vinden op de website van NOREA (NOREA - de beroepsorganisatie van IT-Auditors).*

### Actiepunten

- Neem kennis van de eisen vermeld in de Handreiking DigiD-assessment 2.0 (update Meervoudige Aansluiting 2020) def. v 1.0.
- Voer een gap-analyse uit t.o.v. de normen in de Handreiking (dit is zeker relevant als er nog geen ervaring is met het DigiD-assessment).
- Selecteer een auditor (RE).
- Stel met de auditor de scope van het assessment vast.
- Plan met de auditor desgewenst een pre-audit en laat deze uitvoeren.

# Stap 4

## Contractformalisatie

**Pas het bestaande contract tussen leverancier en zorgaanbieder aan of stel een nieuw contract op.**
De eisen die Logius aan u als leverancier stelt voor het mogen toepassen van het meervoudig assessment dienen deels opgenomen te zijn in de overeenkomst die u heeft met bij u aangesloten zorgaanbieders. Dit kan door de verplichtingen tussen leverancier en zorgaanbieders (zoals beschreven in het document DigiD 'meervoudige aansluiting verplichtingen LMA AMA') bijvoorbeeld op te nemen in een bijlage bij de bestaande overeenkomst tussen partijen.

**Actiepunten**
- Stel het contract met de deelnemende zorgaanbieders op en onderteken dit wederzijds.
- Zorg dat de voorwaarden uit deze contracten zijn gerealiseerd en dat de zorgaanbieders de relevante onderdelen uit de 'Norm ICT beveiligingsassessment DigiD' naleven.
- Voer een (initiële) dataclassificatie uit of update een bestaande dataclassificatie, zoals vereist in het document DigiD meervoudige aansluiting verplichtingen LMA AMA.

# Stap 5

## Ondertekenen aangepast contract

**De leverancier vult het contract dat u met hen heeft aan met de voorwaarden voor de clusteraansluiting.**
U dient akkoord te gaan met het aangepaste contract. Daarmee machtigt u de leverancier tevens om namens u activiteiten uit te voeren die nodig zijn voor de DigiD-aansluiting. Uw leverancier heeft daarmee ook de plicht en bevoegdheid om de DigiD-aansluiting te deactiveren als blijkt dat u niet aan de gestelde voorwaarden voldoet. De opzet van de cluster-aansluiting is zo, dat de leverancier een groep aan te sluiten zorgaanbieder het (meeste) werk uit handen neemt.
Dit betreft onder andere de formele aanvraag, het afsluiten van een contract met Logius, de technische aansluiting en het laten uitvoeren van het meervoudig assessment. In het contract zijn de onderdelen opgenomen zoals vastgelegd in het document 'DigiD meervoudige aansluiting verplichtingen LMA AMA.pdf', eveneens te vinden op de website van Logius.

**Let op: U blijft als zorgaanbieder verantwoordelijk voor het (doen) uitvoeren van het meervoudig assessment!**

**Let op:** Het assessment kan pas plaatsvinden nadat de twee DigiD-aansluitingen geactiveerd zijn (in 'productie') en moet zijn afgerond binnen twee maanden nadat de aansluitingen zijn geactiveerd.

### Actiepunten

- Onderteken het aangepaste contract.
- Machtig de leverancier tot het doen uitvoeren van een meervoudig assessment.

Door het ondertekenen van de (bijlage van de bestaande) overeenkomst die u met uw leverancier heeft, geeft u hen toestemming om een dataclassificatie uit te voeren.

# Stap 6

## Akkoordverklaring

**De leverancier ziet toe op ondertekening van de akkoordverklaring door de zorgaanbieder.**

U bent door het tekenen van een standaardcontract met Logius (de 'zelfverklaring') en het afsluiten van een overeenkomst met de aan te sluiten zorgaanbieders gerechtigd om - namens deze zorgaanbieders - de meeste zaken in het kader van de clusteraansluiting te regelen. Echter, formeel blijft de zorgaanbieder verantwoordelijk voor het juiste gebruik ervan.
Dit is vastgelegd in de 'akkoordverklaring' die de zorgaanbieder ondertekent, voordat de aansluiting op DigiD plaatsvindt. Zij sturen deze akkoordverklaring(en) aan hun leverancier toe. De leverancier dient ze op hun beurt in bij DICTU.

Voor een vlot verloop van het aansluitproces is het van belang dat de zorgaanbieder:
- Zorgt voor een correcte (actuele) KVK-vermelding met daarin de juiste tekenbevoegden.
- De beschikbaarheid van de tekenbevoegden voor ondertekening van de akkoordverklaring regelt.
- Tijdig kennisneemt van - en akkoord gaat met de aansluitvoorwaarden.

**Actiepunten**

- Stel het contract met de deelnemende zorgaanbieders op en onderteken dit wederzijds.
- Lever de akkoordverklaring aan bij de zorgaanbieder met verzoek deze te ondertekenen.
- Verzamel ondertekende akkoordverklaringen en dien ze in bij DICTU.
- Zorg dat de voorwaarden uit deze contracten zijn gerealiseerd en dat de zorgaanbieders de relevante onderdelen uit de 'Norm ICT beveiligingsassessment DigiD' naleven.
- Voer een (initiële) dataclassificatie uit of update een bestaande dataclassificatie, zoals vereist in het document DigiD meervoudige aansluiting verplichtingen LMA AMA.

Directe aansluiting

Clusteraansluiting

# Stap 7

## Ondertekenen akkoordverklaring

**Onderteken de akkoordverklaring en geef daarmee aan dat u de voorwaarden voor het (juiste) gebruik van de meervoudige DigiD-aansluiting kent en deze zult naleven.**

Behalve met uw leverancier sluit u ook een overeenkomst met Dictu, de zogenaamde 'akkoordverklaring'. U bent de feitelijke houder van de DigiD aansluiting op TVS en dus verantwoordelijk voor het juiste gebruik ervan. Met het ondertekenen van de akkoordverklaring verklaart u te zullen (blijven) voldoen aan de 'Algemene aansluitvoorwaarden TVS', een algemene routeringsvoorziening, zoals deze zijn te vinden op de website van Dictu.

### Actiepunten

- Onderteken de akkoordverklaring en stuur deze terug naar uw leverancier.

Voor een vlot verloop van het aansluitproces is het van belang dat u:

- Zorgt voor een correcte (actuele) KVK-vermelding met daarin de juiste tekenbevoegden.
- Zorgt dat de tekenbevoegden beschikbaar zijn voor ondertekening van de akkoordverklaring.
- Tijdig kennisneemt van - en akkoord gaat met - de aansluitvoorwaarden.

Directe aansluiting

Clusteraansluiting

# Stap 8

## Laten uitvoeren meervoudig DigiD-assessment inclusief penetratietest

**U toont aan dat uw organisatie voldoet aan de voorwaarden om te mogen aansluiten.**
Voorafgaand aan het assessment vindt een penetratietest plaats, die zich richt op de daadwerkelijke aanwezigheid en juiste instelling van een aantal technische vereisten in de infrastructuur. De scope van de penetratietest omvat tenminste de webapplicatie en de infrastructuur voor het netwerksegment met de DigiD webapplicatie.

**Let op!** Direct na het aansluiten in productie van de eerste twee zorgaanbieders start de periode van twee maanden waarbinnen u het meervoudig assessment laat uitvoeren en het rapport aan Logius oplevert.

### Actiepunten

- Plannen en (laten) uitvoeren van een penetratietest.
- Opstellen en uitvoeren van actieplan naar aanleiding van de resultaten van de penetratietest.
- Laat een Meervoudig DigiD Assessment uitvoeren door een IT auditor (RE).

Directe aansluiting

Clusteraansluiting

# Stap 9

## Vaststellen uitkomst assessment

Uw leverancier dient bij Logius een auditrapportage in om aan te tonen dat het assessment conform voorwaarden heeft plaatsgevonden.

Als zorgaanbieder blijft u zelf verantwoordelijk voor de DigiD-aansluiting en in die hoedanigheid heeft u ook recht op inzage in de uitkomsten van het assessment. Mocht uw leverancier deze (nog) niet beschikbaar hebben gesteld, kunt u daar om vragen.

**Actiepunten**

- Onderteken de akkoordverklaring en stuur deze terug naar uw leverancier.

Voor een vlot verloop van het aansluitproces is het van belang dat u:

- Zorgt voor een correcte (actuele) KVK-vermelding met daarin de juiste tekenbevoegden.
- Zorgt dat de tekenbevoegden beschikbaar zijn voor ondertekening van de akkoordverklaring.
- Tijdig kennisneemt van - en akkoord gaat met - de aansluitvoorwaarden.

# Stap 9

## Indienen auditrapportage

**U stuurt het rapport met de bevindingen uit het meervoudig assessment aan Logius.**

Nadat het auditrapport aan Logius is gestuurd hebt u twee maanden de tijd om eventuele bevindingen te verhelpen. Informeer uw zorgaanbieders over het verloop van het assessment en geef hen inzage in het auditrapport. Zij zijn immers officieel aansluithouder. Zodra Logius de auditrapportage als voldoende heeft beoordeeld en u hierover heeft ingelicht, kunt u starten met het grootschalig aansluiten van zorgaanbieders.

Zie de webpagina IT-auditrapportage voor DigiD: indienen en vervolgstappen? | Logius voor de adressen en voorwaarden.

**Actiepunten**

- Zend het definitieve auditrapport naar Logius; dit kan per e-mail of per post.
- Stel aan de hand van een planning vast dat uw organisatie en/of die van de leverancier de gerapporteerde tekortkomingen binnen twee maanden kan herstellen.
- Informeer Logius tijdig, ook in het geval dat de termijn van twee maanden overschreden dreigt te worden.
- Informeer betrokken zorgaanbieders en stel rapportage beschikbaar.

Directe aansluiting

Clusteraansluiting

# Meer informatie over meervoudige assessments

**Relevante documenten en informatie over meervoudige assessments**

Meer informatie en relevante documenten is gepubliceerd op de website van Logius.

U vindt hier onder andere:

- DigiD meervoudige assessment: Overeenkomst Logius en LMA
- DigiD meervoudige aansluiting: Verplichtingen tussen LMA en aansluithouders die in (een bijlage bij) het contract tussen deze partijen opgenomen dienen te worden

NOREA – de beroepsorganisatie voor IT-auditors

Handreiking DigiD-assessments

DICTU stelt de akkoordverklaring op verzoek beschikbaar.

# *Colofon*

Publicatie van Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid

*november 2021*