Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DigiD Meervoudige aansluiting -
Verplichtingen tussen LMA en AMA

Versie	1.0
Datum	30 november 2020
Status	Definitief

Inleiding

Indien gebruik wordt gemaakt van een DigiD Meervoudige Aansluiting en de LMA (Leverancier Meervoudige Aansluiting) wil één assessment op de DigiD aansluitingen en het aangesloten platform laten uitvoeren, heeft dit gevolgen voor de wijze waarop het DigiD ICT-beveiligingsassessment wordt uitgevoerd. Hiertoe heeft de LMA een overeenkomst gesloten met Logius.

Dit document geeft een nadere invulling van artikel 4 uit de overeenkomst tussen de LMA en Logius. Het beschrijft de verplichtingen tussen de leverancier en de AMA (Aansluithouder Meervoudige aansluiting).

1 Verplichtingen tussen Leverancier (LMA) en Aansluithouder (AMA)

Ten aanzien van het toetsen en inzichtelijk maken van het stelsel als genoemd in artikel 4 van de overeenkomst tussen de Leverancier en Logius zal de leverancier tenminste de volgende punten borgen in de overeenkomst met de aansluithouder:

1.1 Aansluithouder wordt afgesloten van dienstverlening door de Leverancier als de Aansluithouder de beheersmaatregelen ten behoeve van het DigiD-assessment niet naleeft. De aansluiting op DigiD is hiermee niet komen te vervallen; doorbelasting en assessmentplicht zijn dan nog van toepassing;

1.2 Er wordt jaarlijks een schriftelijke gegevensclassificatie, zoals bedoeld in de Norm ICT-beveiligingsassessements DigiD, uitgevoerd waarbij de juridische grondslag ten behoeve van het gebruik van het Burgerservicenummer de basis is. Aan de gegevensclassificatie ligt een juridisch oordeel van een ter zake kundige medewerker ten grondslag;

1.3 Aansluithouder geeft een vergaande volmacht aan de Leverancier voor onder andere de gegevensclassificatie;

1.4 Aansluithouder dient akkoord te gaan met de gegevensclassificatie zoals opgesteld door de Leverancier;

1.5 Leverancier verantwoordt zich jaarlijks schriftelijk aan de Aansluithouder over (veranderingen in) gegevensclassificatie en de naleving van gerelateerde maatregelen;

1.6 Aansluithouder heeft enkel op applicatieniveau toegang tot zijn data;

1.7 Wachtwoordinstellingen worden centraal door de Leverancier beheerd en hebben voldoende sterke instellingen. Wijzigingen in deze instellingen worden vastgelegd in een audittrail (bewaartermijn 7 jaar).

1.8 Indien Aansluithouder vanuit de functionaliteit toegang heeft tot de applicatie ondersteunt Leverancier de Aansluithouder voor het toekennen, controleren en intrekken van autorisaties binnen de applicatie. Hiervan wordt een audittrail bijgehouden.

1.9 Per Aansluithouder wordt door een poweruser een aantoonbare controle op joiners, movers en leavers verplicht elke drie maanden uitgevoerd als onderdeel van de functionaliteit van de applicatie. Hiervan wordt een audittrail bijgehouden. Een kwaliteitsfunctionaris van de leverancier bewaakt dit proces. Voor het assessment is per jaar een samenvattende rapportage beschikbaar.

1.10 Technische maatregelen zijn op basis van een risicoafweging ingericht ten behoeve van het correcte gebruik van gebruikersaccounts van de Aansluithouder. Hierbij kan gedacht worden aan het automatisch blokkeren van gebruikersaccounts na vier weken niet gebruikt en het beëindigen van voorgaande sessies als dezelfde gebruiker opnieuw inlogt ter voorkoming van het gebruik van dezelfde useraccounts door meerdere personen.

1.11 Audittrails hebben een bewaartermijn van zeven jaar.

1.12 Er is een generiek en uniform aansluitproces, met voorwaarden en controles, dat op alle Aansluithouders van toepassing is.