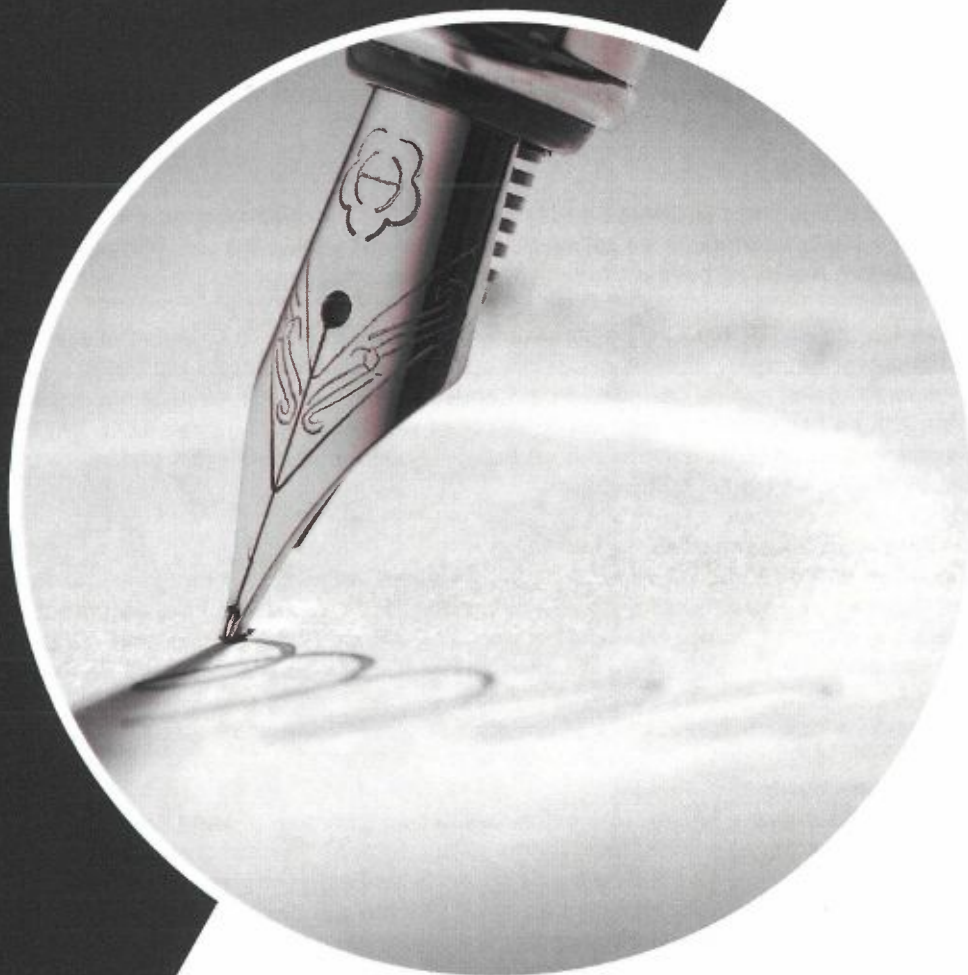


ACCORIS



gemeente Midden-Drenthe

ENSIA 2017

Datum rapport: 26 april 2018

Dit rapport heeft 12 pagina's

Rapportnummer: AAS2018-401

Assurancerapport van de onafhankelijke IT-auditor

Aan: College van burgemeester en wethouders van gemeente Midden-Drenthe

Ons oordeel

Wij hebben de bijgevoegde Collegeverklaring ENSIA 2017 inzake informatiebeveiliging van DigiD (inclusief de bijlage DigiD waarnaar in de collegeverklaring wordt verwezen) van gemeente Midden-Drenthe onderzocht.

Naar ons oordeel is bijgevoegde Collegeverklaring ENSIA 2017 inzake informatiebeveiliging van DigiD (inclusief bijlage DigiD waarnaar in de collegeverklaring wordt verwezen) van gemeente Midden-Drenthe, in alle van materieel belang zijnde aspecten, juist.

De Collegeverklaring ENSIA 2017 inzake informatiebeveiliging van DigiD (hierna Collegeverklaring ENSIA 2017) omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK). Wij benadrukken dat het specifiek geselecteerde normen zijn en daarmee geen uitspraak wordt gedaan over de informatiebeveiliging als geheel omtrent DigiD.

Benadrukking aangelegenheden

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van de collegeverklaring en dit assurancerapport. Wij hebben wel vastgesteld dat onze assurance bij deze collegeverklaring en de assurance bij de verantwoording van de dienstverlener aan wie de beheersingsmaatregelen zijn uitbesteed tezamen de geselecteerde normen inzake DigiD afdekken.

Deze aanvullende informatie is niet bedoeld om afbreuk te doen aan ons oordeel.

De basis voor ons oordeel

Wij hebben onze assurance-opdracht met betrekking tot de Collegeverklaring ENSIA 2017 uitgevoerd volgens Nederlands recht, waaronder de Richtlijn 3000 (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA. Deze assurance-opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Onze verantwoordelijkheden voor de assurance-opdracht betreffende de Collegeverklaring ENSIA 2017'.

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

Wij vinden dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor ons oordeel.

Beperking in gebruik en verspreidingskring

Dit assurancerapport is bestemd voor gebruikers van de Collegeverklaring ENSIA 2017. De Collegeverklaring ENSIA 2017 is opgesteld voor de gemeenteraad en voor het departement dat toeziet op de veiligheid van DigiD.

Doel van de Collegeverklaring ENSIA 2017 is om de gemeenteraad en het departement dat toeziet op de veiligheid van DigiD te informeren over het in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen DigiD. Ons assurancerapport is derhalve uitsluitend bestemd voor de gemeenteraad en het departement dat toeziet op de veiligheid van DigiD en dient niet te worden verspreid aan of te worden gebruikt door anderen.

Beperkingen van interne beheersingsmaatregelen

Interne beheersingsmaatregelen kunnen vanwege hun aard niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken.

Werking niet onderzocht

Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen en brengen daarover geen oordeel tot uitdrukking.

Verantwoordelijkheden van het college van gemeente Midden-Drenthe

Het college van burgemeester en wethouders van gemeente Midden-Drenthe is verantwoordelijk voor het opstellen van de Collegeverklaring ENSIA 2017. De gemeenteraad en het departement dat toeziet op de veiligheid van DigiD dient voldoende inzicht te hebben om deze collegeverklaring, samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die zelf worden uitgevoerd, te beschouwen wanneer zij de risico's van afwijkingen van materieel belang in relatie tot DigiD inschatten.

De criteria waarvan bij het maken van deze verklaring gebruik werd gemaakt hielden in dat:

- De risico's die het bereiken van de geselecteerde normen DigiD in gevaar brengen, werden geïdentificeerd;
- De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen.
- Het college ook verantwoordelijk is voor een zodanige interne beheersing als het noodzakelijk acht om het opstellen van de Collegeverklaring ENSIA 2017 mogelijk te maken zonder afwijkingen van materieel belang als gevolg van fraude of fouten.

Onze verantwoordelijkheden voor de assurance-opdracht betreffende de Collegeverklaring ENSIA 2017

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van een assurance-opdracht dat wij daarmee, met een redelijke mate van zekerheid voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordeel. Een redelijke mate van zekerheid wil zeggen dat onze assurance-opdracht is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens onze assurance-opdracht niet alle materiële fouten en fraude ontdekken.

Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van de ethische voorschriften, professionele standaarden en andere wet- en regelgeving.

Afwijkingen kunnen ontstaan als gevolg van fraude of fouten en zijn materieel indien redelijkerwijs kan worden verwacht dat deze, afzonderlijk of gezamenlijk, van invloed kunnen zijn op de beslissingen die gebruikers op basis van de Collegeverklaring ENSIA 2017 nemen. De materialiteit beïnvloedt de aard, timing en omvang van onze assurancewerkzaamheden en de evaluatie van het effect van onderkende afwijkingen op ons oordeel.

Wij hebben deze assurance-opdracht professioneel kritisch uitgevoerd en hebben waar relevant professionele oordeelsvorming toegepast in overeenstemming met de Richtlijn 3000 (Herzien) 'Assuranceopdrachten door IT-auditors' van NOREA.

Onze assurance-opdracht bestond onder andere uit:

- het verkrijgen van kennis omtrent de Collegeverklaring ENSIA 2017 en andere omstandigheden rond de opdracht waaronder het verkrijgen van kennis omtrent de interne beheersingsmaatregelen. Deze werkzaamheden hebben niet als doel om een oordeel uit te spreken over de effectiviteit van de interne beheersing van de gemeente;
- het op basis van deze kennis inschatten van de risico's dat de Collegeverklaring ENSIA 2017 onjuistheden van materieel belang bevat als gevolg van fraude en fouten, het in reactie op deze risico's bepalen en uitvoeren van assurancewerkzaamheden en het verkrijgen van assurance-informatie die voldoende en geschikt is als basis voor ons oordeel. Bij fraude is het risico dat een afwijking van materieel belang niet ontdekt wordt groter dan bij fouten. Bij fraude kan sprake zijn van samenspanning, valsheid in geschrifte, het opzettelijk nalaten transacties vast te leggen, het opzettelijk verkeerd voorstellen van zaken of het doorbreken van de interne beheersing;
- het reageren op de ingeschatte risico's, waaronder het ontwikkelen van een algehele aanpak, en het bepalen van de aard, de tijdsfasering en de omvang van verdere procedures;
- het uitvoeren van verdere procedures die duidelijk zijn gekoppeld aan de gesignaleerde risico's, waarbij gebruik wordt gemaakt van een combinatie van inspectie, waarnemingen ter plaatse en inwinnen van inlichtingen; en
- het evalueren van de toereikendheid van de assurance-informatie.

Zoetermeer, 26 april 2018

Accoris Audit Services B.V.

P.C.M. Holierhoek RE RA
Managing Partner

Bijlage 1 - DigiD

Vragen vooraf:

Vraag	Antwoord
Vraag 1: Bent u aansluithouder van DigiD aansluitingen?	ja
Vraag 2: Hoeveel assessmentplichtige DigiD aansluitingen heeft u?	1

Eigename DigiD aansluitingen	Antwoord
Nummer DigiD aansluiting Vul het Logius aansluitnummer in:	1000079
Naam DigiD aansluiting Vul de aansluitnaam in van de aansluiting:	Gemeente Midden-Drenthe3
Externe infrastructuur-leverancier Maakt u voor deze DigiD aansluiting gebruik van een externe infrastructuur-leverancier?	Nee
Naam leveranciers Geef de namen op van alle leveranciers die betrokken zijn bij deze DigiD aansluiting.	
TPM datum Voer hier de datum in van het TPM rapport.	
Applicatieleverancier Maakt u voor deze DigiD aansluiting gebruik van een externe leverancier voor de applicatie?	ja
Naam leverancier Geef de naam op van de applicatieleverancier.	Mozard
TPM datum Vult u hier de datum in van het TPM rapport van de applicatieleverancier.	01-12-2017
TPM kenmerk Vul hier het kenmerk in van het TPM rapport van de applicatieleverancier.	TPM-MZD-MAP-CN-MV
Bij applicatieleverancier: U kunt de TPM's hier uploaden.	
SaaS-leverancier Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Nee
Naam leverancier Geef de naam op van de SaaS-leverancier.	
TPM datum Voer hier de datum in van het TPM rapport.	
TPM kenmerk Voer hier het kenmerk in van het TPM rapport.	
Bij SaaS-leverancier: U kunt de TPM's hier uploaden	
TPM aanwezigheid Leveren alle leveranciers een TPM op?	

ACCORIS

P.C.M. Holierhoek RERA

• 26 april 2018 •

'voor indicatiedoeleinden'

Heeft uw eigen auditor vastgesteld dat deze leverancier aan de DigiD normen voldoet?	Ja
Reikwijdte TPM Hebben de TPM's dezelfde scope als de DigiD aansluiting?	Ja
Reikwijdte TPM Hanteren de TPM's hetzelfde normenkader als het DigiD normenkader 2.0?	Ja
Reikwijdte TPM Zijn de TPM's maximaal 1 jaar oud?	Ja
Reikwijdte TPM Heeft u als coördinator vastgesteld dat de overige normen, buiten de 5 waar u verantwoordelijk voor bent, door de TPM worden afgedekt?	Ja
Reikwijdte TPM Zijn de TPM's eerder gebruikt voor een DigiD assessment voor dezelfde aansluiting?	Nee
Externe auditor bedrijf Vul de namen in van het bedrijf van de externe auditors:	AuditConnect B.V.
Externe auditor Vul de namen in van de externe auditors:	M.R. van der Vliet RE
Heeft de auditor opmerkingen gemaakt in de TPM van de leverancier over normen die bij de aansluithouder moeten worden onderzocht?	Ja
Kunt u aangeven over welke normen opmerkingen zijn gemaakt in alle aanwezige TPM's en waar u dus zekerheid over moet verkrijgen?	• B.05 • U/TV.01 • U/WA.02 • U/WA.05 • U/PW.02 • U/PW.03 • U/PW.05 • U/PW.07 • U/NW.03 • U/NW.04 • U/NW.06 • C.03 • C.04 • C.06 • C.07 • C.08 • C.09

Object van onderzoek

Het object van onderzoek was de webomgeving van de DigiD-aansluiting 1000097 van de gemeente Midden-Drenthe. De gemeente Midden-Drenthe heeft de webomgeving van de DigiD-aansluiting gehost in 2 datacenters in Beilen (waarvan één dient als uitwijk), die beheerd worden

Totaaloverzicht getoetste normen ICT-beveiligingsassessment DiGiD-aansluiting van Midden-Drenthe

In deze bijlage brengen wij de oordelen samen, op basis van de diverse uitgevoerde werkzaamheden / uitgebrachte rapportages. Het doel van deze samenvatting is om Logius een totaaloverzicht te verschaffen over de resultaten vanuit de verschillende assessments t.a.v. de DigiD-aansluiting 100079 Midden-Drenthe3.

- Volgens de NOREA-handreiking inzake de DigiD-assessments moeten de volgende normen bij de gebruikersorganisatie worden getoetst:
- B.05
- U/TV.01
- U/WA.02
- U/WA.05
- U/PW.02
- U/PW.03
- U/PW.05
- U/PW.07
- U/NW.03
- U/NW.04
- U/NW.06
- C.03
- C.04
- C.06
- C.07
- C.08

C.09 Ten behoeve van de hierna vermelde samenvatting hebben wij, gebruik gemaakt van het rapport van AuditConnect B.V. inzake Mozard, kenmerk TPM-MZD-MAP-CN-MV, afgegeven op 01-12-2017 ondertekend door M.R. van der Vliet en de rapportage van Accoris Audit Services B.V. inzake UW Samenwerking, kenmerk AAS2018-239 afgegeven op 18 april 2018, ondertekend door P.C.M. Holierhoek RE RA. Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van [TPM-rapportage van de serviceorganisatie, referentie/rapportnummer, datum]. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet niet/Voldoet/ niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie ¹ Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet/ niet van toepassing	Referentie/ rapportnummer
------	--------------------------	--	---------------------------	---	---	---------------------------

¹ Gebruikersorganisatie voert de hosting van de applicatie in eigen beheer uit.

B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	Voldoet	TPM-MZD-MAP-CN-MV	Ja	Voldoet	AAS2018-239
U/TV. 01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	Voldoet	TPM-MZD-MAP-CN-MV	Ja	Voldoet	AAS2018-239
U/WA. 02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet	TPM-MZD-MAP-CN-MV	Ja	Voldoet	AAS2018-239
U/WA. 03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet	TPM-MZD-MAP-CN-MV	Nee	Niet van toepassing	

ACCORIS

P.C.M. Holierhoek RERA

• 26 april 2018 •

'voor indicatiedoeleinden'

U/WA. 04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet	TPM-MZD-MAP-CN-MV	Nee	Niet van toepassing	
U/WA. 05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderen de en cryptografische technieken.	Voldoet	TPM-MZD-MAP-CN-MV	Ja	Voldoet	AAS2018-239
U/PW. 02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet	TPM-MZD-MAP-CN-MV	Ja	Voldoet	AAS2018-239
U/PW. 03	De webserver is ingericht volgens een configuratie-baseline.	Voldoet	TPM-MZD-MAP-CN-MV	Ja	Voldoet	AAS2018-239
U/PW. 05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.			Ja	Voldoet	AAS2018-239
U/PW. 07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.			Ja	Voldoet	AAS2018-239
U/NW. 03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het			Ja	Voldoet	AAS2018-239

	internet gepositioneerd is.					
U/NW. 04	De netwerkcomponent en en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanis men.			Ja	Voldoet	AAS2018- 239
U/NW. 05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.			Ja	Voldoet	AAS2018- 239
U/NW. 06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.			Ja	Voldoet	AAS2018- 239
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).			Ja	Voldoet	AAS2018- 239
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Voldoet	TPM-MZD- MAP-CN- MV	Ja	Voldoet	AAS2018- 239
C.06	In de webapplicatieomg eving zijn signaleringsfunctie s (registratie en detectie) actief en efficiënt, effectief			Ja	Voldoet	AAS2018- 239

	en beveiligd ingericht.					
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.			Ja	Voldoet	AAS2018-239
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	TPM-MZD-MAP-CN-MV	Ja	Voldoet	AAS2018-239
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.			Ja	Voldoet	AAS2018-239