

Rapportage DigiD Assessment - ENSIA 2017

gemeente Lansingerland

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

Gegevens DigiD aansluiting(en)	Antwoord
Nummer DigiD aansluiting: Vul het Logius aansluitnummer in:	1001857
Naam DigiD aansluiting: Vul de aansluitnaam in van de aansluiting:	Zaaksysteem Gemeente Lansingerland
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.	N.v.t.
TPM datum: Voer hier de datum in van het TPM rapport.	N.v.t.
Applicatieleverancier: Maakt u voor deze DigiD aansluiting gebruik van een externe leverancier voor de applicatie?	Nee
Naam leverancier: Geef de naam op van de applicatieleverancier.	N.v.t.
TPM datum: Vult u hier de datum in van het TPM rapport van de applicatieleverancier.	N.v.t.
TPM kenmerk: Vul hier het kenmerk in van het TPM rapport van de applicatieleverancier.	N.v.t.
Bij applicatieleverancier: U kunt de TPM's hier uploaden.	N.v.t.
SaaS-leverancier: Maakt u voor deze DigiD aansluiting gebruik van een SaaS-leverancier?	Ja
Naam leverancier: Geef de naam op van de SaaS-leverancier.	Zaaksysteem.nl
TPM datum: Voer hier de datum in van het TPM rapport.	28-11-2017
TPM kenmerk: Voer hier het kenmerk in van het TPM rapport.	MMC/DIGID/LSL28112017
Bij SaaS-leverancier: U kunt de TPM's hier uploaden	Is geüpload via de ENSIA-tool


MAZARS
 MAZARS PAARDEKOOPER HOFFMAN NV
 Gewaarmerkt voor identificatiedoeleinden

 26-04-2018

TPM aanwezigheid: Leveren alle leveranciers een TPM op?	Ja
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:	Mazars
Externe auditor: Vul de namen in van de externe auditors:	Jan Matto RI RE en Achmed Bouazza RE CISA
Heeft de auditor opmerkingen gemaakt in de TPM van de leverancier over normen die bij de aansluithouder moeten worden onderzocht?	Nee
Kunt u aangeven over welke normen opmerkingen zijn gemaakt in alle aanwezige TPM's en waar u dus zekerheid over moet verkrijgen?	N.v.t.


MAZARS
 MAZARS PAARDEKOOPEL HOFFMAN NV
 Gewaarmerkt voor identificatiedoeleinden

 26-04-2018

Bijlage B - Object van onderzoek

Het object van onderzoek was de webomgeving van DigiD aansluiting 1001857 en Zaaksysteem Gemeente Lansingerland.

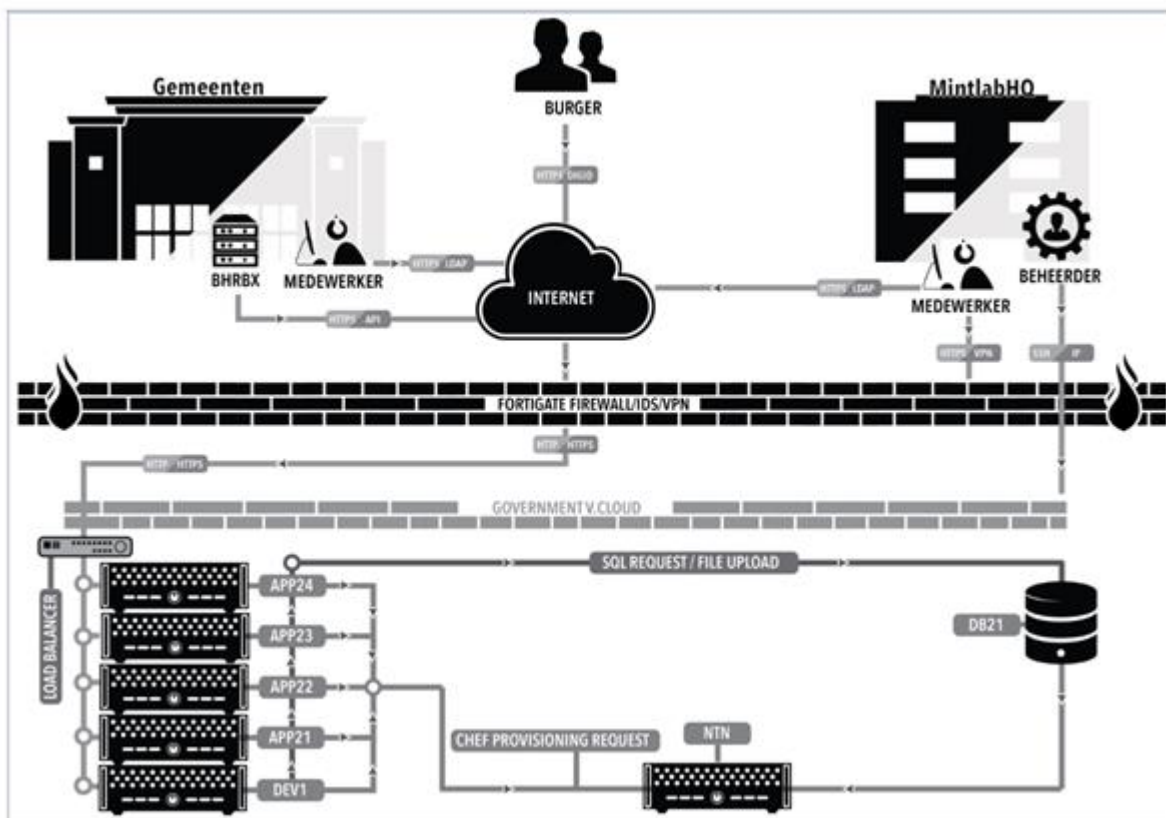
Gemeente Lansingerland biedt de volgende functionaliteit aan waarvoor DigiD aansluiting 1001857 voor authenticatie wordt gebruikt: aanvragen digitale dienstverlening/producten. Deze functionaliteit wordt geboden door de volgende webapplicatie: Zaaksysteem.nl .

Deze applicatie betreft een geheel standaard pakket en wordt onderhouden door 'Zaaksysteem.nl'.

Deze applicatie is extern benaderbaar via de volgende URL(s): mijn.lansingerland.nl.

De infrastructuur waar deze applicaties op draaien wordt beheerd door 'Zaaksysteem.nl' in de vorm van SAAS.

Het object van onderzoek was de webomgeving van DigiD aansluiting 1001857 ('DigiD webomgeving'). Het onderzoek heeft zich gericht op de webapplicaties, de URLs waarmee deze kunnen worden benaderd, de infrastructuur (binnen de DMZ waar webapplicaties zich bevinden) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD" van Logius. Het onderstaande schema toont de webomgeving die is onderzocht door middel van een infrastructurele test.



MAZARS
MAZARS PAARDEKOOPER HOFFMAN NV
Gewaarmerkt voor identificatiedoeleinden

26-04-2018

Gemeente Lansingerland heeft een deel van de DigiD webomgeving uitbesteed aan Zaaksysteem.nl. Als gevolg hiervan zijn er een aantal maatregelen belegd bij deze service organisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT auditor van deze service organisatie. De richtlijnen waar deze maatregelen betrekking op hebben zijn door ons dan ook niet onderzocht. Waar relevant geven wij, per richtlijn, specifieke verwijzingen naar het rapport van de service organisatie.



Bijlage C - Totaaloverzicht getoetste normen ICT-beveiligingsassessment DigiD-aansluiting van gemeente Lansingerland

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 1001857 en Zaaksysteem Gemeente Lansingerland.

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. en C.08.

Als input voor de hierna vermelde samenvatting hebben wij, naast de voorliggende rapportage, gebruik gemaakt van de rapportage van Mazars met het kenmerk MMC/DIGID/LSL28112017 d.d. 28 november 2017 ondertekend door Jan Matto RI RE en Achmed Bouazza RE CISA.

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de rapportage van Mazars met het kenmerk MMC/DIGID/LSL28112017 d.d. 28 november 2017. Wij kunnen dan ook geen verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

 **MAZARS**
MAZARS PAARDEKOOPEL HOFFMAN NV
Gewaarmerkt voor identificatiedoeleinden



26-04-2018

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet niet/Voldoet/ niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet/niet van toepassing	Referentie/ rapportnummer
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	MMC/DIGID/LSL28112017	Ja	Voldoet	Lan_ENSIA/DMK/20180425
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	MMC/DIGID/LSL28112017	Ja	Voldoet	Lan_ENSIA/DMK/20180425
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet	MMC/DIGID/LSL28112017	Ja	Voldoet	Lan_ENSIA/DMK/20180425


MAZARS
 MAZARS PAARDEKOOPEL HOFFMAN NV
 Gewaarmerkt voor identificatiedoeleinden

[Handwritten signature]

26-04-2018

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet niet/Voldoet/niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet/niet van toepassing	Referentie/ rapportnummer
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet	MMC/DIGID/LSL28112017	Ja	Voldoet	Lan_ENSIA/DMK/20180425
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	


MAZARS
 MAZARS PAARDEKOOPEL HOFFMAN NV
 Gewaarmerkt voor identificatiedoeleinden



26-04-2018

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet niet/Voldoet/niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet/niet van toepassing	Referentie/ rapportnummer
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.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
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 internet gepositioneerd is.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	


MAZARS
 MAZARS PAARDEKOOPEL HOFFMAN NV
 Gewaarmerkt voor identificatiedoeleinden

26-04-2018

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet niet/Voldoet/niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet/niet van toepassing	Referentie/ rapportnummer
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	


MAZARS
 MAZARS PAARDEKOOPEL HOFFMAN NV
 Gewaarmerkt voor identificatiedoeleinden

[Handwritten signature]

26-04-2018

Norm	Beschrijving van de norm	Getoetst bij leverancier: Voldoet niet/Voldoet/niet van toepassing	Referentie/ rapportnummer	Aanvullende beheersmaatregelen gebruikersorganisatie Ja/Nee	Getoetst bij gebruiker Voldoet niet/Voldoet/niet van toepassing	Referentie/ rapportnummer
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.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	MMC/DIGID/LSL28112017	Ja	Voldoet	Lan_ENSIA/DMK/20180425
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	Voldoet	MMC/DIGID/LSL28112017	Nee	Niet van toepassing	


MAZARS
 MAZARS PAARDEKOOPEL HOFFMAN NV
 Gewaarmerkt voor identificatiedoeleinden



26-04-2018

T18.05042

 **MAZARS**
MAZARS PAARDEKOOPER HOFFMAN NV
Gewaarmerkt voor identificatiedoeleinden



26-04-2018