

Bijlage 1 DigiD(1) – Parkeerproducten gemeente Nijmegen - 1004917

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2023 van gemeente Nijmegen.

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Parkeerproducten gemeente Nijmegen met aansluitnummer 1004917

Gemeente Nijmegen biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Parkeerproducten gemeente Nijmegen voor authenticatie wordt gebruikt:

- Het aanvragen, wijzigen en verlengen van parkeervergunningen

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Citypermit versie 2.1

Deze applicatie betreft een standaard software en wordt onderhouden door Sigmax Law Enforcement.

Deze applicatie is extern benaderbaar via het volgende internetadres:

<https://parkeerproducten.nijmegen.nl/>

DigiD-aansluiting Parkeerproducten gemeente Nijmegen bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Fundaments B.V. in samenwerking met Sigmax Law Enforcement in de vorm van IaaS.

Het object van de zelfevaluatie ENSIA is de webomgeving van DigiD-aansluiting Parkeerproducten gemeente Nijmegen. De zelfevaluatie heeft zich gericht op de webapplicatie die gebruik maakt van DigiD voor de identificatie en authenticatie van de gebruikers. Specifiek zijn in scope de internet-facing webpagina's waarmee de interactie naar de gebruiker plaatsvindt als deze is geïdentificeerd en geauthentiseerd via DigiD, de systeemkoppelingen en de infrastructuur die met DigiD gekoppeld is en betrekking heeft op het DigiD identificatie en authenticatieproces. Ook de verschillende vormen van beheer op de webapplicaties zijn in scope voor zover relevant voor de doelstelling van het zelfassessment. De URL www.digid.nl, de token uitwisseling tussen Logius en de webserver, de systemen die gegevens leveren of ophalen uit de webapplicatie, zoals backoffice informatiesystemen vallen buiten de scope. Subsystemen en koppelvlakken zijn in scope indien de primaire authenticatie van het systeem op basis van DigiD tot stand is gekomen.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Gemeente Nijmegen heeft een deel van de DigiD-webomgeving uitbesteed aan Sigmax Law Enforcement. Als gevolg hiervan is een aantal interne beheersingsmaatregelen betreffende dit normenkader belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is uitgevoerd door de onafhankelijke IT-auditor/RE van deze serviceorganisatie. De normen waar deze maatregelen betrekking op hebben zijn onderdeel van de zelfevaluatie. Over de uitkomsten van dit onderzoek heeft de onafhankelijke IT-auditor/RE van de serviceorganisatie de onderstaande TPM/ assurancerapportage opgesteld.

Serviceorganisatie

Naam serviceorganisatie:	Sigmax Law Enforcement
Referentie/rapportnummer:	2309R.AH78
Afgiftedatum:	6 oktober 2023
Naam onafhankelijke IT-auditor/RE:	Drs. A.J.A. Hassing RE RA
Ondertekend door onafhankelijke IT-auditor/RE:	Ja

Subserviceorganisatie

Naam serviceorganisatie:	Fundaments B.V.
Referentie/rapportnummer:	1 juli 2022 t/m 30 juni 2023
Afgiftedatum:	15 september 2023
Naam onafhankelijke IT-auditor/RE:	Ronald Snoep RE
Ondertekend door onafhankelijke IT-auditor/RE:	Ja

Onze onafhankelijke IT-auditor/RE heeft tevens getoetst of de zelfevaluatie, waarin opgenomen de TPM / assurancerapportage van onze serviceorganisatie, het gehele normenkader afdekt. Het kan voorkomen dat een norm deels bij een serviceorganisatie en deels bij de gemeente is getoetst (zogenaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze onafhankelijke IT-auditor/RE. De conclusie van deze onafhankelijke IT-auditor/RE is opgenomen in het assurancerapport met kenmerk AAS2024-2259.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm die zijn getoetst bij de serviceorganisatie.

DigiD-norm		Getoetst bij gemeente Nijmegen	Getoetst bij Sigmax Law Enforcement	Getoetst bij Fundaments B.V.	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Niet van toepassing	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.04	Normaliseren uitvoer	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/PW.02	Garanderen webprotocollen	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.03	Configureren webserver	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.05	Toegang tot beheermechanismen	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.07	Hardening van platformen	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.03	DMZ	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.05	Scheiding beheer- en productie-omgeving	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Niet van toepassing	Voldoet
C.03	Vulnerability-assessments	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.04	Penetratietesten	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet

DigiD-norm		Getoetst bij gemeente Nijmegen	Getoetst bij Sigmax Law Enforcement	Getoetst bij Fundaments B.V.	Totaaloordeel norm
C.06	Signaleringsfuncties	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.07	Monitoringfuncties	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Niet van toepassing	Voldoet
C.09	Patchmanagement	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet

Bijlage 1 DigiD(2) – Gemeente Nijmegen - Inkomensondersteuning - 1003381

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2023 van gemeente Nijmegen.

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Nijmegen - Inkomensondersteuning met aansluitnummer 1003381

Gemeente Nijmegen biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Nijmegen - Inkomensondersteuning voor authenticatie wordt gebruikt:

- De webapplicatie Forus & Me wordt door de inwoners/burgers van klanten van Forus Operations BV gebruikt voor de aanvraag van sociale regelingen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Forus & Me

Deze applicatie betreft een geheel standaard pakket en wordt onderhouden door Forus Operations BV.

Deze applicatie is extern benaderbaar het volgende internetadres:

<https://inkomensondersteuning.nijmegen.nl/>

DigiD-aansluiting Gemeente Nijmegen - Inkomensondersteuning bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Forus Operations BV in de vorm van SaaS.

Het object van de zelfevaluatie ENSIA is de webomgeving van DigiD-aansluiting Inkomensondersteuning. De zelfevaluatie heeft zich gericht op de webapplicatie die gebruik maakt van DigiD voor de identificatie en authenticatie van de gebruikers. Specifiek zijn in scope de internet-facing webpagina's waarmee de interactie naar de gebruiker plaatsvindt als deze is geïdentificeerd en geauthentiseerd via DigiD, de systeemkoppelingen en de infrastructuur die met DigiD gekoppeld is en betrekking heeft op het DigiD identificatie en authenticatieproces. Ook de verschillende vormen van beheer op de webapplicaties zijn in scope voor zover relevant voor de doelstelling van het zelfassessment. De URL www.digid.nl, de token uitwisseling tussen Logius en de webserver, de systemen die gegevens leveren of ophalen uit de webapplicatie, zoals backoffice informatiesystemen vallen buiten de scope. Subsystemen en koppelvlakken zijn in scope indien de primaire authenticatie van het systeem op basis van DigiD tot stand is gekomen.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Gemeente Nijmegen heeft een deel van de DigiD-webomgeving uitbesteed aan Forus Operations BV. Als gevolg hiervan is een aantal interne beheersingsmaatregelen betreffende dit normenkader belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is uitgevoerd door de onafhankelijke IT-auditor/RE van deze serviceorganisatie. De normen waar deze maatregelen betrekking op hebben zijn onderdeel van de zelfevaluatie. Over de uitkomsten van dit onderzoek heeft de onafhankelijke IT-auditor/RE van de serviceorganisatie de onderstaande TPM/ assurancerapportage opgesteld.

Serviceorganisatie	
Naam serviceorganisatie:	Forus Operations BV
Referentie/rapportnummer:	BKBO/200916-1/V4/TPM
Afgiftedatum:	10 oktober 2023
Naam onafhankelijke IT-auditor/RE:	drs. M.B.H. Ijpelaar RE CEH CISA mr W.R. Nanninga RE CISA MMC
Ondertekend door onafhankelijke IT-auditor/RE:	Ja

Onze onafhankelijke IT-auditor/RE heeft tevens getoetst of de zelfevaluatie, waarin opgenomen de TPM / assurancerapportage van onze serviceorganisatie, het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een serviceorganisatie en deels bij de gemeente is getoetst (zogenaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze onafhankelijke IT-auditor/RE. De conclusie van deze onafhankelijke IT-auditor/RE is opgenomen in het assurancerapport met kenmerk AAS2024-2259.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm die zijn getoetst bij de serviceorganisatie.

DigiD-norm		Getoetst bij gemeente Nijmegen	Getoetst bij Forus Operations BV	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Niet van toepassing	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Niet van toepassing	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen	Niet van toepassing	Voldoet	Voldoet
U/PW.03	Configureren webserver	Niet van toepassing	Voldoet	Voldoet
U/PW.05	Toegang tot beheermechanismen	Niet van toepassing	Voldoet	Voldoet
U/PW.07	Hardening van platformen	Niet van toepassing	Voldoet	Voldoet
U/NW.03	DMZ	Niet van toepassing	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Niet van toepassing	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Niet van toepassing	Voldoet	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Voldoet
C.03	Vulnerability-assessments	Niet van toepassing	Voldoet	Voldoet
C.04	Penetratietesten	Niet van toepassing	Voldoet	Voldoet
C.06	Signaleringsfuncties	Niet van toepassing	Voldoet	Voldoet
C.07	Monitoringfuncties	Niet van toepassing	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Niet van toepassing	Voldoet	Voldoet

Bijlage 1 DigiD(3) – Gemeente Nijmegen Belasting prod CGI - 1003645

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2023 van gemeente Nijmegen.

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Nijmegen Belasting prod CGI met aansluitnummer 1003545

Gemeente Nijmegen biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Nijmegen Belasting prod CGI voor authenticatie wordt gebruikt:

- Digitaal belastingloket voor belastingzaken

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- eGouw7R2

Deze applicatie betreft een geheel standaard pakket en wordt onderhouden door GouwIT

Deze applicatie is extern benaderbaar via het volgende internetadres:

<https://belastingen.nijmegen.nl/view/LOGIN/>

DigiD-aansluiting Gemeente Nijmegen Belasting prod CGI bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door GouwIT in de vorm van SaaS.

Het object van de zelfevaluatie ENSIA is de webomgeving van DigiD-aansluiting Gemeente Nijmegen Belasting prod CGI. De zelfevaluatie heeft zich gericht op de webapplicatie die gebruik maakt van DigiD voor de identificatie en authenticatie van de gebruikers. Specifiek zijn in scope de internet-facing webpagina's waarmee de interactie naar de gebruiker plaatsvindt als deze is geïdentificeerd en geauthentiseerd via DigiD, de systeemkoppelingen en de infrastructuur die met DigiD gekoppeld is en betrekking heeft op het DigiD identificatie en authenticatieproces. Ook de verschillende vormen van beheer op de webapplicaties zijn in scope voor zover relevant voor de doelstelling van het zelfassessment. De URL www.digid.nl, de token uitwisseling tussen Logius en de webserver, de systemen die gegevens leveren of ophalen uit de webapplicatie, zoals backoffice informatiesystemen vallen buiten de scope. Subsystemen en koppelvlakken zijn in scope indien de primaire authenticatie van het systeem op basis van DigiD tot stand is gekomen.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Gemeente Nijmegen heeft een deel van de DigiD-webomgeving uitbesteed aan GouwIT. Als gevolg hiervan is een aantal interne beheersingsmaatregelen betreffende dit normenkader belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is uitgevoerd door de onafhankelijke IT-auditor/RE van deze serviceorganisatie. De normen waar deze maatregelen betrekking op hebben zijn onderdeel van de zelfevaluatie. Over de uitkomsten van dit onderzoek heeft de onafhankelijke IT-auditor/RE van de serviceorganisatie de onderstaande TPM/ assurancerapportage opgesteld.

Serviceorganisatie	
Naam serviceorganisatie:	GouwIT
Referentie/rapportnummer:	IAS0988-23-6511
Afgiftedatum:	12 oktober 2023
Naam onafhankelijke IT-auditor/RE:	R. Driehuis RE CISA CIPM
Ondertekend door onafhankelijke IT-auditor/RE:	Ja

Onze onafhankelijke IT-auditor/RE heeft tevens getoetst of de zelfevaluatie, waarin opgenomen de TPM / assurancerapportage van onze serviceorganisatie, het gehele normenkader afdekt. Het kan voorkomen dat een norm deels bij een serviceorganisatie en deels bij de gemeente is getoetst (zogenaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze onafhankelijke IT-auditor/RE. De conclusie van deze onafhankelijke IT-auditor/RE is opgenomen in het assurancerapport met kenmerk AAS2024-2259.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm die zijn getoetst bij de serviceorganisatie.

DigiD-norm		Getoetst bij gemeente Nijmegen	Getoetst bij GouwIT	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet
U/TV.01¹	Identificatie en authenticatie	Niet van toepassing	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Niet van toepassing	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Niet van toepassing	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen	Niet van toepassing	Voldoet	Voldoet
U/PW.03	Configureren webserver	Niet van toepassing	Voldoet	Voldoet
U/PW.05	Toegang tot beheermechanismen	Niet van toepassing	Voldoet	Voldoet
U/PW.07	Hardening van platformen	Niet van toepassing	Voldoet	Voldoet
U/NW.03	DMZ	Niet van toepassing	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Niet van toepassing	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Niet van toepassing	Voldoet	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Voldoet
C.03	Vulnerability-assessments	Niet van toepassing	Voldoet	Voldoet
C.04	Penetratietesten	Niet van toepassing	Voldoet	Voldoet
C.06	Signaleringsfuncties	Niet van toepassing	Voldoet	Voldoet
C.07	Monitoringfuncties	Niet van toepassing	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Niet van toepassing	Voldoet	Voldoet

¹ Volgens de TPM van Inergy valt de norm U/TV.01 out of scope.

Bijlage 1 DigiD(4) – Gemeente Nijmegen - 1004183

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2023 van gemeente Nijmegen.

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Nijmegen met aansluitnummer 1004183

Gemeente Nijmegen biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Nijmegen voor authenticatie wordt gebruikt:

- Webformulieren voor verschillende zaken (vergunningaanvragen, bezwaar maken etc)
- Mijn-nijmegen (inzage persoonsgegevens en uitkering)
- Verstrekken van Yivi attributen voor de Yivi identity wallet

Deze functionaliteit wordt geboden door de volgende webapplicaties:

- Webformulieren (op basis van formio) (<https://app6.nijmegen.nl>)
- Mijn-nijmegen (<https://mijn.nijmegen.nl>)
- Yivi (<https://yivi.nijmegen.nl>)

Deze applicatie is ontwikkeld door Gemeente Nijmegen. Authenticatie verloopt via

<https://authenticatie.nijmegen.nl>

Voor het verifiëren van de identiteit van de gebruikers maakt de DigiD aansluithouder gebruik van de authenticatie voorzieningen van Connected Information System B.V.

DigiD-aansluiting Gemeente Nijmegen bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Amazon Web Services (AWS) in de vorm van Platform-as-a-service (PaaS) en Infrastructure-as-a-service (IaaS).

Het object van de zelfevaluatie ENSIA is de webomgeving van DigiD-aansluiting Gemeente Nijmegen. De zelfevaluatie heeft zich gericht op de webapplicaties die gebruik maken van DigiD voor de identificatie en authenticatie van de gebruikers. Specifiek zijn in scope de internet-facing webpagina's waarmee de interactie naar de gebruiker plaatsvindt als deze is geïdentificeerd en geauthentiseerd via DigiD, de systeemkoppelingen en de infrastructuur die met DigiD gekoppeld is en betrekking heeft op het DigiD identificatie en authenticatieproces. Ook de verschillende vormen van beheer op de webapplicaties zijn in scope voor zover relevant voor de doelstelling van het zelfassessment. De URL www.digid.nl, de token uitwisseling tussen Logius en de webserver, de systemen die gegevens leveren of ophalen uit de webapplicatie, zoals backoffice informatiesystemen vallen buiten de scope. Subsystemen en koppelvlakken zijn in scope indien de primaire authenticatie van het systeem op basis van DigiD tot stand is gekomen.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Gemeente Nijmegen heeft een deel van de DigiD-webomgeving uitbesteed aan Signicat. Als gevolg hiervan is een aantal interne beheersingsmaatregelen betreffende dit normenkader belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is uitgevoerd door de onafhankelijke IT-auditor/RE van deze serviceorganisatie. De normen waar deze maatregelen betrekking op hebben zijn onderdeel van de zelfevaluatie. Over de uitkomsten van dit onderzoek heeft de onafhankelijke IT-auditor/RE van de serviceorganisaties de onderstaande TPM's/ assurancerapportages opgesteld.

Serviceorganisatie	
Naam serviceorganisatie:	Connected Information Systems B.V.
Referentie/rapportnummer:	22012024 (AWS) -2
Afgiftedatum:	29022024
Naam onafhankelijke IT-auditor/RE:	Drs. A.E. Klaassen RE CIPP/E CIPM
Ondertekend door onafhankelijke IT-auditor/RE:	Ja

Subserviceorganisatie	
Naam serviceorganisatie:	Amazon Web Services (AWS)
Referentie/rapportnummer:	8b89a093-2ec4-4c3e-87bd-9039ea798477
Afgiftedatum:	2023
Naam onafhankelijke IT-auditor/RE:	Ernst & Young LLP
Ondertekend door onafhankelijke IT-auditor/RE:	Nee

Onze onafhankelijke IT-auditor/RE heeft tevens getoetst of de zelfevaluatie, waarin opgenomen de TPM's / assurancerapportages van onze serviceorganisaties, het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een serviceorganisatie en deels bij de gemeente is getoetst (zogenaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze onafhankelijke IT-auditor/RE. De conclusie van deze onafhankelijke IT-auditor/RE is opgenomen in het assurancerapport met kenmerk AAS2024-2259.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm die zijn getoetst bij de serviceorganisatie.

DigiD-norm		Getoetst bij gemeente Nijmegen	Getoetst bij Signicat	Getoetst bij AWS ²	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Voldoet	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.04	Normaliseren uitvoer	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.05	Cryptografie/ Privacybeveiliging	Voldoet	Voldoet	Voldoet	Voldoet
U/PW.02	Garanderen webprotocollen	Voldoet	Voldoet	Niet van toepassing	Voldoet

² De auditor van de serviceorganisatie is verantwoordelijk voor het vaststellen van de overeenkomst van het DigiD normenkader en het normenkader van de subserviceorganisatie. Voor de in deze kolom vermelde oordelen wordt verwezen naar de bevindingen en de daarop gebaseerde conclusie van de auditor van de subserviceorganisatie, die zijn opgenomen in de rapportage over de subserviceorganisatie.

DigiD-norm		Getoetst bij gemeente Nijmegen	Getoetst bij Signicat	Getoetst bij AWS ²	Totaaloordeel norm
U/PW.03	Configureren webserver	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/PW.05	Toegang tot beheermechanis- men	Voldoet	Voldoet	Voldoet	Voldoet
U/PW.07	Hardening van platformen	Voldoet	Voldoet	Voldoet	Voldoet
U/NW.03	DMZ	Voldoet	Voldoet	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanis- men	Voldoet	Voldoet	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productie- omgeving	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Voldoet	Voldoet
C.03	Vulnerability-assessments	Voldoet	Voldoet	Voldoet	Voldoet
C.04	Penetratietesten	Voldoet	Voldoet	Voldoet	Voldoet
C.06	Signaleringsfuncties	Voldoet	Voldoet	Voldoet	Voldoet
C.07	Monitoringfuncties	Voldoet	Voldoet	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Voldoet	Voldoet	Voldoet	Voldoet

Bijlage 1 DigiD(5) – Gemeente Nijmegen - 1004255

Deze bijlage is een afzonderlijk onderdeel van de Collegeverklaring ENSIA 2023 van gemeente Nijmegen.

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Nijmegen met aansluitnummer 1004255

Gemeente Nijmegen biedt de volgende functionaliteit aan waarvoor DigiD-aansluiting Gemeente Nijmegen voor authenticatie wordt gebruikt:

- Een digitaal loket voor burgers met onder meer het inzien van gegevens en het indienen van formulieren.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- SIMform
- PIP (Persoonlijke Internet Pagina)

Deze applicatie betreft een geheel standaard pakket en wordt onderhouden door SIMgroep.

Deze applicatie is extern benaderbaar via het volgende internetadres:

<https://app8.nijmegen.nl/>

DigiD-aansluiting Gemeente Nijmegen bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door SIMgroep in samenwerking met Amazon Web Services in de vorm van PaaS.

Het object van de zelfevaluatie ENSIA is de webomgeving van DigiD-aansluiting Gemeente Nijmegen. De zelfevaluatie heeft zich gericht op de webapplicatie die gebruik maakt van DigiD voor de identificatie en authenticatie van de gebruikers. Specifiek zijn in scope de internet-facing webpagina's waarmee de interactie naar de gebruiker plaatsvindt als deze is geïdentificeerd en geauthentiseerd via DigiD, de systeemkoppelingen en de infrastructuur die met DigiD gekoppeld is en betrekking heeft op het DigiD identificatie en authenticatieproces. Ook de verschillende vormen van beheer op de webapplicaties zijn in scope voor zover relevant voor de doelstelling van het zelfassessment. De URL www.digid.nl, de token uitwisseling tussen Logius en de webserver, de systemen die gegevens leveren of ophalen uit de webapplicatie, zoals backoffice informatiesystemen vallen buiten de scope. Subsystemen en koppelvlakken zijn in scope indien de primaire authenticatie van het systeem op basis van DigiD tot stand is gekomen.

Een DigiD-aansluiting dient aan het gehele normenkader te voldoen. Gemeente Nijmegen heeft een deel van de DigiD-webomgeving uitbesteed aan SIMgroep. Als gevolg hiervan is een aantal interne beheersingsmaatregelen betreffende dit normenkader belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is uitgevoerd door de onafhankelijke IT-auditor/RE van deze serviceorganisatie. De normen waar deze maatregelen betrekking op hebben zijn onderdeel van de zelfevaluatie. Over de uitkomsten van dit onderzoek heeft de onafhankelijke IT-auditor/RE van de serviceorganisatie de onderstaande TPM/ assurancerapportage opgesteld.

Serviceorganisatie

Naam serviceorganisatie:	SIMgroep
Referentie/rapportnummer:	230/422400/2023/21155_34
Afgiftedatum:	29 september 2023
Naam onafhankelijke IT-auditor/RE:	drs. F.W. Hanekamp RE
Ondertekend door onafhankelijke IT-auditor/RE:	Ja

Subserviceorganisatie

Naam serviceorganisatie:	Amazon Web Services
Referentie/rapportnummer:	System_and_Organization_Controls_(SOC)_2_Report_-_Current_(Oct_1_2022_-_Mar_31_2023)
Afgiftedatum:	12 mei 2023
Naam onafhankelijke IT-auditor/RE:	Ernst + Young LLP
Ondertekend door onafhankelijke IT-auditor/RE:	Ja

Onze onafhankelijke IT-auditor/RE heeft tevens getoetst of de zelfevaluatie, waarin opgenomen de TPM / assurancerapportage van onze serviceorganisatie, het gehele normenkader afdekken. Het kan voorkomen dat een norm deels bij een serviceorganisatie en deels bij de gemeente is getoetst (zogenaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze onafhankelijke IT-auditor/RE. De conclusie van deze onafhankelijke IT-auditor/RE is opgenomen in het assurancerapport met kenmerk AAS2024-2259.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm die zijn getoetst bij de serviceorganisatie.

DigiD-norm		Getoetst bij gemeente Nijmegen	Getoetst bij SIMgroep	Getoetst bij Amazon Web Services	Totaaloordeel norm
B.01	Informatiebeveiligingsbeleid	Voldoet	Voldoet	Voldoet	Voldoet
B.05	Contractmanagement	Voldoet	Voldoet	Voldoet	Voldoet
U/TV.01	Identificatie en authenticatie	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.02	Webapplicatiebeheerproces	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.03	Automatische data-invoercontrole	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.04	Normaliseren uitvoer	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.05	Cryptografie/ Privacybevordering	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/PW.02	Garanderen webprotocollen	Niet van toepassing	Voldoet	Voldoet	Voldoet
U/PW.03	Configureren webserver	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.05	Toegang tot beheermechanismen	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.07	Hardening van platformen	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.03	DMZ	Niet van toepassing	Voldoet	Voldoet	Voldoet
U/NW.04	Protectie- en detectiemechanismen	Niet van toepassing	Voldoet	Voldoet	Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	Niet van toepassing	Voldoet	Voldoet	Voldoet

DigiD-norm		Getoetst bij gemeente Nijmegen	Getoetst bij SIMgroep	Getoetst bij Amazon Web Services	Totaaloordeel norm
U/NW.06	Hardening van netwerken	Voldoet	Voldoet	Voldoet	Voldoet
C.03	Vulnerability-assessments	Niet van toepassing	Voldoet	Voldoet	Voldoet
C.04	Penetratietesten	Niet van toepassing	Voldoet	Voldoet	Voldoet
C.06	Signaleringsfuncties	Niet van toepassing	Voldoet	Voldoet	Voldoet
C.07	Monitoringfuncties	Niet van toepassing	Voldoet	Voldoet	Voldoet
C.08	Wijzigingenbeheer	Voldoet	Voldoet	Voldoet	Voldoet
C.09	Patchmanagement	Niet van toepassing	Voldoet	Voldoet	Voldoet