

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

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 verlenen van parkeervergunningen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: CityPermit
- Versie: 2.1

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

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

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Parkeerproducten gemeente Nijmegen. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD versie 3.0" van Logius.

Deze webapplicatie betreft een geheel standaardpakket. De webapplicatie wordt onderhouden door Sigmax Law Enforcement B.V.

DigiD-aansluiting Parkeerproducten gemeente Nijmegen bevindt zich in de Demilitarized Zone (DMZ). De applicatie wordt beheerd en ontwikkeld door Sigmax Law Enforcement B.V., in de vorm van een Software-as-a-service (SaaS) oplossing. De onderliggende laag wordt beheerd door Sigmax Law Enforcement B.V. De infrastructuur wordt beheerd, onderhouden en ontwikkeld door Fundaments B.V.

Gemeente Nijmegen heeft de DigiD web-omgeving uitbesteed aan:

- Sigmax Law Enforcement B.V.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

De DigiD-webomgeving moet aan het gehele normenkader voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier(s) van de gemeente valt voor de periode:

Aansluithouder	
Oordeelsdatum:	20 februari 2025
Controleperiode:	1 juli 2024 tot en met 31 december 2024

De overige normen worden afgedekt door onderstaande TPM / assurancerapportage(s) van de (toe)leverancier(s):

SaaS-leverancier	
Naam SaaS-leverancier:	Sigmax Law Enforcement B.V.
Referentie/rapportnummer:	TPM: 2410R.AH96 Sub-TPM: N.v.t.
Oordeelsdatum:	TPM: 10-10-2024 Sub-TPM: N.v.t.
Controleperiode:	TPM: 10 april 2024 tot 10 oktober 2024 Sub-TPM: N.v.t.
Naam RE-auditor	TPM: drs. A.J.A. Hassing RE RA Sub-TPM: N.v.t.
Ondertekend door RE-auditor:	TPM: Ja Sub-TPM: N.v.t.

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportages van onze serviceorganisatie(s) het gehele normenkader afdekken. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk AAS2024-2342.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij de bovengenoemde leveranciers.

DigiD-norm	Toetsing op	Aansluithouder	SaaS-leverancier	Totaaloordeel
		Oordeel	Oordeel TPM	
B.01 Informatiebeveiligingsbeleid	Opzet en bestaan	Voldoet	Voldoet	Voldoet
B.05 Contractmanagement	Opzet en bestaan	Voldoet	Voldoet	Voldoet
U/TV.01 Identificatie en authenticatie	Opzet en bestaan	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet
U/WA.02 Webapplicatiebeheerproces	Opzet en bestaan	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet
U/WA.03 Automatische data-invoercontrole	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/WA.04. Normaliseren uitvoer	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/WA.05 Cryptografie/ Privacybevordering	Opzet en bestaan	Voldoet	Voldoet	Voldoet
U/PW.02 Garanderen webprotocollen	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/PW.03 Configureren webserver	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/PW.05 Toegang tot beheermechanismen	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/PW.07 Hardening van platformen	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/NW.03 DMZ	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/NW.04 Protectie- en detectiemechanismen	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/NW.05 Scheiding beheer- en productieomgeving	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/NW.06 Hardening van netwerken	Opzet en bestaan	Voldoet	Voldoet	Voldoet
C.03 Vulnerability-assessments	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
C.04 Penetratietesten	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
C.06 Signaleringsfuncties	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
C.07 Monitoringfuncties	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
	Werking	Niet van toepassing	Voldoet	Voldoet
C.08 Wijzigingenbeheer	Opzet en bestaan	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet
C.09 Patchmanagement	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
	Werking	Niet van toepassing	Voldoet	Voldoet

Bijlage 1 DigiD(2) - Gemeente Nijmegen - 1004183

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,
- Mijn-Nijmegen,
- Verstrekken Yivi attributen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

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

Deze webapplicatie is extern benaderbaar het volgende internetadres:

- <https://authenticatie.nijmegen.nl/>

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Nijmegen. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD versie 3.0" van Logius.

Deze webapplicatie betreft geheel maatwerk. De webapplicatie wordt onderhouden door Connected Information Systems.

DigiD-aansluiting Gemeente Nijmegen bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Amazon Web Services met beheervorm PaaS en IaaS.

Voor het verifiëren van de identiteit van de gebruiker maakt gemeente Nijmegen gebruik van authenticatiedienst van Connected Information Systems.

Gemeente Nijmegen heeft de DigiD web-omgeving uitbesteed aan:

- Signicat/Connected Information Systems B.V.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

De DigiD-webomgeving moet aan het gehele normenkader voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier(s) van de gemeente valt voor de periode:

Aansluithouder	
Oordeelsdatum:	20 februari 2025
Controleperiode:	1 juli 2024 tot en met 31 december 2024

De overige normen worden afgedekt door onderstaande TPM / assurancerapportage(s) van de (toe)leverancier(s):

SaaS-leverancier	
Naam SaaS-leverancier:	Signicat
Referentie/rapportnummer:	TPM: 22112024(AWS)-1 Sub-TPM: KhfuBEfyMRNYWD hiUD6fZUsJ Brugletter: KhfuBEfyMRNYWD hiUD6fZUsJ
Oordeelsdatum:	TPM: 13 november 2024 Sub-TPM: 14 mei 2024 Brugletter: 1 november 2024
Controleperiode:	TPM: 1-1-2024 tot 13-11-2024 Sub-TPM: 1 April 2023 – 31 Maart 2024 Brugletter: 1 april 2024 tot en met 30 September 2024
Naam RE-auditor	TPM: Drs. A.E. Klaassen RE CIPP/E CIPM Sub-TPM: Ernst & Young LLP Brugletter: Ernst & Young LLP
Ondertekend door RE-auditor:	TPM: Ja Sub-TPM: Ja Brugletter: Ja

Identity Broker	
Naam Identity Broker:	Connected Information Systems
Referentie/rapportnummer:	TPM: 22112024(AWS)-1 Sub-TPM: KhfuBEfyMRNYWD hiUD6fZUsJ Brugletter: KhfuBEfyMRNYWD hiUD6fZUsJ
Oordeelsdatum:	TPM: 13 november 2024 Sub-TPM: 14 mei 2024 Brugletter: 1 november 2024
Controleperiode:	TPM: 1-1-2024 tot 13-11-2024 Sub-TPM: 1 April 2023 – 31 Maart 2024 Brugletter: 1 april 2024 tot en met 30 September 2024
Naam RE-auditor	TPM: Drs. A.E. Klaassen RE CIPP/E CIPM Sub-TPM: Ernst & Young LLP Brugletter: Ernst & Young LLP
Ondertekend door RE-auditor:	TPM: Ja Sub-TPM: Ja Brugletter: Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportages van onze serviceorganisatie(s) het gehele normenkader afdekken. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk AAS2024-2342.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij de bovengenoemde leveranciers.

DigiD-norm	Toetsing op	Aansluithouder	SaaS-leverancier		Identity Broker		Totaaloordeel
		Oordeel	Oordeel TPM	Oordeel sub-TPM	Oordeel TPM	Oordeel sub-TPM	
B.01 Informatiebeveiligingsbeleid	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
B.05 Contractmanagement	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
U/TV.01 Identificatie en authenticatie	<i>Opzet en bestaan</i>	Voldoet [1]	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
	<i>Werking</i>	Voldoet / Voldoet niet [3]	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.02 Webapplicatiebeheerproces	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
	<i>Werking</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.03 Automatische data-invoercontrole	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA04. Normaliseren uitvoer	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.05 Cryptografie/ Privacybevordering	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.02 Garanderen webprotocollen	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.03 Configureren webserver	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.05 Toegang tot beheermechanismen	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
U/PW.07 Hardening van platformen	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet

U/NW.03 DMZ	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
U/NW.04 Protectie- en detectiemechanismen	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
U/NW.05 Scheiding beheer- en productieomgeving	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
U/NW.06 Hardening van netwerken	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.03 Vulnerability-assessments	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
C.04 Penetratietesten	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.06 Signaleringsfuncties	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.07 Monitoringfuncties	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
	<i>Werking</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.08 Wijzigingenbeheer	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
	<i>Werking</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
C.09 Patchmanagement	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet
	<i>Werking</i>	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet	Voldoet

Beperkingen en bijzonderheden:

[1] Bestaan - Non-occurrence. Voor beveiligingsrichtlijn U/TV.01 hebben wij vastgesteld dat de DigiD Aansluithouder maatregelen heeft ontworpen en ingericht met betrekking tot deze norm en hebben deze gevalideerd. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij het bestaan niet kunnen vaststellen. Relevante audit evidence voor het bestaan van de betreffende beheersmaatregel is verzameld door een deelwaarneming te doen in een proces dat onderworpen is aan dezelfde control (i.c. dezelfde control owner, dezelfde tools, dezelfde registratie, dezelfde workflow, et cetera). Hierdoor zijn wij van oordeel dat de organisatie voldoet aan deze norm.

[3] Werking - non-occurrence. Voor beveiligingsrichtlijn U/TV.01 hebben wij vastgesteld dat de organisatie maatregelen heeft ontworpen (opzet) [optioneel indien getoetst voor andere deelpopulatie: en voor een andere deelpopulatie heeft geïmplementeerd (bestaan)]. Er zijn geen afwijkingen door ons geconstateerd. Wij zijn van oordeel dat de organisatie in opzet (of: opzet en bestaan) voldoet aan deze norm. Vanwege non-occurrence kan de effectieve werking niet worden vastgesteld en daarom geven wij daarover geen oordeel.

Bijlage 1 DigiD(3) - Gemeente Nijmegen – Inkomensondersteuning (vergoedingen) - 1005507

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Nijmegen – Inkomensondersteuning (vergoedingen) met aansluitnummer 1005507

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

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

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: Forus & Me
- Versie: 129

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

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

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Nijmegen – Inkomensondersteuning (vergoedingen). De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de “Norm ICT-beveiligingsassessments DigiD versie 3.0” van Logius.

Deze webapplicatie betreft een geheel standaardpakket. De webapplicatie wordt onderhouden door Forus Operations B.V.

DigiD-aansluiting Gemeente Nijmegen – Inkomensondersteuning (vergoedingen) bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Forus Operations B.V. met beheervorm SaaS.

Gemeente Nijmegen heeft de DigiD web-omgeving uitbesteed aan:

- Forus Operations B.V.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie(s). Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie(s). De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

De DigiD-webomgeving moet aan het gehele normenkader voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier(s) van de gemeente valt voor de periode:

Aansluithouder	
Oordeelsdatum:	20 februari 2025
Controleperiode:	1 juli 2024 tot en met 31 december 2024

De overige normen worden afgedekt door onderstaande TPM / assurancerapportage(s) van de (toe)leverancier(s):

SaaS-leverancier	
Naam SaaS-leverancier:	Forus Operations B.V.
Referentie/rapportnummer:	TPM: BKBO/200916-1/V5/TPM Sub-TPM: System and Organisation Controls 2 (SOC2) Type 2 Report Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy Brugletter: Niet van toepassing
Oordeelsdatum:	TPM: 15 oktober 2024 Sub-TPM: 14 mei 2024 Brugletter: 1 april 2024 tot en met 1 september 2024
Controleperiode:	TPM: 15 maart 2024 – 15 oktober 2024 Sub-TPM: 1 april 2023 tot en met 31 maart 2024 Brugletter: 1 april 2024 tot en met 1 september 2024
Naam RE-auditor	TPM: drs. M.B.H. Ijpelaar RE CEH CISA CIPP/e Sub-TPM: Ernst + Young LLP Brugletter: Ja
Ondertekend door RE-auditor:	TPM: Ja Sub-TPM: Ja Brugletter: Sara Duffer

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportages van onze serviceorganisatie(s) het gehele normenkader afdekken. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk AAS2024-2342.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij de bovengenoemde leveranciers.

DigiD-norm	Toetsing op	Aansluithouder	SaaS-leverancier		Totaaloordeel
		Oordeel	Oordeel TPM	Oordeel sub-TPM	
B.01 Informatiebeveiligingsbeleid	Opzet en bestaan	Voldoet	Voldoet	Voldoet	Voldoet
B.05 Contractmanagement	Opzet en bestaan	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/TV.01 Identificatie en authenticatie	Opzet en bestaan	Voldoet	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.02 Webapplicatiebeheerproces	Opzet en bestaan	Voldoet	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.03 Automatische data-invoercontrole	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.04. Normaliseren uitvoer	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.05 Cryptografie/ Privacybevordering	Opzet en bestaan	Voldoet	Voldoet	Niet van toepassing	Voldoet
U/PW.02 Garanderen webprotocollen	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.03 Configureren webserver	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.05 Toegang tot beheermechanismen	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.07 Hardening van platformen	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.03 DMZ	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.04 Protectie- en detectiemechanismen	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.05 Scheiding beheer- en productieomgeving	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet

U/NW.06 Hardening van netwerken	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Niet van toepassing	Voldoet
C.03 Vulnerability-assessments	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.04 Penetratietesten	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.06 Signaleringsfuncties	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.07 Monitoringfuncties	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
	<i>Werking</i>	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
C.08 Wijzigingenbeheer	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet
	<i>Werking</i>	Voldoet	Voldoet	Voldoet	Voldoet
C.09 Patchmanagement	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet
	<i>Werking</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet

Bijlage 1 DigiD(4) - Gemeente Nijmegen Belasting prod CGI - 1003645

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Nijmegen Belasting prod CGI met aansluitnummer 1003645

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

- Het digitaal burgerloket voor belastingzaken.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: eGouw7R2
- Versie: 2024.2, 2024.3 en 2024.4

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

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

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Nijmegen Belasting prod CGI. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD versie 3.0" van Logius.

Deze webapplicatie betreft een geheel standaardpakket. De webapplicatie wordt onderhouden door GouwIT.

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 met beheervorm SaaS.

Gemeente Nijmegen heeft de DigiD web-omgeving uitbesteed aan:

- GouwIT.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

De DigiD-webomgeving moet aan het gehele normenkader voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier(s) van de gemeente valt voor de periode:

Aansluithouder	
Oordeelsdatum:	20 februari 2025
Controleperiode:	1 juli 2024 tot en met 31 december 2024

De overige normen worden afgedekt door onderstaande TPM / assurancerapportage(s) van de (toe)leverancier(s):

SaaS-leverancier	
Naam SaaS-leverancier:	GouwIT
Referentie/rapportnummer:	TPM: SEC_eGouw7R220241011 Sub-TPM: N.v.t.
Oordeelsdatum:	TPM: 11-10-2024 Sub-TPM: N.v.t.

Controleperiode:	TPM: 1 januari 2024 tot 1 oktober 2024 Sub-TPM: N.v.t.
Naam RE-auditor	TPM: Drs. C.C.A. Pietersma RE CRMA CIA Sub-TPM: N.v.t.
Ondertekend door RE-auditor:	TPM: Ja Sub-TPM: N.v.t.

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportages van onze serviceorganisatie(s) het gehele normenkader afdekken. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk AAS2024-2342.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij de bovengenoemde leveranciers.

DigiD-norm	Toetsing op	Aansluithouder	SaaS-leverancier	Totaaloordeel
		Oordeel	Oordeel TPM	
B.01 Informatiebeveiligingsbeleid	Opzet en bestaan	Voldoet	Voldoet	Voldoet
B.05 Contractmanagement	Opzet en bestaan	Voldoet	Voldoet	Voldoet
U/TV.01 Identificatie en authenticatie	Opzet en bestaan	Out of scope	Voldoet	Voldoet
	Werking	Out of scope	Voldoet	Voldoet
U/WA.02 Webapplicatiebeheerproces	Opzet en bestaan	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet
U/WA.03 Automatische data-invoercontrole	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/WA.04. Normaliseren uitvoer	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/WA.05 Cryptografie/ Privacybevordering	Opzet en bestaan	Voldoet	Voldoet	Voldoet
U/PW.02 Garanderen webprotocollen	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/PW.03 Configureren webserver	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/PW.05 Toegang tot beheermechanismen	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/PW.07 Hardening van platformen	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/NW.03 DMZ	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/NW.04 Protectie- en detectiemechanismen	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/NW.05 Scheiding beheer- en productieomgeving	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
U/NW.06 Hardening van netwerken	Opzet en bestaan	Voldoet	Voldoet	Voldoet
C.03 Vulnerability-assessments	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
C.04 Penetratietesten	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
C.06 Signaleringsfuncties	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
C.07 Monitoringfuncties	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
	Werking	Niet van toepassing	Voldoet	Voldoet
C.08 Wijzigingenbeheer	Opzet en bestaan	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet
C.09 Patchmanagement	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet
	Werking	Niet van toepassing	Voldoet	Voldoet

Bijlage 1 DigiD(5) - Gemeente Nijmegen - 1004255

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:

- Naam: SIMform en PIP
- Versie: 1.78.0 en 2.113.0

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

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

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Nijmegen. De zelfevaluatie heeft zich gericht op de webapplicatie, de internetadressen waarmee deze kan worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie zich bevindt) en een aantal ondersteunende processen conform de "Norm ICT-beveiligingsassessments DigiD versie 3.0" van Logius.

Deze webapplicatie betreft een geheel standaardpakket. De webapplicatie wordt onderhouden door Shift2.

DigiD-aansluiting Gemeente Nijmegen 2 bevindt zich in de Demilitarized Zone (DMZ). De applicatie wordt beheerd en ontwikkeld door Shift2 in een Private Cloud oplossing van Amazon Web Services (AWS), in de vorm van Platform-as-a-Service (PaaS). De onderliggende infrastructuur van de Private Cloud wordt beheerd door Amazon Web Services (AWS).

Gemeente Nijmegen heeft de DigiD web-omgeving uitbesteed aan:

- Shift2.

Als gevolg hiervan is een aantal maatregelen belegd bij deze serviceorganisatie. Het onderzoeken van deze maatregelen is dan ook uitgevoerd door de IT-auditor van deze serviceorganisatie. De normen waar deze maatregelen betrekking op hebben maken geen onderdeel uit van de zelfevaluatie, tenzij sprake is van een gedeelde norm.

De DigiD-webomgeving moet aan het gehele normenkader voldoen. Deze zelfevaluatie ENSIA voor DigiD is toegepast op dat deel van het normenkader dat niet onder uitbesteding aan de leverancier van de gemeente valt voor de periode:

Aansluithouder	
Oordeelsdatum:	20 februari 2025
Controleperiode:	01 juli 2024 tot en met 31 december 2024

De overige normen worden afgedekt door onderstaande TPM / assurancerapportage(s) van de (toe)leverancier(s):

SaaS-leverancier	
Naam SaaS-leverancier:	Shift2
Referentie/rapportnummer:	TPM: 230/422400/2024/22527_36

	Sub-TPM: System and Organization Controls (SOC) 2 Report Brugletter: SOC Continued Operations Letter
Oordeelsdatum:	TPM: 26 september 2024 Sub-TPM: 14 mei 2025 Brugletter: 1 juli 2024
Controleperiode:	TPM: 15 maart 2024 tot 26 september 2024 Sub-TPM: 1 april 2023 tot en met 31 maart 2024 Brugletter: 1 juli 2024
Naam RE-auditor	TPM: drs. F.W. (Wilfred) Hanekamp RE Sub-TPM: Ernst + Young LLP Brugletter: Sara Duffer
Ondertekend door RE-auditor:	TPM: Ja Sub-TPM: Ja Brugletter: Niet van toepassing

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM's / assurancerapportages van onze serviceorganisatie(s) het gehele normenkader afdekken. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk AAS2024-2342.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm inclusief de normen die getoetst zijn bij de bovengenoemde leveranciers.

DigiD-norm	Toetsing op	Aansluithouder	SaaS-leverancier		Totaaloordeel
		Oordeel	Oordeel TPM	Oordeel sub-TPM	
B.01 Informatiebeveiligingsbeleid	Opzet en bestaan	Voldoet	Voldoet	Voldoet	Voldoet
B.05 Contractmanagement	Opzet en bestaan	Voldoet	Voldoet	Voldoet	Voldoet
U/TV.01 Identificatie en authenticatie	Opzet en bestaan	Voldoet	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.02 Webapplicatiebeheerproces	Opzet en bestaan	Voldoet	Voldoet	Voldoet	Voldoet
	Werking	Voldoet	Voldoet	Voldoet	Voldoet
U/WA.03 Automatische data-invoercontrole	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.04. Normaliseren uitvoer	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/WA.05 Cryptografie/ Privacybevordering	Opzet en bestaan	Voldoet	Voldoet	Voldoet	Voldoet
U/PW.02 Garanderen webprotocollen	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet	Voldoet
U/PW.03 Configureren webserver	Opzet en bestaan	Niet van toepassing	Voldoet	Voldoet	Voldoet
U/PW.05 Toegang tot beheermechanismen	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/PW.07 Hardening van platformen	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.03 DMZ	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.04 Protectie- en detectiemechanismen	Opzet en bestaan	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet

U/NW.05 Scheiding beheer- en productieomgeving	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Niet van toepassing	Voldoet
U/NW.06 Hardening van netwerken	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet
C.03 Vulnerability-assessments	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet
C.04 Penetratietesten	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet
C.06 Signaleringsfuncties	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet
C.07 Monitoringfuncties	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet
	<i>Werking</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet
C.08 Wijzigingenbeheer	<i>Opzet en bestaan</i>	Voldoet	Voldoet	Voldoet	Voldoet
	<i>Werking</i>	Voldoet	Voldoet	Voldoet	Voldoet
C.09 Patchmanagement	<i>Opzet en bestaan</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet
	<i>Werking</i>	Niet van toepassing	Voldoet	Voldoet	Voldoet