Gemeentelijk kenmerk bijlage 1 DigiD:	E21.000390

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal Loket en aansluitnummer 1000281

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

- Digitaal Loket

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Exxellence Suite (Digitaal Loket en eFormulieren)

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Exxellence.

Deze applicatie is extern benaderbaar via het volgende internetadres(sen): www.nijmegen.nl via call to action knoppen op diverse plekken op deze site.

DigiD-aansluiting Digitaal Loket bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Exxellence in de vorm van SAAS.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Digitaal Loket. 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” van Logius.

Gemeente Nijmegen heeft een deel van de DigiD web-omgeving uitbesteed aan Exxellence. 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.

Een DigiD-aansluiting dient aan het gehele normenkader te 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. De overige normen worden afgedekt door onderstaande assurancerapportage van de gemeentelijke serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Exxellence
Referentie/rapportnummer:	AB/1024473/01
Afgiftedatum:	14 oktober 2020
Naam RE-auditor:	Jan Matto RE RI en Achmed Bouazza RE CISA
Ondertekend door RE-auditor:	Ja

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

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk 2C-2021-237.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle		• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer		• Voldoet	• Voldoet
U/WA.05	Cryptografie/Privacybevordering	• Voldoet	• Voldoet	• Voldoet
U/PW.02	Garanderen webprotocollen		• Voldoet	• Voldoet
U/PW.03	Configureren webserver		• Voldoet	• Voldoet
U/PW.05	Toegang tot beheermechanismen		• Voldoet	• Voldoet
U/PW.07	Hardening van platformen		• Voldoet	• Voldoet
U/NW.03	DMZ		• Voldoet	• Voldoet
U/NW.04	Protectie- en detectiemechanismen		• Voldoet	• Voldoet
U/NW.05	Scheiding beheer- en productieomgeving		• Voldoet	• Voldoet
U/NW.06	Hardening van netwerken	• Voldoet	• Voldoet	• Voldoet
C.03	Vulnerability-assessments		• Voldoet	• Voldoet
C.04	Penetratietesten			

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
			• Voldoet	• Voldoet
C.06	Signaleringsfuncties		• Voldoet	• Voldoet
C.07	Monitoring functies		• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet

Bijlage 1 DigiD (2)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Parkeerproducten gemeente Nijmegen en aansluitnummer 1000397

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

- Het aanvragen, wijzigen en verlengen van parkeervergunningen
- De DigiD-koppeling zelf

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- CityPermit versie 1.24

Deze applicatie betreft [[maak een keuze uit een geheel standaardpakket en wordt onderhouden door Exite ICT B.V.

Deze applicatie is extern benaderbaar via het volgende internetadres(sen): 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 Exite ICT B.V. in de vorm van SAAS.

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” van Logius.

Gemeente Nijmegen heeft een deel van de DigiD web-omgeving uitbesteed aan Sigmax. 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.

Een DigiD-aansluiting dient aan het gehele normenkader te 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. De overige normen worden afgedekt door onderstaande assurancerapportage van de gemeentelijke serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Sigmax
Referentie/rapportnummer:	2009R.AH70
Afgiftedatum:	18 november 2020
Naam RE-auditor:	Drs. A.J.A. Hassing RE RA
Ondertekend door RE-auditor:	Ja

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

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk 2C-2021-237.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle		• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer		• Voldoet	• Voldoet
U/WA.05	Cryptografie/Privacybevordering	• Voldoet niet	• Voldoet	• Voldoet niet
U/PW.02	Garanderen webprotocollen		• Voldoet	• Voldoet
U/PW.03	Configureren webserver		• Voldoet niet	• Voldoet niet
U/PW.05	Toegang tot beheermechanismen		• Voldoet	• Voldoet
U/PW.07	Hardening van platformen		• Voldoet	• Voldoet
U/NW.03	DMZ		• Voldoet	• Voldoet
U/NW.04	Protectie- en detectiemechanismen		• Voldoet	• Voldoet
U/NW.05	Scheiding beheer- en productieomgeving		• Voldoet	• Voldoet
U/NW.06	Hardening van netwerken	• Voldoet	• Voldoet	• Voldoet
C.03	Vulnerability-assessments		• Voldoet	• Voldoet
C.04	Penetratietesten			

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
			• Voldoet	• Voldoet
C.06	Signaleringsfuncties		• Voldoet	• Voldoet
C.07	Monitoring functies		• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet

Bijlage 1 DigiD (3)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting gemeente Nijmegen en aansluitnummer 1000697

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

- Het opladen van persoonsgegevens in de IRMA-app

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- IRMA

Deze applicatie betreft een combinatie van maatwerk en standaard software en wordt onderhouden door gemeente Nijmegen.

Deze applicatie is extern benaderbaar via de volgende internetadres(sen):

https://services.nijmegen.nl/irma/gemeente/start

DigiD aansluiting gemeente Nijmegen bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door gemeente Nijmegen in de vorm van fysieke hosting.

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” van Logius.

Een DigiD-aansluiting dient aan het gehele normenkader te 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.

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie het gehele normenkader afdekt. Het kan voorkomen dat een norm deels bij een leverancier en deels bij de gemeente getoetst is (zogenaamde gedeelde norm).

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk 2C-2021-237.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle	• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer	• Voldoet	• Voldoet

DigiD Norm		Getoetst bij Gemeente	Totaal oordeel norm
U/WA.05	Cryptografie/Privacybevordering	• Voldoet	• Voldoet
U/PW.02	Garanderen webprotocollen	• Voldoet	• Voldoet
U/PW.03	Configureren webserver	• Voldoet niet	• Voldoet niet
U/PW.05	Toegang tot beheermechanismen	• Voldoet	• Voldoet
U/PW.07	Hardening van platformen	• Voldoet	• Voldoet
U/NW.03	DMZ	• Voldoet	• Voldoet
U/NW.04	Protectie- en detectiemechanismen	• Voldoet	• Voldoet
U/NW.05	Scheiding beheer- en productieomgeving	• Voldoet	• Voldoet
U/NW.06	Hardening van netwerken	• Voldoet	• Voldoet
C.03	Vulnerability-assessments	• Voldoet	• Voldoet
C.04	Penetratietesten	• Voldoet niet	• Voldoet niet
C.06	Signaleringsfuncties	• Voldoet	• Voldoet
C.07	Monitoring functies	• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet
C.09	Patchmanagement	• Voldoet	• Voldoet

Bijlage 1 DigiD (4)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Nijmegen Inkomensondersteuning en aansluitnummer 1003381

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

- Aanvraag van sociale regelingen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Forus & Me versie 0.8.2

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Stichting Forus.

Deze applicatie is extern benaderbaar via het volgende internetadres(sen): 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 Stichting Forus in de vorm van SAAS.

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting Gemeente Nijmegen Inkomensondersteuning. 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” van Logius.

Nijmegen heeft een deel van de DigiD web-omgeving uitbesteed aan Stichting Forus. 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.

Een DigiD-aansluiting dient aan het gehele normenkader te 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. De overige normen worden afgedekt door onderstaande TPM van de gemeentelijke serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Stichting Forus
Referentie/rapportnummer:	BKBO/200916-1/V1/TPM
Afgiftedatum:	8 maart 2021
Naam RE-auditor:	Drs. M.B.H. IJpelaar RE CEH CISA Mr W.R. Nanninga RE CISA MMC
Ondertekend door RE-auditor:	Ja

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

De uitkomst uit de zelfevaluatie is getoetst door onze RE-gecertificeerde IT-auditor. De conclusie van de auditor is opgenomen in het assurancerapport met kenmerk 2C-2021-237.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
B.05	Contractmanagement	• Voldoet	• Voldoet	• Voldoet
U/TV.01	Identificatie en authenticatie	• Voldoet	• Voldoet	• Voldoet
U/WA.02	Webapplicatiebeheer proces	• Voldoet	• Voldoet	• Voldoet
U/WA.03	Automatische data invoer controle		• Voldoet	• Voldoet
U/WA.04	Normaliseren uitvoer		• Voldoet	• Voldoet
U/WA.05	Cryptografie/Privacybevordering		• Voldoet	• Voldoet
U/PW.02	Garanderen webprotocollen		• Voldoet	• Voldoet
U/PW.03	Configureren webserver		• Voldoet	• Voldoet
U/PW.05	Toegang tot beheermechanismen		• Voldoet	• Voldoet
U/PW.07	Hardening van platformen		• Voldoet	• Voldoet
U/NW.03	DMZ		• Voldoet	• Voldoet
U/NW.04	Protectie- en detectiemechanismen		• Voldoet	• Voldoet
U/NW.05	Scheiding beheer- en productieomgeving		• Voldoet	• Voldoet
U/NW.06	Hardening van netwerken	• Voldoet	• Voldoet	• Voldoet
C.03	Vulnerability-assessments		• Voldoet	• Voldoet
C.04	Penetratietesten			

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier 1	Totaal oordeel norm
			• Voldoet	• Voldoet
C.06	Signaleringsfuncties		• Voldoet	• Voldoet
C.07	Monitoring functies		• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet