

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Raalte en aansluitnummer 1002569

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

- Aangifte geboorte
- Aangifte verhuizing
- Aanvraag afschrift Burgerlijke stand
- Aanvraag afschrift Burgerlijke stand voor bedrijven
- Aanvraag bewijs van in leven zijn
- Aanvraag bewijs van Nederlanderschap
- Aanvraag uittreksel BRP
- Aanvraag uittreksel BRP voor bedrijven
- Verstrekking beperking
- Wijziging naamgebruik
- Melding huwelijk/geregistreerd partnerschap
- Aangifte overlijden

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- iBurgerzaken, versie 3.7

Deze applicatie betreft geheel standaardpakket en wordt onderhouden door PinkRoccade LG.

Deze applicatie is extern benaderbaar via de volgende URL: <https://iburgerzaken.raalte.nl>.

DigiD aansluiting Gemeente Raalte bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd Pink Roccade LG in de vorm van SAAS.

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Gemeente Raalte. De zelfevaluatie heeft zich gericht op de webapplicatie, de URL 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 Raalte heeft een deel van de DigiD webomgeving uitbesteed aan Pink Roccade LG. 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 onze leverancier[s] valt. De overige normen worden afgedekt door onderstaande TPM van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	PinkRoccade Local Government B.V.
Referentie/rapportnummer:	20201112 DBA-PRLG
Afgiftedatum:	12 november 2020

Alleen voor identificatie doeleinden

M. Hommes RE

Gemeentelijk kenmerk bijlage 1 DigiD:	DigiD 24008-2021
--	------------------

Naam RE-auditor:	Frank Kossen RE Laurens van Thiel CISA CISSP CEH Drs. M. El Aarbaoui RE (QA)
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 202103 100 Raalte.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm opnemen indien van toepassing inclusief de normen die getoetst zijn bij leverancier.

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

Hoeft volgens de gemeente en volgens hoofdstuk “verantwoordelijkheden gebruikersorganisatie” van de TPM van de serviceorganisatie niet bij de gemeente en/of bij leverancier getoetst te worden.

Alleen voor identificatie doeleinden

M. Hommes RE

Bijlage 1 DigiD (2)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Digitaal Loket Gemeente Raalte en aansluitnummer 1000313

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

- Digitaal loket voor burgers en bedrijven met daarin formulieren.
- Een Producten en Diensten Catalogus (PDC).

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Atos e-Suite, versie 4.24

Deze applicatie betreft geheel standaardpakket en wordt ontwikkeld en onderhouden door Atos

Deze applicatie is extern benaderbaar via de volgende URL: <https://dloket.raalte.nl>.

DigiD aansluiting Digitaal Loket Gemeente Raalte bevindt zich in een DMZ. De infrastructuur waar deze applicatie op draait wordt beheerd door SSC Twente in de vorm van fysieke hosting.

Het object van zelfevaluatie is de webomgeving van DigiD aansluiting Digitaal Loket Gemeente Raalte. De zelfevaluatie heeft zich gericht op de webapplicatie, de URL 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 Raalte heeft een deel van de DigiD webomgeving uitbesteed aan Dimpact en Dimpact heeft het ontwikkelen van de webapplicatie en het beheer van de infrastructuur uitbesteed aan serviceorganisaties Atos en SSC Twente. Dimpact maakt voor haar beschrijving gebruik van de opnamemethode ('inclusive method'). De beschrijving van de serviceorganisatie van haar systeem omvat tevens de aard van de diensten die door de subserviceorganisaties worden verleend. De relevante interne beheersingsdoelstellingen van die subserviceorganisaties en daarmee verband houdende interne beheersingsmaatregelen zijn opgenomen in de beschrijving van de serviceorganisatie van haar systeem en in de reikwijdte van de opdracht van de auditor van de serviceorganisatie. Als gevolg hiervan is 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 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 onze leverancier[s] valt. De overige normen worden afgedekt door onderstaande TPM van onze serviceorganisatie:

Leverancier 1	
Naam serviceorganisatie:	Dimpact (inclusief Atos en SSC Twente)
Referentie/rapportnummer:	2011R.AH130
Afgiftedatum:	4 december 2020
Naam RE-auditor:	drs. A.J.A. Hassing RE RA
Ondertekend door RE-auditor:	Ja

Alleen voor identificatie doeleinden

M. Hommes RE

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 (zogenoemde 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 202103 100 Raalte.

Onderstaande tabel toont de uitkomsten van de zelfevaluatie per norm.

DigiD Norm		Getoetst bij Gemeente	Getoetst bij leverancier	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		• <i>Voldoet niet</i>	• <i>Voldoet niet</i>
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		• Voldoet	• Voldoet
C.06	Signaleringsfuncties		• Voldoet	• Voldoet
C.07	Monitoring functies		• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet
Hoeft volgens de gemeente en volgens hoofdstuk "verantwoordelijkheden gebruikersorganisatie" van de TPM van de serviceorganisatie niet bij de gemeente en/of bij leverancier getoetst te worden.				

Alleen voor identificatie doeleinden

M. Hommes RE