

Bijlage 1 DigiD (1)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Rijswijk en aansluitnummer 1000433

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

- Het aanvragen en volgen van gemeentelijke producten en diensten;
- Het maken van afspraken.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Mijn Rijswijk

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

Deze applicatie is extern benaderbaar via het volgende internetadres: secure.rijswijk.nl.

DigiD-aansluiting Gemeente Rijswijk bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door de gemeenschappelijke regeling bedrijfsvoering Delft-Rijswijk in de vorm van fysieke hosting.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Rijswijk. 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.

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 VDB.20210413.02.

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
U/WA.05	Cryptografie/ Privacy bevordering	• 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	• Voldoet
C.06	Signaleringsfuncties	• Voldoet	• Voldoet
C.07	Monitoring functies	• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet
C.09	Patchmanagement	• Voldoet	• Voldoet

Bijlage 1 DigiD (2)

Totaaloverzicht getoetste normen ICT-beveiligingsassessment

DigiD-aansluiting Gemeente Rijswijk - Parkeerloket en aansluitnummer 1002318

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

- Het aanvragen, wijzigen en verlengen van parkeervergunningen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- CityPermit

Deze applicatie betreft een geheel standaardpakket en wordt onderhouden door Sigmax Law Enforcement B.V.

Deze applicatie is extern benaderbaar via het volgende internetadres: parkeren.rijswijk.nl.

DigiD aansluiting Gemeente Rijswijk - Parkeerloket bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait wordt beheerd door Sigmax Law Enforcement B.V. in de vorm van SAAS.

Het object van zelfevaluatie is de web-omgeving van DigiD aansluiting Gemeente Rijswijk - Parkeerloket. 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.

Rijswijk heeft een deel van de DigiD web-omgeving uitbesteed aan Sigmax Law Enforcement B.V.. 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[s] van de gemeente valt. De overige normen worden afgedekt door onderstaande TPM / assurancerapportage van de gemeentelijke serviceorganisatie[s]:

Leverancier 1	
Naam serviceorganisatie:	Sigmax Law Enforcement B.V.
Referentie/rapportnummer:	2009R.AH72
Afgiftedatum:	18 november 2020
Naam RE-auditor:	drs. A.J.A. Hassing
Ondertekend door RE-auditor:	Ja

Onze IT-auditor heeft tevens getoetst of de zelfevaluatie en de TPM / assurancerapportage 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 VDB.20210413.02.

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

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 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		• Voldoet	• Voldoet
C.06	Signaleringsfuncties		• Voldoet	• Voldoet
C.07	Monitoring functies		• Voldoet	• Voldoet
C.08	Wijzigingenbeheer	• Voldoet	• Voldoet	• Voldoet
C.09	Patchmanagement		• Voldoet	• Voldoet