

## Bijlage 1 DigiD - Gemeente Aalsmeer - Mijn Aalsmeer - 1003953

### Totaaloverzicht getoetste normen ICT-beveiligingsassessment

#### DigiD-aansluiting Gemeente Aalsmeer - Mijn Aalsmeer met aansluitnummer 1003953

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

- Het aanvragen van verscheidene producten en diensten en het doen van meldingen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Naam: Rx.Enterprise
- Versie: 2.19.6

Deze webapplicatie is extern benaderbaar via het volgende internetadres:

- <https://loket.aalsmeer.nl>.

Het object van zelfevaluatie is de web-omgeving van DigiD-aansluiting Gemeente Aalsmeer - Mijn Aalsmeer. 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 standaardpakket. De webapplicatie wordt onderhouden door Visma Roxit BV.

DigiD-aansluiting Gemeente Aalsmeer - Mijn Aalsmeer bevindt zich in de Demilitarized Zone (DMZ). De infrastructuur waar deze applicatie op draait, wordt beheerd door Visma Roxit BV met beheervorm SaaS-dienst. Technisch beheer leverancier, functioneel beheer gemeente; team applicatiebeheer.

Gemeente Aalsmeer heeft de DigiD web-omgeving uitbesteed aan:

- Visma Roxit BV.

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:	30-10-2024
Controleperiode:	1 juli 2024 t/m 31 december 2024

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

SaaS-leverancier	
Naam SaaS-leverancier:	Visma Roxit BV
Referentie/rapportnummer:	TPM: BKBO/240402-01/1/TPM Sub-TPM: N.v.t.
Oordeelsdatum:	TPM: 30-08-2024 Sub-TPM: N.v.t.
Controleperiode:	TPM: 1 januari 2024 tot 30 augustus 2024

SaaS-leverancier	
	Sub-TPM: N.v.t.
Naam RE-auditor	TPM: drs. M.B.H. Ijpelaar RE CEH CISA CIPP/e, drs. M.T.C. Akay CISA 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 Wdn/nda/9874.

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