Third Party Memorandum DigiD

2022-2023

ISAE3000/D Type I

Visma Circle

Djuma eLoket 2022.180.001

Kenmerk BKBO/220524-1/TPM

23 september 2022
Dit assurancerapport heeft 20 pagina's
www.bkbo.nl

Heelal

Hoe verder men keek,
hoe groter het leek.

Jules Deelder

Colofon

Voor u ligt het TPM rapport van het DigiD ICT beveiligingsassessment dat wij uitvoerden op de betrouwbare en integere werking van de webapplicatie Djuma eLoket van Visma Circle BV. In dit rapport worden de door ons vastgestelde bevindingen, conclusies en aanbevelingen beschreven.

Inhoudsopgave

1 Assurancerapport van de onafhankelijke auditor

1.1 Opdracht

Ingevolge de opdracht van Visma Circle BV (hierna: "opdrachtgever") hebben wij een DigiD ICT-beveiligingsassessment uitgevoerd op de webomgeving van de DigiD aansluitingen zoals gespecificeerd in hoofdstuk 3 Object van onderzoek.

Het onderzoek is conform Normenkader 3.0 van Logius uitgevoerd, aangevuld met NOREA update 20 november 2020 DigiD Assessments met meervoudige aansluiting versie 1.0 en de vigerende FAQ DigiD assessment van NOREA.

Wij hebben de regelgeving van de NOREA voor kwaliteitsbeheersing toegepast en onderhouden een inzichtelijk stelsel van kwaliteitsbeheersing met inbegrip van gedocumenteerde beleidslijnen en procedures met betrekking tot het naleven van ethische voorschriften, professionele richtlijnen en van toepassing zijnde, door wet- of regelgeving gestelde, vereisten.

De opdracht omvatte het onderzoeken van de opzet en het bestaan van maatregelen en procedures gericht op de ICT-beveiliging van de webomgeving voor de in hoofdstuk 3 gespecificeerde houders van DigiD aansluitingen.

De opdrachtgever maakt gebruik van de sub-serviceorganisatie Enable-U voor de levering van 2Secure Gateway, en maakt gebruik van de IAAS oplossing van Uniserver BV. De opdrachtgever maakt voor haar beschrijving gebruik van de inclusive methode. De beschrijving van de sub-serviceorganisatie(s) van haar systeem omvatten daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de sub-serviceorganisatie(s). Onze werkzaamheden strekken zich dan ook uit tot de interne beheersingsmaatregelen van de sub-serviceorganisatie(s).

Hoofdstuk 4 'Verantwoordelijkheid gebruikersorganisatie' verwijst naar de behoefte aan aanvullende interne beheersingsmaatregelen van de gebruikersorganisaties. De geschiktheid van de opzet, het bestaan of de werking van deze aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie hebben wij niet geëvalueerd. Aan de beveiligingsrichtlijnen van de vigerende 'Norm ICT-beveiligingsassessments DigiD' wordt alleen voldaan, indien aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie samen met de interne beheersingsmaatregelen van de serviceorganisatie op afdoende wijze zijn opgezet en geïmplementeerd.

1.2 Verantwoordelijkheden van de opdrachtgever

De opdrachtgever is verantwoordelijk voor de beschrijving van het object van onderzoek, het verlenen van diensten, het onderkennen van de beveiligingsrisico's van de webomgeving en het opzetten en implementeren van interne beheersingsmaatregelen om te voldoen aan de "Norm ICT-beveiligingsassessments DigiD" zoals opgesteld door Logius.

1.3 Verantwoordelijkheden van de auditor

Onze verantwoordelijkheid is, op basis van onze werkzaamheden, het geven van oordelen per beveiligingsrichtlijn van de vigerende "Norm ICT-beveiligingsassessments DigiD" van Logius, over de opzet en het bestaan van de maatregelen gericht op de ICT beveiliging van de webomgeving van de DigiD aansluiting.

We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht en de NOREA richtlijn 3000, 'Richtlijn Assurance-opdrachten door IT-auditors'. Dit vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of de interne beheersingsmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet en bestaan.

Een assuranceopdracht om te rapporteren over *opzet* en *bestaan* van interne beheersingsmaatregelen bij een organisatie omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet en het bestaan van interne beheersingsmaatregelen. De geselecteerde werkzaamheden zijn afhankelijk van de door de auditor van de organisatie toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet of niet bestaan.

Zoals hierboven staat vermeld, hebben wij geen werkzaamheden uitgevoerd met betrekking tot de *werking* van interne beheersingsmaatregelen die bij de beschrijving waren inbegrepen; wij brengen derhalve daarover geen oordelen tot uitdrukking. Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor onze oordelen te bieden.

1.4 Beperkingen

Wij kunnen geen verantwoordelijkheid aanvaarden voor wijzigingen in de door ons gehanteerde feiten en omstandigheden na de datum waarop wij de desbetreffende

werkzaamheden hebben afgerond, tenzij wij tijdig van de wijzigingen in de door ons gehanteerde feiten en omstandigheden op de hoogte zijn gebracht.

De 'Norm ICT-beveiligingsassessments DigiD' is een selectie van beveiligingsrichtlijnen uit de "ICT-beveiligingsrichtlijnen voor webapplicatie" van het Nationaal Cyber Security Centrum (NCSC). Daarom zijn we niet in staat om een overall oordeel te verschaffen omtrent de beveiliging van de DigiD-aansluiting.Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen van de betreffende DigiD-aansluiting en brengen daarover geen oordeel tot uitdrukking.

Logius heeft de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties. Wij adviseren de organisatie om in aanvulling op de richtlijnen in de "Norm ICT-beveiligingsassessments DigiD", ook de andere richtlijnen uit de "ICT-beveiligingsrichtlijnen voor webapplicaties" van het NCSC te adopteren.

Wij wijzen u erop dat, indien wij aanvullende beveiligingsrichtlijnen zouden hebben onderzocht wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.

In de volgende paragraaf geven wij onze oordelen ten aanzien van de 'Norm ICT-beveiligingsassessments DigiD'.

1.5 Oordelen

Onze oordelen zijn gevormd op basis van de werkzaamheden zoals ze zijn beschreven in deze rapportage. Per beveiligingsrichtlijn van de 'Norm ICT-beveiligingsassessments DigiD' van Logius wordt een oordeel gegeven over de opzet en het bestaan per 23 september 2022. De criteria waarvan wij gebruik hebben gemaakt, zijn opgenomen in onderstaande tabel en een toelichting is te vinden in hoofdstuk 2.

Per beveiligingsrichtlijn hebben wij hieronder vermeld of met redelijke mate van zekerheid wordt voldaan aan de beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de conclusies in deze tabel weergegeven als "voldoet" of "voldoet niet". Hierbij moet "voldoet" worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn volgens de criteria genoemd in hoofdstuk 2 in alle materiële opzichten effectief zijn". "Voldoet niet" moet worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel

aangegeven beveiligingsrichtlijn volgens de criteria genoemd in hoofdstuk 2 niet in alle materiële opzichten effectief zijn".

De uitspraak "voldoet" of "voldoet niet" beperkt zich tot de eigen oordeelsvorming van de auditor. Ons onderzoek was beperkt tot de beveiligingsrichtlijnen die de verantwoordelijkheid zijn van de serviceorganisatie Visma Circle BV.

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	☑
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	☑
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	☑
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	☑
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	☑
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	☑
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	☑
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	☑
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	☑
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.	☑
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	☑
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.	☑
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	☑
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	☑
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	☑
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	☑
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	☑
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	☑

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	☑
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	☑
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	☑

1.6 Beoogde gebruikers en doel

De minister van BZK wil een structurele en forse impuls geven aan de kwaliteitsverhoging van ICT-beveiliging bij overheidsorganisaties die gebruik maken van DigiD. Deze organisaties moeten jaarlijks een ICT beveiligingsassessment laten verrichten onder verantwoordelijkheid van een gekwalificeerde IT-auditor (RE), teneinde de DigiD gebruikende organisaties en Logius inzicht te geven in de ICT beveiliging van de webomgeving van DigiD aansluiting.

Onze schriftelijke rapportage is alleen bestemd voor de serviceorganisatie Visma Circle BV, haar cliënten en hun auditors en Logius aangezien anderen, die niet op de hoogte zijn van de precieze scope, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren. De rapportage, bijlagen, onderdelen of samenvattingen daarvan mogen niet mondeling of schriftelijk aan derden beschikbaar worden gesteld zonder onze voorafgaande schriftelijke toestemming. De bijlagen A en B zijn alleen bestemd voor de serviceorganisatie.

Voor zover het de opdrachtgever is toegestaan het rapport aan derden beschikbaar te stellen, zal het rapport origineel, volledig en ongewijzigd beschikbaar worden gesteld. Indien de producten van onze werkzaamheden aan derden ter beschikking worden gesteld, dient erop te worden gewezen dat zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming geen rechten aan het product kunnen worden ontleend. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden.

Vlijmen d.d. 23 september 2022

BKBO b.v.

	{{Signer1}} Signed By: IJPELAAR MARTINUS BENEDICTUS HERMANN 2022-09-23T10:45:43+02:00 ID: f1655132-2df6-457a-9639-a2a1ee7b302f Auth: itsmesign	
mr W.R. Nanninga RE CISA MMC, partner	drs. M.B.H. IJpelaar RE CEH CISA, directeur	drs. M.T.C. Akay CISA, auditor

2 Criteria

Logius heeft de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties. De criteria waarvan gebruik is gemaakt bij het uitvoeren van deze assurance opdracht hielden in dat:

a) De interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd.

b) De risico's die het voldoen aan de beveiligingsrichtlijnen in gevaar brengen en daarmee de betrouwbaarheid van DigiD aantasten, werden onderkend.

c) De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het voldoen aan beveiligingsrichtlijnen niet zouden verhinderen.

3 Object van onderzoek

Het object van onderzoek was de webomgeving van de volgende DigiD aansluitingen:

Houder DigiD aansluiting	URL
Aa en Maas	Eloket.aaenmaas.nl
Almere	Eloket.almere.nl
Apeldoorn	Eloket.apeldoorn.nl
Arnhem	eloket.arnhem.nl
Bergen	eloket.bergen.nl
Brabantse Delta	Eloket.brabantsedelta.nl
Brunssum	eloket.brunssum.nl
BVOWB - Culemborg	eloket.culemborg.nl
BVOWB - Tiel	eloket.tiel.nl
BVOWB - West-Betuwe	eloket.westbetuwe.nl
CvdM	Eloket.cvdm.nl
de Dommel	Mijnwaterschap.dommel.nl
Dommelvallei - Geldrop Mierlo	Eloket.geldropmierlo.nl
Dommelvallei - Nuenen	Eloket.Nuenen.nl
Dommelvallei - Son en Breugel	Eloket.sonenbreugel.nl
Dronten	eloket.dronten.nl
Elburg	eloket.elburg.nl
Gennep	Eloket.gennep.nl
H2O	
Haarlemmermeer	
Harlingen	Eloket.harlingen.nl
Helmond	eloket.helmond.nl/#/p.
Heumen	Eloket.heumen.nl
Hulst	eloket.gemeentehulst.nl
Ijsselstein	eloket.gemeenteijsselstein.nl
Katwijk	loket.katwijk.nl
Krimpenerwaard	Eloket.krimpenerwaard.nl
Leusden	loket.leusden.nl
Maastricht	eloket.gemeentemaastricht.nl
Meerssen	Eloket.meerssen.nl
Meierijstad	zaken.meierijstad.nl
Meppel	eloket.meppel.nl
Middelburg	Eloket.middelburg.nl
Midden-Groningen	Eloket.midden-groningen.nl
Nationale Ombudsman	
Nieuwkoop	mijnloket.nieuwkoop.nl
Nissewaard	
Peel en Maas	Eloket.peelenmaas.nl
Putten	Eloket.putten.nl
Rijn en Braassem - Alphen	onlineregelen.alphenaandenrijn.nl

Rijn en Braassem - Kaag en Braassem	onlineregelen.kaagenbraassem.nl
Rijn en Ijssel	Eloket.wrij.nl
SBB	eloket.s-bb.nl
s-Hertogenbosch	
Twenterand	eloket.twenterand.nl
Veldhoven	Formulieren.veldhoven.nl
Vlissingen	eloket.vlissingen.nl
Waddinxveen	
Weert	eloket.weert.nl
Winterswijk	Eloket.Winterswijk.nl

Specifiek zijn in scope de internet-facing webpagina's, de systeemkoppelingen (authenticatieverzoek en uitwisselen RID en verificatieverzoek van de webdienst) en de infrastructuur die met DigiD gekoppeld is en betrekking heeft op het DigiD identificatie en authenticatieproces. Ook de verschillende vormen van beheer op de webomgeving zijn in scope voor zover relevant voor de doelstelling van de audit. Deze TPM geldt dus niet voor eventuele andere inlogmethoden.

De opdrachtgever biedt de volgende functionaliteit aan waarvoor DigiD ter authenticatie wordt gebruikt:

Het Djuma eLoket is onderdeel van het multi-tenant zaaksysteem Djuma. Binnen het Djuma eLoket is er een onderscheid tussen de eFormulieren en het klantportaal PIP. Via de eFormulieren, kunnen burgers formulieren kunnen ontsluiten en inzenden. Middels het PIP kan een burger de status bekijken van de door hem/haar aangemaakt zaak. Eventueel kunnen opmerkingen en/of documenten worden toegevoegd.

Deze functionaliteit wordt geboden door de volgende webapplicatie(s):

- Djuma eLoket
- Enable-U 2Secure API Gateway

De gateway van Enable-U functioneert hierbij als koppeling tussen Logius en het zaaksysteem en voorziet in validatie van verbindingskenmerken.

De onderzochte versie van Djuma eLoket is:

- 2022.180.001

Deze applicatie betreft geheel standaard software en wordt als SAAS onderhouden door Visma Circle BV. De infrastructuur waarop de applicatie draait wordt eveneens beheerd door Visma Circle BV.

Het onderzoek heeft zich gericht op de webapplicatie, de URLs waarmee deze applicatie 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.

In bijlage B geven wij u een meer gedetailleerde beschrijving van het object van onderzoek.

4 Verantwoordelijkheden gebruikersorganisatie

Bij de opzet en implementatie van interne beheersingsmaatregelen bij de serviceorganisatie wordt aangenomen dat voor sommige beveiligingsrichtlijnen van de "Norm ICT-beveiligingsassessments DigiD", enkele interne beheersingsmaatregelen door de houderorganisaties zelf zullen worden geïmplementeerd om te kunnen voldoen aan deze beveiligingsrichtlijnen.

In de onderstaande tabel wordt aangegeven voor welke beveiligingsrichtlijn(en) deze aanname is gedaan en welke gewenste interne beheersingsactiviteit bij de gebruikersorganisaties kunnen worden geïmplementeerd om te voldoen aan de desbetreffende beveiligingsrichtlijn van de 'Norm ICT-beveiligingsassessments DigiD' van Logius.

De geschiktheid van de opzet en het bestaan van deze aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie hebben wij niet geëvalueerd. Aan de beveiligingsrichtlijnen van de 'Norm ICT-beveiligingsassessments DigiD' wordt alleen voldaan, indien aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie samen met de interne beheersingsmaatregelen van de serviceorganisatie op afdoende wijze zijn opgezet en geïmplementeerd.

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	De gebruikersorganisatie dient ervoor zorg te dragen dat: • het eigenaarschap t.a.v. de DigiD webapplicatie adequaat op een hoog organisatorisch niveau is inricht; • de eigenaar passende bevoegdheden heeft; • in het informatiebeveiligingsbeleid, of in een hiervoor apart ontwikkeld beleid, expliciet aandacht is besteed aan het stelsel van beveiligingsmaatregelen t.a.v. het functioneel beheer van de webapplicatie • toegangsvoorziening (U/TV.01), • dataclassificatie (U/WA.05) en kwetsbaarhedenbeheer (U/NW.06, t.a.v. DNSSEC) hierin zijn geadresseerd.
B.05	In een contract met een derde partij voor de uitbestede levering of beheer van een webapplicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	De houder(s) van de DigiD-aansluiting moeten de afspraken met de serviceorganisatie vastleggen in een overeenkomst waarbij o.a. de volgende zaken zijn opgenomen: • een beschrijving van de te leveren diensten die onder het contract vallen; • de van toepassing zijnde leveringsvoorwaarden; • informatiebeveiligingseisen met de relevante eisen vanuit het beveiligingsbeleid; • het melden van beveiligingsincidenten;

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
		• de behandeling van gevoelige gegevens; • wanneer en hoe de leverancier toegang tot de systemen/ data van de gebruikersorganisatie mag hebben; • Service Level Reporting; • het jaarlijks uitvoeren van audits bij de leverancier(s); • beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke sub-leveranciers. De serviceorganisatie Visma Circle BV moet een Service Level Rapportage (= SLR) aanleveren over de behaalde serviceniveaus.
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.	Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van Visma Circle BV en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie. De gebruikersorganisatie moet maatregelen ontwerpen en inrichten met betrekking tot toegangsbeveiliging en -beheer. Hierbij valt te denken aan: • het toekennen, controleren en intrekken van autorisaties; • het stellen van eisen aan de wachtwoordinstellingen; • een aantoonbare controle op joiners/movers/leavers; • het wijzigen van de standaard wachtwoorden van administrator accounts; • het beperken eventuele shared accounts. • Het uitvoeren periodieke (minimaal jaarlijkse) reviews. Alle accounts dienen individueel te zijn en er dient door de houder van de DigiD-aansluiting een autorisatiematrix te worden opgesteld en beheerd. Specifieke aandacht gaat uit naar wachtwoorden die leveranciers hebben om toegang tot de systemen of data van de houder van de DigiD aansluiting te krijgen (wie hebben die wachtwoorden, hoe worden die opgeslagen en wie hebben toegang. Hoe vaak worden ze gewijzigd, etc.).
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van Visma Circle BV en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie. De houder van de DigiD aansluiting moet maatregelen ontwerpen en inrichten met betrekking tot: • de beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen;

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
		• het opstellen van een incidentenprocedure; • het registreren, analyseren, opvolgen en afhandelen van incidenten; • het analyseren en zo nodig opvolgen van meldingen van het NCSC of IBD of Z-CERT of andere CERTS; • het periodiek rapporteren aan het management inzake beveiligingsincidenten.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van Visma Circle BV en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie. In ons onderzoek is vastgesteld dat de serviceorganisatie de vereiste maatregelen heeft genomen om de gevoelige gegevens te kunnen beschermen. Mede als gevolg van het wetsvoorstel Digitale Overheid, vinden we dat de gebruikersorganisatie als verwerkingsverantwoordelijke een risico analyse uit zou moeten voeren om na te gaan hoe de gevoelige persoonsgegevens beveiligd zijn. Men dient zorg te dragen voor: • het classificeren van de gegevens die met DigiD worden ontsloten conform de vigerende privacywetgeving en zo nodig met de leverancier in overleg te gaan over aanvullende beveiligingsmaatregelen zoals het versleutelen of hashen van gevoelige gegevens.
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van Visma Circle BV en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie. Onder deze beveiligingsrichtlijn valt dan ook het verplicht gebruik van DNSSEC (DNS Security Extensions) voor de URL van het object van onderzoek. Met DNSSEC wordt de authenticiteit van DNS-antwoorden geverifieerd om misbruik te voorkomen. Het regelen van DNSSEC is de verantwoordelijkheid van de gebruikersorganisatie.

Toelichting

C.08
De service organisatie onderhoudt maar één versie van de applicatie en deze wordt in productie gebracht door de leverancier. De gebruikersorganisatie heeft geen mogelijkheden om te testen. Wijzigingsbeheer is niet van toepassing voor de gebruikersorganisatie.

Aanvullende beheersmaatregelen voor de gemeente Almere en de gemeente Weert:

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersingmaatregelen van de gebruikersorganisatie
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	De API Gateway dient door de gebruikersorganisatie correct geconfigureerd te zijn, zodat op basis van een beschreven ontwerp netwerkverbindingen en veilige protocollen toegepast worden.
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.	De API Gateway dient door de gebruikersorganisatie correct geconfigureerd te zijn, zodat op basis van een beschreven ontwerp netwerkverbindingen en veilige protocollen toegepast worden.
U/NW.03	Het netwerk is gescheiden in fysieke en logische domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd worden.	De gebruikersorganisatie dient documentatie omtrent netwerkarchitectuur vastgesteld te hebben en aantoonbaar te maken of de API Gateway geconfigureerd is in lijn met vereisten vanuit de Norm ICT Beveiligingsassessments 3.0.
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	De gebruikersorganisatie dient te voorzien in inrichtingsdocumentatie van fysieke of logische scheiding tussen beheer- en productieverkeer over en richting de API Gateway, alsook de aantoonbaarheid hiervan.

Bijlage A – Rapport van bevindingen DigiD

Deze bijlage is niet bestemd voor de gebruikersorganisatie en wordt slechts verstrekt aan Visma Circle BV.

Bijlage B – Object van onderzoek

Deze bijlage is vertrouwelijk en niet bestemd voor de gebruikersorganisatie en wordt slechts verstrekt aan Visma Circle BV.

Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. Deze penetratietest zou specifiek gefocust mogen zijn op wijzigingen in de applicatie of de infrastructuur en behoeft niet noodzakelijkerwijs door een penetratietester te worden uitgevoerd die onafhankelijk staat ten opzichte van het te onderzoeken object.

Bijlage C – Rapportage penetratietest Defenced

Deze bijlage is niet bestemd voor de gebruikersorganisatie en wordt slechts verstrekt aan Visma Circle BV.