DigiD assessment serviceorganisatie

2023-2024

ISAE3000/D Type I

Forus Operations B.V.

Forus & Me v0.77.0

Kenmerk BKBO/200916-1/V4/TPM

Rapportdatum 10 oktober 2023
Oordeelsdatum 4 oktober 2023
Dit assurancerapport heeft 19 pagina's
www.bkbo.nl

Heelal

Hoe verder men keek,
hoe groter het leek.

Jules Deelder

Colofon

Voor u ligt het assurance rapport van het DigiD ICT beveiligingsassessment dat wij uitvoerden op het betrouwbaar en integer functioneren van de webapplicatie Forus & Me van Forus Operations B.V. In dit rapport worden de door ons vastgestelde bevindingen, conclusies en aanbevelingen beschreven.

Inhoudsopgave

1 Assurancerapport van de onafhankelijke auditor

Aan: management van Forus Operations B.V. en gebruikersorganisaties

1.1 Onze oordelen

Wij hebben een DigiD-beveiligingsassessment met redelijke mate van zekerheid uitgevoerd op de webomgeving van de aansluithouders welke zijn vermeld in paragraaf 1.4.1 Object van onderzoek.

Per beveiligingsrichtlijn hebben wij hieronder vermeld of 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 effectief is opgezet en geïmplementeerd op 4 oktober 2023". "Voldoet niet" moet worden geïnterpreteerd als "Wij zijn van oordeel dat de interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief is opgezet en/of geïmplementeerd op 4 oktober 2023".

De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die zijn beschreven in de sectie 'Van toepassing zijnde criteria'.

Onze oordelen zijn gevormd op basis van de van de aangelegenheden die in dit assurancerapport zijn uiteengezet. Ons onderzoek was beperkt tot de beveiligingsrichtlijnen die de verantwoordelijkheid zijn van de serviceorganisatie.

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.	Voldoet
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.	Voldoet
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.	Voldoet
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Voldoet

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel
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.	Voldoet
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	Voldoet
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.	Voldoet
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Voldoet
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Voldoet
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	Voldoet
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Voldoet
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Voldoet
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Voldoet
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.	Voldoet
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	Voldoet

1.2 De basis voor onze oordelen

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, waaronder de NOREA Richtlijn 3000D 'Assurance-opdrachten door IT-auditors (Directe-opdrachten)'. Deze opdracht is gericht op het verkrijgen van een redelijke mate van zekerheid. Onze verantwoordelijkheden op grond hiervan zijn beschreven in de sectie 'Verantwoordelijkheden van de IT-auditor'.

Wij zijn onafhankelijk van Forus Operations B.V. en hebben voldaan aan de overige vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is als basis voor onze oordelen.

1.3 Van toepassing zijnde criteria

Voor deze opdracht heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties en heeft deze vermeld in 'Norm ICT-beveiligingsassessments DigiD' welke wij hebben gehanteerd bij dit onderzoek.

De criteria waarvan gebruik wordt gemaakt bij het uitvoeren van de assurance-opdracht houden in dat:

- de interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd;
- de risico's die het voldoen aan de beveiligingsrichtlijnen in gevaar brengen en daarmee de betrouwbaarheid van DigiD aantasten, werden onderkend;
- 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.

1.4 Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

1.4.1 Object van onderzoek

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

Houder DigiD aansluiting	DigiD aansluitnummer	DigiD aansluitnaam
Gemeente Nijmegen	1003381	Gemeente Nijmegen - inkomensondersteuning
Gemeente Westerkwartier	1003671	Gemeente Westerkwartier - Potjeswijzer
Gemeente Groningen	1003635	Gemeente Groningen - Stadjerpas
Gemeente Geertruidenberg	1003931	Gemeente Geertruidenberg - Kindregelingen
Gemeente Waalwijk	1004289	Gemeente Waalwijk - Paswijzer
Gemeente Schagen	1005121	Gemeente Schagen – Mee doen
Gemeente Eemsdelta		

Forus Operations B.V. biedt de volgende functionaliteit aan waarvoor DigiD aansluiting ter authenticatie wordt gebruikt:

- De webapplicatie Forus & Me wordt door de inwoners/burgers van de klanten van Forus Operations B.V. gebruikt voor de aanvraag van sociale regelingen.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- Forus & Me en aangezien de serviceorganisatie gebruik maakt van Continuous Deployment geldt deze rapportage vanaf 4 oktober 2023.

Deze applicatie betreft een geheel standaard pakket en wordt onderhouden door Forus Operations B.V.

De infrastructuur waarop de applicatie draait wordt beheerd door Forus Operations B.V.

Het onderzoek heeft zich gericht op de webapplicatie die gebruik maakt van DigiD voor de identificatie en authenticatie van de gebruikers. Specifiek zijn in scope de internet-facing webpagina's waarmee de interactie naar de gebruiker plaatsvindt als deze is geïdentificeerd en geauthentiseerd via DigiD, de systeemkoppelingen 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 webapplicaties zijn in scope voor zover relevant voor de doelstelling van de audit. De URL www.digid.nl, de token uitwisseling

tussen Logius en de webserver, de systemen die gegevens leveren of ophalen uit de webapplicatie, zoals backoffice informatiesystemen vallen buiten de scope. Subsystemen en koppelvlakken zijn in scope indien de primaire authenticatie van het systeem op basis van DigiD tot stand is gekomen.

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

1.4.2 Subservice organisaties

Forus Operations B.V. maakt gebruik van het PaaS-platform van de subserviceorganisatie Amazon Webservices, Inc. Forus Operations B.V. maakt voor het verschaffen van zekerheid over haar volledige webomgeving zoals beschreven onder het object van onderzoek gebruik van de uitsluitingsmethode ('carve-out method'). De beschrijving van de serviceorganisatie van haar systeem sluit daarmee de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van de subserviceorganisatie uit. Onze werkzaamheden strekken zich dan ook niet uit tot de interne beheersingsmaatregelen van de subserviceorganisatie. Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de genoemde assurance-rapportage(s). Wij kunnen dan ook geen enkele verantwoordelijkheid nemen m.b.t. de in die rapportage vermelde oordelen.

1.4.3 Norm ICT-beveiligingsassessment DigiD

De 'Norm ICT-beveiligingsassessments DigiD' is een selectie van beveiligingsrichtlijnen uit de 'ICT-beveiligingsrichtlijnen voor webapplicaties' 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.

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft de richtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact hebben op de veiligheid van DigiD-webapplicaties. Logius houdt in opdracht van BZK toezicht op het naleven van de Voorwaarden DigiD, waaronder de uitvoering van DigiD-assessments. Wij adviseren Forus Operations B.V. 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.

1.4.4 Beperkingen met betrekking tot interne beheersingsmaatregelen

Interne beheersingsmaatregelen bij een serviceorganisatie kunnen, vanwege hun aard, niet alle fouten of omissies voorkomen of ontdekken en corrigeren.

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.

Bovendien is het projecteren naar de toekomst van onze oordelen met betrekking tot de opzet en implementatie van interne beheersingsmaatregelen om de richtlijnen te bereiken, onderhevig aan het risico dat interne beheersingsmaatregelen ineffectief kunnen worden.

Ons oordeel is niet aangepast als gevolg van deze aangelegenheden.

1.5 Beoogde gebruikers en doel

Ons assurancerapport is uitsluitend bestemd voor de houder(s) van de DigiD-aansluiting van de webomgeving, haar cliënten en hun auditors en Logius om inzicht te geven in de ICT beveiliging van de webomgeving van DigiD aansluiting. Logius kan hiermee toezicht houden op de koppeling van DigiD met de webapplicatie van een aangesloten organisatie voor het vertrouwen in en de integriteit van elektronische (overheids)dienstverlening.

Bijlage A bevat de beschrijving van de uitgevoerde (test)werkzaamheden en onze oordelen en aanbevelingen ter verbetering van de DigiD-webomgeving.

Bijlage B bevat de (uitgebreide) beschrijving van het 'Object van onderzoek'.

De bijlagen A en B zijn alleen bestemd voor Forus Operations B.V.

Bijlage C is bedoeld om Logius een totaaloverzicht te verschaffen (‘volledigheid van de scope’) over de resultaten van verschillende assessments, indien gebruik is gemaakt van rapporten inzake subserviceorganisatie(s).

Bijlage D is bedoeld om Logius een totaaloverzicht te verschaffen (‘identificatie’) over de identificerende kenmerken van het DigiD-assessment, indien gebruik is gemaakt van assurancerapporten inzake subserviceorganisatie(s).

Ons assurancerapport inclusief bijlagen mag enkel worden gebruikt voor het doel waarvoor het is opgesteld door de beoogde gebruikers en dient niet te worden verspreid aan of te worden gebruikt door anderen.

1.6 Verantwoordelijkheden van Forus Operations B.V.

Het management van Forus Operations B.V. is verantwoordelijk voor het verlenen van DigiD-diensten, het onderkennen van de beveiligingsrisico’s van de DigiD-webomgeving en het opzetten en implementeren van interne beheersingsmaatregelen om te voldoen aan de vigerende ‘Norm ICT-beveiligingsassessments DigiD’.

1.7 Verantwoordelijkheid van de IT-auditor

Onze verantwoordelijkheid is het zodanig plannen en uitvoeren van ons onderzoek dat wij daarmee voldoende en geschikte assurance-informatie verkrijgen voor het door ons af te geven oordelen over de opzet en implementatie van interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen in overeenstemming met de hiervoor vermelde criteria.

Ons onderzoek is uitgevoerd met een hoge mate maar geen absolute mate van zekerheid waardoor het mogelijk is dat wij tijdens ons onderzoek niet alle materiële fouten en fraude ontdekken.

1.8 Onze onafhankelijkheid en kwaliteitsbeheersing

Wij passen de ‘Reglement Kwaliteitsbeheersing NOREA' (RKBN) toe. Op grond daarvan beschikken wij over een samenhangend stelsel van kwaliteitsbeheersing inclusief vastgelegde richtlijnen en procedures inzake de naleving van ethische voorschriften, professionele standaarden en andere relevante wet- en regelgeving.

Ons onderzoek om te rapporteren over opzet en bestaan van interne beheersingsmaatregelen bestond onder andere uit:

- Het verkrijgen van inzicht in de relevante kenmerken van de DigiD-webomgeving.
- Het vaststellen van de scope van het assessment, inclusief het vaststellen van de maatregelen die bij de service organisatie moeten worden onderzocht.
- Het houden van interviews met verantwoordelijke functionarissen, vooral gericht op het onderkennen van risico's en het onderzoek in hoeverre deze risico's worden afgedekt door maatregelen.
- Het evalueren van de opzet en het vaststellen van het bestaan van de relevante maatregelen. Dit door middel van het kennis nemen van documentatie, het kennis nemen van de resultaten van de uitgevoerde interne controles en uitgevoerde pentesten, alsmede eigen waarnemingen.
- Het evalueren van de uitkomsten van onze werkzaamheden.

Vlijmen d.d. 10 oktober 2023

BKBO b.v.

Signed By: IJPELAAR MARTINUS BENEDICTUS HERMANN 2023-10-10T05:37:29+02:00 ID: fe583731-e02e-4b75-b0b6-17d7059544d6 Auth: itsmesign	
drs. M.B.H. IJpelaar RE CEH CISA, directeur	mr W.R. Nanninga RE CISA MMC, partner
V.C.W.M. Paijmans MA, auditondersteuner	

2 Verantwoordelijkheden gebruikersorganisatie

Bij de opzet en implementatie van interne beheersingsmaatregelen bij de serviceorganisatie neemt deze voor een aantal beveiligingsrichtlijnen van de 'Norm ICT-beveiligingsassessments DigiD' aan, dat enkele interne beheersingsmaatregelen door de houderorganisaties zullen worden geïmplementeerd om te 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.	Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van de serviceorganisatie en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie. 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 gebruikersorganisatie moet de afspraken met Forus Operations B.V. 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; • de behandeling van gevoelige gegevens; • wanneer en hoe de leverancier toegang tot de systemen/ data van de gebruikersorganisatie mag hebben;

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
		• Service Level Reporting; • het jaarlijks uitvoeren van audits bij Forus Operations B.V.; • beding dat deze voorwaarden back-to-back worden doorgegeven aan mogelijke sub-leveranciers. De serviceorganisatie Forus Operations B.V. 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 Forus Operations B.V. 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.). Onder gebruikersorganisatie kan de DigiD aansluithouder worden verstaan maar ook een (sub)serviceorganisatie die door de aansluithouder is ingeschakeld.
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 Forus Operations B.V. en is voor dat deel onderzocht. Voor het overige valt dit onder verantwoordelijkheid van de gebruikersorganisatie.

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
		De gebruikersorganisatie moet maatregelen ontwerpen en inrichten met betrekking tot: • de beschrijving van taken, verantwoordelijkheden en bevoegdheden van de verschillende beheerrollen; • 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. Onder gebruikersorganisatie kan de DigiD aansluithouder worden verstaan maar ook een (sub)serviceorganisatie die door de aansluithouder is ingeschakeld.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Deze beveiligingsrichtlijn valt deels onder verantwoordelijkheid van Forus Operations B.V. 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 Wet 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. • Het zodanig inrichten van de netwerkarchitectuur dat databases met gevoelige gegevens (zoals BRP, WOZ, AD, etc.) zich niet hetzelfde netwerksegment bevinden als de DigiD applicatie én daar waar gevoelige gegevens wél in het netwerksegment als de DigiD applicatie staan, deze worden versleuteld.
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	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

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersmaatregelen van de gebruikersorganisatie
		van DNS-antwoorden geverifieerd om misbruik te voorkomen. Het regelen van DNSSEC is de verantwoordelijkheid van de gebruikersorganisatie. De gebruikersorganisatie moet maatregelen ontwerpen en zodanig inrichten dat het object van onderzoek wordt beveiligd via DNSSEC.
C.08	Wijzigingsbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	De gebruikersorganisatie dient kennis te nemen van de releasedocumentatie van Forus Operations B.V. om de effecten op het eigen werkproces in kaart te brengen. De releasenotes zijn online raadpleegbaar via https://github.com/teamforus/forus/releases

Bijlage A – Rapport van bevindingen DigiD

Deze bijlage is niet bestemd voor de gebruikersorganisaties en wordt slechts verstrekt aan Forus Operations B.V.

Bijlage B – Object van onderzoek

Deze bijlage is vertrouwelijk en niet bestemd voor de gebruikersorganisatie en wordt slechts verstrekt aan Forus Operations B.V.

Bijlage C –Overzicht onderverdeling getoetste normen bij Forus Operations B.V.

Deze bijlage richt zich op het ten dienste van Logius inzichtelijk maken van de wijze waarop Forus Operations B.V. gebruik heeft gemaakt van subserviceorganisaties die betrekking hebben op het object van onderzoek.
Als input voor de hierna vermelde samenvatting is, naast de voorliggende rapportage, gebruik gemaakt van de volgende rapportage(s):

Omschrijving assurancerapportage	Subservice organisatie	Bij subservice-organisatie getoetste beveiligings-richtlijnen	Referentie	Afgifte-datum	Ondertekend door naam RE
SOC2 assurancerapportage voor de periode van 1 oktober 2022 tot 31 maart 2023	Amazon Web Services, Inc.	B.01, B.05, U/TV.01, U/PW.05, U/PW.07, U/NW.03, U/NW.04, U/NW.05, U/NW.06, C.03, C.04, C.06, C.07, C.08, C.09	SOC2 Type 2 Report "Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy"	31 maart 2023	Ernst + Young LLP
Bijbehorende Bridge Letter met betrekking tot de periode van 31 maart 2023 tot en met 1 september 2023	Amazon Web Services, Inc.	Idem		1 september 2023	Chad Woolf, VP AWS Security

Wij hebben geen onderzoek uitgevoerd naar de juistheid van de oordelen die zijn vermeld in de genoemde assurancerapportage(s). Wij kunnen dan ook geen enkele verantwoordelijkheid nemen met betrekking tot de in die rapportage vermelde oordelen.

Wij hebben kennis genomen van de genoemde assurancerapportage(s) en hebben te behoeve van Logius in onderstaande tabel per beveiligingsrichtlijn aangegeven tot welk oordeel de service auditor is gekomen.

Norm	Beschrijving van de norm	Getoetst bij Forus	Getoetst bij AWS
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	Voldoet	Voldoet
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.	Voldoet	Voldoet
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.	Voldoet	Voldoet
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Voldoet	Nee
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Voldoet	Nee
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	Voldoet	Nee
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Voldoet	Nee
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Voldoet	Nee
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	Voldoet	Nee
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.	Voldoet	Voldoet
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	Voldoet	Voldoet
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.	Voldoet	Voldoet
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	Voldoet	Voldoet
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Voldoet	Voldoet
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Voldoet	Voldoet
C.03	Vulnerability assesments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Voldoet	Voldoet
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Voldoet	Voldoet
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	Voldoet	Voldoet
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.	Voldoet	Voldoet
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Voldoet	Voldoet
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	Voldoet	Voldoet

Bijlage D - Overzicht ICT-beveiligingsassessment DigiD

Hieronder treft u een verkort overzicht aan van de identificerende kenmerken en de gebruikte assessmentrapportage(s) van subserviceorganisaties die invulling geeft/ geven aan het uitgevoerde DigiD-beveiligingsassessment bij Forus Operations B.V.

Auditor serviceorganisatie	Object van onderzoek	Sub-serviceorganisatie Amazon Web Services Inc.
Auditor Dhr. M.B.H. IJpelaar RE CEH CISA Kenmerk rapport BKBO/200916-1/V4/TPM Oordeelsdatum 4 oktober 2023 Rapportdatum 10 oktober 2023	De webapplicatie Forus & Me wordt door de inwoners/burgers van de klanten van Forus Operations B.V. gebruikt voor de aanvraag van sociale regelingen. Deze webapplicatie maakt gebruik van de PaaS-oplossing van Amazon Virtual Private Cloud Services.	Naam Amazon Web Services, Inc. Auditor Ernst + Young LLP Kenmerk rapport SOC2 Type 2 Report "Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy" Oordeelsdatum 31 maart 2023 Rapportdatum 12 mei 2023

Bijlage E – Rapportage penetratietest Defenced

Deze bijlage is niet bestemd voor de gebruikersorganisaties en wordt slechts verstrekt aan Forus Operations B.V.