

**Third Party Memorandum DigiD
2020
Stichting Forus**



DigiD assessment
Forus & Me versie 0.8.2
Kenmerk BKBO/200107-2/TPM

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 Forus & Me van Stichting Forus. In dit rapport worden de door ons vastgestelde bevindingen, conclusies en aanbevelingen beschreven.

Inhoudsopgave

| | | |
|-----|---|----|
| 1 | Assurancerapport van de onafhankelijke auditor | 4 |
| 1.1 | Opdracht | 4 |
| 1.2 | Verantwoordelijkheden van de opdrachtgever | 4 |
| 1.3 | Verantwoordelijkheden van de auditor | 5 |
| 1.4 | Beperkingen | 5 |
| 1.5 | Oordelen | 6 |
| 1.6 | Beoogde gebruikers en doel | 8 |
| 2 | Criteria | 9 |
| 3 | Object van onderzoek | 10 |
| 4 | Verantwoordelijkheden gebruikersorganisatie | 11 |
| | Bijlage A – Beschrijving van de testresultaten van de auditor | 14 |
| | Bijlage B – Object van onderzoek | 15 |
| | Bijlage C – Rapportage penetratietest Defenced | 16 |

1 Assurancerapport van de onafhankelijke auditor

1.1 Opdracht

Ingevolge de opdracht van Stichting Forus (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 de 'Handleiding uitvoering ICT-beveiligingsassessment' versie 2.2 van Logius uitgevoerd.

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 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).

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 18 maart 2020. 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 Stichting Forus.

| Nr | Beschrijving van de beveiligingsrichtlijn | Oordeel |
|---------|---|---------|
| 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 assessments (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. | ✓ |
| 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 Stichting Forus, 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. We geven de Stichting Forus toestemming om deze TPM te publiceren via GitHub als zijnde behorende bij de documentatie van de applicatie Forus & Me. De bijlagen A, B en C 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. 18 maart 2020

Bureau voor Kwaliteitsborging Bij de Overheid b.v.

| | |
|---|---|
|  |  |
| drs. M.B.H. Ijpelaar RE CEH CISA, directeur | mr W.R. Nanninga RE CISA MMC, partner |

2 Criteria

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 | DigiD aansluiting |
|--------------------------|------------------------------------|---|
| Gemeente Nijmegen | nijmegen.nl/inkomensondersteuning. | Gemeente Nijmegen - Inkomensondersteuning |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

De DigiD webapplicatie wordt door de klanten van Forus gebruikt voor de aanvraag van sociale regelingen.

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

- Forus & Me, release v0.8.2

De code van de versie van de webapplicatie waarover de TPM wordt afgegeven is online in te zien via: <https://github.com/teamforus/forus/releases/tag/v0.8.2>

Forus maakt gebruik van Git version control. De versie van de webapplicatie heeft de commithash [fae4301975559b8aded55eab9f031601b4cb3c4](https://github.com/teamforus/forus/commit/fae4301975559b8aded55eab9f031601b4cb3c4) en is in te zien via: <https://github.com/teamforus/forus/commit/fae4301975559b8aded55eab9f031601b4cb3c4>

Deze applicatie betreft geheel standaard software en wordt als SAAS onderhouden door Stichting Forus. De infrastructuur waarop de applicaties draaien wordt eveneens beheerd door Stichting Forus.

Het onderzoek heeft zich gericht op de webapplicatie(s), de URLs waarmee deze applicaties kunnen worden benaderd, de infrastructuur (binnen de DMZ waar de webapplicatie(s) zich bevinden) 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 beheersingmaatregelen van de gebruikersorganisatie |
|------|---|---|
| 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. | <p>De houder(s) van de DigiD-aansluiting van de webomgeving van de serviceorganisatie Stichting Forus moeten de afspraken met de serviceorganisatie vastleggen in een overeenkomst waarbij o.a. de volgende zaken zijn opgenomen:</p> <ul style="list-style-type: none"> • een beschrijving van de te 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; • 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. |

| Nr | Beschrijving van de beveiligingsrichtlijn | Gewenste interne beheersingmaatregelen van de gebruikersorganisatie |
|---------|---|---|
| | | De serviceorganisatie Stichting Forus moet een rapportage 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. | <p>De gebruikersorganisatie moet maatregelen ontwerpen en inrichten met betrekking tot toegangsbeveiliging en -beheer. Hierbij valt te denken aan:</p> <ul style="list-style-type: none"> • 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. <p>Alle accounts dienen individueel te zijn en er dient door de houder van de DigiD-aansluiting een autorisatiematrix te worden opgesteld en beheerd.</p> |
| U/WA.02 | Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten. | <p>De houder van de DigiD aansluiting moet maatregelen ontwerpen en inrichten met betrekking tot:</p> <ul style="list-style-type: none"> • 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. |
| U/NW.06 | Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar. | <p>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.</p> <p>Het regelen van DNSSEC is de verantwoordelijkheid van de gebruikersorganisatie.</p> <p>De gebruikersorganisatie moet maatregelen ontwerpen en zodanig inrichten dat het object van onderzoek wordt beveiligd via DNSSEC.</p> |

| Nr | Beschrijving van de beveiligingsrichtlijn | Gewenste interne beheersingmaatregelen van de gebruikersorganisatie |
|------|--|--|
| C.08 | Wijzigingsbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. | Voor wat betreft de applicatie dient men kennis te nemen de functionaliteit van nieuwe releases. Releasenotes worden publiekelijk bijgehouden via Github. Zie hiervoor https://github.com/teamforus/forus/releases |

Voor beveiligingsrichtlijn U/WA.05 "De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende en cryptografische technieken." is vastgesteld dat de serviceorganisatie alle persoonsgegevens adequaat versleutelt. De gebruikersorganisatie hoeft derhalve geen aanvullende beheersingsmaatregelen te nemen om dit specifieke risico af te dekken.

Bijlage A – Beschrijving van de testresultaten van de auditor

Deze bijlage is niet bestemd voor de gebruikersorganisatie en wordt slechts verstrekt aan Stichting Forus.

Bijlage B – Object van onderzoek

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

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 Stichting Forus.