DigiD-assessment ten behoeve van de gebruikers van xxllnc Zaken

Aan:	Management xxllnc Zaken en Logius
Kenmerk:	ITAA/DIGID/XXLL29012025
Datum:	29 januari 2025
Van:	Achmed Bouazza RE CISA
Aansluiting:	Zie bijlage E voor de aansluitingen

forvis mazars

Inhoudsopgave

Assurancerapport van de onafhankelijke IT-auditor

Aan:	Management van xxllnc Zaken en Logius
Kenmerk:	ITAA/DIGID/XXLL29012025
Datum:	29 januari 2025
Van:	Achmed Bouazza RE CISA
Aansluiting:	Zie bijlage E voor de aansluitingen

Aan: Management xxllnc Zaken

1.1. Inleiding

Initieel zijn per 25 augustus 2024 alle DigiD-normen in scope bij xxllnc Zaken beoordeeld in opzet, bestaan en (waar van toepassing) werking. Hierbij zijn afwijkingen geconstateerd op de normen U/TV.01 en C.07 inzake de werking. Deze twee normen zijn onderworpen aan een hertest voor de werking. In dit rapport wordt alleen gerapporteerd over deze twee normen.

1.2. Onze oordelen

Wij hebben een DigiD-beveiligingsassessment met redelijke mate van zekerheid uitgevoerd ten behoeve van de gebruikers van xxllnc Zaken. Zie bijlage E voor de aansluitingen.

Per beveiligingsrichtlijn hebben wij hieronder vermeld of wordt voldaan aan de beveiligingsrichtlijn. Om de leesbaarheid van dit rapport te vergroten zijn de oordelen in deze tabel weergegeven als “voldoet” of “voldoet niet”.

Bij beveiligingsrichtlijnen waarbij ook de effectieve werking wordt vastgesteld moet “voldoet” worden geïnterpreteerd als “Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn effectief werkten tijdens de controleperiode van 15 juli 2024 tot 16 januari 2025”. “Voldoet niet” moet vervolgens worden geïnterpreteerd als “Wij zijn van oordeel dat de getoetste interne beheersingsmaatregelen die verband houden met de op die regel aangegeven beveiligingsrichtlijn niet in alle materiële opzichten effectief werkten tijdens de controleperiode van 15 juli 2024 tot 16 januari 2025”.

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 aangelegenheden die in dit assurance-rapport zijn uiteengezet. Ons onderzoek was beperkt tot de beveiligingsrichtlijnen die de verantwoordelijkheid zijn van de serviceorganisatie.

Nr	Beschrijving van de beveiligingsrichtlijn	Oordeel opzet en bestaan	Oordeel werking
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.	NVT	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.	NVT	Voldoet [1]

1.3. De basis voor onze oordelen

[1] Werking – Non-occurrence. Voor beveiligingsrichtlijn C.07 hebben wij vastgesteld dat xxllnc Zaken IDS/IPS heeft ontworpen en ingericht. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij de werking niet kunnen vaststellen. Wij hebben wel kunnen vaststellen dat de IDS/IPS actief was gedurende de gehele controleperiode. Hierdoor zijn wij van oordeel dat de organisatie voldoet aan deze norm.

Wij hebben ons onderzoek uitgevoerd volgens Nederlands recht, waaronder de NOREA Richtlijn 3000D ’Assurance-opdrachten door IT-auditors (Directe-opdrachten)’ en de nadere regels zoals opgenomen in de Handreiking DigiD 2024 (versie 1.0) van NOREA. 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 xxllnc Zaken 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.

1.4. Van toepassing zijnde criteria

Voor deze opdracht hanteren wij het Normenkader 3.0 voor ICT-beveiligingsassessments DigiD dat door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is vastgesteld. Het Ministerie BZK heeft uit de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties versie 2015 de 21 beveiligingsrichtlijnen geselecteerd waarvan zij vindt dat deze de hoogste impact op de veiligheid van DigiD hebben en heeft deze vermeld in het Normenkader 3.0 voor ICT-beveiligingsassessments DigiD'. Het Normenkader 3.0 voor ICT-beveiligingsassessments DigiD bestaat uit 21 richtlijnen die zijn gebaseerd op de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties versie 2015. De versie 3.0 geldt vanaf 1 augustus 2022. De geselecteerde 21 beveiligingsrichtlijnen worden tevens aangeduid als de 21 DigiD-normen.

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

- 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;
- de interne beheersingsmaatregelen die verband houden met de beveiligingsrichtlijnen op afdoende wijze zijn opgezet en daadwerkelijk zijn geïmplementeerd;
- de interne beheersingsmaatregelen die verband houden met een selectie van specifieke beveiligingsrichtlijnen gedurende de controleperiode consistent zijn toegepast zoals opgezet.

1.5. Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek

1.4.1. Object van onderzoek

Het object van onderzoek was de webomgeving van xxllnc Zaken.

xxllnc Zaken biedt de volgende functionaliteit aan waarvoor een DigiD aansluiting ter authenticatie wordt gebruikt: Via xxllnc Zaken worden door de DigiD aansluithouders zaken (verzoeken en/of aanvragen van burgers of interne registraties) digitaal geregistreerd, gemonitord en afgehandeld door middel van een workflow.

Deze functionaliteit wordt geboden door de volgende webapplicatie:

- xxllnc Zaken, versienummer 2024.6.2

Deze applicatie betreft geheel maatwerk en wordt onderhouden door xxllnc Zaken. De infrastructuur waarop de applicatie draait (virtuele machines en cloud omgeving) wordt beheerd door xxllnc Zaken. xxllnc Zaken maakt gebruik van de Infrastructure as a Service diensten van Amazon Web Services (AWS).

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. Subserviceorganisaties

xxllnc Zaken maakt gebruik van subserviceorganisatie Amazon Web Services (AWS) voor Infrastructure as a Service diensten. xxllnc Zaken 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-beveiligingsassessments DigiD

Het Normenkader 3.0 voor ICT-beveiligingsassessments DigiD ‘Norm ICT-beveiligingsassessments DigiD 3.0’ bevat 21 beveiligingsrichtlijnen is een selectie van beveiligingsrichtlijnen uit de ‘ICT-beveiligingsrichtlijnen voor webapplicaties versie 2015’ van het Nationaal Cyber Security Centrum (NCSC). Daarom zijn we niet in staat om één overkoepelend oordeel af te geven met betrekking tot 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 xxllnc Zaken 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.

Voor wat betreft de werking hebben wij alleen werkzaamheden uitgevoerd naar de interne beheersingsmaatregelen zoals aangegeven in 'Normenkader 3.0 voor ICT-beveiligingsassessments DigiD' voor zover van toepassing binnen de scope van ons onderzoek.

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

Ons oordeel is niet aangepast als gevolg van deze aangelegenheden.

1.6. Beoogde gebruikers en doel

Ons assurance-rapport 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 xxllnc Zaken.

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, ongeacht of gebruik is gemaakt van rapporten inzake subserviceorganisatie(s).

Ons assurance-rapport en bijlagen mogen enkel worden gebruikt door de beoogde gebruikers en/of verspreidingskring voor het doel waarvoor deze zijn opgesteld en dient niet te worden verspreid aan of te worden gebruikt door anderen.

1.7. Verantwoordelijkheden van xxllnc Zaken

Het bestuur van de xxllnc Zaken 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 ‘Normenkader 3.0 voor ICT-beveiligingsassessments DigiD'.

1.8. Verantwoordelijkheden 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.

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, bestaan en voor de van toepassing zijnde beveiligingsrichtlijnen uit 'Normenkader 3.0 voor ICT-beveiligingsassessment DigiD' de werking 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 de 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, het vaststellen van het bestaan en voor de van toepassing zijnde beveiligingsrichtlijnen uit 'Normenkader 3.0 voor ICT-beveiligingsassessment DigiD' de werking 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.

Rotterdam, 29 januari 2025

Forvis Mazars N.V.
IT Audit & Advisory

Digitaal ondertekend door:

Achmed Bouazza
29 januari 2025 19:45 +01:00

Achmed Bouazza RE CISA

Partner

2. Verantwoordelijkheden gebruikersorganisatie

Bij de opzet en implementatie van interne beheersingsmaatregelen bij de serviceorganisatie neemt deze voor een aantal beveiligingsrichtlijnen van het ‘Normenkader 3.0 voor ICT-beveiligingsassessments DigiD’ aan, dat enkele interne beheersingsmaatregelen door de gebruikersorganisaties zullen worden geïmplementeerd om te voldoen aan deze beveiligingsrichtlijnen.

In de onderstaande tabel wordt aangegeven voor welke beveiligingsrichtlijn(en) deze afweging is gemaakt en welke gewenste interne beheersingsactiviteit bij de gebruikersorganisaties kunnen worden geïmplementeerd om te voldoen aan de desbetreffende beveiligingsrichtlijn van het 'Normenkader 3.0 voor ICT-beveiligingsassessments DigiD'.

De geschiktheid van de opzet, het bestaan en/of de werking van deze aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie hebben wij niet geëvalueerd. Aan de beveiligingsrichtlijnen van het ‘Normenkader 3.0 voor 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 beheersingsmaatregelen van de gebruikersorganisatie
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteed hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	De gebruikersorganisatie dient het eigenaarschap inzake de DigiD webapplicatie ingericht te hebben en te zorgen voor een actueel en vastgesteld informatiebeveiligingsbeleid dat actief wordt uitgedragen en waarin specifieke aandacht is besteed aan: • beveiligingsmaatregelen ten aanzien van webapplicaties en/of infrastructuren en DigiD in het bijzonder; • dataclassificatie; • toegangsvoorzieningen; • kwetsbaarhedenbeheer. Daarnaast dient de gebruikersorganisatie ervoor zorg te dragen dat periodiek gerapporteerd wordt over informatiebeveiliging aan het verantwoordelijk hoger management.

Nr	Beschrijving van de beveiligingsrichtlijn	Gewenste interne beheersingsmaatregelen 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.	De gebruikersorganisatie dient afspraken met xxllnc Zaken in een overeenkomst vast te leggen.
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.	De gebruikersorganisatie dient te waarborgen dat maatregelen voor toegangsbeveiliging tot de webapplicatie zijn ingericht. Hierbij valt te denken aan het toekennen, wijzigen en intrekken van toegang en het vaststellen van een toegangsbeleid en wachtwoordbeleid.
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	De gebruikersorganisatie dient te waarborgen dat beheerrollen zijn beschreven, dat het proces voor het melden, afhandelen en rapporteren van beveiligingsincidenten is beschreven en geïmplementeerd, dat meldingen van CERTS worden geanalyseerd en opgevolgd en dat er periodiek gerapporteerd wordt over beveiligingsincidenten aan het management.
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	De gebruikersorganisatie dient de classificatie van gegevens op basis van een risico analyse uit te voeren.
U/NW.06	Voor het configureren van netwerken is een hardeningsrichtlijn beschikbaar.	De gebruikersorganisatie dient te waarborgen dat DNSSEC is geïmplementeerd voor het subdomein dat verwijst naar de DigiD-applicatie.
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	De gebruikersorganisatie dient te waarborgen dat aangevraagde wijzigingen geregistreerd en gemonitord worden. Hierbij valt te denken aan een registratie van wijzigingsverzoeken, het uitvoeren van gebruikersacceptatietesten en het formeel accorderen van wijzigingen voor in productiename.

Bijlage C – Totaaloverzicht getoetste normen ICT-beveiligingsassessment DigiD-aansluiting van xxllnc Zaken

Deze bijlage richt zich op het ten dienste van Logius inzichtelijk maken van de wijze waarop xxllnc Zaken gebruik heeft gemaakt van service organisaties 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 rapportages:

Omschrijving assurance-rapportage	Subserviceorganisatie	Bij subserviceorganisatie getoetste beveiligingsrichtlijnen	Referentie / Rapportnummer/ controleperiode	Oordeelsdatum	Ondertekend door naam auditor/ auditeenheid
SOC2 Type II assurancerapportage	Amazon Web Services (AWS)	B.01, U/TV.01, U/WA.05, U/PW.07, U/NW.03, U/NW.06, C.03, C.08 en C.09.	System and Organization Controls 2 (SOC 2) Type 2 Report Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy For the Period October 1, 2023 to September 30, 2024	13 december 2024	Ernst & Young LLP

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.

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

Nr	Beschrijving van de norm	Getoetst bij AWS Referentie: System and Organization Controls 2 (SOC 2) Type 2 Report Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy. For the Period October 1, 2023 to September 30, 2024
B.01	De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	**Opzet en bestaan** Voldoet [AWSCA-1.1, AWSCA-1.2, AWSCA-1.3]
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.	N/A
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.	**Opzet en bestaan** Voldoet [AWSCA-2.1, AWSCA-2.2, AWSCA-2.3, AWSCA-2.4, AWSCA-2.5, AWSCA-2.6] **Werking** Voldoet [AWSCA-2.1, AWSCA-2.2, AWSCA-2.3, AWSCA-2.4, AWSCA-2.5, AWSCA-2.6]
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	N/A
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	N/A
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.	N/A
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	**Opzet en bestaan** Voldoet

Nr	Beschrijving van de norm	Getoetst bij AWS Referentie: System and Organization Controls 2 (SOC 2) Type 2 Report Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy. For the Period October 1, 2023 to September 30, 2024
		[AWSCA-1.6, AWSCA-4.5, AWSCA-4.6, AWSCA-4.7]
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	N/A
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	N/A
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.	N/A
U/PW.07	Voor het configureren van platformen een hardeningsrichtlijn beschikbaar.	**Opzet en bestaan** Voldoet [AWSCA-3.9, AWSCA-3.10, AWSCA-9.4]
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.	**Opzet en bestaan** Voldoet [AWSCA-3.1, AWSCA-3.11, AWSCA-3.13, AWSCA-3.14]
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van detectie- en protectiemechanismen.	N/A
U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	N/A
U/NW.06	Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	**Opzet en bestaan** Voldoet [AWSCA-3.2, AWSCA-3.3, AWSCA-3.7]
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	**Opzet en bestaan** Voldoet [AWSCA-3.4]

Nr	Beschrijving van de norm	Getoetst bij AWS Referentie: System and Organization Controls 2 (SOC 2) Type 2 Report Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy. For the Period October 1, 2023 to September 30, 2024
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	N/A
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.	N/A
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.	N/A
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	**Opzet en bestaan** Voldoet [AWSCA-6.1, AWSCA-6.2, AWSCA-6.3, AWSCA-6.4, AWSCA-6.5, AWSCA-6.6] **Werking** Voldoet [AWSCA-6.1, AWSCA-6.2, AWSCA-6.3, AWSCA-6.4, AWSCA-6.5, AWSCA-6.6]
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.	**Opzet en bestaan** Voldoet [AWSCA-3.4, AWSCA-3.6] **Werking** Voldoet [AWSCA-3.4, AWSCA-3.6]

Bijlage D – Totaaloverzicht ICT-beveiligingsassessment DigiD xxllnc Zaken

Hieronder treft u een verkort overzicht aan van de identificerende kenmerken en de gebruikte assessmentrapportage van subserviceorganisaties die invulling geeft aan het uitgevoerde DigiD-beveiligingsassessment bij xxllnc Zaken.

Aansluiting	**Aansluitnummer:**	Zie bijlage E voor de aansluitingen
	Aansluitnaam:	Zie bijlage E voor de aansluitingen
	Aansluithouder:	Zie bijlage E voor de aansluitingen
Auditor Serviceorganisatie	**Naam auditor:**	Achmed Bouazza RE CISA
	Auditorganisatie:	Forvis Mazars N.V.
	Kenmerk rapport:	ITAA/DIGID/XXLL29012025
Object van onderzoek	**Naam webapplicatie:**	xxllnc Zaken
	Versienummer:	2024.6.2
	Omschrijving:	Via xxllnc Zaken worden door de DigiD aansluithouders zaken (verzoeken en/of aanvragen van burgers of interne registraties) digitaal geregistreerd, gemonitord en afgehandeld door middel van een workflow
Subserviceorganisatie	**Subserviceorganisatie:**	Amazon Web Services (AWS)
	Auditor Subserviceorganisatie:	Ernst & Young LLP
	Kenmerk rapport:	System and Organization Controls 2 (SOC 2) Type 2 Report Description of the Amazon Web Services System Relevant to Security, Availability, Confidentiality, and Privacy For the Period October 1, 2023 to September 30, 2024
	Oordeelsdatum:	1 oktober 2023 t/m 30 september 2024
	Rapportdatum:	13 december 2024

Bijlage E – Lijst kenmerk rapport en aansluitnummers

Nr	Kenmerk rapport	TPM aansluitingsnummer
1	ITAA/DIGID/ETTE11102024	1001441
2	ITAA/DIGID/GOUD11102024	1002797
3	ITAA/DIGID/ZUTP11102024	1004287
4	ITAA/DIGID/WIJK11102024	1000373
5	ITAA/DIGID/BILT11102024	999997
6	ITAA/DIGID/HEUS11102024	1003197
7	ITAA/DIGID/ZEIS11102024	1004149
8	ITAA/DIGID/BERK11102024	1003187
9	ITAA/DIGID/OSS11102024	1005217
10	ITAA/DIGID/ALKM11102024	1002723
11	ITAA/DIGID/SOES11102024	1003697
12	ITAA/DIGID/TERN11102024	849682
13	ITAA/DIGID/BAAR11102024	1000001
14	ITAA/DIGID/THOL11102024	999989
15	ITAA/DIGID/OUDE11102024	1000273
16	ITAA/DIGID/SCHO11102024	1001141
17	ITAA/DIGID/HORI16102024	1005881
18	ITAA/DIGID/MIDD16102024	1003883
19	ITAA/DIGID/MUNI16102024	1004343
20	ITAA/DIGID/BEUN16102024	1002831
21	ITAA/DIGID/VENL16102024	1005077
22	ITAA/DIGID/GOOI16102024	1003975
23	ITAA/DIGID/GEPE17102024	1000181
24	ITAA/DIGID/MOER17102024	1001769
25	ITAA/DIGID/DIJK21102024	1004301
26	ITAA/DIGID/BARN25102024	1004661
27	ITAA/DIGID/VLAA22102024	1004113

Nr	Kenmerk rapport	TPM aansluitingsnummer
28	ITAA/DIGID/VOER22102024	1000177
29	ITAA/DIGID/HOFT22102024	1003107
30	ITAA/DIGID/WAAL22102024	1002324
31	ITAA/DIGID/LING22102024	1000462
32	ITAA/DIGID/ZUID22102024	1004215
33	ITAA/DIGID/ROOS22102024	1000173
34	ITAA/DIGID/MAAS25102024	1002963
35	ITAA/DIGID/VIJF25102024	1002553
36	ITAA/DIGID/OMME25102024	1002747
37	ITAA/DIGID/HARD25102024	1002749
38	ITAA/DIGID/VOOR30102024	1005111
39	ITAA/DIGID/MONT30102024	1004367
40	ITAA/DIGID/HALD30102024	1001805
41	ITAA/DIGID/LANS05112024	1001857
42	ITAA/DIGID/PURM05112024	1003575
43	ITAA/DIGID/NOOR06112024	1002967
44	ITAA/DIGID/WATE15112024	1005997
45	ITAA/DIGID/ZALT15112024	1003173
46	ITAA/DIGID/MAAS15112024	1004377
47	ITAA/DIGID/NOAB15112024	1002283
48	ITAA/DIGID/HILV21112024	1003789
49	ITAA/DIGID/HART14012025	1002961
50	ITAA/DIGID/MEPP14012025	1006015
51	ITAA/DIGID/AMER14012025	1005967

Contacts

Achmed Bouazza RE CISA

Partner

T: 088 277 13 88
M: 06 4399 4867

achmed.bouazza@forvismazars.com

Watermanweg 80
Postbus 23123
3001 KC Rotterdam

Forvis Mazars is een toonaangevend wereldwijd netwerk in de financiële dienstverlening dat onder één merknaam opereert met twee leden: Forvis Mazars, LLP in de Verenigde Staten en Forvis Mazars Group SC, een internationale geïntegreerde partnership. Beide leden zijn sterk betrokken bij hun klanten, leveren een 'unmatched client experience' en bieden wereldwijd diensten aan op het gebied van audit, accountancy, tax, financial advisory, consulting en sustainability.