RAPPORT B

Organisatie-overstijgende analyse Pre-Check DigiD Caribisch Nederland

RAPPORT B

Organisatie-overstijgende analyse Pre-Check DigiD

Caribisch Nederland

Cleo van Engelen, René Volwerk, Joep Janssen

DATUM	**31-3-2025**
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20231158

INHOUDSOPGAVE

1 INLEIDING

1.1 Achtergrond

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna min BZK) heeft de opdracht uitgezet voor een 'pre-check DigiD'. Ter voorbereiding op de feitelijke aansluiting op DigiD wil min BZK inzicht krijgen op welke aspecten de betrokken overheidsorganisaties (nog) niet voldoen aan de voorwaarden en advies krijgen omtrent te nemen maatregelen. Het doel van de opdracht is om hieraan invulling te geven zodat de benodigde correctieve maatregelen inzichtelijk worden en kunnen worden uitgevoerd. Zo wordt bereikt dat de invoering van DigiD zo spoedig mogelijk na het van kracht worden van de toepasselijke wetgeving kan worden ingeregeld.

1.2 Vraagstelling

Per organisatieonderdeel levert Highberg een Rapport A op, waarin op basis van het bestaande DigiD normenkader[1] een analyse wordt gegeven van:

- de punten waar wel en de punten waar niet aan voldaan wordt;
- de belangrijkste risico's voor beveiliging, privacybescherming en beheer
- Een advies over de te nemen maatregelen, in volgorde van mitigeren van de belangrijkste risico's;
- de bijbehorende inspanning van de overheidsorganisatie en overige overheidsdienstverleners en;
- een kostenindicatie voor de inzet van eigen personeel en inhuur/uitbesteding van IT diensten en ook de kosten voor het DigiD assessment en eventuele penetratietest op de applicatie en de infrastructuur.

Als onderdeel van die opdracht levert Highberg tevens een 'Rapport B' op. Dit betreft: "*Een algemene organisatie-overstijgende analyse die beschrijft wat er moet gebeuren om DigiD in Caribisch Nederland uit te rollen inclusief aanbevelingen om dit succesvol te maken en een overzicht van de belangrijkste risico's en suggesties omtrent risico mitigerende maatregelen*". De hoofdvragen die in Rapport B behandeld worden zijn:

- Welke organisatie-overstijgende risico's zijn er in Caribisch Nederland die een aansluiting op een succesvolle aansluiting op DigiD uit te rollen
- Welke organisatie-overstijgende maatregelen moeten er worden genomen (en door wie) om die aansluiting succesvol uit te rollen;
- Welke aanbevelingen vloeien voort uit deze analyse.

1.3 Doel van dit document en doelgroep

Dit document is Rapport B waarmee antwoord wordt gegeven op bovenstaande vragen. Dit rapport geldt als aanvulling op de opgeleverde rapporten A. Rapport B wordt gedeeld met het projectteam van min BZK, dat vervolgens het rapport zal delen met stakeholders.

[1] https://www.logius.nl/domeinen/toegang/digid/ict-beveiligingsassessments-digid/documentatie/norm-ict-beveiligingsassessments-digid

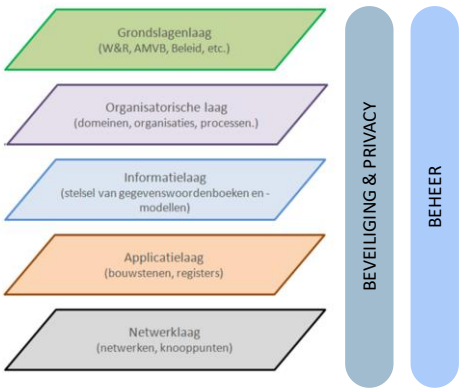
Rapport B is een groeidocument. De voorliggende versie is de actuele versie, gebaseerd op de oplevering van meerdere Rapporten A. Indien Rapporten A van nog meer overheidsorganisaties worden opgeleverd kunnen de daarin opgedane ervaringen aanleiding zijn een update te maken van Rapport B.

1.4 Methode

Voor dit rapport maken wij gebruik van het vijflaagsmodel van de NORA[2] dat wij meerdere malen binnen de overheid gebruikt hebben en ook door het ministerie van BZK is omarmt[3]. Het vijflaagsmodel, aangevuld met twee extra vlakken voor Beveiliging & Privacy en Beheer, biedt een gestructureerd overzicht van wat nodig is zodat inwoner van Caribisch Nederland (hierna CN) met DigiD veilig kunnen inloggen bij de overheidsorganisaties in Caribisch Nederland. Het gaat om de volgende invalshoeken:

1. Beleid en wet- en regelgeving laag
2. Organisatie en processen laag
3. Informatielaag
4. Applicatielaag
5. Netwerklaag
6. Beveiliging & Privacy
7. Beheer

NORA vijflaagsmodel



1.5 Leeswijzer

Hoofdstuk 1 geeft de inleiding op dit rapport. Hoofdstuk 2 een toelichting op de fasering van de aansluiting op DigiD voor de verschillende organisaties in CN. Hoofdstuk 3 is een uitwerking van de analyse op de verschillende lagen van het NORA model. Aparte paragrafen worden besteed aan beveiliging en beheer. Hoofdstuk 4 omvat onze aanbevelingen.

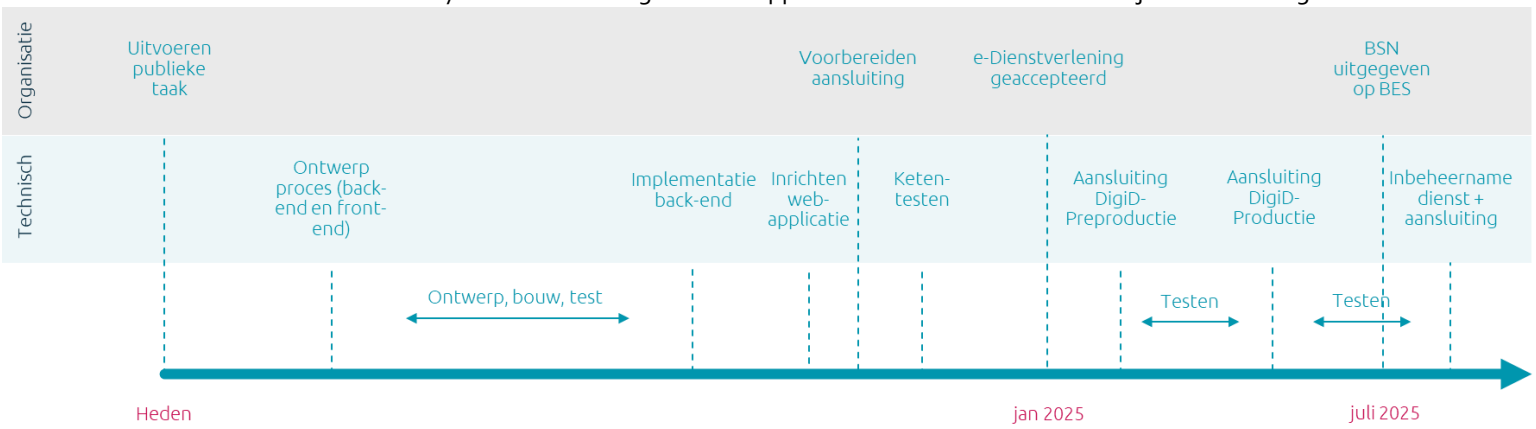
[2] https://www.noraonline.nl/wiki/Vijflaagsmodel

[3] https://www.rijksoverheid.nl/documenten/rapporten/2019/08/30/inventarisatie-standaardisatie

2 FASERING

2.1 Fasering van aansluiten op DigiD

Om de analyse en aanbevelingen in dit rapport te kunnen duiden achten wij het van belang om



aan te geven waar de verschillende onderzochte organisaties staan met betrekking tot hun aansluiting op DigiD. Onderstaand hebben wij daarom een tijdslijn gevisualiseerd. Belangrijk voor deze tijdslijn is dat wij er van uit gaan dat de organisaties die wij onderzocht hebben niet alleen de front-end van het proces willen digitaliseren, maar ook de back-end. Wij concluderen dat de mate van digitaliseren van de back-end (dus het eigen werkproces van de organisaties nog zeer beperkt is gedigitaliseerd of 'vernieuwd' moet worden).[4]

Om een aansluiting te krijgen en te houden moet elke organisatie:

- Akkoord gaan met de aansluitvoorwaarden;
- De systemen voldoen aan de beveiligingsnorm;
- Elk jaar een ICT-beveiligingsassessment (lees: DigiD-audit) afnemen.

Bovenstaande tijdslijn is erop gebaseerd dat vanaf de stap "aansluiting DigiD op pre-productie" tot en met de inbeheername van de dienst en aansluiting door Logius ongeveer één maand in beslag neemt. Na inbeheername van de aansluiting moet binnen twee maanden een DigiD-audit zijn uitgevoerd.

NB: in bovenstaande visualisatie wordt gesproken over 'ketentesten'. Hiermee worden de aansluittest van Logius bedoeld. Dus de koppeling van de webapplicatie aan het DigiD platform.

2.2 Uitgangspunten

Uit ons onderzoek is gebleken dat er eigenlijk geen e-dienstverleningsprocessen "klaar zijn" voor aansluiting op DigiD. Daarmee bedoelen wij dat er dus veel meer moet gebeuren dan enkel de webdienst gereed krijgen. Bijna elke organisatie zit nog in een verkenningsfase van processen die

[4] De planning van activiteiten is gebaseerd op de eerst mogelijke datum om gebruik te maken van DigiD, juli 2025. Gezien de voortgang van de verschillende organisaties en de nog uit te voeren activiteiten is een aansluiting in 2026 meer waarschijnlijk.

(her)ontworpen moeten worden om burgers online te bereiken. Enerzijds geeft dat de mogelijkheid om in een zeer vroeg stadium al rekening te houden met de voorwaarden en consequenties van een toekomstige aansluiting op DigiD, anderzijds betekent dat dat er nog zeer veel moet gebeuren voordat het aansluiten op DigiD waarde toe kan voegen.

Daarnaast is het van belang om de keuze voor DigiD te onderscheiden van de keuze voor het (verder) digitaliseren van de processen die leiden tot het uitvoeren van de publieke zaak. Het aansluiten op DigiD geeft de mogelijkheid om op een veilige en betrouwbare manier geïdentificeerd en geauthentiseerd te worden. Dit kan gezien worden als een ontwerpkeuze binnen een groter geheel. Elke organisatie moet voor zich bepalen welke diensten en in welke mate die gebruik van automatisering maken om informatie en diensten aan burgers, bedrijven en overheden ter beschikking te stellen. Dit rapport en onderzoek focust zich dus primair op aansluiting op DigiD, waarna deze informatie meegenomen kan worden in de bredere discussie rondom digitalisering van de dienstverlening.

3 ANALYSE

3.1 Inleiding

De organisatie-overstijgende analyse is uitgevoerd aan de hand van het vijflagenmodel van NORA. Bij elke laag van het model is ruimte om uiteen te zetten welke generieke en specifieke punten van toepassing zijn op dit (maatschappelijke) vraagstuk.

3.2 Wet- en regelgeving laag

Deze laag bevat de wet- en regelgeving die van toepassing is op dit vraagstuk. Omdat ook IT diensten voor de BES eilanden vanuit Curaçao geleverd worden zijn ook de Landsverordeningen van Aruba, Curaçao en Sint Maarten meegenomen. Dit betreft de volgende wetgeving:

1. AVG/UAVG;
2. Cyberbeveiligingswet;
3. Wet algemene bepalingen Burgerservicenummer (WABB);
4. Wet basisadministraties persoonsgegevens BES (Wet BAP BES);
5. Wet basisregistratie personen (Wet BRP);
6. Wet digitale overheid (WDO);
7. Wet bescherming persoonsgegevens BES;
8. Landsverordening Persoonsregistratie voor Aruba;
9. Landsverordening Bescherming Persoonsgegevens voor Curaçao en Sint Maarten.

Ook van belang zijn 2 wetten in ontwikkelingen:

10. Wetsvoorstel "Wet invoering BSN en voorzieningen digitale overheid BES"
11. Consensusrijkswet harmonisatie gegevensbescherming

De volgende regelgeving kan van belang zijn, afhankelijk van de gekozen architectuur:

1. Rijks breed cloudbeleid 2022
2. Implementatiekader risicoafweging cloudgebruik

3.2.1 Introductie

Het wetsvoorstel "Wet invoering BSN en voorzieningen digitale overheid BES" beoogt te bewerkstelligen voor Caribisch Nederland dat:

1. Geregistreerde inwoners een BSN krijgen,
2. Inwoners toegang krijgen tot digitale inlogmiddelen zoals DigiD en
3. Overheidsinstanties het BSN mogen gebruiken (verwerken) in hun dienstverlening.

Daartoe worden gewijzigd:

1. Wet algemene bepalingen Burgerservicenummer (Wabb),
2. Wet basisadministraties persoonsgegevens BES (Wet BAP BES),
3. Wet basisregistratie personen (Wet BRP) en
4. Wet digitale overheid (WDO).

3.2.2 De juridische status van privacy

De Consensusrijkswet harmonisatie gegevensbescherming heeft als doel de harmonisatie van de gegevensbescherming tussen Europees Nederland, de landen Aruba, Curaçao, Sint Maarten en de openbare lichamen Bonaire, Sint Eustatius en Saba. Deze wet is nog niet ingevoerd dus gelden tot aan die tijd de volgende gegevensbescherming wet- en regelgeving:

1. De AVG voor Europees Nederland;
2. Wet bescherming persoonsgegevens BES;
3. Wet basisadministraties persoonsgegevens BES (Wet BAP BES);
4. Landsverordening Persoonsregistratie voor Aruba;
5. Landsverordening Bescherming Persoonsgegevens voor Curaçao en Sint Maarten.

In de memorie van toelichting van het wetsvoorstel "Wet invoering BSN en voorzieningen digitale overheid BES" wordt verder een aantal uitgangspunten geformuleerd ten aanzien van privacy:

1. De AVG is niet van toepassing op de BES, omdat deze buiten de EU en buiten de Europese Economische Ruimte (EER) liggen. Bij uitwisseling van persoonsgegevens naar de BES geldt wel vanuit de AVG de noodzaak tot een gelijkwaardig beschermingsniveau ;
2. Dit wetsvoorstel bevat geen regeling voor de verwerking van bijzondere persoonsgegevens (artikel 9 AVG) Er wordt echter wel vermeld dat er al wel bijzondere persoonsgegevens uitgewisseld worden in het kader van andere overheidsdiensten.

Deze wetgevingsstatus leidt tot een gecompliceerde privacy-situatie betreffende drie landen en drie openbare lichamen buiten de EU en buiten de Europese Economische Ruimte (EER). Deze 6 vallen niet onder de AVG. Dit resulteert in drie specifieke situaties met betrekking tot de uitwisseling van persoonsgegevens, namelijk:

1. Uitwisseling van persoonsgegevens tussen Europees Nederland en de BES-eilanden;
2. Uitwisseling van persoonsgegevens tussen Europees Nederland en de CAS-landen;
3. Uitwisseling van persoonsgegevens tussen de BES-eilanden en de CAS-landen.

Ad 1. zal plaatsvinden als het wetsvoorstel "Wet invoering BSN en voorzieningen digitale overheid BES" wordt gerealiseerd. (Voor zover dat nu al niet plaatsvindt.) Dit betreft:

1. Antwoorden op de presentievraag aan bestuurscolleges (artikel 8, lid 4, WABB)
2. Inlichtingen aan BSN-gebruikers (artikelen 14 en 15, WABB)

3. Inlichtingen aan bestuurscolleges voor de basisadministratie (artikel 30b, Wet BAP BES)
4. Inlichtingen naar aanleiding van vergelijkend onderzoek tussen BRP-V en PIVA-V (artikel 4.3a, lid 2, Wet BRP)

Daarnaast worden persoonsgegevens vanuit Europees Nederland verstrekt aan organisaties in Caribisch Nederland die DigiD en BV-BSN gebruiken (artikelen 5 en 8, WDO en artikelen 14 en 15, WABB).

Ad 2. Is van belang indien de IT-infrastructuur en de leverancier daarvan, die voor de BES wordt gebruikt, op Curaçao is gevestigd. Dat houdt dus in de alle gegevensuitwisselingen via Curaçao verlopen*.

> * De doorgifte van persoonsgegevens van Nederland naar Bonaire via Curaçao valt onder de AVG. Bonaire valt onder de AVG, maar Curaçao niet, waardoor doorgifte naar Curaçao als internationaal wordt beschouwd. Voor doorgifte naar Curaçao zijn technische en organisatorische maatregelen vereist, zoals encryptie en netwerkbeveiliging. Curaçao heeft eigen privacywetgeving, maar geen adequaatheidsbesluit van de EU, dus aanvullende maatregelen zijn nodig. Mogelijke rechtsgronden voor doorgifte zijn standaardcontractbepalingen, binding corporate rules, toestemming van betrokkenen, of noodzaak voor contractuitvoering. Extra beveiligingsmaatregelen omvatten data-encryptie en evaluatie van overheidsrisico's. Aanbevolen wordt een Data Protection Impact Assessment uit te voeren, SCC's te gebruiken, encryptie te implementeren, en de wetgeving in Curaçao te monitoren.

Ad 3. is van belang vanwege punt 2. Daardoor lopen alle gegevensuitwisselingen via Curaçao naar de BES.

3.2.3 De juridische status van informatiebeveiliging

De NIS2- en CER-richtlijn zijn sinds 17 oktober 2024 geldig in de Europese Unie. In Nederland is het niet gelukt om deze EU-richtlijnen op tijd om te zetten in nationale wetgeving. De verwachting is dat de nationale wetten, de Cyberbeveiligingswet (Cbw/NIS2) en de Wet weerbaarheid kritieke entiteiten (Wwke/CER), in het 3e kwartaal van 2025 in EUNL in werking treden. Voor beide wetten is bepaald dat de onderwerpen die in deze wetten worden geregeld, op dit moment nog niet uitvoerbaar zijn in Caribisch Nederland voor onder meer de openbare lichamen. Citaat uit MvT bij Cbw: "Echter de regering vindt wel degelijk dat er in Caribisch Nederland regels gelden voor cyberbeveiliging en dat het lagere cyberbeveiligingsniveau geen reden kan zijn om geen wettelijke ondergrens neer te zetten"[5].
Ter voorbereiding wordt op dit moment nog uitvoering gegeven aan een aantal randvoorwaarden voor het versterken van de weerbaarheid op de BES. In het kader van de Veiligheidsstrategie van het Koninkrijk wordt gewerkt aan het in kaart brengen welke processen op de BES mogelijk maatschappelijk ontwrichtende effecten hebben, zodat duidelijk is welke processen betere bescherming behoeven.

[5] Pagina 71 Memorie van toelichting Cyberbeveiligingswet

In de memorie van toelichting van het wetsvoorstel "Wet invoering BSN en voorzieningen digitale overheid BES" wordt verder een aantal uitgangspunten geformuleerd ten aanzien van informatiebeveiliging:

1. Er wordt vanuit gegaan dat er gebruik wordt gemaakt voor aansluiting op de BSN, BRP en Wdo voorzieningen van de systemen van Europees Nederland (o.a. Diginetwerk en PKI-certificaten);
2. De BIO zal gaan gelden voor de BES aansluiting op de BSN, BRP en Wdo voorzieningen van de systemen van Europees Nederland (o.a. Diginetwerk en PKI-certificaten)*;

   * Dit is heel in hoge mate afhankelijk van de gekozen organisatievorm van de IT-provider. Een IT-provider, die meer dan alleen aansluiting op de BSN, BRP en Wdo voorzieningen doet zal dat voor alle processen die BSN, BRP en Wdo voorzieningen doen moeten doen. Die zijn dan vaak generiek. Bijvoorbeeld een wijzigingsproces zal voor de hele organisatie gelden. Dat zal dit waarschijnlijk een standaard als ISO27001 betekenen.

3. Zelfevaluatie voor de bevolkingsadministratie zoals voor Europees Nederlandse gemeenten geldt, zal ook worden ingevoerd.

Wat niet is meegenomen hierbij is de complexe situatie van de uitwisseling van persoonsgegevens door de aanwezige technische invulling door het gebruik van een IT-provider op Curaçao. Dit betekent dat de IT-infrastructuur en de leverancier daarvan zullen moeten voldoen aan de eisen van de BIO.

3.2.4 Consequenties van de statussen

INLEIDING
De invoeringsdatum van de wetten, die hierboven zijn beschreven, is nog onduidelijk. Idealiter zouden bij de invoering van de wetten de privacy en informatiebeveiliging, alsmede alle randvoorwaarden voor een beveiligd gebruik van DigiD bij alle betrokken organisatiezijn ingevuld. Dit zal waarschijnlijk niet volledig haalbaar zijn. Daarom zal er voor de stelselhouder BRP en de architectuurkeuze een minimumniveau van gegevensbescherming moeten worden gedefinieerd dat voldoende waarborgen biedt en kan worden gebruikt als de wetten daadwerkelijk worden ingevoerd. Hieronder wordt hiervoor een eerste aanzet beschreven. Ontwikkelingen volgen elkaar snel op. Daarom kan het wenselijk zijn onderstaande analyse in een volgende fase van het programma aan te passen.

DE STELSELHOUDER BRP (MIN BZK)
De stelselhouder zal rekening moeten houden met de AVG en de Cyberbeveiligingswet om te komen tot een minimumniveau. Vanuit de AVG en de Cyberbeveiligingswet worden als eerste stap een DPIA en een risicoanalyse geadviseerd. Deze rapportage levert daar een aandeel in maar vanuit de bredere verantwoordelijkheid en het zwaardere accent dat de Cyberbeveiligingswet daarop legt, lijkt een verbreding nog nodig.

DE ARCHITECTUURKEUZE

Er loopt een parallel onderzoek naar een datacenter architectuur. Dat onderzoek zal zich moeten richten op de afvragen of:

1. De systemen van Europees Nederland zonder meer bruikbaar zijn vanwege de grote afstand;
2. Gebruik kan worden gemaakt van een Amerikaanse cloudleverancier;
3. Gebruik gemaakt kan worden van een leverancier op de CAS eilanden;
4. Een lokale (BES) leverancier kan voldoen aan de BIO en de Cyberbeveiligingswet.

Voor punt 2 is het nodig dat wordt gekeken naar de eisen uit:

1. Rijks breed cloudbeleid 2022;
2. Implementatiekader risicoafweging cloudgebruik.

Wat daarbij zeer relevant is en de privacy-situatie nog complexer maakt, is het feit dat bijzondere persoonsgegevens niet zomaar in de Amerikaanse Cloud mogen worden geplaatst vanwege het Rijks breed cloudbeleid 2022. De huidige onzekerheid over het Trans-Atlantisch Gegevensbeschermingskader (TADPF) door het ontslag door President Trump van de Privacy- en Burgerrechtentoezichtsraad (PCLOB) maakt dit nog onzekerder.

Voor punt 4 geldt dat het van belang is wie de contractpartij is. Dat zullen de BES-organisaties zijn, maar als tussenmaatregel is het mogelijk dat Europees Nederland de grote kennis en kunde als opdrachtgever inzet om een minimumniveau te realiseren en daarna de verantwoordelijkheid overdraagt. Dit zou samen kunnen lopen met het verder groeien in volwassenheid van de IT-organisatie van de BES zelf. Hierbij lijkt een traject om ISO27001 gecertificeerd te worden voor zowel de lokale leverancier als de IT-organisatie van de BES een goede optie. Ook omdat de BIO2.0 die volgt uit de Cyberbeveiligingswet zwaar leunt op de ISO27001.

3.3 Organisatie en processen laag

Deze laag uit het model gaat in op de organisaties en processen om de afgesproken producten en diensten van de overheid te kunnen leveren. Hieronder valt ook de manier waarop de organisaties daarbij het een dienstverleningsconcept uitwerken en toepassen en de manier waarop de organisaties hun uiteindelijke werkwijzen inrichten. Onderstaand een opsomming en analyse hierop.

3.3.1 Mate van digitalisering processen

Vanuit dit onderzoek kunnen wij constateren dat voordat BSN en DigiD kan worden gebruikt, de processen waarvoor deze 'middelen' kunnen worden ingezet nog zeer beperkt gedigitaliseerd zijn. Dit brengt kansen en risico's met zich mee. Als voornaamste kansen, die ook (h)erkend worden door de onderzochte organisaties zijn:

- Efficiëntieverbetering van werkzaamheden: Taken die handmatig worden uitgevoerd, kunnen nu geautomatiseerd worden, wat de doorlooptijd van processen verkort. Deze 'winst' wordt vooral gezien bij de digitalisering van gestandaardiseerde processen die veel voorkomen.
- Toegankelijkheid en flexibiliteit: de afhankelijkheid van een fysieke identificatie van een persoon maakt veel overheidsprocessen inflexibel en ontoegankelijk.
- Betere dienstverlening.

NB: Dit zijn kansen die benut kunnen worden indien de eigen processen worden gedigitaliseerd. DigiD is slechts een inlogmiddel om de burger toegang te geven tot die dienstverlening. De keuze voor DigiD is dus niet gekoppeld aan deze kansen, maar is een nadere inrichtingskeuze die een organisatie kan maken om op een veilige manier burgers te laten inloggen.

De risico's die (h)erkend worden door de onderzochte organisatie zijn:

- Beveiliging: Digitalisering brengt beveiligingsrisico's met zich mee, zoals cyberaanvallen, datalekken, onbeschikbaarheid van dienstverlening en inbreuken op de privacy. Het is essentieel om robuuste beveiligingsmaatregelen te implementeren om gevoelige informatie te beschermen. DigiD is een inlog en authenticatiemiddel die meerdere beveiligingsmaatregelen met zich meebrengt, maar dekt (indien goed geïmplementeerd) slechts een deel van de te nemen beveiligingsmaatregelen af.
- Technologische afhankelijkheid: Bijna alle onderzochte organisaties hebben 1 of slechts enkele leveranciers waar zij op leunen voor de digitale ondersteuning van hun dienstverlening. Logischerwijs zijn dit ook de leveranciers die betrokken zijn bij het digitaliseren van de processen en de implementatie van DigiD. Dit kan de organisaties zowel inhoudelijk als technologisch afhankelijk maken van die leveranciers. Aandacht voor continuïteit van de dienstverlening is daarbij dus van groot belang.
- Technische innovatie: Technologie evolueert snel, en digitale systemen kunnen na verloop van tijd verouderd raken. Het vereist voortdurende investeringen en updates om relevant te blijven.

3.3.2 Kennis, beschikbaarheid en capaciteit

Het digitaliseren van processen en het implementeren van DigiD vereist een bepaald kennisniveau binnen de werknemers van de organisaties en voldoende beschikbaarheid en capaciteit van die medewerkers.

Een helder knelpunt dat wij wel zien is beschikbaarheid en capaciteit: zowel de beschikbare tijd van die medewerkers voor dit onderwerp, als de beperkte omvang van de groep medewerkers. Met name de ontwikkeling van de benodigde kennis en capaciteit om te voldoen aan de aansluitvoorwaarden en de beveiligingseisen van het DigiD assessment is nu al een knelpunt. Ook de begeleiding van die overheidsorganisaties die kunnen aansluiten op DigiD is een knelpunt.

De aanstaande digitaliseringsslag omvat het ontwerpen van processen, de inrichting ervan, het in beheer nemen ervan en de organisatieverandering (en opleiding) voor de implementatie. Dit zal niet alleen een grote claim leggen op de beschikbare kennis en capaciteit van de organisaties. Het is dus zeer aannemelijk dat er een groei nodig is van de beschikbare capaciteit: zowel op proces als op inhoud. Een risico is dat de omvang van de organisatie simpelweg niet toereikend is om de noodzakelijke maatregelen te nemen die uit deze pre-check volgen.

Het gebrek aan capaciteit lijkt hier wel een generiek probleem, dat zich duidelijk aanbiedt voor DigiD.

3.3.3 Adoptie gebruiker

Gezien de fase waar de onderzochte organisaties in zitten is gebruikersadoptie nog geen 'issue'. Vanuit onze ervaring is het echter wel van groot belang dat hier al in een vroegtijdig stadium expliciete aandacht voor is. Gebruikersadoptie zien wij als een essentiële voorwaarde voor een succesvolle uitrol van o.a. DigiD: zowel de interne gebruikers (medewerkers) als de externe gebruikers (burgers).

Voor burgers zien wij de noodzaak voor een intensieve begeleiding om met behulp van de eigen computer en DigiD 'zaken' te gaan doen met de overheidsorganisaties en die inwoners te leren e-formulieren in te vullen met hulp van DigiD. Ook medewerkers kunnen weerstand bieden tegen veranderingen in processen, vooral als ze niet goed zijn opgeleid voor de nieuwe digitale tools. Investeringen in training zijn noodzakelijk om een soepele overgang te waarborgen.

3.3.4 Communicatie

Niet alleen de communicatie naar de burger toe, maar alle communicatie rondom de verdere digitalisering op CN - waar de aansluiting op DigiD een onderdeel van is - moet worden begeleid en doordacht. Een communicatieplan kan hierbij hulp bieden om effectief te communiceren over het aansluitingsproces op DigiD en ervoor zorgen dat belanghebbenden goed geïnformeerd en betrokken zijn. Een dergelijk plan moet per organisatie worden opgesteld, maar ook aansluiten op andere organisaties: de boodschap die gecommuniceerd moet worden moet immers breed gedragen zijn en niet in strijd zijn met andere uitingen: de 'rode draad' moet helder zijn. Het opstellen van een dergelijk plan is een stevige exercitie, maar hierbij moet ten minste helder zijn: welke doelgroepen worden onderkent en welke doelstellingen moeten worden bereikt per doelgroep, welke (kern)boodschap wordt gegeven en welke communicatiemiddelen worden ingezet die boodschap te verspreiden, welke timing en planning hiervoor worden gehanteerd, hoe training en opleiding wordt ingezet, welke risico's en uitdagingen worden gezien in het proces, en hoe de effectiviteit van de communicatie wordt getoetst (en hoe hierop (bij)gestuurd kan worden) en hoe de verdeling van verantwoordelijkheden is geregeld.

3.3.5 Uitbesteding dienstverlening

In de huidige situatie zien wij veel taken en verantwoordelijkheden die uitbesteed zijn aan externe partijen. Hierbij wordt gebruik gemaakt van Europees Nederlandse contractpartijen of zelf

gecontracteerde partijen. Omdat capaciteit en kennis een knelpunt is binnen de organisaties ligt een verdergaande uitbesteding van dienstverlening voor de hand. Hier kleven ook risico's aan, de voornaamste daarvan is de afhankelijkheid van de dienstverlener, maar ook de veranderende rol die de CN organisatie moet aannemen (van uitvoering naar regie). Ook biedt de CN IT dienstverleners beperktere mogelijkheden dan in EUNL. Dit vergt weer andere capaciteiten, een andere governance en een andere financiering.

a) Het volledig uitbesteden van de webportaal voor DigiD (applicatie, platform en infrastructuur) is goed mogelijk. OL Bonaire kiest daarvoor met Wind Internet.
b) Het uitbesteden van de applicatie is nu al gebruikelijk.
c) Het uitbesteden van platform en infrastructuur. Dit is zeker een optie. Een nadere afweging of dit in de cloud belegd kan worden. Dat kan dan wel alleen in Europa of in Caribisch Nederland. Dit maakt onderdeel uit van de op te stellen Datacenter strategie van RCN. Het laatste woord is hier nog niet over gesproken.

3.3.6 Afweging uitbesteden of zelf doen

Veel organisatie gaan over tot het uitbesteden van het ICT-beheer. Bijvoorbeeld omdat binnen de organisatie te weinig kennis van ICT-beheer of om te concentreren op de kernactiviteiten van de organisatie. Hier zijn voor- en nadelen aan.
Voordelen uitbesteden

- De zorg voor goed personeel ligt bij je dienstverlener en niet langer bij de eigen organisatie.
- De dienstverlener kan door schaalgrootte zorgen voor continuïteit
- De dienstverlener kan investeren in innovaties.

Er zitten natuurlijk ook nadelen aan het uitbesteden van ICT-beheer. De drie belangrijkste zijn:

- Het is doorgaans duurder dan een ICT-medewerker in dienst nemen.
- Afhankelijkheid van een andere partij.
- Niet iedere ICT-leverancier biedt hulp op je kantoor oftewel on-site support aan. Sommige bedrijven werken dus alleen op afstand. Het is belangrijk dat organisaties een doelbewuste keuze maken tussen zelf doen of uitbesteden.

3.3.7 ICT-beheer deels uitbesteden en zelf regievoeren

Uitbesteden stelt eisen aan het aansturen van de dienstverlener, vooral op het gebied van contract en servicemanagement. Vaak wordt het operationele ICT-beheer uitbesteed, gecombineerd met een deel zelf doen, de regievoering. Zo kan de externe partij de dagelijkse operaties uitvoeren en bewaken (ook wel monitoren genoemd). Gaat er ergens iets mis (een server dreigt vast te gaan lopen, een harddisk raakt te vol, een applicatie laadt te traag), dan krijgt de regievoerder een signaal om snel actie ondernemen. Ook kan een deel van het ICT-beheer (bijvoorbeeld upgrades regelen van systemen of nieuwe software installeren) op afstand gebeuren.

Van belang is in een zorgvuldig uitbestedingsproces hier afwegingen op te maken.
Onderwerpen die daarbij meegewogen worden zijn:

- Welke taken doen we zelf en welke besteden we uit?
- Hoe houden we controle over de uitbestede taken?
- Voldoet de leverancier aan de vereiste beheer en beveiligings-standaarden en kan ze daar een auditrapport dat voldoet aan de DigiD normen voor overleggen?
- Hoe zorgen we voor een goede transitie na beëindigen samenwerking?

Van belang is dit contractueel goed te regelen, bijvoorbeeld met de Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten (ARBIT) van de rijksoverheid of de Gemeentelijke Inkoopvoorwaarden bij IT (GibiT) voor gemeenten. De Inkoopeisen Cybersecurity Overheid Wizard (ICO Wizard) van de Baseline Informatiebeveiliging Overheid (BIO) helpt hierbij. Met de ICO-Wizard kunnen eisenpakketten worden geselecteerd die aansluiten op verschillende typen aan te besteden/in te kopen producten/diensten.

3.3.8 Cloud sourcing

Veel organisaties brengen de ICT dienstverlening naar de cloud. Cloudtechnologie biedt schaalbare en flexibele oplossingen, maar vereist robuuste verbindingen en duidelijke afspraken over dataregulering en kostenbeheersing.
Een recent rapport van de Algemene Rekenkamer waarschuwt dat organisaties onvoldoende grip hebben op cloudgebruik, wat leidt tot grote risico's voor gegevensbescherming, datasoevereiniteit en continuïteit. Kortom, meer aandacht voor de risico's van het gebruik van clouddiensten is gewenst.
Caribisch Nederland neemt een unieke positie in als Nederlands grondgebied binnen het Amerikaanse continent. Deze geografische en geopolitieke situatie brengt specifieke juridische vraagstukken met zich mee die van groot belang zijn bij clouddienstverlening. Een zorgvuldige aanpak is essentieel om te voldoen aan zowel Nederlandse als internationale wet- en regelgeving, met bijzondere aandacht voor gegevenslocatie en privacybescherming. Daarnaast zien wij de volgende aandachtspunten:

- Specifieke juridische situatie: Het beheer en de opslag van data in Caribisch Nederland vereisen een grondige evaluatie van de locatie waar gegevens worden verwerkt en opgeslagen. Vanwege de geografische nabijheid tot Amerika is het belangrijk om te waarborgen dat data uitsluitend toegankelijk blijft voor bevoegde partijen en beschermd is tegen eventuele Amerikaanse juridische of politieke invloeden, zoals via de Amerikaanse Cloud Act. De Amerikaanse Cloud Act verplicht techbedrijven om data met de Amerikaanse overheid te delen, wat botst met de Europese AVG, vooral sinds de Schrems II-uitspraak. Dit roept juridische onzekerheid en vragen op over de wenselijkheid van afhankelijkheid van mondiale cloudproviders.
- Toegang tot data en beveiliging: De vraag "Waar staan de data?" is van cruciaal belang, vooral gezien de gevoeligheid van overheidsinformatie. Het is noodzakelijk dat gegevens opgeslagen worden op locaties waar gegarandeerd kan worden dat ze beschermd zijn

tegen buitenlandse toegang, tenzij dit expliciet is toegestaan volgens internationale afspraken. Dit geldt met name voor gevoelige gegevens zoals persoonlijke informatie en identificatiemiddelen.

De juridische aspecten worden verder besproken in 3.2 Wet- en regelgeving.

3.3.9 Auditing

Een voorwaarde om een webapplicatie te kunnen aansluiten op DigiD is het voldoen aan het zogenaamde DigiD assessment door een Register EDP-auditor (RE-auditor).
De toezichthouder Logius heeft de aansluitvoorwaarden gepubliceerd:
https://www.logius.nl/domeinen/toegang/digid/ict-beveiligingsassessments-digid/ict-beveiligingsassessments-digid-in-het-algemeen

Logius hanteert hiervoor het normenkader 3.0 voor ICT-beveiligingsassessments DigiD, ontleend aan de NCSC richtlijnen voor webapplicaties:
https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties.

De NOREA heeft op basis van de normenset de Handreiking DigiD assessments ontwikkeld, die op gedetailleerd niveau aangeeft waar de bewijsvoering voor het voldoen aan de normen moet voldoen: https://www.norea.nl/organisatie/werkgroepen/werkgroep-digid-assessments
.

Een pentest kan onderdeel zijn van dit assessment. Deze pentest moet specifiek gericht zijn op kwetsbaarheden van webfacing applicaties. De OWASP Top 10 is een standaard voor ontwikkelaars en webapplicatiebeveiliging. Het vertegenwoordigt een brede consensus over de meest kritische veiligheidsrisico's voor webapplicaties: https://owasp.org/www-project-top-ten/

Bij het DigiD assessment wordt onderscheid gemaakt tussen de carve-out methode, waarbij de auditor steunt op assurance-rapporten (ISAE 3000 of 3402) volgens een overeengekomen normenkader van de betroffen serviceorganisatie en de inclusive methode, waarbij de auditor zelf onderzoek uitvoert bij de betroffen serviceorganisatie.
De carve-out methode houdt in dat systemen of diensten die door derden worden beheerd (zoals cloudproviders of externe softwareleveranciers) niet rechtstreeks binnen de scope van de audit van de aansluithouder vallen. In plaats daarvan zal de audit zich richten op de interne beheersmaatregelen van de aansluithouder en het vertrouwen in de serviceorganisatie zal worden gebaseerd op het DigiD assurance-rapport door een RE van de serviceorganisatie. Dit werd voorheen ook wel de Third Party Memorandum (TPM) genoemd.
Dit rapport door de auditor van de aansluithouder wordt beoordeeld om te verifiëren of de externe partij adequate DigiD beveiligingsmaatregelen heeft geïmplementeerd en onderhoudt (Opzet, bestaan en werking).

Een mogelijke toekomstige mogelijkheid is het gebruik maken van de Leverancier Meervoudig Assessement (LMA), dan worden alle normen getoetst bij de leverancier en heeft de aansluithouder geen auditkosten. Dit zijn dan wel hoog gestandaardiseerde SaaS-diensten waar de aansluithouder zelf geen enkele beheertaak en beheerbevoegdheid in heeft. Op dit moment is dit alleen mogelijk in de zorgsector (huisartsen en apotheken). Er worden nu beleidsvoorstellen gedaan om dit ook mogelijk te maken voor overheidsdiensten.

3.3.10 Kosten

Voor een overheidsorganisatie zijn er kosten verbonden om aan te sluiten op DigiD. Hierbij maken wij onderscheid tussen directe en indirecte kosten.

Voorheen werd er gewerkt met een doorbelasting aan afnemers van de dienstverlening van Logius voor onder andere DigiD. De Generieke Digitale Infrastructuur (GDI, waar DigiD onderdeel van is) van de overheid wordt vanaf 2023 gefinancierd vanuit een centraal budget. Het budget is beschikbaar voor Beheer & Exploitatie, Doorontwikkeling en Vernieuwing. BZK beheert dit budget. De directe kosten voor de aansluiting op DigiD zijn hiermee weggevallen.
De overige kosten die gemoeid zijn met het digitaliseren van de werkprocessen en dus het feitelijk bouwen en beheren van de webapplicatie die gebruik maakt van DigiD vallen buiten scope van deze analyse.

Ter indicatie kan rekening worden gehouden met de volgende DigiD assessment kosten.

- DigiD assessment bij volledige uitbesteding en steunen op de TPM van serviceorganisatie kost ongeveer €6.000,-
- DigiD assessment bij on-premise €12.000, - plus pentest á €12.000, -
- PKI-O certificaat Digipoort[6] € 300,- tot € 400,-.

Indirecte kosten voor het voldoen aan de DigiD normen zijn per organisatie die de pre-check hebben doorlopen uitgewerkt (zie rapporten A). Deze kosten komen veelal neer op het opstellen van beleidsdocumenten en het inrichten en onderhouden van beheerprocessen. Deze kosten variëren van € 10-20.000 incidenteel en € 5-10.000 structureel.

3.4 Informatielaag

Op deze laag uit het model gaan wij in op de daadwerkelijke informatie die uitgewisseld moet worden en omvat de gegevens en de logica die nodig zijn voor de verwerking van de gegevens.

Op de informatielaag zien wij als belangrijke voorwaarde een intensieve begeleiding van de overheidsdiensten om hard copy formulieren om te zetten naar elektronische formulieren. Ook

[6] Digipoort is de ICT-centrale waar berichtenverkeer voor de overheid afgehandeld wordt. Digipoort werkt als een elektronisch postkantoor. Digipoort ontvangt het bericht; controleert het bericht op een aantal eisen; bevestigt, desgewenst namens de organisatie, de ontvangst van het bericht. Logius zorgt voor de beschikbaarheid, juiste werking, continuïteit en beveiliging van Digipoort.

om in de toekomst meer processen te digitaliseren én daarmee dus gebruik te kunnen maken van een veilig inlogmiddel zoals DigiD.

3.4.1 Informatiehuishouding

In haar model geeft NORA ook aan dat "Een belangrijke basis voor samenwerking, is het delen van taal en begrippen (woorden), zodat we elkaar kunnen begrijpen en voor het uitwisselen en (her)gebruiken van elkanders informatie". Een informatiehuishouding die op orde is, per organisatie, is dus van groot belang. Die informatiehuishouding moet ervoor zorgen dat informatie effectief wordt beheerd, beschermd en gebruikt. Wij doen de aanname dat dit bij de onderzochte organisaties in CN nog niet het geval is. In de laatste jaren worden er zeer veel projecten en programma's uitgevoerd in Europees Nederland ten behoeve van een verbeterde informatiehuishouding. Van dit soort programma's zou CN nu al kunnen profiteren. Of hier tijd, capaciteit en middelen voor zijn is buiten scope van onze analyse. Belangrijkste lessen (globaal) die voor CN getrokken kunnen worden zijn:

Begin met het definiëren van de doelstellingen van het digitale proces. Welke informatie moet worden vastgelegd, verwerkt en bewaard? Zorg ervoor dat de doelstellingen nauwkeurig en meetbaar zijn. Analyseer de soorten informatie die binnen het proces worden gegenereerd en verwerkt. Veelal betreft het de verwerking en soms opslag van persoonsgegevens, gevoelige persoonsgegevens en soms zelf bijzondere persoonsgegevens. Dit speelt bij de DigiD norm U/WA.05. Classificeer de informatie op basis van gevoeligheid, urgentie en andere relevante criteria. Dit helpt bij het bepalen van de juiste beveiligings- en bewaarprocedures. Beveiligingsmaatregelen moeten worden geïntegreerd in alle stadia van het digitale proces, inclusief gegevensinvoer, -verwerking en -opslag. Implementeer adequate authenticatie, autorisatie en versleuteling om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen. Werk een framework van de governance uit (IT governance en data governance) waarin ook (naleving op) relevante wet- en regelgeving is opgenomen. Implementeer procedures voor het beheren van de levenscyclus van informatie, van creatie tot vernietiging. Dit omvat het vaststellen van bewaartermijnen, het archiveren van oude gegevens en het veilig verwijderen van informatie die niet langer nodig is. Maak de informatiehuishouding ook onderdeel van je opleidingsaanbod en bewustwordingscampagnes zodat zij op de hoogte zijn van de relevante informatiebeheerpraktijken en -richtlijnen. Richt ook toezicht en naleving in op deze processen.

3.4.2 Gegevensverwerking binnen DigiD:

DigiD verwerkt persoonsgegevens, omdat met DigiD de authenticiteit van een (natuurlijk) persoon vastgesteld kan worden en gebruikt kan worden om in te loggen. Hiervoor gebruikt DigiD diverse persoonsgegevens, alsmede diverse unieke waardes die de persoon representeren of herleidbaar zijn naar een persoon. Deze unieke waardes kunnen ook cryptografische sleutels zijn die gebruikt worden in de gegevensverwerking van DigiD.

Om alle persoonsgegevens binnen DigiD te kunnen beschrijven is eerst een beschrijving nodig van de containerbegrippen die binnen DigiD gehanteerd worden voor gegevens. Deze containerbegrippen vormen samen het conceptuele gegevensmodel van DigiD.

Account
Het centrale begrip binnen DigiD is het account, waarmee een persoon wordt vastgelegd die gebruik maakt van DigiD. Bij de vastlegging van het account worden diverse persoonsgegevens gebruikt. Het centrale gegeven bij DigiD is het BSN van de persoon. Andere gegevens die gebruikt worden bij het account zijn pseudoniemen, cryptografische sleutels en andere unieke waardes. Bij een account kunnen een of meer authenticatiemiddelen horen.

Authenticatiemiddel
Het gebruik van DigiD door een persoon vindt plaats met behulp van een authenticatiemiddel. Een gebruiker heeft een of meerdere authenticatiemiddelen. Bij de vastlegging van een authenticatiemiddel kan gebruik gemaakt worden van unieke waardes en/of cryptografische sleutels, die direct of via het account herleidbaar zijn naar een persoon.
Bij de authenticatiemiddelen van DigiD worden verschillende unieke gegevens gebruikt:

- Unieke gebruikersnaam met wachtwoord (of een representatie ervan)
- Unieke installatie van de DigiD app (unieke waardes van software en hardware) met pincode (of een representatie ervan)
- Digitale identiteit op een identiteitsbewijs met pincode (eID-middel). Het ontwerp van de Digitale identiteit (eID) valt niet onder deze DPIA, maar is uitgelegd in de PIA van DigiD Hoog.

Transactie
Het gebruik van DigiD vindt plaats door middel van transacties. Dit zijn handelingen die de gebruiker uitvoert op het account en/of het authenticatiemiddel. Een transactie begint meestal met een gebruikershandeling en kan vervolgd worden met diverse andere handelingen, alsmede geautomatiseerde systeemhandelingen. Een transactie wordt normaalgesproken voltooid, maar door diverse omstandigheden (verbindingsproblemen, controles etc.) kan een transactie voortijdig worden afgebroken. Ook kan een transactie tijdelijk onderbroken worden omdat het wacht op een ander proces of op een andere transactie. Elke transactie is uniek en heeft daarom een unieke waarde. Via het account en/of authenticatiemiddel is een transactie herleidbaar naar een persoon.

Tijdelijke code
Wanneer een transactie tijdelijk onderbroken wordt, omdat deze pas verder kan als er een ander proces of een andere transactie wordt voltooid, maakt DigiD gebruik van een tijdelijke code. Deze tijdelijke code wordt naar de gebruiker verstuurd, die deze kan gebruiken om de transactie te voltooien. Binnen de context van de transactie is deze tijdelijke code uniek en is, via de transactie, het account en/of authenticatiemiddel herleidbaar naar een persoon. Voorbeelden van de tijdelijke codes bij DigiD zijn: sms-code, activatie-code, balie-code, etc.

Notificatiekanaal

Een bericht (notificatie) van DigiD kan verstuurd worden naar een gebruiker via een notificatiekanaal. Naast berichten over het DigiD account en/of authenticatiemiddel, kunnen ook tijdelijke codes via het notificatiekanaal verstuurd worden. Het notificatiekanaal zelf valt niet binnen de verantwoordelijkheid van DigiD. Er kan dus niet met zekerheid bepaald worden door DigiD, of de gebruiker daadwerkelijk de notificatie ontvangt en/of het daadwerkelijk de beoogde gebruiker is. Bovendien kan een notificatiekanaal door meerdere personen gebruikt worden en/of zelfs door derden.

3.4.3 Taal

Anders dan in Europees Nederland is ook de taal zelf waarin gecommuniceerd wordt van belang, zowel intern in de organisaties als naar de burgers toe. Hoewel Papiaments, Engels en Nederlands allemaal officiële talen zijn in Caribisch Nederland, kan het gebruik van elke taal variëren afhankelijk van de context en de lokale bevolking. De Papiamentse, Engelse en Nederlandse taal dienen als basis voor alle technische voorzieningen én communicatie met burgers, ondernemers en medewerkers. In de informatievoorziening moet hier dus ook expliciet rekening mee worden gehouden.

3.4.4 Gebruikersondersteuning

Bij het gebruik van DigiD in CN moet ook aan aanvullende risico's worden gedacht als het gaat om het gebruik en de ondersteuning van die gebruikers. Hierbij kan worden gedacht aan bijvoorbeeld de gewenste ondersteuning voor de eindgebruiker (burger) vanuit Europees Nederland of van de gebruiker (CN organisatie). De risico's die voor de hand liggen hierbij zijn onder andere het tijdsverschil tussen Europees Nederland en CN, de gesproken en/of geschreven taal van de ondersteuning en de kennis van de (technische) inrichting van het applicatielandschap. Afspraken moeten worden gemaakt met leveranciers en stakeholders over servicelevels, beschikbaarheid en dergelijke. Daarnaast zal het gebruik van DigiD ook beslag leggen op de capaciteit van de eigen organisatie: dit is een nieuwe dienstverlening waar extra ondersteuning voor nodig zal zijn. Voorbeelden van activiteiten die ondernomen moeten worden zijn:

- eFormulieren ontwikkelen en onderhouden
- Helpfuncties een helpteksten maken
- Communicatie over eFormulieren opstellen
- Ondersteunen minder digitaal vaardigen (service desk)
- FAQ's opstellen en onderhouden

3.5 Applicatielaag

Op de applicatielaag is een randvoorwaarde dat de webapplicatie van de overheidsorganisatie voldoet de aansluitvoorwaarden en beveiligingseisen van het DigiD assessment en dat de applicatie eenvoudig is te gebruiken is door burgers en door de organisatie te beheren. Wenselijk is het hierbij aan te sluiten bij de standaarden van het Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden).

Maar ook voor de internetbrowsers van de inwoners is soms een update noodzakelijk, bijvoorbeeld om een beveiligingsprobleem op te lossen. Updaten gaat bijna altijd automatisch. Toch is het slim om af en toe te controleren of er een nieuwere versie van het programma is.

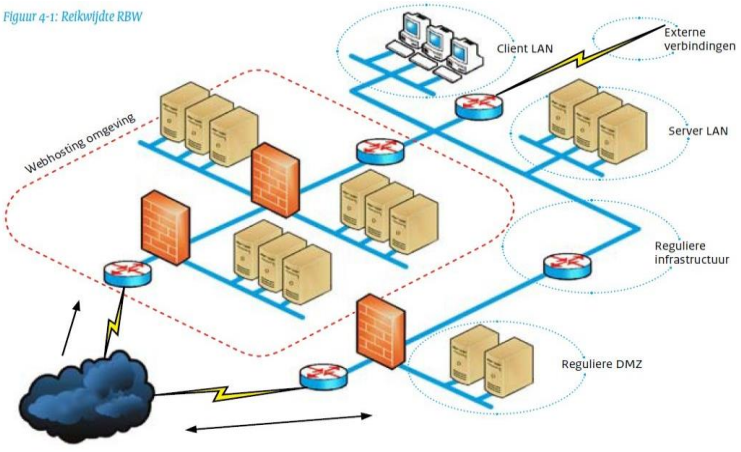
3.5.1 DigiD webapplicatie

De webapplicatie die gekoppeld is aan DigiD kan verschillende verschijningsvormen hebben. Zo kan de DigiD webapplicatie een onderdeel zijn van een webapplicatie, bijvoorbeeld in de vorm van een formulieren generator. De DigiD webapplicatie kan een webfacing front-end zijn van een back-office zaaksysteem. Ook kan de DigiD webapplicatie een zelfstandig systeem zijn dat enerzijds gekoppeld is aan DigiD en anderzijds aan via een generiek koppelvalk aan een back-office systeem. De checklist DigiD aansluiting geeft de specificaties voor de DigiD webapplicatie: https://www.logius.nl/onze-dienstverlening/domeinen/toegang/digid/documentatie/checklist-aansluiten-op-digid-en-digid-machtigen.

Het DigiD assessment richt zich 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. Het onderstaande schema toont de webomgeving die wordt onderzocht door middel van een infrastructurele test.

Figuur 4-1: Reikwijdte RBW



3.5.2 DigiD

DigiD is de elektronische authenticatievoorziening die zorgdraagt voor de uitgifte van elektronische authenticatiemiddelen. Hiermee kunnen natuurlijke personen (gebruikers) zich online (via internet) authentiseren bij dienstverleners die een aansluiting hebben op DigiD. Hierbij wordt het burgerservicenummer (BSN) doorgegeven aan de dienstverlener. Dienstverleners zijn overheidsorganisaties en/of privaatrechtelijke organisaties, die op basis van een wet of wettelijke regeling belast zijn met de uitvoering van een publieke taak. Dienstverleners kunnen DigiD gebruiken ten behoeve van de uitvoering van de publieke taak. Dienstverleners zijn wettelijk bevoegd om de BSN's te gebruiken voor de uitvoering van de publieke of wettelijke taak. Deze dienstverleners zijn onder andere ministeries en gemeenten, pensioenfondsen en zorgverzekeraars.

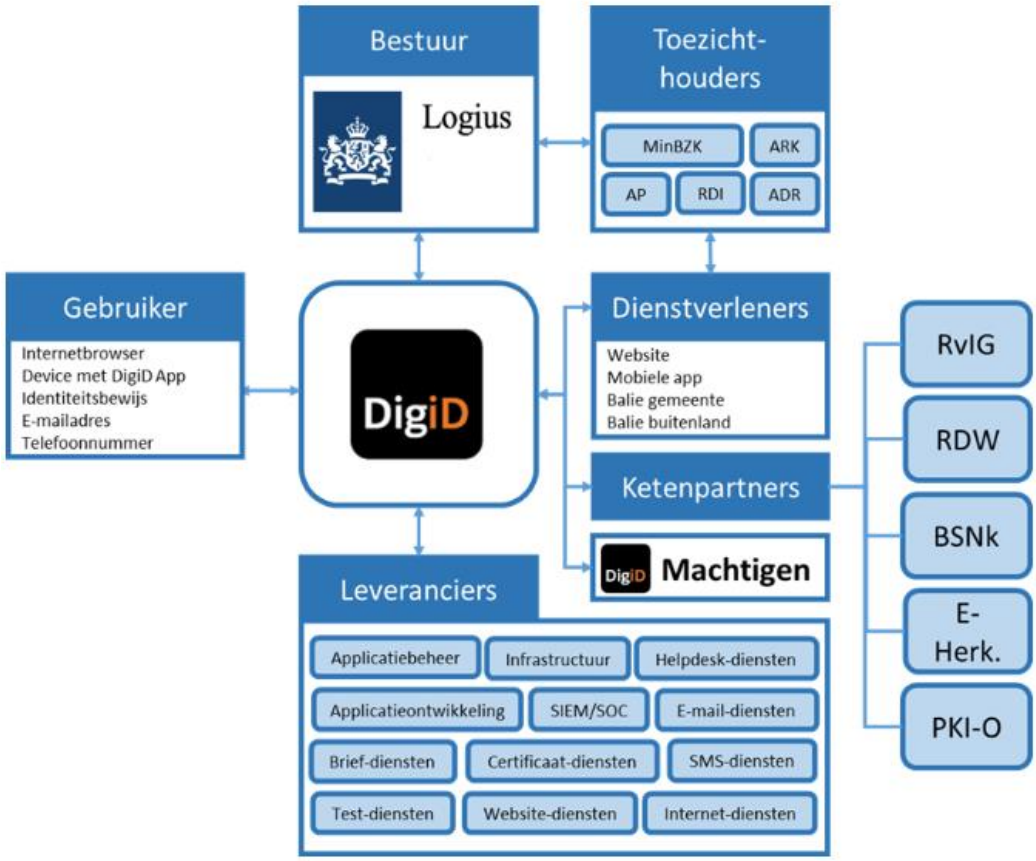
De gegevensverwerkingen, in het kader van DigiD, vinden plaats ter uitvoering van de taak van de minister van Binnenlandse Zaken en Koninkrijksrelaties. De grondslag voor deze gegevensverwerkingen is de wet Digitale overheid (voorganger Wet elektronisch berichtenverkeer). Deze grondslag is verder uitgewerkt in het Besluit Digitale Overheid (voorganger besluit verwerking persoonsgegevens generieke digitale infrastructuur) en de Regeling voorzieningen WDO (voorganger Regeling voorzieningen GDI). Gelet hierop is sprake van gegevensverwerkingen die vallen onder de verwerkingsgrond van artikel 6, eerste lid onder e van de AVG: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang. Deze voorgaande wet- en regelgeving voorziet in de verwerking van het BSN in het stelsel van voorzieningen GDI. Het BSN mag worden verwerkt voor zover dit noodzakelijk is voor de goede uitvoering van hun taken en verplichtingen ingevolge de wet Digitale overheid (WDO).
Binnen het huidige stelsel voorziet DigiD in diverse elektronische authenticatiemiddelen op basis van het BSN.

A Het betreft de volgende inlogmethodes :
- Gebruikersnaam met wachtwoord, eventueel aangevuld met sms-controle (betrouwbaarheidsniveau Laag)
- DigiD app met pincode (betrouwbaarheidsniveau Laag), eventueel aangevuld met ID-check (betrouwbaarheidsniveau Substantieel)*
- Digitale identiteit op een identiteitsbewijs** met pincode (eID-middel op betrouwbaarheidsniveau Hoog)

B * De ID-check uitvoeren (niveau Substantieel) kan met de volgende identiteitsbewijzen:
- Nederlands rijbewijs uitgegeven na 14 november 2014 (door Rijksdienst voor het Wegverkeer)
- Nederlandse identiteitskaart
- Nederlands paspoort

C ** Inloggen op niveau Hoog kan met de volgende identiteitsbewijzen:
- Nederlands rijbewijs uitgegeven vanaf 26-5-2018 (door Rijksdienst voor het Wegverkeer)
- Nederlandse identiteitskaart uitgegeven vanaf 13-3-2021 (door Rijksdienst voor Identiteitsgegevens)

D De reikwijdte van de gegevensverwerkingen van DigiD kan bepaald worden aan de hand van het onderstaande omgevingsmodel.Zie verder: https://www.logius.nl/domeinen/toegang/digid/documentatie/gegevensverwerkingen-digid



DigiD valt als voorziening onder het bestuur van Logius, de dienst digitale overheid, en is onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (ministerie van BZK). Het ministerie van BZK heeft naast de aansturende functie ook een toezichthoudende functie, net als andere partijen zoals de Autoriteit Persoonsgegevens (AP), de Rijksinspectie digitale infrastructuur (RDI), de Algemene Rekenkamer (ARK) en de Auditdienst Rijk (ADR).

De voorziening DigiD maakt gebruik van dienstverleners en ketenpartners. Dit zijn partijen binnen of buiten Logius die bepaalde dienstverlening bieden die noodzakelijk zijn voor het functioneren van DigiD. De eveneens onder Logius vallende voorziening DigiD Machtigen is voor bepaalde processen afhankelijk van de voorziening DigiD. Daarnaast maakt DigiD voor bepaalde onderdelen gebruik van leveranciers, die gecontracteerd worden vanuit Logius of vanuit een breder (rijks)overheid verband.

De processen die direct gerelateerd zijn aan de voorziening DigiD, met gegevensverwerking van de (beoogde) gebruiker(s), zijn onderdeel van de DPIA. Gerelateerde processen die niet zichtbaar

zijn voor de gebruiker(s), o.a. in het door Logius uitgevoerde relatiebeheer met de dienstverleners, ketenpartners en leveranciers, het bestuur (de besturing) van DigiD en de toezichthouders, vormen geen onderdeel van de DPIA.

3.5.3 TVS

ToegangVerleningService (TVS) maakt het voor overheidsorganisaties en zorgaanbieders eenvoudig om via inlogmiddelen zoals eHerkenning en DigiD hun digitale dienstverlening te ontsluiten voor ondernemers en burgers. In onze analyse heeft de implementatie of het gebruik van TVS nog geen prominente positie gehad. Er is een CN brede overeenkomst voor het gebruik van TVS. Deze laat nog wel vrijheid. Het gebruik van TVS stelt organisaties in staat om toegang te verlenen tot hun onlinediensten met behulp van DigiD, zonder dat gebruikers aparte inloggegevens voor die specifieke diensten nodig hebben. Met andere woorden, TVS integreert de authenticatiefunctionaliteit van DigiD naadloos in de onlinediensten van de betreffende organisatie. TVS voegt dus een extra laag toe aan het DigiD-authenticatieproces, waardoor gebruikers met hun bestaande DigiD-inloggegevens toegang kunnen krijgen tot specifieke diensten van een bepaalde organisatie, zonder aparte inloggegevens te hoeven gebruiken. Dit verhoogt het gemak en de gebruikerservaring bij het gebruik van onlinediensten.

Indien er in de toekomst meer publieke en private inlogmiddelen toegestaan worden, dan is TVS nodig. TVS fungeert namelijk als toegangspoort voor dienstverleners. Daardoor is het niet langer nodig dat overheidsorganisaties en zorgaanbieders zelf aansluitingen ontwikkelen en beheren voor deze inlogmiddelen. TVS neemt hen daarmee een zorg uit handen. Ook als er nieuwe inlogmiddelen komen. Deze dienst kan dus – eventueel – ook voordelen voor CN opleveren.

Vooralsnog is TVS alleen beschikbaar voor (rijks)overheidsorganisaties en zorgaanbieders. Op dit moment wordt TVS al gebruikt op verschillende portalen van RVO, NVWA en Rijksinspectie Digitale Infrastructuur (RDI). Ook bij ziekenhuizen, tandartsen en andere zorgverleners is de service in gebruik. Op beleidsniveau is inmiddels de ruimte geboden om dit uit te breiden naar andere overheidsorganisaties. De feitelijke realisatie dient nog plaats te vinden.

3.5.4 Beveiligingsniveau en inlogmiddel

Om DigiD te kunnen gebruiken is er een methode van inloggen nodig. In Europees Nederland wordt het beveiligingsniveau gekoppeld aan het inlogmiddel. Gebruikers loggen in met een gebruikersnaam en wachtwoord, eventueel aangevuld met een extra controle via SMS of de DigiD-app. Bij het gebruik van DigiD in CN zal ook aan diezelfde voorwaarden moeten worden voldaan. DigiD kent verschillende betrouwbaarheidsniveaus die aansluiten op de eIDAS verordening.

Voor het bepalen van het benodigde betrouwbaarheidsniveau van de dienstverlening is er een Handreiking Betrouwbaarheidsniveaus[7] van het Forum Standaardisatie om een goede keuze te maken.

Sinds 1 juli 2023 bestaat de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening. Deze schrijft voor welk betrouwbaarheidsniveau vereist is voor de betreffende overheidsdienstverlening. De regeling vloeit voort uit de Wdo.

3.5.5 Basisregistraties en sectorregistraties

Op dit moment kent CN nog niet het begrip basisregistraties zoals dat in Europees Nederland wordt herkend.

3.5.6 PIVA

De registratie van persoonsgegevens van de eilanden vindt plaats in een systeem waar alle eilanden gebruik van maken: de PIVA. PIVA staat voor Persoonsinformatievoorziening Nederlandse Antillen en Aruba. RvIG zorgt ervoor dat de PIVA's zowel onderling kunnen communiceren als met de Basisregistratie Personen in Europees Nederland. RvIG beheert de PIVA-Verstrekkingsvoorziening (PIVA-V) waarin een kopie van de PIVA's van de BES-eilanden is opgeslagen. RvIG verstrekt deze persoonsgegevens aan geautoriseerde overheidsinstanties zowel in Europees als in Caribisch Nederland. Deze overheidsorganisaties gebruiken de persoonsgegevens in hun dienstverlening aan de burger. Door het gebruik van DigiD, maar vooral door het digitaliseren van de dienstverlening, kan er een grote kwaliteitsslag worden gemaakt in de PIVA. Dit houdt echter ook in dat er een helder proces moet komen voor het (online) doorgeven en verwerken van wijzigingen, en dergelijke. De vormgeving van deze processen valt buiten de scope van deze analyse.

3.5.7 Opzetten registraties

BZK en CN hebben met de invoering van het Burgerservicenummer (BSN) en inlogmiddelen van de digitale overheid een start gemaakt met de invoering van de eerste basisregistratie. Door Het BSN te koppelen aan andere basisregistraties uit het Stelsel van Basisregistraties kan de overheid efficiënter opereren en de dienstverlening verbeteren. CN en BZK hebben het initiatief genomen de registratie van adressen en gebouwen op de eilanden te verbeteren. Samen werken zij toe naar één centraal register voor elk eiland waarin adressen en gebouwen worden geregistreerd. In dat register worden luchtfoto's gebruikt om de precieze locatie van een adres of gebouw op een kaart te bepalen.

Er zijn 10 basisregistraties. Een basisregistratie is een door de overheid officieel aangewezen registratie met daarin gegevens van hoogwaardige kwaliteit, die door alle overheidsinstellingen

[7] https://www.forumstandaardisatie.nl/onderwerpen/veilig-internet/betrouwbaarheidsniveaus

verplicht en zonder nader onderzoek, worden gebruikt bij de uitvoering van publiekrechtelijke taken.
Iedere individuele basisregistratie moet voldoen aan de 12 eisen aan het Stelsel van Basisregistraties.

Eis 1: De registratie is bij wet geregeld
Eis 2: De afnemers hebben een terugmeldplicht
Eis 3: De basisregistratie wordt verplicht gebruikt door de hele overheid
Eis 4: Er is duidelijkheid over de aansprakelijkheid
Eis 5: De realisatie en exploitatie gebeuren tegen redelijke kosten en er is eenduidigheid over de verdeling ervan
Eis 6: Er is duidelijkheid over inhoud en bereik van de registratie
Eis 7: Er zijn sluitende afspraken en procedures tussen de houder van het register aan de ene kant en de leveranciers en de afnemers van gegevens aan de andere kant
Eis 8: Er zijn duidelijke procedures voor de toegankelijkheid van de basisregistratie
Eis 9: Er is een streng regime van kwaliteitsborging
Eis 10: Er is vastgelegd dat en hoe afnemers van gegevens op een niet-vrijblijvende manier betrokken worden bij de besluitvorming over de registratie
Eis 11: De positie van de basisregistratie binnen het stelsel van basisregistraties is duidelijk en de relaties met de basisregistraties zijn beschreven
Eis 12: De zeggenschap over de basisregistratie berust bij een bestuursorgaan en er is een minister verantwoordelijk voor het realiseren, resp. het functioneren van de registratie

Vier Stelselvoorzieningen ondersteunen de basisregistraties om hun product- en dienstenportfolio eenduidig te (gaan) ontsluiten naar de afnemers. Het Stelsel van Basisregistraties onderscheidt de volgende Stelselvoorzieningen:

- Digikoppeling. Dit is een set standaarden voor digitaal berichtenverkeer tussen overheidsorganisaties.
- Digimelding. Dit is een generieke oplossing voor het melden van fouten in basisregistraties op een uniforme manier.
- Digilevering. Hiermee kunnen afnemers zich 'abonneren' op gebeurtenisberichten uit de basisregistraties. Digilevering verspreidt deze berichten op basis van abonnementen.
- De stelselcatalogus. Dit is een online catalogus die de structuur van het Stelsel van Basisregistraties en de definities van soorten objecten, gegevens en berichten beschrijft.

CN is gestart met de implementatie van de eerste basisregistraties. Indien het stelsel van basisregistraties ook in CN ingevoerd wordt, dan dient aan een groot aantal organisatorische, technische en beveiligingsvoorwaarden voldaan te worden om de benodigde kwaliteit te kunnen waarborgen. De DigiD voorziening regelt alleen betrouwbare en veilige inlogmogelijkheid voor burgers (eHerkenning voor ondernemers). Voor een betrouwbare en veilige uitwisseling tussen basisregistraties zijn in ieder geval de vier stelselvoorzieningen nodig.

3.5.8 Bouwstenen en voorzieningen

Een bouwsteen is gedefinieerd in NORA[8] als: "Voorziening die deel uitmaakt van de infrastructuur van de e-overheid." In de praktijk kan je bij bouwstenen denken aan een systeem, een product, een standaard of een stelsel van afspraken.
De "Generieke Digitale Infrastructuur" (GDI) vormt de ruggengraat van de digitale overheid en omvat alle daarvoor benodigde bouwstenen. DigiD, MijnOverheid, Digipoort en gegevensuitwisseling met de basisregistraties zijn onmisbaar voor de digitale dienstverlening aan burgers en bedrijven. Deze oplossingen (afspraken, standaarden en voorzieningen) ondersteunen dienstverleners met een publieke taak bij de inrichting van hun digitale dienstverlening aan burgers en bedrijven en waar nodig bij hun onderlinge digitale samenwerking.

De Programmeringsraad GDI bepaalt welke bouwstenen tot de GDI worden gerekend. Daaruit blijkt dat er een verschil is tussen de lijst met bouwstenen van GDI en NORA: in de NORA zijn alle bouwstenen opgenomen die in de praktijk worden onderkend, hetgeen er méér zijn dan in de GDI. Ze hiervoor het overzicht van bouwstenen en voorzieningen[9]. Voor CN is het van belang zoveel mogelijk gebruik te maken van de bouwstenen en voorzieningen uit de GDI, zodat gesteund kan worden op de ontwikkel- en beheercapaciteit die hiervoor centraal beschikbaar is.

[8] https://www.noraonline.nl/wiki/Bouwstenen

[9] https://www.noraonline.nl/wiki/Bouwstenen_en_voorzieningen

3.5.9 Aansluittest

Voordat een webapplicatie gekoppeld kan worden aan DigiD is een pre-productie en daarna een productietest benodigd door Logius. Logius heeft hiervoor een checklist ontwikkeld. Ontwikkelaars van een webdienst gebruiken de checklist voor zelfcontrole. Logius controleert periodiek en bij elke nieuwe aansluiting of een aansluiting aan de criteria in deze checklist voldoet. De dienstaanbieder blijft altijd zelf verantwoordelijk voor de veilige en correcte werking van de systemen die op DigiD aansluiten. Logius heeft voor het aansluiten op DigiD een stappenplan ontwikkeld[10]

3.6 Netwerk laag

Op de netwerklaag is een randvoorwaarde dat inwoners toegang hebben tot een internet en op een beveiligde wijze kunnen communiceren met de overheidsorganisaties. Binnen deze laag vallen de netwerken, middleware, knooppunten en infrastructuur die nodig is om systemen te hosten en gegevens tussen die systemen uit te wisselen. Ook het netwerk van de overheidsorganisatie dient te voldoen aan de aansluitvoorwaarden en beveiligingseisen van het DigiD assessment. Voor elke organisatie moet besloten worden of de informatie-uitwisseling via het openbare internet kan, of moet het via (semi-)besloten netwerken of zelfs via een netwerk dat in eigen beheer is. Vervolgvraag betreft de standaarden die dan van toepassing zijn.

3.6.1 Jitter en latency

Jitter verwijst naar variaties in de vertraging van de pakketten tijdens de overdracht, terwijl latency de totale tijd aanduidt die het kost voor een pakket om van de bron naar de bestemming te reizen. Bij hoge latency kunnen gebruikers time-outs ervaren bij het laden van webpagina's of het uitvoeren van acties op de webdienst. Dit kan resulteren in foutmeldingen of onderbrekingen van de dienst. Het gebruik van DigiD kan hierdoor verslechterd of zelfs onmogelijk worden.

De fysieke afstand tussen de locatie van de webdienst (bijvoorbeeld Europees Nederland) en de gebruikers in Caribisch Nederland kan leiden tot aanzienlijke latency problemen. De tijd die nodig is voor datapakketten om heen en weer te reizen tussen de twee locaties kan aanzienlijk zijn, wat resulteert in verhoogde latentie. Ook kan het internetverkeer variëren afhankelijk van het tijdstip van de dag en andere factoren. Als er veel internetverkeer is tussen Nederland en Caribisch Nederland op een bepaald moment, kan dit leiden tot netwerkcongestie, wat de latency verder kan verhogen. Ten slotte kan het zijn dat de kwaliteit van de netwerkinfrastructuur in Caribisch Nederland kan variëren. Als de infrastructuur niet optimaal is, kan dit resulteren in hogere jitter en latency vanwege problemen zoals packet loss, congestie op lokale netwerken, of verouderde apparatuur.

Dit soort problemen kunnen dus voorkomen worden indien er (te veel) fysieke afstand zit tussen de hosting van de webdienst en de gebruiker. Heel concreet kan dit betekenen dat DigiD niet te gebruiken is in CN bij grote jitter en latency problemen. Als concreet voorbeeld hebben wij dit al

[10] https://www.logius.nl/domeinen/toegang/digid/aansluiten-wijzigen

ervaren tijdens ons onderzoek: het was veelal niet mogelijk organisaties toegang te geven tot onze teams omgeving, omdat het te lang duurde voordat de verificatiemail aangekomen was (en de toegestuurde toegangscode dus verlopen was).

Om deze problemen te verminderen kunnen maatregelen worden genomen, zoals het optimaliseren van de netwerkconfiguratie, het gebruik van content delivery networks (CDN's) om de distributie van content te optimaliseren, en het implementeren van caching om de belasting op de netwerkverbinding te verminderen. Maar ook het gebruik van geografisch verspreide datacenters kan helpen om de jitter en latency te verminderen door de afstand tussen de gebruikers en de server te verkorten. Dit brengt verdere afhankelijkheden met zich mee van de enkele lokale aanbieders, of maakt gebruik van datacenters in de Americas aantrekkelijker. Die laatste optie kan in het kader van wetgeving weer relevant zijn.

3.6.2 Internet standaarden

Door deze internetstandaarden toe te passen, kan DigiD een veilige en betrouwbare methode bieden voor het authenticeren en autoriseren van gebruikers. Ook bevordert het de interoperabiliteit. Enkele voorbeelden die wij kunnen noemen zijn:

- IPv6 en IPv4 bij het berichtenverkeer over het Internet
- HTTPS (Hypertext Transfer Protocol Secure) voor het versleutelen van de communicatie tussen de webbrowser en de DigiD-servers
- OAuth (Open Authorization) voor het autoriseren van toegang tot gebruikersgegevens
- SAML (Security Assertion Markup Language) voor single sign-on (SSO) functionaliteit
- TLS (Transport Layer Security) voor het beveiligen van de communicatie tussen de webbrowser en de DigiD-servers.

Het NCSC bericht regelmatig over het gewenste beveiligingsniveau bij webapplicaties[11]. Verder dienen de standaarden uit de Pas-toe-of-leg-Uit lijst[12] van het Forum Standaardisatie gevolgd te worden.

3.7 Beveiliging en privacy

Het aansluiten op DigiD brengt stevige beveiligings- en privacy maatregelen met zich mee. Hierdoor kan het lijken alsof het aansluiten op DigiD het doel is, en je als organisatie hierdoor investeringen moet doen in beveiliging en digitalisering. Dit lijkt ons onjuist: DigiD is niet het doel. Het wel of niet aanbieden van onlinediensten is het doel in CN. DigiD is de oplossing
Indien er in CN online diensten worden aangeboden, is een stevige investering nodig in de digitalisering en beveiliging. Een pre-check op de DigiD aansluiting is dus een hulpmiddel om die inspanning en investering inzichtelijk te maken.

[11] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties

[12] https://www.forumstandaardisatie.nl/open-standaarden/verplicht

3.7.1 Beveiligingseisen voor applicatie, platform en infrastructuur

Voor de veilige inrichting van de applicatie, het platform en de infrastructuur kunnen naast de BIO normen de NCSC-beveiligingsrichtlijnen voor webapplicaties[13] gebruikt worden. De DigiD assessment normen zijn afgeleid van de NCSC-richtlijnen. Voor verdere standaarden kan aangesloten worden op de standaarden van het Forum Standaardisatie.

3.7.2 Beveiliging van de toeleveringsketen

De toeleveringsketen verwijst naar supply chain management (SCM), waarbij een organisatie die een dienst levert, gebruik maakt van (deel)producten of diensten van toeleveranciers. Deze toeleverancier maakt daarbij vaak ook weer gebruik van andere toeleveranciers. Zo ontstaat er een toeleveringsketen. Volgens het Amerikaanse National Institute of Science and Technology (NIST) vindt naar schatting zo'n 80% van de cyberaanvallen wereldwijd plaats via supply chains. Voorbeelden die het Digital Trust center van digitale supply chain risico's aangeeft zijn een toeleverancier die niet meer levert als gevolg van een digitale aanval, een (IT-)dienstverlener is gehackt en hierdoor heeft de aanvaller mogelijk ook toegang tot jouw (digitale) systemen, er is een kritieke kwetsbaarheid ontdekt in één van de (digitale) producten of diensten die je gebruikt in je bedrijfsproces. Bij DigiD dienen van alle (sub-) serviceverleners auditverklaringen beschikbaar te zijn over het voldoen aan de DigiD normen. Dat geldt ook voor de grote cloudleveranciers Microsoft Azure, AWS en Google.

3.8 Beheer

3.8.1 ITIL, Scrum en DevOps

Webapplicaties moeten worden onderhouden, beheerd en beveiligd. Daarbij kan een onderscheid gemaakt worden in applicatiebeheer, databasemanagement, infrastructuurbeheer en beveiligingsbeheer. Voor het beheer van de webapplicatie kan aangesloten bij het ITIL framework. ITIL is een afkorting die staat voor Information Technology Infrastructure Library. ITIL bestaat uit een reeks best practices voor het leveren van efficiënte IT-ondersteuningsdiensten. De kern wordt gevormd door het afhandelen van incidenten, problemen en wijzigingen in de systemen. ITIL zorgt ervoor dat de taken in de organisatie hiërarchie zijn gerangschikt op het gebied van verantwoordelijkheid en bevoegdheid. Er zijn 26 ITIL-processen die onderdeel uitmaken van de vijf fasen van de ITIL service levenscyclus.

De ontwikkeling en vernieuwing van webapplicaties wordt steeds kortcyclischer en meer gebaseerd op het Agile Scrum aanpak. Scrum is een specifieke manier om resultaten te leveren. Het is een iteratieve, adaptieve en incrementele aanpak en een raamwerk voor het ontwikkelen en onderhouden van complexe producten, zoals webapplicaties. ITIL en Scrum kunnen goed samengaan. Zo is bijvoorbeeld het ITIL proces Wijzigingenbeheer ook een belangrijk onderwerp binnen Scrum. Iedere Sprint binnen een Scrumteam eindigt bijvoorbeeld met de Sprint Review

[13] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties

waarin de Product Owner de Sprint beoordeeld en goedkeurt. Tijdens serviceontwerp fungeert de Product Owner als poortwachter voor iedere user story (wijzigingenbeheer boven vereisten). Scrum kent drie belangrijke rollen: De Product Owner (namens de gebruiker), de Scrum Master (de facilitator) en het Ontwikkelteam (de professionals). ITIL kent vele rollen, in de context van Scrum zijn de rollen Service Owner, Change Manager, CAB en CSI Manager de meest relevante. Steeds meer doet DevOps de intrede bij ontwikkeling en beheer van webapplicaties. DevOps is een combinatie van ontwikkeling (Dev) en bedrijfsactiviteiten (Ops) en brengt mensen, processen en technologie samen. Bij DevOps worden rollen die voorheen in silo's waren geplaatst, zoals ontwikkeling, IT-activiteiten, kwaliteitsengineering en beveiliging, samen gecoördineerd en gebruikt om producten te maken. Bij DevOps wordt in principe Agile gewerkt. Dat wil zeggen in korte, iteratieve sprints, zodat er heel snel veel waarde voor de business wordt geleverd. Bij DevOps moet ook de aansturing in de organisatie daarop ingericht worden. Een belangrijke verbindende schakel daarbij is de product Owner.

4 AANBEVELINGEN

De analyse in dit rapport biedt inzicht in de risico's en maatregelen die genomen moeten worden om een succesvolle aansluiting op DigiD te borgen. Deze analyse omvat ook aanbevelingen die wij doen, deels op basis van de pre-checks, deels op basis van onze eigen ervaringen bij de implementatie van DigiD in Europees Nederland. Onderstaand een opsomming van deze aanbevelingen. Deze zijn niet geordend naar prioritering, omvang en belang.

4.1 Aanbevelingen algemeen

Programmatische aanpak aansluiting DigiD: Wij adviseren om de aansluiting op DigiD voor heel CN programmatisch aan te pakken. Deze programmatische aanpak moet borgen dat voortgang wordt gemaakt (en inzichtelijk wordt gemaakt) voor alle deelnemende organisaties in CN. Ook moet de onderlinge kennisdeling (best/worst practices) mogelijk maken rondom de planning, te ondernemen activiteiten en dergelijke. Ook de technische haalbaarheid van de verschillende trajecten worden hierdoor gemonitord en het maakt overkoepelende ketentesten mogelijk. Dit programma zou vervolgens ook kunnen voorzien in ondersteuning bij ondersteunende activiteiten waar eventueel geen capaciteit of middelen op CN voor beschikbaar zijn, zoals communicatie, adoptie en/of gebruikersondersteuning.

Praktische aandachtspunten voor de fase waar Caribisch Nederland nu in zit:

- Hou bij het ontwerp van het hele proces dus rekening met het voornemen om op DigiD aan te sluiten (m.a.w.: de inrichting van de webdienst);
- Plan ruimte in voor een 'invoeringsplan' voor de aansluiting op DigiD;
- Neem in de ontwerpfase van uw webdienst mee welk betrouwbaarheidsniveau gewenst / nodig is voor uw dienst;
- Voer een risicoanalyse uit op de voorgenomen nieuwe dienst, waarbij expliciet de risico's rondom de Beschikbaarheid, Integriteit en Vertrouwelijkheid (en Privacy) worden onderzocht en mitigerende maatregelen worden benoemd;
- In Europees Nederland verplicht de AVG het uitvoeren van een Data Protection Impact Assessment (DPIA) bij een nieuwe gegevensverwerking, bij samenwerkingsverbanden zoals tussen CN en Europees Nederland. Een DPIA kan u helpen om in duidelijk beeld te krijgen van wat de risico's zijn voor de rechten en vrijheden van betrokkenen. Een DPIA helpt hierbij en is ook een goed hulpmiddel om te beoordelen in hoeverre de huidige maatregelen voldoen en wat er nodig is om de risico's te verminderen.

Aansluittest: Voordat webapplicatie gekoppeld kan worden aan DigiD is een pre-productie en daarna een productietest benodigd door Logius. Logius heeft hiervoor een checklist ontwikkeld. Ontwikkelaars van een webdienst gebruiken de checklist voor zelfcontrole. Logius controleert periodiek en bij elke nieuwe aansluiting of een aansluiting aan de criteria in deze checklist voldoet. De dienstaanbieder blijft altijd zelf verantwoordelijk voor de veilige en correcte werking van de

systemen die op DigiD aansluiten. Logius heeft voor het aansluiten op DigiD een stappenplan ontwikkeld[14]

4.2 Aanbevelingen wet- en regelgeving

Uitwerking analyse wet- en regelgeving: Onze analyse omvatte enkele bevindingen omtrent de privacywetgeving, wetgeving rondom BSN, wetgeving rondom DigiD en wetgeving rondom doorgifte in CN.
De invoeringsdatum van de wetten is nog onduidelijk. Idealiter zouden bij de invoering van de wetten de privacy en informatiebeveiliging, alsmede alle randvoorwaarden voor een beveiligd gebruik van DigiD bij alle betrokken organisatiezijn ingevuld. Dit zal waarschijnlijk niet volledig haalbaar zijn. Daarom zal er voor de stelselhouder BRP en de architectuurkeuze een minimumniveau van gegevensbescherming en beveiliging moeten worden gedefinieerd dat voldoende waarborgen biedt en kan worden gebruikt als de wetten daadwerkelijk worden ingevoerd. Dit zou samen kunnen lopen met het verder groeien in volwassenheid van de het IT beheer en de IT security van de BES-organisaties. Hierbij lijkt een traject om ISO27001 gecertificeerd te worden voor zowel de lokale leverancier als de BES-organisaties een goede optie. Ook omdat de BIO2.0 die volgt uit de Cyberbeveiligingswet zwaar leunt op de ISO27001.

4.3 Aanbevelingen organisatie en processen

Kennis, beschikbaarheid en capaciteit: het is evident dat er meer capaciteit nodig is bij de organisaties op CN om een aansluiting op DigiD (en verdere digitalisering van dienstverlening) mogelijk te maken. Onze aanbeveling is om te overwegen of ook de beheertaak van bijvoorbeeld de DigiD aansluiting van de CN organisatie kan worden weggenomen. Het zou een nieuw concept van samenwerking met een leverancier zijn waarin alle verantwoordelijkheden rondom de aansluiting bij de leverancier worden belegd, en alleen de financiële en opdrachtgeversverantwoordelijkheid belegd blijft bij de CN organisatie.

Communicatie: Stel een standaard template (incl. handreikingen en voorbeelden) op van een communicatieplan dat de verschillende organisaties in CN kunnen gebruiken en specificeren. Borg in een project of programma de samenhang en uitvoering van deze plannen.

Prioriteer op winstgevende processen: Prioriteer de digitalisering van processen die de meeste 'winst' opleveren: in tijd en kosten. Dit zijn processen die zichtbaar zijn voor de organisaties én voor de burgers.

Adoptie: Stel mensen en middelen beschikbaar om de adoptie van 'digitaal zakendoen met de overheid' te vergroten. Maak gebruikersadoptie een kernpunt in alle projecten in CN, waarbij BZK eventueel kennis en capaciteit beschikbaar kan stellen. Met en op de eilanden. Adoptie van gebruikers neemt tijd in beslag. Ga dus in de planning niet uit van een uitrol of inbeheername van

[14] https://www.logius.nl/domeinen/toegang/digid/aansluiten-wijzigen

DigiD aansluiting per juli 2025, want dat is de inwerkingtreding van de wet voor BSN. Houdt in de planning rekening met de 'gewenning' aan en adoptie van dit nummer en DigiD als inlogmiddel.

Auditing: Jaarlijkse DigiD audits zijn verplicht. Elke organisatie moet hier capaciteit én geld voor vrijmaken. Deze jaarlijkse kosten moeten ook een plek op de begroting van de organisaties krijgen. Op dit moment zien wij voor zowel de kosten die dit met zich meebrengt als voor de interne capaciteit waar een claim op wordt gelegd een groot knelpunt.
Het heeft sterk de voorkeur zoveel mogelijk te steunen op de zogenaamde carve-out methode, waarbij zoveel mogelijk wordt gesteund op het rapport van de RE auditor van de serviceorganisatie, waarbij het merendeel van de DigiD normen afgedekt wordt. Bij de aansluithouder worden dan een 7-tal meer organisatorische normen getoetst.

Privacy-and-security-by-design applicatie en infrastructuur: Om de (toekomstige) e-Dienstverlening op CN duurzaam én bruikbaar te maken zijn de concepten 'privacy-by-design' en 'security-by-design' van essentieel belang. Veel onderzochte organisatie op CN zitten nog in de ontwerpfase van hun digitale processen of hebben de mogelijkheid deze nog in de kern aan te passen. Gebruik deze mogelijkheid om by-design alle digitale dienstverleningsprocessen naar de burger en ondernemer toe te ontwerpen. Aanvullende expertise en/of handreikingen kunnen gewenst zijn vanuit CN.

Business Continuity Management: Bij het ontwerpen van processen en digitalisering ervan is er een groot belang voor BCM. Neem dus standaard business continuïteit op en definieer vooraf maatregelen om continuïteitsrisico's te mitigeren.

4.4 Aanbevelingen informatie

Informatiehuishouding: Ondersteun de verschillende organisaties op CN met een basis opzet voor Informatiehuishouding (op Orde). Kijk of er op een meer generiek niveau alsnog concrete handreikingen, templates en opleidingsaanbod kan worden opgesteld en gedeeld met CN. De volwassenheid van de verschillende 'open op orde' programma's binnen BZK, andere departementen en CIO-Rijk kunnen handvaten bieden voor organisaties in CN.
Heel specifiek adviseren wij om de verbinding te leggen tussen Overheid op Orde en elke organisatie die binnen scope van dit onderzoek valt. Laat dit programma een opdracht uitvoeren waarin zij met een handreiking kunnen komen voor CN om hun informatiehuishouding op orde te krijgen.

4.5 Aanbevelingen beheer, beveiliging en privacy

Uitbesteding en regie: Besteed zo veel als mogelijk uit als organisatie als het gaat om de aansluiting op DigiD en leg expliciet verantwoordelijkheden voor de inrichting en beheer van het DigiD koppelvlak bij de leverancier. Focus zelf op een sterke regievoeringstaak.
Het wordt voor individuele organisaties steeds lastiger om de juiste beveiligings- en verantwoordingseisen te stellen aan ICT-leveranciers. Hiervoor is het nodig dat meer centrale kaders worden meegegeven en ondersteuning wordt gegeven. Onze aanbeveling is dat BZK zou

moeten overwegen ondersteuning te bieden bij de aansturing van leveranciers door de CN organisaties.

Overweeg een vergaande vorm van uitbesteden: overweeg een nieuw model voor de uitbesteding, waarin de opdrachtgever in CN alleen de opdracht geeft en betaalt en waarin alle beheertaken bij de leverancier (incl. de activiteiten conform de governance-normen van de DigiD assessment) worden belegd.

Clouddienstverlening: Een verantwoord cloudbeleid begint met een gestructureerde aanpak, opgebouwd uit vier belangrijke stappen. Eerst is het essentieel om risicoprofielen op te stellen. Dit houdt in dat er een impactanalyse wordt uitgevoerd om de gevoeligheid van data te beoordelen en mogelijke risico's in kaart te brengen. Vervolgens moet data worden geclassificeerd. Door gegevens onder te verdelen in categorieën zoals vertrouwelijk, intern of publiek, kan elk type data op een passende manier worden behandeld. De derde stap is het kiezen van de juiste cloud. Op basis van de classificatie wordt bepaald of data het beste thuishoort in een publieke, private of hybride cloud, of dat een on-premise oplossing geschikter is.

Contractafspraken: In veel gevallen zal sprake zijn van uitbesteding van de IT-dienstverlening aan serviceorganisaties. Goede contractafspraken zijn daarbij essentieel. Hierin kan BZK ondersteunen en deze organisaties wellicht voorzien van standaarden, templates en eventueel capaciteit. Een goed hulpmiddel is de ICO-Wizard.