Richtlijnen en stappenplan voor de invoering van e-governancesystemen in Suriname

Datum: 9 oktober 2020
Auteur: drs. P.R. Mehilal
Versie: 0.1

Inhoudsopgave

Voorwoord

We ervaren op dit moment een wereldwijde digitale revolutie met dezelfde omvang als van de industriële revolutie in de 19e eeuw. Dit biedt volop kansen en e-governancesystemen zijn daarvan een voorbeeld. Suriname kan profiteren van deze groei en kansen, met meer dan 380.000 internetgebruikers waarvan 90% via smartphones. Het potentieel van deze digitale technologieën wordt in Suriname echter nog niet volledig benut: e-governancesystemen zijn onvoldoende ontwikkeld. Met de e-Gov-organisatie lopen we die achterstand in.

Huidige benadering is ontoereikend

Een duurzame ontwikkeling hiervan en inclusieve groei zijn pas mogelijk als we digitale technologieën inzetten op basis van informatie- en communicatietechnologieën (ICT) én we hieraan diensten koppelen die deze technologieën ondersteunen. We zien dat veel private en parastatale instellingen de digitale ontwikkelingen omarmd hebben maar dat de overheid nog worstelt met de digitale revolutie.

Toch zijn er binnen de overheid tussen 2012 en nu wel degelijk stappen ondernomen. Denk aan deliverables als elektronische identiteit (e-ID), e-Visa, Safe City en e-Rijbewijs. Maar doordat de technische architectuur niet passend is gemaakt voor e-governance en veel software is aangekocht van derden is er geen coherent geheel ontstaan. Daarnaast zijn er hoge bedragen betaald voor maatwerksoftware en is er sprake van een vendor lock-in. Naarmate de e-services zullen toenemen in aantal en complexiteit is de huidige benadering qua ontwerp en onderhoud steeds minder toereikend.

Kansen van e-governancesystemen

De digitale overheid is een verlengstuk van de traditionele overheid. Waar mogelijk wordt daarmee de zelfredzaamheid van burgers, het bedrijfsleven én de overheid vergroot. Door te informeren en door 24/7 toegang te geven tot publieke diensten via selfservice-internetapplicaties (e-services).

Een digitale overheid biedt unieke mogelijkheden om ICT te gebruiken voor economische groei, productiviteitsverhoging en betere dienstverlening van de overheid. Impliciet voorziet een digitale overheid ook in elementen om corruptie en witwassen te reduceren. Deze vooruitgang zal het land meer aantrekkelijk maken voor business, waaronder buitenlandse investeringen.

Wat is daarvoor nodig?

Dit kan alleen als de overheid zich hiervoor inzet door zo goed mogelijk gebruik te maken van digitale technologieën en op te treden als facilitator, enabler en regelgever, waarbij alle belanghebbenden worden betrokken door middel van een transparante samenwerking. Daarbij staat steeds voorop: de burger staat centraal, niet de techniek.

De huidige e-Gov-organisatie zal de Surinaamse overheid ondersteunen om zo sterke, faciliterende e-governancesystemen te creëren. Daarbij hoort ook de implementatie van e-governance. E-services moeten deel uitmaken van de algehele herziening van de verordening: want alleen onnodig complexe of niet-transparante services digitaal maken zal niet alle problemen oplossen. Het moet dus een alomvattend proces zijn, waarin naast technologie ook organisatorische en regelgevende kwesties worden meegenomen. E-governance en de reguliere overheid zijn met

elkaar verbonden. En daarom zijn steun van toppolitiek leiderschap en coördinatie op hoog niveau essentieel.

Doel van e-Gov

Het doel van de e-Gov-organisatie is om te komen tot een excellente e-governance voor Suriname. Veel landen hebben in de afgelopen drie decennia enorme vooruitgang geboekt bij de implementatie van hun e-governance. Estland loopt daarbij voorop en richtte in samenwerking met andere partijen de consultancyorganisatie e-Governance Acadamy (eGA) op, om hun kennis en ervaringen te delen. e-Gov Suriname zal zoveel mogelijk gebruikmaken van best practices in de wereld (met name Estland en instanties als eGA) zodat Suriname snel de achterstanden in kan lopen.

Inhoud van dit document

In dit document zetten we uiteen welke stappen nodig zijn om e-governance te bereiken.
Die stappen zijn afhankelijk van de volgende factoren:

- de ICT-beschikbaarheid en het ICT-gebruik
- de huidige status van e-governance
- de structuur van en keuzes voor overheidsbeleid in het algemeen

Doelstelling en scope van het document

Dit document heeft twee doelen:

1) Komen tot een analyse van de huidige status van e-governance in Suriname (matrix).
2) Komen tot een plan van aanpak (Roadmap to Excellence).

1 Introductie

De overheid heeft een faciliterende rol bij de totstandbrenging van een moderne informatiemaatschappij waarbij digitale technologie optimaal ingezet wordt ten dienste van de burger. Ze fungeert als enabler en zorgt voor wet- en regelgeving. Digitale technologieën die afhankelijk zijn van ICT en de diensten die deze technologieën ondersteunen, maken deze duurzame ontwikkeling en inclusieve groei mogelijk.

Terminologie

Bij deze moderne informatiemaatschappij horen een digitale overheid (e-government) en een digitaal beleid (e-governance). De digitale overheid wordt in Suriname geïmplementeerd door e-Gov Suriname.

De precieze betekenis van de term e-government staat in veel opzichten nog in de kinderschoenen in veel landen, zo ook in Suriname. Er is geen universele benadering voor e-government en dit laat ruimte voor verschillende interpretaties. Wij volgen de definitie van de Wereldbank:

> E-government verwijst naar het gebruik door overheidsinstanties van informatie-technologieën (zoals Wide Area Networks, het internet en mobiele computing) die de mogelijkheid hebben om relaties met burgers, bedrijven en andere overheidswapens te transformeren. Deze technologieën kunnen verschillende doelen dienen: een betere levering van overheidsdiensten aan burgers, verbeterde interacties met het bedrijfsleven en de industrie, empowerment van burgers door toegang tot informatie of efficiënter overheidsbeheer. De daaruit voortvloeiende voordelen kunnen minder corruptie, meer transparantie, meer gemak, omzetgroei en/of kostenbesparingen zijn.

Overheid transparanter en toegankelijker voor iedereen

Connectiviteit en betaalbaarheid van ICT zijn relevante zorgen. Een gebrek aan toegang tot ICT op scholen, in het binnenland of zelfs bij overheidsinstellingen verhindert de ontwikkeling van e-services. Gezien de beperkte (ICT-)resources van de overheid is de betrokkenheid van alle belanghebbenden door middel van transparante samenwerking van essentieel belang. Op deze manier benutten we de voordelen van digitale technologieën voor de verbetering van het leven van alle mensen: arm en rijk, jong en oud, wonend in stad en binnenland. Voor al deze mensen wordt de overheid zo toegankelijker en transparanter.

Succesvolle implementatie van e-governance

De implementatie van e-governance moet een alomvattend proces zijn. Het is niet primair gericht op technologie, maar is een proces waarin organisatorische en regelgevende kwesties worden aangepakt. Anders ontbreekt het draagvlak, wordt het e-Gov (opnieuw) ineffectief en ontstaan er problemen als: digitale gegevens en transacties die geen juridische betekenis hebben, gegevens die niet worden hergebruikt, service delivery-processen die worden gekopieerd uit het papieren tijdperk zonder optimalisatieslagen, computers die als typemachine worden gebruikt (er zijn zelfs gevallen bekend waarbij online aanvraagformulieren uitgeprint werden waarna gegevens handmatig werden ingevuld).

Onderdeel van het bestuur

e-Gov moet zorgdragen voor functionele technologie die op een duurzame manier in de overheidsprocessen wordt geïntegreerd, met de juiste institutionele en wetgevende steun. E-governance wordt daardoor een integraal en ondeelbaar onderdeel van het bestuur van Suriname, waarbij digitale technologieën worden gebruikt om het bestuur te verbeteren.

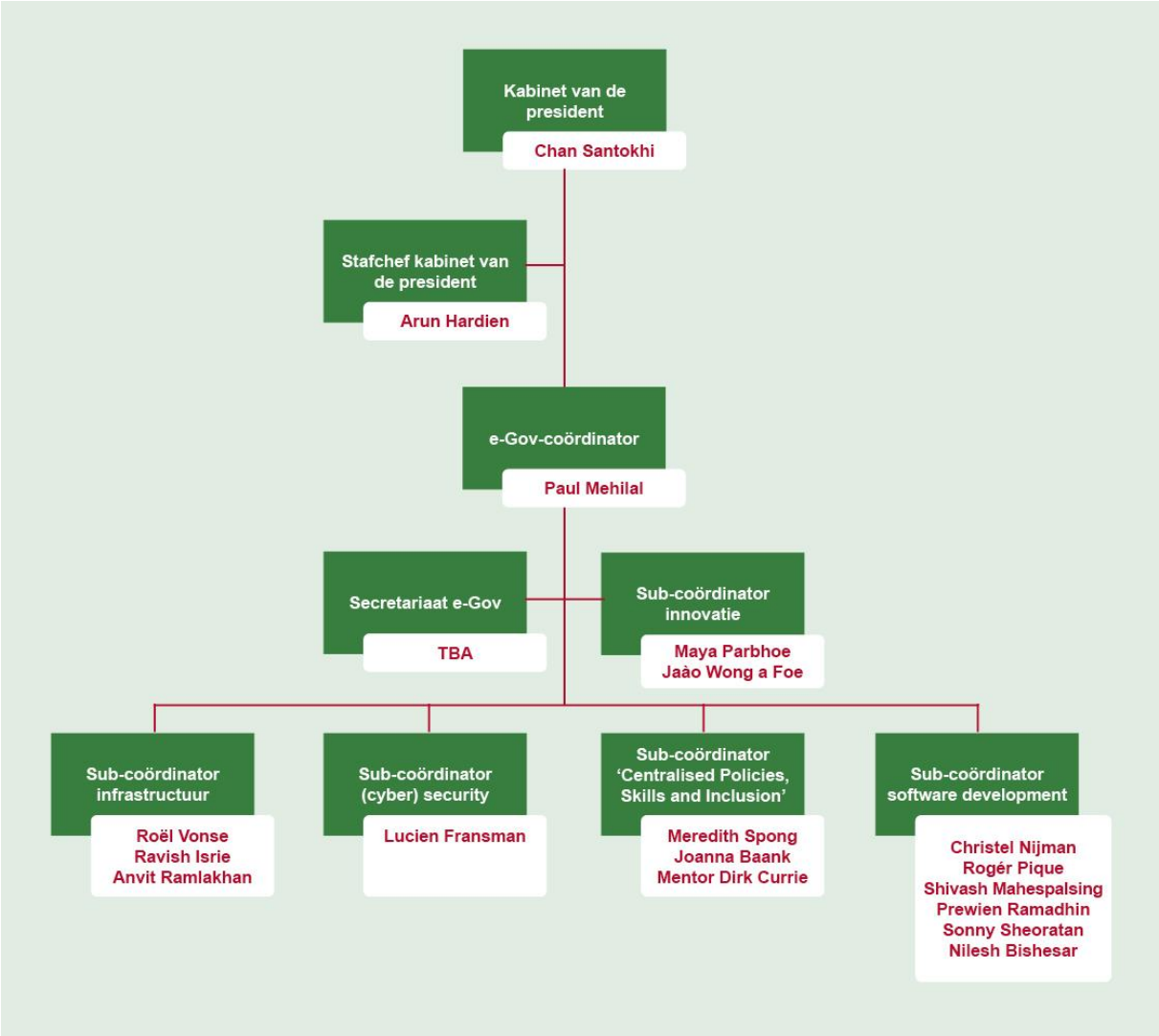
Onmisbaar: steun en coördinatie

Daarvoor is er behoefte aan steun van toppolitiek leiderschap aan coördinatie op hoog niveau tussen overheidsdiensten en andere actoren. Dergelijke interventies ondersteunen het creëren van een duurzaam sociaal-economisch klimaat. Dat op zijn beurt de oprichting van nieuwe vormen van ondernemerschap en het maatschappelijk middenveld ondersteunt, bureaucratische barrières en scheidslijnen vermindert en inclusiviteit ondersteunt. Zonder dergelijke steun zal het niet mogelijk zijn om duurzaam e-governance in te voeren.

1.1 Over het e-Gov-team

Het huidige e-Gov-team bestaat uit één technische man, één coördinator en één processpecialist. Het technische deel is voor een digitale overheid te summier en governance wise erg riskant. Ook de programmeertak ontbreekt volledig.

Om te komen tot een volwaardig e-Gov-team (e-Gov SR 2020-2025) is er in Suriname gezocht naar de meest geschikte personen binnen hun vakgebied. Personen met een hart voor Suriname en met de gezamenlijke doelstelling: Suriname technologisch hoogwaardig aan laten sluiten bij de rest van de wereld. Wat we voor ogen hebben: een volwassen zelfsturend team dat het masterplan executeert. De teamleden en hun functie zijn weergegeven in onderstaand organogram:


Kabinet van de president
Chan Santokhi
Stafchef kabinet van de president
Arun Hardien
e-Gov-coördinator
Paul Mehilal
Secretariaat e-Gov
TBA
Sub-coördinator innovatie
Maya Parbhoe
Jaào Wong a Foe
Sub-coördinator infrastructuur
Roël Vonse
Ravish Isrie
Anvit Ramlakhan
Sub-coördinator (cyber) security
Lucien Fransman
Sub-coördinator 'Centralised Policies, Skills and Inclusion'
Meredith Spong
Joanna Baank
Mentor Dirk Currie
Sub-coördinator software development
Christel Nijman
Rogér Pique
Shivash Mahespalsing
Prewien Ramadhin
Sonny Sheoratan
Nilesh Bishesar

1.2 Introductie: basiselementen voor succesvolle e-governance

In hoofdstuk 2 schetsen we de huidige status van e-governance in Suriname. Dit doen we aan de hand van de belangrijkste elementen van e-governance. Die elementen zijn in twee secties verdeeld, die elkaar aanvullen:

1. Digitale elementen

Deze elementen zijn direct verbonden met technologie. Dit zijn:

- overheidsportalen
- digitale databases en digitalisering van records
- veilige uitwisseling van data
- veilige digitale identiteit en digitale handtekening
- infrastructurele kwesties
- digitale dienstverlening (e-services) per sector.

2. Analoge elementen

Deze elementen ondersteunen de technologie met regelgeving, organisatie, financiering, verandermanagement, bewustmaking en politieke wil. Dit zijn:

- internationale kaders
- wettelijke kaders (wet- en regelgeving die digitale transacties mogelijk maakt en de privacy beschermen)
- coördinerende instellingen
- politieke wil en verandermanagement
- toegang tot digitale diensten (e-services inclusion)
- bewustwording stimuleren.

Oplossingen per sector

De bovengenoemde digitale elementen dienen als basis voor e-government. Daarnaast is er de mogelijkheid om een eindeloos aantal oplossingen per sector te creëren, die diensten op verschillende gebieden mogelijk kunnen maken: onderwijs, gezondheidszorg, belastingen, recht, economische ontwikkeling, landbouw, vervoer, etc.
Deze sectorale oplossingen kunnen worden ondersteund met bredere programma's, zoals 'ICT voor scholen', 'Mobiele oplossingen voor de agrosector' of 'Modernisering van openbaar vervoer'.

1.3 Introductie: implementatiematrix en roadmap

Op basis van de analyse van de huidige situatie in Suriname, presenteren we in hoofdstuk 3 een implementatiematrix. Deze matrix onderscheidt de stappen die leiden tot de volledige implementatie van e-governancesystemen. Het is dus een instrument om het huidige niveau van e-government in Suriname aan te geven. In de roadmap (hoofdstuk 4) bepalen we vervolgens wat de belangrijkste elementen zijn die aangepakt moeten worden om de e-governance naar een hoger niveau te brengen.

De exacte volgorde waarin deze punten daarna aangepakt worden, is afhankelijk van het huidige niveau van e-governance in Suriname. De matrix en roadmap zijn niet in beton gegoten. Het zijn instrumenten die Suriname moeten ondersteunen om te komen tot excellente e-governance.

2 Voorwaarden voor een succesvolle e-governance

Dit hoofdstuk geeft een overzicht van de belangrijkste elementen voor succesvolle e-governance, te beginnen met de elementen die specifiek digitaal van aard zijn.

2.1 Digitale basiselementen

2.1.1 Overheidsportaal, digitale databases en veilige uitwisseling van gegevens

De overheidsportalen (bijvoorbeeld Gov.sr, waarschijnlijk naar Nederlands model) zijn de centrale informatiepoorten naar alle online en offline overheidsdiensten.

Technische opbouw overheidsportals

Vanuit technisch oogpunt zijn overheidsportals meestal verdeeld in twee lagen: de presentatielaag en de serviceslaag. De presentatielaag biedt visuele informatie, de serviceslaag maakt het mogelijk om services te ontwikkelen. Dat zijn toepassingssjablonen, gegevensquery's en indiening. Als deze twee lagen goed gescheiden zijn, hebben wijzigingen in de visuele laag (nieuwe visuele inzichten, wijzigingen in de teksten, etc.) geen invloed op de technische mogelijkheden van het portaal.

Gecentraliseerd of decentraal?

Afhankelijk van de structuur kunnen we kiezen voor alleen gecentraliseerde overheidsportalen (Gov.sr), voor decentrale portalen per ministerie of zelfs regionale of districtsportalen. Decentraliseren heeft als voordeel dat dat proefprojecten in een kleiner deelgebied uitgevoerd kunnen worden en resultaten sneller zichtbaar zijn.

Waarde van offline informatie

De waarde van offline informatie (tekstuele informatie, zonder interactieve diensten) wordt vaak onderschat. De informatie over de diensten moet duidelijk, goed georganiseerd en goed gepresenteerd zijn. Zodat mensen begrijpen hoe de overheid hen kan helpen in verschillende situaties, zoals registratie van geboorte, trouwen, het vinden van een baan of een bezoek aan een arts.

Mogelijke verbeteringen

Overheidsportalen worden toegankelijker en gebruiksvriendelijker door harmonisatie van verklarende teksten in de webpagina's van verschillende instellingen, goed ontwerp met een coherente lay-out (ook bij verschillende ministeries) of ontwikkeling van mobile first-sites. Idealiter wordt de inhoud van de portals up-to-date gehouden door het desbetreffende departement zelf, via toegang tot het contentmanagementsysteem.

Een andere verbetering is de toevoeging van een mobile messaging gateway, die de mogelijkheid biedt om korte (sms-)berichten te versturen naar mobiele netwerken van de overheidsportaal. Een groot aantal mensen heeft een mobiele telefoon, dus dit kan een handige en snelle methode zijn om mensen te informeren. Berichten kunnen worden gebruikt voor individuele berichten (herinnering om een rijbewijs af te halen) of bulkberichten (om de bevolking in een bepaald gebied voor natuurrampen te waarschuwen). In Nederland is een voorbeeld van zo'n bulkbericht de AMBER Alert, die wordt uitgestuurd bij kindervermissingen en -ontvoeringen.

Voor diensten is het ten slotte belangrijk om ook een betalingsgateway te ontwikkelen. Daarmee kunnen overheden online aanvraagformulieren ontvangen, samen met de betalingen voor de servicekosten van de overheid. Met hyperlinks kan zo doorgeklikt worden naar selfserviceapplicaties van e-Gov (en eventueel derde partijen, in andere woorden: e-banking).

Elektronische databases

Bij het creëren van e-governance zijn elektronische databases de ruggengraat. In de afgelopen decennia heeft de Surinaamse overheid daarom grote delen van de gegevens van papier naar digitaal formaat omgezet of zijn ze bezig dit te doen.

Elektronische databases zijn een voorwaarde voor veel e-governancediensten. Belangrijke databases (hoofdregisters) omvatten normaal gesproken het bevolkingsregister (CBB), het onroerendgoedregister (Kadaster) en het bedrijfsregister (KKF). Dit zijn belangrijke databases die veel geraadpleegd worden bij e-services.

Noodzakelijk: interoperabiliteit

Veel e-services zullen gegevens uit verschillende databases gebruiken. Interoperabiliteit van databases is daarom van belang en dit kan aanzienlijke efficiëntieverbeteringen opleveren. Interoperabiliteit van de Surinaamse databronnen is vooralsnog niet geborgd maar dat kan worden opgelost door adapters te bouwen.

Minder administratieve lasten en minder risico's

Moderne gegevensverwerking biedt de mogelijkheden om een 'slechts eenmalig' principe te hanteren. Dat betekent dat overheden slechts één keer om informatie kunnen vragen, waarna de overheidsinstanties de gegevens moeten delen indien nodig. Wat dit in de praktijk betekent, is bijvoorbeeld dat de overheid niet dezelfde gegevens (zoals een adres) in verschillende databanken kan opnemen, maar alleen bij bijvoorbeeld de burgerlijke stand. Andere overheidseenheden hoeven dus niet meer iemand om gegevens te vragen, maar krijgen zelf het adres van dit register. Dit vermindert de administratieve lasten voor particulieren en bedrijven en voorkomt risico's in verband met gegevensduplicatie en de kwaliteit van data.

Secure data exchange

Om die data veilig uit te wisselen, is een secure data exchangeoplossing via een Enterprise Service Bus (ESB) nodig (zie 2.1.2), die conformeert aan de internationale privacy- en securityregels. Die oplossing voor data-uitwisseling moet aan verschillende criteria voldoen:

1) Zowel de afzender als de ontvanger van de gegevens moeten worden geregistreerd en geverifieerd, wat betekent dat deze via overeengekomen procedures en mechanismen worden geïdentificeerd.
2) De vertrouwelijkheid van de uitgewisselde gegevens moet met versleuteling worden gewaarborgd.
3) De gegevenstransacties moeten worden 'getimestamped' (in dit geval door de Republiek Suriname), zodat later kan worden nagegaan of op een bepaald moment de gegevens in de database zijn gepresenteerd.
4) Elektronische dossiers moeten worden geregistreerd en gearchiveerd om een juridisch controlespoor te garanderen,
5) Er moet een solide juridische status zijn voor gegevensverzoeken en -antwoorden.

Samen met veilige gegevensuitwisseling moet het beheer van digitale informatiemiddelen worden georganiseerd. Met inbegrip van de juiste informatie over de databases, diensten en gebruikersrechten (metadata).

ESB ontbreekt nog

Er is momenteel geen ESB-architectuur. Hierdoor worden applicaties rechtstreeks tegen de databronnen van instanties aan gebouwd. Dat is geen houdbare situatie: het aantal databronnen/entiteiten zal in de toekomst enorm toenemen en applicaties zullen databronnen van verschillende instanties nodig hebben. Het onderhoud van de applicaties wordt daarom ondoenlijk. Verder is het onderhevig aan politieke willekeur per databron.

Succesvol digitaliseren: meer dan technologie

Digitalisering moet niet in een vacuüm worden ingevoerd, maar als onderdeel van een reeks structurele maatregelen ter verbetering van belangrijke databases. Verbetering van de integriteit, effectiviteit en volledigheid van dergelijke registers is kardinaal en zeker niet alleen een technologiekwestie.

De redenen voor onvolledige of gebrekkige databases zijn talrijk. Culturele kwesties, gebrek aan toegankelijke contactpunten met autoriteiten of angst voor onvoldoende gegevensbescherming (big brother, privacy) zijn een aantal factoren.

2.1.2 Werking van een ESB

ESB in het kort

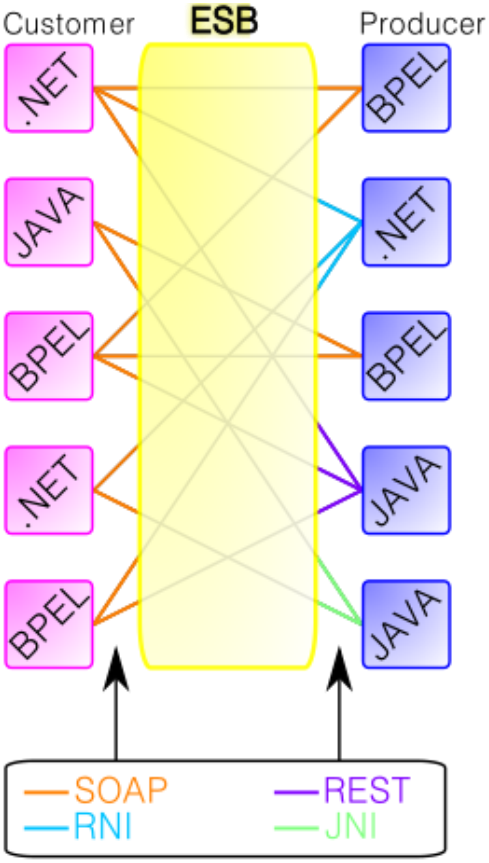
De kenmerken van een ESB op een rij. Een ESB:

- 'bemiddelt' tussen serviceaanvragers en serviceaanbieders.
- zorgt voor standaardisatie van de communicatie met serviceaanvragers.
- handelt de transformatie van gegevens af tussen aanvrager en aanbieder.
- orkestreert de afhandeling van aanvragen en het doorsturen naar aanbieders.
- monitort de serviceaanvragen en rapporteert over het gebruik van aanvragen.
- zorgt voor beveiliging van het transport.

Eenvoudige communicatie

Een ESB is een architecturale softwareconstructie ('pattern'). Hiermee wordt de communicatie tussen de afnemers van diensten ('service') en aanbieders vereenvoudigd. De ESB biedt de aanvrager de interface die met hem is afgesproken. Dit kan een webservice zijn, of bijvoorbeeld een SMTP-(e-mail)interface.

Met de aanbieder wordt er via de interface gecommuniceerd die hij heeft uitgekozen. Zo kan het zijn dat een aanvrager van een dienst op compleet andere wijze met de ESB communiceert dan de ESB met de aanbieder. Onderstaande figuur geeft dit schematisch weer:



De customer-services kunnen allemaal op dezelfde manier communiceren met de ESB. De ESB vertaalt het bericht naar het juiste berichttype en stuurt het door naar de juiste producer-service.

Standaardisering

De wijze waarop serviceaanvragers en -aanbieders met elkaar communiceren wordt gestandaardiseerd door de ESB-component toe te voegen aan een softwarearchitectuur. Er is immers alleen een afspraak tussen de ESB en de aanvragers die van dezelfde service gebruikmaken. De taak van de ESB is: alle informatie die binnenkomt en behoort bij een aanvraag op de juiste wijze vertalen (transformeren) naar het formaat dat de serviceaanbieder verwacht.

Orkestratie

De ESB-component is verantwoordelijk voor de aflevering van een aanvraag op de juiste plaats: bij de juiste aanbieder(s) van services. Ook zorgt de ESB voor de foutafhandeling en eventuele prioritering van aanvragen: welke wordt als eerste afgehandeld? Dit geheel van aanvraagafhandeling en controle noemen we ‘orkestratie van serviceaanvragen’.

Beveiliging

Een volgend aspect van de ESB-component is de beveiliging van aanvragen en de gegevens die erbij horen. Naast de beveiliging van het communicatiekanaal (zoals een beveiligde webservice via HTTPS) gaat het ook om: wie (welke gebruiker of rol) mag een service aanvragen?

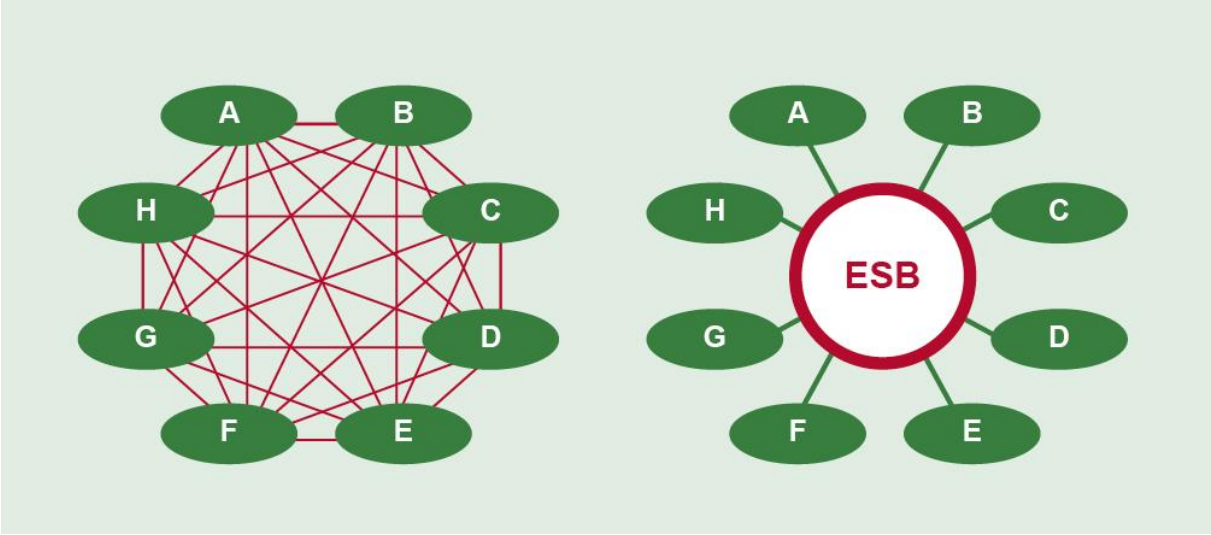
Monitoring

Een laatste veelvoorkomende taak die we uitlichten is de monitoring van aanvragen en het bijhouden van bijbehorende statistische gegevens. Zoals: hoe vaak wordt een service aangeroepen, hoe vaak gaat dit fout of juist goed en hoelang duurt een aanvraag? Met deze gegevens kan later gerapporteerd worden. Ook is direct een reactie mogelijk: als binnen de orkestratie van een aanvraag een service aangeroepen wordt die een foutafhandeling uitvoert. Onder monitoring valt eveneens de controle op vooraf gestelde Service Level Agreements (SLA) voor een service, inclusief acties als een SLA niet gehaald wordt.

Waarom een ESB?

Wat zijn de redenen om een ESB te gebruiken en welke voordelen levert het op? Vijf punten:

1) Compleet loskoppelen of gedeeltelijk ontkoppelen (loosely coupled) van serviceaanbieders en serviceaanvragers. → Aanvragers communiceren met de ESB en niet direct met de aanbieder.
2) Versimpelen en standaardiseren van interfaces tussen aanbieders en aanvragers → Een generieke manier van communiceren met de ESB. De ESB zorgt voor communicatie met de onderliggende systemen.
3) Het stimuleren van hergebruik → Services zijn beschikbaar op een centraal niveau (binnen de ESB) en zijn gemakkelijk toegankelijk. Zo kunnen ze sneller worden toegepast in andere systemen.
4) Centrale en generieke manier van servicemonitoring → Op een generieke manier kunnen binnen de ESB services gemonitord worden en gecontroleerd op afgesproken SLA's. De monitoring hoeft niet meer bij iedere serviceaanbieder te worden ingericht, dit gebeurt centraal in de ESB.
5) Reduceren van 'time-to-market' door hergebruik en minder implementatietijd → Hierdoor kunnen we sneller inspringen op veranderingen.



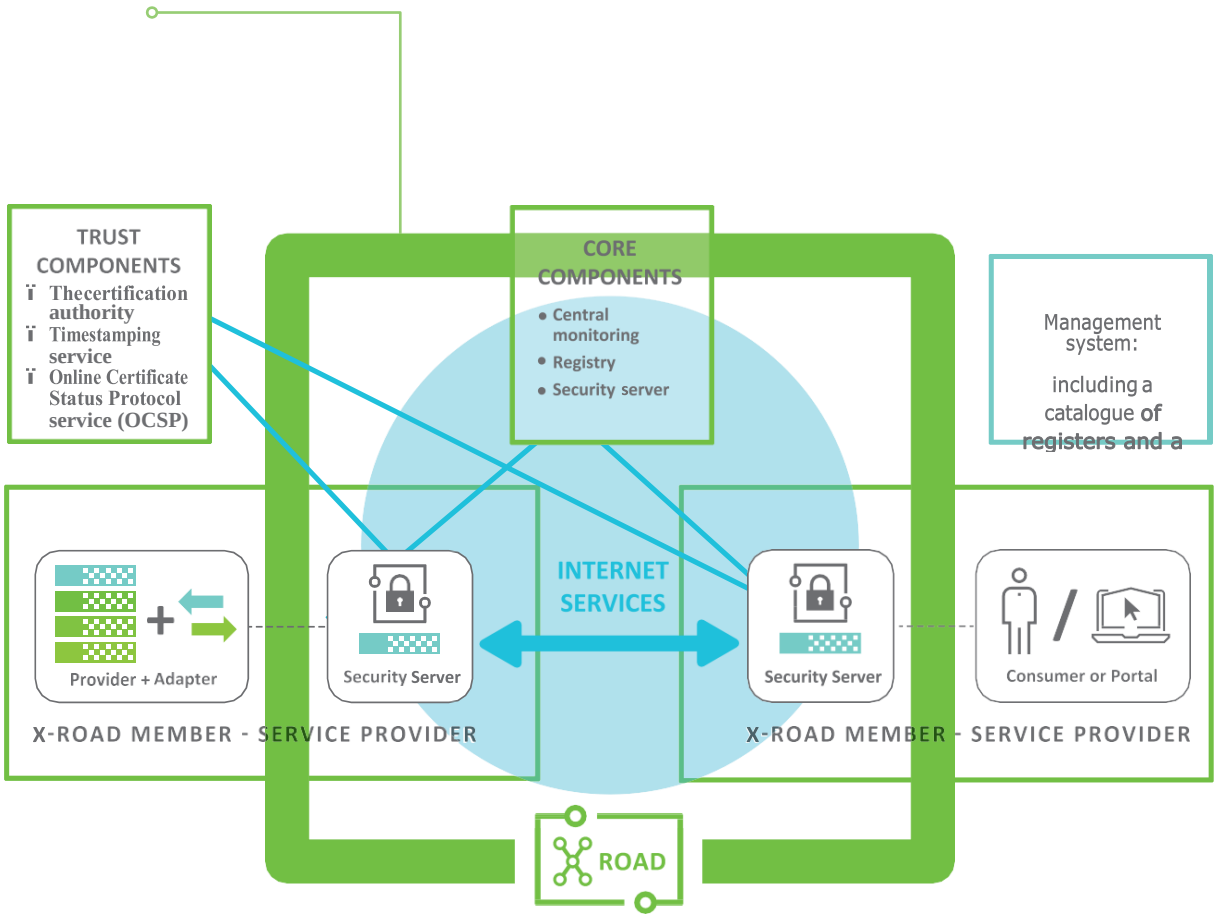
Bovenstaande figuur verduidelijkt nog eens de eerste twee punten van de lijst hierboven: zonder een ESB hebben aanvragers en aanbieders zogenaamde 'point-to-point'-verbindingen. Deze lopen kriskras. Met een ESB hebben aanvragers één gestandaardiseerde interface met de ESB. Aanvragen worden dan via de ESB afgehandeld.

Conclusie: ESB is onmisbaar

Concluderend kunnen we zeggen: een ESB is onmisbaar als 'enabler' in een omgeving waar een service oriented architecture wordt ontwikkeld. De ESB zorgt voor de juiste infrastructuur: waarop op hoger niveau, vanuit de functionele gedachte (business) wordt gekeken naar processen en procesverbetering binnen een organisatie.

Estland als voorbeeld

De ESB-architectuur in Estland ziet er als volgt uit:



2.1.3 Veilige digitale identiteit en digitale handtekening

Suriname is in 2012 begonnen met de implementatie van e-governance. Helaas ontbrak het aan structuur in de aanpak. In eerste aanleg is men begonnen met eenvoudige websites met overheidsinformatie (static, offline). Voor de nabije toekomst ligt de focus van het huidige e-Gov-team op geïntegreerde diensten die interactie met burgers toestaan, zoals het online indienen van documenten of het vernieuwen van het rijbewijs of paspoort (dynamic, online).

Volledige database creëren

Zodra e-overheidsdiensten interactie voorstaan, speelt het belang van een veilig identificatiesysteem een rol. Suriname is begonnen met de invoering van een elektronische identiteit (e-ID) maar de landelijke penetratie is niet 100% waardoor de onderliggende database niet volledig is. Er zijn hiervoor twee oplossingen. De CBB-database zou na opschoning samengevoegd kunnen worden met de e-ID-database om te komen tot een volledige database. Of er kan gekozen worden voor een sterfhuisconstructie van de CBB-gegevens naarmate de e-ID-database zich vult.

Elektronische functies e-ID

Als e-ID slechts een reeks getallen is op een pasje, zonder elektronische functies of als er door verschillende instanties een veelheid aan e-ID's uitgedeeld worden, dan gaat de kracht van een e-ID verloren. Ook het uitgangspunt dat de burger zijn gegevens eenmaal aan hoeft te leveren wordt daardoor tenietgedaan. De lange rijen voor (overheids)instanties zoals het CBB, en dus het verlies aan arbeidsproductiviteit, worden daarmee niet weggewerkt.

Veilige digitale identiteit en handtekening

Voor het gebruik van digitale diensten is het essentieel om een digitale identiteit en een digitale handtekening te hebben die veilig genoeg zijn om transacties juridische waarde te laten hebben. Dergelijke identiteiten moeten veilig verbonden zijn met de fysieke identiteit en vertrouwd worden door de overheid. Het geëigende orgaan om e-ID uit te geven en te beheren is het Ministerie van Binnenlandse Zaken (BiZa). BiZa zorgt voor geauthentiseerde en transparante communicatie tussen de overheid, de burger en het bedrijfsleven.

Identificatiemethode met kaart

De identificatiemethode kan een identiteitskaart bevatten, zoals een smartcard die een voor machines leesbare chip bevat, die niet alleen de non-privacygegevensvelden bevatten die zichtbaar zijn op de kaart (inclusief de foto van de persoon), maar ook gegevensvelden die privacygevoelig zijn en alleen leesbaar voor bepaalde overheidsfunctionarissen. Een correcte digitale identiteit voorziet in veilig online gebruik, voor verschillende transacties.

Vereisten voor een identiteitskaart

Kaarten dragen een digitale identiteit op een chip – een set van gegevens en software, beschermd met cryptografische middelen. Om deze kaarten te gebruiken, moeten gebruikers kaartlezers in hun computer hebben (of die via USB aansluiten) én speciale shareware (software, meestal gratis en openbaar beschikbaar) hebben. De kaart draagt een specifiek stuk geïndividualiseerde software (de sleutel). Gebruikers voeren een pincode in om de kaart te gebruiken, meestal in combinatie met een tweede nummer om een digitale handtekening te geven.

Mobiele ID

In Suriname hebben niet alle mensen toegang tot computers, terwijl de toegangsgraad tot mobiele telefoons en mobiele netwerken zeer hoog is. Er zijn mogelijkheden om een mobiele ID te gebruiken die is gekoppeld aan subscriber identification module-kaarten, de simkaart. Een soortgelijke set van gegevens en software, gebruikt in smartcards en beschermd met cryptografische middelen, wordt overgebracht naar de simkaart van de gebruiker van de mobiele telefoon.

Overeenstemming met andere landen

Technologieën voor veilige digitale identiteiten en handtekeningen kunnen variëren en er is geen noodzaak om identieke middelen in verschillende landen te gebruiken. Maar een zekere interoperabiliteit, harmonisatie en instrumenten voor wederzijdse herkenning in de regio en wereldwijd, voorzien in gemak en zijn belangrijk voor de concurrentiepositie van Suriname.

Partnerschappen

Het is mogelijk om voor veel diensten dezelfde identificatiesystemen te gebruiken, ook voor openbare en particuliere diensten. Financiële instellingen bieden vaak digitale identificatiesystemen, wat mogelijkheden biedt voor publiek-private partnerschappen, aangezien de vereisten voor een veilige identificatie vergelijkbaar zijn met die van de openbare diensten. Daarnaast biedt het in de toekomst mogelijkheden voor derde partijen om open data te gebruiken. Nederlandse voorbeelden hiervan zijn:

- Buienradar (KNMI)
- Parkmobile (RDW, geodata)

Andersom is uiteraard ook mogelijk en dat zal de insteek zijn van e-Gov Suriname.

Essentieel: (semantische) interoperabiliteit

Interoperabiliteitskaders vormen een essentieel onderdeel van de hele overheidsaanpak en maken de integratie van verschillende technologische platforms en oplossingen van gemeenschappelijke oplossingen en diensten mogelijk. Vanuit het oogpunt van e-governance verwijst interoperabiliteit naar het samenwerkingsvermogen tussen ministeries onderling en grensoverschrijdende diensten voor burgers, bedrijven en overheidsdiensten.

Het uitwisselen van gegevens kan een uitdaging zijn als gevolg van taalbarrières, verschillende specificaties van formaten en variëteiten van standaarden en categorisaties. Daarom moeten e-governance-toepassingen op een semantisch interoperabele manier gegevens uitwisselen. Dit bespaart tijd en geld en vermindert fouten. Op elk beleidsterrein zijn praktische gebieden te vinden, of het nu gaat om justitie, handel of participatie.

Standaarden voor data-uitwisseling

In de toekomst willen we qua data-uitwisseling niet voor verrassingen komen te staan. Daarom conformeren we ons zoveel mogelijk aan open standaarden. Lokaal en internationaal voorziet Nederland in een gespreid bedje voor e-Gov: www.forumstandaardisatie.nl. Met thema's als betalingsverkeer, wifistandaarden en geodata.

Best practices

Goede voorbeelden van de voordelen van interoperabiliteitskaders in de praktijk zijn te vinden in het European Interoperability Framework-proces.

2.1.4 Infrastructuur

Toegang tot het internet is een belangrijke factor voor de ontwikkeling van een informatiemaatschappij, omdat dit de basis vormt voor het leveren en gebruiken van e-overheidsdiensten. Internettoegang wordt meestal verzorgd door particuliere telecommunicatiebedrijven, die ook telecommunicatienetwerken beheren.

Bekabeld of mobiel

Toegang kan worden verleend via bekabelde of mobiele netwerken. Voor bekabelde netwerken kunnen de laatste meters thuis of op kantoor via de kabel of via draadloze toegangspuntverbinding (wifi) worden gebruikt. In sommige delen van de Suriname is de omvang van bekabelde netwerken voor zowel internet als telefonie beperkt, mobiel is vaker de oplossing.

Status quo in Suriname

Een moderne internetverbinding gaat normaal gesproken via breedband. Mobiele netwerk-technologieën zijn voortdurend in ontwikkeling en blijven betere verbindingen ontwikkelen. Nieuwe mobiele communicatiegeneraties worden regelmatig geüpgraded (NMT > 2G > 3G > 4G > 5G).

Wat betreft infrastructuur zijn er in Suriname dus geen noemenswaardige beperkingen voor e-Gov. Datacentra zijn modern en de telecomproviders zijn up-to-speed met de laatste stand van internettechnologie. Qua security moeten de Huawei-servers op verzoek van de president gescreend worden.

Radiofrequenties

Mobiele communicatie vereist radiofrequenties, een natuurlijke beperkte hulpbron, gereguleerd door internationale overeenkomsten en nationaal recht. Regelgevende instanties in Suriname behandelen de praktische toepassing van dergelijke regels. Suriname heeft mobiele communicatie en de landelijke penetratie daarvan redelijk goed op orde.

2.2 Analoge basiselementen

2.2.1 Internationale kaders

Om te profiteren van de voordelen die e-governance kan bieden voor internationale betrekkingen (zoals handel, vrij verkeer, onderzoek en onderwijs) is het zeer gunstig voor Suriname om deel te nemen aan internationale kaders. Bovendien kan zo'n samenwerking helpen om van elkaar te leren en om gezamenlijke projecten en dergelijke te creëren.

eGA Estland

Dat kan met landen in de regio maar ook met bijvoorbeeld Estland, een land dat wereldwijd vooroploopt op het gebied van e-governance. Het land heeft een consultancyorganisatie opgezet (eGA) om landen specifiek te helpen bij de implementatie van e-governance inclusief standaardisatie. We maken de concepten van Estland waar nodig op maat voor de Surinaamse samenleving, maar kopiëren zoveel mogelijk van de 'proven concepts and technologies'. Dit om de digitale transformatie zo snel en soepel mogelijk te laten verlopen.

Internationale initiatieven

Er bestaan een aantal internationale initiatieven om te profiteren van het ontbreken van fysieke grenzen in cyberspace en om internationale samenwerking te bevorderen. De Agenda voor Duurzame Ontwikkeling 2030 die in 2015 door de Algemene Vergadering van de Verenigde Naties (VN) is aangenomen, onderstreept het belang van ICT. De VN bevorderen initiatieven die verband houden met connectiviteit en infrastructuur, zoals de Breedbandcommissie van de Verenigde Naties voor duurzame ontwikkeling. Internationaal standaardiseren bij de implementatie van e-governance is zeer aan te bevelen.

2.2.2 Wettelijk kader

Volgens de beginselen van de rechtsstaat wordt het bestuur van een land uitgevoerd door middel van wetgeving en moeten alle activiteiten, met inbegrip van die van overheidsinstellingen, in overeenstemming met de wet worden uitgevoerd. Daarom is het van groot belang dat er passende regelgeving is voor e-governance. Maar: het is een veelvoorkomende misvatting dat e-governance veel nieuwe wetgeving vereist. Dit is niet het geval en dergelijke nieuwe wetgeving kan zelfs schadelijk zijn, omdat dit het risico met zich meebrengt dat het een parallel bestuurssysteem creëert in plaats van het bestuur te ondersteunen en te verbeteren.

Uitzondering

Slechts op een paar gebieden is speciale wetgeving nodig. Dit omvat onder andere erkenning van elektronische identiteiten en handtekeningen en elektronische documenten. Dit kan door middel van speciale wetten of wijzigingen in bestaande wetten, zoals wetgeving voor administratieve en strafrechtelijke procedures en contractenrecht.

Bescherming van privacy

Daarnaast is bescherming van de privacy essentieel. Al betekenen elektronische gegevens niet noodzakelijkerwijs verhoogde risico's voor de privacy, maar de perceptie is nog steeds dat dit het geval is. Bescherming van privacy is in de meeste landen in de wereld een grondwettelijk recht. Privacy wordt beschermd door internationale afspraken met betrekking tot de mensenrechten. De algemene regels worden in veel gevallen aangevuld met specifieke regelgeving voor gegevensbescherming (GDPR, 27001).

Cybersecurity

Er zijn ook situaties waarin technologie meer of andere risico's met zich meebrengt. Cybersecurity is een brede term die wordt gebruikt voor verschillende aspecten van het beveiligen van digitale systemen. Het bestaat niet op zichzelf, maar is een fundamenteel onderdeel van de ontwikkeling van e-overheid. Het is geïntegreerd in juridisch werk, maar gaat ook over bewustmaking en training, omdat veel cyberincidenten eenvoudige menselijke fouten of technische storingen zijn. Andere incidenten kunnen worden georganiseerd door criminelen of terroristen of zelfs deel uitmaken van militaire operaties.

Wat essentieel is om in het achterhoofd te houden over cyberveiligheid, is dat bedreigingen rechtstreeks van invloed zijn op de normale werking van nationale informatie- en communicatiesystemen. Verschillende elektronische diensten kunnen worden aangevallen, waaronder kritieke e-diensten zoals paspoort- en migratiecontrole, douane, algemene kritieke infrastructuur van het land (zoals elektriciteitsproductie en -distributie, drinkwater en riolering) of bankkaartbetalingen.

Beheer van cyberbedreigingen

Om cyberbedreigingen te beheren, moet Suriname beschikken over passende wetgeving en specifiek aangewezen overheidsinstanties die verantwoordelijk zijn voor de cyberbeveiliging en incidentmanagement. Suriname heeft bovendien behoefte aan wetgeving en instanties ter bestrijding van cybercriminaliteit en terrorisme.

2.2.3 Coördinerende instellingen

Er is behoefte aan coördinatie van e-governmentactiviteiten op hoog niveau, tussen verschillende eenheden van de overheid én andere instanties. Het idee van coördinatie is niet om de besluitvorming en de technische capaciteiten te centraliseren maar om de modernisering van de innovatie en de dienstverlening in elke overheidsinstelling op een geharmoniseerde manier te ondersteunen, waarbij dubbel werk en overinvesteringen worden voorkomen.

Instrumenten

De instrumenten voor coördinatie zijn:

- beleid, wet- en regelgeving
- budgettering
- toezicht
- gemeenschappelijke normen
- het toestaan van nationaal hergebruik van gegevens
- gegevensuitwisseling
- hergebruik van de softwareoplossingen
- een snelle ontwikkeling van de online diensten.

Scheiding besluitvormingsniveaus

Volgens de beginselen van good governance is het passend om de besluitvormingsniveaus te scheiden: strategische beslissingen, toezicht, coördinatie en uitvoering worden beter bewaakt in afzonderlijke instellingen.

Er moeten duidelijke rollen, mandaten en verantwoordelijkheden zijn tussen die instellingen. Het kan nodig zijn om naast de bestaande organisaties een nieuwe centrale coördinatie-eenheid op te zetten of deze taak op een andere manier expliciet aan een bestaand orgaan te geven. Dit kan een onafhankelijk agentschap zijn of bijvoorbeeld in het kabinet van de president worden gehuisvest. De centrale coördinatie-eenheid moet een duidelijk mandaat hebben van het parlement of het kabinet van ministers.

Centrale coördinatie-eenheid

Het is belangrijk dat de centrale coördinatie-eenheid rechtstreeks verslag uitbrengt aan de president om ervoor te zorgen dat besluiten en vooruitgang op hoog niveau politieke steun en passende middelen krijgen. Als een ministerie verantwoordelijk is voor de ontwikkeling van e-governance, bestaat het gevaar dat andere ministeries – normaal horizontaal hiërarchisch geplaatst – de basis voor dit ene ministerie in twijfel trekken, om zo kwesties voor alle ministeries te bepalen.

Het wordt aanbevolen de ontwikkeling van het beleid en de normen te centraliseren, waarna de uitvoering eventueel decentraal kan plaatsvinden.

Toezichthouders

Toezichthoudende instellingen die toezien op de juiste uitvoering van wettelijke en regulerende normen vormen een belangrijke aanvulling op de uitvoerende instellingen. Het kan gaan om gegevensbeschermingsinstanties, ICT-regelgevende instanties, consumentenbeschermings-instanties of nationale controlebureaus. In hoeverre deze instanties in Suriname aanwezig zijn en

wat hun capaciteiten zijn om toezicht te houden is momenteel onbekend.

Belangrijke steun voor de ontwikkeling van e-governance kan ook worden verleend door de ICT-associatie.

2.2.4 Politieke wil en verandermanagement

Om veranderingen op lange termijn veilig te stellen, zijn politieke wil en leiderschap nodig. Een belangrijk deel van de leden van het parlement moet zich bewust zijn van de voordelen van e-governance, trends en vooruitgang in het land. Met deze kennis kunnen zij het belangrijke wetgevingsproces ondersteunen.

Persoonlijk leiderschap is belangrijk, zowel op politiek als op bestuurlijk niveau. Want het hele implementatieproces van e-governance gaat niet alleen over technologie. Het gaat ook niet om de overdracht van de diensten van papier naar computer: het is het opnieuw uitvinden van openbare diensten. Of nog breder: het is het opnieuw uitvinden van bestuur.

Nieuwe vaardigheden en competenties

De belangrijkste vraag voor verandermanagement is dan ook: hoe energie en ideeën vrij te maken voor de re-engineering van de bestaande overheidsdiensten en aanverwante bedrijfsprocessen bij de overheid? Daarvoor zijn nieuwe vaardigheden nodig, zoals computervaardigheden, evenals nieuwe competenties, zoals het analyseren van big data, het begrijpen van verbanden tussen openbare diensten en hun impact en het ontwerpen van nieuwe diensten op basis van deze kennis.

2.2.5 Toegang tot diensten en stimuleren bewustwording

Een zeer belangrijk element van de implementatie van e-governance is meer bewustwording onder mensen en organisaties over de kansen die het biedt. Anders zullen beide groepen geen gebruikmaken van de e-diensten en zal er ook geen noodzaak gezien worden om daarin te investeren.

Verschillende aspecten

Aspecten op vele vlakken moeten bij die bewustwording worden meegenomen, waaronder:

- Cultureel: de voorkeur voor fysieke bezoeken aan de kantoren en face-to-facecontact met ambtenaren.
- Economisch: de kosten voor toegang tot onlinediensten kunnen nog steeds hoog zijn voor particulieren.
- Religieus: in sommige religies kunnen nummers in plaats van namen (zoals een persoonlijk identiteitsnummer) onaanvaardbaar zijn.
- Security en privacy: individuen kunnen zich zorgen maken over hoe hun gegevens worden verzameld, verwerkt en opgeslagen.

Er is geen standaardrecept hoe om te gaan met culturele, economische, religieuze of veiligheidsaspecten, maar alle vragen hierover moeten duidelijk worden beantwoord. Voor het grote publiek, voor de groepen belanghebbenden als voor deskundigen. Aangezien e-governance transparantie kan bieden, moet de uitvoering van e-governance-instrumenten en -programma's ook transparant zijn.

3 Implementatiematrix

De ontwikkeling van e-governance vereist bepaalde organisatorische en technologische capaciteiten. Voordat we in Suriname e-governance kunnen opbouwen, moeten we eerst het huidige niveau bepalen en, indien nodig, de vereisten naar het juiste minimumniveau brengen.

In dit hoofdstuk presenteren we de Implementatiematrix (tabel 1): een instrument om het niveau van e-government in Suriname aan te geven en om de belangrijkste elementen te bepalen die moeten worden aangepakt, zelfs als het werk op verschillende fronten parallel moet verlopen.

Tabel 1. Implementatiematrix

BELANGRIJKE ELEMENTEN VOOR E-OVERHEID	MINIMUMNIVEAU	BASISNIVEAU	NUTTIG NIVEAU	DUURZAAM NIVEAU
Politieke wil en verandermanagement	Er is geen politieke steun voor e-governance en bestaande digitale systemen werken onder sectoriële ministeries. ☐	Politiek leiderschap op hoog niveau, bijv. het staatshoofd is een e-governance-woordvoerder. ☐	Op hoog niveau zijn beleidsdocumenten aangenomen, bijv. 'Fundamentals of Information Policy' of 'Digitale Agenda'. ☐	De ontwikkeling van e-governance is al lange tijd een nationale prioriteit, bijvoorbeeld ten minste drie jaar. ☐
Coördinerende instelling	Bestaande digitale systemen werken en worden ontwikkeld zonder coördinatie. ☐	Een dergelijke instelling is opgericht en gemandateerd. ☐	Beleidsnota's en aanverwante documenten, een e-government-strategie, begroting en actieplannen worden opgesteld. ☐	Beheert de algehele e-governancearchitectuur en ontwikkelingen vanuit een holistisch oogpunt. ☐
Coördinerende instelling: financieringsmodel	Budgettering van bestaande digitale systemen is gebaseerd op ICT-inkoop zonder impactanalyse. ☐	Elk ministerie en elke overheidsinstantie heeft een ICT-budgetrecord. ☐	Op staatsniveau is bekend wat de totale kosten zijn van e-governance en hoeveel middelen er elk jaar voor e-governance worden gepland. ☐	Het nationale financiële model van de digitale overheid is in overeenstemming met de langetermijnstrategie voor het digitale beleid, dat ministeries en overheden helpt de risico's van de cyclische planning van de overheidsbegroting te beheersen. ☐
Wettelijk kader	Bestaande wetgeving omvat basis-ICT-gerelateerde wetgeving op basis van internationale vereisten. ☐	Er is bereidheid om de bestaande wetgeving aan te vullen met details die voortvloeien uit e-governanceoplossingen , bijvoorbeeld via een bepaling als '... het recht om informatie elektronisch te ontvangen'. ☐	Er is een minimumaantal rechtshandelingen aangenomen die specifiek relevant zijn voor e-governance. Zo is er regelgeving voor gegevensbescherming, elektronische identiteit en handtekening en voor burgerlijke registers. ☐	Alle rechtshandelingen houden rekening met de details van e-governanceoplossingen. ☐
Internationale kaders	Geen of zeer beperkte activiteiten in internationale kaders. ☐	Lid van en deelnemen aan internationale kaders, maar geen activiteiten in verband met e-governance. ☐	Neemt deel aan en profiteert van samenwerking. ☐	Actieve deelnemer van projecten in verband met e-governance. ☐

Veilige digitale identiteit	Er zijn verschillende technologische methoden voor digitale gebruikersverificatie bij verschillende overheidsinstellingen. ☐	Identiteitsregister is opgericht en unieke persoonlijke identificatie mechanisme is overeengekomen. ☐	Een afgiftesysteem voor identiteitskaarten is vastgesteld en een aanzienlijke hoeveelheid burgers heeft identiteitskaarten. Persoonlijke identificatie-informatie is elektronisch bruikbaar. ☐	Veilige technologie die wordt gebruikt voor de digitale identiteit. ☐
Digitale handtekening	Technische oplossing is gepland. ☐	Technische oplossing is geïmplementeerd. ☐	De verordening is van kracht. ☐	De digitale handtekening wordt in belangrijke mate gebruikt in het dagelijks leven. ☐
Veilige digitale identiteit en digitale handtekening: interoperabiliteitskader	Interoperabiliteit vindt plaats bij bilaterale overeenkomsten tussen verschillende overheidsinstellingen. ☐	De vereisten voor technische interoperabiliteit worden beschreven. ☐	De syntactische en semantische interoperabiliteit (overeengekomen gemeenschappelijke gegevensformaat en het delen van betekenis van de gegevens) worden beschreven. ☐	De organisatorische interoperabiliteit wordt beschreven. ☐
Veilige digitale identiteit en digitale handtekening: beveiligingskader en het systeem van veiligheidsmaatregelen	Verantwoordelijkheid van cybersecurity ligt op het niveau van ICT-systeemoperaties bij verschillende overheidsinstellingen. ☐	Cybersecurity is beoordeeld en het bewustzijn van de werkelijke situatie is opgemerkt. Bijvoorbeeld: voldoet aan vragenlijst voor cybersecurity-index. De instelling die verantwoordelijk is voor de coördinatie van cybersecuritykwesties is opgericht en gemandateerd. ☐	Het nationale CERT is opgericht en gemandateerd en het systeem van veiligheidsmaatregelen is opgesteld. ☐	Alle ministeries en overheidsinstanties maken gebruik van het systeem van veiligheidsmaatregelen en er wordt een passend auditproces toegepast. ☐
Infrastructuurkwesties	De toegang tot infrastructuur en diensten van telecommunicatie is beperkt tot geselecteerde instellingen. ☐	Een telecommunicatienetwerkinfrastructuur is ontwikkeld door toegewijde bedrijven met internationale connectiviteit. ☐	Concurrerende markt voor telecommunicatiedienst en met stimulans voor voortdurende innovatie en verbetering van de dekking. ☐	Private en public cloud (beheerd door principe van publiek-private partnerschappen) en geautomatiseerde ontwikkelomgeving. ☐

4 Roadmap voor de implementatie van de matrix

Deze roadmap is bedoeld om op een korte maar alomvattende manier aan te tonen welke verschillende stappen zijn opgenomen in de ontwikkeling van e-governance. Zowel de matrix als de roadmap kunnen dienen als checklist. Daarnaast stelt e-Gov een reeks activiteiten voor om capaciteit op te bouwen die bijdraagt aan een verhoging van het niveau van deskundigheid onder personen die betrokken zijn bij de ontwikkeling en uitvoering van e-governance.

De componenten van alle belangrijke elementen in de matrix kunnen – en in veel gevallen, moeten – voor een groot deel parallel worden behandeld, omdat de verschillende zaken nauw met elkaar verbonden zijn. De stappen hoeven niet in een specifieke volgorde te worden gezet.
Om te illustreren wat dit betekent, kan het voorbeeld worden genoemd dat een land wijdverspreide interoperabiliteit van databanken kan invoeren voor een efficiënter beheer. Zelfs zonder rechtstreeks diensten aan het publiek te verlenen, waarbij persoonlijke digitale identificatie geen prioriteit hoeft te zijn.

4.1 Politieke wil en verandermanagement

Dit onderdeel omvat het waarborgen van politiek leiderschap op hoog niveau dat leidt tot de goedkeuring en uitvoering van relevante beleidsmaatregelen en agenda's. De invoering van e-governance moet een politieke prioriteit zijn en een overeenkomst tussen alle politieke krachten in het land is wenselijk. De politieke wil moet op het hoogst mogelijke politieke niveau worden uitgesproken, bijvoorbeeld door de president, de VP of het parlement.

Om dit naar behoren te laten werken, is het belangrijk om rollen te identificeren en verantwoordelijkheden voor coördinatie en uitvoering te bepalen en het stimuleren van publiek-private samenwerking en samenwerking met academische instellingen.

In de overeenkomst wordt het gebruik van digitale technologieën vermeld als opeenvolgende en belangrijkste methode voor de ontwikkeling van de samenleving en de aanpak van de uitdagingen en problemen in de samenleving. De politieke wil moet, indien mogelijk, worden bevestigd met een politiek document, zoals ‘Fundamentals of Information Policy’, dat een garantie voor een dergelijke wil zou zijn.

Per definitie, de overheid is er door én voor het volk. Het wordt natuurlijk ook gerund door mensen. Het veranderen van de dagelijkse routines van de mensen die werkzaam zijn in de overheid vereist motivatie, maar ambtenaren kunnen gemotiveerd worden. Change management gaat dan ook over het meenemen van ambtenaren in de vernieuwing en het stimuleren van hun ideeën om bestaande openbare diensten en aanverwante activiteiten binnen de overheid opnieuw te ontwerpen.

Zoals hierboven vermeld, moeten politieke leiders betrokken blijven en tijd, budget en zelfs politiek kapitaal inzetten voor het slagen van e-governance. Daarnaast is een voortdurende capaciteitsopbouw van de overheid en e-governance noodzakelijk. De onderstaande stappen kunnen in de meest gunstige gevallen parallel lopen.

BASISLEVEL
- Er is met politieke krachten overeenstemming bereikt over e-governance.
- Er is een e-governancewoordvoerder benoemd.
- Er is voortdurende bewustmaking.

NUTTIG LEVEL
- Overeenkomst op het hoogst mogelijke politieke level is verklaard (politieke prioriteit).
- De politieke wil is bevestigd met een politiek document.
- Strategieplannen voor e-governance-implementatie zijn samengesteld (transparantie).
- Er is voortdurende bewustmaking.

DUURZAAM LEVEL
- Publieke-private samenwerkingen met academische instituties worden aangemoedigd.
- Er wordt hulp geboden bij de ontwikkeling (financieel en/of via support van een expert).
- Digitale databases zijn geïmplementeerd.
- Interoperabiliteit van deze databases is ontwikkeld.
- Er is voortdurende bewustmaking.

4.2 Coördineren van instellingen, inclusief het financieringsmodel

4.2.1 Coördineren van de instellingen

Dit onderdeel omvat het aanwijzen van een instelling die het mandaat heeft om besluiten te nemen over e-governance voor de gehele overheid. Het is mogelijk om regionale (federale staats)oplossingen te hebben, maar in ieder geval zal coördinatie nodig zijn. Het gaat dan niet om centraliseren, maar om ervoor te zorgen dat relevante besluiten naar behoren worden gecoördineerd.

De coördinerende instelling is verantwoordelijk voor de strategische planning die nodig is voor een e-governance en, meer in het algemeen, een informatiemaatschappij. Hoe hoger in de hiërarchie de aangewezen eenheid staat, hoe groter de kans dat ministeries en agentschappen worden aangestuurd. De bevoegdheden van de coördinerende instelling moeten via wetgeving worden bepaald.

BASISLEVEL
- Er is een geschikte organisatie of geschikt persoon aangewezen voor de ontwikkeling van e-governance.
- Macht en competenties zijn opgelegd via wetgeving.
- De vaardigheid van de betrokken personen wordt getraind (er wordt doorlopend aan de vaardigheid gewerkt).

NUTTIG LEVEL
- Coördinatietools zijn toegepast (beleidslijnen, wetgeving en regulering, budgettering, monitoren, een gemeenschappelijke standaard, toestaan van landelijk hergebruik van data, data-uitwisseling, hergebruik van softwareoplossingen en snelle ontwikkeling van de online services, etc.).

DUURZAAM LEVEL
- Goede e-governance-principes zijn geïmplementeerd.
- Beleidslijnen en standaard ontwikkelingen zijn gecentraliseerd.
- Implementatie is gedecentraliseerd.

4.2.2 Het financieringsmodel

Om de duurzaamheid te waarborgen, moeten algemene financiële en financieringsmodellen voor e-diensten worden ontwikkeld. Voor elke e-governanceoplossing moeten de totale eigendomskosten van de oplossing worden gepland. De invoering van e-governance brengt kosten met zich mee, hoewel het uiteindelijk zal leiden tot besparingen in andere opzichten. Het is dus van essentieel belang dat er voldoende voorzieningen zijn voor de nodige middelen op een duurzame manier. De voorziening kan centraal plaatsvinden, maar ook op het niveau van specifieke instellingen. In ieder geval is voor de middellange tot lange termijn voldoende financiering nodig, bij voorkeur volgens een meerjarenbegroting.

Het is belangrijk dat autoriteiten in staat zijn om de risico's van de cyclische planning van de overheidsbegroting te beheersen. In de financiële prognose van de staat wordt bijvoorbeeld een aparte begrotingslijn toegewezen voor de ontwikkeling van e-governance. Om deze toewijzing te ondersteunen, dient de wetgeving de procedures vast te stellen voor de planning van de begroting voor e-governance en het gebruiksbeheer van begrotingsmiddelen. In principe is transparantie en verantwoordingsplicht van het financiële model noodzakelijk.

BASISLEVEL
- De gehanteerde aanpak is gebaseerd op een impactanalyse (kostenanalyse).
- Er is een apart budget aangewezen (ICT-budget wordt bijgehouden voor ieder ministerie en/of iedere overheidsinstantie).

NUTTIG LEVEL
- Budgetplanningprincipes worden ontwikkeld en verplicht via de wet.
- Er worden tools gebruikt die zorgen dat de transparantie en verantwoordingsplicht voor begrotingsprocedures wordt toegepast.
- Mogelijke financiële hulpmechanismes worden vastgesteld.

DUURZAAM LEVEL
- Bronnen voor duurzame financiering worden geïdentificeerd.
- E-governancebegrotings-strategieën worden voor de lange termijn toegepast.
- Er wordt rekening gehouden met de risico's van het cyclisch planningsproces van het staatsbudget.

4.3 Juridisch kader

Hoewel er geen wettelijke eisen zin voor het invoeren van e-governance, is wetgeving wel degelijk van belang. Er zijn een aantal wetten die onder de loep genomen moeten worden. Dit juridische overzicht moet worden gemaakt in de vroege stadia van de ontwikkeling van e-governance.

Hoe innovatiever de e-governanceoplossing, hoe meer het de workflow binnen de overheid verandert. Grotere wijzigingen in de workflow vragen om meer fundamentele veranderingen in de wetgeving. Het is daarom van belang om vast te stellen of er wijzigingen nodig zijn om bijvoorbeeld elektronische informatie te accepteren. Er kan ook aanvullende wetgeving nodig zijn voor elektronische handtekeningen en gegevensbescherming. Politieke wil speelt een belangrijke rol bij het veranderen van de wetgeving.

BASISLEVEL
- Elke wetgeving die onverenigbaar is met e-governance wordt in kaart gebracht.
- Er is een analyse van het rechtssysteem uitgevoerd.

NUTTIG LEVEL
- Er is een minimumniveau van relevante wetgeving voor e-governance aangenomen.
- Er zijn specifieke regulaties aangenomen voor databescherming, elektronische identiteit en handtekening, bevolkingsregisters en voor de bescherming van de nationale cyberspace.

DUURZAAM LEVEL
- Iedere rechtshandeling stemt overeen met de details van e-governance.
- De juridische omgeving wordt afgestemd op regionaal en/of Afrikaanse Unie-niveau.

4.4 Internationaal kader

Om te profiteren van de voordelen die e-governance kan bieden voor internationale betrekkingen (zoals handel, vrij verkeer, onderzoek en onderwijs) is het voor Suriname verstandig om kennis te delen binnen bijvoorbeeld CARICOM (Caribbean Community).

BASISLEVEL
- Er is een geschikte instantie of geschikt persoon aangewezen als verantwoordelijke voor de samenwerking.
- Een vertegenwoordiger van een land neemt deel aan een internationale samenwerking.

NUTTIG LEVEL
- Een samenwerkingsstrategie is gemaakt.
- Een vertegenwoordiger van een land neemt regelmatig deel aan internationale samenwerkingen.
- Enige voordelen voor een land worden ontvangen.

DUURZAAM LEVEL
- Een land neemt actief deel aan projecten gelinkt aan e-governance.
- Samenwerking met academische instanties is opgericht.

4.5 Toegang tot services en bewustwording

De betrokkenheid van de burger is een parallelle en overkoepelende kwestie. Voor succesvol e-governance is het nuttig om te onderzoeken hoe het maatschappelijk middenveld ondersteund kan worden en hoe de betrokkenheid van burgers kan worden gestimuleerd. Dit is onderdeel van het proces van bewustwording over de digitale samenleving en de algemene ontwikkeling van computergeletterdheid.

BASISLEVEL
- Een aantal e-governanceservices is beschikbaar voor de meeste burgers.
- Informatie over hoe deze services worden gebruikt is publiekelijk beschikbaar (transparantie).
- Er is een aantal campagnes geïmplementeerd over hoe deze services worden gebruikt.

NUTTIG LEVEL
- Veel e-governanceservices zijn beschikbaar.
- Services zijn makkelijk in gebruik.
- Veel burgers gebruiken deze services.
- Er zijn voortdurend campagnes over hoe deze services worden gebruikt.

DUURZAAM LEVEL
- Een breed scala aan e-governanceservices zijn beschikbaar.
- Burgers hebben goede kennis over hoe deze services worden gebruikt.
- Burgers gebruiken deze services in het dagelijks leven.
- Hulp voor gebruikers is beschikbaar en wordt goed uitgevoerd (inclusief technische hulp).
- De burgermaatschappij (bestaande organisaties) is betrokken.

4.6 Overheidsportaal, inclusief data- en servicecatalogus, digitale databases en veilige data-uitwisseling

4.6.1 Overheidsportaal

Om met het publiek te communiceren, moet de overheid een apparaat- en technologieneutraal digitaal informatiekanaal opzetten, zoals een overheidsportaal dat op verschillende apparaten werkt. Het informatiekanaal wordt ingezet om zowel informatiediensten als procedurele diensten aan te bieden. Met een goed functionerend digitaal informatiekanaal kunnen overheidsdiensten één geheel vormen en de beschikbaarheid van openbare diensten verbeteren. In Suriname is het ontwikkelen van diensten voor mobiele apparaten prioriteit (mobile first).

BASISLEVEL
- Er bestaat een overheidsportaal.
- Het portaal wordt alleen gebruikt om informatie te delen.
- De informatie wordt regelmatig geüpdatet.

NUTTIG LEVEL
- Het overheidsportaal biedt ook toegang tot e-services.
- Services zijn makkelijk in gebruik.

DUURZAAM LEVEL
- De informatie op het portaal en de e-services zijn veilig te gebruiken vanaf verschillende e-channels op ieder apparaat.
- Capaciteit van personen die betrokken zijn bij de ontwikkeling en implementatie van e-governance is aanwezig.

4.6.2 Data- en servicecatalogus, digitale databases en veilige data-uitwisseling

Om databanken verder te digitaliseren en middelen te creëren voor veilige gegevensuitwisseling is een duidelijk overzicht van gegevens en diensten essentieel. Tegelijkertijd biedt de catalogus een dienst op zich, door een overzicht te geven van wat er beschikbaar is, zodat bijvoorbeeld nieuwe diensten en het nut daarvan kunnen worden vastgesteld.

Digitalisering van overheidsdiensten houdt in dat ministeries en overheidsinstanties gegevens vastleggen en verwerken in een machineleesbare vorm. Voor de ontwikkeling van e-governance zijn ten minste enkele digitale databases nodig én de behoefte aan digitale gegevensuitwisseling tussen databases. Het is wenselijk om zo snel mogelijk een persoonlijke identiteitsdatabase op te zetten.

BASISLEVEL
- Er bestaat een data- en servicecatalogus.
- Enkele digitale databases zijn uitgerold en een governanceorganisatie is opgericht.
- Een technische oplossing voor een veilige data-uitwisseling is uitgerold en een governance-organisatie is opgericht.

NUTTIG LEVEL
- Een significante hoeveelheid data is omschreven in de catalogus.
- Een significant aantal registers en databases is gedigitaliseerd.
- Een significant aantal overheidsregisters en databases wisselt gegevens uit via een veilige 'data exchange layer'.
- Er is een specifiek(e) organisatie/persoon aangewezen.

DUURZAAM LEVEL
- Alle data is omschreven in de catalogus.
- Alle gedigitaliseerde data wordt gedeeld.
- Enkele privé-informatiesystemen zijn aangesloten.
- Er bestaat grensoverschrijdende interoperabiliteit.
- Capaciteit van personen die betrokken zijn bij de ontwikkeling en implementatie van e-governance is aanwezig.

4.7 Veilige digitale identiteit en handtekening, inclusief een interoperabiliteitskader en veiligheidskader

4.7.1 Veilige digitale identiteit en handtekening

Ontwikkeling van het concept en instrumenten van de digitale identiteit zijn noodzakelijk. Om e-governancediensten nuttig te maken voor alle soorten governancetaken, is het belangrijk dat gebruikers zich op een veilige manier identificeren. Het gaat dan om een mobiele of digitale identificatie, inclusief een digitale handtekening. Daarbij moeten handtekeningen veilig genoeg zijn om herkenbaar te zijn in diverse situaties, zoals als bewijs in de rechtbank.

BASISLEVEL
- Een identiteitsregister is opgericht.
- Er is overeengekomen over een uniek persoonlijk identificatiesysteem.
- Een technische oplossing voor een digitale handtekening is uitgerold.

NUTTIG LEVEL
- Een systeem dat ID-kaarten verstrekt is opgericht.
- Een significant aantal burgers heeft een ID-kaart.
- Burgers gebruiken de digitale identiteit en handtekening.
- De digitale handtekening wordt erkend door de wet.
- Er zijn programma's opgericht om (het gebruik van) de digitale identiteit en handtekening bekend te maken bij de burgers.

DUURZAAM LEVEL
- Veilige technologie is geïntroduceerd.
- Er bestaan 'trust services'.
- De digitale identiteit wordt gebruikt bij communicatie met overheidsinstanties.
- De digitale handtekening wordt in het dagelijks leven door burgers gebruikt.

4.7.2 Interoperabiliteitskader en veiligheidskader

Het interoperabiliteitskader is onderdeel van de veilige digitale identiteit. Het is belangrijk om de vereisten voor technische interoperabiliteit in een vroeg stadium te beschrijven. Er is een geleidelijke ontwikkeling nodig van syntactische, semantische en organisatorische interoperabiliteit. E-governanceoplossingen die waarde creëren voor de samenleving worden gecreëerd in verschillende ministeries en overheidsinstanties.

Verder moet er overeenstemming zijn over een minimumset van regels die de ontwikkeling van e-governanceoplossingen waarborgen. De noodzakelijke regels voor coördinatie moeten op politiek, organisatorisch, juridisch en technisch niveau overeenstemmen. Het ontwerp van het interoperabiliteitskader moet onder de verantwoordelijkheid van de coördinerende instelling vallen. De eerste versie van het interoperabiliteitskader moet zo snel mogelijk worden vastgesteld, waarbij de naleving ervan voor alle partijen verplicht moet zijn. Naleving helpt om de bestaande staatsmiddelen opportuun te gebruiken. Het interoperabiliteitskader zal evolueren met de ontwikkeling van kernelementen voor e-governance.

De groeiende cyberdreigingen op wereldwijd niveau vereisen dat overheden zich richten op het waarborgen van e-governancebeveiligingsmaatregelen. Bewustwording van bedreigingen en het veiligheidsniveau van de e-governance is daarbij belangrijk. De coördinerende instelling is verplicht om de ontwikkeling, monitoring en het toezicht op relevante cyberveiligheidsregels en -maatregelen te organiseren. Er moet een CERT en goede controleprocessen worden opgezet. Daarbij moeten alle ministeries en autoriteiten adequate veiligheidsmaatregelen toepassen. Het cyberbeveiligingskader en het systeem van beveiligingsmaatregelen moeten bij wetgeving worden vastgesteld.

BASISLEVEL
- Het kader voor e-governmentarchitectuur en interoperabiliteit is ontwikkeld.
- Het cybersecurityassessment is voltooid.

NUTTIG LEVEL
- Er is overeenstemming over een dataformat en het delen van data (interoperabiliteit).
- Een nationaal CERT is gecreëerd.

DUURZAAM LEVEL
- Organisatorische interoperabiliteit is afgesproken.
- Er is een relevant kennisniveau bij ministeries en instanties (beveiligingsmaatregelen en auditprocessen zijn vastgesteld).

4.8 Problemen met de infrastructuur

Toegang tot ICT is een belangrijke basisvoorwaarde voor e-governance. Echter maakt ondersteuning voor de opbouw van infrastructuurcapaciteit normaliter geen deel uit van e-governanceactiviteiten.
Een minimumniveau van ICT-infrastructuurcapaciteit is een voorwaarde om e-governanceprojecten uit te voeren. Commerciële bedrijven bouwen de communicatienetwerken. Het is vervolgens de taak van de Republiek Suriname om de ontwikkeling van de netwerken te reguleren en gunstige voorwaarden te scheppen voor de bewoners, zodat zij toegang krijgen tot de netwerken.

Het is de verantwoordelijkheid van de Republiek Suriname om alle overheidsinstanties en lokale overheidsinstanties, scholen, bibliotheken, ziekenhuizen en andere overheden met elkaar te verbinden via het bestaande netwerk. Surinaamse telecomorganisaties hebben de netwerken al goed ingeregeld. Echter is de toegang voor alle burgers en instanties is nog niet geborgd.

BASISLEVEL
- De infrastructuur van het telecommunicatienetwerk wordt ontwikkeld door toegewijde bedrijven.
- Internationale connectiviteit wordt geboden.

NUTTIG LEVEL
- ICT-regulatie wordt toegepast (inclusief competitie, regulatie en regelgevende instanties)
- Deelnemers aan de telecommunicatiemarkt zijn geïnteresseerd in voortdurende innovatie en verbetering van de dekking.

DUURZAAM LEVEL
- De private en publieke cloud is tot stand gebracht.
- Er bestaan publiek-private samenwerkingen.
- Er bestaat een omgeving die voortdurend is gericht op ontwikkeling.