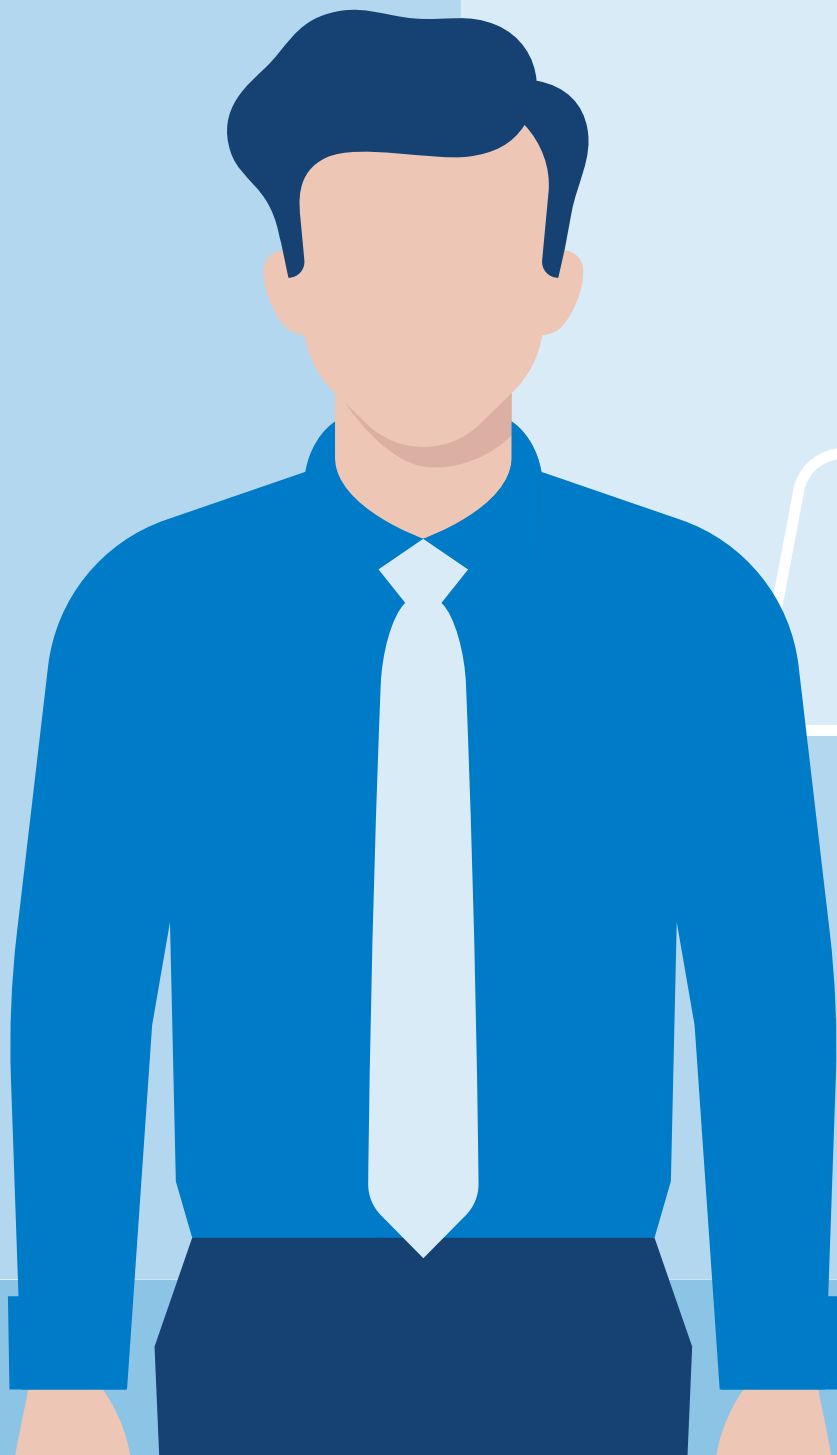




Architectuur Digitale Overheid 2030

versie 2024

Werkdocument voor bestuurders,
beleidsmakers en architecten





Voorwoord

Het maakt burgers en ondernemers bijna niet uit met welke overheidsinstantie zij te maken hebben. Zij willen de verschillende overheidsinstanties als één overheid ervaren. Maar hoe kun je zo'n 1600 overheidsorganisaties laten toegroeien naar een samenhangende digitale overheid? Hoe kun je zorgen dat overheidsorganisaties onderling naadloos samenwerken?



Daarvoor moeten afspraken gemaakt worden. Afspraken over de inrichting van de digitale overheid, over toe te passen standaarden en over belangrijke, gemeenschappelijke voorzieningen, zoals DigiD, MijnOverheid of Overheid.nl. Deze afspraken vormen – bij elkaar opgeteld – de architectuur van de digitale overheid.

Dit document is het resultaat van een breed samengesteld overleg. Vertegenwoordigers van het Rijk, grote uitvoeringsorganisaties, provincies, gemeenten en waterschappen. Zij werken samen in de Architectuurraad Digitale Overheid. Dit document biedt houvast voor overheidsorganisaties die dagelijks in de weer zijn om hun

dienstverlening te verbeteren en hun informatiehuishouding te moderniseren. Er worden jaarlijks honderden programma's en projecten uitgevoerd. Digitalisering staat hierbij vaak centraal. Dit document geeft een solide kader voor deze vernieuwingsactiviteiten. Door binnen de afspraken in dit document te blijven, groeien we de komende jaren toe naar een overheid die op moderne wijze diensten verleent aan burgers en ondernemers.

Guido Bayens

Onafhankelijk voorzitter
Architectuurraad Digitale Overheid



Inhoudsopgave

- ▶ Voorwoord

Deel 1 Voor bestuurders en beleidsmakers

- ▶ 1 Dit document in 1 minuut
- ▶ 2 Samenvatting
- ▶ 3 Beeld van de digitale overheid in 2030

Deel 2 Voor architecten

- ▶ 1 Inleiding en afbakening
- ▶ 2 Verantwoording en vervolgstappen
- ▶ 3 Richtlijnen voor deze architectuur
- ▶ 4 Structuur
- ▶ 5 Opbouw van de architectuur
- ▶ 6 Architectuurbeschrijving
- ▶ 7 Aspectgebieden

Bijlagen

- ▶ 1 Overzicht bouwstenen digitale overheid
- ▶ 2 Relatie bouwstenen met E.U.-verordeningen
- ▶ 3 Begrippenlijst
- ▶ 4 Betrokkenen bij de totstandkoming van deze versie





Deel 1

Voor bestuurders en beleidsmakers

- ▶ 1 Dit document in 1 minuut
- ▶ 2 Samenvatting
- ▶ 3 Beeld van de digitale overheid in 2030





1 Dit document in 1 minuut

Dit werkdocument beschrijft de architectuur van de digitale overheid in 2030. Veel van de bouwstenen voor de gewenste Digitale Overheid zijn er al. Deze architectuur biedt samenhang voor de verdere ontwikkeling daarvan, vergelijkbaar met een stedenbouwkundige planologie.

Het werkdocument 'Architectuur Digitale Overheid 2030' beschrijft de architectuur van de digitale overheid in 2030. Het geeft richting aan de ontwikkeling van de digitale overheid. Het document biedt ook een goede basis voor een op architectuur gebaseerd programma- en projectenportfolio. Het werkdocument is gebaseerd op bestaand beleid en vastgestelde beleidsdocumenten. Denk aan de Werkagenda Waardengedreven Digitaliseren en de GDI-meerjarenvisie.

Het document legt het fundament voor een verbindende architectuur van de digitale overheid. Het maakt verbindingen tussen overheidsorganisaties op alle bestuurslagen en hun architecturen. Het document stelt dat overheden vooral gebruik moeten maken van bestaande bouwstenen van de digitale overheid, mits goed beheerd en doorontwikkeld. Het geeft ook aan wat ontbreekt en doet voorstellen voor het toevoegen van nog ontbrekende bouwstenen. Dit document wordt actueel gehouden volgens een afgesproken procedure. De meest actuele versie is te vinden op pgdi.nl/ado.

De kern van de architectuur

De Nederlandse digitale overheid heeft nu al heel veel goede bouwstenen. Maar overheidsorganisaties moeten deze breder, beter en meer kunnen gebruiken. Daarnaast moeten dienstverleners de kans krijgen om nog meer en beter op basis van generieke afspraken, standaarden en voorzieningen met elkaar samen te werken. Alleen zo ervaren burgers en ondernemers één digitale overheid.

Architectuur als planologisch instrument

Het document beschrijft het beeld van de architectuur van de digitale overheid in 2030 en legt de basis voor een samenhangende en consistente invulling van de digitale overheid. Deze architecturale aanpak is te vergelijken met stedenbouwkundige planologie: beide geven een beeld van een goed functionerende en samenhangende toekomstige structuur. Stedenbouwkundige planologie richt zich op de fysieke inrichting van de stad waaronder de verbindingen tussen de verschillende gebouwen en de infrastructuur. De architectuur van de digitale overheid richt zich op de digitale infrastructuur en de verbindingen tussen diverse overheidsorganisaties en hun architecturen. Beide disciplines hebben wetgeving en beleid nodig om een samenhangende structuur te kunnen realiseren. Beide zijn een gids. Architectuur van de digitale overheid draagt bij aan het tot stand brengen van een goed functionerende digitale overheid. Het verwijst naar wetgeving, bestaand beleid en verdiepende informatie bij verschillende onderwerpen. Stedenbouwkundige planologie maakt gebruik van beleid en regelgeving om een samenhangende stad te creëren.

Het document heeft een bredere scope dan de Generieke Digitale Infrastructuur (GDI). Dat komt omdat de digitale overheid die burgers en ondernemers ervaren, opgebouwd is uit veel meer onderdelen dan de GDI. De bredere scope biedt de mogelijkheid om concreet te kunnen sturen op de bijdrage van GDI-bouwstenen aan de digitale overheid. Het document schetst, in termen van stedenbouwkunde, de



stad en geeft aan wat er al aan functionaliteit is. Maar het geeft ook aan welke kernen nog ontbreken en welke straten moeten worden gelegd.

Werken met architectuur

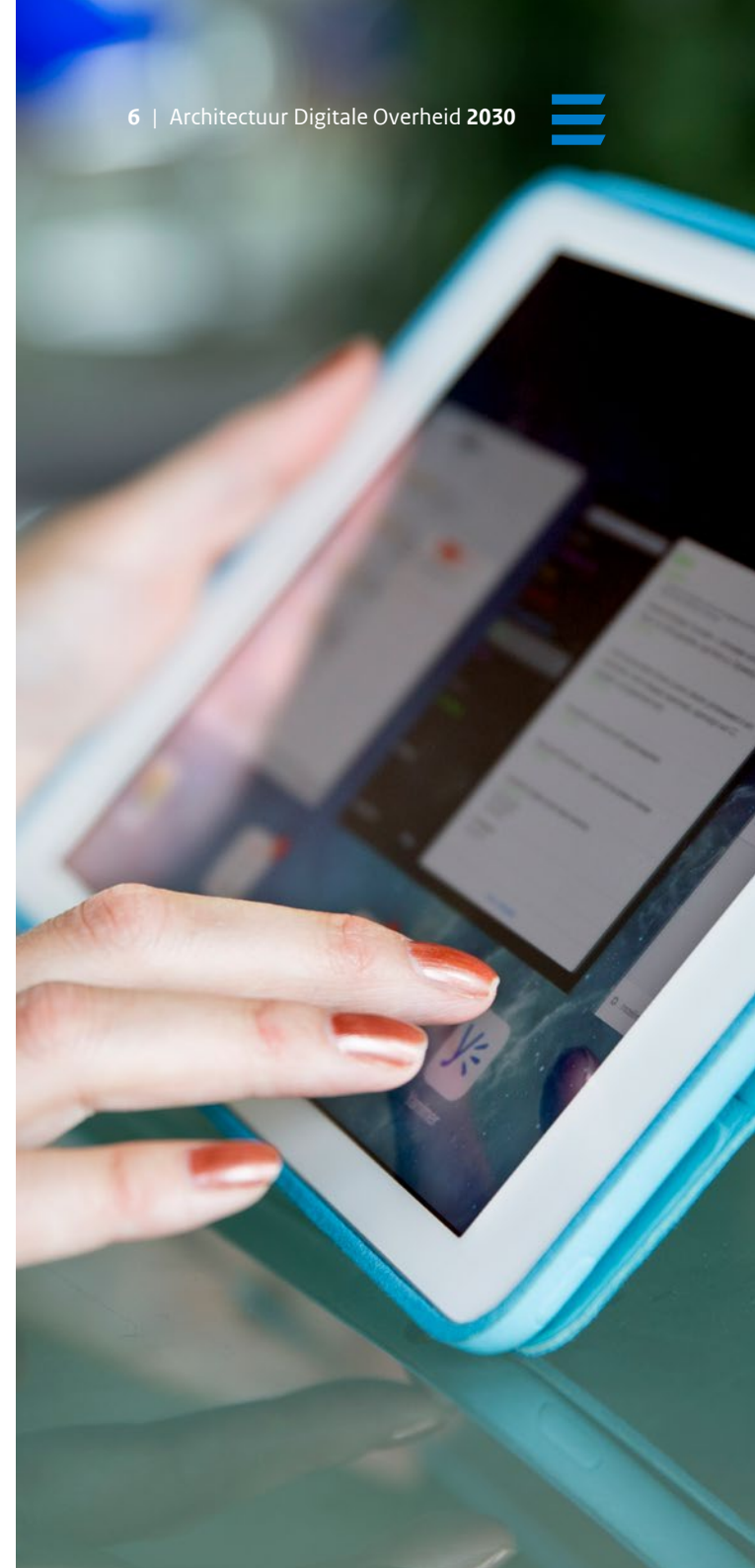
De architectuur van de Nederlandse digitale overheid in 2030 beschrijft de doelen, uitgangspunten en benodigde bouwstenen voor het creëren van een samenhangende digitale overheid. Het document beschrijft een breed toepasbare architectuur voor alle overheidsorganisaties. De organisaties kunnen het document gebruiken om hun eigen architecturen optimaal aan te laten sluiten op de architectuur van de digitale overheid en de (werkende) bouwstenen ervan.

Het document beschrijft niet de architectuur van de digitale samenleving, zoals slimme robots, hartbewaking op afstand, digitale regelaars en digitale vrachtbrieven. Het legt wel waar nodig een relatie met de architectuur van de digitale economie en de digitale samenleving. Het document is ook niet bedoeld als informatieplan voor afzonderlijke overheidsorganisaties, maar biedt wel een referentie voor het opstellen van hun eigen architecturen. Het document bevat verwijzingen naar bestaande afspraken, standaarden en voorzieningen en doet waar zinvol suggesties voor nieuwe.

Het document is dus ook een wegwijzer naar het grote aantal al beschikbare afspraken, standaarden en voorzieningen. Het geeft professionals in de overheidsorganisaties handvatten om de interactie van burgers en bedrijven met de overheid te bevorderen en om de samenwerking tussen overheidsorganisaties onderling te bevorderen. Het doel is om de ketenprocessen binnen de (digitale) overheid optimaal in te richten: van beleidsontwikkeling via uitvoering tot en met handhaving en verantwoording. Dit zorgt ervoor dat de digitale overheid voor burgers en ondernemers zo goed mogelijk werkt en leidt tot een overheid die toegankelijker, inclusiever en persoonlijker is.

Kortom: Architectuur zorgt voor afspraken, standaarden en – voor zover nodig – gemeenschappelijke voorzieningen voor de inrichting van de digitale overheid. De digitale overheidsarchitectuur geeft op een hoog niveau een kapstok voor overheidsdiensten, interoperabiliteit, gegevensuitwisselbaarheid, het gebruik van een beperkt aantal gemeenschappelijke bouwstenen, een hoog beveiligingsniveau en bescherming van privacy.

Het document bevat verder een samenvatting en in het tweede deel vanaf pagina 13 ongeveer 50 pagina's met details voor de fijnproevers. Deze details zijn gebaseerd op verschillende best practice principes. Denk daarbij aan de Nederlandse Overheids Referentie Architectuur (NORA) en het Digitale Kompas van de Europese Commissie.





2 Samenvatting

Dit document beschrijft de hoofdlijn van de verwachte architectuur van de digitale overheid in 2030.

Het document richt zich op de stand van zaken in 2030 op basis van wat we nu weten. Het document is voor bestuurders, beleidsmakers en andere geïnteresseerden. Het tweede deel vanaf pagina 13 is voor een andere doelgroep; dit is namelijk specifiek gericht op architecten.

Deze samenvatting beschrijft vooral de werking van de digitale overheid in 2030. Uiteraard is dit een inschatting. Nieuwe wetgeving, politieke prioriteiten en technologische innovaties tussen nu en 2030 beïnvloeden het beeld waarschijnlijk nog. Daarom zullen we dit document periodiek actualiseren. De meest actuele versie is te vinden op pgdi.nl/ado.

Het beleid besteedt veel aandacht aan zaken als digitale overheid, digitale samenleving, interbestuurlijke gegevensstrategie, cybersecurity en Europese ontwikkelingen. Denk daarbij aan de invoering van de datarichtlijn, de Europese digitale identiteit of de Europese wallet. Ook via programma's als Open Overheid, Werken aan Uitvoering¹, het Federatief Datastelsel, Cyber Security, Privacybescherming en het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO) werken we aan een betere informatievoorziening. Werken met een gezamenlijk beeld en architectuur helpt om fouten en herhalingen te voorkomen, de coördinatie te verbeteren en kosten te verlagen. Werken met een gezamenlijke architectuur is daarom noodzakelijk. Het draagt bij aan een betere digitale overheid voor zowel burgers als ondernemers.

In de architectuurbeschrijving gaan wij uit van het huidige beleid, bestaande bouwstenen en bestaande visie- en beleidsdocumenten. Denk aan de vastgestelde GDI-Meerjarenvisie, de Werkagenda Waardengedreven Digitaliseren² en andere bestaande visiestukken. Deze beschrijving bevat naast bestaande uitgangspunten en bouwstenen ook voorstellen voor nieuwe uitgangspunten en bouwstenen die (nog) niet op vastgesteld beleid zijn gebaseerd. Na het vaststellen van de architectuurbeschrijving is het mogelijk om hiervoor afzonderlijke beleidsvoorstellen en notities op te stellen om aan de reguliere gremia voor te leggen. Dit alles via de governance zoals beschreven in het Besluit Sturing Digitale Overheid 2022³.

Scope van de architectuurbeschrijving

Dit document heeft de digitale overheid als onderwerp. Het begrip “Digitale Overheid” is afgebakend in overeenstemming met de hoofdlijnen van het digitaliseringsbeleid⁴ en de Werkagenda. Het gaat over een digitale overheid die burgers en bedrijven centraal stelt, slagvaardig optreedt en een transparant toegankelijke dienstverlening biedt. Hierbij hoort een sterk “digitaal fundament” dat voldoet aan de belangrijke voorwaarden zoals beschreven in het digitaliseringsbeleid en de Werkagenda.

¹ In Werken aan Uitvoering is ook diepgaande analyse gemaakt van wat er beter kan. Dat geldt hier als relevant achtergrondmateriaal

² www.digitaleoverheid.nl/document/werkagenda-waardengedreven-digitaliseren

³ wetten.overheid.nl/BWBR0046935

⁴ www.rijksoverheid.nl/documenten/kamerstukken/2022/03/08/kamerbrief-hoofdlijnen-beleid-voor-digitalisering



Dit document beschrijft *niet* de architectuur van de digitale samenleving of digitale economie. Het gaat dus *niet* over onder andere *smart industry* (bijvoorbeeld slimme robots); zorg (bijvoorbeeld hartbewaking op afstand); energie (bijvoorbeeld besparing door digitale regelaars) of mobiliteit (bijvoorbeeld digitale vrachtbrieven).

Dit document is nadrukkelijk *niet* bedoeld als informatieplan, roadmap of projectenportfolio. Dat is te vinden in het jaarlijkse GDI Programmeringsplan.

Om een samenhangende digitale overheid te vormen, is het essentieel dat verantwoordelijke bestuurders en managers bewuste beslissingen nemen die daaraan bijdragen. Wetgeving geeft daartoe duidelijkheid. De architectuur van de digitale overheid is geen oplossing voor complexe wet- en regelgeving. Denk aan moeilijk leesbare toelichtingen, onduidelijke formulieren en ingewikkelde processen. Het streven naar goed uitvoerbare wet- en regelgeving en ook beleid blijft belangrijk.

Tot slot

Het is belangrijk te beseffen dat een digitale overheid vaak geen passende oplossing is voor burgers die laag- of ongeletterd zijn, de Nederlandse taal niet beheersen of anderszins niet kunnen omgaan met digitale dienstverlening. De omvang van deze groep wordt geschat op 20 á 30% van de volwassen Nederlanders. Een goede digitale overheid ondersteunt daarom alternatieve vormen van communicatie met en dienstverlening aan deze groep burgers. Vooral via direct contact tussen medewerkers van de overheid, burgers en (kleine) ondernemers. Overheidsmedewerkers moeten daarom toegang hebben tot optimale digitale ondersteuning.



3 Beeld van de digitale overheid in 2030

De overheid is van iedereen en voor iedereen. Van geboorteaangifte tot de wet op de lijkbezorging, van het stimuleren van theaterbezoek tot het bestrijden van de zware misdaad. Op veel terreinen neemt de overheid maatregelen, vaardigt zij wetten uit, en ziet zij toe op naleving.

Moderne informatiesystemen ofwel de ‘digitale overheid’ ondersteunen al deze taken en processen van de overheid steeds vaker.

Vanuit het perspectief van burgers en bedrijven is “de digitale overheid” één geheel. Voor hen is het onderscheid in afzonderlijke taken en uitvoeringsorganisaties minder belangrijk⁵. Daarom is een architectuur die de samenhang weergeeft en aangeeft wat we generiek met elkaar samen realiseren, essentieel. Dat maakt de digitale overheid voor burger en bedrijf herkenbaar en toegankelijk. Het zorgt dat publieke waarden eenduidig zichtbaar zijn. De focus van de architectuurbeschrijving van de digitale overheid ligt daarom op dit gezamenlijke deel. Wat al goed werkt, en terugkerende zaken zoals de jaarlijkse belastingaangifte moeten daarbij blijven werken zoals de burger gewend is. De behoefte aan één overheid geldt voor complexere vraagstukken en niet voor routines. De digitale overheid raakt daarmee alle burgers, bedrijven en andere organisaties inclusief overheidsorganisaties en (semi-)publieke organisaties.

Processen

We willen dat burgers en bedrijven de dienstverlening of “verplichte handelingen” als transparante, doorlopende

processen ervaren. We willen dat burgers en bedrijven het proces kunnen volgen en waar nodig kunnen bijsturen. De algemene uitgangspunten van behoorlijk bestuur en de daaruit volgende eisen uit de Algemene wet bestuursrecht moeten daarbij geborgd zijn.

Processen worden vaak digitaal ondersteund. Daarbij wordt ook gebruik gemaakt van algoritmes. Waar algoritmes belangrijk zijn voor de onderbouwing van beslissingen moet dit proces transparant zijn en moeten we dit toetsen aan de rechten van de mens en aan andere wetgeving. Mede om discriminatie en vooroordelen te voorkomen.

Data en datadeling

Data spelen een belangrijke rol in de (proactieve) beleidsontwikkeling en dienstverlening van de overheid op terreinen als klimaat, energie, huisvesting, economie, arbeidsmarkt, zorg, onderwijs en gezondheid. De toegang tot betrouwbare data voor het eigen onderzoek, de beleidsontwikkeling en de dienstverlening is dan ook van groot belang. Data leveren als zelfstandige onderdelen een belangrijke bijdrage aan het oplossen van maatschappelijke vraagstukken en het creëren van economische waarde. Vanuit de Europese Unie wordt ook stevig ingezet op

⁵ Zie b.v. *Eindrapport onderzoek overheidsdienstverlening 2020, Pieterse*. De realisatie van één landelijke website voor alle overheden waarop alle zaken met de overheid geregeld kunnen worden, is de enige innovatie die net als vorig jaar, door een meerderheid van 52% van de respondenten gewenst is.



datagedreven werken en onder meer het tot stand brengen van *dataspaces*⁶.

Verantwoord gebruik van data maakt een overheid mogelijk die niet naar de bekende weg vraagt, klantgericht is, zich niet voor de gek laat houden, weet waar ze het over heeft, haar zaken op orde heeft en niet meer uitgeeft dan nodig. Daarom willen we – om misverstanden te voorkomen – dat data goed gedefinieerd zijn en hun betekenis helder is (semantiek). We willen wildgroei en kwaliteitsverlies voorkomen door zoveel mogelijk data te hergebruiken. Data moeten daarvoor goed vindbaar zijn. Dit doen we door data waarover overheidsorganisaties beschikken zoveel mogelijk – binnen wettelijke kaders – te delen met andere overheidsorganisaties. Maar alleen als dit bijdraagt aan de dienstverlening immers, het delen van data moet in balans zijn met dataminimalisatie. We vragen gegevens waarover de overheid al beschikt, niet opnieuw uit. We maken het voor burgers en bedrijven ook mogelijk om zelf regie te nemen over het delen en uitwisselen van data, bijvoorbeeld via een Wallet⁷. Burgers, bedrijven en overheidsorganisaties moeten vermeende onjuistheden in data via eenvoudige procedures kunnen (laten) corrigeren.

De Nederlandse Basisregistraties vervullen een essentiële rol in het vastleggen en gecontroleerd beheren van data. In aanvulling daarop willen we dat organisaties aan elkaar data ter beschikking stellen vanuit “kernregistraties”.

We noemen dit het Federatief Datastelsel⁸: afspraken over het uitwisselen van data. Deze afspraken hebben betrekking op de betekenis van data (semantiek), de vastlegging en het beheer ervan en de logistiek voor de uitwisseling ervan.

We willen dat duidelijk is wat de authentieke bron is, wie de verantwoordelijke bronhouder is en wie verantwoordelijk is voor de kwaliteit van de data.

Voor een optimale samenwerking tussen overheidsorganisaties onderling willen we dat gegevens betrouwbaar zijn en we ze eenvoudig kunnen delen. We gaan uit van het idee van ‘gegevens aan de bron’, zodat andere overheidsorganisaties altijd actuele gegevens gebruiken. Hiervoor richten we een federatief datastelsel in. Voor het medegebruik van gegevens hanteren we moderne uitwisselingsstandaarden, zoals API’s.

Infrastructuur

Voor een betrouwbare informatievoorziening voor de digitale overheid is betrouwbare onderliggende infrastructuur en voorzieningen voor dagelijks gebruik nodig. We willen dat we via netwerkservices data door middel van (bij voorkeur) API’s op een snelle, betrouwbare en veilige manier kunnen uitwisselen. Keuzes worden gebaseerd op bewezen concepten (*proven technology*) en moderne

technologie (zoals bijvoorbeeld cloudtechnologie). Dit is een randvoorwaarde voor de benodigde wendbaarheid, hergebruik en kostenefficiëntie in de inrichting van de digitale overheid. Daarvoor zijn er ten minste drie wegen:

- eigen voorzieningen;
- voorzieningen in een gezamenlijk datacenter in overheidsverband of van een private partij, of;
- gebruikmaken - onder strikte voorwaarden - van een public cloud.

Apparaten zoals voertuigen, verkeersregelsystemen, pompen, poortjes, camera’s en sensoren hebben eigen waarnemings- en regelsystemen. We spreken over *smart devices of Internet of Things*. Ook de overheid beschikt steeds vaker over slimme apparaten. Al ver voor 2030 hebben we te maken met autonome apparaten gebaseerd op kunstmatige intelligentie. Daarvoor geldt ook dat “regulering” en inpassing nodig is; nieuwe EU-regelgeving legt daarvoor de basis. Software zorgt niet alleen voor een goed functioneren van deze apparaten, maar genereert ook veel data. Met deze data kunnen de apparaten op afstand in de gaten gehouden worden, en kunnen zij gekoppeld worden aan onder meer besturingssystemen. Ook kan er managementinformatie mee geproduceerd worden. We willen de controle hebben over deze systemen. Het op basis van (mogelijk verder uitgebreide) registraties kunnen identificeren van slimme apparaten, hun locatie en wie ervoor verantwoordelijk is, wordt belangrijker. We willen ook de data ontvangen die

⁶ De E.U. heeft 16 *dataspaces* gedefinieerd. Deze liggen op het terrein van de Digitale Samenleving en worden daarom hier niet verder uitgewerkt. Uiteraard kunnen ook overheidsorganisaties gebruikmaken van deze *dataspaces* en er zelf een bijdrage aan leveren.

⁷ Zie ook: www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/regie-op-gegevens

⁸ Het FDS vloeit voort uit de Interbestuurlijke Datastrategie. Zie: *Kamerbrief over Interbestuurlijke Datastrategie Nederland* | *Kamerstuk* | *Rijksoverheid.nl* en *realisatiebids.pleio.nl*



de apparaten produceren en gebruiken om datagedreven te kunnen sturen en beslissen. En we willen voorkomen dat er ongeoorloofd meegeluisterd wordt of zelfs ingebroken wordt in deze vaak cruciale systemen. Informatiebeveiliging is dan ook van groot belang.

Daarbij moet gedacht worden aan concepten als *edge computing*⁹, *robotica*, *sensing*, *SMART assets* en *digital twinning*¹⁰. Hiervoor bestaan momenteel nog geen echte bouwstenen. Richting 2030 zijn die wel nodig.

Het is noodzakelijk te kunnen beschikken over goed uitgeruste huisvesting, die voldoet aan klimaat en milieueisen, en beveiliging geeft tegen digitale en fysieke aanvallen. Dat gebeurt onder beheer van de overheid. Ook vraagt het om uitgewerkte afspraken met private aanbieders van cloudvoorzieningen vanuit hun datacentra binnen de EU, zodat specifieke overheidseisen vanuit “soevereiniteit” geborgd blijven.

Informatiebeveiliging en privacybescherming

In de architectuurbeschrijving besteden we uiteraard ook aandacht aan informatiebeveiliging en privacybescherming. Daarbij verwijzen we naar eisen die gesteld worden vanuit diverse Europese en nationale wetgeving, richtlijnen en standaarden. We moeten ons realiseren dat de bouwstenen van de digitale overheid meer en meer beschouwd worden als vitale infrastructuur, waaraan hoge eisen worden gesteld.

Als het gaat over persoonsgegevens biedt de Algemene Verordening Gegevensbescherming de kaders voor het verwerven, verwerken, delen en vernietigen van gegevens.

Samenhang

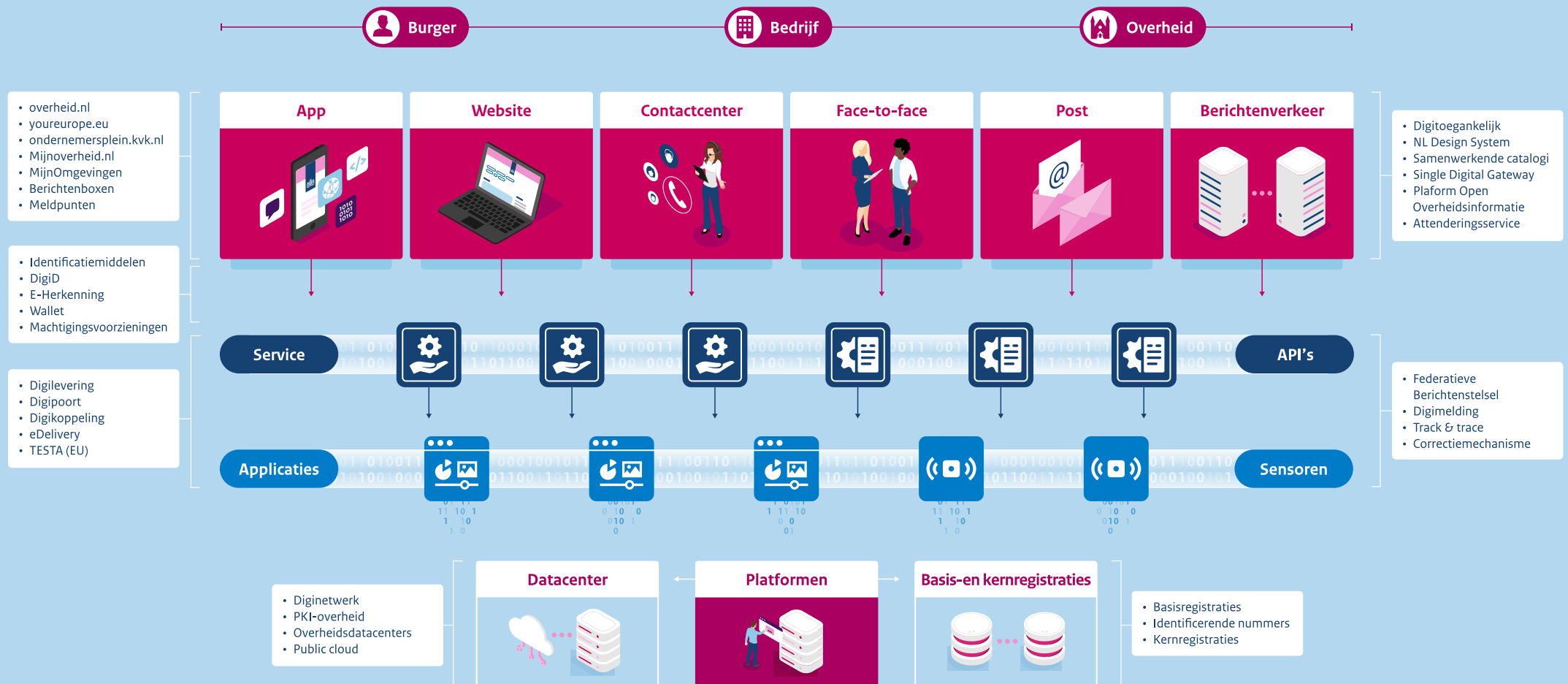
In de voorgaande paragrafen is een groot aantal voorzieningen of werkende componenten van de Digitale Overheid de revue gepasseerd. Met de nevenstaande opbouw van de architectuur, kunnen we een deel van deze voorzieningen enigszins groeperen. Het model op de volgende pagina toont een groot aantal belangrijke, vooral bestaande, voorzieningen dat invulling geeft aan de architectuur van een (werkende) digitale overheid. In een bijlage bij het architectuurdocument geven we een overzicht van ongeveer 75 bouwstenen voor de digitale overheid.

Veel voorzieningen hangen onderling samen. Met name de voorzieningen in de linker- en rechterbovenhoek van het model, kunnen niet bestaan zonder gebruik te maken van een of (vaak) meerdere voorzieningen in het midden en in de linker- en rechterhoek beneden. Door deze voorzieningen te beschouwen als ‘legoblokjes’ kan de digitale overheid vanuit verschillende verantwoordelijkheden en organisaties worden gebouwd.

⁹ Zie: www.iso.org/standard/74846.html

¹⁰ Zie onder meer: www.wijsmetlocatie.nl/wat-we-doen/digital-twin

Architectuur digitale overheid 2030





Deel 2

Voor architecten

- ▶ 1 Inleiding en afbakening
- ▶ 2 Verantwoording en vervolgstappen
- ▶ 3 Richtlijnen voor deze architectuur
- ▶ 4 Structuur
- ▶ 5 Opbouw van de architectuur
- ▶ 6 Architectuurbeschrijving
- ▶ 7 Aspectgebieden





1 Inleiding en afbakening

Dit document beschrijft de verwachte architectuur van de digitale overheid in 2030. Het richt zich op de stand van zaken in het jaar 2030 op basis van wat we nu weten. Het is geschreven voor architecten die betrokken zijn bij de inrichting van de digitale overheid.

Het document vormt een architectuurbeschrijving met daarin de concretisering van een samenhangende inrichting van de digitale overheid. Voor een goed functionerende digitale overheid zijn samenwerking en coördinatie essentieel, want data en gedigitaliseerde processen overschrijden snel de grenzen van individuele organisaties en bestuurlijke lagen.

Er wordt vanuit het beleid veel aandacht besteed aan zaken als digitale overheid, digitale samenleving, interbestuurlijke gegevensstrategie, cybersecurity en Europese ontwikkelingen zoals de invoering van de datarichtlijn, de Europese digitale identiteit en de Europese wallet. Ook via een aantal programma's wordt gewerkt aan een betere informatievoorziening, bijvoorbeeld in het kader van Open Overheid, Werken aan Uitvoering¹¹, het Federatief Datastelsel, Cyber Security, Privacybescherming en het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO). Werken met een gezamenlijke visie en architectuur helpt om divergentie, dubblures te voorkomen, coördinatie te verbeteren en kosten te verlagen. Werken met een gezamenlijke architectuur is daarom steeds noodzakelijker en draagt bij aan een betere digitale overheid voor burgers en bedrijven.

In deze architectuurbeschrijving is uitgegaan van vastgesteld beleid, bestaande bouwstenen en visie- en beleidsdocumenten. De eerder in OBDO vastgestelde

GDI-Meerjarenvisie, de Werkagenda Waardengedreven Digitaliseren¹² en de vele al bestaande visiestukken zijn als uitgangspunt bij deze beschrijving gebruikt. De GDI-Meerjarenvisie en Architectuur Digitale Overheid moeten een onderlinge wisselwerking hebben. Deze doelarchitectuur bevat naast bestaande uitgangspunten en bouwstenen ook voorstellen voor uitgangspunten en bouwstenen die niet op vastgesteld beleid zijn gebaseerd. Hiervoor zullen, na vaststelling van deze architectuur, afzonderlijke beleidsvoorstellen en beslisnotities moeten worden opgesteld en ter besluitvorming worden voorgelegd. Dit alles via de governance zoals beschreven in het Besluit Sturing Digitale Overheid 2022¹³. De voorstellen in deze architectuurbeschrijving voor nieuwe uitgangspunten en bouwstenen zijn onderstreept.

1.1 Scope van deze architectuur

De scope van deze architectuur is de digitale overheid. Dit begrip "Digitale Overheid" is afgebakend in overeenstemming met de hoofdlijnen van het digitaliseringsbeleid¹⁴ en de Werkagenda. Het gaat over een digitale overheid die burgers en bedrijven centraal stelt, slagvaardig optreedt en met een transparante houding toegankelijke dienstverlening biedt. Hierbij hoort een sterk

¹¹ In Werken aan Uitvoering is ook diepgaande analyse gemaakt van wat er beter kan. Dat geldt hier als relevant achtergrondmateriaal

¹² www.digitaleoverheid.nl/document/werkagenda-waardengedreven-digitaliseren

¹³ wetten.overheid.nl/BWBR0046935

¹⁴ www.rijksoverheid.nl/documenten/kamerstukken/2022/03/08/kamerbrief-hoofdlijnen-beleid-voor-digitalisering



“digitaal fundament” dat voldoet aan een aantal cruciale voorwaarden zoals beschreven in het digitaliseringsbeleid en de Werkagenda.

Vanuit het perspectief van burgers en bedrijven is “de digitale overheid” één geheel: voor hen is het onderscheid in afzonderlijke taken en uitvoeringsorganisaties minder belangrijk¹⁵. Daarom is een architectuur die “het generieke” en de samenhang weergeeft essentieel. Dat maakt de digitale overheid voor burger en bedrijf herkenbaar, toegankelijk en zorgt dat publieke waarden eenduidig zichtbaar zijn. De focus van deze architectuur van de digitale overheid ligt daarom op dit gezamenlijke deel. Wat al goed werkt, de vele terugkerende zaken als jaarlijkse aangifte of melden losliggende stoeptegel, moet daarbij blijven werken zoals de burger gewend is. De behoefte aan één overheid geldt veelal voor complexere vraagstukken en niet voor routines.

Het document hanteert bewust een bredere scope dan de Generieke Digitale Infrastructuur (GDI)¹⁶. Deze brede scope is nodig, omdat de digitale overheid die burgers en bedrijven ervaren is opgebouwd uit veel meer componenten dan alleen de GDI. Het document biedt de basis om te kunnen sturen op de bijdrage van GDI-bouwstenen aan de digitale overheid en om de GDI-bouwstenen te kunnen positioneren

ten opzichte van elkaar en ten opzichte van andere componenten van de digitale overheid.

Dit document beschrijft *niet* de architectuur van de digitale samenleving of digitale economie, waarbij het gaat om onder andere *smart industry* (bijvoorbeeld slimme robots); zorg (bijvoorbeeld hartbewaking op afstand); energie (bijvoorbeeld besparing door digitale regelaars) of mobiliteit (bijvoorbeeld digitale vrachtbrieven). Waar nodig wordt wel een relatie gelegd met die architecturen van de digitale economie en de digitale samenleving¹⁷.

1.2 Rol van bestaande bouwstenen in deze architectuurbeschrijving

In dit document wordt verwezen naar bestaande bouwstenen van de digitale overheid. We beginnen niet vanaf een nulpunt; er is al veel. Functionaliteiten¹⁸ van de digitale overheid die waarschijnlijk nog wel een jaar of acht “mee zullen gaan”, bepalen mede de keuzes in dit document. Onder bouwsteen verstaan we in het kader van de GDI-afspraken, standaarden en/of voorzieningen. Daarbij

geldt dat afspraken voor standaarden gaan en deze voor voorzieningen. Vaak is een bouwsteen een combinatie van afspraken, standaarden en voorzieningen¹⁹.

Het benoemen van bestaande bouwstenen heeft als doel om concreet en begrijpelijk te zijn. Het gaat daarbij om de functionele bijdrage die deze bouwstenen leveren, niet om de huidige opbouw en technische implementatie. In 2030 zullen deze bouwstenen uiteraard doorontwikkeld zijn, o.a. op basis van de toenemende aandacht voor lifecyclemanagement, nieuwe wetgeving etc. Ook kan het zijn dat bepaalde bouwstenen van voorziening verschuiven naar meer op afspraken en standaarden gebaseerde oplossingen of omgekeerd. In dit document worden de afzonderlijke bouwstenen (afspraken, standaarden en voorzieningen) niet nader uitgewerkt. Dat gebeurt in andere documenten.

1.3 Relatie tot andere bronnen

Voor deze architectuur is gebruik gemaakt de Nederlandse Overheid Referentie Architectuur (NORA) en haar ‘dochteren’. Het is een concretisering van de NORA: enerzijds door in meer detail aan te geven hoe de digitale overheid er in

¹⁵ Zie b.v. *Eindrapport onderzoek overheidsdienstverlening 2020, Pieterse*. De realisatie van één landelijke website voor alle overheden waarop alle zaken met de overheid geregeld kunnen worden, is de enige innovatie die net als vorig jaar, door een meerderheid van 52% van de respondenten gewenst is.

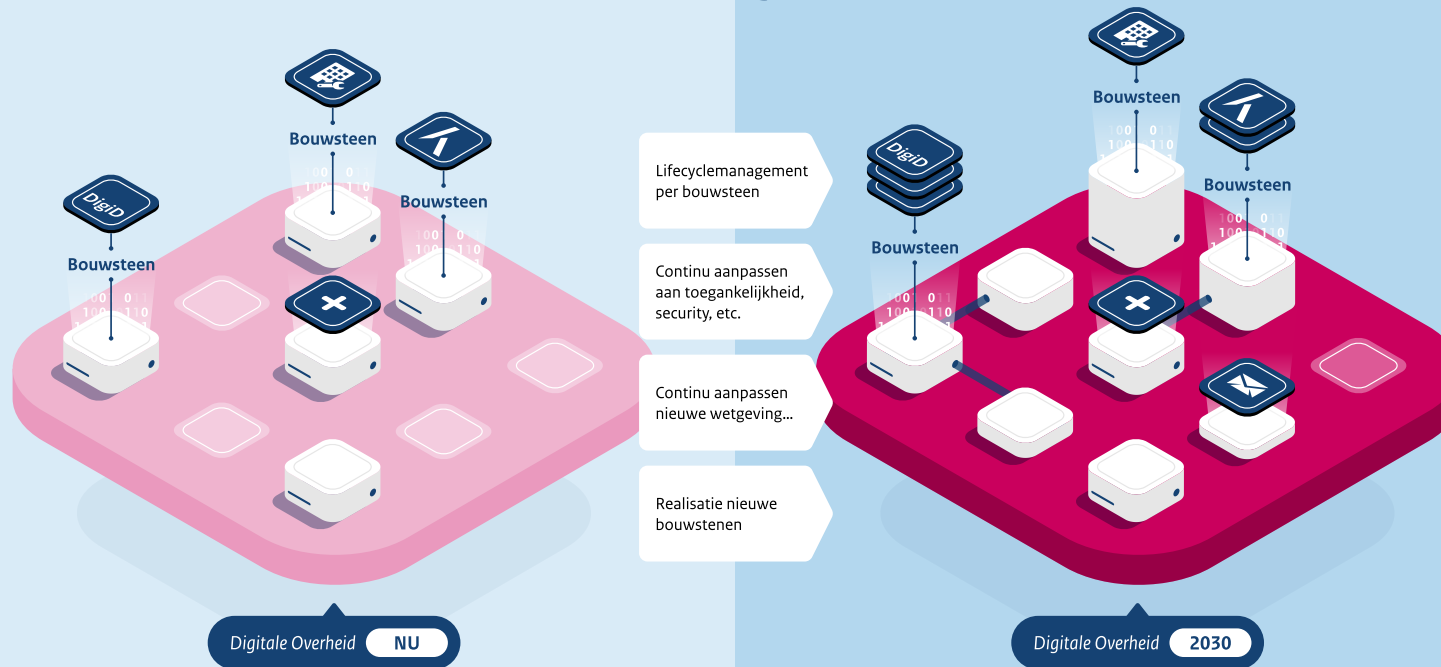
¹⁶ In de meerjarenvisie GDI 2022 – 2026 is de huidige afbakening van de GDI vastgelegd, onder verwijzing naar afwegingskader GDI, MIDO-kader en kamerbrief 6643 nr. 706.

¹⁷ Zie: www.rijksoverheid.nl/documenten/rapporten/2022/11/18/rapport-strategie-digitale-economie en de constatering in het digitaliseringsbeleid dat digitaal fundament, digitale overheid, samenleving en economie “sterk vervlochten” zijn

¹⁸ In bijvoorbeeld kamerstukken 26 643 Nr. 706, 13 juli 2020, duidt “functionaliteiten” de bouwstenen in nog algemenere zin aan. In termen van architectenraamwerken als Togaf en Archimate wordt dit verstaan als “Capability”, het gedrag van het “systeem” ten behoeve van de buitenwereld, het “wat het doet”. Zie hoofdstuk 4 en pubs.opengroup.org/togaf-standard/business-architecture/business-capabilities.html

¹⁹ De term GDI-bouwsteen is gedefinieerd in het Besluit Sturing Digitale Overheid 2022. Het is geen strikt architectuurbegrip. Het kan met enige voorzichtigheid geassocieerd worden met het in Togaf gedefinieerde Architectural Building Block. Het subtype “voorziening” kan geassocieerd worden met Solution Building Block. Zie TOGAF Standard v10 — Introduction and Core Concepts § 3.6.

Doorontwikkeling op weg naar betere GDI voor een betere digitale overheid



Dit document geeft een architectuurbeschrijving van de digitale overheid in 2030 en in het bijzonder van de bouwstenen waaruit deze bestaat. Waar deze functionaliteiten al bestaan wordt dit gedaan aan de hand van bestaande bouwstenen, zodat herkenbaar en concreet is waar het om gaat. In 2030 zal dat een doorontwikkelde versie van die bouwsteen betreffen. "Lifecyclemanagement" en het continu aanpassen aan kaders en standaarden werkt door in de 2030 situatie. Waar in dit document dus over bijvoorbeeld "DigiD" gesproken wordt, betreft dit de versie van DigiD zoals die in 2030 zal bestaan en niet exact de huidige. ("BAG": Basisregistratie Adressen en Gebouwen, MO/BB: MijnOverheid / Berichtenbox).



2030 uit zal zien en anderzijds door delen van de referentiearchitectuur te vertalen naar doelarchitectuur. Bij de uitwerking is ook gebruik gemaakt van architecturen die zijn opgesteld voor overheidssectoren en voor thema's binnen de digitale overheid.

Het document bevat vele verwijzingen naar wetgeving, bestaand beleid en verdiepende informatie bij de verschillende onderwerpen. In die zin is het een gids voor iedereen die bijdraagt aan het tot stand brengen van een goed functionerende digitale overheid en daar met architecturale bril naar wil kijken. De verwijzingen zorgen ervoor dat de tekst van dit document compact blijft, doublures en afwijkingen worden voorkomen en steeds verwezen wordt naar de jongste versie van de uitwerking.

Het document is geen alternatief voor enterprise-architecturen van afzonderlijke overheidsorganisaties, zoals ministeries, provincies, gemeenten, waterschappen of uitvoeringsorganisaties en organisaties met een publieke taak, zoals pensioenfondsen²⁰. Deze overheidsorganisaties blijven zelf verantwoordelijk voor het verwerken van de veranderingen ten gevolge van digitalisering, de doorwerking van de verwachtingen van burgers in de eigen architecturen.

De beschrijving van de architectuur van de digitale overheid is nadrukkelijk *niet* bedoeld als informatieplan, roadmap of projectenportfolio. Er is een duidelijk onderscheid met het jaarlijkse GDI Programmeringsplan. Programma's en projecten die nodig zijn om van de bestaande situatie tot de gewenste situatie in 2030 te komen horen in het jaarlijkse

Programmeringsplan. Voorstellen en programma's worden daarbij getoetst aan de architectuur om de samenhang te bewaken, doublures te voorkomen en goede besluitvorming te ondersteunen.

1.4 Tot slot

Het is belangrijk te beseffen dat een digitale overheid vaak geen adequate oplossing is voor de groep burgers die laag- of ongeletterd zijn, de Nederlandse taal niet beheersen of anderszins niet in staat zijn om te gaan met digitale dienstverlening. De omvang van deze groep wordt geschat op 20 á 30% van de volwassen Nederlanders. Een goede digitale overheid ondersteunt alternatieve vormen van communicatie met en dienstverlening aan deze (groeierende) groep burgers. Dit "kanaal" vereist evengoed digitale ondersteuning.

Een meer samenhangende digitale overheid kan alleen gerealiseerd worden als uitvoeringsbesluiten en keuzes van verantwoordelijke bestuurders en managers binnen overheidsorganisaties daaraan bijdragen. Wetgeving geeft daartoe duidelijkheid. In de verdere uitwerking is het adopteren van de uitgangspunten en bouwstenen van de digitale overheid nodig. ArchitectuurdOCUMENTEN als deze dragen daaraan bij door inzicht in de samenhang te geven. We dienen ons ook te realiseren dat de architectuur van de digitale overheid geen remedie is tegen complexe wet- en regelgeving met als gevolg moeilijk leesbare toelichtingen, onduidelijke formulieren en ingewikkelde processen. Het streven naar goed uitvoerbare wet- en regelgeving en ook beleid blijft van groot belang.

²⁰ Ter wille van de leesbaarheid spreken we in dit document verder gemakshalve over overheidsorganisaties.



2 Verantwoording en vervolgstappen

Deze architectuur is tot stand gekomen via het MIDO werkproces. Na vaststelling van de huidige versie is in de Architectuurraad een proces voor het actueel houden afgesproken en zijn vervolgstappen in gang gezet. Bureau MIDO voert de eindredactie van het document uit.

Deze architectuur²¹ is het product van bijdragen van de overkoepelende werkgroep van de Architectuurraad en van een grote groep betrokkenen. Bureau MIDO voert de eindredactie van het document uit. Zie bijlage 4.

De eerste conceptversies van het document zijn besproken in de overkoepelende werkgroep. Een eerste toelichting is verzorgd voor leden van de Architectuurraad en voorzitters van de Programmeringstafels van het Meerjarenprogramma Infrastructuur Digitale Overheid (MIDO) en voor medewerkers van de Directie Digitale Overheid van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Dit is gevolgd door een brede reviewronde in de NORA-community, de architectuurwerkgroepen van de Architectuurraad, programma's en projecten in de digitale overheid en andere geïnteresseerden. Hiervoor is een grondig reviewproces ingericht. De reacties tijdens deze besprekingen en toelichtingen zijn verwerkt en vervolgens besproken in de Architectuurraad²². In deze versie zijn enkele verdere aanpassingen gedaan na bespreking in de Architectuurraad. Na goedkeuring hiervan door de Architectuurraad op 28 augustus 2023 is de architectuur toegelicht in de Programmeringsraad Generieke Digitale Infrastructuur (PGDI) en op 21 september 2023 is het document vastgesteld in het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). Op basis van de in de Architectuurraad van 2 oktober 2023 goedgekeurde

procedure zal dit document steeds geactualiseerd worden. De actuele versie zal steeds gepubliceerd worden op pgdi.nl/ado.

Daarmee vormt deze versie een eerste vastgestelde doelarchitectuur: een versie die voor de komende periode overzicht biedt en op basis van regelmatige herijking overzicht blijft bieden op weg naar 2030.

Dit document is geschreven voor bedrijfs- en informatie-architecten. Het dient als basis voor andere documenten, zoals:

- Een voor een breed publiek toegankelijke versie, bijvoorbeeld een grafische of audiovisuele weergave.
- Notities voor de hiervoor genoemde beleids- en beslisvoorstellen in het document.
- Thematische architectuuruitwerkingen waarin – voor zover nodig – de vertaling plaatsvindt van de in dit document benoemde bouwstenen naar afspraken, standaarden en voorzieningen.

Omdat onze samenleving, de wetgeving, de uitvoeringspraktijk en de technologie niet stil staan, ligt het in de bedoeling om met regelmaat via nader af te spreken procedures geactualiseerde versies van deze architectuur digitale overheid op te stellen en vast te stellen.

²¹ Conform de internationale Togaf architectuurstandaard vormt deze architectuurbeschrijving van de toekomstige / 2030 situatie een doelarchitectuur, nl. “de architectuurbeschrijving van een toekomstige stand van zaken” The Open Group Standard TOGAF® Standard — Introduction and Core Concepts § 4.78.

²² Zie het verslag in 1 minuut van de Architectuurraad op 12 juni 2023: <https://pgdi.nl/architectuurraad>.



3 Richtlijnen voor deze architectuur

Een brede context heeft richting
gegeven aan deze architectuur.
Bijvoorbeeld: Europees beleid,
nationale wetgeving en beleid,
de Werkagenda Waardengedreven
Digitaliseren, de Meerjarenvisie
GDI en de NORA.

Bij het opstellen van de architectuur van de digitale overheid zijn de volgende richtlijnen van belang:

- Het doel van de beschrijving van de architectuur van de digitale overheid is het bieden van overzicht over de samenhang tussen bouwstenen van de digitale overheid. We nemen daarbij het jaar 2030 als richtpunt.
- Dit document beoogt samenhang aan te brengen tussen uitgangspunten en architecturale keuzes in de NORA en de vele programma's en projecten, die bijdragen aan het tot stand komen van de digitale overheid, zoals de Interbestuurlijke Datastrategie, Open Overheid en Werk aan Uitvoering. Het is een actualisering en nadere uitwerking van de GDI-architectuur²³.
- De architecturale keuzes en standaarden in dit document zijn – naast alle overheidsorganisaties – ook van belang voor organisaties die een rol spelen in het in praktische zin realiseren van de digitale overheid, waaronder Logius, RINIS, overheidsdatacenters, BKWI, Inlichtingenbureau, NICTIZ en private ICT-dienstverleners.
- Dit document biedt een basis voor een **afgeleide** versie voor een breed publiek (incl. managers en bestuurders).
- Onderdelen van deze architectuur van de digitale overheid kunnen meer diepgaand worden uitgewerkt in meer vakmatige documenten voor architecten en

ontwerpers. In het vervolgproces met de werkgroepen per domein zal worden bepaald waar dit aan de orde is. Doel is een continu proces van samenhang bewaken tussen globale documenten op het niveau van deze architectuur en specifieke onderwerpen die een groter detailniveau vragen.

- Als inhoudelijke kaders en uitgangspunten voor dit document gelden met name:
 - Nationale ontwikkelingen in wet- en regelgeving, zoals de Wet Digitale Overheid²⁴, Wet Open Overheid, Wet Hergebruik Overheidsinformatie en de Wet Modernisering Elektronisch Bestuurlijk Verkeer²⁵;
 - De Werkagenda Waardengedreven Digitaliseren²⁶;
 - De Interbestuurlijke Datastrategie (IBDS); in het bijzonder wat daar is opgenomen over verantwoord datagebruik:
 - Integraal en afgewogen datagebruik door de overheid, waarbij de potentie van data op een verantwoorde manier wordt benut voor maatschappelijke opgaven.
 - Opbouw van systeemfuncties of voorzieningen die het makkelijker maken om binnen de overheid datagedreven te werken.

²³ Zoals eerder in OBDO vastgesteld en gepubliceerd op [www.noraonline.nl/wiki/GDI-Architectuur_\(GA\)\)](http://www.noraonline.nl/wiki/GDI-Architectuur_(GA)))

²⁴ Het belang van deze wet is niet alleen de inhoud van de nu aangenomen eerste tranche, maar ook dat er daarmee een aanknopingspunt gerealiseerd is voor verdere wetgeving aangaande de Digitale Overheid; waarover uiteraard nog besloten moet worden.

²⁵ Zie www.noraonline.nl/wiki/Beleidskaders voor overzicht van al geldende wetgeving en beleidskaders

²⁶ www.digitaleoverheid.nl/document/werkagenda-waardengedreven-digitaliseren/ Onder de kopjes "Wat willen we?" verderop in dit Architectuurdocument zijn delen van deze Werkagenda overgenomen.



- Waardecreatie in de domeinen, door inzage te bieden in de belangrijkste datatoepassingen per domein.
- De Meerjarenvisie GDI (2022) ²⁷, in het bijzonder:
 - Afspraken gaan voor standaarden en die gaan voor generieke voorzieningen.
 - Marktconforme standaarden worden toegepast. Het mechanisme van Forum Standaardisatie is daarvoor leidend.
 - Waar mogelijk benut en stimuleert de overheid het gebruik van open source conform de beleidslijn “Open, tenzij”²⁸ de Woo en Wdo.
 - Hergebruik en harmonisatie van begrippen, en waar dat niet kan inzicht geven in de samenhang tussen begrippen.
 - Dataminimalisatie: delen van informatie daar waar het delen van het ruwe basisgegevens niet nodig is.
 - Delen van de GDI zijn vitale infrastructuur²⁹.
- Initiatieven en kaders vanuit de Europese Commissie, met name:
 - **het Digitale Kompas**, de in 2021 gepresenteerde visie, strategie en routekaart voor de digitale transformatie van Europa tot 2030.
 - Al aangenomen wetsvoorstellen, zoals de **Single Digital Gateway** (SDG), de **Cyber Security Act**, de **Data Governance Act**, **Digital Markets Act** en **Digital Services Act**.
 - Wetsvoorstellen waarover nog wordt onderhandeld, zoals de **Artificial Intelligence Act**, de **Data Act**, de



Interoperability Act, de **ePrivacy Act** en de nieuwe **eIDAS2-Verordening**. Via de komst van de Europese **Cyber Resilience Act** wordt gewerkt aan een kader voor cybersecurityeisen aan ICT-producten en -diensten op de Europese markt. Recent publiceerde de Commissie daarnaast een **verklaring voor digitale grondrechten en beginselen**.

²⁷ Zie: www.tweedekamer.nl/kamerstukken/detail?id=2022D51673&did=2022D51673

²⁸ www.digitaleoverheid.nl/document/kamerbrief-over-vrijgeven-broncode-overheidssoftware

²⁹ Uitgangspunt uit MIDO-kader, tevens gevolg van EU Cybersecurity Act



4 Structuur

Paragraafindeling, gelaagdheid en het gebruik van het begrip bouwsteen sluiten aan op gangbare architectuurmodellen en worden hier geïntroduceerd.

In dit document kiezen we voor de volgende indeling:

Bedrijfsarchitectuur

- Diensten en producten
- Kanalen
- Organisatie
- Processen
- Bedrijfsfuncties

Informatie-architectuur (Information systems architecture)

- Api's / Services
- Applicaties
- Berichtenverkeer / gegevensuitwisseling
- Data / gegevens

Technische architectuur (Technical architecture)

- Netwerken
- Platformen voor dagelijkse exploitatie
- Huisvesting
- Slimme apparaten

Aspectgebieden

- Privacybescherming, Informatiebeveiliging, Software-ontwikkeling, Beheer en exploitatie

Deze 'proven' indeling is tegen een stootje bestand, want gebaseerd op inzichten van de internationale architectuurcommunity. De vier domeinen van de GDI, Toegang, Interactie, Gegevensuitwisseling en Infrastructuur, zitten hierin en er is ruimte voor data en diensten en

andere onderwerpen die samen een volledige beschrijving van de architectuur van de digitale overheidsarchitectuur geven, zoals de aspecten informatiebeveiliging en privacybescherming.

Bovenstaande indeling is meer gelaagd. De bedrijfsarchitectuur behandelt zaken abstracter dan de informatie-architectuur en verder. Met andere woorden: Deze Architectuur Digitale Overheid gaat uit van een holistisch perspectief op de architectuur van de digitale overheid en werkt toe naar een gelaagde beschrijving die bijdraagt aan scheiden van architectuur op hoofdlijnen en detailontwerp.

Hoewel "bouwsteen" een belangrijk begrip is in GDI-kader komt dit concept niet 1:1 overeen met een item uit deze structuur. Bovendien bestaan bouwstenen ook uit afspraken en standaarden, wat in deze structuur geen aparte gezichtspunten zijn, maar waar relevant expliciet aangeduid wordt.

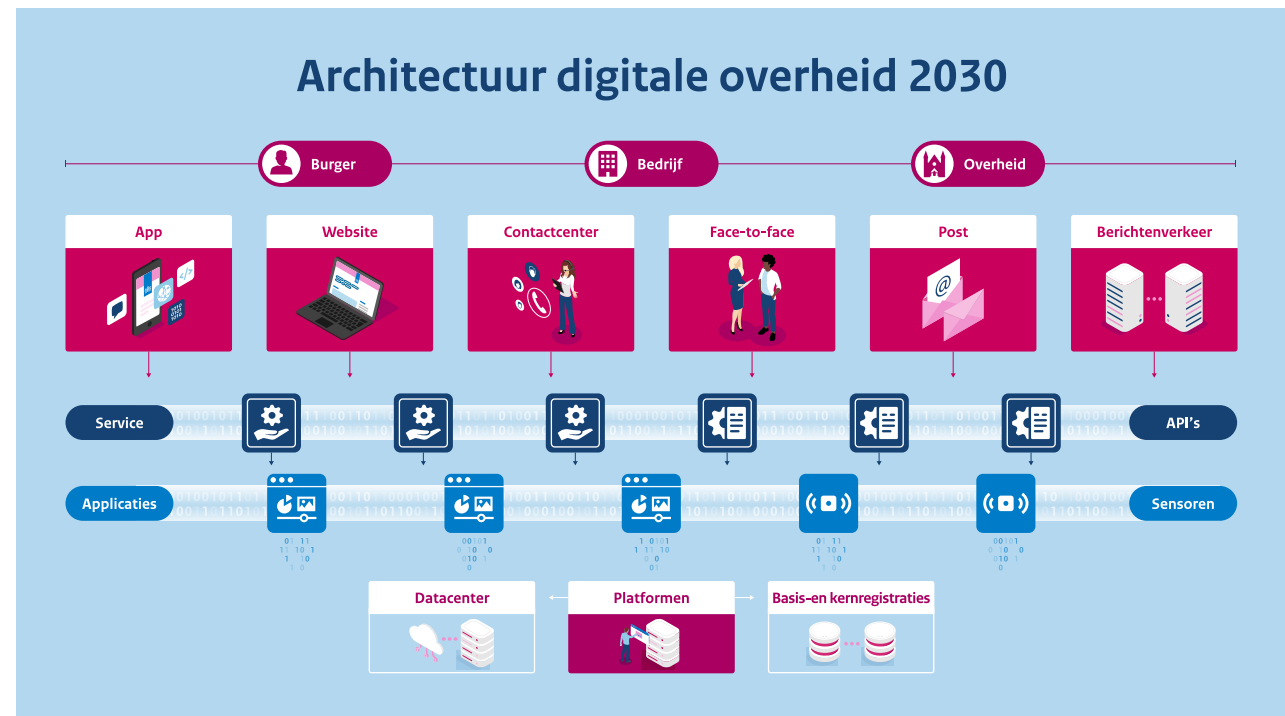
Deze architectuur bevat niet alleen bestaande beleidskeuzes en bouwstenen. Waar nodig worden nieuwe beleidskeuzes en bouwstenen³⁰ voorgesteld voor witte vlekken in de gewenste situatie. Dit is noodzakelijk om te komen consistentie in het ontwerp van de digitale overheid. Voorstellen waarover nog niet besloten is, zijn onderstreept. Voorstellen hieromtrent, op initiatief van bijvoorbeeld BZK of de Programmeringstafels GDI, volgen de gebruikelijke governance en besluitvorming³¹.

³⁰ De items die in de lijsten met bouwstenen zijn opgenomen beperken zich derhalve niet tot GDI-bouwstenen in strikte zin.

³¹ Zie vastlegging governance in Besluit Digitale Overheid wetten.overheid.nl/BWBR0046935

5 Opbouw van de architectuur

Om de samenhang tussen de bouwstenen van de digitale overheid inzichtelijk te maken, hanteren we in dit document het globale model hiernaast.



De gelaagdheid in de opbouw van de architectuur is herkenbaar; de blauwe lijntjes staan voor uitwisseling tussen de verschillende lagen in het schema. De blauwe 'tonnetjes' staan symbool voor de data laag, die ingevuld wordt door middel van de Nederlandse Basisregistraties en kernregistraties in het kader van het Federatief Datastelsel. Aangezien overheden steeds meer informatie uit apparaten halen (sensoren, poortjes, pompen, verkeerscirculatie-

systemen en deze informatie ook benutten in digital twins³²), is dat meegenomen. De lagen in dit model kunnen gezien worden als een (vereenvoudigde) grafische weergave van de eerder geïntroduceerde structuur van dit document. Het model blijkt in de praktijk verhelderend te werken voor bestuurders en managers om beter zicht te krijgen op de samenhang tussen de verschillende bouwstenen die samen de digitale overheid vormen.

³² Soms worden deze ontwikkelingen ook wel samengevat met de term Internet of Things.



6 Architectuurbeschrijving

Bedrijfsarchitectuur, informatie-architectuur en technische architectuur worden beschreven met per onderwerp de opbouw wat willen we?, uitgangspunten en bestaande en beoogde bouwstenen.

De beschrijving van de architectuur hanteert de volgende indeling:

- Beschrijving van bestuurlijke doelen bij het betreffende onderwerp (*Wat willen we?*)
- Vertaling van bestuurlijke doelen in uitgangspunten.
- Beschrijven van de wijze waarop de bestuurlijke doelen, via toe te passen bouwstenen worden bereikt.

Dit alles verrijkt met de nodige verwijzingen naar bestaande documenten en uitwerkingen van standaarden, waardoor dit document leesbaar blijft en de bronnen waarnaar verwezen wordt, actueel blijven.

6.1 Bedrijfsarchitectuur

Gesprekken in bestuurlijke gremia, zoals de 2e Kamer, Gemeenteraden of Raden van Bestuur van grote uitvoeringsinstellingen, hebben voornamelijk betrekking op de functionele aspecten van de werking van de digitale overheid. Het gaat dan om de aard van de (digitale) dienstverlening, de samenwerking met andere overheidsorganisaties of het zorgen voor een adequate informatiebeveiliging of privacybescherming. Het gaat, met andere woorden, over de werking van de digitale overheid.

6.1.1 Op wie is de digitale overheid gericht? Burgers, bedrijven, overheidsorganisaties

De overheid is van iedereen, voor iedereen, altijd, overal. Van geboorteaangifte tot de wet op de lijkbezorging, van het stimuleren van theaterbezoek tot het bestrijden van de zware misdaad. Op tal van terreinen neemt de overheid maatregelen, vaardigt wetten uit, ziet toe op

naleving. Al deze taken en processen van de overheid worden in toenemende mate ondersteund met moderne informatiesystemen ofwel door de 'digitale overheid'.

De digitale overheid raakt daarmee alle burgers, bedrijven en overheidsorganisaties. In Europees en internationaal verband kan het ook gaan om burgers en bedrijven die zich in het buitenland bevinden of publieke organisaties die internationaal samenwerken. Uiteraard zijn hierbinnen subgroepen te onderkennen: Niet alle burgers en bedrijven maken gebruik van alle diensten. Niet iedereen beschikt over mogelijkheden om digitaal diensten af te nemen. Burgers, bedrijven en andere organisaties kunnen nu eens afnemer van overheidsdiensten zijn, dan weer samenwerkingspartner of leverancier van gegevens, goederen of diensten.

In dit document houden we de indeling van betrokkenen beperkt tot drie hoofdgroepen: burgers, bedrijven en instellingen met een publieke taak. Bij verdere verdieping van onderdelen van deze Architectuur Digitale Overheid kan het noodzakelijk zijn tot een verdere onderverdeling van betrokkenen te komen.

6.1.2 Diensten en producten

> Wat willen we?

We willen dat 'iedereen mee kan doen in het digitale tijdperk, iedereen de digitale wereld kan vertrouwen en iedereen regie heeft op het digitale leven'³³. We willen dat het perspectief van burgers en bedrijven leidend is en de publieke digitale diensten en producten beschikbaar, veilig en gemakkelijk in gebruik zijn. We willen hoogwaardige, inclusieve diensten en producten verlenen, die voor burgers



en bedrijven goed vindbaar zijn. Overheidsorganisaties bieden een groot scala producten en diensten aan. We willen dat producten en diensten goed op elkaar zijn afgestemd. We willen dat burgers en bedrijven gaan ervaren dat verschillende overheden en uitvoeringsorganisaties steeds meer als één overheid optreden. Burgers willen één (digitaal) overheidsloket voor verlening van diensten en producten³⁴. We willen een digitale overheid die aan publieke waarden voldoet die uniform voor alle diensten en producten gelden.

Tegelijk willen we dat een specifieke dienst van de overheid goed wordt uitgevoerd door de daarvoor aangewezen organisatie, met kwaliteit, specifieke kennis van zaken en kostenefficiënt. Producten en diensten van de digitale overheid hebben dus zowel een generiek aspect als een specifiek aspect. Bovendien nemen overheidsorganisaties allerlei diensten bij elkaar af om daarmee burger en bedrijf ten dienste te staan; de meeste dienstverlening vindt plaats in keten- of netwerkverband. Het digitale overheidsbeleid en de GDI richten zich op het generieke aspect, inclusief de noodzakelijke afspraken over ketens en de standaarden voor netwerksamenwerking. Dit doet niets af aan het belang van hoogwaardige uitvoering van iedere specifieke dienst en de inzet daarvoor van betreffende overheidsorganisatie. Wat we willen, wat burgers en bedrijven willen betekent dat het specifieke soms aangepast moet worden aan

dit algemene belang. In toenemende mate geldt dit ook over onze landsgrenzen heen. De Single Digital Gateway (SDG-verordening, zie [youreurope.eu](https://your.europa.eu)) bevordert de ontwikkeling van een overheidsbrede set van afspraken over overheidsdiensten en producten, naamgeving en uitwisselbaarheid ervan en de eIDAS2 verordening introduceert een wallet en verdere interoperabiliteit van toegangsmiddelen.

Interactie met 1 Overheid en eenduidige Toegang

1 overheidsbeleving: Gestreefd wordt naar één digitale plek met overheidsbrede informatie over publieke producten en diensten in 2025³⁵. Proactieve dienstverlening gericht op het voorkomen van problemen bij burgers of ondernemers en ten tweede dienstverlening die georganiseerd is vanuit het perspectief van burgers en bedrijven o.a. aan de hand van levensgebeurtenissen³⁶. Waar relevant levert dit de burger een “één overheidsbeleving”³⁷. SDG verplicht hiertoe voor een beperkte set overheidsdiensten.

Samenhangende communicatie: We willen dat burgers en bedrijven op één plek overzicht hebben van alle berichten die ze van de overheid ontvangen en dat ze bij ieder bericht een handelingsperspectief geboden wordt om direct te reageren³⁸. Dit vraagt het aan de gehele overheid kunnen aangeven van communicatievoorkeuren; dat burgers en

bedrijven op één plek aan kunnen geven op welke wijze zij berichten van de overheid willen ontvangen.

Geïntegreerde communicatie: Bedrijven en organisaties willen massale veel voorkomende berichtstromen gestandaardiseerd afhandelen geïntegreerd met hun bedrijfssystemen, veelal uitbesteed aan intermediairs.

Eén toegangstelsel: We willen de digitale toegang tot overheidsdienstverlening generiek inrichten zodat alle burgers en bedrijven met één of meer generieke identificatiemiddelen eenvoudig toegang verkrijgen tot elektronische diensten en producten van zowel de overheid als van private aanbieders; e.e.a. conform eIDAS verordening en de ontwikkeling daarvan. Het toegangstelsel maakt gebruik van het stelsel van identificerende nummers en wettelijke identificatiemiddelen.

Uniform machtigen en vertegenwoordigen: We willen dat burgers en bedrijven zich digitaal kunnen laten vertegenwoordigen voor alle diensten en producten.

Regie op Gegevens³⁹

Inzicht in gegevens over jezelf: We willen de informatiepositie van burgers en bedrijven ten opzichte van de overheid

³⁴ Zie ook onder meer www.werkaanuitvoering.nl/dienstverlening/overheidsbrede-loketten en GDI meerjarenvisie die stelt dat dit “een van de belangrijkste wensen van burgers en bedrijven is”

³⁵ Werkagenda Waardengedreven Digitaliseren, § 1.2 met daar duidelijk gedefinieerde acties 1.2.1, 1.2.4, 1.2.6.

³⁶ Nieuwe beleidsinitiatieven om de dienstverlening fundamenteeler proactief te maken zijn in ontwikkeling en de consequenties daarvan zijn in deze architectuurbeschrijving nog niet doorgevoerd; reikt naar verwachting verder dan 2030.

³⁷ Zie *Kamerbrief stand van zaken 1 overheid-beleving (nov 2022)*

³⁸ De gedachte dat een burger die “mail” krijgt een “reply” wil kunnen geven ligt voor de hand. Voor bepaalde hoog volume stromen zoals aangiften bestaan er “handelingsperspectieven” om meer gestructureerd te antwoorden en zo ook bij hoog volume responsief te kunnen blijven naar burger of bedrijf.

³⁹ Met dank aan Frans de Kok (Logius) voor sterk verbeterde volgorde op dit punt



sterk verbeteren zodat zij meer grip op en inzicht in hun persoonsgebonden gegevens hebben.

We willen dat burgers en bedrijven op eenduidige en eenvoudige manier overzicht hebben via welke intermediairs zij met welke dienstverleners gegevens delen c.q. hebben gedeeld, en waar zij moeten zijn om hun toestemming voor het delen van gegevens in te trekken.

Hergebruik gegevens: Een bijzonder aspect betreft ‘regie op gegevens’ in de zin van iets kunnen doen met gegevens die de overheid over je verzameld heeft. Naast inzien en correctie gaat het ook om hergebruik van die gegevens bij andere partijen dan de overheid die ze primair heeft vastgelegd.

Wallet: We willen dat iedereen veilig, privacy vriendelijk, toegankelijk en betrouwbaar een of meerdere ID-wallets⁴⁰ zowel publiek als privaat kan gebruiken om hiermee eenvoudig online en offline digitaal zaken te doen (zoals identificeren, authenticeren, gegevens delen, handtekeningen zetten en decentraal autorisaties beheren).

Verantwoord datagebruik en ruimer meervoudig gebruik gegevens: We willen dat overheidsorganisaties zich volledig aan de Avg houden en dat er goede afspraken zijn over breed te benutten gegevens en de gebruikte algoritmes⁴¹. Het verbeteren van de afspraken hierover is nodig om de bovengenoemde “regie op gegevens” diensten mogelijk te maken. Onnodige barrières, die niet bijdragen aan gerechtvaardigde privacybescherming, tegen meervoudig gebruik van data moeten worden opgeheven⁴². Op basis van SDG-verordening moet dit ook Europa-breed gaan werken, inclusief de doorwerking van de Verordening gegevensbeheer (DGA) en toekomstige Data Verordening (DA).

Transparante Overheid

Open overheid: Burgers, (media-)organisaties en parlement krijgen inzicht in het handelen en de besluiten van de overheid, en de beweegredenen daarachter. Op verzoek én proactief. Om de overheid ter verantwoording te roepen of om belangen te behartigen⁴³.

We willen dat burgers en bedrijven het recht hebben op inzicht in alle gegevens die voor een voor hen specifiek overheidsbesluit gebruikt zijn.

We willen dat burgers en bedrijven kunnen zien wat de overheid doet om fouten te corrigeren en de gevolgen daarvan te herstellen.

Burgers, bedrijven en andere organisaties kunnen gebruik maken van (publieke) veilige alternatieven voor online platformen en diensten bij publieke instellingen⁴⁴. We willen een internet waarop de belangrijkste functies van algemeen nut niet afhankelijk zijn van één of een klein aantal grote buitenlandse techbedrijven.

> Uitgangspunten

In de NORA vinden we een aantal principes die beogen invulling te geven aan de wens om een transparante en kwalitatief hoogwaardige dienstverlening tot stand te brengen⁴⁵. Ook de GDI-meerjarenvisie en in andere architectuurdocumenten vinden we uitgangspunten voor de aard van producten en dienstverlening. Bijvoorbeeld het initiatief “Gebruiker Centraal”⁴⁶ biedt hulpmiddelen voor een toegankelijke en begrijpelijke overheid.

⁴⁰ Omwille van concreetheid noemen we dit “wallet”, wetend dat de invulling nog in beweging is evenals de EU-wetgeving. Het achterliggende functionele doel is o.a. “regie op gegevens”.

⁴¹ Zie algoritmes.overheid.nl/

⁴² *Brede Maatschappelijke Heroverweging, nr. 13, § 2.10*

⁴³ De Wet Open Overheid verplicht een groot aantal overheidsorganisaties om publieke informatie actief openbaar te maken en de Wet elektronische publicaties (WEP) verplicht bestuursorganen om alle officiële publicaties online te zetten.

⁴⁴ Zie: *Werkagenda Waardengedreven Digitaliseren, paragraaf 2.1, doel 3.*

⁴⁵ Zie: www.noraonline.nl/wiki/Architectuurprincipes

⁴⁶ Zie: www.gebruikercentraal.nl/over-gebruiker-centraal



Alle overheidsdienstverlening is⁴⁷:

- *Proactief en georganiseerd vanuit het perspectief van burgers en ondernemers o.a. aan de hand van levensgebeurtenissen (geboorte, studie, werk, verhuizing, pensionering, starten, voeren en eindigen bedrijf);*
- *Gebruikersvriendelijk, begrijpelijk, transparant en toegankelijk voor iedereen;*
- *Digitaal waar mogelijk met altijd een alternatief voor hen die niet digitaal kunnen of willen;*
- *Op maat waar nodig, als mensen (tijdelijk) niet mee kunnen komen;*
- *In samenhang als één overheid, ondersteund door breed toepasbare GDI -bouwstenen.*
- *Sommige elementen zijn hierbij wettelijk verplicht, op basis van officiële normen die gelden voor de hele overheid (bijvoorbeeld toegankelijkheidsnormen)*

> Bouwstenen

De hierboven beschreven globale producten/diensten van de digitale overheid worden gerealiseerd met de volgende bouwstenen. Voor goed begrip van deze weergave benadrukken we de in hoofdstuk 1 besproken rol van bouwstenen ter concretisering. Over bijbehorende afspraken en standaarden is per bouwsteen meer te vinden in de voetnoten.

*1*overheid: Producten en diensten van de overheid worden eenduidig beschreven in Samenwerkende Catalogi⁴⁸, dit wordt gekoppeld aan Single Digital Gateway en de “Europese versie” Your Europe^{49 50} en levensgebeurtenissen.

Producten en diensten van de overheid zijn via één (digitaal) overheidsloket vindbaar⁵¹, Samenwerkende Catalogi wordt daarbij als universele producten- en dienstencatalogus benut en alle overheidsorganisaties gebruiken dezelfde aanduidingen voor dezelfde producten (o.a. via de Uniforme Productnamenlijst⁵²).

⁴⁷ Zie: [Werkagenda Waardengedreven Digitaliseren | Rapport | Rijksoverheid.nl § 1.2.1.](#)

⁴⁸ Zie: [www.logius.nl/diensten/samenwerkende-catalogi](#). Ook hier is conform de in hoofdstuk 1 beschreven bedoeling voor de generieke functie “catalogus” de huidige bouwsteen genoemd. Om deze daadwerkelijk een overheidsbrede digitale vormgeving te laten ondersteunen die burger waar dat relevant is de overheid als geheel laat ervaren is verdere doorontwikkeling nodig, zowel in termen van afspraken en standaarden, als qua generieke voorziening.

⁴⁹ [europa.eu/youreurope/index_nl.htm](#)

⁵⁰ “De Single Digital Gateway (SDG) geeft burgers en bedrijven makkelijk toegang tot digitale overheidsdienstverlening in de Europese Unie, via een centraal portaal Your Europe. Zie: [europa.eu/youreurope/](#) Dit centrale portaal verwijst gebruikers door naar de juiste websites in de verschillende lidstaten.” Zie: [www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/europa/single-digitale-gateway/](#).

⁵¹ Reviewers merken op dat deze vindbaarheid momenteel niet gerealiseerd is. Voor vindbaarheid zijn we volkomen afhankelijk van private commerciële zoekmachines als Google.

⁵² [standaarden.overheid.nl/upl](#)



Voor burgers, bedrijven en eenmanszaken is er een centrale ingang naar overheidsdienstverlening beschikbaar: www.overheid.nl⁵³. Via meerdere zoekmogelijkheden (naam organisatie, type dienst, levensgebeurtenis) wordt de bezoeker doorgeleid naar de juiste dienstverlenende instantie(s). Dit zonder iets te wijzigen aan directe toegang tot specifieke overheidsorganisaties voor alle gevallen waar die route bekend is en voor de hand ligt.

Grensoverschrijdende dienstverlening van en naar Europa verloopt conform de afspraken gemaakt in het kader van de Single Digital Gateway.

Samenhangende communicatie: Burgers, bedrijven en eenmanszaken kunnen post van de overheid digitaal ontvangen via voorzieningen van het Federatief Berichten Stelsel (FBS)⁵⁴ waar bestaande Berichtenbox^{55 56 57} in op zal gaan en waar de werking voor burger en bedrijf meer eenduidig zal worden.

Burgers en bedrijven kunnen per traditionele brief of digitaal post van de overheid ontvangen. In het kader van dit stelsel wordt alle correspondentie, inclusief post, gedurende een

bepaalde termijn voor de burger ontsloten⁵⁸. In het kader van dit stelsel wordt consequent een handelingsperspectief aan burgers geboden om te reageren op een ontvangen bericht en wordt het gemak waarmee aan overheden via e-mail (of vergelijkbaar) een vraag gesteld kan worden, vergroot.

Poort voor geïntegreerde bedrijfscommunicatie: Digipoort en enkele vergelijkbare berichtvoorzieningen standaardiseren de communicatie van bedrijven en grotere organisaties naar de overheid, inclusief ontvangstbevestiging en afhandelingsberichten van overheid retour.

Eén toegangsstelsel: Er is één stelsel van toegangsbouwstenen voor burgers en bedrijven, publiek (DigiD) en privaat waarop ook Europese erkende middelen werken. Paspoort, ID-kaart, rijbewijs en wallet kunnen worden gebruikt als onderliggende rechtsgeldige identificatiebewijzen in zowel digitale als fysieke communicatie. Deze middelen benutten de identificerende nummers uit BRP, RNI en Handelsregister op een eenduidige manier, ook voor restgroepen. Dit middel biedt voor dienstverleningsprocessen waarbij meerdere

overheidsorganisaties betrokken zijn, een doorlopende gebruikerservaring.

Het Centraal Meldpunt Identiteitsfraude fungeert als ‘alarmcentrale’ voor identiteitsfraude⁵⁹.

Uniform machtigen en vertegenwoordigen: Voor het machtigen of vertegenwoordigen van personen of organisaties wordt gebruik gemaakt van DigiD Machtigen of van andere in relatie tot de identificatiemiddelen bruikbare ‘vertegenwoordigingenregisters’ binnen het stelsel.

Inzicht in gegevens over jezelf: Burgers kunnen via “MijnOverheid” (een deel van) de gegevens waarover de overheid beschikt inzien. Dit kan ook via de app “mijngegevens”. Richting 2030 komen nieuwe typen gegevens beschikbaar⁶⁰ en de burger zal deze graag vanuit 1 ingang benaderen. In 2030 zullen er wallets zijn die waarschijnlijk een rol gaan spelen in de manier waarop de burger dit soort informatie over zichzelf bekijkt en verwerkt.

⁵³ Het noemen van webadres overheid.nl is hier – in lijn met hoe bouwstenen in dit document benut worden om concreet te zijn – geen uitspraak over de vraag of dit de huidige taak van de huidige beheerder van overheid.nl betreft. “Overheid.nl” is vanuit het perspectief van de burger wel een logischer adres dan “rijksoverheid.nl”, immers de vraag welke bestuurslaag het doet is niet van buiten naar binnen gedacht. Een dergelijke ingang doet niets af aan nut van bijvoorbeeld ondernemersplein.

⁵⁴ logius.nl/domeinen/interactie/federatief-berichten-stelsel

⁵⁵ Verplicht op basis van de Dienstenrichtlijn. Zie: ondernemersplein.kvk.nl/berichtenbox-voor-bedrijven

⁵⁶ Zie: www.kvk.nl/mijnondernemingen

⁵⁷ Minister H. Bruins heeft tijdens debat MEBV gesteld: “Een burger hoeft bij voorkeur maar 1 berichtenbox in de gaten te houden”. Nota bene: ook hier geldt dat het gaat om de functionaliteit “berichtenbox”, los van de vraag of de huidige implementatie ideaal is en in 2030 nog exact zo zal zijn.

⁵⁸ De vraag is nog op welke wijze de overheid verantwoordelijkheid kan dragen voor het archiveren van door haar verzonden berichten / post.

⁵⁹ Zie: [Centraal Meldpunt Identiteitsfraude \(CMI\)](https://centraalmeldpuntidentiteitsfraude.nl) | [Contact](https://contact.rijksoverheid.nl) | [Rijksoverheid.nl](https://rijksoverheid.nl)

⁶⁰ Het [vorderingenoeverzicht](https://vorderingenoeverzicht.nl) is een voorbeeld daarvan



Hergebruik gegevens en/of Wallet: Ofwel op basis van een wallet en/of als doorontwikkeling van “mijngegevens” kunnen burgers een betrouwbare versie van gegevens over henzelf benutten en verstrekken aan andere organisaties.

Open overheid: Publieke overheidsinformatie wordt actief ontsloten en centraal toegankelijk gemaakt⁶¹. Dit vindt plaats via een te ontwikkelen, verbeterde versie van het Platform Open Overheidsinformatie (PLOOI)⁶² en andere bouwstenen van het Kennis- en exploitatiecentrum Officiële Overheids Publicaties (KOOP) voor openbare mededelingen. Daarnaast zijn er sectorale voorzieningen voor open informatie zoals PDOK voor geo-informatie.

Via de attenderingsservice kunnen burgers en bedrijven zich abonneren op overheidsinformatie over voor hen relevant gebied of op basis van andere criteria⁶³.

6.1.3 Kanalen

> Wat willen we?

Een deel van de producten en zeer veel diensten van de overheid worden via meerdere kanalen aangeboden: via onder meer het fysieke loket of product, via post- of pakketverzending, via (video)bellen, via websites, app's en – voor 'business-to-business' – via services en API's. Nederland wil hoog scoren op de Europese eGovernment

Benchmark 2022⁶⁴ die o.a. aangeeft dat het websitekanaal dominant is in digitale dienstverlening en ondersteuning van op smartphone toegespitste dienstverlening (apps) daarbij achterblijft. De Europese ambitie (verwoord in “Shaping Europe's digital future”) is dat alle belangrijke openbare diensten in 2030 online aangeboden worden. Aan de andere kant vereist het streven naar inclusiviteit dat ook andere kanalen beschikbaar blijven voor de aanzienlijke groep on-, anders- en laaggeletterden en mensen met een lichamelijke beperking.

We willen dat burgers en bedrijven zelf kunnen aangeven via welk kanaal ze gebruik willen maken van dienstverlening door de overheid (click, call, face).⁶⁵ Ontwikkelingen op dit gebied gaan snel, door komst van chatbots, online en spraak, komen click en call dicht bij elkaar, maar neemt ook het aantal kanalen waar de overheid rekening mee moet houden toe. We willen dat welk kanaal burgers en bedrijven ook kiezen, de informatie, de transactie en de resulterende dienst in gelijke gevallen gelijk is. Zij hebben het recht digitaal berichten te zenden aan een bestuursorgaan (Wet Modernisering Elektronisch Bestuurlijk Verkeer).

Nota bene: uit review komt naar voren dat het kanalenbeleid verdere uitwerking behoeft. De samenhang tussen telefonie (call), fysiek loket (inclusief Informatiepunten Digitale Overheid⁶⁶) en internet, met varianten website, tekstchat,

sociale mediakanalen en app is niet expliciet beschreven c.q. ontworpen. Gevolg is dat binnen de overheid zeer uiteenlopende keuzes gemaakt worden, waardoor de burger de verschillende kanalen als losstaand ervaart. De basisvraag die daaraan voorafgaat is of het realistisch en kostenefficiënt is dit overheidsbreed “op te lossen” en voor welke maatschappelijke opgaven dat prioriteit zou moeten hebben. Een daarmee samenhangend vraagstuk zijn mogelijkheden voor vertegenwoordiging die kanaalafhankelijk werken.

Voor klantcontactcenters kan gedacht worden aan de volgende mogelijkheid: De medewerker KCC kan – indien nodig - een bericht sturen naar de beller met vraag om akkoord te geven op inzage.

⁶¹ Zie: www.koopoverheid.nl/voor-overheden/rijksoverheid/plooi-platform-open-overheidsinformatie

⁶² www.koopoverheid.nl/voor-overheden/rijksoverheid/plooi-platform-open-overheidsinformatie In de doorontwikkeling is dit waarschijnlijk geen voorziening, maar een set van afspraken en standaarden

⁶³ Een voorbeeld hiervan is www.overheid.nl/berichten-over-uw-buurt

⁶⁴ Deze benchmark van de Europese Commissie vergelijkt de digitale overheidsdienstverlening van 35 Europese landen.

⁶⁵ Zie vng.nl/projecten/omnichannel-kanaalstrategie-dienstverlening

⁶⁶ www.kb.nl/over-ons/projecten/informatiepunt-digitale-overheid



> Uitgangspunten

- De overheid biedt diensten en producten via meerdere kanalen aan, met voor burgers te allen tijde ook een niet-digitaal kanaal⁶⁷.
- Elk ingezet kanaal (balie, callcenter, website, app, e.d.⁶⁸) kent een maximale toegankelijkheid voor mensen met een beperking. Communicatie vanuit de overheid naar burgers en bedrijven dient digitoegankelijk te zijn. Digitale kanalen, zoals Overheidswebsites en app's voldoen aan het Tijdelijk Besluit Digitale Toegankelijkheid Overheid⁶⁹.
- Kanalen dienen – waar nodig – ook via machtigen en vertegenwoordigen toegankelijk te zijn.
- Het toegepaste kanaal heeft geen invloed op de aard en de inhoud van producten en diensten. Producten en diensten die via meerdere kanalen worden aangeboden, zijn functioneel gelijk.
- Voor het ontwerpen van dienstverlening en processen wordt uitgegaan van een digitale wereld. Deze ondersteunt ook de niet digitale kanalen. Intern functioneert de overheid dus digitaal⁷⁰.

- Door het beschikbaar stellen van API's door overheidsorganisaties kunnen⁷¹ burgers, bedrijven (softwareleveranciers) en overheidsorganisaties zelf het initiatief nemen om digitaal gegevens af te nemen of met overheidsorganisaties te communiceren. Dit werkt innovatie in de hand die verder gaat dan de standaardmogelijkheden van de dienstverlening aan burgers en bedrijven.

> Bouwstenen

- Burgers en bedrijven kunnen op 'MijnOverheid' resp. 'Mijn eenmanszaak' aangeven op welke wijze zij met uiteenlopende overheidsorganisaties willen communiceren (generieke profielservice).
- Overheidswebsites worden voorzien van dezelfde domeinnaam (www.organisatie.overheid.nl) of een andere samenhangende oplossing die maakt dat burgers en bedrijven herkennen dat zij online echt te maken hebben met de overheid en dat herleidbaar is, ook in de toeleiding, welke informatie van de overheid afkomstig is^{72 73 74}.

- Overheidswebsites worden gebaseerd op een universele vormgeving en structuur⁷⁵, welke mede is gebaseerd op een gestandaardiseerde lijst van levensgebeurtenissen⁷⁶. NL Design system⁷⁷ kan een belangrijke rol spelen in consistent voor de burger herkenbare websites en hetzelfde geldt voor andere bouwstenen van Gebruiker Centraal⁷⁸. Websites van de overheid worden ontwikkeld via concepten als het Platform Rijksoverheid Online (PRO).

⁶⁷ Werkagenda Waardengedreven Digitalisering, doel 1.2.

⁶⁸ System-to-system verkeer is uiteraard uitgezonderd van eisen voor menselijke gebruikers. Maar de service portalen van b.v. de Digipoort moeten wel aan deze eisen voldoen, ook bedrijven hebben medewerkers met beperkingen.

⁶⁹ Zie Tijdelijk Besluit Digitale Toegankelijkheid Overheid op zoek.officielebekendmakingen.nl/stb-2018-141.html waarin de Web Content Accessibility Guidelines (WCAG) versie 2.1. worden toegepast. Daarnaast wordt ook de bredere EU-toegankelijkheidsrichtlijn in Nederlandse wetgeving geïmplementeerd. Zie www.digitoegankelijk.nl/uitleg-van-eisen

⁷⁰ Consequentie is dat waar in dit document staat dat iets "digitaal" is, dat niet uitsluit dat het ook via een IDO of ander fysiek loket – als kanaal – wordt aangeboden aan burgers en bedrijven.

⁷¹ Meerdere reviewers geven aan dat steviger API-first beleid dat verder gaat dan vrijblijvendheid hier zou helpen

⁷² De huidige situatie is dat o.a. Google een grote rol speelt in de toeleiding op een wijze waar de overheid geen verantwoordelijkheid voor kan nemen.

⁷³ Werkagenda Waardengedreven Digitalisering, actie 2.4.4 in kader van cybersecurity / betrouwbaarheid. Een internationaal gangbaar alternatief (dat ernaast zou kunnen bestaan) is www.organisatie.gov.nl

⁷⁴ Er wordt gewerkt aan een register van overheidswebsites. Dit is een eerste stap op weg naar meer transparantie en mogelijke reductie en uniformering van overheidswebsites.

⁷⁵ Zie ook het VNG-project, "Standaard Dienstverlening overheidsportalen" en vng.nl/sites/default/files/2020-03/def-brochure-digitale_inclusie-2020.pdf

⁷⁶ Bijvoorbeeld: geboorte, kinderen, school, studie, werk, verhuizing, belasting, uitkering, pensionering, verblijf, bedrijf starten, voeren en eindigen, etc.

⁷⁷ nldesignsystem.nl

⁷⁸ www.gebruikercentraal.nl/hulpmiddelen



6.1.4 Organisatie

> Wat willen we?

De overheid bestaat uit veel (semi-)autonome organisaties⁷⁹. Toch willen we graag dat burgers en bedrijven de overheid als één organisatie ervaren; zeker wat betreft de dienstverlening. In de Werkagenda wordt dit als volgt verwoord⁸⁰:

“Burgers en ondernemers ervaren dienstverlening van de overheid die aansluit bij hun behoefte en leefwereld. (...) Alle overheidsdienstverlening is (...) in samenhang als één overheid, ondersteund door breed toepasbare GDI-bouwstenen”.

Om dit te bereiken is coördinatie, kaderstelling en samenwerking van groot belang. Dit moet leiden tot het realiseren van drempelloze ketenprocessen: Het op een logische manier verbinden van dienstverlening door meerdere organisaties ofwel: ketensamenwerking of samenwerking in netwerken van organisaties. We willen dat gegevens van burgers en bedrijven die al binnen de overheid bekend zijn niet voor een tweede keer worden uitgevraagd⁸¹. Dit is niet mogelijk zonder het goed regelen van wettelijke grondslagen voor gegevensuitwisseling⁸² en de benodigde organisatorische afspraken.

> Uitgangspunten

- Bewindspersonen, bestuurders, overheidsorganisaties en instellingen met een publieke taak maken afspraken die leiden tot een aaneensluitende dienstverlening aan burgers en bedrijven⁸³.
- Overheidsorganisaties en instellingen met een publieke taak zorgen voor een helder afgebakend, maar aaneensluitend pakket van diensten en producten.

> Bouwstenen

- Zie: www.noraonline.nl/wiki/Ketensturing/Bouwstenen_voor_ketensturing

6.1.5 Processen

> Wat willen we?

We willen dat burgers en bedrijven de dienstverlening (of ‘verplichte handelingen’) als transparante, doorlopende processen ervaren. We willen dat burgers en bedrijven het proces kunnen volgen en waar nodig bijsturen. De algemene beginselen van behoorlijk bestuur en mede daaruit volgende minimale eisen uit de Awb moeten daarbij geborgd worden.

Processen worden ondersteund met workflow-, casemanagement-, en zaaksystemen. Daarbij wordt ook gebruik gemaakt van business rule engines en algoritmes. Waar algoritmes belangrijk zijn voor de onderbouwing van beslissingen moet dit transparant zijn en getoetst worden aan de rechten van de mens (en aan vigerende wetgeving) mede om discriminatie en vooroordelen te voorkomen. Momenteel ontwikkelt wet- en regelgeving zich snel, o.a. de EU AI verordening. Dit zal de Digitale Overheid richting 2030 in toenemende mate beïnvloeden.

> Uitgangspunten

- Overheidsorganisaties en instellingen met een publieke taak werken op basis van afspraken⁸⁴ die leiden tot aaneensluitende dienstverleningsprocessen aan burgers en bedrijven⁸⁵.
- Overheidsorganisaties ontwikkelen volledig digitale processen aan de hand van levensgebeurtenissen (bijvoorbeeld geboorte, studie, werk, verhuizing, pensionering, starten en eindigen bedrijf)⁸⁶. Dit betreft de complexere behoeften voor zover die vaak genoeg voorkomen, het melden van kapotte stoeptegels bij de gemeente is geen levensgebeurtenis.

⁷⁹ Voor een overzicht van overheidsorganisaties, zie www.overheid.nl/

⁸⁰ Werkagenda Waardengedreven Digitalisering, pag. 11.

⁸¹ Zoals in de Wet “eenmalige gegevensuitvraag werk en inkomen”. Zie: wetten.overheid.nl/BWBR0023299/2008-01-01

⁸² Zoals volgt uit analyses van Werken Aan Uitvoering en Brede Maatschappelijke Heroverweging 13 wordt de Avg vaak ten onrechte als argument voor beperkingen gebruikt terwijl diezelfde Avg ook de basis biedt voor verantwoorde datadeling. Bijvoorbeeld in België wordt anders omgegaan met het besluiten over datadeling en dat binnen diezelfde Europese Avg regels.

⁸³ Besluit Sturing Digitale Overheid, GDI-meerjarenvisie geven uiting aan het stap voor stap verder opnemen in de governance van dit uitgangspunt, evenals Europese verplichtingen vanuit SDG.

⁸⁴ Voor een beperkt aantal processen vormt de SDG-verordening een wettelijke basis hiervoor.

⁸⁵ Zie www.noraonline.nl/wiki/Dienstverleningsconcept

⁸⁶ Werkagenda Waardengedreven Digitalisering en SDG annex II verplicht dit voor een beperkte set procedures



- Overheidsorganisaties bieden een helder inzicht in het procesverloop. Burgers, bedrijven en andere organisaties kunnen – wanneer ze dat willen – de voortgang van het proces of de procedure volgen (*track & trace*) en daarop reageren (*feedback* functie)⁸⁷.
- Overheidsorganisaties zorgen voor onderlinge samenhang van zaakgegevens en data, zodat burgers en bedrijven een naadloze dienstverlening ervaren en daarover worden geïnformeerd, ook als daarbij meerdere organisaties een rol spelen^{88 89}.
- Dienstverlening vanuit het perspectief van burgers betekent dat er processen moeten zijn op basis waarvan feedback van burgers en bedrijven verwerkt kan worden. Dit betreft feedback over samenhang, vindbaarheid en begrijpelijkheid van informatie, feedback op gegevens over jezelf en het meervoudig gebruik van die gegevens en mogelijkheden voor tips, klachten, bezwaar en beroep (als al genoemd bij track & trace).

> Bouwstenen

- Netwerk-, keten- en bedrijfsprocessen worden ontworpen startend vanuit (doorlopende) klantreizen over organisaties heen, gebaseerd op levensgebeurtenissen⁹⁰.
- Via afspraken over een 'track and trace' mechanisme als onderdeel van 'mijnoverheid/Lopende Zaken' kunnen burgers en bedrijven de voortgang over organisaties heen van een proces volgen. Dit is ook mogelijk door tussenkomst van medewerkers van bijvoorbeeld een klantcontactcenter.
- Dossier- en dataoverdracht tussen overheidsorganisaties vindt digitaal plaats met medeweten van de burger of het bedrijf via een notificatie-oplossing⁹¹.
- Voor het doorgeven van (vermeende) fouten in overheidsregistraties kunnen burgers, bedrijven en overheidsorganisaties gebruikmaken van het Meldpunt Fouten in Overheidsregistraties (MFO)^{92 93}.
- Voor het doorgeven van (vermeende) identiteitsfraude kan gebruikgemaakt worden van het Centraal Meldpunt Identiteitsfraude (CMI)⁹⁴.

- Voor het doorgeven van mogelijke onjuistheden in de gegevens van een (basis)registratie gebruiken overheidsorganisaties Digimelding. Digimelding zorgt voor een uniforme, betrouwbare en efficiënte terugmelding aan de bronhouder van deze registratie⁹⁵.
- De overheidsorganisaties kennen publiek toegankelijke algoritmeregisters, waarin de werking van specifieke algoritmes worden toegelicht⁹⁶.

6.1.6 Bedrijfsfuncties

> Wat willen we?

We willen een transparante overheid, waarbij helder is welke overheidsinstantie verantwoordelijk is voor het leveren van een product of dienst of de behandeling van een zaak. We willen een efficiënte overheid, die geen dingen dubbel doet. Bedrijfs(sub)functies vormen de basis voor de inrichting van overheidsorganisaties, omdat zij richting geven aan onder meer de organisatie-inrichting en -besturing, de inzet van benodigde informatiesystemen en de verantwoordelijkheid voor de kwaliteit van diensten, producten, applicaties en data.

⁸⁷ Werkagenda Waardengedreven Digitaliseren en actielijnen uit Open op Orde

⁸⁸ Uiteraard binnen de grenzen van privacyborging. Met 'zaken' bedoelen we de behandeling van een afzonderlijke zaak of casus.

⁸⁹ Dit uitgangspunt vloeit voort uit één van de doelen van de Werkagenda Waardengedreven Digitaliseren, samengevat door "één overheid".

⁹⁰ Zie bijvoorbeeld: www.overheid.nl/dienstverlening/levensgebeurtenissen.

⁹¹ Over hoe dit moet worden vormgegeven bestaan nog verschillende beelden: regie op gegevens, mogelijke rol van een wallet, SDG OOTS zijn allemaal mogelijke oplossingsrichtingen.

⁹² Zie: www.rvig.nl/meldpunt-fouten-in-overheidsregistraties

⁹³ Reviewers merken op dat er te veel overlappende meldpunten zijn en dat de burger niet direct geholpen is met het melden. Stevigere mechanismen om fouten te herstellen zijn nodig.

⁹⁴ Zie: www.rvig.nl/centraal-meldpunt-identiteitsfraude

⁹⁵ Zie: www.logius.nl/diensten/digimelding

⁹⁶ Zie bijvoorbeeld: algoritmeregister.amsterdam.nl



> Uitgangspunten

- Bedrijfsfuncties van overheidsinstanties zijn helder en eenduidig belegd.
- Bedrijfsfuncties bieden een solide basis voor het maken van samenwerkingsafspraken tussen overheidsorganisaties.
- Functies binnen de overheid kennen het volgende patroon:
 - a. beleid/ontwikkeling wet- en regelgeving;
 - b. besluitvorming;
 - c. uitvoering;
 - d. verantwoording/monitoring/inspectie;
 - e. handhaving.

> Bouwstenen

- Gelijksortige overheidsorganisaties kennen een gelijksortige indeling in bedrijfsfuncties⁹⁷.

6.2 Informatie-architectuur

Mede op basis van dit architectuurdocument werken we aan verbeterde informatiesystemen en infrastructuur, een modern ICT-landschap en de juiste afspraken, standaarden en voorzieningen, als basis voor een effectief functioneren van de overheid, intern en naar de burger en bedrijven⁹⁸.

In dit en het volgende hoofdstuk werken we dit verder uit. De uitwerking is van buiten naar binnen conform het eerdere genoemde uitgangspunt “vanuit het perspectief van burgers en ondernemers”: eerst de API’s die afnemers benutten, daarna de applicaties die deze API’s – en daarnaast oudere vormen van integratie – aanbieden. Eerst gegevensuitwisseling en daarna de gegevensbronnen.

6.2.1 Api’s / Services

> Wat willen we?

Voor een optimale samenwerking tussen overheids-organisaties onderling en met name met generieke voorzieningen willen we dat gegevens en diensten betrouwbaar zijn en eenvoudig uitgewisseld en geleverd kunnen worden. Voor de GDI is in de afgelopen jaren een transformatie in gang gezet van een silo-gewijze structuur met naast elkaar staande voorzieningen naar een meer stelselmatige opzet, waarbij gegevens en toepassingen via generieke functies en API’s onderling worden verbonden⁹⁹. Dit is, inclusief architectuur, nader uitgewerkt in de Nederlandse API Strategie¹⁰⁰.

We willen dat overheidsorganisaties API’s publiekelijk beschikbaar stellen zodat die door uiteenlopende belanghebbenden kunnen worden ‘aangesproken’

om services en data van overheidsorganisaties in geautomatiseerde vorm – binnen Avg-grenzen - te kunnen afnemen. Het feit dat API’s autorisatie kunnen vereisen of dat gebruik ervan op andere manieren door de aanbieder gecontroleerd wordt, doet niets af aan het belang de beschikbare API’s te publiceren.

> Uitgangspunten

- De architectuur Digitale Overheid is gebaseerd op service oriëntatie. Organisaties leveren burgers, bedrijven en elkaar services, die in toenemende mate worden aangeboden in de vorm van API’s.
- Overheidsorganisaties standaardiseren op gelijkvormige en breed inzetbare API’s voor het leggen van verbindingen tussen applicaties *en als ontkoppelpunt tussen presentatie (front-end) en voorziening (back end applicatie)*.
- Geautomatiseerde digitale uitwisseling tussen voorzieningen verloopt bij voorkeur via API’s.
- Specificaties van overheids-API’s worden openbaar gepubliceerd (conform de in de API standaard vastgelegde kaders, zie bouwsteen).
- Alvorens zelf een API te ontwikkelen, kijken we eerst in het service-/API-register op developer.overheid.nl om te zien of de gewenste API al bestaat. Deze dient de daartoe benodigde functionele documentatie aan te bieden.

⁹⁷ Zie bijvoorbeeld het bedrijfsfunctiemodel van gemeenten www.gemmaonline.nl/index.php/GEMMA_Bedrijfsfuncties

⁹⁸ i-strategie Rijk- 3 & 4

⁹⁹ Overgenomen uit meerjarenvisie GDI § 8.2

¹⁰⁰ Zie docs.geostandaarden.nl/api/API-Strategie/ API’s als concept wordt hier verder bekend verondersteld. Voor meer uitleg daarvan zie deze verwijzing naar Nederlandse API strategie.



- Overheids-api's zijn open te gebruiken, ook voor niet-overheidsorganisaties bruikbaar, tenzij wettelijke of privacyeisen dat verhinderen. Overheidsaanbieders kunnen bandbreedte voor openbaar gebruik beperken.
- Overheids-API's worden op robuuste manier aangeboden zodat ze bestand zijn tegen overbelasting en voldoen aan beveiligingseisen (bijvoorbeeld door hiertoe een API-Gateway¹⁰¹ in te richten).

> Bouwstenen

- API's worden ontwikkeld op basis van de REST API Design Rules¹⁰². Binnen Digikoppeling zijn deze vastgelegd in een variant¹⁰³ (Digikoppeling Koppelvlakstandaard REST-API)¹⁰⁴.
- Voor publicatie van API's is er de generieke voorziening developer.overheid.nl
- Bouwstenen voor Toegang werken naadloos samen met de API-standaard voor Toegang zodat het makkelijker wordt overheidsapps te maken waarop ingelogd kan worden met DigiD en andere toegelaten toegangsmiddelen.

6.2.2 Applicaties

> Wat willen we?

Organisaties met een publieke taak gebruiken voor het realiseren van hun functies vele duizenden applicaties. Met deze applicaties worden de processen ondersteund die zorgen voor het tot stand brengen van diensten, producten, gegevensuitwisseling, management- en verantwoordingsinformatie, etc. Keuze en gebruik van deze applicaties is een verantwoordelijkheid van de afzonderlijke organisaties en valt dus buiten het aandachtsgebied van deze Architectuur Digitale Overheid. Iedere overheidsorganisatie heeft daarbij vanuit het uitgangspunt “in samenhang” (zie § 6.1.2) de verantwoordelijkheid de afspraken en standaarden die in het kader van de Digitale Overheid zijn overeengekomen te implementeren. Dit kan gevolgen hebben voor de eigen applicaties.

Om het functioneren van de digitale overheid te ondersteunen zijn – naast bovengenoemde afspraken en standaarden – generieke voorzieningen nodig. Deze worden in dit hoofdstuk nader beschreven. Velen ervan worden beheerd door dienstverleners als onder meer Logius en ININIS. Generieke voorzieningen ondersteunen

burgers, bedrijven en organisaties met een publieke taak bij hun interactie, ondersteunen die organisaties bij hun onderlinge samenwerking en voorkomen dubbele kosten en complexiteit.

Deze generieke voorzieningen hebben invloed op de architectuur van afzonderlijke organisaties, want om goed gebruik te kunnen maken van generieke voorzieningen, moeten zij voldoen aan bepaalde aansluitvoorwaarden en standaarden voor bijvoorbeeld gegevensuitwisseling.

Binnen het gemeentelijk domein heeft de Common Ground ontwikkeling inmiddels geleid tot een aantal herbruikbare softwareproducten, waarmee de functies en processen van gemeenten kunnen worden ondersteund. Dit betreft herbruikbare applicaties: één keer ontwikkelen en door elke gemeente binnen het eigen applicatielandschap in te zetten¹⁰⁵. Een vergelijkbare ontwikkeling betreft Open Webconcept: gezamenlijk ontwikkelde softwarecomponenten voor gemeenten¹⁰⁶. Deze applicaties zijn geen onderdeel van de GDI. Dit laat zien dat er meerdere vormen van generieke bouwstenen zijn – ook buiten de huidige GDI – die relevant kunnen zijn voor de Digitale Overheid.

¹⁰¹ docs.geostandaarden.nl/api/API-Strategie/

¹⁰² publicatie.centrumvoorstandaarden.nl/api/adr/ In sommige gevallen zijn andere of uitgebreidere architectuurpatronen dan REST gewenst, dan worden de delen van deze standaarden, bijvoorbeeld naamgevingsconventies, die ook in die gevallen toepasbaar zijn onverkort gevolgd.

¹⁰³ deze API-standaard voor toegang volgt de marktstandaard Open ID Connect (OIDC) en is onderdeel van bovengenoemde Digikoppeling standaard die dus in volledigheid moet worden toegepast

¹⁰⁴ publicatie.centrumvoorstandaarden.nl/dk/restapi/ en www.forumstandaardisatie.nl/open-standaarden/openapi-specification

¹⁰⁵ Zie voor een overzicht componentencatalogus.commonground.nl/

¹⁰⁶ Zie: openwebconcept.nl



> Uitgangspunten

- We maken alleen generieke voorzieningen als afspraken en/of standaarden onvoldoende zijn of als deze aanvullend en conform afspraken en standaarden nodig zijn.
- Naast afspraken en standaarden biedt een beperkt aantal generieke voorzieningen de basis voor de digitale overheid¹⁰⁷.
- Berichten aan burgers en bedrijven worden beschikbaar gesteld door de overheidsorganisatie die verantwoordelijk is voor bijbehorende proces. Via de bouwstenen van het Federatief Berichtenstelsel¹⁰⁸ wordt dit “in samenhang” en via 1 plek, teruggevonden. Hetzelfde bericht wordt beschikbaar gesteld in de bijbehorende mijn-omgeving; dit ongeacht welke locatie bij welke organisatie de meest aangewezen opslag is.

6.2.3 Berichtenverkeer / gegevensuitwisseling

> Wat willen we?

Om goed te kunnen samenwerken willen we dat gegevens en berichten eenvoudig en zoveel mogelijk geautomatiseerd kunnen worden uitgewisseld; zowel tussen overheid en burgers en bedrijven als tussen overheidsorganisatie onderling. Dit verloopt beter als we gebruikmaken van overheidsbrede afspraken, standaarden en voorzieningen

> Uitgangspunten

- Wijzigingen in opgeslagen gegevens die voor andere overheidsorganisaties van belang zijn, worden geautomatiseerd doorgegeven.
- Per domein / sector dienen afspraken gemaakt te worden over standaarden van berichten (informatiemodel, semantiek, e.d.)¹⁰⁹. Daarbij zijn overheidsbrede kaders en standaarden nodig om semantische interoperabiliteit ook sectoroverstijgend mogelijk te maken.

> Bouwstenen

- De afspraken, standaarden en voorzieningen van het Federatief Berichtenstelsel. Het betreft qua voorzieningen de Generieke FBS Services en het BBO Berichtenmagazijn (BBO staat voor Berichtenbox Burgers en Ondernemers).
- Voor het transporteren van massale, gestructureerde berichtenstromen die voortkomen uit systemen van bedrijven en met de overheid worden uitgewisseld, wordt de doorontwikkelde versie van Digipoort¹¹⁰ gebruikt.

¹⁰⁷ Zie: OBDO: Beleidskader digitale basisinfrastructuur 23/04/2019 op www.noraonline.nl/images/noraonline/2/25/Beleidskader_digitale_basisinfrastructuur.pdf

¹⁰⁸ Onder 'berichten' worden in het kader van FBS (digitale) brieven en notificaties aan burgers en bedrijven verstaan.

¹⁰⁹ Een voorbeeld hiervan is Standard Business Reporting.

¹¹⁰ Digipoort is het 'elektronische postkantoor' van de overheid voor bedrijven. Voor veilige en gestandaardiseerde gegevensuitwisseling met het bedrijfsleven. Digipoort zorgt voor de ontvangst, controle en bevestiging van berichten.



- Voor abonnementen op gebeurtenissen in de Basis- en kernregistraties gebruiken we Digilevering¹¹¹ en NL GOV profile for CloudEvents¹¹².
- De standaard voor de logistiek van het berichtenverkeer is Digikoppeling¹¹³.
- Het Organisatie Identificatie Nummer (OIN) dat is opgenomen in het register ‘International Code Designators’ en het verdere OIN-stelsel¹¹⁴ worden gebruikt om organisaties te identificeren;
- Voor het overheidsberichtenverkeer met andere landen, kan gebruik worden gemaakt van diensten van het Nationaal Aansluitpunt¹¹⁵.
- Ter vereenvoudiging van het berichtenverkeer kunnen¹¹⁶ overheidsorganisaties gebruikmaken van één “Algemeen Aansluitpunt” dat de benodigde koppelingen biedt naar alle¹¹⁷ basisregistraties, en GDI-voorzieningen. Het bestaande aanbod van enerzijds Centraal Aansluitpunt (bij Logius)¹¹⁸ en anderzijds “Aansluiting

Digivoorzieningen” (bij RINIS)¹¹⁹ voorzien daar al gedeeltelijk in.

- Burgers kunnen voor de uitwisseling van gegevens ook gebruikmaken van een Wallet¹²⁰.
- Voor internationale data-uitwisseling kan gekeken worden naar de Service Metadata Publisher (SMP)¹²¹. De SMP bevat alle gegevens die andere partijen nodig hebben om met Nederlandse organisaties data uit te wisselen, zoals het digitale adres en benodigde certificaten¹²².

6.2.4 Data / gegevens

> Wat willen we?

De digitale overheid draait op data. We willen dat de overheid verantwoord gebruik maakt van data voor dienstverlening, het oplossen van maatschappelijke vraagstukken, beleidsvorming en -monitoring.

Verantwoord gebruik van data maakt een overheid mogelijk die niet naar de bekende weg vraagt, klantgericht is, zich niet voor de gek laat houden, weet waar ze het over heeft en haar zaken op orde heeft en niet meer uitgeeft dan nodig¹²³. Daarom willen we – om misverstanden te voorkomen – dat data goed gedefinieerd zijn en hun betekenis helder is (semantiek). We willen wildgroei en kwaliteitsverlies in data voorkomen door zoveel mogelijk data te hergebruiken, data moet daarvoor goed vindbaar zijn. Dit doen we door data waarover overheidsorganisaties beschikken zoveel mogelijk – binnen wettelijke kaders – te delen met andere overheidsorganisaties als dat bijdraagt aan de dienstverlening (immers, datadelen zal altijd in balans moeten zijn met dataminimalisatie). We vragen gegevens waarover de overheid al beschikt, niet opnieuw uit¹²⁴. We maken het voor burgers en bedrijven ook mogelijk om zelf regie te nemen over het delen en uitwisselen van data, bijvoorbeeld via een Wallet¹²⁵.

¹¹¹ Via Digilevering krijgt een organisatie direct bericht bij wijzigingen in basisregistraties na een gebeurtenis zoals een verhuizing van een bedrijf. Digilevering is een abonnementenvoorziening.

Zie: www.logius.nl/diensten/digilevering. Digilevering wordt gemoderniseerd naar de NL GOV profile for CloudEvents standaard

¹¹² logius.nl/domeinen/gegevensuitwisseling/nl-gov-profile-cloudevents

¹¹³ Digikoppeling is een set van standaarden, die logistieke afspraken bevat voor elektronisch berichtenverkeer tussen (overheids)organisaties. Zie: www.logius.nl/diensten/digikoppeling

¹¹⁴ Zie publicatie.centrumvoorstandaarden.nl/dk/join/ en ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Registry+of+supporting+artefacts+to+implement+EN16931

¹¹⁵ “Uitwisseling Nederland” van RINIS, dat gebruik maakt van het besloten overheidsnetwerk Diginetwerk. Zie: www.rinis.nl/nl/uitwisseling-nederland

¹¹⁶ Uitdrukkelijk “kunnen”. Het is een optie met name voor kleinere organisatie en beperkte stromen. Daardoor is geen sprake van single point of failure en ongewenste afhankelijkheden. Het voorkomt dat kleine organisaties niet mee kunnen doen in “grote” standaardisaties en afsprakenstelsels.

¹¹⁷ Bestaande basisregistraties WOZ, Voertuig en Inkomen en mogelijke nieuwe basisregistraties nog niet aangesloten

¹¹⁸ www.logius.nl/domeinen/infrastructuur/centraal-aansluitpunt

¹¹⁹ www.rinis.nl/nl/aansluiting-mijnoverheid

¹²⁰ Onder ander via de MIDO-werkgroep Toegang wordt deze samenhang gevolgd en waar nodig verder uitgewerkt. Benodigde wettelijke basis op dit gebied is onderwerp van 2e tranche Wdo.

¹²¹ De SMP wordt namens de Nederlandse overheid beheerd door RINIS. Zie: www.rinis.nl/nl/edelivery

¹²² Dit vraagt nader onderzoek, o.a. omdat in kader van SDG OOTS juist een andere keuze gemaakt is

¹²³ Zie: zoek.officielebekendmakingen.nl/kst-26387-18.html

¹²⁴ Zoals bijvoorbeeld geregeld is in de Wet eenmalige gegevensuitvraag werk en inkomen.

¹²⁵ Zie ook: www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/regie-op-gegevens



Burgers, bedrijven en overheidsorganisaties moeten vermeende onjuistheden in data via eenvoudige procedures kunnen (laten) corrigeren.

Data spelen een belangrijke rol in het (proactieve) beleidsontwikkeling en dienstverlening van de overheid op terreinen als klimaat, energie, huisvesting, economie, arbeidsmarkt, zorg, onderwijs en gezondheid. De toegang tot betrouwbare data en het kunnen aanwenden binnen het eigen onderzoek, de beleidsontwikkeling en dienstverlening is dan ook van groot belang. Data levert als zelfstandig *asset* een belangrijke bijdrage aan het oplossen van maatschappelijke vraagstukken en het creëren van economische waarde. Vanuit de Europese Unie wordt ook stevig ingezet op datagedreven werken en onder meer het tot stand brengen van *dataspaces*¹²⁶.

De Nederlandse Basisregistraties¹²⁷ vervullen een essentiële rol in het vastleggen en gecontroleerd beheren van data. In aanvulling daarop willen we dat organisaties aan elkaar data ter beschikking stellen vanuit ‘kernregistraties’¹²⁸. We noemen dit het Federatief Datastelsel¹²⁹:

Er worden afspraken gemaakt over het uitwisselen van data. Deze afspraken hebben betrekking op de betekenis van data (semantiek), de vastlegging en het beheer ervan en de logistiek voor de uitwisseling ervan.

We willen dat van vastgelegde data duidelijk is wat de authentieke bron is, wie de verantwoordelijke bronhouder is en wie verantwoordelijk is voor de kwaliteit van de data.

> Uitgangspunten

- Burgers en bedrijven kunnen eenvoudig zien welke data de overheid over hen heeft (inzagerecht).
- Burgers, bedrijven en overheden kunnen vermeende onjuistheden in data eenvoudig laten corrigeren (correctierecht).
- Burgers en bedrijven welke gegevens gebruikt zijn als basis voor ieder overheidsbesluit over hen.
- Voor het delen van data maken we gebruik van de principes van het Federatief Datastelsel¹³⁰: Data worden door middel van API's opgeslagen in- en verstrekt uit basis- en kernregistraties, conform de Interbestuurlijke Datastrategie¹³¹.

- We harmoniseren definities en betekenis (semantiek) van gegevens¹³².
- Voor het opstellen van informatiemodellen wordt gebruik gemaakt van het Metamodel Informatie Modelling (MIM)¹³³. Dit draagt ook bij aan betere semantiek en toepassing van linked data.
- Data wordt beschikbaar gemaakt met toepassing van de “FAIR” principes, te weten: Findable / Vindbaar, Accessible / Toegankelijk, interoperabel, Reusable / Herbruikbaar¹³⁴. Dit komt onder andere neer op het grondig toepassen van metadata en sluit aan op andere hier genoemde uitgangspunten.
- Bronhouders zijn verantwoordelijke voor de kwaliteit van hun data. Welke data daarbij binnen de overheid uit welke bron komt is duidelijk vastgelegd en afnemers zijn verplicht te zorgen dat data actueel blijven en conform deze bron zijn¹³⁵.

¹²⁶ De E.U. heeft 16 dataspace gedefinieerd. Deze liggen op het terrein van de Digitale Samenleving en worden daarom hier niet verder uitgewerkt. Uiteraard kunnen ook overheidsorganisaties gebruikmaken van deze dataspace en er zelf een bijdrage aan leveren.

¹²⁷ Zie: stelselvanbasisregistraties.nl/home

¹²⁸ Een voorbeeld hiervan is het Landelijk Register Zorgaanbieders.

¹²⁹ Het FDS vloeit voort uit de Interbestuurlijke Datastrategie. Zie: [Kamerbrief over Interbestuurlijke Datastrategie Nederland](#) | [Kamerstuk](#) | [Rijksoverheid.nl](#) en [realisatiebids.pleio.nl](#)

¹³⁰ Zie: www.digitaleoverheid.nl/achtergrondartikelen/federatief-datastelsel-het-organiseren-van-vertrouwen

¹³¹ www.rijksoverheid.nl/documenten/rapporten/2021/10/31/nl-digitaal-interbestuurlijke-datastrategie-nederland

¹³² Ook wel semantische interoperabiliteit conform het EU Interoperability Framework (EIF). Een onderwerp dat in gegevensuitwisseling in België veel aandacht heeft gekregen en waarmee daar resultaten geboekt zijn.

¹³³ www.geonovum.nl/geo-standaarden/metamodel-informatiemodelling-mim

¹³⁴ en.wikipedia.org/wiki/FAIR_data

¹³⁵ Dit wordt vaak “data bij de bron” genoemd; het gaat om bron in “logische/functionele” zin.



- Burgers kunnen via ‘Mijnoverheid’¹³⁶ zicht krijgen op door overheden uitgewisselde gegevens over henzelf¹³⁷
 - Via het principe van *linked data* kunnen verbanden tussen dataobjecten in meerdere kernregistraties worden vastgelegd¹³⁸.
 - Wetsvoorstel open datarichtlijn (herziening Wet Hergebruik overheidsinformatie) en ander beleid om de beschikbaarheid en kwaliteit van overheidsdata te vergroten.
- > **Bouwstenen**
- De Nederlandse Basisregistraties zijn cruciaal voor functioneren digitale overheid.
 - Er is een voorziening waarmee overheidsorganisaties onjuistheden in basisregistraties kunnen melden, Digimelding¹³⁹. Deze beperkt zich momenteel tot de authentieke gegevens in specifieke omstandigheden (gerede twijfel in relatie tot rechtsfeiten).
 - Voor definities en semantiek conformeren we ons aan de Stelselcatalogus van de Nederlandse Basisregistraties en benutten we data.overheid.nl en waar van toepassing de DCAT standaard¹⁴⁰ voor het vindbaar maken en beschrijven van concrete datasets.
 - Voor het metadateren van overheidsinformatie hanteren we de MDTO-standaard (Metagegevens voor duurzaam toegankelijke overheidsinformatie)¹⁴¹.
 - Huidige overheidsbrede semantische en logische gegevensmodellen c.q. informatiemodellen beperken zich tot de basis- en kernregistraties (zie het schema op de volgende pagina). Een model op dat niveau dat interactie ondersteunt draagt bij aan betere afspraken en standaarden voor dienstverlening¹⁴².

¹³⁶ Conform omgang met bouwstenen als beschreven in inleiding (hfd. 1) is dat niet per se een functie van de huidige mijnoverheid.nl dienst. Er zijn ook andere implementaties denkbaar.

¹³⁷ Dit is nadrukkelijk “via”. Mijnoverheid is dus geen alomvattende centrale voorziening, maar vaak een toegang naar achterliggende portalen of informatiebronnen.

¹³⁸ Bijvoorbeeld: Linked Data Overheid (LiDO): een databank met miljoenen hyperlinks - om snel inzicht te krijgen in de verbanden tussen nationale en Europese regelgeving, uitspraken van Nederlandse en Europese rechters, parlementaire documenten en officiële bekendmakingen. LiDO maakt daartoe onder meer gebruik van intelligente software die tal van citatievormen kan herkennen.

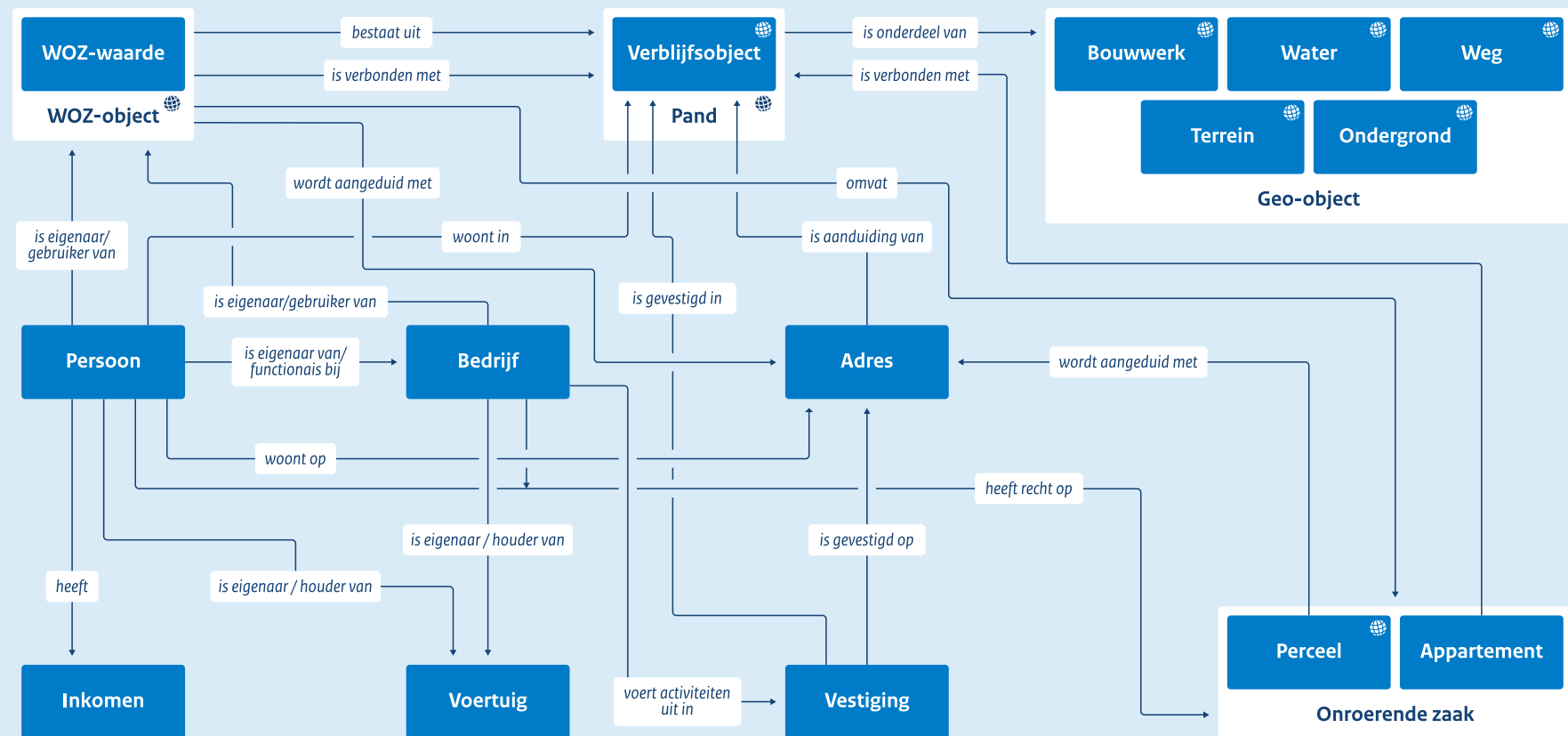
¹³⁹ www.logius.nl/diensten/digimelding

¹⁴⁰ standaarden.overheid.nl/dcat

¹⁴¹ www.nationaalarchief.nl/archiveren/mdto Er loopt een proces om te zorgen dat de MDTO breed genoeg is voor toepassing in de hele overheid. Brede metadatastandaarden die zowel voor archivering als voor openbaarmaking geschikt zijn vereisen nog nadere beleidsvorming; onder andere in relatie tot TOOI (als verderop genoemd).

¹⁴² Bijvoorbeeld voor het concept “zaak” is dat voor gemeenten in de GEMMA wel gedaan, maar niet overheidsbreed. Bijvoorbeeld “Bericht” en “Notificatie” zijn begrippen die verdere gestandaardiseerd kunnen worden.

 Bevat geometrie





6.3 Technische architectuur / infrastructuur

6.3.1 Netwerken

> Wat willen we?

We willen dat we via netwerkservices data door middel van (bij voorkeur) API's op een snelle, betrouwbare en veilige manier kunnen uitwisselen. In het kader van informatiebeveiliging geven we de voorkeur aan een of enkele netwerken die volledig onder verantwoordelijkheid van de overheid vallen. Ter wille van technische eenvoud, flexibiliteit en kostenbesparing, willen we een zo beperkt mogelijk aantal netwerkkoppelingen tussen netwerken.

> Uitgangspunten

- Voor onderlinge communicatie tussen overheidsorganisaties maken we bij waar nodig gebruik van besloten netwerken als Diginetwerk en het Rijksoverheids Netwerk (RON)¹⁴³. Met Diginetwerk kunnen alle organisaties met een publieke taak onderling

gegevens uitwisselen in het kader van de dienstverlening aan burgers en bedrijven. Het besloten karakter biedt veiligheidsvoordelen zolang zero trust (zie § 7.2) nog onvoldoende is doorgevoerd en biedt ook daarna bescherming tegen capaciteits-aanvallen (DDOS e.d.) vanuit openbare internet¹⁴⁴. Mits goed toegepast kan het ook efficiënter zijn grootschalige datastromen over verbindingen in eigen beheer te routeren.

- Zie voor een nadere uitwerking van netwerkstandaarden: www.logius.nl/diensten/diginetwerk/documentatie/diginetwerk-architectuurdocument en Herziening Europese Richtlijn Netwerk- en Informatiebeveiliging (NIB2)¹⁴⁵ welke opgenomen gaat worden in nieuwe versie van de Cybersecuritywet (Wet beveiliging netwerk- en informatiesystemen).
- Met het oog op betrouwbare werking, security en schaalbaarheid vormt software defined networking de voorkeursoplossing.¹⁴⁶

> Bouwstenen

- Voor het onderling uitwisselen van gegevens maken organisaties met een publieke taak waar nodig gebruik van het besloten Diginetwerk¹⁴⁷ of RON¹⁴⁸.

- Diginetwerk biedt ook een oplossing voor koppeling met cloudomgevingen van commerciële partijen¹⁴⁹.
- RINIS biedt het Nationaal Aansluit Punt (NAP) van EU-netwerk TESTA¹⁵⁰ en eDelivery.
- Overheidsorganisaties implementeren consequent de volledige set internet beveiligingsstandaarden die via Forum Standaardisatie verplicht wordt¹⁵¹. Deze standaarden zijn niet alleen op grond van het pas-toe-of-leg-uit beleid voorgeschreven maar veelal ook de voorgeschreven implementatie om aan de Baseline Informatiebeveiliging Overheid (BIO) en andere wettelijke verplichtingen te voldoen.

6.3.2 Platformen voor dagelijkse exploitatie

> Wat willen we?

Betrouwbare informatievoorziening voor de digitale overheid vereist betrouwbare onderliggende infrastructuur en platformen voor dagelijkse exploitatie “in productie”. Enerzijds gebaseerd op bewezen concepten (betrouwbare *proven technology*), maar anderzijds optimaal gebruik makend van moderne technologie (cloud native). Dit is randvoorwaardelijk voor de benodigde wendbaarheid,

¹⁴³ Er moet nog nader worden bekeken in welke gevallen dit verplicht is en in welke gevallen gewenst. In kader van het cloudbeleid verdient het goed aansluiten van public cloud datacenters op deze besloten netwerken ook nadere aandacht. Mogelijk niet intuïtief, maar het veilig aansluiten van een besloten netwerk op een publieke cloud voorziening is goed mogelijk en ook in andere sectoren gebruikelijk.

¹⁴⁴ Diginetwerk is een publiek-private samenwerking waarover Logius de regie voert, in opdracht van het ministerie van BZK.

¹⁴⁵ Het betreft de richtlijn inzake netwerk- en informatiebeveiliging NIB2 (in het Engels NIS2). Zie: www.nis-2-directive.com

¹⁴⁶ Dit is in toenemende mate de best practice, zie bijvoorbeeld Supply Chain Levels for Secure Artefacts (SLSA) framework of cloud.google.com/blog/products/devops-sre/dora-2022-accelerate-state-of-devops-report-now-out en en.wikipedia.org/wiki/Software-defined_networking

¹⁴⁷ www.logius.nl/diensten/diginetwerk

¹⁴⁸ Ook voor voorzieningen in een (publieke) cloud kan netwerkverkeer via besloten netwerkverbinding voordelen hebben. Aansluitingen van de besloten netwerken op cloudproviders bestaan al en zullen in belang toenemen.

¹⁴⁹ Er staat een actie uit om nader onderzoek te doen naar de datatransportinfrastructuur, inclusief het aspect van direct koppelen van ISP's

¹⁵⁰ “Uitwisseling Internationaal” van RINIS. Zie: www.rinis.nl/nl/uitwisseling-internationaal. Naast TESTA bestaan ook sectorale netwerken voor aansluiting op 'Europa'.

¹⁵¹ www.forumstandaardisatie.nl/open-standaarden/verplicht?domein=125 het betreft o.a.: DNSSEC, IPv6, HSTS, TLS v1.3, RPKI, security.txt, STIX, TAXII en voor e-mail DKIM, DMARC, SPF, STARTTLS, DANE.



hergebruik en kostenefficiëntie in de inrichting van de informatiehuishouding¹⁵². Daarvoor staan ten minste drie wegen open: a) eigen voorzieningen; b) voorzieningen in een gezamenlijk datacenter in overheidsverband of van een private partij of c) gebruikmaken - onder strikte voorwaarden - van een public cloud.

> Uitgangspunten

- Bij het kiezen van technische platformen maken we gebruik van moderne, maar bewezen technologie waarvoor voldoende kennis beschikbaar is.
- We passen de marktstandaarden van gelaagde opbouw van infrastructuur en platform zo conservatief mogelijk toe ("plain vanilla", dat wil zeggen standaard verkiezen boven specifieke aanpassingen die upgrading en patching etc. hinderen) zodanig dat applicaties (cloud native) en data migreerbaar zijn.
- In lijn met de aandacht voor soevereiniteit is portabiliteit, de mogelijkheid om te kunnen migreren ook contractueel en juridisch geborgd.

- Beperkingen op bovenstaande twee punten worden vastgelegd en gerapporteerd als "technische schuld" en meegewogen in het lifecyclemanagement van voorzieningen¹⁵³.
- Overstappen naar de cloud gebeurt veilig en verantwoord volgens een rijksbrede cloudstrategie¹⁵⁴ (die ook geadviseerd wordt voor niet tot rijk behorende overheidsorganisaties). Dat betekent o.a. dat er ruimte is voor hybride cloud oplossingen, waarbij in ieder geval ontwikkel- en testvoorzieningen maximaal gebruik maken van publieke cloud terwijl productie (en gevoelige data) waar nodig in overheidsdatacentra (ODC's) blijven.
- De ene laag van de infrastructuur van het ene overheids-SSC afnemen en dan een volgende laag van een andere SSC leidt tot ongewenste organisatorische complexiteit en afhankelijkheden en dient te worden voorkomen (of tenminste heel goed te worden afgesproken).
- Met het oog op betrouwbare werking, security en schaalbaarheid vormt software defined infrastructuur de voorkeursoplossing.

> Bouwstenen

- Huidige aanbod van infrastructuur (IaaS) vanuit ODC's wordt doorontwikkeld tot een beperkt aantal robuuste voorzieningen waarvan kwaliteit extern toetsbaar is en continuïteit van doorontwikkeling en beschikbaarheid experts geborgd is.
- Huidige aanbod van platformdiensten (PaaS) daarbovenop wordt doorontwikkeld tot een beperkt aantal robuuste platformdiensten. Tenminste enkele daarvan ondersteunen ook hybrid cloud zodat ontwikkel- en test in gestandaardiseerde public cloud kan terwijl productie in één van bovengenoemde ODC IaaS diensten blijft.
- Applicaties van overheidsorganisaties draaien bij voorkeur op een containerplatform¹⁵⁵. Ondanks werk van de Cloud Native Computing Foundation¹⁵⁶ om op dit gebied standaardisatie te bereiken, vereist gebruik van hoogwaardige containerplatformen (bijvoorbeeld gebaseerd op de Kubernetes open standaard¹⁵⁷) veel kennis en ervaring. De innovatie en hoeveelheid keuzes is moeilijk te onderschatten. Er lopen enkele initiatieven om hier binnen de overheid richting aan te geven zoals

¹⁵² Zie Meerjarenvisie GDI § 8.2: De infrastructuur maakt gebruik van hedendaagse technologieën en (cloud)platformen om wendbaar te zijn en gebruik te kunnen maken van nieuwe kansen. Waar mogelijk wordt gebruik gemaakt van gestandaardiseerde technologieën.

¹⁵³ Zie Werkagenda Waardengedreven Digitalisering § 4.3.2 "Implementeren (normen) Rijksbrede Lifecycle Convenant"

¹⁵⁴ www.rijksoverheid.nl/documenten/kamerstukken/2022/08/29/kamerbrief-rijksbreed-cloudbeleid-2022

¹⁵⁵ Met een containerplatform worden de business applicaties van overheidsorganisaties en het onderliggend platform waar deze applicaties op draaien ontkoppeld. Leveranciers van business applicaties richten zich op het ontwikkelen van business functionaliteit en hoeven zich geen zorgen meer te maken over het onderliggende platform.

¹⁵⁶ www.cncf.io

¹⁵⁷ Dit is weliswaar een standaard, zie kubernetes.io, maar in de praktijk moeten daarbinnen vele keuzes gemaakt worden, zie bijvoorbeeld landscape.cncf.io/card-mode?category=certified-kubernetes-distribution&grouping=category



bijvoorbeeld HAVEN¹⁵⁸. Een veel grotere effort is nodig om op dit punt daadwerkelijk van voor GDI bruikbare bouwstenen te spreken¹⁵⁹.

- Overheidsorganisaties maken waar nodig gebruik van de Overheidsdatacenters¹⁶⁰.
- Datacenters zijn ingericht op basis van het “Infra as a service” concept.

6.3.3 Slimme apparaten

> Wat willen we?

Apparaten zoals voertuigen, verkeersregelsystemen, pompen, poortjes, camera’s en sensoren zijn voorzien van eigen waarnemings- en regelsystemen. We spreken over *smart devices* of *Internet of Things*. Ook de overheid beschikt in toenemende mate over slimme apparaten. Ruim voor 2030 hebben we te maken met autonome apparaten gebaseerd op generatieve AI. Daarvoor geldt ook dat „regulering” en inpassing nodig is; nieuwe EU-regelgeving legt daar de basis voor. Software zorgt niet alleen voor een deugdelijk functioneren van deze apparaten, maar genereert ook veel data. Met deze data kunnen de apparaten op afstand in de gaten gehouden worden, maar kunnen zij ook gekoppeld worden aan onder meer besturingssystemen en kan er managementinformatie mee geproduceerd worden. We willen ‘in control’ zijn over deze systemen. Het op basis

van (mogelijk verder uitgebreide) registraties kunnen identificeren van slimme apparaten, hun locatie en wie ervoor verantwoordelijk is, wordt belangrijker. We willen ook de data die zij produceren gebruiken om datagedreven te kunnen sturen en beslissen. En we willen voorkomen dat er ongeoorloofd meegeluisterd wordt of zelfs ingebroken wordt in deze vaak cruciale systemen. Informatiebeveiliging is ook hier van groot belang.

> Uitgangspunten

- Slimme apparaten en hun verbindingen met rekencentra en andere apparaten zijn optimaal beveiligd tegen af luisteren en inbreken.
- Het EU-beleid (Data Verordening) leidt tot Europees geharmoniseerde regels over het gebruik van Internet-of-Things-data en faire toegang tot data geproduceerd door smart producten t.b.v. recht op reparatie, overstap van aanbieder, combineren data uit meerdere IoT-apparaten en gratis toegang tot data van bedrijven bij rampen.
- Door slimme apparaten gegenereerde data wordt alleen tegen afgesproken condities voor derden toegankelijk gemaakt.
- Voor sensordata wordt gebruik gemaakt van internationaal erkende standaarden¹⁶¹.

> Bouwstenen

Op dit punt bestaan er momenteel nog geen echte bouwstenen. Richting 2030 zullen die wel nodig zijn. Daarbij moet gedacht worden aan concepten als *edge computing*¹⁶², *robotica*, *sensing*, *SMART assets* en *digital twinning*¹⁶³.

6.3.4 Huisvesting / fysieke datacenters

> Wat willen we?

Het is noodzakelijk te kunnen beschikken over goed geoutilleerde huisvesting, die voldoet aan klimaat en milieueisen, beveiliging tegen digitale en fysieke aanvallen. Dat gebeurt onder beheer van de overheid, maar het vraagt ook om uitgewerkte afspraken met Publieke Cloud aanbieders voor toepassen publieke cloud vanuit datacentra binnen de landsgrenzen of tenminste binnen de EU, zodat specifieke overheids-eisen vanuit “soevereiniteit” geborgd blijven.

> Uitgangspunten

- Afhankelijk van de ontwikkeling van internationale public cloud datacenterproviders, moet steeds een zorgvuldige afweging worden gemaakt of een datacenter van een (internationale) private partij mag zijn of eigendom van de overheid (EU of NL).

¹⁵⁸ Haven schrijft een specifieke configuratie van Kubernetes voor die dient te worden geïmplementeerd op bestaande technische infrastructuur en het eenvoudiger maakt over te stappen naar een andere infrastructuur indien deze dezelfde Haven-specificatie volgt. Zie: haven.commonground.nl

¹⁵⁹ Dit roept de vraag op of het MIDO-kader de juiste plek is daar meer aan te doen en tenminste de kennisdeling binnen de overheid op dit punt te versterken. (Met dank aan diverse reviewers die aangegeven hebben dat dit een issue is waar we niet licht overheen kunnen stappen).

¹⁶⁰ In verband met continuïteitsgarantie voor maatschappelijk kritische dienstverlening, dienen ook ZBO’s de mogelijkheid te krijgen gebruik te maken van fysieke infrastructuur en datacenters die in eigendom van de overheid zijn.

¹⁶¹ Zie onder andere: www.geonovum.nl/themas/platform-voor-verkenning-sensordata-making-sense-for-society#verkenning

¹⁶² Zie: www.iso.org/standard/74846.html

¹⁶³ Zie onder meer: www.wijsmetlocatie.nl/wat-we-doen/digital-twin



- Overheidsorganisaties moeten weten op welke fysieke locatie en in welke jurisdictie hun voorzieningen en data zich bevinden, dit o.a. in kader van vanuit wet- en regelgeving verplichte risicoanalyses en privacyassessments.
- In 2030 zal ICT-infrastructuur aantoonbaar aan duurzaamheidseisen moeten voldoen. Dit heeft al ruim voor 2030 impact op te maken keuzes.

> **Bouwstenen**

Enkele door de rijksoverheid beheerde datacenters met onderlinge uitwijkmogelijkheden.

6.4 Samenhang

In de voorgaande paragrafen is een groot aantal voorzieningen of werkende componenten van de Digitale Overheid de revue gepasseerd. Met het in hoofdstuk 5 gepresenteerde model van de architectuur, kunnen we de besproken voorzieningen enigszins groeperen. Het verrijkte model op de volgende pagina' toont een groot aantal belangrijke, vooral bestaande, voorzieningen die samen invulling geven aan de architectuur van een (werkende) digitale overheid.

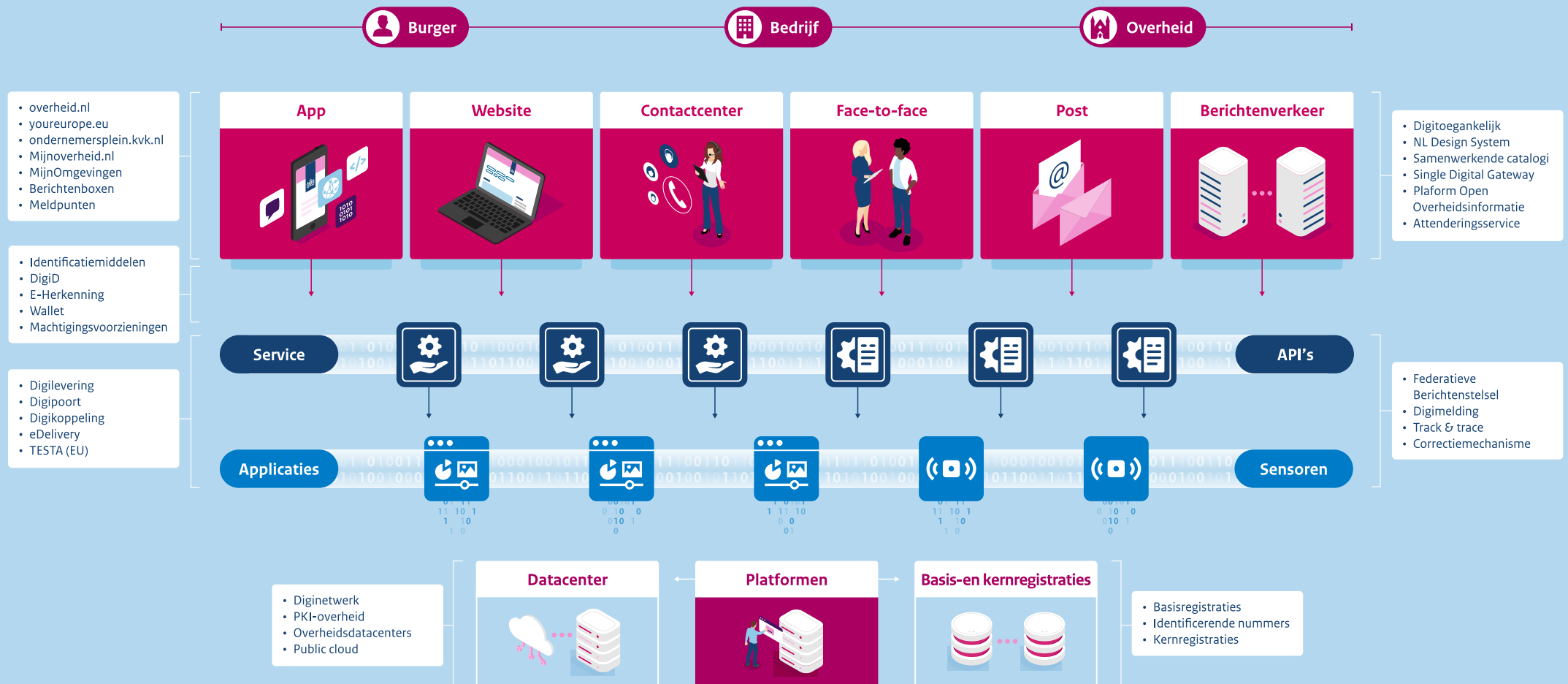
We moeten ons realiseren dat veel voorzieningen onderling samenhangen. Met name de voorzieningen in de linker- en rechterbovenhoek van het model, kunnen niet bestaan

zonder gebruik te maken van een of (vaak) meerdere voorzieningen in het midden en in de linker- en rechterhoek beneden.

Elke voorziening kent op zijn beurt vaak al een nader uitgewerkte architectuur. Daarin zijn – als het goed is – ook de relaties met andere voorzieningen meer expliciet zichtbaar. Door deze voorzieningen te beschouwen als 'legoblokjes' kan vanuit verschillende verantwoordelijkheden en organisaties de digitale overheid gebouwd worden.

In bijlage 1 is een tabel opgenomen waarin deze voorzieningen kort worden omschreven. Tevens is een link toegevoegd naar een (belangrijke) vindplaats van meer informatie over de betreffende voorziening.

Architectuur digitale overheid 2030



7 Aspectgebieden

De aspectgebieden privacy, beveiliging, ontwikkeling en beheer vormen een andere doorsnede met aandachtspunten over de gehele breedte van de digitale overheid. Deze worden hier apart beschreven.

Voor de aspectgebieden geldt dat iedere overheidsorganisatie haar eigen verantwoordelijkheid neemt. De bouwstenen van de Digitale Overheid hiervoor bestaan enkel uit standaarden en afspraken. Veelal direct afgeleid van wettelijke verplichtingen die ook los van de Digitale Overheid gelden.

7.1 Privacybescherming

> Wat willen met betrekking tot privacybescherming?

We willen dat persoonsgegevens afdoende beschermd zijn¹⁶⁴. We willen dat mensen regie kunnen houden over hun gegevens. In onze samenleving moeten mensen erop kunnen vertrouwen dat bedrijven en de overheid zorgvuldig omgaan met hun gegevens¹⁶⁵. De Algemene verordening gegevensbescherming en aanvullende specifieke wetten voor bijvoorbeeld justitiële of zorgdomein bieden hiervoor de kaders.

> Uitgangspunten, gebaseerd op de Algemene verordening gegevensbescherming (Avg)

- Overheden mogen alleen persoonsgegevens verwerken als het niet anders kan. Dus: als zij zonder deze gegevens hun doel niet kunt bereiken.

- Er is een grondslag nodig om persoonsgegevens te mogen verwerken¹⁶⁶. Bij de overheid is dit vrijwel altijd een grondslag vanuit een wet¹⁶⁷.
- Mensen hebben het recht een kopie te ontvangen van de persoonsgegevens die worden verwerkt.¹⁶⁸
- Mensen hebben in bepaalde mate het recht om 'vergeten' te worden. Voor de overheid prevaleren de wettelijke bewaartermijnen en archiveringsvoorschriften.
- Mensen hebben verschillende rechten zoals: rectificatie, aanvulling, beperking van de verwerking, profilering, bezwaar en het recht om te weten wat een organisatie met de persoonsgegevens doet. Consequentie is dat overheden uitgebreide verplichtingen tot het loggen van gegevensverwerking hebben.
- De organisatie moet kunnen aantonen aan de Avg te voldoen, een actueel verwerkingsregister bijhouden en bij veranderingen bepalen of een verwerking van persoonsgegevens in een van de categorieën valt waarvoor uitvoeren van een Data Protection Impact Assessment (DPIA) verplicht is.

¹⁶⁴ Veel privacy-management gerelateerde normen en methoden zijn te vinden op de site van het Centrum Informatiebeveiliging en Privacybescherming (CIP), www.cip-overheid.nl

¹⁶⁵ Voor een architectuuruitwerking hiervan zie www.noraonline.nl/wiki/Privacy

¹⁶⁶ Voor een aantal bijzondere gegevens zijn aanvullende beperking van toepassing. Zie Avg.

¹⁶⁷ Er is momenteel terecht interesse in het Belgische model waarin er een wettelijk aangestelde commissie is die goedkeuring geeft aan verwerking. Dat levert een veel wendbaardere werkwijze die nog steeds binnen Avg kader past.

¹⁶⁸ Er wordt gewerkt aan uitbreiding van deze rechten via de tweede tranche van de Wdo



In de Avg staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

1. U heeft toestemming van de persoon om wie het gaat (tenzij er sprake is van wettelijke toestemming).
2. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
3. Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
4. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
5. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen.
6. Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

Bron: Autoriteit Persoonsgegevens.

(Zie: www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken)

> Bouwstenen

- Verplichte uitvoering van Data protection impact assessment (DPIA) wanneer persoonsgegevens door de overheid verwerkt worden.
- *Privacy by design* (in het ontwerp aandacht voor o.m. doelbinding, dataminimalisatie en afscherming van

gegevens). Op basis van in losse projecten uitgewerkte bouwstenen zullen overheidsbrede *Privacy Enhancing Technology*¹⁶⁹ bouwstenen ontstaan.

- Met organisaties of vertegenwoordigers die een bepaalde groep van belanghebbenden representeren, kunnen afspraken gemaakt worden over het delen van persoonsgegevens. Medegebruik of overhevelen van persoonsgegevens is dan mogelijk, mits er voorzien is in een opt out regeling voor mensen die bezwaar hebben tegen het delen of overhevelen van hun persoonsgegevens naar andere organisaties met het oog op betere en meer pro-actieve dienstverlening. Dit gebeurt al in afsprakenstelsels als Medmij en is ook één van de mogelijke gevolgen van de invoering van Wallet(s) als bouwsteen. Dit kan alleen indien er expliciete persoonlijke toestemming is of wanneer er aanvullende wettelijke ruimte voor wordt afgesproken¹⁷⁰.
- BSNk is een bestaande bouwsteen om het BSN op privacy veilige manier om te zetten in een pseudoniem voor Toegangsvoorzieningen.
- Logging en het voldoen aan transparantieplichtingen vanuit Avg is een bouwsteen die generiek voor de hele digitale overheid geldt. Hier zijn diverse bouwstenen voor ontwikkeld. Meer hergebruik en standaardisatie is mogelijk en kan bijdragen aan de begrijpelijkheid en toegankelijkheid van deze oplossingen voor burgers.

7.2 Informatiebeveiliging

Wat betreft beveiliging is het aanwijzen van onderdelen van de digitale overheid als “vitale of essentiële voorziening” een belangrijk aspect. Dit biedt een duidelijk kader. Meerdere basisregistraties en GDI-voorzieningen (BRP, HR en DigiD)¹⁷¹ zijn al aangewezen als vitaal en op grond van de EU NIS2 richtlijn zal dit verder worden uitgebreid.

> Wat willen we?

We willen dat:

- de beschikbaarheid, vertrouwelijkheid en integriteit;
- van diensten, processen, infrastructuur, informatie en data;
- die de overheid produceert, beheert, gebruikt, verwerkt en aanbiedt;

op een passende wijze zijn beveiligd tegen compromittatie¹⁷². Er wordt gezorgd dat de overheid zowel haar intern- als extern gerichte diensten goed toegankelijk zijn. Ook wordt voorkomen dat vertrouwelijke of persoonlijke gegevens in verkeerde handen komen. Onweerlegbaarheid, transparantie en privacy worden op een passende wijze toegepast om beveiligingsincidenten en eventueel de bron van compromittatie te achterhalen.

Om bovenstaande te realiseren is het nodig dat beveiliging door de gehele architectuur wordt beleefd¹⁷³. Beveiliging is geen afzonderlijke tak van sport en niet enkel behouden voor de IT-organisatie. Op alle vlakken van de architectuur

¹⁶⁹ Zie: Nationaal Innovatiecentrum Privacy Enhancing Technologies (NICPET), Ministerie BZK.

¹⁷⁰ Een voorbeeld hiervan is de Belgische parlementaire commissie die daar dit soort uitwisselingen vooraf goedkeurt onder Avg regime

¹⁷¹ zie www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

¹⁷² Veel cyber security normen en methodes zijn te vinden op de site van NCSC NL, [Alle publicaties | Nationaal Cyber Security Centrum \(ncsc.nl\)](http://Allepublicaties.NationaalCyberSecurityCentrum(ncsc.nl))

¹⁷³ Voor een architectuuruitwerking hiervan zie www.noraonline.nl/wiki/Beveiliging



is beveiliging een onderdeel – van de inrichting van doelstellingen en processen tot het implementeren van beveiligingsmaatregelen.

Het ontwerp op de verschillende architectuurlagen wordt gebaseerd op criteria die worden vastgesteld als uitkomst van een risicoanalyse. Onderdeel van deze analyse is een classificatie van te beschermen belangen, zoals (industriële) objecten, (gevoelige, bestuurlijke) overheidsinformatie, persoonsgebonden (bijzondere) gegevens, et cetera. Ook worden er realistische dreigingsscenario's opgesteld. Deze vormen samen de basis voor het uitvoeren van omgevings- en risicoanalyses.

Risico-eigenaarschap is fundamenteel vervlochten met de architectuurinrichting en vereist het onderbouwen van ontwerpkeuzes in de architectuur. Er wordt hierbij een koppeling gemaakt tussen de risico's op het niveau van bedrijfsarchitectuur met daarbij een doorvertaling richting informatie- en technische architectuur. Beveiliging kan enkel goed worden ingericht als deze een traceerbare vertaling kent van breed-gedragen (bedrijfs-)risico's naar implementatie.

Dat wil zeggen: Het moet duidelijk zijn waarom bepaalde beveiligingsmaatregelen getroffen worden.

> Uitgangspunten

- Combinatie van EU-richtlijnen op gebied van cyberveiligheid en Nederlands beleid vormt de basis voor maatregelen. Bouwstenen van de Digitale Overheid geven prioriteit aan het tijdig voldoen aan alle maatregelen.¹⁷⁴
- Architectuurkeuzes (een passend controle framework) baseren zich op een omgevingsanalyse en een risicoanalyse¹⁷⁵.
- In risicoanalyses wordt zowel gekeken naar de noodzaak toegang te beperken als het belang om informatie en API's openbaar toegankelijk te maken.
- Beveiliging is een onderwerp in alle architectuurlagen, met een traceerbare duiding tussen risico's en beveiligingskeuzes tussen deze lagen.
- Flexibiliteit in de architectuur zodat deze veerkrachtig en wendbaar is voor veranderende risicobeelden.
- (Concept) e-Privacy Directive¹⁷⁶
- Voorstel Cyber Resilience Act¹⁷⁷
- Baseline Informatiebeveiliging Overheid¹⁷⁸ (BIO),

concreet gemaakt een Information Security Management System (ISMS) waarin de koppeling wordt gelegd tussen geclassificeerde risico's en de voor betreffende organisatie geïmplementeerde maatregelen. ISO27001¹⁷⁹ biedt hiervoor meer handvatten dan BIO op zichzelf.

- Zero Trust is in toenemende mate een uitgangspunt voor het afschermen en modereren van infrastructuur en de toegang tot informatie. Dit hangt samen met toenemende opsplitsing van functionaliteit over losjes gekoppelde services met API's en met cloud native architectuur. Bestaande voorzieningen die niet met dit uitgangspunt gerealiseerd zijn, kunnen echter niet eenvoudig worden omgezet¹⁸⁰.
- #### > Bouwstenen
- Baseline Informatiebeveiliging Overheid (BIO) en daaruit voortvloeiende verdere inrichting en verplichtingen
 - Privacy by design (in het ontwerp aandacht voor o.m. doelbinding, dataminimalisatie en afscherming van gegevens). Toepassen Privacy Enhancing Technologies¹⁸¹
 - Bij het gebruik van open standaarden worden deze conform de door Forum Standaardisatie beschreven

¹⁷⁴ Kamerbrief "Hoofdpijnen beleid voor digitalisering" 8 maart 2022, 0000123877, blz. 6.

¹⁷⁵ NCSC factsheet over Risicomanagement: *Risico's beheersen: de waarde van informatie als uitgangspunt*.

¹⁷⁶ *Proposal for an ePrivacy Regulation* (europa.eu)

¹⁷⁷ *Cyber Resilience Act* (europa.eu)

¹⁷⁸ BIO (Baseline Informatiebeveiliging Overheid) - NORA Online Toepassing is verplicht op basis van wetten.overheid.nl/BWBR0043146/2020-02-12/#Bijlage en er is aangekondigd in het Actieplan Nederlandse Cybersecuritystrategie 2022-2028 (zie ook brief aan Tweede Kamer 29-9-2022, 26643 Nr. 917) dat dit een zwaardere directe wettelijke verplichting wordt via de Wdo.

¹⁷⁹ NEN-ISO/IEC 27001 - NORA Online

¹⁸⁰ NCSC publiceert factsheet 'Bereid u voor op Zero Trust'

¹⁸¹ Zie: Nationaal Innovatiecentrum Privacy Enhancing Technologies (NICPET), Ministerie BZK.



richtlijnen ontworpen en geïmplementeerd, zowel de verplichte standaarden¹⁸² als de aanbevolen standaarden¹⁸³.

- Toepassing van vanuit pas-toe-of-leg-uit beleid en vanuit BIO maatregelen verplichte standaarden (ook al genoemd bij netwerk-bouwstenen) wordt consequent uitgevoerd en getest¹⁸⁴
- Gebruik van de tool inkoop-eisen cybersecurity overheid (ICO) of vergelijkbare in uniforme inkoopvoorwaarden verwerkte eisen¹⁸⁵
- Voor Industriële Automatisering en Control Systemen hanteren we de Cybersecurity Implementatierichtlijn Objecten (CSIR) als normering¹⁸⁶.

7.3 Softwareontwikkeling

> Wat willen we?

In de eerste plaats willen we zoveel mogelijk gebruikmaken van applicaties en voorzieningen die binnen de overheid al beschikbaar zijn (hergebruik, medegebruik) of van op de markt beschikbare standaard-applicaties¹⁸⁷, componenten en voorzieningen. Daarmee verschuift het zelf ontwikkelen naar het derde plan. Waar het ontwikkelen van specifieke functionaliteit door eigen medewerkers of door gespecialiseerde bedrijven in opdracht van de overheid toch de beste keuze is, moet dit leiden tot een voor andere overheidsorganisaties herbruikbaar product ("open source"). Bij de aanschaf of ontwikkeling van software, speelt de eis van het waar mogelijk toepassen van 'open source' een belangrijke rol.

> Uitgangspunten

- Hergebruik/medegebruik van software, gaat voor aanschaf van standaard software, gaat voor zelfbouw voor gelijkwaardige functionaliteiten.
- Wanneer in opdracht van de overheid software geproduceerd wordt, wordt afgewogen of het

verantwoord is deze openbaar te maken, conform de beleidslijn Open, tenzij.

- Hergebruik binnen de overheid stelt hoge eisen aan de onderliggende software, dit maakt de toenemende aandacht voor Lifecyclemanagement des te belangrijker¹⁸⁸.
- We streven naar Continuous Integration en Continuous Deployment (CI/CD). Dit stelt ons in staat snel in te spelen op bedreigingen en onvoorziene ontwikkelingen en omstandigheden. Dit is in lijn met de brede marktontwikkeling naar DevOps¹⁸⁹.
- > **Bouwstenen**
 - Door overheid gestandaardiseerde licenties voor het publiek beschikbaar maken van in opdracht van overheid geproduceerde software (bijvoorbeeld EU PL¹⁹⁰)
 - Voor het ontwikkelen van software hanteren we de methode en normen voor Secure Software Ontwikkeling¹⁹¹ en de Non Product Related NEN-norm voor softwareontwikkeling en onderhoud¹⁹².
 - Software voldoet aan de meest recente ISO 25010 norm.

¹⁸² Verplichte standaarden | Forum Standaardisatie

¹⁸³ Aanbevolen standaarden | Forum Standaardisatie

¹⁸⁴ Een goede testmethode is beschikbaar in de vorm van internet.nl, een publiek-private samenwerking.

¹⁸⁵ Gemeenten hebben cybersecurity eisen verwerkt in de GIBIT. Aannee is dat daarin gelijksoortige eisen zijn opgenomen. Zie vng.nl/projecten/gibit

¹⁸⁶ Zie: www.cert-wm.nl/csir

¹⁸⁷ Waarbij de valkuil dat een bepaalde applicatie "standaard" lijkt maar in praktijk een soort van maatwerkoplossing voor een te kleine doelgroep is, vermeden moet worden.

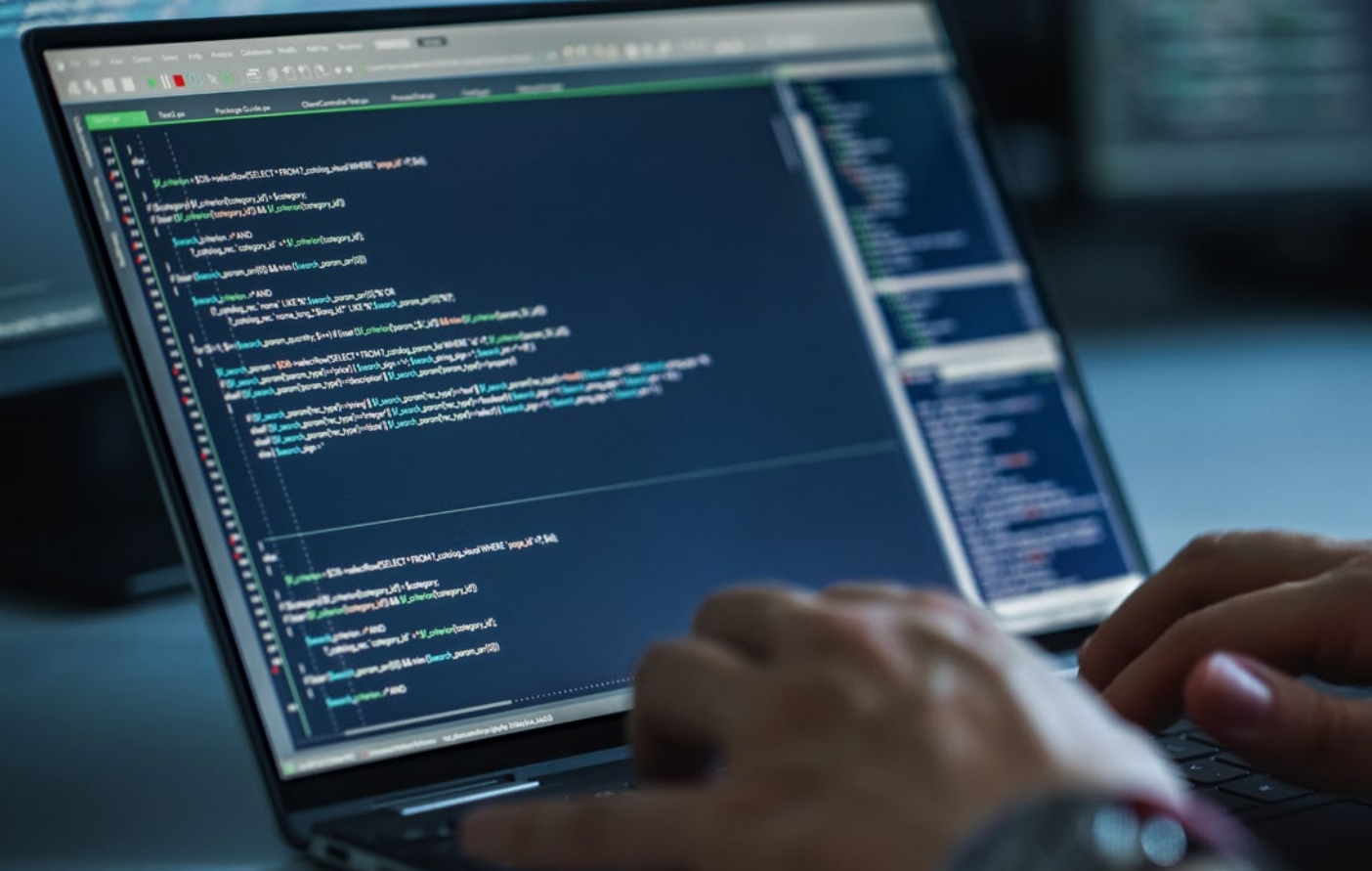
¹⁸⁸ www.rekenkamer.nl/onderwerpen/verantwoordingsonderzoek/over-dit-onderzoek/beoordelingskaders/beoordelingskader-it-lifecyclemanagement

¹⁸⁹ Zie bijvoorbeeld cloud.google.com/blog/products/devops-sre/dora-2022-accelerate-state-of-devops-report-now-out

¹⁹⁰ commission.europa.eu/content/european-union-public-licence_en

¹⁹¹ Zie: www.cip-overheid.nl/productcategorieen-en-workshops/?type=Secure%20Software

¹⁹² www.nen.nl/npr-5326-2019-nl-262885



- We stappen over op nieuwe standaarden en technologie zodra deze zijn vastgesteld, resp. dominant gaan worden.
- We laten door onafhankelijke experts periodiek audits uitvoeren op de werking en beveiliging van onze systemen.

> Bouwstenen

- Voor het monitoren van systemen en apparaten maken we gebruik van Open Telemetry¹⁹⁵.
- Voor beheer en onderhoud werken we volgens ITIL-principes (die inmiddels goed compatibel zijn met Agile en DevOps werkwijzen)¹⁹⁶.
- Voor het beheren van open standaarden hanteren we het Beheer- en OntwikkelModel voor Open Standaarden (BOMOS-model)¹⁹⁷.

7.4 Beheer en exploitatie

> Wat willen we?

Vanwege de afhankelijkheid van een goede informatievoorziening, stellen we hoge eisen aan het beheer en onderhoud ervan. We zorgen voor een uitstekend lifecyclemanagement, zodat we gelijke tred houden met modernisering, nieuwe technologieën en nieuwe dreigingen¹⁹³.

> Uitgangspunten

- We hanteren een solide lifecyclemanagement¹⁹⁴.
- We beschikken over uitstekende beheer en monitoringsystemen.
- We maken gebruik van de jongste versie van open standaarden (zeker waar het beveiliging betreft) en we spreken elkaar aan op het voldoen aan dit uitgangspunt. Achterblijven wordt vastgelegd in de vorm van technische schuld en gerapporteerd.

¹⁹³ Zie Werkagenda Waardengedreven Digitalisering § 4.3.2 LCM en § 2.4 cybersecurity

¹⁹⁴ Hiervoor dient bij de ontwikkeling en ingebruikname een goede afspraak gemaakt te worden over het benodigde budget op langere termijn.

¹⁹⁵ Zie: opentelemetry.io

¹⁹⁶ Zie: nl.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

¹⁹⁷ logius.nl/domeinen/infrastructuur/bomos/wat-is-het. Zie ook Forum Standaardisatie: Uitstekend Beheer op www.forumstandaardisatie.nl/open-standaarden/toetsen-en-aanmelden

Bijlagen

- ▶ 1 Overzicht bouwstenen digitale overheid
- ▶ 2 Relatie bouwstenen met E.U.-verordeningen
- ▶ 3 Begrippenlijst
- ▶ 4 Betrokkenen bij de totstandkoming van deze versie





Bijlage 1: Overzicht bouwstenen digitale overheid

De onderstaande lijst bevat een overzicht van de bouwstenen van de digitale overheid, zoals bekend per mei 2023.

1.1 Bouwstenen voor Diensten en producten

Bouwsteen	Bouwsteenonderdelen	Toelichting
Attenderingsservice	Berichten over uw buurt	Via Berichten over uw buurt zoekt u naar berichten van overheidsorganisaties, die invloed hebben op uw leefomgeving. Vanuit het zoekresultaat kunt u doorklikken naar het bericht zelf. Deze berichten staan op officiële bekendmakingen.nl. Het is ook mogelijk een abonnement te nemen.
Basisregistratie Personen en Handelsregister (voor registratie van personen die een relatie met de Nederlandse overheid hebben)	BRP	Authentieke bron voor persoonsgegevens van burgers en van buitenlanders die met Nederland te maken hebben.
	Handelsregister	Authentieke bron voor gegevens van ondernemers, rechtspersonen en gemeenten in Nederland.
	Burgerservicenummer (BSN)	Het burgerservicenummer (BSN) is een uniek persoonsnummer voor iedereen die ingeschreven staat in de Basisregistratie Personen (BRP).
	Beheervoorziening BSN	De Beheervoorziening burgerservicenummer (BV BSN) is het geheel van voorzieningen dat zorgt voor het beheer van het burgerservicenummer (BSN).
	BSNk PP	BSNk zorgt ervoor dat zowel publieke als private toegangsdiens op een veilige, consistente en privacy vriendelijke manier een burger kan identificeren voor publieke en private dienstverlener met een BSN (indien geautoriseerd) of dienstverlener specifiek persistent pseudoniem (technisch een zogeheten polymorf pseudoniem).
Berichtenbox voor Bedrijven	KvK-nummer en Rechtspersonen en Samenwerkingsverbanden Informatienummer (RSIN)	Elke onderneming of maatschappelijke activiteit krijgt in het Handelsregister één KVK-nummer. Elke Niet Natuurlijke Persoon (samenwerkingsverband of rechtspersoon), hierna te noemen NNP krijgt in het Handelsregister één door KVK uit te geven Rechtspersonen Samenwerkingsverbanden Informatie Nummer (het RSIN).
	berichtenbox. antwoordvoorbedrijven.nl	Met de Berichtenbox voor bedrijven kunt u als ondernemer digitaal berichten uitwisselen met Nederlandse overheidsorganisaties. En overheidsorganisaties kunnen veilig en gemakkelijk digitale berichten versturen aan u.
Centraal Meldpunt Identiteitsfraude	Niet van toepassing	Het Centraal Meldpunt Identiteitsfraude (CMI) registreert meldingen van identiteitsfraude en ondersteunt en adviseert slachtoffers.
Certificaten	PKI-overheid	Voor system-to-system toegang worden op certificaten gebaseerde oplossingen toegepast. PKI-overheid is een voorziening voor de uitgifte van certificaten voor betrouwbare identificatie, digitale handtekeningen en veilige gegevensuitwisseling.



Bouwsteen	Bouwsteenonderdelen	Toelichting
Digitaal Ondernemersplein	ondernemersplein.kvk.nl	Via Ondernemersplein.kvk.nl vindt u informatie en advies van de (semi)overheid. Alles wat u nodig heeft om te ondernemen.
Eenmalig inloggen (single sign on)	Security Assertion Markup Language (SAML) (verplichte standaard)	Security Assertion Markup Language (SAML) is een standaard voor het veilig uitwisselen van authenticatie- en autorisatiegegevens van gebruikers tussen verschillende organisaties.
	OpenID Connect (OIDC) (aanbevolen standaard)	OpenID Connect (OIDC) is een open en gedistribueerde manier om één authenticatiedienst naar keuze te kunnen hergebruiken bij meerdere (semi)overheidsdienstverleners, bij gebruik vanuit onder andere webapplicaties en mobiele apps.
Federatief Berichtenstelsel	- Interactielaag - Generieke Services: Berichtenlijst Service, Notificatie Service, Notificatieprofiel Service, Digitale Bereikbaarheid Service - Berichtenmagazijnen - Afsprakenstelsel	FBS is een stelsel waarbij gebruik wordt gemaakt van een aantal generieke services, eigen berichtenmagazijnen van de aangesloten organisaties en één centrale voorziening, de Berichtenbox.
Mijn eenmanszaak	www.kvk.nl/mijnondernemingen	Met 'Mijn eenmanszaak' kun je snel controleren of de gegevens van jouw bedrijf nog juist zijn. Kloppen de gegevens niet? Dan kun je meteen een wijziging doorgeven.
Mijnomgevingen (voor het bewaren en toegankelijk maken van correspondentie)	Niet van toepassing	Burgers en ondernemers kunnen per brief, mail of via een notificatie (digitale) post van de overheid ontvangen. De overheid bewaart deze correspondentie gedurende een bepaalde termijn in diverse mijnomgevingen.
MijnOverheid Berichtenbox	- mijn.overheid.nl - App "Berichtenbox"	MijnOverheid is het persoonlijke portaal van de overheid voor burgers. Op de website van MijnOverheid of via de Berichtenbox en MijnGegevens app hebben burgers overzichtelijk, veilig en gemakkelijk toegang tot de overheid. Zij kunnen gegevens over henzelf inzien en post van de overheid ontvangen in de digitale Berichtenbox.
	Federatief Berichtenstelsel	MijnOverheid Berichtenbox maakt onderdeel uit van het Federatief Berichtenstelsel.
MijnOverheid Persoonlijke Gegevens	- mijn.overheid.nl - App "Mijn Gegevens"	Zie MijnOverheid Berichtenbox Lopende zaken (zal als MijnZaak hier onderdeel van worden) Delen van gegevens (delen van gegevens uit de BRI via MijnOverheid met de woningbranche en verdere uitbreidingen in kader van WWD-prioriteiten)
Nederland Wereldwijd	www.nederlandwereldwijd.nl	Op nederlandwereldwijd.nl vindt u alle informatie van de Nederlandse overheid op 1 plek. Voor als u in het buitenland bent. Of daar naartoe gaat.



Bouwsteen	Bouwsteenonderdelen	Toelichting
Organisatie-identificatienummer (OIN)	Centrale OIN	Het Organisatie-identificatienummer (OIN) is een uniek nummer dat Logius kan toekennen aan organisaties om zich te kunnen identificeren, authenticeren en of autoriseren bij digitaal berichtenverkeer binnen en met de overheid. Dit kunnen publieke en private organisaties zijn.
	Raadpleegvoorziening (COR)	Het COR geeft een overzicht van alle uitgegeven openbare Organisatie -identificatienummers (OIN)
Overheid.nl	www.overheid.nl	De website Overheid.nl is de wegwijzer naar informatie en diensten van alle overheidsorganisaties in Nederland.
	organisaties.overheid.nl (Register Overheidsorganisaties)	Het Register Overheidsorganisaties biedt toegang tot informatie van alle overheidsorganen in Nederland.
	wetten.overheid.nl	In het onderdeel Wet- en regelgeving vindt u de verdragen, wetten, ministeriële regelingen, algemene maatregelen van bestuur en andere koninklijke besluiten, regelgeving van zelfstandige bestuursorganen (ZBO's) en de publiekrechtelijke bedrijfsorganisatie (PBO) en de wetten en regels die per 10-10-2010 van kracht zijn geworden voor de BES-eilanden (Bonaire, Sint Eustatius en Saba).
	officielebekendmakingen.nl	officielebekendmakingen.nl is de authentieke bron voor officiële bekendmakingen en parlementaire documenten
	lokaleregelgeving.overheid.nl	In het onderdeel 'Lokale wet- en regelgeving' vindt u de geconsolideerde teksten van algemeen verbindende voorschriften, vastgesteld door een decentrale overheid.
	Platform Open Overheidsinformatie (PLOOI) open.overheid.nl	Het platform open overheidsinformatie maakt overheidsinformatie op één centrale plaats toegankelijk. De documenten in dit portaal worden actief openbaar gemaakt onder de Wet open overheid (Woo)
	Thesaurus en Ontologie voor OverheidsInformatie (TOOI)	TOOI is een model van de informatie die gepubliceerd wordt door alle organisaties binnen de Nederlandse overheid ¹⁹⁸ . Met behulp van het TOOI-model kan die informatie in samenhang vindbaar gemaakt worden over organisaties en informatiesystemen heen. Organisaties binnen en buiten de overheid kunnen TOOI gebruiken om de inhoud van hun informatiesystemen van metadata te voorzien, waardoor deze eenvoudig gerelateerd kan worden aan inhoud uit andere bronnen die met TOOI zijn verrijkt.
	Verdragenbank.overheid.nl	De verdragenbank bevat de gegevens van de verdragen, waarbij het Koninkrijk der Nederlanden partij is. Deze informatie is toegankelijk via de website verdragenbank.overheid.nl.
	Wetgevingskalender.overheid.nl	Op de website wetgevingskalender.overheid.nl staat alle informatie over wetgeving-in-wording. Iedereen kan zo exact inzien welke aankomende wetten en algemene maatregelen van bestuur er in de wachtlijst staan.
	Internetconsultatie.nl	Via internetconsultatie.nl kan iedereen reageren op concept wet- en regelgeving die door het kabinet of het parlement worden voorbereid.

¹⁹⁸ Er loopt een traject om nader beleid te maken rond metadatering zodat zowel de archiefkant als de openbaarmaking, zaakgericht werken en datagedreven dynamiek van primaire processen bij elkaar komen.



Bouwsteen	Bouwsteenonderdelen	Toelichting
Registraties voor 'restgroepen'	Niet van toepassing	Voor 'restgroepen' (burgers en bedrijven niet bekend in BRP en HR) worden aanvullende oplossingen/bouwstenen ontwikkeld (zoals een entiteitenregister). Het streven is naar een beperkt aantal bouwstenen voor deze restgroepen, bij voorkeur aansluitend op al bestaande registraties
Rijksoverheid.nl	www.rijksoverheid.nl	Op Rijksoverheid.nl informeren ministeries u over wetten en regels van het Rijk
Samenwerkende Catalogi	Afspraken	De Samenwerkende Catalogi (SC) is een set afspraken over het uitwisselen van informatie over producten en diensten van de overheid op het internet. Door productinformatie te labelen met afgesproken labels en waarden kan deze hergebruikt worden.
	Uniforme Productenlijst	De Uniforme Productnamenlijst is een lijst met uniforme naamgeving voor de producten en diensten die de Nederlandse overheid biedt aan burgers en bedrijven.
	OWMS (verplicht)	De Overheid.nl Web Metadata Standaard (OWMS) is de metadatastandaard voor informatie van de Nederlandse overheid op internet. De standaard is gebaseerd op de internationale metadatastandaard van het Dublin Core Metadata Initiative (DCMI)
Single Digital Gateway Your Europe	europa.eu (Your Europe)	Een EU-afsprakenstelsel (EU-verordening) dat moet stimuleren dat alle burgers en bedrijven binnen de EU eenvoudig toegang kunnen krijgen tot overheidsdiensten van alle EU-lidstaten via een Single Digital Gateway in de vorm van de voorziening Your Europe (europa.eu). Your Europe is een EU-site die u helpt problemen en onnodige rompslomp te vermijden als u in een ander EU-land wilt wonen, werken of studeren of daar gewoon iets wilt kopen of op vakantie gaan. Of wanneer u daar als ondernemer actief bent. Your Europe geeft u: 1) informatie over uw grondrechten op basis van de EU-wetgeving, 2) toegang tot een netwerk van nationale portals met informatie over hoe de EU-regels in het betreffende EU-land worden toegepast voor gebruikers uit andere EU-landen (in overeenstemming met de verordening inzake één digitale toegangspoort), 3) gratis uitvoerig en persoonlijk advies van onze EU-hulpdiensten per e-mail of telefoon.
Standaarden voor digitale handtekening	Ades Baseline Profiles (verplicht)	De AdES Baseline Profiles moeten worden toegepast op de ondertekening van XML-, CMS-, PDF- en ZIP-bestanden met geavanceerde en/of gekwalificeerde elektronische handtekeningen, zegels of tijdstempels.
	ETSI TS 119 312 (aanbevolen)	ETSI 119 312 wordt toegepast bij het digitaal ondertekenen van een document of transactie.



Bouwsteen	Bouwsteenonderdelen	Toelichting
Toegangsstelsel incl. machtigen en vertegenwoordigen	Paspoort	Een paspoort is een officieel document dat de houder identificeert als burger van een bepaald land
	Identiteitskaart	De Nederlandse identiteitskaart (NIK) is een plastic kaart met de afmetingen van een bankkaart (zoals gedefinieerd in de internationale standaard ISO 7810) met vrijwel dezelfde gegevens als een paspoort.
	Rijbewijs	Een rijbewijs is een document waarmee een bestuurder van een motorvoertuig kan aantonen dat hij/zij beschikt over voldoende kennis, inzicht en vaardigheid om een motorvoertuig van een bepaalde categorie te kunnen en mogen besturen.
	Elektronische Digitale Identiteit / European Digital Identity	De Europese Digitale Identiteit zal beschikbaar zijn voor EU-burgers, inwoners en bedrijven die zichzelf willen identificeren of bepaalde persoonlijke gegevens op een gewaarmerkte wijze willen verstrekken. Het kan worden gebruikt voor zowel online als offline publieke en private diensten in de hele EU
	European Digital Identity Wallet	The EU Digital ID Wallet will allow European citizens to safely save their documents and personal information in an app (also known as wallet).
	Wet digitale overheid	De Wet digitale overheid (Wdo) regelt de toegang van burgers, ondernemingen en rechtspersonen tot online diensten van publieke dienstverleners.
	Diverse voorzieningen i.h.k.v. het Toegangsstelsel	De Routeringsvoorziening is een voorziening waarop publieke dienstverleners zich éénmalig kunnen aansluiten en daarmee worden ontzorgd voor het afhandelen van alle toegelaten inlogmiddelen (authenticatiemiddelen) die burgers toegang verlenen om hun online zaken te regelen.
	eIDAS verordening	eIDAS verordening: Een EU-afsprakenstelsel over begrippen, digitale identiteiten van burgers, betrouwbaarheidsniveaus en het onderlinge gebruik van digitale infrastructures, waardoor Europese burgers en bedrijven met hun eigen nationale toegangsmiddel kunnen inloggen bij publieke dienstverleners van de andere Europese lidstaten. Vanuit deze verordening bestaan de volgende verdere bouwstenen: • de standaard eIDAS Level of assurance low, substantial and high • de standaard eIDAS minimal dataset (opgelegde gegevensdefinitie) • de NL eIDAS voorzieningen eIDAS koppelpunt, BRPk (identity matching) en eIDAS attributendienst (attribuutvorming).
	- DigiD, mijn.digid.nl, - App "DigiD"	DigiD is een voorziening waarmee overheidsorganisaties en publieke dienstverleners online de identiteit van burgers en kunnen vaststellen.
	eHerkenning	eHerkenning is een authenticatiemiddel waarmee ondernemers, intermediairs en medewerkers veilig kunnen inloggen bij aangesloten (overheids)organisaties
	Toegelaten identificatiemiddelen	Toegelaten identificatiemiddelen: Onder de Wdo toegelaten Nederlandse identificatiemiddelen, waaronder DigiD en eHerkenning.
	Machtigingenregister	In het machtigingenregister staat welke organisatie gemachtigd is voor het digitaal ophalen van berichten en gegevens voor een specifieke klant.
	Inzageregister	Via het inzageregister kan iedereen zelf zien welke middelen er aan zijn of haar BSN zijn gekoppeld. Als blijkt dat er een onbekend middel is gekoppeld, dan kan de persoon zelf actie ondernemen.
	Vertegenwoordigingen-registers	Registers waar vertegenwoordigingsbevoegdheden in zijn vastgelegd of uit kunnen worden afgeleid.



1.2 Bouwstenen voor Kanalen

Bouwsteen	Bouwsteenonderdelen	Toelichting
Customer Operations Performance Center (COPC)	Niet van toepassing	De COPC Customer Experience (CX) standaard biedt richtlijnen en best practices voor het beheren en verbeteren van de gerealiseerde klantervaring.
DigiToegankelijk	- Wet voor digitale toegankelijkheid - Tijdelijk besluit digitale toegankelijkheid overheid - WCAG (verplichte standaard)	DigiToegankelijk is de Nederlandse naam voor de standaard waarmee overheidsorganisaties hun websites en apps toegankelijk moeten maken voor alle burgers. DigiToegankelijk is gebaseerd op een internationale toegankelijkheidsstandaard: de Web Content Accessibility Guidelines (WCAG)
Standaarden voor websites	NL Design System	Set van herbruikbare UX-componenten voor overheidswebsites die ervoor zorgt dat alle overheden die het gebruiken hetzelfde consistente website uiterlijk en gedrag aanbieden.
	Platform Rijksoverheid Online (PRO)	Websites van de Rijksoverheid worden bij voorkeur ontwikkeld via het Platform Rijksoverheid Online (PRO)

1.3 Bouwstenen voor Organisatie

Bouwsteen	Bouwsteenonderdelen	Toelichting
Ketensturing / Bouwstenen voor ketensturing (NORA)	Niet van toepassing	De publicatie “Ketens de baas”

1.4 Bouwstenen voor Processen

Bouwsteen	Bouwsteenonderdelen	Toelichting
Algoritmeregister	algoritme.overheid.nl	Op deze website publiceren overheidsorganisaties de algoritmes die zij gebruiken in hun werk.
Centraal Meldpunt Identiteitsfraude	Niet van toepassing	Zie het Centraal Meldpunt Identiteitsfraude in de tabel Bouwstenen voor Diensten en producten



Bouwsteen	Bouwsteenonderdelen	Toelichting
Digimelding	Niet van toepassing	Met Digimelding kunt u, namens uw organisatie, mogelijke onjuistheden in de gegevens van een (basis)registratie uniform, betrouwbaar en efficiënt terugmelden aan de bronhouder van deze registratie.
Digitale dossier- en dataoverdracht	Niet van toepassing	Dossier- en dataoverdracht tussen overheidsorganisaties vindt digitaal plaats en met medeweten van de burger of het bedrijf.
Doorlopende klantreizen o.b.v. levensgebeurtenissen	Niet van toepassing	Netwerk-, keten- en bedrijfsprocessen worden ontworpen op basis van (doorlopende) klantreizen over organisaties heen, gebaseerd op levensgebeurtenissen
Meldpunt Fouten in Overheidsregistraties	Niet van toepassing	Het MFO helpt burgers, bedrijven en overheidsorganisaties bij het corrigeren van een fout in een overheidsregistratie.
MijnOverheid Lopende Zaken	Niet van toepassing	Zie MijnOverheid Berichtenbox in de tabel Bouwstenen voor Diensten en producten.
Track and trace mechanisme	Niet van toepassing	Via afspraken over een 'track and trace' mechanisme als onderdeel van 'mijnoverheid/Lopende Zaken' kunnen burgers en bedrijven de voortgang over organisaties heen van een proces volgen. Dit is ook mogelijk door tussenkomst van medewerkers van bijvoorbeeld een klantcontactcenter.

1.5 Bouwstenen voor Bedrijfsfuncties

Bouwsteen	Bouwsteenonderdelen	Toelichting
Bedrijfsfuncties gelijksoortig ingedeeld voor gelijksoortige overheidsorganisaties	Niet van toepassing	Gelijksoortige overheidsorganisaties kennen een gelijksoortige indeling in bedrijfsfuncties.



1.6 Bouwstenen voor Api's / Services

Bouwsteen	Bouwsteenonderdelen	Toelichting
API-standaarden	OpenAPI Specification (verplicht)	Een application programming interface (API) is een verzameling definities voor communicatie tussen computerprogramma's. Voor het ontwikkelen van API's en de beveiliging van de gebruikerstoegang tot API's bestaan standaarden.
	REST-API Design Rules (verplicht)	De REST-API Design Rules (ADR) zijn een standaard voor het ontwikkelen van zogenoemde REST-API's.
	NL Gov OAuth profiel (verplicht)	OAuth is een beveiligingstandaard voor het autoriseren van toegang tot REST API's. Het NL GOV-profiel op OAuth 2.0 legt bindende afspraken vast over het gebruik van de standaard OAuth 2.0 bij de Nederlandse overheid.
	NL GOV Assurance profile for OpenID Connect (aanbevolen)	Het NL GOV Assurance-profiel voor OpenID Connect-specificatie verbetert de toepassing van het OpenID Connect-protocol op de volgende punten: de basisbeveiliging, interoperabiliteit en de structuur van implementaties. Dit gebeurt op een manier die specifiek van toepassing is op (maar niet beperkt tot) de overheid en de openbare dienstverlening in Nederland.
	Digikoppeling REST Profiel	Door het Digikoppeling REST profile toe te passen kunnen API's worden ingezet die compatible zijn met de API Standaarden.
Developer Overheid	developer.overheid.nl	De website developer.overheid.nl is een portaal voor developers die voor of met de overheid software ontwikkelen. Op de overzichtspagina's met API's en Open Source repositories wordt software getoond welke gepubliceerd is onder verantwoordelijkheid van organisaties die opgenomen zijn in het Register van Overheidsorganisaties.

1.7 Bouwstenen voor Applicaties

Op dit moment zijn er geen bouwstenen voor applicaties onderkend.



1.8 Bouwstenen voor Berichtenverkeer / gegevensuitwisseling

Bouwsteen	Bouwsteenonderdelen	Toelichting
Algemeen aansluitpunt	Aansluiting Basisregistraties (RINIS)	Eén aansluiting voor berichtenverkeer met alle basisregistraties.
	Aansluiting Digivoorzieningen (RINIS)	Eén aansluiting voor berichtenverkeer met alle Digi-voorzieningen, zoals MijnOverheid, Digipoort, Digilevering en Digimelding.
	Aansluiting MijnOverheid (RINIS)	Eén aansluiting voor alle berichtenverkeer met MijnOverheid.
	Centraal Aansluitpunt	Het Centraal Aansluitpunt (CA) is het koppelpunt voor berichtenverkeer tussen systemen voor overheidsorganisaties.
Digikoppeling	CPA-register	Digikoppeling is een set van standaarden, die logistieke afspraken bevat voor elektronisch berichtenverkeer tussen (overheids)organisaties. Een CPA is het digitale contract voor gegevensuitwisseling op Digikoppeling, met gebruikmaking van Digikoppeling Koppelvlakstandaard ebMS. Het CPA-register is een voorziening voor creatie en beheer van CPA's.
	Digikoppeling Compliance Voorziening	Digikoppeling Compliance Voorziening is een voorziening voor Digikoppeling compliance testen voor WUS “best effort” en ebMS2 (“best effort” en “reliable messaging”).
Digilevering	Niet van toepassing	Digilevering levert berichten over belangrijke gebeurtenissen. Geabonneerde afnemers krijgen zo actuele en accurate gegevens uit basisregistraties zoals de Basisregistratie Adressen en Gebouwen.
Digimelding	Niet van toepassing	Zie Digimelding in de tabel Bouwstenen voor Processen.
Digipoort	Niet van toepassing	Digipoort is de ICT-centrale waar berichtenverkeer voor de overheid afgehandeld wordt.
E-factureren	- e-factuurportaal Peppol - Leveranciersportaal Rijksoverheid - Via Digipoort	Verschillende manieren om e-facturen aan de overheid te sturen.
eDelivery	National Access Point eDelivery / Nationaal Aansluitpunt	Nationaal Aansluit Punt (NAP) van EU-netwerk TESTA en eDelivery.
	Service Metadata Publisher (SMP)	De SMP bevat alle gegevens die andere partijen nodig hebben om met Nederlandse organisaties data uit te wisselen, zoals het digitale adres en benodigde certificaten.
eXtensible Business Reporting Language (XBRL)	Verplichte standaard	eXtensible Business Reporting Language (XBRL) is een internationale open standaard om (financiële)bedrijfsgegevens op eenvoudige wijze uit te wisselen via het internet



Bouwsteen	Bouwsteenonderdelen	Toelichting
Federatief Berichtenstelsel	Niet van toepassing	Zie Federatief Berichtenstelsel in de tabel Bouwstenen voor Diensten en producten
NL GOV profile for CloudEvents	Niet van toepassing	NL GOV profile for CloudEvents is een set Nederlandse afspraken over het gebruik van de internationale standaard CloudEvents. Het beschrijft hoe een plaatsgevonden gebeurtenis gerapporteerd en uitgewisseld kan worden, zoals een verhuizing of overlijden. Zo werken organisaties makkelijker samen en wisselen effectiever informatie uit. Bovendien kan die informatie centraal (bij de bron) geregistreerd blijven. Een kopie maken is dus niet meer nodig.
Peppol	Peppol-standaarden (aanbevolen)	Peppol is de internationale standaard voor het verzenden, ontvangen en verwerken van elektronische facturen en orders.
	Rijksoverheid Access Point op Peppol (ROAP)	Het ROAP verzorgt onder andere de ontvangst, validatie, conversie, routing en aflevering van berichten over facturen.
Standard Business Reporting (SBR)	Niet van toepassing	SBR is de nationale standaard voor de digitale uitwisseling van alle bedrijfsmatige rapportages.
Wallet	Niet van toepassing	Zie Toegangstelsel in de tabel Bouwstenen voor Diensten en producten

1.9 Bouwstenen voor Data / gegevens

Bouwsteen	Bouwsteenonderdelen	Toelichting
Basisregistratie Adressen en Gebouwen (BAG)	Niet van toepassing	Authentieke bron voor basisgegevens van adressen en gebouwen in Nederland.
Basisregistratie Grootchalige Topografie (BGT)	Niet van toepassing	Authentieke bron voor geo-informatie in Nederland: een uniform topografisch basisbestand met objecten (dingen die in het terrein fysiek aanwezig zijn) in heel Nederland, op een schaal van 1:500 tot 1:5.000.
Basisregistratie Inkomens (BRI)	Niet van toepassing	Authentieke bron voor inkomensgegevens van personen die met Nederland te maken hebben.
Basisregistratie Kadaster (BRK)	Niet van toepassing	Authentieke bron voor percelen, eigendom, hypotheek, beperkte rechten (zoals recht van erfpacht, opstal en vruchtgebruik) en leidingnetwerken, alsmede kadastrale kaarten met perceel, perceelnummer, oppervlakte, kadastrale grens en de grenzen van het Rijk, de provincies en gemeenten in Nederland.
Basisregistratie Ondergrond (BRO)	Niet van toepassing	Authentieke bron voor geo-informatie in Nederland: gegevens en modellen over de ondergrond (bodem, geologie, grondwater, mijnbouw).
Basisregistratie Personen (BRP)	Niet van toepassing	Zie Basisregistratie Personen in de tabel Bouwstenen voor Diensten en producten



Bouwsteen	Bouwsteenonderdelen	Toelichting
Basisregistratie Topografie (BRT)	Niet van toepassing	Authentieke bron voor geo-informatie in Nederland: topografische gegevens.
Basisregistratie Voertuigen (BRV)	Niet van toepassing	Authentieke bron voor gegevens over voertuigen in Nederland en de eigenaren daarvan.
Basisregistratie Waarde Onroerende Zaken (WOZ)	Niet van toepassing	Authentieke bron voor de Onroerende Zaak belasting in Nederland.
Dataregister van de Nederlandse Overheid	data.overheid.nl	Een portaal met door de Nederlandse overheid beschikbaar gestelde data.
Handelsregister	Niet van toepassing	Zie Handelsregister in de tabel Bouwstenen voor Diensten en producten
Referentiearchitectuur regie op Gegevens	Niet van toepassing	Een afsprakenstelsel met voorzieningen om burgers regie te kunnen laten voeren op hun eigen persoonsgegevens bij de overheid, binnen de bestaande wettelijke kaders die daarvoor gelden.
Standaarden voor metadata voor duurzame toegankelijkheid	Metagegevens voor duurzaam toegankelijke overheidsinformatie standaard (MDTO)	MDTO (Metagegevens voor duurzaam toegankelijke overheidsinformatie) is een norm voor het vastleggen en uitwisselen van eenduidige metagegevens om de duurzame toegankelijkheid van overheidsinformatie mogelijk te maken.
Stelselcatalogus	Niet van toepassing	De Stelselcatalogus is een online catalogus. Het geeft inzicht, overzicht en duiding binnen het gegevenslandschap van de overheid. Welke gegevens worden er in welke registraties bijgehouden, welke betekenis hebben deze gegevens, en hoe verhouden de gegevens uit de verschillende registraties zich tot elkaar?

1.10 Bouwstenen voor Netwerken

Bouwsteen	Bouwsteenonderdelen	Toelichting
Diginetwerk	Netwerkstandaarden	Diginetwerk is een afsprakenstelsel voor het koppelen van besloten netwerken van de overheid.
	Koppeling met cloudomgevingen van commerciële partijen	Via deze gekoppelde netwerken kunnen alle organisaties met een publieke taak onderling gegevens uitwisselen.
Nationaal Aansluitpunt	Niet van toepassing	Zie eDelivery in de tabel Bouwstenen voor Berichtenverkeer / gegevensuitwisseling



Bouwsteen	Bouwsteenonderdelen	Toelichting
Standaarden voor netwerken	Herziening Europese Richtlijn Netwerk- en Informatiebeveiliging (NIB2)	Europese Netwerk- en Informatiebeveiliging richtlijn
	DNSSEC, IPv6, HSTS, TLS v1.3, RPKI, security.txt, STIX, TAXII en voor e-mail DKIM, DMARC, SPF, STARTTLS, DANE (Verplicht)	TLS en de verdere reeks aan verplichte internetstandaarden zorgen voor beveiligde internetverbindingen, met als doel de veilige uitwisseling van gegevens tussen een internetsystemen (zoals websites of mailservers). Dit maakt het voor cybercriminelen moeilijker om internetverkeer te onderscheppen of te manipuleren.
TESTA	Niet van toepassing	Het Trans European Services for Telematics between Administrations (TESTA)-systeem is het particuliere IP-gebaseerde netwerk van de Europese Unie.

1.11 Bouwstenen voor Platformen voor dagelijkse exploitatie

Bouwsteen	Bouwsteenonderdelen	Toelichting
Overheidsdatacenter (laas)	Niet van toepassing	Voorzieningen in de vorm van duurzame en volledig schaalbare ICT-omgevingen (datacenter), die geheel in eigendom zijn van de Rijksoverheid.
Platformdiensten (Paas)	- Containerplatform - Cloud native overheid standaard	
	Haven	Haven is een standaard voor platform-onafhankelijke cloud hosting. Een applicatie of website die op één Haven omgeving werkt, is herbruikbaar op alle Haven omgevingen.
	Kubernetes	Kubernetes is een open-sourcesysteem voor het automatiseren van de implementatie, het schalen en het beheer van op 'containers' gebaseerde applicaties.
Infra as a service	Niet van toepassing	Datacenters zijn ingericht op basis van het "Infra as a service" concept, waarbij gebruik gemaakt wordt van open source tooling en voorzieningen.



1.12 Bouwstenen voor Slimme apparaten

Bouwsteen	Bouwsteenonderdelen	Toelichting
Digital twinning	Niet van toepassing	Een digitale tweeling (Engels: digital twin) is een digitale representatie van een beoogd of feitelijk fysiek product, systeem of proces in de echte wereld (een fysieke tweeling). De digitale tweeling dient als de feitelijk niet te onderscheiden digitale tegenhanger van de echte wereld voor praktische doeleinden, zoals simulatie, integratie, testen, monitoring en onderhoud.
Edge computing	Niet van toepassing	Edge computing is een gedistribueerd computerparadigma dat berekeningen en gegevensopslag dicht bij de gegevensbronnen brengt. Dit heeft tot doel om de responstijden te verbeteren en bandbreedte te besparen. Edge computing is eerder een architectuur, topologie- en locatiegevoelige vorm van gedistribueerd computergebruik dan een specifieke technologie.

1.13 Bouwstenen voor Huisvesting

Bouwsteen	Bouwsteenonderdelen	Toelichting
Datacenter	Niet van toepassing	Door de overheid beheerde datacenters met uitwijkmogelijkheden.

1.14 Bouwstenen voor Beveiliging en privacybescherming

Bouwsteen	Bouwsteenonderdelen	Toelichting
Standaarden voor beveiliging en privacyborging	Cybersecurity Implementatierichtlijn Objecten (CSIR)	De CSIR staat voor CyberSecurity ImplementatieRichtlijn en is speciaal ontwikkeld om objecten (waterzuiveringsinstallaties, gemalen, bruggen, keringen, sluizen, etc.) te beveiligen.
	Inkoopeisen Cybersecurity Overheid (ICO)	Door cybersecurity-eisen te stellen wanneer de overheid ICT-producten en diensten inkoopt, wordt een impuls gegeven aan de digitale veiligheid in de hele markt. De overheid is namelijk een belangrijke gebruiker van ICT-producten en diensten.
	Privacy by design	Privacy by design is een benadering van systeemontwikkeling, oorspronkelijk ontwikkeld door Ann Cavoukian en geformaliseerd in een gezamenlijk rapport over technologieën voor privacyverbetering door een gezamenlijk team van de Information and Privacy Commissioner van Ontario (Canada), de Autoriteit Persoonsgegevens en TNO in 1995.
	Privacy Enhancing Technologies	Privacybevorderende technologieën (Engels: Privacy-enhancing technologies, afgekort PET) zijn technologieën die fundamentele gegevensbeschermingsprincipes bewerkstellingen door het gebruik van persoonlijke gegevens te minimaliseren, het maximaliseren van gegevensbeveiliging en eigen invloed voor individuen.



Bouwsteen	Bouwsteenonderdelen	Toelichting
Open standaarden	Niet van toepassing	Gebruik open standaarden conform richtlijnen van Forum Standaardisatie.
NIST Risk Management Framework	Niet van toepassing	Het Risk Management Framework biedt een proces waarin activiteiten op het gebied van beveiliging, privacy en cyber risicobeheer worden geïntegreerd in de levenscyclus van systeemontwikkeling.

1.15 Bouwstenen voor Softwareontwikkeling

Bouwsteen	Bouwsteenonderdelen	Toelichting
Standaarden voor Ontwikkeling	ISO 25010	De ISO-norm 25010 beschrijft de kwaliteitskenmerken van software en systemen.
	Non Product Related NEN-norm voor softwareontwikkeling en -onderhoud	De methode SSD: biedt een aanpak voor de samenwerking tussen jouw organisatie en de softwareleverancier (of jouw eigen ontwikkelafdeling). Het is daarmee vooral een handvat voor functionarissen in jouw organisatie die belast zijn met projectmanagement, ontwikkeling, inkoop en contractmanagement rond inkoop of ontwikkeling van software.
	Veilige softwareontwikkeling (secure software development)	Het normenkader SSD: (voor software en voor mobiele apps) voorziet in concrete, testbare en in aanbestedingen en contractmanagement afdwingbare producteisen. Met deze eisen leg je een basisniveau van veiligheid op aan de software die je inkoopt of laat ontwikkelen.
Software licenties	EU PL	Door overheid gestandaardiseerde licenties voor het publiek beschikbaar maken van in opdracht van overheid geproduceerde software.

1.16 Bouwstenen voor Beheer en exploitatie

Bouwsteen	Bouwsteenonderdelen	Toelichting
Standaarden voor Beheer en exploitatie	ITIL	Information Technology Infrastructure Library is een referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie.
	Open Telemetry	OpenTelemetry is een verzameling tools, API's en SDK's. Gebruik het voor het instrumenteren, genereren, verzamelen en exporteren van telemetriegegevens (statistieken, logboeken en traces) om u te helpen de prestaties en het gedrag van uw software te analyseren.
	BOMOS	BOMOS is het Beheer- en OntwikkelModel voor Open Standaarden. Het BOMOS-model ondersteunt u bij het ontwikkelen en beheren van standaarden en stelsels.



Bijlage 2: Relatie bouwstenen met E.U.-verordeningen

Deze bijlage bevat een eerste, voorlopige analyse van de relatie tussen EU-verordeningen en (te ontwikkelen) bouwstenen digitale overheid

Globale bouwstenen	Huidige invullingen (niet volledig / ter oriëntatie)	EU-verordeningen en richtlijnen met impact/implementatie verplichtingen
Toegang		
eID bouwsteen	Paspoort, ID-kaart, rijbewijs	eIDAS
	DigiD	eIDAS (genotificeerd)
	toegelaten private identificatiemiddelen waaronder eHerkenning	eIDAS (eHerkenning genotificeerd)
	toegelaten identificatiemiddelen andere EU-landen	eIDAS
	BSNk	
	Identificatiemiddelen restgroepen	
	Routeringsvoorziening	
Machtigingsbouwsteen	DigiD Machtigen	eIDAS
	Vertegenwoordigingsregisters waaronder eHerkenning	eIDAS
	Single Sign On	
	Digipoort machtigingen	
API-bevragingen	REST API Design Rules centrum voor standaarden / Nederlands profiel OAuth	
Toegang in system-to-system berichtverkeer	Overheid - Bedrijven: Digipoort waarbinnen DigiKoppeling standaard benut wordt	



Globale bouwstenen	Huidige invullingen (niet volledig / ter oriëntatie)	EU-verordeningen en richtlijnen met impact/implementatie verplichtingen
Toegang in system-to-system berichtverkeer	Binnen de overheid: DigiKoppeling standaard, Centraal Aansluitpunt	
	Europees: RINIS en SMP standaard	Sectorale EU-regelgeving
	Gemeenten: NLX	
Wallet	Wallet (EDI-programma)	eIDAS2
Interactie		
Eén toegangspoort	Rijksoverheid.nl	SDG
	overheid.nl	SDG
	Ondernemersplein.kvk.nl / ondernemersplein.nl	SDG
	Nederlandwereldwijd.nl	
	Samenwerkende catalogi	SDG
	Europese samenwerkend catalogi CPSV	SDG
	YourEurope.eu en coördinatieafspraken vanuit bNC-SDG	SDG
	PRO-platform	
	Levensgebeurtenissen over meerdere overheidsorganisatie heen	SDG annex II schrijft minimale set levensgebeurtenissen voor



Globale bouwstenen	Huidige invullingen (niet volledig / ter oriëntatie)	EU-verordeningen en richtlijnen met impact/implementatie verplichtingen
Digitale berichtenbouwsteen	Berichtenbox burger / Mijnoverheid	SDG, GDPR/Avg
	Versturen berichten naar overheid	SDG
	Berichtenbox bedrijven www.berichtenbox.antwoordvoorbedrijven.nl	Dienstenwet
	Mijn eenmanszaak / www.kvk.nl/mijnondernemingen	SDG, Dienstenwet
	Federatief Berichtenstelsel	
	Profielservice Mijnoverheid	
	Digipoort	
	Generieke mijnomgeving (incl. via andere kanalen verzonden post)	
Track & tracebouwsteen	Voorstel Werkagenda Waardengedreven Digitaliseren	
	MijnOverheid Lopende Zaken	
Inzagebouwsteen	Mijnoverheid.nl, mijnoverheid app	GDPR/Avg
Correctiebouwsteen	Digimelding	GDPR/Avg
	Centraal Meldpunt Identiteitsfraude	SDG
	Meldpunt Fouten in Overheidsregistraties (RvIG)	SDG
Bouwsteen voor transparantie over gegevensdeling		GDPR/Avg
Multichannel klantcontactcentrum	14+nummer afspraken	SDG voor zeer beperkt deel
Ketenafspraken over naadloze dienstverlening	Volledige digitale procedures over overheidsorganisaties heen	Voor SDG annex II procedures en betreffende levensgebeurtenissen verplicht



Globale bouwstenen	Huidige invullingen (niet volledig / ter oriëntatie)	EU-verordeningen en richtlijnen met impact/implementatie verplichtingen
Gegevens		
Berichtuitwisseling overheid – bedrijven/instellingen over werknemers	Digipoort	
Berichtuitwisseling overheid – bedrijven/instellingen financieel/economisch	Digipoort	
E-facturatie	Digipoort	
Berichtuitwisseling binnen de overheid	Digilevering	
	Abonnementen (Digilevering doorontwikkeling)	
	RINIS	Sectorale EU-regelgeving
	API's	
Basisregistraties	10 stuks	SDG-verplichtingen vereisen impliciet basisregistraties
Attribuutverstrekkings-bouwstenen.		eIDAS2
Overig		
Actieve openbaarmakingsbouwsteen	PLOOI, KOOP diensten	
Bekendmaking- en attenderingbouwsteen	overheid.nl/berichten-over-uw-buurt	
Open overheidsdata publicatie bouwsteen		Open Data richtlijn



Bijlage 3: Begrippenlijst

Waar mogelijk zijn definities overgenomen uit NORA en andere bestaande begrippenkaders. Voor enkele begrippen is daar een concessie aan gedaan omdat dit voor de context van dit document nodig was.

Afnemer

Een organisatie die een bouwsteen voor de digitale overheid gebruikt voor ondersteuning van dienstverlening of samenwerking met andere organisaties.

Toelichting: Het begrip “afnemer” wordt in dit document gebruikt voor organisaties die bouwstenen voor de digitale overheid afnemen t.b.v. dienstverlening of samenwerking. Het wordt niet gebruikt als verkorte schrijfwijze voor het algemenere begrip “dienstafnemer” waarmee personen en organisaties worden bedoeld die verschillende soorten diensten afnemen van andere personen en organisaties.

Afspraak

Overeenkomst binnen de overheid of een deel (domein of sector) over de inrichting en het toepassen van bepaalde voorzieningen of standaarden.

Bron: NORA

Toelichting: Een afspraak is één van de mogelijke vormen van een bouwsteen voor de digitale overheid. Het kan nodig zijn om afspraken vast te leggen in een wettelijk kader.

Afsprakenstelsel

Zie Stelsel.

Applicatie

Een computerprogramma om specifieke taken uit te voeren.

Bron: gebaseerd op TOGAF: “A classification of computer programs designed to perform specific tasks, such as word processing, database management, or graphics.”

Architectuur

Een beschrijving van een complex geheel en van de principes die van toepassing zijn op de ontwikkeling van het geheel en zijn onderdelen.

Bron: NORA

Toelichting: gebaseerd op TOGAF: “Architecture has two meanings depending upon its contextual usage: (1) A formal description of a system, or a detailed plan of the system at component level to guide its implementation. (2) The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time.”

Architectuurprincipe

Een stelling over een gewenste, generieke, kwalitatieve eigenschap waar architectuur invulling aan moet geven.

Bron: gebaseerd op NORA: “Een stelling over een gewenste, generieke, kwalitatieve eigenschap waar architectuur invulling aan moet geven in de publieke sector.”

De NORA-definitie is gebaseerd op Archimate: “A principle represents a statement of intent defining a general property that applies to any system in a certain context in the architecture.”

Synoniem: principe.

Toelichting: Uitspraak, geldend voor langere termijn, die betrekking heeft op de inrichting van organisatie, processen en informatievoorziening. Richtinggevend voor overheidsorganisaties bij het inzetten van veranderingen en het uitvoeren van projecten.

Authenticatie, authenticeren

Een digitaal proces dat de bevestiging van de digitale identificatie van een persoon in digitale vorm mogelijk maakt.

Bron: gebaseerd op eIDAS: “Authenticatie - een elektronisch proces dat de bevestiging van de elektronische identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt.”

Authentieke bron

Een register of systeem, onder de verantwoordelijkheid van een publiekrechtelijk orgaan of particuliere entiteit, dat attributen omtrent een natuurlijke of rechtspersoon bevat en als de primaire bron van die informatie wordt beschouwd of krachtens nationaal recht als authentiek wordt erkend.

Bron: eIDAS-revisie

Synoniem: Gezaghebbende bron

Autorisatie

Het verlenen van toestemming (een bevoegdheid) aan een geauthentiseerde partij om toegang te krijgen tot een bepaalde dienst of toestemming om een bepaalde actie uit te voeren.



Een autorisatie kan worden vastgelegd in toegangsrechten. Het verlenen van toegang kan (mede) gebaseerd zijn op die in toegangsrechten vastgelegde autorisatie.

Bron: afsprakenstelsel.etoegang.nl

Beheer

Beheer is alle activiteiten die een organisatie uitvoert om IT-diensten voor haar gebruikers te ontwerpen, realiseren, aanbieden, besturen en controleren.

Bron: Wikipedia, Engelse versie

Belanghebbende

Een natuurlijk persoon die zich ter behartiging van zijn belangen in het verkeer met bestuursorganen laat vertegenwoordigen door een gemachtigde.

Bron: Besluit verwerking persoonsgegevens generieke digitale infrastructuur

Bericht

Informatie die de overheid aan burgers en bedrijven stuurt en andersom omdat dit verplicht of noodzakelijk is vanuit wet, regeling, procedure of anderszins.

Bestuursorgaan

Orgaan van een rechtspersoon krachtens publiekrecht ingesteld" (a-orgaan), of "een persoon of college, met enig openbaar gezag bekleed" (b-orgaan).

Bron: Algemene wet bestuursrecht, Awb artikel 1:1 lid 1

Toelichting: Uitzonderingen staan vermeld in art. 1:1 lid 2 Awb.

Betrouwbaarheidsniveau

Mate waarin vertrouwen kan worden gesteld in een identificatiemiddel, gebaseerd op de mate van zekerheid waarmee attributen, identiteiten, identificatiemiddelen en/of bevoegdheden zijn vastgesteld.

Bron: gebaseerd op [Wdo](#) ("mate waarin vertrouwen kan worden gesteld in een identificatiemiddel") en NORA ("Mate waarin vertrouwen kan worden gesteld in een identificatiemiddel, gebaseerd op de mate van zekerheid waarmee attributen, identiteiten, identificatiemiddelen en/of bevoegdheden zijn vastgesteld.").

Bouwsteen

Een afspraak, standaard, organisatorische of technische voorziening of een combinatie hiervan ten behoeve van de realisatie van de digitale overheid.

Burgers en bedrijven

De belanghebbenden van overheidsdienstverlening in de ruimste zin van het woord.

Synoniem: natuurlijke personen en niet-natuurlijke personen.

Toelichting: "Burgers en bedrijven" is een verkorte schrijfwijze voor: burgers, bedrijven, instellingen, intermediairs en hun gemachtigden.

Zo kan in deze context een statushouder gezien worden als een burger.

Bron: gebaseerd op NORA: "Met de term 'burgers en bedrijven' bedoelen we alle belanghebbenden van overheidsdienstverlening in de ruimste zin van het woord."

Data

Zie Gegevens.

Dienst

Een afgebakende prestatie van een persoon of organisatie (de dienstverlener), die voorziet in een behoefte van haar omgeving (de dienstafnemers).

Bron: NORA

Synoniem: Service

Toelichting: Diensten zijn zowel het leveren van informatie als het uitvoeren van andere handelingen. Een betrokkene kan dit positief ervaren (het verkrijgen van een rijbewijs) maar ook negatief (bijvoorbeeld een belastingaanslag). Dat heeft te maken met de maatschappelijk afspraken over individuele diensten en collectieve diensten: ter ondersteuning van individuele hulp dan wel het borgen van collectieve belangen.

Dienstencatalogus

Een elektronisch bevroagbare catalogus die de gestructureerde verzameling van alle diensten, inclusief de onderverdeling in subdiensten en eventuele samengestelde diensten bevat.

Bron: gebaseerd op Afsprakenstelsel eToegang: "Een elektronisch bevroagbare catalogus die de gestructureerde verzameling van alle diensten, inclusief de onderverdeling in subdiensten en eventuele samengestelde diensten bevat, welke voor het vastleggen van bijzondere machtigingen, dat wil zeggen machtigingen die zich beperken tot bepaalde diensten, minimaal noodzakelijk is."



Dienstverlener

De persoon of organisatie die voorziet in het leveren van een afgebakende prestatie (dienst) aan haar omgeving (de dienstafnemers).

Bron: NORA

Synoniem: Dienstaanbieder

Digitale identiteit

Een identiteit die een digitale representatie is van een persoon.

Toelichting: Onder “identiteit” verstaan we: “Een verzameling unieke kenmerken of gegevens (attributen) die een persoon uniek beschrijven in een gegeven context.” Dit is gebaseerd op *Practitioner's Guide van The World Bank*: “identity refers to the combination of characteristics or attributes that make a person unique in a given context.”

Domein

Een inhoudelijk verwante verzameling van publieke dienstverlening. Binnen de context van de GDI zijn dit: Toegang, Interactie, Gegevensuitwisseling en Infrastructuur.

Bron: NORA, Besluit Sturing Digitale Overheid 2022¹⁹⁹

Toelichting: Zie de begrippen Toegang, Interactie, Gegevensuitwisseling en Infrastructuur.

Functionaliteiten

Zie “Generieke functie”.

GDI

Afkorting van Generieke Digitale Infrastructuur

GDI-voorziening

Een voorziening die onderdeel is van de GDI.

Gegevens

Weergave van een feit, begrip of aanwijzing, geschikt voor overdracht, interpretatie of verwerking door een persoon of apparaat

Bron: Archiefterminologie voor Nederland en Vlaanderen, via NORA

Gegevensuitwisseling (domein)

Het domein Gegevensuitwisseling omvat de bouwstenen van de GDI voor uitwisseling van gegevens tussen informatiesystemen van overheidsorganisaties onderling en met informatiesystemen van andere organisaties.

Generieke Digitale Infrastructuur

De verzameling aan afspraken, standaarden en voorzieningen die overheidsorganisaties en dienstverleners met een publieke taak ondersteunt bij de inrichting van hun digitale dienstverlening aan burgers en bedrijven en ook bij hun onderlinge digitale samenwerking (afgekort GDI).

Bron: Besluit Sturing Digitale Overheid 2022

Synoniem: Basisinfrastructuur, Digitale basisinfrastructuur

Toelichting: De GDI bestaat uit de kern van de digitale overheid die niet organisatie-, sector- of domein specifiek is en die wordt begrensd door de generieke functies. De GDI omvat tevens de functies van de in de Wet Digitale Overheid genoemde voorzieningen.

Generieke functie

Iets wat meerdere overheidsorganisaties moeten kunnen voor het uitvoeren van hun taken.

Bron: NORA

Toelichting: Binnen de GDI wordt gebruik gemaakt van generieke functies om de doelen van de GDI te bereiken. Deze zijn uitgewerkt in afspraken, standaarden en voorzieningen die in alle gevallen van toepassing zijn en gebruikt worden.

Voor de definitie van “functie” gebruiken we de definitie van Archimate voor “capability”: “A capability represents an ability that an active structure element, such as an organization, person, or system, possesses.”

Generieke voorziening

Voor generieke voorzieningen geldt dat de afspraak is dat alle overheidsorganisaties deze binnen het toepassingsgebied daarvan gebruiken als ondersteuning voor dienstverlening aan burgers en bedrijven of voor samenwerking met andere organisaties.

Synoniem: GDI-voorziening



Identificatie, identificeren

Het proces van het gebruiken van persoonsidentificatiegegevens in digitale vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden.

Bron: gebaseerd op *eIDAS*: “elektronische identificatie - het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden.”

Identificatiemiddel

Een materiële en/of immateriële eenheid die identificatiegegevens bevat waarmee de identiteit van een persoon is aan te tonen.

Bron: gebaseerd op *eIDAS*: “elektronisch identificatiemiddel - een materiële en/of immateriële eenheid die persoonsidentificatiegegevens bevat en die gebruikt wordt voor authenticatie bij een onlinedienst.”

Synoniem: authenticatiemiddel

Toelichting: identificatiegegevens zijn een verzameling gegevens aan de hand waarvan de identiteit van een persoon kan worden vastgesteld. Dit is gebaseerd op *eIDAS*: “elektronische identificatie - het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden.”

Informatie

Betekenisvolle gegevens.

Bron: NEN-ISO 9000, via NORA

Toelichting: Dit document maakt geen strikt onderscheid tussen “data”, “gegevens” en “informatie”.

Infrastructuur (domein)

Het domein Infrastructuur omvat de bouwstenen van de GDI die van algemeen belang (ofwel: infrastructureel) zijn voor de GDI en die veelal een basis vormen voor de bouwstenen van de andere drie domeinen.

Infrastructuur (object)

Informatietechnologie (IT) infrastructuur is de verzameling van IT-componenten die de basis vormen voor IT-diensten. Typisch bestaat de IT-infrastructuur uit fysieke componenten (computers en netwerkapparatuur, huisvesting e.d.) maar ook programmatuur en netwerk-componenten.

Bron: Wikipedia, Engelse versie

Interactie (domein)

Het domein Interactie omvat de bouwstenen van de GDI ten behoeve van elektronische informatie-uitwisseling met burgers, bedrijven, instellingen, intermediairs en hun gemachtigden. Uitwisseling ten behoeve van Toegang is hiervan uitgezonderd.

Kanaal

Communicatiekanaal dat bij de dienstverlening wordt gebruikt. Elk kanaal kent verschillende vormen waarin informatie kan worden gedeeld.

Bron: NORA

Machtigen

Machtigen is het verlenen van bevoegdheid door een vertegenwoordigde (ook: belanghebbende) aan een vertegenwoordiger (ook: gemachtigde) ten aanzien van de verrichting van een specifieke dienst.

Bron: Globale Architectuur Machtigen

Natuurlijk persoon (NP)

Een mens van vlees en bloed

Toelichting: Naast een natuurlijk persoon (NP) wordt binnen de overheid ook veel gesproken over niet-natuurlijke personen (NNP).

Het CBS definieert “natuurlijk persoon” als “Een mens (individu) die in het recht als rechtssubject is erkend en daarmee drager is van wettelijke rechten en plichten.”

Netwerk (organisatie)

Een organisatie netwerk is een verband waarin organisaties samenwerken om toegevoegde waarde te leveren.



Netwerk (techniek)

De verzamelde functies die uitwisseling van data tussen computers onderling en met hun (rand)apparatuur mogelijk maken om diensten beschikbaar te stellen.

Toelichting: Typisch bestaat een netwerk uit transmissiemedia voor het doorgeven van signalen (zoals kabels, radiofrequenties, licht e.d.), bandbreedte, communicatieprotocollen en netwerkapparatuur (hardware en software).

Niet-natuurlijk persoon (NNP)

Een rechtspersoon of een samenwerkingsverband zonder rechtspersoonlijkheid.

Bron: CBS.

Toelichting: Een samenwerkingsverband zonder rechtspersoonlijkheid is een rechtsvorm behorend bij een georganiseerde groep van natuurlijke personen en/of rechtspersonen die zelf niet in het recht is erkend als drager van wettelijke rechten en plichten.

Voorbeelden: Privaatrechtelijke rechtspersonen zijn besloten vennootschap, naamloze vennootschap, vereniging en stichting. Publiekrechtelijke rechtspersonen zijn ministerie, provincie, gemeente, waterschap, Sociaal-Economische Raad, Publiekrechtelijke bedrijfsorganisatie, Zelfstandig bestuursorgaan. Ook kerkgenootschappen zijn rechtspersonen. Samenwerkingsverbanden zonder rechtspersoonlijkheid zijn de maatschap, de vennootschap onder firma (vof) en de commanditaire vennootschap (cv).

Overheid en overheidsorganisaties

Met overheid en overheidsorganisaties bedoelen we alle organisaties die publieke taken uitoefenen.

Overheidsinformatie

Informatie verstrekt door de overheid.

Platform voor dagelijkse exploitatie

Een samenhangende verzameling van hardware en software (hardware, besturingssystemen, opslag- en netwerkcapaciteit) om informatiesystemen op uit te voeren.

Principe

Zie architectuurprincipe.

Privaat identificatie-middel

Niet van rijkswege uitgegeven identificatiemiddel.

Bron: gebaseerd op [Wdo](#): “niet van rijkswege uitgegeven aan een natuurlijke persoon, onderneming of rechtspersoon verstrekt identificatiemiddel.”

Publieke taak

Een taak waarvoor de overheid de eindverantwoordelijkheid op zich neemt en die wordt uitgevoerd voor de behartiging van een publiek of algemeen belang.

Service

Zie “Dienst”.

Standaard

Een set van regels die beschrijven hoe mensen materialen, producten, diensten, technologieën, taken, processen en systemen dienen te ontwikkelen en beheren.

Bron: NORA

Toelichting: een standaard is één van de mogelijke vormen van een bouwsteen voor de digitale overheid.

Stelsel

Een systeem waarbinnen organisaties via afspraken, standaarden en/of voorzieningen samenwerken om bepaalde functionaliteit te realiseren.

Bron: NORA

Toelichting: Een stelsel is een implementatie voor een of meerdere generieke functies (of delen daarvan). Voorbeelden: Federatief Berichten Stelsel (FBS), eHerkenning-stelsel, stelsel van basisregistraties.

Toegang (domein)

Het domein Toegang bestaat uit twee subdomeinen.

Het subdomein Identificatie & authenticatie omvat de bouwstenen vanuit de GDI om burger, bedrijf, instelling, intermediair uniek te identificeren en authenticeren ten behoeve het verlenen van toegang tot publieke diensten. Het subdomein Machtigen & vertegenwoordigen omvat de bouwstenen om de bevoegdheid tot het digitaal handelen namens een ander vast te stellen.

Toelichting: het woord “toegang” wordt ook gebruikt in de vorm van toegang tot informatie zonder dat daarbij spraken van inloggen (of identificatie en authenticatie) is.



Vertegenwoordigen

De rechtsfiguur die inhoudt dat de rechtsgevolgen van een door een bepaalde Partij (de Vertegenwoordiger of Gemachtigde) in naam van een andere partij (de Vertegenwoordigde dienstafnemer) met een derde verrichte handeling aan de vertegenwoordigde worden toegerekend. De Bevoegdheid tot het verrichten van vertegenwoordigingshandelingen vloeit voort uit hetzij de wet hetzij een volmacht (privaatrecht) hetzij uit een machtiging (bestuursrecht). Zo'n bevoegdheid kan eventueel ingeperkt zijn tot bepaalde rechtshandelingen, of een bepaalde relevante omvang ten aanzien van rechtshandelingen.

In privaatrechtelijke context wordt naast het begrip vertegenwoordiger, agent of gevolmachtigde gehanteerd in plaats van gemachtigde.

Bron: Begrippenlijst eToegang

Vitale infrastructuur

Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur. Elektriciteit, toegang tot internet, drinkwater en betalingsverkeer zijn voorbeelden van vitale processen.

Bron: www.nctv.nl

Voorziening

Een samenhangende verzameling van services en onderdelen die vergezeld van afspraken als een geheel wordt aangeboden.

Bron: gebaseerd op de Archimate-definitie voor "product": *"a product represents a coherent collection of services and/or passive structure elements, accompanied by a contract/set of agreements, which is offered as a whole to (internal or external) customers'."*

Toelichting: Een voorziening is één van de mogelijke vormen van een bouwsteen voor de digitale overheid. Voorzieningen zullen binnen de context van de digitale overheid vaak geautomatiseerde informatiesystemen omvatten, maar kunnen zich ook beperken tot een bedrijfsproces voor het leveren van een dienst.

Wallet

Een apparaat (ook wel: device), online service of softwareprogramma dat vertrouwelijke gegevens kan bevatten, zoals persoonlijke attributen, identificatiegegevens, inloggegevens en bankpassen, en dat de bezitter in staat stelt digitale transacties uit te voeren, zoals aantonen van zijn identiteit, attributen verstrekken en betalingen te doen.

Zaak

Een samenhangende hoeveelheid werk met een gedefinieerde aanleiding en een gedefinieerd resultaat waarvan kwaliteit en doorlooptijd bewaakt moeten worden.

Bron: NORA



Bijlage 4: Betrokkenen bij de totstandkoming van deze versie

Overkoepelende architectuurwerkgroep

Bob te Riele, RvIG
Eric Brouwer, ICTU NORA
Eric Nijenhuis, UWV
Jan Nieuwstad, Logius
Johann Schreurs, DUO
Luc Boss, Belastingdienst
Paul de Pagter, SVB
Peter Lehr, Belastingdienst
Peter Sciamanda, RDW
Peter Visser, Ministerie van BZK
Rogier van Dam, Logius

Diverse leden van de werkgroep hebben collega's uit hun eigen organisatie betrokken.

Bureau MIDO (eindredactie)

Guido Bayens
Michael Stoelinga
Tom Peelen
Wim Bakkeren

Dit is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie Digitale Overheid
Postbus 20011 | 2500 EA Den Haag
www.rijksoverheid.nl

Eindredactie: Voxx content in context
Vormgeving: Optima Forma bv, Voorburg

December 2023