

Onderzoek naar standaarden en standaardisatieactiviteiten voor Cloud



E-Space Adviesdocument
Werkversie 15 augustus 2023

Deze versie:

<https://brienen.github.io/onderzoek-cloudstandaarden/>

Laatst gepubliceerde versie:

<https://brienen.github.io/publish/dk/onderzoek-cloudstandaarden>

Laatste werkversie:

<https://brienen.github.io/onderzoek-cloudstandaarden/>

Vorige versie:

<https://brienen.github.io/publish/dk/wv-ad-onderzoek-cloudstandaarden-20230813>

Redacteur:

Auteurs:

Arjen Brienen (E-Space)

Jeroen de Ruig (E-Space)

Doe mee:

[GitHub brienen/onderzoek-cloudstandaarden](#)

[Dien een melding in](#)

[Revisiehistorie](#)

[Pull requests](#)

Dit document is ook beschikbaar in dit niet-normatieve formaat: pdf



Dit document valt onder de volgende licentie:

[Creative Commons Attribution 4.0 International Public License](#)

Samenvatting

Dit document is geenszins af en rijp voor publicatie!!!! Het is onder bewerking en kan nog geheel en gedeeltelijk wijzigen. Aan de inhoud kan op geen enkele manier enig recht worden ontleend

Status van dit document

Dit is een werkversie die op elk moment kan worden gewijzigd, verwijderd of vervangen door andere documenten. Het is geen door het TO goedgekeurde consultatieversie.

Inhoudsopgave

Samenvatting

Status van dit document

1. Inleiding

- 1.1 Aanleiding
- 1.2 Hoofdvraag
- 1.3 Deelvragen
- 1.4 Aanpak en betrokkenen
- 1.5 Leeswijzer

2. Scope en uitgangspunten

- 2.1 Brief Rijksbreed Cloudbeleid 2022
- 2.2 Overige

3. Wat is Cloud?

- 3.1 Cloudvarianten
- 3.2 Waarom Cloud?
- 3.3 Uitdagingen en Risico's
- 3.4 Cloudontwikkelingen
 - 3.4.1 Mondiale Trends
 - 3.4.2 Europese Cloudontwikkelingen
 - 3.4.3 Cloudontwikkelingen Nederlandse Overheid
- 3.5 Cloudleveranciers
- 3.6 Nederlandse Overheid

4. Cloudtechnologie en cloudstandaarden

- 4.1 Cloudtechnologie
- 4.2 Cloudstandaarden
 - 4.2.1 Analyse Forum: Standaarden voor Cloud interoperabiliteit en dataportabiliteit
 - 4.2.2 Algemene standaarden
 - 4.2.3 Interoperabiliteitsstandaarden
 - 4.2.4 Beveiligingsstandaarden
 - 4.2.5 Privacystandaarden

- 4.2.6 Standaarden voor Servicebeheer en -orchestratie
- 4.2.7 Portabiliteitsstandaarden
- 4.2.8 Beheerstandaarden
- 4.3 Witte vlekken

5. **Conclusies en aanbevelingen**

6. **Conformiteit**

A. **Index**

- A.1 Begrippen gedefinieerd door deze specificatie
- A.2 Begrippen gedefinieerd door verwijzing

§ 1. Inleiding

§ 1.1 Aanleiding

In uw offerteaanvraag schetst u de context van de beoogde opdracht via de kamerbrief Rijksbreed cloudbeleid 2022 en de belangrijke rol van standaardisatie en in het bijzonder standaarden voor portabiliteit van gegevens, cloud-interoperabiliteit en informatieveiligheid.

Bureau Forum Standaardisatie zet namens Forum Standaardisatie de beoogde opdracht uit met de volgende opdrachtoomschrijving:

Om de digitale overheid gevraagd en ongevraagd te kunnen adviseren over standaardisatie voor de Cloud, wil het Forum Standaardisatie graag een beeld krijgen van de standaarden die van strategisch belang zijn voor het Cloudbeleid. In het bijzonder wil Forum Standaardisatie weten welke cruciale standaarden al bestaan, welke nog moeten worden gespecificeerd, en op welke (Europese en internationale) standaardisatie- activiteiten de overheid nog invloed op kan en zou moeten uitoefenen.

§ 1.2 Hoofdvraag

Wij vragen de opdrachtnemer om een onderzoek uit te voeren dat een beeld geeft van de Europese, internationale en nationale standaarden en standaardisatieactiviteiten die relevant zijn voor Cloud platformen, systemen en diensten. Tevens vragen wij aan de opdrachtnemer om ‘witte vlekken’ te

identificeren, dat wil zeggen domeinen waar open standaarden voor de Cloud nodig zijn maar nog niet bestaan.

§ 1.3 Deelvragen

Hierbij vraagt u ons de volgende onderzoeksvragen te beantwoorden:

1. Welke Europese, internationale en nationale standaarden bestaan er voor Cloud, in het bijzonder voor Cloud-interoperabiliteit, dataportabiliteit, informatieveiligheid en processen?
2. Welke Europese, internationale en nationale Cloud-standaarden zijn nog in ontwikkeling, of gepland?
3. Zijn er witte vlekken? Dat wil zeggen, Cloud-technologieën of -toepassingen waar open standaarden nodig zijn, maar nog niet bestaan en nog niet ontwikkeling zijn?
4. Op welke (Europese en internationale) standaardisatieactiviteiten voor Cloud zou de overheid of de private sector in Nederland invloed op moeten uitoefenen? Bijvoorbeeld omdat zij zich bewegen in een richting die niet overeenstemt met Nederlandse waarden zoals openheid, inclusie, veiligheid, privacy, digitale soevereiniteit, en een evenwichtige markt? En is dat nog mogelijk?

§ 1.4 Aanpak en betrokkenen

Voor dit onderzoek zijn allereerst bestaande onderzoeken en bronnen geanalyseerd. (zie bijlage 1). Vervolgens hebben er individuele interviews plaatsgevonden met experts op het gebied van standaarden, normeringen, digitale identiteit, Europese en Nederlandse digitale ontwikkelingen en ontwerp en architectuur. De gesprekken hebben plaatsgevonden van medio oktober tot medio november. Hiermee is een beeld ontstaan van de huidige stand van zaken met betrekking tot standaarden voor Regie op Gegevens en meningen die op dat moment leefde. De opgehaalde inzichten uit de gesprekken zijn geanalyseerd en vergeleken met de bestaande informatie en onderzoeken. Op basis hiervan zijn vervolgens de conclusies en aanbevelingen uit deze verkenning opgesteld. Daarna is op 1 december een expert bijeenkomst geweest waarin de resultaten van de verkenning zijn gepresenteerd en verschillende vraagstukken zijn besproken. De resultaten en individuele opmerkingen van de experts tijdens en na de expertbijeenkomst zijn zoveel mogelijk verwerkt in dit eindrapport.

Tabel 1

Aanpak verkenning

Wat	Activiteit	Resultaat	Wanneer
Vorbereiding	Gesprekken met opdrachtgever en adviseurs van deze voor afkadering	Duidelijke focus en afkadering onderzoek	Oktober 2022
	Desk research		
	Benaderen experts		
Onderzoek	Individuele (online) gesprekken met 10 experts	Kennis, meningen en ideeën experts ophalen	Oktober-November 2022
Analyse en opmaak conceptrapport	Analyseren en verwerken resultaten interviews en deskresearch	Beeld van de huidige stand van zaken	November 2022
Toetsing en validatie	Delen conceptrapport met experts voor feedback Organiseren expert bijeenkomst voor discussie inzichten, aanbevelingen en vragen	Verdieping op de resultaten, aanvullende inzichten en validatie door experts	November-December 2022
Definitief eindrapport	Verwerken feedback experts en inzichten expert bijeenkomst	Gevalideerde verkenning naar benodigde standaarden	December 2022-Maart 2023

Betrokken experts

Onderstaande experts zijn geraadpleegd voor deze verkenning. In de selectiecriteria is rekening gehouden met een representatie van experts vanuit diverse (overheids)organisaties en aanverwante organisaties die betrokken zijn bij het thema Regie op Gegevens. Het betreft de volgende experts:

-

§ 2. Scope en uitgangspunten

§ 2.1 Brief Rijksbreed Cloudbeleid 2022

In deze brief wordt geïnformeerd over het Rijksbrede cloudbeleid 2022. Dit beleid richt zich op het gebruik van publieke clouddiensten door de Rijksoverheid, als vervanging van het eerdere beleid uit 2011 dat de focus legde op private clouddiensten.

Hoofdpunten:

1. **Overheidsdiensten** mogen onder bepaalde voorwaarden en uitzonderingen gebruik maken van publieke clouddiensten.
2. **Verwerking van persoonsgegevens** in publieke clouddiensten vereist een goedgekeurde pre-scan gegevens-beschermingseffectbeoordeling. Bij een hoog risico is een volledige data protection impact assessment noodzakelijk.
3. Elk **departement** is zelf verantwoordelijk voor het inzicht in de risico's van het gebruik van publieke cloud toepassingen.
4. Er komt een “implementatierichtlijn risicoafweging cloudgebruik” voor het einde van 2022.
5. Overheidsentiteiten die niet tot de Rijksdienst behoren, wordt geadviseerd het Rijksbeleid te volgen.
6. **Uitzonderingen:** Publieke clouddiensten mogen niet worden gebruikt voor staatsgeheim gerubriceerde informatie. Het Ministerie van Defensie valt niet onder dit beleid.
7. **Voorwaarden:**
 - Departementen moeten hun eigen cloudbeleid formuleren.
 - Een relevante risicoafweging is vereist.
 - Jaarlijkse rapportage over het gebruik van publieke clouddiensten aan CIO Rijk.
 - Er moet een ‘exit strategie’ zijn in overeenkomsten met cloudleveranciers.
 - Clouddienstverlening moet voldoen aan bestaande ICT-voorwaarden.
 - Cyberveiligheid is essentieel, vooral met betrekking tot gegevensverwerking in andere landen.
 - Besluitvorming moet openbaar zijn volgens de Wet Open Overheid.

- Opslag en verwerking van persoonsgegevens moet in lijn zijn met de AVG.
- Extra bescherming is vereist voor bijzondere persoonsgegevens.

De brief benadrukt het belang van een evenwichtige benadering, waarbij gebruik wordt gemaakt van de voordelen van publieke clouddiensten terwijl de risico's worden beheerst

§ 2.2 Overige

De uitgangspunten en doelstellingen van het Forum Standaardisatie kunnen als volgt worden samengevat:

1. **Interoperabiliteit:** Eén van de belangrijkste doelstellingen van het Forum is het waarborgen van interoperabiliteit. Dit betekent dat verschillende ICT-systemen en applicaties probleemloos met elkaar kunnen communiceren.
2. **Open standaarden:** Het Forum promoot het gebruik van open standaarden. Een open standaard is een specificatie die publiek beschikbaar is en waarvan het gebruik niet beperkt is door patenten of licentierechten.
3. **Level playing field:** Door het gebruik van open standaarden wordt een gelijk speelveld gecreëerd voor aanbieders van ICT-producten en -diensten. Dit stimuleert innovatie en voorkomt dat overheidsorganisaties afhankelijk worden van één leverancier.
4.

§ 3. Wat is Cloud?

Hiermee geven de afbakening van het onderzoek en een algemene beschrijving van Cloud-technologie en -ontwikkelingen. De uitwerking bevat: wat verstaan we onder Cloud en wat niet? Welke globale ontwikkelingen zijn er en welke problemen worden hiermee opgelost? Deze afbakening en beschrijving dient als kader voor het verdere onderzoek.

Het moderne bestuurlijke landschap van Nederland heeft, net als de rest van de wereld, een technologische transformatie ondergaan, en cloud computing heeft hierbij een cruciale rol gespeeld. Als centrum van beleidsvorming, regelgeving en dienstverlening aan burgers, heeft de Nederlandse overheid baat gehad bij de vele voordelen van de cloud. Laten we deze ontwikkeling nader bekijken.

Cloud computing stelt gebruikers in staat om gegevens op te slaan, op te vragen en applicaties uit te voeren via het internet in plaats van op lokale servers of computers. Voor de overheid betekent

dit een verhoogde capaciteit en flexibiliteit bij het leveren van diensten, zonder de noodzaak van enorme fysieke IT-infrastructuren.

Cloud computing heeft het potentieel om de manier waarop de Nederlandse overheid opereert en integreert met haar burgers te transformeren. Door de kansen te benutten en tegelijkertijd de uitdagingen te herkennen en aan te pakken, kan de overheid een duurzamere, efficiëntere en meer responsieve toekomst voor Nederland creëren

§ 3.1 Cloudvarianten

Wanneer we het hebben over cloudoplossingen, zijn er drie vooraanstaande servicemodellen die de ruggengraat vormen van wat de cloud te bieden heeft, met name voor organisaties zoals de Nederlandse overheid. Dit zijn Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS).

1. **Infrastructure as a Service (IaaS):** IaaS biedt gebruikers toegang tot essentiële infrastructuur zoals fysieke machines, virtual machines, netwerk, opslag en andere fundamenteën zonder dat ze de daadwerkelijke hardware hoeven te bezitten of te onderhouden. Voor de Nederlandse overheid kan dit betekenen dat er minder behoefte is aan grote datacenters of serverfarms, omdat deze resources op aanvraag vanuit de cloud kunnen worden verkregen.
2. **Platform as a Service (PaaS):** PaaS gaat een stap verder door naast de basisinfrastructuur ook een platform te bieden waarop applicaties kunnen worden ontwikkeld, uitgevoerd en beheerd. Denk hierbij aan besturingssystemen, databases, webserver, ontwikkeltools, toegangsbeheer, identiteitenbeheer, portaalfunctionaliteiten en integratiefaciliteiten. Voor overheidsinstellingen die unieke applicaties willen bouwen voor hun diensten, kan PaaS een waardevol hulpmiddel zijn door het ontwikkelproces te stroomlijnen zonder zich zorgen te maken over het onderliggende systeembeheer.
3. **Software as a Service (SaaS):** Dit is wellicht het bekendste model, waarbij gebruikers toegang hebben tot softwaretoepassingen via het web. Denk bijvoorbeeld aan e-maildiensten, CRM-systemen of samenwerkingstools, zoals: bijvoorbeeld kantoorapplicaties (bijv. Microsoft365), cliëntenbeheer (CRM, bijv. Salesforce), softwareontwikkeling (bijv. GitHub). Voor de Nederlandse overheid betekent dit dat verschillende departementen en agentschappen toegang kunnen hebben tot de nieuwste software zonder zich zorgen te hoeven maken over installaties, updates of compatibiliteitsproblemen.

Voor de overheid kunnen deze modellen helpen om diensten efficiënter te leveren, te reageren op veranderende technologische behoeften en tegelijkertijd de overheadkosten te verlagen. Door de juiste mix van IaaS, PaaS en SaaS te kiezen, kan de Nederlandse overheid een technologische infrastructuur creëren die zowel flexibel als robuust is.

Publiek, gemeenschappelijk, privaat

Voor de toegankelijkheid van cloud bestaan drie varianten:

- **Publiek:** De software en data staan dan volledig op de servers van de cloudprovider en er wordt een generieke (voor alle afnemers gelijke) functionaliteit geleverd.
- **Gemeenschappelijk:** De cloudvoorziening is toegankelijk voor een beperkte groep afnemers, die elkaar onderling voldoende vertrouwen.
- **Privaat:** Er wordt gewerkt op een (virtueel) private ICT-infrastructuur. In deze cloud heeft de gebruiker volledige controle over data, beveiliging en kwaliteit van de dienst. De applicaties die via de Private Cloud beschikbaar worden gemaakt, maken gebruik van gedeelde infrastructuurcomponenten die slechts voor één organisatie worden ingezet.

Intern, extern

Cloud is ook te beschouwen als een technologie, welke zowel in een eigen rekencentrum kan worden gehuisvest (on premise) of bij een externe serviceprovider (cloudprovider). Een aantal overheidsorganisaties beschikt over interne cloudtechnologie.

§ 3.2 Waarom Cloud?

Cloudcomputing biedt een scala aan voordelen voor zowel individuen als bedrijven. Hier zijn enkele van de meest prominente voordelen:

1. **Schaalbaarheid:** Een van de grootste voordelen van cloudservices is de mogelijkheid om gemakkelijk op te schalen naarmate de behoeften van een organisatie groeien, zonder dat er grote investeringen in fysieke hardware nodig zijn.
2. **Kostenbesparing:** Door gebruik te maken van de cloud kunnen bedrijven besparen op de kosten van aanschaf en onderhoud van hardware. Ze betalen vaak alleen voor wat ze daadwerkelijk gebruiken.
3. **Toegankelijkheid en mobiliteit:** Gegevens en applicaties in de cloud kunnen over het algemeen vanaf elke locatie met internettoegang worden benaderd. Dit maakt telewerken en toegang onderweg gemakkelijker.
4. **Disaster recovery en back-ups:** Veel cloudproviders bieden data-replicatie aan over meerdere locaties, wat zorgt voor een snellere gegevensherstel in het geval van een ramp.
5. **Automatische software-updates:** Cloudproviders voeren regelmatig systeemonderhoud en software-updates uit, wat betekent dat bedrijven zich geen zorgen hoeven te maken over het beheer van deze taken.

6. **Flexibiliteit:** Cloudoplossingen bieden de mogelijkheid om snel nieuwe gebruikers toe te voegen, bronnen aan te passen of zelfs nieuwe services te implementeren.
 7. **Beveiliging:** Hoewel beveiliging in de cloud een veelbesproken onderwerp is, bieden veel cloudproviders geavanceerde beveiligingsfuncties die bedrijven wellicht niet zelf zouden kunnen implementeren.
 8. **Milieu-impact:** Door gebruik te maken van gedeelde resources in de cloud, kunnen bedrijven hun koolstofvoetafdruk verkleinen. Ze gebruiken alleen de serverruimte die ze nodig hebben, wat helpt bij het verminderen van het energieverbruik.
 9. **Concurrentievoordeel:** Met toegang tot geavanceerde technologieën kunnen zelfs kleine bedrijven concurreren met grotere spelers in hun industrie.
 10. **Samenwerking:** Cloudoplossingen zoals Google Workspace of Microsoft 365 bevorderen samenwerking door gebruikers in staat te stellen gelijktijdig in documenten te werken en informatie in realtime te delen.
 11. **Beheer van IT-capaciteit:** Door gebruik te maken van de cloud kunnen bedrijven hun IT-capaciteit optimaliseren, waardoor pieken in de vraag beter worden opgevangen zonder overinvestering in infrastructuur.
1. **Efficiëntie en Flexibiliteit:** Met de veranderende eisen van de moderne samenleving kan de overheid haar dienstverlening snel aanpassen door de flexibele capaciteit van de cloud.
 2. **Kostenbesparing:** De cloud vermindert de noodzaak voor de overheid om te investeren in fysieke infrastructuur, wat resulteert in aanzienlijke besparingen.
 3. **Toegankelijkheid en Transparantie:** Door gegevens in de cloud op te slaan, kan de overheid zorgen voor een bredere en gemakkelijkere toegang voor haar burgers, wat bijdraagt aan transparantie en openheid.
 4. **Beveiliging en Compliance:** Gerenommeerde cloud-aanbieders bieden geavanceerde beveiligingsfuncties en kunnen helpen om te voldoen aan strenge regelgevingsnormen.

Gemeenten willen de veranderkracht van digitalisering benutten en tegelijkertijd een antwoord vinden op de risico's en uitdagingen die dit met zich meebrengt. Met als doel: op weg naar een veilige, mensgerichte, transparante, effectieve digitale toekomst.

De gemeente kan daarbij de volgende doelstellingen hanteren:

§ 3.3 Uitdagingen en Risico's

Hoewel de voordelen evident zijn, brengt de migratie naar de cloud ook uitdagingen met zich mee. Vragen over dataprivacy, beveiliging en de integratie met bestaande systemen zijn zaken die zorgvuldig moeten worden aangepakt. De Nederlandse overheid moet ook zorgen voor de naleving van zowel nationale als Europese regelgeving met betrekking tot gegevensbescherming.

Hoewel cloudcomputing veel voordelen biedt, zijn er ook verschillende risico's en uitdagingen waarmee organisaties en individuen rekening moeten houden:

1. **Beveiligingszorgen:** De data van een organisatie bevindt zich buiten de directe controle van die organisatie, wat kan leiden tot zorgen over datalekken, hackpogingen en andere cyberbeveiligingsbedreigingen.
2. **Privacy van gegevens:** De opslag van gevoelige gegevens in de cloud kan leiden tot privacyzorgen, vooral als de cloudprovider gegevens opslaat in een ander rechtsgebied met andere privacywetten.
3. **Downtime:** Cloudserviceproviders kunnen te maken krijgen met downtime, waardoor klanten tijdelijk geen toegang hebben tot hun gegevens of applicaties.
4. **Afhankelijkheid van de provider:** Als een cloudprovider besluit om een bepaalde dienst stop te zetten, kunnen bedrijven gedwongen worden om alternatieven te zoeken en hun gegevens te migreren, wat zowel tijdrovend als kostbaar kan zijn.
5. **Overdrachtssnelheden:** Hoewel de toegang tot de cloud vaak snel is, kunnen de overdrachtssnelheden voor zeer grote datavolumes beperkt zijn, vooral als er een trage internetverbinding is.
6. **Kosten kunnen oplopen:** Terwijl initieel cloudservices kostenbesparingen kunnen opleveren, kunnen onverwachte kosten optreden bij verhoogd gebruik, met name als organisaties niet zorgvuldig hun verbruik monitoren.
7. **Integratie en compatibiliteit:** Het kan een uitdaging zijn om bestaande on-premises systemen te integreren met cloudoplossingen, vooral als er sprake is van verouderde technologie.
8. **Beheer van meerdere clouds:** Met de opkomst van multi-cloudstrategieën kunnen organisaties het moeilijk vinden om meerdere cloudomgevingen effectief te beheren.
9. **Contractuele en SLA-zorgen:** De service level agreements (SLA's) van cloudproviders kunnen beperkingen en uitsluitingen bevatten die organisaties moeten begrijpen en waarover

ze moeten onderhandelen.

10. **Wettelijke en regelgevende kwesties:** In sommige sectoren en landen zijn er wettelijke beperkingen op waar en hoe gegevens kunnen worden opgeslagen.
11. **Data-eigendom en -controle:** Het kan onduidelijk zijn wie de eigenaar is van de gegevens in de cloud en hoe gemakkelijk het is om gegevens te verplaatsen of te verwijderen.

Het is belangrijk dat organisaties en individuen deze risico's en uitdagingen grondig evalueren en de juiste voorzorgsmaatregelen nemen, zoals het regelmatig beoordelen van beveiligingsprotocollen, het zorgvuldig lezen van contracten en het hebben van een back-upstrategie.

§ 3.4 Cloudontwikkelingen

§ 3.4.1 Mondiale Trends

Cloud computing heeft de manier waarop bedrijven, overheden en individuen technologie gebruiken en benaderen getransformeerd. Dit dynamische veld blijft evolueren met nieuwe innovaties, gebruikspatronen en businessmodellen. Hier is een overzicht van de belangrijkste mondiale trends in cloud computing:

1. **Hybride en Multi-Cloud Strategieën:** Bedrijven en organisaties gaan steeds meer voor een hybride cloudbenadering, waarbij ze zowel private als public cloud resources combineren. Bovendien adopteren ze multi-cloud strategieën, waarbij ze gebruikmaken van diensten van meerdere cloudproviders, om flexibiliteit te vergroten en risico's te verminderen.
2. **Serverloze Architecturen:** Serverloos computing, vaak aangeduid als 'Function as a Service' (FaaS), stelt ontwikkelaars in staat om applicaties te bouwen en uit te voeren zonder zich zorgen te maken over de onderliggende infrastructuur. Dit leidt tot snellere ontwikkeling en kan kosten verminderen.
3. **Edge Computing:** Met de opkomst van IoT (Internet of Things) devices is er een groeiende behoefte om gegevensverwerking dichterbij de bron van gegevensgeneratie te brengen. Edge computing stelt organisaties in staat om gegevens te verwerken aan de "rand" van het netwerk, vaak op het apparaat zelf of in lokale servers, in plaats van in een gecentraliseerd datacenter.
4. **AI en Machine Learning Integratie:** Cloudproviders breiden hun diensten uit met tools en platforms die AI en machine learning integreren. Dit stelt organisaties in staat om krachtige data-analyses uit te voeren en intelligentie toe te voegen aan hun applicaties zonder grote voorafgaande investeringen.

5. **Verbeterde Beveiligingsmaatregelen:** Met de toenemende zorgen over cyberbeveiliging investeren cloudproviders in geavanceerde beveiligingstechnologieën, zoals AI-gedreven beveiligingsanalyses, encryptie en zero-trust beveiligingsmodellen.
6. **Containers en Orkestratie:** Containers, zoals Docker, en orkestratietools, zoals Kubernetes, zijn in populariteit gestegen, omdat ze ontwikkelaars helpen om applicaties te bouwen die gemakkelijk kunnen worden geschaald en over verschillende cloudomgevingen kunnen worden verplaatst.
7. **Duurzaamheid:** Met de groeiende zorgen over klimaatverandering kijken bedrijven en consumenten steeds meer naar de milieueffecten van technologie. Cloudproviders reageren hierop door duurzamere datacenters te bouwen en groene energie te gebruiken.
8. **Verticale Cloudoplossingen:** Cloudproviders bieden steeds vaker branchespecifieke cloudoplossingen aan, die zijn afgestemd op de unieke behoeften van sectoren zoals gezondheidszorg, financiën en productie.
9. **Data-soevereiniteit en Lokale Regulaties:** Met strengere gegevensbeschermingswetten in verschillende landen en regio's zijn cloudproviders begonnen met het bouwen van regionale datacenters en het aanbieden van specifieke oplossingen om aan lokale regelgeving te voldoen.
10. **Uitbreiding van Cloud naar Traditionele Sectoren:** Sectoren die traditioneel terughoudend waren in het adopteren van de cloud, zoals overheid, financiële dienstverlening en gezondheidszorg, zijn nu actief op zoek naar cloudoplossingen vanwege de bewezen voordelen op het gebied van schaalbaarheid, flexibiliteit en kosten.

De mondiale trends in cloud computing zijn een reflectie van de snel veranderende technologische landschap en de behoeften van organisaties en individuen. Terwijl cloud computing blijft evolueren, zullen de fundamentele principes van flexibiliteit, schaalbaarheid en on-demand toegang de drijvende krachten achter deze transformatie blijven. Het is cruciaal voor organisaties om deze trends te begrijpen en te benutten om concurrentievoordeel te behalen en te voldoen aan de veranderende verwachtingen van klanten en stakeholders.

§ 3.4.2 Europese Cloudontwikkelingen

De EU ziet standaardisatie als een strategisch instrument om de markt voor clouddiensten gezonder en veiliger te maken. Acties voor Cloud computing in het Rolling Plan 2022:

“Action 1 - Identify needs for ICT standards and open source technologies to further improve the interoperability, data protection and portability of cloud services and continue or start respective development activities...

Action 2 - Promote the use of the ICT standards needed to further improve the interoperability, data protection and portability of cloud services as well as multi-cloud management.”

Open standaarden vormen ook een van de componenten van Gaia-X.

Eén van de Europese verordeningen die Cloud het meest direct raakt, is de Data Act. Deze verordening stelt dat aanbieders van Clouddiensten het mogelijk moeten maken om over te stappen naar een andere dienstverlener zonder verlies van gegevens en functionaliteit. Hiervoor moeten dienstverleners waar mogelijk Europese standaarden of anders open specificaties gebruiken.

Aan interoperabiliteit tussen Clouddiensten stelt de Data Act minder expliciete eisen. De Autoriteit Consument en Markt heeft bij de Europese Commissie een voorstel ingediend om ook interoperabiliteit met open standaarden af te dwingen. De ACM wil met de Data Act bovendien verplichten dat aanbieders van Clouddiensten de door hen gebruikte standaarden openbaar te maken.

Over de inhoud van de Data Act wordt nog onderhandeld. Het is niet te verwachten dat de Triloog onderhandelingen voor het tweede kwartaal van 2023 worden afgerond

In een tijdperk waarin gegevens de nieuwe olie zijn en technologie centraal staat in beleidsvorming, regelgeving en dienstverlening, is het cruciaal voor de Nederlandse overheid om op de hoogte te blijven van belangrijke Europese cloudontwikkelingen. Deze ontwikkelingen zijn van invloed op de manier waarop gegevens worden opgeslagen, verwerkt en gedeeld op Europees niveau. Hier zijn enkele van de belangrijkste ontwikkelingen en hun implicaties:

1. **Europese Datastrategie:** In 2020 heeft de Europese Commissie een datastrategie gelanceerd die beoogt een gemeenschappelijke Europese data-ruimte te creëren. Deze strategie heeft directe implicaties voor cloud computing, aangezien het beoogt sectorspecifieke, gedeelde Europese datasystemen te ontwikkelen. Voor Nederland betekent dit dat overheidssystemen compatibel en in lijn moeten zijn met deze Europese initiatieven.
2. **GAIA-X:** Dit initiatief, voornamelijk aangestuurd door Duitsland en Frankrijk, streeft naar de oprichting van een concurrerend, veilig en betrouwbaar cloudbaanbod voor Europa. GAIA-X heeft als doel Europese waarden en regelgeving rondom data te waarborgen. De Nederlandse overheid moet de ontwikkelingen rondom GAIA-X nauwlettend volgen, gezien de potentiële implicaties voor interoperabiliteit en data-sovereiniteit.
3. **Digitale Soevereiniteit:** De EU heeft de ambitie uitgesproken om de digitale soevereiniteit van haar lidstaten te vergroten. Dit heeft betrekking op de capaciteit van Europa om

onafhankelijke digitale oplossingen te ontwikkelen, waaronder cloud infrastructuren. Dit kan gevolgen hebben voor waar en hoe overheidsgegevens worden opgeslagen.

4. **Versterking van de GDPR:** De Algemene Verordening Gegevensbescherming (AVG of GDPR in het Engels) blijft zich ontwikkelen met aanvullende richtlijnen en interpretaties. Het is cruciaal voor de Nederlandse overheid om zich aan te passen aan deze evoluerende normen, vooral in de context van cloud-diensten.
5. **EU Cloud Code of Conduct:** Deze gedragscode, goedgekeurd door de Europese Autoriteit voor gegevensbescherming, biedt richtlijnen voor cloud service providers over hoe zij de GDPR in hun diensten kunnen integreren. Het zorgt voor een uniforme interpretatie van de GDPR binnen de cloud-sector, wat relevant is voor de Nederlandse overheid bij het selecteren van cloud partners.
6. **Europese Cybersecurity Act:** Ingesteld in 2019, deze wet introduceert een EU-breed kader voor cybersecurity-certificering. Als de Nederlandse overheid gebruik maakt van cloud-diensten, is het belangrijk te waarborgen dat deze diensten voldoen aan de Europese cybersecurity-normen.

In de dynamische wereld van cloud computing is het essentieel voor de Nederlandse overheid om op de hoogte te blijven van de ontwikkelingen op Europees niveau. Deze veranderingen bieden zowel uitdagingen als kansen. Door proactief te zijn en een weloverwogen benadering van cloud-adoptie te handhaven, kan Nederland zorgen voor een veilige, efficiënte en conform de regelgeving cloud-omgeving voor zijn burgers en instellingen

§ 3.4.3 Cloudontwikkelingen Nederlandse Overheid

De Kamerbrief Rijksbreed cloudbeleid 2022 van Staatssecretaris van Huffelen noemt standaardisatie onder het kopje ‘Voordelen gebruik publieke clouddiensten’. De Staatssecretaris zegt hierover:

“Daarnaast vereist de inzet van de publieke cloud een hoge mate van standaardisatie. Dit kan in potentie kostenbesparend werken en de kwaliteit en implementatiesnelheid van ICT-projecten binnen het Rijk verhogen.”

Op 15 november 2022 organiseerde CIO Rijk een bijeenkomst over 'werken in de publieke cloud'. Hier sprak onder andere Chris Wauters, de nieuwe CTO van SSC-ICT, die standaardisatie direct in de opening van zijn presentatie noemde. Tijdens de bijeenkomst noemde Aart Jochem, de CISO Rijk dataportabiliteit en ‘multi-Cloud’ als middelen om de afhankelijkheid van één (Amerikaanse) marktpartij te beperken. Standaardisatie speelt daarbij een cruciale rol.

De Marktstudie Clouddiensten van de Autoriteit Consument en Markt van 2022 gaat uitgebreid in op de rol van standaarden in Cloud, en onderkent dat er zowel open als leveranciersafhankelijke standaarden bestaan. De ACM onderstreept in het rapport het belang van open standaarden voor dataportabiliteit en interoperabiliteit:

“Voor SaaS-diensten is het advies om zoveel mogelijk gebruik te maken van diensten die gebruik maken van open standaarden en formats.”

Tenslotte heeft de NORA een beslisboom voor risicobeoordeling Clouddiensten als onderdeel van het BIO thema Clouddiensten. Daarnaast onderhoudt de NORA een Wiki over Cloudcomputing. Hier staan voortsnog oudere artikelen over Cloud, en de NORA is nog op zoek naar een expertgroep die deze Wiki actueel kan houden.

De cloudtransitie heeft zich wereldwijd volop ingezet en de Nederlandse overheid is daarop geen uitzondering. Als reactie op de wereldwijde technologische ontwikkelingen en in lijn met haar eigen ambitie om moderner, efficiënter en dienstbaarder te zijn voor haar burgers, heeft de Nederlandse overheid verschillende cloudinitiatieven ontplooid. Hier volgt een blik op de belangrijkste cloudontwikkelingen binnen de Nederlandse overheid:

1. **Digitale Overheid en Cloud Eerst-Beleid:** Onder het streven naar een meer digitale overheid is er een 'cloud eerst'-beleid ontstaan. Dit betekent dat bij de overweging van nieuwe IT-projecten de voorkeur uitgaat naar cloudoplossingen, tenzij er overtuigende redenen zijn om dit niet te doen.
2. **DigiD in de Cloud:** Als een centrale dienst voor identiteitsverificatie heeft DigiD onderzocht hoe cloudtechnologieën de service betrouwbaarder en schaalbaarder kunnen maken, met name gezien het groeiend aantal gebruikers en diensten die DigiD vereisen.
3. **Focus op Open Standaarden:** Er is een groeiende nadruk gelegd op het gebruik van open standaarden bij cloud-implementaties. Dit zorgt voor interoperabiliteit tussen verschillende overheidsdiensten en vermindert het risico van 'vendor lock-in', waarbij de overheid te afhankelijk wordt van één leverancier.
4. **Cloudbeveiligingsbeleid:** In lijn met de wereldwijde zorgen over cyberbeveiliging heeft de Nederlandse overheid specifieke richtlijnen en best practices ontwikkeld voor het beveiligen van cloudservices. Dit omvat zaken zoals encryptie, toegangscontroles en regelmatige beveiligingsaudits.
5. **Dataopslag binnen Nederland:** Gezien de gevoeligheid van overheidsgegevens en de wettelijke beperkingen rondom gegevensopslag, geven sommige overheidsinstanties de voorkeur aan cloudoplossingen waarbij de gegevensopslag binnen Nederlandse grenzen blijft.
6. **Integratie van AI en Cloud:** Met de opkomst van kunstmatige intelligentie (AI) heeft de overheid onderzoek gedaan naar hoe cloud-infrastructuren kunnen worden geoptimaliseerd

voor AI-toepassingen, zoals voorspellende analyses en automatisering.

7. **Scholing en Training:** Erkenning van het feit dat cloudtechnologieën andere vaardigheden vereisen, heeft geleid tot initiatieven om overheidsmedewerkers op te leiden en te trainen in cloudcompetenties.
8. **Samenwerking met de Private Sector:** De overheid werkt steeds nauwer samen met de private sector, zowel om expertise te verkrijgen als om gezamenlijke cloud-oplossingen te ontwikkelen die kunnen worden gebruikt door zowel publieke als private entiteiten.

De cloudontwikkelingen binnen de Nederlandse overheid zijn een weerspiegeling van zowel de mondiale technologische trends als de unieke behoeften en uitdagingen van Nederland als natie. Door voorop te lopen in deze transitie en tegelijkertijd rekening te houden met beveiliging, privacy en interoperabiliteit, streeft de Nederlandse overheid ernaar een modern en effectief technologisch landschap te creëren voor haar burgers en instellingen

§ 3.5 Cloudleveranciers

de Nederlandse markt voor cloud computing is in veel opzichten een weerspiegeling van de bredere Europese en mondiale trends, maar heeft ook zijn eigen unieke kenmerken. Hier is een overzicht van de cloudleveranciers in Nederland:

Belangrijkste wereldwijde cloudleveranciers actief in Nederland:

1. **Amazon Web Services (AWS):** AWS heeft een actieve aanwezigheid in Nederland en biedt diensten aan vanuit datacenters in de regio Europa (Frankfurt, Ierland, Londen, Parijs, Stockholm, en sinds 2020 ook een aangekondigde regio in Spanje). Veel Nederlandse bedrijven en startups gebruiken AWS vanwege de brede reeks diensten en schaalbaarheid.
2. **Microsoft Azure:** Gezien de diepgewortelde relatie van veel Nederlandse bedrijven met Microsoft-producten, is Azure een populaire keuze. Microsoft heeft ook een datacenterregio in Nederland, wat helpt bij compliance- en datalocatievereisten.
3. **Google Cloud Platform (GCP):** Google heeft in 2020 zijn datacenteruitbreiding in Eemshaven voltooid, waarmee het zijn capaciteit in Nederland versterkte. Dit heeft het voor lokale bedrijven aantrekkelijker gemaakt om GCP te gebruiken.
4. **IBM Cloud:** Met een sterke aanwezigheid in de zakelijke markt biedt IBM Cloud diensten aan die populair zijn bij grotere Nederlandse organisaties, vooral die welke al in een IBM-ecosysteem zitten.
5. **Oracle Cloud:** Oracle heeft relaties met veel grote Nederlandse bedrijven, vooral op het gebied van database- en bedrijfssoftware. Hun cloudbaanbod wordt vaak overwogen door

bedrijven die al gebruik maken van Oracle-producten.

Lokale en regionale spelers:

1. **KPN Cloud:** Als een van de grootste telecomproviders in Nederland biedt KPN ook cloudservices aan, vooral gericht op de lokale markt.
2. **TransIP:** Een Nederlandse webhosting- en cloudserviceprovider, populair bij kleinere bedrijven en individuele gebruikers.
3. **LeaseWeb:** Met hoofdkantoor in Amsterdam, biedt LeaseWeb een scala aan cloudhostingdiensten en heeft het een aanzienlijke aanwezigheid in Nederland.
4. **Interxion:** Een grote Europese aanbieder van colocatie datacenterdiensten, met meerdere datacenters in Nederland.

§ 3.6 Nederlandse Overheid

De Nederlandse overheid heeft de afgelopen jaren flink geïnvesteerd in het moderniseren van haar IT-infrastructuur. Cloud-oplossingen zijn hierbij naar voren gekomen als een strategisch middel om efficiëntie te verhogen, kosten te besparen en diensten te verbeteren. Verschillende overheidsinstanties hebben projecten en initiatieven geïmplementeerd om de overgang naar de cloud te faciliteren.

§ 4. Cloudtechnologie en cloudstandaarden

§ 4.1 Cloudtechnologie

Hier zijn de belangrijkste cloudtechnologieën waar de Nederlandse overheid rekening mee moet houden:

1. **Hybride Cloud Infrastructuren:** Deze stellen de overheid in staat om gegevens en applicaties te verdelen over private en public clouds, waardoor er flexibiliteit ontstaat in gegevensbeheer en -toegang, terwijl de veiligheid en compliance worden gewaarborgd.
2. **Serverloze Computing:** Hiermee kan de overheid applicaties uitvoeren zonder zich bezig te houden met de onderliggende infrastructuur. Dit kan leiden tot kostenbesparingen en een snellere time-to-market voor overheidsapplicaties.

3. **Containers en Orkestratiesystemen:** Met technologieën zoals Docker en Kubernetes kan de overheid applicaties bouwen die zowel schaalbaar als draagbaar zijn, waardoor ze gemakkelijk kunnen worden overgebracht tussen verschillende cloudomgevingen.
4. **Edge Computing:** Vooral relevant voor smart city-initiatieven en IoT-projecten van de overheid. Het verwerken van data dichtbij de bron zorgt voor snellere reactietijden en vermindert de belasting op centrale systemen.
5. **AI en Machine Learning Services:** Cloud-gebaseerde AI-diensten kunnen de overheid helpen bij het analyseren van grote datasets, het voorspellen van trends en het bieden van gepersonaliseerde diensten aan burgers.
6. **Cloud-gebaseerde Analysetools:** Deze kunnen de overheid helpen bij het beter begrijpen van grote hoeveelheden data, van verkeerspatronen tot sociale dienstverlening, wat leidt tot beter geïnformeerde besluitvorming.
7. **Blockchain in de Cloud:** Voor bepaalde toepassingen, zoals transparante overheidsuitgaven of beveiligde digitale identiteiten, kan blockchain-technologie in de cloud van belang zijn.
8. **Data Lakes en Opslagoplossingen:** Gezien de enorme hoeveelheid data die door overheidsdiensten wordt gegenereerd, zijn schaalbare en flexibele opslagoplossingen essentieel.
9. **Unified Communications:** Cloud-gebaseerde communicatiesystemen kunnen de samenwerking tussen overheidsafdelingen verbeteren en een efficiënte externe communicatie mogelijk maken.
10. **Cloud Security en Identity Access Management (IAM) Systemen:** Naarmate meer diensten naar de cloud verhuizen, wordt de beveiliging ervan van cruciaal belang. IAM-systemen zorgen ervoor dat alleen geautoriseerde gebruikers toegang hebben tot bepaalde bronnen.

Het is van essentieel belang voor de Nederlandse overheid om proactief te zijn in het begrijpen en integreren van deze cloudtechnologieën. De juiste implementatie kan leiden tot verbeterde dienstverlening, operationele efficiëntie en kostenbesparingen. Tegelijkertijd moeten potentiële risico's, zoals beveiligingszorgen en gegevensbescherming, zorgvuldig worden aangepakt om het vertrouwen van het publiek te behouden

§ 4.2 Cloudstandaarden

Cloudcomputing heeft een scala aan standaarden nodig om interoperabiliteit, veiligheid, privacy en effectieve serviceprovisie te waarborgen. Wij maken onderscheid in de volgende soorten cloudstandaarden:

1. **Interoperabiliteitsstandaarden:** Deze zorgen ervoor dat verschillende cloudservices en -componenten met elkaar kunnen werken. Ze kunnen helpen bij het vermijden van vendor lock-in en het ondersteunen van multi-cloudstrategieën.
2. **Beveiligingsstandaarden:** Deze hebben betrekking op aspecten zoals data-encryptie, authenticatie, autorisatie en auditlogboekregistratie. Voorbeelden zijn de ISO/IEC 27017 standaard voor cloudbeveiliging en de ISO/IEC 27018 standaard voor de bescherming van persoonsgegevens in de cloud.
3. **Privacystandaarden:** Deze richten zich op de bescherming van persoonlijke gegevens die worden opgeslagen of verwerkt in de cloud. Hierbij kan gedacht worden aan standaarden die betrekking hebben op gegevensmaskering, anonimisering en pseudonimisering.
4. **Standaarden voor Servicebeheer en -orchestratie:** Deze standaarden richten zich op hoe cloudservices worden georkestreerd, beheerd en geautomatiseerd, zoals de Open Cloud Computing Interface (OCCI).
5. **Portabiliteitsstandaarden:** Deze standaarden maken het gemakkelijker om applicaties en gegevens van de ene cloudomgeving naar de andere te verplaatsen. Denk hierbij aan standaarden voor containerization.
6. **Beheer- en compliancestandaarden:** Standaarden die nodig zijn om clouddiensten te beheren.

Er kunnen standaarden en normen worden onderscheiden:

- **Standaarden:** Deze zijn technische specificaties of andere nauwkeurige criteria die worden gebruikt als regels of richtlijnen om consistentie en interoperabiliteit te waarborgen. Ze kunnen worden opgesteld door officiële normeringsorganisaties, door brancheorganisaties, of kunnen zelfs de facto standaarden worden door wijdverbreid gebruik.
- **Normen:** In de context van technologie en IT, zijn normen vaak officiële documenten die best practices, methodologieën, processen of specificaties bevatten die algemeen worden geaccepteerd. Normen worden meestal uitgegeven door officiële normeringsorganisaties.

In deze analyse worden beiden meegenomen.

Tussen 2014 en 2016 heeft het Forum Standaardisatie een verkenning uitgevoerd naar standaarden voor Cloud. Deze verkenning leverde al een inventarisatie op van open standaarden voor Cloud. NEN heeft hier recentelijk nog enkele ISO standaarden aan toegevoegd.

De lijst is niet noodzakelijk volledig en up-to-date, maar geeft wel een startpunt voor onderzoek naar standaardisatiebehoeften en mogelijke acties van het Forum Standaardisatie om standaarden status te geven. De volgende twee paragrafen geven een overzicht van de standaarden die uit de verkenning naar voren kwamen.

§ 4.2.1 Analyse Forum: Standaarden voor Cloud interoperabiliteit en dataportabiliteit

<u>DMTF</u>	DSP0263	Logisch model voor beheerinteractie tussen een afgenomen IaaS dienst en de aanbieder van die dienst, gebaseerd op RESTful API
<u>DMTF</u>	DSP8009	Het XML schema behorende bij DSP0263
<u>ISO</u>	ISO/IEC 17826:2012	Interface voor ontwikkelaars om opslag in de cloud te implementeren en/of gebruiken.
<u>ISO</u>	ISO/IEC 27036-1-3	Richtlijnen voor informatiebeveiliging in waardeketens van cloud aanbieders.
<u>ISO</u>	ISO/IEC 17788:2014	Definitie van standaard begrippen voor toepassingen in de cloud
<u>ISO</u>	ISO/IEC 17789:2014	Referentie architectuur (Cloud Computing Reference Architecture – CCRA) voor rollen, activiteiten en functionele componenten van een cloud service.
<u>ISO</u>	ISO-IEC 19941:2017	'Information technology — Cloud computing — Interoperability and portability' (deze komt dit jaar mogelijk in herziening)
<u>ISO</u>	ISO/IEC 27017	'Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services'
<u>ISO</u>	ISO/IEC 19944	delen 1 en 2, over data flow, data categories and data use bij cloud computing
<u>ISO</u>	ISO/IEC TS 23167:2020	'Information technology — Cloud computing — Common technologies and techniques'
<u>ISO</u>	ISO/IEC 19086	Serie over Service level agreement (SLA) framework bij cloud computing
<u>ISO</u>	ISO/IEC JTC 15C38	Cloud en gedistribueerde platformen
<u>ITU</u>	Y.3500	Hetzelfde als ISO17788.
<u>ITU</u>	Y.3502	Hetzelfde als ISO17789
<u>ITU</u>	Y.3510	Vereisten voor een cloud infrastructuur waaronder verwerkingsmogelijkheden, opslag en netwerk resources.
<u>ITU</u>	Y.3512	Uitbreiding van Y.3510 specifiek voor NaaS en IaaS cloud services
<u>ITU</u>	Y.3513	Aanbevelingen en functionele vereisten voor een IaaS Cloud service
<u>ITU</u>	Y.3520	Raamwerk voor end-to-end resource management in een cloud omgeving

<u>DMTF</u>	DSP0263	Logisch model voor beheerinteractie tussen een afgenomen IaaS dienst en de aanbieder van die dienst, gebaseerd op RESTful API
<u>OASIS</u>	TOSCA	Topology and Orchestration Specification for Cloud Applications (TOSCA). Standaard taal (XML gebaseerd) om applicatie laag diensten te porteren naar alternatieve cloud implementaties met behoud van interoperabiliteit.
<u>OGF</u>	GFD.183	Is eerste deel van Open Cloud Computing Interface (OCCI) en beschrijft een RESTful API voor beheer van IaaS, PaaS en SaaS cloud diensten. GFD.183 is de OCCI-Core specificatie
<u>OGF</u>	GFD.184	Is tweede deel van Open Cloud Computing Interface (OCCI) en beschrijft een RESTful API voor beheer van IaaS cloud diensten. GFD.184 is de OCCI http Rendering specificatie en beschrijft hoe de OCCI core kan communiceren op basis van http.
<u>OGF</u>	GFD.185	Is derde deel van Open Cloud Computing Interface (OCCI) en beschrijft een RESTful API voor beheer van IaaS cloud diensten. GFD.185 is de OCCI Infrastructuur specificatie en bevat extensies van de OCCI core specifiek voor IaaS diensten.
<u>SNIA</u>	CDMI	Cloud Data Management Interface (CDMI™) Definieert een functionele interface voor applicaties om gegevens elementen te muteren indien deze in de cloud zijn opgeslagen. De interface kan ook gebruikt worden voor beheer van dataopslag.
<u>ONF</u>	OpenFlow	Besturing van Software Defined Networking switches en routers, OpenFlow wordt veel toegepast door organisaties die een open SDN netwerk bouwen met apparatuur van verschillende fabrikanten.
<u>NIST</u>	FIPS 140-2 level 4	Een standaard van de Amerikaanse regering om cryptografische modules te beoordelen. Kan relevant zijn voor end-to-end encryptie van data in de cloud.

§ 4.2.2 Algemene standaarden

De volgende standaarden zijn niet in een van de hoofdcategorieën in te delen, maar zijn wel van belang:

1. **NIST SP 500-292:** Het NIST Cloud Computing Reference Architecture is een generiek high-level conceptueel model dat dient als een gebruikersgericht referentiepunt.
2. **GAIA-X:** Een initiatief in Europa, gericht op het creëren van een uniform framework voor cloud services, dat bepaalde principes en beleidsregels vaststelt die functioneren als normen.

§ 4.2.3 Interoperabiliteitsstandaarden

Verder zijn voor clouddiensten mogelijk relevant:

- REST API Design Rules
- Open API Specification

§ 4.2.4 Beveiligingsstandaarden

1. **OAuth:** Een open standaard voor toegangsdelegatie, die veel wordt gebruikt voor token-gebaseerde authenticatie en autorisatie op het internet.
2. SAML (wordt op termijn waarschijnlijk uitgefaseerd ten gunste van OIDC)
3. **OpenID Connect:** Een simpele identiteitslaag bovenop het OAuth 2.0-protocol, die gebruikersauthenticatie mogelijk maakt.
4. **ISO/IEC 27001:** Een wereldwijd erkende norm voor het beheren van risico's op het gebied van informatiebeveiliging.
5. **ISO/IEC 27017:** Een cloud-specifieke norm die extra beveiligingscontroles bevat bovenop ISO/IEC 27001 specifiek voor cloudservices.
6. **Cloud Security Alliance (CSA) Best Practices:** Hoewel niet een "norm" in de traditionele zin, biedt CSA richtlijnen en best practices voor cloudbeveiliging die algemeen worden geaccepteerd in de industrie.

§ 4.2.5 Privacystandaarden

3. **ISO/IEC 27018:** Een code voor de bescherming van persoonlijke gegevens in de cloud, op basis van ISO/IEC 27001.

§ 4.2.6 Standaarden voor Servicebeheer en -orchestratie

§ 4.2.7 Portabiliteitsstandaarden

1. **Open Virtualization Format (OVF):** Een open standaard voor het verpakken en distribueren van gevirtualiseerde applicaties.

§ 4.2.8 Beheerstandaarden

1. **Cloud Data Management Interface (CDMI):** Een set van protocollen die zijn gedefinieerd voor het beheer van cloud storage.
2. **ENISA Cloud Computing Risk Assessment:** Een norm van het European Network and Information Security Agency (ENISA) dat zich richt op risicobeoordeling in de cloudomgeving.

§ 4.3 Witte vlekken

§ 5. Conclusies en aanbevelingen

§ 6. Conformiteit

Naast onderdelen die als niet normatief gemarkeerd zijn, zijn ook alle diagrammen, voorbeelden, en noten in dit document niet normatief. Verder is alles in dit document normatief.

§ A. Index

§ A.1 Begrippen gedefinieerd door deze specificatie

§ A.2 Begrippen gedefinieerd door verwijzing

↑