Cloud-Portabiliteit

Uitdagingen, Ontwikkelingen & Standaarden

innovalor

Colofon

Publicatiedatum

1 juni 2026

Projectnaam

Onderzoek cloud-portabiliteit, uitdagingen, ontwikkelingen en standaarden

Auteurs

- C. Vermeulen (InnoValor Advies)
- A. Brandt (InnoValor Advies)
- B. den Haan (InnoValor Advies)

Opdrachtgever

Forum Standaardisatie

Postbus 96810

2509 JE Den Haag

info@forumstandaardisatie.nl

Forum Standaardisatie

Creative commons

Inhoudsopgave

Managementsamenvatting

Wat is de aanleiding voor dit onderzoek?

De cloud-markt wordt gedomineerd door enkele grote aanbieders buiten de EU, wat leidt tot toenemende afhankelijkheidsrisico's, mede door geopolitieke ontwikkelingen. Dit vergroot de behoefte aan meer digitale soevereiniteit en een beter functionerende, concurrerende cloud-markt. In Nederland heeft de ontwikkeling van een overheidsbrede soevereine clouddienst daarom hoge prioriteit, evenals de versterking van de Europese cloud-markt.

Tegen deze achtergrond wil het Forum Standaardisatie met dit onderzoek gericht bijdragen aan het vergroten van cloud-portabiliteit (ofwel het technisch kunnen migreren of exit uit een clouddienst), door inzicht te bieden in relevante standaarden en het stimuleren van hun toepassing.

Wat doen standaarden voor portabiliteit?

Standaarden die bijdragen aan portabiliteit van data en applicaties maken het mogelijk voor (overheids-)organisaties om eenvoudiger te migreren tussen verschillende cloud-aanbieders of uit de cloud te gaan.

Zonder portabiliteit geen keuzevrijheid, zonder keuzevrijheid geen soevereiniteit

Beleidsinitiatieven voor meer soevereiniteit en autonomie falen in de praktijk, als data en applicaties niet overdraagbaar zijn tussen clouddiensten. In de huidige situatie is die portabiliteit namelijk beperkt. Overstappen is complex, kostbaar en vaak nauwelijks uitvoerbaar. Hierdoor ontstaat een fundamenteel risico: zonder substantiële verbetering van data- en applicatie-portabiliteit blijft de overstap naar soevereine en Europese cloud-oplossingen beperkt, en worden nieuwe initiatieven structureel onderbenut met alle gevolgen van dien.

Wat is er onderzocht?

Dit onderzoek licht de verschillende facetten van cloud-portabiliteit toe, brengt (internationale) ontwikkelingen in kaart, identificeert probleemgebieden, duidt witte vlekken op de open standaarden lijsten en identificeert kansrijke portabiliteit-standaarden voor opname op de lijsten van het Forum Standaardisatie. De kennis uit dit onderzoek stelt het Forum Standaardisatie in staat om gericht bij te dragen aan meer cloud-portabiliteit.

Hoewel de initiële focus lag op infrastructuurniveau (IaaS), richt dit onderzoek zich primair op portabiliteit van data en applicaties tussen verschillende clouddiensten. Juist rond data en applicaties ontstaat in de praktijk immers de grootste lock-in.

Waarom is het moeilijk om data of applicaties over te zetten?

Er zijn echter grote financiële, contractuele en technische drempels. Technisch gezien zijn bepaalde typen data en applicaties sterk verweven met leverancierspecifieke clouddiensten en -platforms, waardoor zij niet eenvoudig los te koppelen zijn.

Beperkte standaardisatie en openheid leiden tot grote complexiteit bij migraties tussen cloud-omgevingen of bij het verlaten van de cloud.

Hoe werkt de vendor lock in?

In theorie is overstappen tussen cloud-leveranciers mogelijk. In de praktijk blijkt dit vaak zeer kostbaar en complex, waardoor de overstapdrempels zo hoog zijn dat een positieve businesscase moeilijk haalbaar is. Door bundeling van diensten (koppelverkoop) en het gebruik van 'handige' functies wordt werken in de cloud eenvoudig en efficiënt. Tegelijkertijd ontstaat een keerzijde: organisaties raken stap voor stap steeds sterker afhankelijk van één leverancier. Hierdoor wordt het systeem na verloop van tijd steeds moeilijker te verlaten.

Wat is de rol van open standaarden?

Open standaarden maken uitwisseling en overdraagbaarheid van data en applicaties mogelijk en beperken daarmee de afhankelijkheid van specifieke cloud-leveranciers. Daarnaast faciliteren open standaarden het realiseren van migratie- en exitmogelijkheden. Zij vormen een belangrijk instrument

voor leveranciersonafhankelijkheid en ondersteunen overheden bij het maken van toekomstbestendige keuzes in de inkoop en inzet van clouddiensten.

Wat zijn de grootste aandachtsgebieden waarop open standaarden ontbreken?

Open standaarden voor cloud-portabiliteit zijn momenteel nog onvoldoende ontwikkeld en toegepast op een aantal cruciale domeinen. Met name bij key management, identity & access management en databases bestaan duidelijke lacunes. Op het gebied van containerisatie en orchestratie is daarentegen meer volwassenheid zichtbaar. Dit domein draagt bij aan applicatie-portabiliteit doordat applicaties gestandaardiseerd kunnen worden verpakt en uitgerold.

Wat zijn de Europese kansen voor cloud-portabiliteit en nieuwe standaarden?

- Met name de Data Act, de Digital Markets Act (DMA) en de Cloud and AI Development Act bieden een juridisch kader om portabiliteit te versterken en overstappen tussen cloud-aanbieders te stimuleren.
- De Data Act introduceert een Europees standaardenregister met portabiliteit-standaarden waar aanbieders aan moeten voldoen. Het register moet nog gevuld worden.
- Standaarden worden ontwikkeld onder mandaat van een Europees standaardisatieverzoek door standaardisatie-organisaties CEN, CENELEC en ETSI (in het daarvoor opgerichte JTC 25) momenteel aan ontwikkeling van standaarden, waar ook wordt samengewerkt met ISO/IEC JTC 1/SC 38 (Cloud Computing and Distributed Platforms).
- De DMA richt zich specifiek op zogeheten poortwachters en kan hen direct verplichtingen opleggen. Indien uit het lopende onderzoek (in opdracht van de Europese Commissie) blijkt dat clouddienstaanbieders Amazon en Microsoft als poortwachter geïdentificeerd worden, dan levert dit een extra juridisch instrument richting deze dominante cloud-aanbieders op.

Wat zijn de belangrijkste risico's voor portabiliteit-standaarden?

- Grote cloud-leveranciers passen open standaarden weinig toe. Daardoor blijven deze standaarden beperkt gebruikt. Ze halen zo onvoldoende marktadoptie om ze verplicht te kunnen stellen op Europees niveau of op nationaal niveau door Forum Standaardisatie.
- De Europese Commissie stuurt 'zacht en bottom-up' op de ontwikkeling van standaarden. De realisatie verloopt geleidelijk. Het is onzeker hoe snel dit daadwerkelijk leidt tot nieuwe en volwassen standaarden voor de belangrijkste portabiliteit-problemen.
- Het risico bestaat dat licentiekosten en gebruiksvoorwaarden een belemmering vormen voor opname in het Europese standaardenregister. Hierdoor zou een deel van de beschikbare standaarden (waaronder sommige ISO-normen) bij voorbaat afvallen op EU-niveau.
- Open source tools en methodieken vormen een concurrerend alternatief voor open standaarden. De inzet hiervan kan de praktische prikkel verlagen voor het ontwikkelen van open standaarden. Anderzijds kunnen tools de ontwikkeling en adoptie van open standaarden stimuleren, maar regie hierop ontbreekt.

Welke aanbevelingen worden gedaan?

1. **Neem regie en toon leiderschap.** Stimuleer actief adoptie van portabiliteit-standaarden en wacht niet op hyperscalers of Europese besluitvorming. Wijs relevante standaarden nationaal aan en bevorder gebruik via inkoop en (waar nodig) verplichtstelling. Doe dit in samenhang met relevante stakeholders, zodat beleid, architectuur, standaardisatie en toepassing in de praktijk op elkaar aansluiten. Organiseer regie op het samenspel tussen architectuur, standaarden en open source tools.
2. **Versterk het toetsingskader van standaarden.** Veranker cloud-portabiliteit (migratie en exit) expliciet in de beoordelingssystematiek van standaarden. Ontwikkel daarnaast een specifiek beoordelingskader voor potentiële cloud-standaarden met helder onderscheid tussen standaarden, methoden, implementaties, tooling en architectuur en hun potentie voor lijsten.

3. **Stuur op toepassing in de praktijk.** Stimuleer gebruik van open standaarden bij cloud-aanbestedingen en (soevereine) cloud-architecturen. Veranker uniforme definities voor gebruik in inkoop en ontwikkeling door de overheid.
4. **Focus op kansrijke standaarden en witte vlekken.** Zet in op beschikbare standaarden in het containerdomein. Onderzoek versterking of opname van de voorgestelde standaarden in dit rapport, waaronder HAVEN, OCI, TOSCA, HELM Charts en KMIP. Prioriteer de aanpak hiervan. Maak met experts nog een nadere prioritering van de overige standaarden uit dit rapport.
5. **Sluit aan bij Europese ontwikkelingen.** Volg en beïnvloed actief het Europese standaardenregister en standaardisatie-initiatieven. Europese verplichtingen richten zich primair op aanbieders; nationale sturing via de 'Pas toe of leg uit'-lijst blijft daarom nodig voor overheidsinkoop. Zorg dat juridische kaders, zoals de Data Act, worden ondersteund door toepasbare standaarden.
6. **Versterk samenwerking en kennisontwikkeling.** Werk structureel samen met gremia zoals Tiido (MIDO) voor kennisdeling en vroegsignalering**.** Ontwikkel een portabiliteitsarchitectuur en technische baseline**.** Faciliteer kennisdeling via een dynamisch kennisplatform.

1. Inleiding

In dit hoofdstuk worden de achtergronden van het Forum Standaardisatie en open standaarden geschetst.

1.1 Achtergrond Forum Standaardisatie

Het Forum Standaardisatie is een adviescommissie met deskundigen uit diverse overheidsorganisaties, het bedrijfsleven en de wetenschap. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties benoemt de leden op persoonlijke titel. Het Forum wordt ondersteund door een secretariaat, het Bureau Forum Standaardisatie (BFS). Dit bureau is gehuisvest bij Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Een van de manieren van Forum Standaardisatie om de onderlinge samenwerking van overheden te bevorderen is door open standaarden te toetsen en voor te schrijven aan publieke organisaties. (Zie bijlage B voor de definitie van open standaarden.) Op de 'Pas toe of leg uit'-lijst (PTLU) van het Forum Standaardisatie staan standaarden die overheden verplicht moeten uitvragen volgens de 'Pas toe of leg uit'-verplichting op het moment dat ze een ICT-dienst of -product aanschaffen dat binnen het desbetreffende toepassingsgebied valt van de standaard. Op de 'Aanbevolen standaarden'-lijst staan standaarden die door het Forum Standaardisatie worden aanbevolen voor gebruik.

Het Forum Standaardisatie geeft hier invulling aan door open standaarden te toetsen en – waar passend – voor te schrijven aan publieke organisaties. Overheden passen deze standaarden toe bij de inkoop van ICT-diensten en -producten en bij de ontwikkeling van nieuwe voorzieningen. Dit biedt marktpartijen duidelijkheid over de geldende eisen, waardoor zij hun producten en diensten hierop kunnen inrichten. Het hanteren van open standaarden bevordert een gelijk speelveld, versterkt interoperabiliteit en draagt bij aan duurzame samenwerking tussen overheid, bedrijfsleven en burgers.

Om tot goed onderbouwde adviezen te komen voert het Forum Standaardisatie onderzoek uit naar het gebruik van open standaarden, evalueert het periodiek de standaarden op de lijsten en verkent het nieuwe vraagstukken waarbij standaardisatie een rol kan spelen. Deze kennisbasis stelt het Forum in staat om gericht en onderbouwd bij te dragen aan maatschappelijke en technologische ontwikkelingen, waaronder actuele vraagstukken rond cloud-portabiliteit en de rol die open standaarden daarin dienen in te nemen.

1.2 Aanleiding onderzoek

Cloud computing is al jaren populair bij de overheid. Tegelijkertijd zijn er zorgen over 'vendor lock-in', interoperabiliteit en portabiliteit. Vendor lock-in ontstaat wanneer technische, contractuele, economische of organisatorische afhankelijkheden ertoe leiden dat het overstappen naar een andere leverancier significante inspanning, kosten of risico's met zich meebrengt. In het kader van deze toenemende aandacht voor digitale soevereiniteit groeit de behoefte aan cloud-standaarden, met nadruk op open standaarden, om op meer leveranciers-onafhankelijke (en met name Big Tech-onafhankelijke) wijze de verschillende soorten clouddiensten te kunnen ontwikkelen en inkopen.

Het Forum Standaardisatie liet in 2024 reeds onderzoek doen naar cloud-standaardisatie. Uit dat onderzoek bleek dat er een gebrek is aan open standaarden voor data-portabiliteit en interoperabiliteit, wat leidt tot een toenemende afhankelijkheid van cloud-leveranciers. Het Forum Standaardisatie heeft in de vergadering van 15 april 2025 besloten om een dossier 'markt en open standaarden' (voorheen leveranciersbetrokkenheid) te starten met cloud als inhoudelijk onderwerp. Op 25 juni 2025 heeft het Forum Standaardisatie ingestemd met het 'Plan van aanpak en achtergrondnotitie vervolgaanpak standaarden en standaardisatieactiviteiten clouddiensten' van de Sponsorgroep Markt en (Cloud)standaarden, als onderdeel van dit dossier.

Eén van de vier aandachtsgebieden van het plan van aanpak vormt ‘het identificeren en overzicht onderhouden van open standaarden rondom cloud’. Dit door InnoValor Advies uitgevoerde onderzoek draagt bij aan de invulling van dit aandachtsgebied, door te focussen op portabiliteit-standaarden die relevant zijn voor de Nederlandse context.

Portabiliteit-standaarden maken het mogelijk voor (overheids-)organisaties om eenvoudiger te migreren tussen verschillende cloud-aanbieders, wat zorgt voor een verminderd risico op leveranciersafhankelijkheid. De opdracht van Bureau Forum Standaardisatie aan InnoValor Advies is dan ook om concrete en volwassen open portabiliteit-standaarden te identificeren, waardoor de toepassing van deze standaarden bevorderd kan worden.

Het onderzoek vormt hiermee een vervolgstap die sterk samenhangt met onder andere de Nederlandse Digitaliseringsstrategie (NDS) – waarin Cloud is aangemerkt als prioriteit - en de Architectuur Digitale Overheid - Domeinarchitectuur Infrastructuur. Beiden sporen, naast de oproep tot het ontwikkelen van een soevereine overheidscloud, sturen aan op het ontwikkelen van een marktplaats voor clouddiensten waarop overheidsorganisaties gemakkelijk kunnen wisselen van cloud-aanbieder. Voldoende portabiliteit is een belangrijke voorwaarde voor het goed laten werken van zo’n marktplaats.

1.3 Doel van dit onderzoek

Het doel is het identificeren van cloud-portabiliteit standaarden die kansrijk zijn voor opname op de lijsten van het Forum Standaardisatie. Hierbij wordt er voortgebouwd op een brede cloud-verkenning die het Forum Standaardisatie heeft laten uitvoeren in 2024. Het huidige onderzoek biedt verdieping op het vlak van portabiliteit-standaarden voor clouddiensten door een specifiek op portabiliteit gerichte analyse. Daarnaast biedt het onderzoek een geactualiseerd overzicht van marktontwikkelingen, signaleert het relevante lacunes en anticipeert het op aankomende Europese standaardisatie-initiatieven om de besluitvorming van het Forum te ondersteunen.

1.4 Aanpak van dit onderzoek

- Bij de uitvoering van dit onderzoek is de volgende aanpak gehanteerd:
- Bureau-onderzoek: Verkenning naar beschikbaar materiaal over portabiliteit-standaarden voor clouddiensten, relevante Europese verordeningen, normalisatie-initiatieven, Nederlandse beleidsinitiatieven en beleids-‘stacks’.
- Ruim 20 interviews met sponsorgroepleden, stakeholders, gebruikers en leveranciers (hierna gezamenlijk aangeduid als experts) die in hun werkzaamheden met clouddiensten te maken hebben.
- Bespreking van de tussentijdse bevindingen aan een brede groep experts in de Tiido-werkgroep (MIDO), aan de hand waarvan de praktijk use cases zijn uitgewerkt.
- Validatie en verdiepende expertsessie: Bespreking van de resultaten in een expertbijeenkomst voor nadere duiding, aanscherping en mapping van de bevindingen. Tijdens deze expertsessie zijn de belangrijkste aandachtsgebieden in cloud-portabiliteit geduid, wat focus voor de vervolgstappen van het onderzoek gaf.
- Verdieping op de aandachtspunten middels specifieke deskresearch en interviews.

1.5 Scope

Dit onderzoek richt zich primair op het identificeren van standaarden voor data- en applicatie-portabiliteit binnen en tussen clouddiensten, met het oog op toepassing in de Nederlandse overheidscontext. Het onderzoek richt zich met name op het vinden van standaarden die mogelijk potentie hebben voor plaatsing op de lijsten van Forum Standaardisatie.

Daarbij ligt de focus op cloud-native toepassingen; de migratie van legacy-systemen naar de cloud valt expliciet buiten de scope van dit onderzoek. Dit wordt in onderstaande alinea toegelicht.

In lijn met het Architectuur Digitale Overheid - Domeinarchitectuur Infrastructuur richt dit onderzoek zich uitsluitend op “moderne cloud-native applicaties, gebouwd met containertechnologie”. Dit architectuurdocument positioneert containerisatie als de norm voor cloud-native ontwikkeling en stelt dat binnen het beoogde cloud-marktplaatsmodel (zie paragraaf 3.2.4) geen ruimte is voor functionaliteit die uitsluitend op traditionele virtual machines (VM’s) draait.

De scope van dit onderzoek beperkt zich daarom tot containertechnologie en de informatiesystemen die daarop kunnen worden ontwikkeld en uitgevoerd. Zogenaamde legacy-systemen vallen buiten de scope. Migratie van legacy-systemen naar de cloud betreft een bredere transformatieopgave, waarin naast portabiliteit ook modernisering, herontwerp en organisatorische aspecten een belangrijke rol spelen. In bijlage C (paragraaf C.3) is een nadere toelichting op legacy-systemen opgenomen.

1.6 Periode

Dit onderzoek is uitgevoerd in de periode augustus 2025 tot en met mei 2026.

1.7 Leeswijzer

Introductie:

- Hoofdstuk 1 beschrijft de achtergrond, aanleiding, onderzoeksopdracht en aanpak.
- Hoofdstuk 2 introduceert de belangrijkste begrippen rond cloud en cloud-portabiliteit.

Relevante ontwikkelingen:

- Hoofdstuk 3 geeft een overzicht van relevante ontwikkelingen die kansen of bedreigingen veroorzaken in de context van cloud-portabiliteit, cloud-switching en cloud-standaarden. Onder andere ontwikkelingen in de cloud-markt, de impact van Europese verordeningen, alsook nationale en internationale beleidsontwikkelingen komen in dit hoofdstuk aan bod.

Standaarden:

- Hoofdstuk 4 omschrijft de aanpak om standaarden te identificeren en geeft een overzicht van de belangrijkste vier aandachtsgebieden voor cloud-portabiliteit standaarden.
- Hoofdstukken 5 tot en met 8 diepen de vier aandachtsgebieden meer inhoudelijk uit, duiden specifieke standaarden, ontwikkelingen hierin en witte vlekken op de lijsten van Forum Standaardisatie.
- Hoofdstuk 9 gaat in op een aantal standaarden buiten de geïdentificeerde aandachtsgebieden.
- Hoofdstuk 10 vat de inzichten over standaarden (van hoofdstuk vier tot en met negen) samen.

Conclusies & Aanbevelingen:

- Hoofdstuk 11 presenteert de conclusies en aanbevelingen.

Bijlagen:

- In de bijlagen staat achtergrondmateriaal opgenomen, waaronder:
    - begrippen over cloud, en over standaarden
    - toelichting op de verschillende cloud-portabiliteitsfacetten
    - longlist standaarden overzicht

1.8 Definities

In Bijlage B zijn de belangrijkste begrippen en definities uit dit onderzoeksrapport opgenomen. In de tekst zijn deze begrippen vetgedrukt weergegeven; zij zijn tevens opgenomen in de begrippenlijst in de bijlage.

2 Introductie cloud & portabiliteit

In dit hoofdstuk worden de kernbegrippen rond cloud en cloud-portabiliteit toegelicht. Ter illustratie wordt ingegaan op voorbeelden van clouddiensten met uiteenlopende niveaus van portabiliteit

2.1 Basis voor begrippen en definities

Dit onderzoek neemt het door het Overheidsbreed Beleidsoverleg Digitale Overheid, ofwel OBDO, op 16 april 2026 vastgestelde Clouddefinities en begrippenlijst V1.0 zoveel mogelijk als uitgangspunt voor de gehanteerde terminologie rond cloud. Omdat de documentatie van het OBDO niet openbaar beschikbaar is, staan de belangrijkste definities onderstaande weergegeven. Als basis wordt de breed aanvaarde National Institute of Standards and Technology (NIST) definitie gevolgd, net als in het Rijkscloudbeleid 2022. In Bijlage B staat daarnaast nog een totaaloverzicht van termen en definities, aangevuld van definities die niet opgenomen staan in de Cloud-definities en begrippenlijst V1.0. De dikgedrukte termen in dit rapport staan in Bijlage B gedefinieerd.

2.2 Afwegingen en afhankelijkheden

De verdeling van verantwoordelijkheden tussen de clouddienstverlener en de afnemer varieert per **cloud-servicemodel** (IaaS, PaaS, SaaS), waarbij de organisatie altijd eindverantwoordelijk blijft voor het gekozen uitbestedingsniveau en de bijbehorende risico's. Het uitbesteden van taken creëert operationele afhankelijkheden die vooraf getoetst moeten worden aan het acceptatiekader van de organisatie. In de praktijk blijkt deze strategische afweging echter vaak ontoereikend; zo concludeert de Algemene Rekenkamer in het rapport 'Donkere wolken pakken samen: Het Rijk in de cloud' dat de men ondoordacht cloud-transities heeft aangegaan, zonder essentiële risicoanalyses vooraf. Dit geldt niet alleen voor de rijksoverheid en is een overheidsbreed aandachtspunt melden experts.

2.3 Bron voor kerndefinitie cloud-portabiliteit

In dit hoofdstuk worden diverse nieuwe termen geïntroduceerd en toegelicht. Hierbij wordt zoveel mogelijk gebruik gemaakt van bestaande gedragen definities. Specifiek rond cloud-portabiliteit worden er twee belangrijke ISO-normen gebruikt om portabiliteit tussen clouddiensten te definiëren, te noemen;

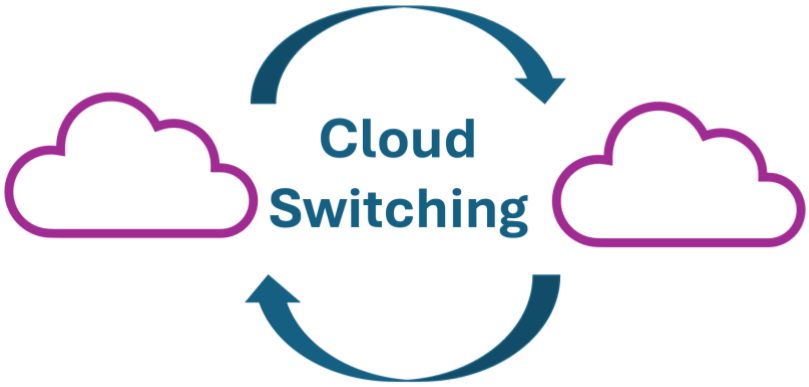
- ISO/IEC 22123-1:2023 Information technology - Cloud computing Part 1: Vocabulary omschrijft de concepten, kenmerken en typen van interoperabiliteit en portabiliteit in cloud computing; en
- ISO/IEC 19941:2017- Cloud computing – Interoperability and portability bouwt hierop voort en werkt de verschillende facetten van data-portabiliteit en applicatie-portabiliteit nader uit. (ISO/IEC 19941:2017 is in 2023 voor het laatst gereviewed en wordt binnenkort mogelijk vervangen door ISO/IEC DIS 19941-1 welke op het moment van schrijven de status draft heeft).

Figuur 1 Cloud-Portabiliteit

2.4 Cloud switching vereist portabiliteit

In dit onderzoek wordt (**cloud) portabiliteit** opgevat als het vermogen van een cloud-afnemer om data, applicaties of systemen tussen twee verschillende clouddiensten te verplaatsen tegen lage kosten en met minimale verstoring of aanpassingen, of exit uit de cloud. De termen portabiliteit en cloud-portabiliteit worden in dit onderzoek door elkaar gebruikt.

Cloud switching is een breder begrip dat vaak wordt gebruikt in de context van marktregulering (zoals de EU Data Act). Het verwijst naar het daadwerkelijke proces van overstappen van cloud-leverancier; Het beëindigen van een contract bij aanbieder A en het starten bij aanbieder B. Het gaat bij cloud switching niet alleen om de technische overdracht (portabiliteit), maar ook om de operationele en contractuele aspecten, zoals opzegtermijnen, kosten voor data-exit (zogenaamde egress fees) en het behoud van functionele continuïteit. Portabiliteit is dus een randvoorwaarde voor cloud switching.



Figuur 2 Cloud Switching

De technische invulling van cloud switching sluit inhoudelijk aan op het portabiliteitsbegrip uit ISO/IEC 19941:2017, waarin met name data- en applicatie-portabiliteit worden onderscheiden. De Data Act operationaliseert deze principes juridisch door ze te vertalen naar afdwingbare verplichtingen voor cloud-providers.

2.5 De mate van portabiliteit is een schaal

Portabiliteit is geen binair concept; het is niet een kwestie van alles of niets, maar een schaal. Vrijwel alle data of applicaties kan op één of andere manier worden overgezet naar een gelijkwaardige andere clouddienst als er genoeg in wordt geïnvesteerd door de cloud-afnemer. De overwegingen om voor een organisatie dit wel of niet te doen, liggen op het vlak van kosten, de risico's en hoe deze te beheersen is in verhouding tot de verwachte voordelen van de migratie.

2.6 Meer marktwerking draagt bij aan meer portabiliteit

Cloud-portabiliteit bestaat grofweg uit twee onderdelen: het overzetten van data en het overzetten van applicaties. Bij een migratie tussen SaaS-diensten ligt het accent op migratie van data. Bij een migratie van een applicatie tussen PaaS-diensten komt er veel meer bij kijken. Onderstaande (alsook in de volgende paragraaf) wordt dit nader toegelicht:

2.6.1 Software as a Service migratie in competitieve markten gaat vrij goed

Bij veel voorkomende Software as a Service (SaaS)-diensten, zoals HR-systemen of webportalen, is overstappen doorgaans relatief goed uitvoerbaar. Dit komt doordat deze markten competitief zijn en deze SaaS-leveranciers migratie actief ondersteunen. In deze gevallen gaat het vooral om het

overzetten van bepaalde typen data, wat relatief eenvoudig is doordat gebruik wordt gemaakt van gestandaardiseerde formaten en interfaces.

Bij SaaS-systemen zoals HR-systeem, CRM-systeem of webportalen gaat het vaak om:

- tabellen met records (zoals: medewerkers, klanten, contracten)
- duidelijke velden (zoals: naam, adres, salaris, etc.)
- vaste datamodellen

Dit is vaak klassieke gestructureerde data. Die is goed te exporteren via breed geadopteerd open standaarden zoals CSV of XML bijvoorbeeld. Dit verschilt niet wezenlijk van niet-cloud gebaseerde software migraties. Dergelijke standaarden zijn ook niet cloud-specifiek.

2.6.2 Software as a Service migratie in oligopolie markten is complex

In andere SaaS-markten is de situatie complexer. Een voorbeeld is de markt voor digitale werkplekken, waarbij Microsoft 365 de markt sterk domineert. Hoewel dit formeel ook een SaaS-dienst is, betreft het hier geen afzonderlijke applicatie, maar een geïntegreerd geheel van allerlei diensten zoals e-mail, documenten, samenwerking, identiteit en beveiliging. Bij dit soort oplossingen gaat het niet alleen om het migreren van data (zoals e-mail en documenten), maar ook om:

- uitgebreide configuraties (rechten, groepen, policies)
- integraties tussen verschillende diensten
- ongestructureerde data (chat, documenten, bijlagen); en
- de dagelijkse werkomgeving van gebruikers.

Daarnaast zijn deze omgevingen sterk verweven met leverancier-specifieke platformdiensten, waardoor volledige overdraagbaarheid beperkt is. Migratie betekent daarom niet alleen dataoverdracht, maar ook herinrichting van de gehele omgeving en aanpassing van processen en werkwijze.

De mate van portabiliteit is in dit soort markten daardoor veel kleiner, ondanks dat het technisch ook om een SaaS-dienst gaat.

2.6.3 Applicatie-migratie tussen PaaS-diensten

De PaaS-markt wordt gedomineerd door enkele aanbieders. Bij migraties tussen platform- en databasegeoriënteerde clouddiensten (PaaS) is de situatie wezenlijk anders. Hier zijn data, applicaties en onderliggende technologie vaak sterk met elkaar verweven. Overstappen betekent dan niet alleen het verplaatsen van data, maar ook het aanpassen of zelfs opnieuw ontwikkelen van applicaties. Dit maakt migraties in de praktijk complex, kostbaar en risicovol.

Daarbij vormen met name onderliggende platformdiensten, zoals databases en identity- en toegangsbeheer (IAM), extra knelpunten. (In hoofdstuk 4-8 komt dit terug bij de door experts genoemde aandachtsgebieden.) Op deze vlakken zijn data, logica en beveiliging vaak nauw geïntegreerd in leverancierspecifieke technologie, waardoor overdraagbaarheid beperkt is en migratie vaak aanvullende herinrichting vereist.

In essentie bepaalt niet het cloud-servicemodel (zoals SaaS of PaaS), maar de mate van marktwerking, standaardisatie en technische verwevenheid hoe eenvoudig migratie daadwerkelijk is; ofwel hoe portabel data of een applicatie is. Voor PaaS-diensten, of SaaS-oplossingen die sterk geïntegreerd zijn met onderliggende platformdiensten, geldt dat de portabiliteit in de praktijk vaak zeer beperkt is. Meer marktwerking jaagt meer standaardisatie en technisch ontvlechten aan.

2.7 Onderscheid tussen data-portabiliteit en applicatie-portabiliteit

Bij portabiliteit is het essentieel om onderscheid te maken tussen data-portabiliteit en applicatie-portabiliteit, conform ISO/IEC 19941. **Data-portabiliteit** gaat over het overdraagbaar maken van gegevens, terwijl **applicatie-portabiliteit** betrekking heeft op het kunnen verplaatsen van volledige software-componenten. Deze twee vormen vereisen andere standaarden en leiden tot verschillende lock-in-mechanismen, die in deze paragraaf worden uitgewerkt.

2.7.1 Data-portabiliteit

In ISO/IEC 19941 worden drie verschillende facetten van data-portabiliteit beschreven, te noemen syntactische data-portabiliteit, semantische data-portabiliteit en beleidsmatige data-portabiliteit. Deze drie facetten zijn randvoorwaardelijk om data-portabiliteit mogelijk te maken.

Facet	Vraag	Kern
Syntactisch	Kan het worden verplaatst?	Data is beschikbaar in een gangbaar, machine-leesbaar en uitwisselbaar formaat (bijv. CSV, XML, JSON), waardoor technische overdracht mogelijk is.
Metadata	Is de context bekend?	De structuur, betekenis en context van de data zijn gedocumenteerd (bijv. datamodellen, definities), zodat de data ook in een andere omgeving correct kan worden geïnterpreteerd.
Beleid	Mag het gebruikt worden?	Juridische, organisatorische en beveiligingsvoorwaarden (zoals toegang, privacy en compliance) staan hergebruik en verwerking van de data in een andere omgeving toe.

2.7.2 Applicatie-portabiliteit

In ISO/IEC 19941 worden vijf verschillende facetten van applicatie-portabiliteit voor cloud omschreven, te noemen:

1 syntactische applicatie-portabiliteit
2 instructie-applicatie-portabiliteit
3 metadata-applicatie-portabiliteit
4 gedragsmatige applicatie-portabiliteit
5 beleidsmatige applicatie-portabiliteit

Wederom moet aan al deze facetten gedacht worden als het gaat over applicatie-portabiliteit. Onderstaande worden deze facetten toegelicht, maar eerst geven we de scoping voor het onderzoek aan, en de duiding van applicatie. De onderstaande tabel worden de verschillende facetten toegelicht.

Facet	Vraag	Kern
Syntactisch	Kan het worden verplaatst?	De applicatie is zo verpakt dat deze technisch kan worden overgezet naar een andere omgeving.
Instructie	Kan het worden uitgerold?	De deployment- en configuratie-instructies kunnen ook op een andere omgeving worden uitgevoerd.
Metadata	Is de context bekend?	De beschrijving van de applicatie (zoals afhankelijkheden en structuur) kan worden meegenomen en begrepen in een andere omgeving.
Gedrag	Werkt het hetzelfde?	De applicatie werkt in de nieuwe omgeving op dezelfde manier als in de oude omgeving.
Beleid	Mag het gebruikt worden?	Regels, rechten en voorwaarden (zoals security en compliance) blijven geldig in de nieuwe omgeving.

Voor het beschrijven van applicatie-portabiliteit is het van belang of er van cloud-omgeving naar cloud-omgeving wordt gemigreerd of van non-cloud-omgeving (on premise) naar cloud-omgeving. Dit komt doordat applicaties van een non-cloud-omgeving doorgaans andersoortige afhankelijkheden hebben dan applicaties die al van een andere cloud-omgeving komen. Dit onderzoek richt zich mede daarom enkel op migratie tussen cloud-omgevingen, niet naar of van een niet-cloud-omgeving.

In bijlage C staat meer verdieping op de verschillen facetten van cloud-portabiliteit, als ook enkele praktijkcases geschetst.

3 Ontwikkelingen rond portabiliteit

In dit hoofdstuk wordt een schets gegeven van: relevante ontwikkelingen die kansen of bedreigingen veroorzaken in de context van cloud-portabiliteit, cloud-switching en cloud-standaarden. Het betreft geen volledig of uitputtend overzicht, maar een momentopname van een snel veranderend domein. Onder andere ontwikkelingen in de cloud-markt, de impact van Europese verordeningen, nationale en internationale beleidsontwikkelingen komen in dit hoofdstuk aan bod. Aan het eind van het hoofdstuk (in paragraaf 3.7) staat een samenvatting van de impact van deze ontwikkelingen en hun samenhang.

3.1 Cloud-markt

Onderstaande worden enkele cloud-markt kenmerken en trends geschetst die van invloed zijn op portabiliteit.

3.1.1 Hoge marktconcentratie vraagt om overheidsregie op cloud

De hoge mate van marktconcentratie (oligopolie) binnen de cloud-sector vormt een kritiek risico voor de keuzevrijheid en continuïteit van de digitale overheid. Een klein aantal bedrijven heeft substantiële marktmacht. Hyperscalers (AWS, Microsoft en Google) hebben gezamenlijk een wereldwijd marktaandeel van circa 65–70%, en domineren ook de Europese markt. Vrijwel 100% van de gemeenten gebruikt bijvoorbeeld de SaaS-dienst Microsoft 365 voor de werkplekken.

Bovendien is cloud geen gewone markt, want “het betreft cruciale infrastructuur en er staan publieke belangen op het spel. Toezichthouders zoals de Autoriteit Consument & Markt (ACM) waarschuwen dat dit gebrek aan concurrentie de innovatie en digitale weerbaarheid remt, wat actieve overheidssturing noodzakelijk maakt. “Actieve overheidsregie op nationaal en Europees niveau, gecombineerd met mededingingstoezicht en sectorspecifieke maatregelen, is noodzakelijk om de afhankelijkheid te verminderen.” aldus de ACM in haar publicatie (januari 2026). Cloud-portabiliteit is voor de ook één van de speerpunten voor 2026.

3.1.2 Massale keuze voor enkele cloud-leveranciers is risicovol

Het gebruik van clouddiensten binnen de Nederlandse overheid is de afgelopen jaren sterk gegroeid. In de praktijk wordt daarbij in overwegende mate gebruikgemaakt van clouddiensten van enkele grote Amerikaanse leveranciers. Dit leidt tot grote en toenemende afhankelijkheid van een beperkt aantal marktpartijen. Naast deze commerciële clouddiensten beschikt de Nederlandse overheid over een eigen infrastructuur in de vorm van vijf overheidsdatacenters (ofwel ODC’s). Deze vertegenwoordigen slechts een deel van het totale cloud-gebruik binnen de overheid.

3.1.3 Koppelverkoop en ‘sticky features’

De leveranciersafhankelijkheid wordt verder versterkt door koppelverkoop en het gebruik van zogenoemde sticky features, zo geven experts aan. Sticky features zijn leverancierspecifieke cloud-functionaliteiten die sterke afhankelijkheden creëren en overstappen bemoeilijken, zo melden experts. Organisaties nemen steeds vaker meerdere samenhangende clouddiensten en producten af van dezelfde leverancier, zoals applicatieplatformen, identity-oplossingen (bijvoorbeeld IAM) en security-diensten (zoals SOC-voorzieningen). Deze diensten zijn onderling sterk geïntegreerd en geoptimaliseerd voor gebruik binnen hetzelfde ecosysteem van één leverancier.

Hierdoor ontstaat een groeiende en structurele leveranciersafhankelijkheid op meerdere lagen tegelijk (applicatie, identity en security). Overstappen van cloud-leverancier wordt zeer complex en kostbaar, en actief ontmoedigd of vertraagd. Dit versterkt vendor-lock-in en beperkt de feitelijke portabiliteit, zelfs wanneer formeel ogenschijnlijk gebruik wordt gemaakt van open technologieën.

3.1.4 Groeiend aantal migraties naar Europese cloud-alternatieven

Hoewel de huidige cloud-markt sterk geconcentreerd is, is deze tegelijkertijd in beweging. Tegelijkertijd groeit de vraag naar Europese en soevereine cloudoplossingen snel. Experts verwachten dat het aandeel van workloads met expliciete soevereiniteitsvereisten sterk zal toenemen. Hoewel de vraag naar soevereine cloudoplossingen toeneemt, betreft dit in de praktijk vooral aanvullende eisen op bestaande clouddiensten (zoals data-lokalisatie en compliance), en niet een brede verschuiving naar volledig onafhankelijke Europese cloud-voorzieningen.

Experts geven aan dat het niet realistisch is dat op korte termijn een substantieel deel van de cloud-markt volledig soeverein wordt ingevuld. Dit gezien de huidige marktdominantie van hyperscalers en de complexiteit van migraties. De markt bevindt zich wel aan het begin van een overgangsfase, waarin afhankelijkheden blijven bestaan, zo geven experts aan. Er is een sterk groeiende behoefte aan meer controle, meer portabiliteit en meer soevereine alternatieven. Dit onderstreept het belang van open standaarden om feitelijke overstapmogelijkheden te creëren.

In de praktijk zijn inmiddels ook migratiebewegingen gaande, waarbij overheden en grote organisaties workloads (deels) verplaatsen naar:

- nationale of Europese aanbieders;
- meer ‘soevereine’ cloud-varianten van de Amerikaanse hyperscalers; en
- hybride modellen met eigen infrastructuur (waaronder de ODC’s).

Ondanks de groei blijft het marktaandeel van Europese aanbieders relatief beperkt (enkele procenten tot circa 10–15 afhankelijk van de definitie). De bestaande afhankelijkheden blijven vooralsnog groot en migraties zijn complex en traag.

3.1.5 Opkomst AI versterkt cloud-afhankelijkheden en verlaagd portabiliteit

De inzet van AI vergroot de afhankelijkheid van cloud-leveranciers. AI-ontwikkeling leunt sterk op de rekenkracht en gespecialiseerde infrastructuur van deze aanbieders, zoals ook benoemd in de DOSA en de Nederlandse Technologiestrategie (NTS). Grote aanbieders leveren AI steeds vaker als geïntegreerde platformdiensten, waardoor applicaties zowel technisch als economisch sterk verbonden raken met één cloud-omgeving.

Daarbovenop wordt de afhankelijkheid versterkt door marktdynamiek. De integratie van AI-functionaliteit binnen bredere cloud-platformen, in combinatie met koppelverkoop en dominante marktposities, leidt ertoe dat organisaties steeds meer functies bij één leverancier afnemen, waaronder leveranciersgebonden AI-modellen en bijbehorende PaaS-diensten.

Hierdoor ontstaat niet alleen technische, maar ook economische en data-gedreven lock-in. De concentratie van generatieve AI-innovatie rond een beperkt aantal grote cloud-platformen versterkt deze ontwikkeling, zo laat onder meer Brits onderzoek zien. De intelligentie van toepassingen is daardoor in de praktijk moeilijk los te koppelen van de onderliggende cloud-omgeving. Hoge kosten voor datatransport en de schaal van benodigde data vormen daarbij extra drempels. Dit leidt ertoe dat portabiliteit van AI-toepassingen in de praktijk beperkt is, zelfs wanneer deze technisch gezien mogelijk blijft.

3.1.6 Cloud stack-indeling IaaS, PaaS, SaaS wordt meer losgelaten

De klassieke cloud stack indeling in IaaS, PaaS en SaaS wordt nog vaak als referentiekader gebruikt, maar deze wordt steeds meer losgelaten. Dit heeft gevolgen voor portabiliteit. Overstappen wordt dan immers niet langer benaderd langs abstracte cloud-lagen, maar langs meer concrete clouddiensten en hun feitelijke afhankelijkheden.

Deze benadering zien we al terug bij ENISA (Cloud Computing Risk Assessment), en de Certification Scheme on Cloud Services (EUCS) die beide cloud-risico’s en verantwoordelijkheden

analyseren op basis van dienstkenmerken en verantwoordelijkheidsverdeling in plaats van service labels (‘lagen’).

Dit maakt portabiliteit inhoudelijk realistischer: lock-in ontstaat in de praktijk vooral bij geïntegreerde, managed diensten die meerdere cloud-lagen combineren, zoals managed databases, Key management, AI-diensten of geïntegreerde platforms die meerdere lagen combineren. Juist de afhankelijkheidsproblemen met die managed diensten worden beter zichtbaar wanneer de laagindeling wordt losgelaten. Dit komt ook terug in hoofdstuk 5 waarin experts de aandachtsgebieden rond cloud-portabiliteit geduid hebben.

3.2 Nederlandse beleidsontwikkelingen

Cloud-portabiliteit staat steeds explicieter in relatie tot bredere Nederlandse digitale beleidsontwikkelingen rond strategische autonomie, digitale soevereiniteit, weerbaarheid en geopolitieke afhankelijkheden. Deze paragraaf beschrijft hoe nationale beleidskaders en ontwikkelingen cloud-portabiliteit standaarden beïnvloeden.

3.2.1 Geopolitieke spanningen stimuleren ambities op cloud-soevereiniteit

Toenemende geopolitieke spanningen dwingen de overheid tot een scherpere regie op de herkomst en locatie van cloud-infrastructuren. De afhankelijkheid van buitenlandse tech-giganten wordt niet langer slechts als economisch risico gezien, maar als een directe bedreiging voor de nationale veiligheid en continuïteit van vitale processen. In een instabiel mondiaal speelveld is het beheersen van de volledige cloud-stack essentieel om te voorkomen dat data of diensten instrument worden van politieke druk of buitenlandse wetgeving (zoals de Cloud Act). Strategische autonomie is hierdoor verschoven van een economisch ideaal naar een noodzakelijke veiligheidsprioriteit voor de digitale overheid.

Gartner raamt de wereldwijde investeringen in soevereine cloudoplossingen voor 2026 op maar liefst 80 miljard dollar. Tegen 2030 zal meer dan 75% van de organisaties in EMEA hun virtuele workloads migreren naar oplossingen die geopolitiek risico moeten verminderen, een stijging ten opzichte van minder dan 5% in 2025.

3.2.2 Nationale Technologie Strategie - Open Strategische Autonomie

De Nationale Technologie Strategie (NTS) van het ministerie van Economische Zaken (EZ) benadrukt de noodzaak om afhankelijkheden van niet-Europese aanbieders (zoals Amerikaanse hyperscalers op cloud-gebied) te verminderen. Het beleid stelt dat de overheid strategischer moet kunnen sturen, onder andere via inkoop en marktontwikkeling. Er is aandacht voor het versterken van Europese ecosystemen en alternatieven. Openheid en interoperabiliteit (waaronder open standaarden) worden als belangrijk gezien. Cloud-technologie komt niet als sleuteltechnologie, maar als randvoorwaarde voor onder andere AI en data naar voren in de NTS. De NTS is indirect relevant voor cloud-portabiliteit: zij onderstreept het belang van openheid, interoperabiliteit en het verminderen van afhankelijkheden, maar bevat geen expliciete doelen of maatregelen gericht op cloud-portabiliteit of cloud-switching zelf.

De NTS en de Europese CADA versterken elkaar beleidsmatig; De NTS formuleert de nationale ambitie om afhankelijkheden te verminderen en openheid te bevorderen, terwijl de CADA dit op Europees niveau concreet ondersteunt door te investeren in soevereine cloud en AI-infrastructuur.

3.2.3 Van IT-stacks naar beleidsstacks

Het gebruik van 'stacks' transformeert het van oorsprong puur technisch IT-concept (‘lagen’) naar een instrument voor strategische beleidssturing. Door de digitale infrastructuur gelaagd te analyseren (van fysieke kabels tot applicatieniveau) krijgt de overheid grip op haar digitale autonomie. Deze methodiek, onder meer toegepast binnen de Strategische Autonomie (DOSA), maakt kritieke afhankelijkheden inzichtelijk en legt bloot waar risico’s op vendor lock-in of ongewenste buitenlandse invloed ontstaan. Hiermee fungeert de stack-benadering als het

fundament voor gerichte maatregelen die de Nederlandse en Europese soevereiniteit in een complex ecosysteem veiligstellen.

Het verlangen naar standaardisatie voor het bevorderen van cloud-portabiliteit en -interoperabiliteit wordt ook gereflecteerd in de Europese juridische kaders en beleidsinitiatieven. Zo worden er, op zowel nationaal als Europees niveau, beleidsstacks ontwikkeld. Dit zijn gelaagde beleidsmodellen die afhankelijkheden laten zien. Voorbeelden zijn het EuroStack-initiatief (zie paragraaf Bijlage D), wat is ontstaan vanuit het Europese Parlement in samenwerking met een aantal Europese tech-CEO's, of de Nederlandse PublicStack (zie Bijlage D), die de samenhang van de burger en publieke waarden met hedendaagse technologie benadrukt.

3.2.4 NDS prioriteit Cloud

Met de Nederlandse Digitaliseringsstrategie (NDS) prioriteren Rijksoverheid, provincies, gemeenten, waterschappen en publieke dienstverleners de onderwerpen waar de urgentie en impact het grootst is. In de prioriteit staan twee doelen centraal:

- het realiseren van een overheidsbrede soevereine clouddienst; en
- het ontwikkelen van een centrale overheidsmarktplaats voor clouddiensten.

Het Aanjaagteam NDS Cloud verkent deze doelen sinds 2025 via onder andere marktdialogen, en er worden stappen gezet richting een architectuur en een ontwerp van de soevereine overheidscloud.

De NDS onderstreept het belang van cloud-portabiliteit en standaarden, zonder deze nog normatief vast te leggen. De soevereine clouddienst, de bijbehorende architectuur en de cloud-marktplaats zijn hierin bepalend en worden hieronder toegelicht.

Architectuur ontwikkeling

Een belangrijke stap binnen deze NDS prioriteiten vormt het ontwikkelen van de architectuur. Deze architectuur richt zich in eerste instantie primair op IaaS en later op PaaS, met een beoogde architectuurplaat medio 2026. De ODC's en rijksbrede CIO-structuren zijn hierbij betrokken.

Deze architectuur is direct relevant voor cloud-portabiliteit, omdat zij expliciet ontwerpkeuzes raakt rond modulariteit, koppelvlakken en exit-scenario's op IaaS- en PaaS-niveau. Daarmee vormt zij een belangrijke vertaling van portabiliteit-standaarden naar de overheidspraktijk. Zij beïnvloedt de toepassing en selectie van open cloud-portabiliteit-standaarden, en steunt naar verwachting op de aanwezigheid van open standaarden voor portabiliteit op de lijsten van het Forum Standaardisatie.

Standaarden die aandacht krijgen in deze architectuur

In de architectuur die ontwikkeld wordt, krijgen standaarden zoals Haven, OCI, OpenAPI (OAS) en OpenTelemetry aandacht. Daarnaast spelen onder meer de Kubernetes-API, S3-compatibele API's voor data- en storage-portabiliteit en OIDC/OAuth2/SAML voor identity- en accessmanagement een belangrijke rol. Ook oplossingen zoals Open Policy Agent (OPA) voor policy- en governanceportabiliteit en **Infrastructure as Code** voor infrastructuur-portabiliteit maken mogelijk onderdeel uit van het (concept)architectuurontwerp.

Hoewel deze standaarden en technologieën belangrijke bouwstenen vormen voor portabiliteit, richten zij zich vooralsnog vooral op de infrastructuur- en containerlaag. De belangrijkste uitdagingen rond portabiliteit liggen echter vaak op hogere lagen (met name PaaS), zoals data, identity en applicatielogica. Zonder aanvullende standaardisatie en expliciete borging op deze lagen blijft de daadwerkelijke overdraagbaarheid van systemen beperkt.

Scenario's soevereine clouddienst

Om de soevereine clouddienst te realiseren wordt momenteel nagedacht over vier verschillende scenario's variërend van een volledig nieuwe centrale overheidscloud, modernisering van bestaande

infrastructuur, een decentraal model op basis van standaarden of een federatief/marktplaatsmodel. Deze scenario's variëren in mate van centrale regie, standaardisatie en inzet van marktpartijen.

Experts verwachten dat de huidige NDS-ontwikkelingen het sterkst aansluit bij een centraal model, waarbij standaardisatie en eigen regie voorop staan, en minder bij een marktplaats- of federatief model met meerdere aanbieders. Zij verwachten dat via een centraal model een hogere mate van soevereiniteit haalbaar is.

NDS Cloud-marktplaats krijgt lagere prioriteit – marktwerking vertraagd

Ook de centrale overheidsmarktplaats voor clouddiensten zal op de standaarden uit de architectuur moeten leunen, omdat overstappen tussen aanbieders van clouddiensten praktisch mogelijk moet zijn wil de marktplaats voldoende kunnen functioneren.

Experts geven aan dat de cloud-marktplaats momenteel niet verder wordt uitgewerkt. De focus is verschoven naar ontwikkeling van de soevereine clouddienst voor de overheid. De cloud-marktplaats heeft minder urgentie gekregen, maar blijft een toekomstbeeld.

Door deze prioriteitstelling verschuift ook de invulling van portabiliteit enigszins; Waar de marktplaats uitgaat van keuzevrijheid en concurrentie tussen cloud-aanbieders, wordt portabiliteit in de overheidsclouddienst vooral ingevuld via standaardisatie van de onderliggende architectuur (voornamelijk IaaS en deels PaaS).

Enerzijds komt het faciliteren van cloud-switching hierdoor minder centraal te staan. Anderzijds is succesvolle inzet van een soevereine clouddienst juist afhankelijk van de mogelijkheid om hiernaartoe te migreren. Bij onvoldoende portabiliteit vanuit bestaande clouddiensten ontstaat het risico dat overheden deze overstap in de praktijk niet realiseren.

In een cloud-marktplaatsmodel ontstaat vanzelf druk op portabiliteit, interoperabiliteit en open standaarden: cloud-aanbieders moeten voldoen aan open standaarden om toegang te krijgen tot de markt en overstappen tussen leveranciers mogelijk te maken. Dit stimuleert brede standaardadoptie en marktwerking.

In de huidige markt lijkt de portabiliteit en standaardisatie ook hoger naarmate de marktwerking hoger is. Deze beleidskeuze om minder prioriteit te geven aan de cloud-marktplaats heeft daarmee mogelijk negatieve impact op de marktwerking, op de cloud switches die daadwerkelijk worden gemaakt door overheden en de aantrekkelijkheid van de overheidcloud-markt voor cloud-aanbieders.

Een nieuw stopcontact helpt niet als al je huidige apparaten een andere stekker hebben. Het creëren van nieuw cloud-aanbod betekent dus ook niet dat afhankelijkheden bij bestaande clouddiensten vanzelf verdwijnen. Nieuwe alternatieven zijn waardevol, maar zolang de drempels om bestaande diensten te verlaten hoog blijven, zal overstappen in de praktijk beperkt blijven. Hier spelen Europese regelgeving en open standaarden een cruciale rol, doordat zij deze overstapdrempels kunnen verlagen en daadwerkelijke portabiliteit mogelijk maken. Nederlandse regie hierop lijkt vooralsnog beperkt.

3.2.5 NDS aanjaagteam stelt EU Cloud Sovereignty Framework voor

Op 11 mei 2026 heeft het NDS Aanjaagteam cloud het EU Cloud Sovereignty Framework voorgesteld aan het OBDO om als leidraad te hanteren. Dit Europese framework helpt om te bepalen hoeveel soevereiniteit nodig is of wordt geboden door een bepaalde cloud infrastructuur of clouddienst.

Het EU Cloud Sovereignty Framework maakt inzichtelijk dat hogere soevereiniteit samengaat met strengere eisen aan onder meer open standaarden en portabiliteit. Deze zijn immers noodzakelijk om afhankelijkheden van individuele leveranciers te minimaliseren en controle over digitale infrastructuur te behouden. Onderstaande wordt het framework op hoofdlijnen toegelicht en wordt de relatie met ISO/IEC 19941 gelegd:

Dit framework hanteert een gelaagd soevereiniteitsmodel (SEAL 0–4) om de mate van digitale autonomie van clouddiensten te beoordelen. Daarbij wordt gekeken naar juridische, technische, operationele en organisatorische aspecten.

1 Op SEAL 0 is sprake van volledige afhankelijkheid van niet-EU leveranciers.

2 Op SEAL 1 en 2 respectievelijk juridische en data-soevereiniteit deels zijn geborgd, maar nog significante afhankelijkheden bestaan.

3 Vanaf SEAL 3 ontstaat digitale veerkracht, waarbij EU-partijen de dienst grotendeels zelfstandig kunnen beheren en voortzetten.

4 Het hoogste niveau is SEAL 4 en staat voor volledige soevereiniteit, waarbij technologie, exploitatie en governance volledig onder EU-controle vallen zonder kritieke externe afhankelijkheden.

De SOV's beschrijven 8 perspectieven op soevereiniteit (van strategie tot techniek en operatie) die samen bepalen hoe onafhankelijk en controleerbaar een cloudoplossing is:

1 SOV-1 – Strategische soevereiniteit. Wie bepaalt de koers van de dienst (eigendom, bestuur, financiering)? Gericht op invloed en verankering binnen de EU.

2 SOV-2 – Juridische soevereiniteit. Onder welke wetgeving valt de dienst en kan externe toegang (bijv. via buitenlandse autoriteiten) worden afgedwongen?

3 SOV-3 – Data & AI soevereiniteit. Mate van controle over data en AI, inclusief datapositie, verwerking, en sleutelbeheer.

4 SOV-4 – Operationele soevereiniteit. Kun je de dienst zelfstandig blijven exploiteren zonder afhankelijkheid van externe (niet-EU) partijen? Kun je workloads migreren?

5 SOV-5 – Supply chain soevereiniteit. Afhankelijkheid van buitenlandse leveranciers in hardware, software en ketens.

6 SOV-6 – Technologische soevereiniteit. Mate van openheid en onafhankelijkheid van technologie (open standaarden, open source vs. proprietary).

7 SOV-7 – Beveiliging & compliance soevereiniteit. Kunnen security, audits en compliance volledig binnen EU-controle plaatsvinden? (o.a. GDPR, NIS2, DORA spelen hier een rol)

8 SOV-8 – Ecologische duurzaamheid. Autonomie en robuustheid van de dienst op lange termijn (energie, grondstoffen, duurzaamheid).

Portabiliteit, zoals bedoeld in ISO/IEC 19941, lijkt vooral een invulling van SOV-6, SOV-4 en SOV-3, omdat portabiliteit (en interoperabiliteit) noodzakelijke voorwaarden zijn voor operationele autonomie en controle over data. Exacte mapping van portabiliteit op dit soevereiniteit-framework vraagt nadere analyse.

3.2.6 ACM: "open standaarden verplicht stellen"

Volgens de ACM (april 2026) schakelen overheden en bedrijven nauwelijks over naar meer soevereine (veelal Europese) cloud-aanbieders omdat zij vastzitten in het huidige cloud-aanbod van machtige leveranciers. Die macht wordt versterkt door hoge overstapdrempels. Marktwerking en regulier mededingingstoezicht zijn volgens de ACM onvoldoende om dit te doorbreken; het probleem is een structureel coördinatieprobleem.

De hoofdeconoom van de ACM riep de overheid op om als launching customer bewust een deel van de cloudvraag Europees te beleggen. Alsook om open standaarden verplicht te stellen in aanbestedingen en vraag te bundelen op Europees niveau. Zo kan de overheid de overstapdrempels verlagen, Europese aanbieders helpen opschalen en haar onderhandelingsmacht richting hyperscalers vergroten. Digitale autonomie vraagt volgens de hoofdeconoom van de ACM om stapsgewijze, gecoördineerde beleidskeuzes en niet om afwachten op marktinitiatieven

3.2.7 *Rijksinspectie Digitale Infrastructuur vraagt aandacht voor meer autonomie*

De Rijksinspectie Digitale Infrastructuur (RDI) speelt een belangrijke rol in het versterken van de digitale weerbaarheid van Nederland. In haar aanpak wordt cloud-afhankelijkheid nadrukkelijk gezien als een strategisch risico voor continuïteit en leveringszekerheid. Cloud-portabiliteit en interoperabiliteit worden daarbij niet als doel op zich gepositioneerd, maar als middelen om risico's te beheersen, bijvoorbeeld door het mogelijk maken van exit-strategieën, fallback-scenario's en het spreiden van afhankelijkheden. Hiermee sluit de RDI-benadering aan op bredere beleidskaders zoals de Nederlandse Technologiestrategie (NTS) en Europese regelgeving, zonder zelf specifieke technische standaarden voor te schrijven.

In recente duiding (april 2026) benadrukt de RDI dat digitale autonomie niet primair draait om de locatie van de cloud, maar om de mate van controle over afhankelijkheden. Digitale weerbaarheid wordt daarmee bepaald door het vermogen van organisaties om inzicht en grip te hebben op risico's, leveranciers en ketens. Dit onderstreept het belang van portabiliteit en exitmogelijkheden als randvoorwaarde voor daadwerkelijke digitale autonomie. In lijn hiermee stelt de RDI dat een niet-Europese leverancier acceptabel kan zijn wanneer risico's beheerst worden, terwijl een Europese leverancier juist kwetsbaar kan zijn als die controle ontbreekt.

3.3 Europese verordeningen relevant voor portabiliteit

Er zijn diverse Europese verordeningen die impact hebben op cloud switching, cloud-leverancier-afhankelijkheid en portabiliteit. Eerder lag de beleidsfocus op cloud-interoperabiliteit, maar deze beweegt steeds sterker naar dwingende portabiliteit. Onderstaande wordt de EU Data Act, de Digital Markets Act (DMA), en de Cloud and AI Development Act (CADA) en Certification Scheme on Cloud Services (EUCS) behandeld.

3.3.1 *Samenhang Europese instrumenten rond cloud en portabiliteit*

Instrument	Rol
Data Act	Dwingt cloud switching en portabiliteit af via juridische verplichtingen (bijv. exit, data-portabiliteit en beperking van overstapkosten). Verwijst naar EU Standaardenregister.
Cloud and AI Development Act	Versterkt het aanbod van Europese cloud en AI-infrastructuur, zodat er daadwerkelijk alternatieven zijn om naartoe te switchen.
Digital Markets Act	Beperkt marktmacht van dominante aanbieders en kan verplichtingen opleggen die interoperabiliteit en overstapmogelijkheden versterken. Specifieke clouddiensten moeten expliciet aangewezen worden om hieronder te vallen
EU Cloud Services Certification Scheme	Borgt beveiliging en betrouwbaarheid van cloud-diensten, en vergroot vertrouwen en vergelijkbaarheid tussen aanbieders.
EU Cloud Sovereignty Framework	Geeft beleidsmatige richting voor controle en zeggenschap over cloud-gebruik en afhankelijkheden (geen direct technisch instrument).
EU Standaardenregister (Data Act repository)	Operationaliseert portabiliteit door het vastleggen van concrete standaarden waaraan cloud-aanbieders moeten voldoen.

3.3.2 *Data Act maakt portabiliteit een speerpunt*

De Data Act is grotendeels in werking en is van grote invloed op portabiliteit-standaarden. Het doel van de Data Act is om meer geprivatiseerde data beschikbaar te krijgen voor hergebruik onder eerlijke en uniforme regels. Portabiliteit en interoperabiliteit zijn speerpunten in deze verordening.

De Data Act legt regels op over het kunnen verplaatsen van zowel data als applicaties. Het bepaalt onder andere dat portabiliteit pas geslaagd is wanneer een klant een dienst kan beëindigen en bij een concurrent kan voortzetten met behoud van minimale functionaliteit en zonder uitval.

De EU Data Act maakt zo cloud-portabiliteit juridisch afdwingbaar en vraagt daarbij expliciet om de ontwikkeling van verplichtende technische standaarden die verder gaan dan data-uitwisseling en ook de operationele overstap van clouddiensten mogelijk maken. Dit dwingt tot een herwaardering van standaarden die verder gaan dan alleen communicatie; standaarden moeten de volledige operationele staat van de dienst overdraagbaar maken.

De Data Act geeft tevens mandaat dat er standaarden voor cloud-portabiliteit worden ontwikkeld die een verplichtend karakter zullen krijgen in het Europese standaardenregister. Deze standaarden worden momenteel ontwikkeld door de Europese standaardisatie-instellingen via een formeel standaardisatieverzoek M/614 (2025) (zie paragraaf 3.4 voor meer details). Daarnaast is er door de EC opdracht gegeven tot een onderzoek naar standaarden voor dit register in het kader van de Data Act. Dit onderzoek komt aan bod in paragraaf 3.4.3 en in het hoofdstuk 9 ‘Overige Standaarden’.

3.3.3 Digital Market Act heeft grote impact op cloud-portabiliteit en standaarden

De Digital Markets Act (DMA) is in werking sinds 2023 en richt zich op zogeheten gatekeepers ofwel poortwachters, binnen digitale platformmarkten. De focus ligt op platform-interoperabiliteit, niet primair op portabiliteit tussen clouddiensten. Toch is de DMA wel relevant.

Op 18 november 2025 is de Europese Commissie drie formele (markt)onderzoeken gestart onder de DMA. Twee daarvan richten zich specifiek op de clouddiensten Amazon Web Services (AWS) en Microsoft Azure. De Europese Commissie onderzoekt of deze diensten kunnen worden aangemerkt als poortwachter (‘gatekeeper’).

Hoewel de DMA formeel draait om interoperabiliteit, richt het onderzoek zich expliciet op situaties waarin interoperabiliteit tekortschiet en overstappen in de praktijk niet mogelijk is. Daarmee raakt het onderzoek direct aan cloud-portabiliteit.

Op het moment van schrijven is geen eindrapport of formele beslissing gepubliceerd. De Europese Commissie heeft aangekondigd de onderzoeken binnen twaalf maanden af te ronden. Een besluit wordt uiterlijk in november 2026 verwacht.

De DMA is al van kracht, maar verplichtingen voor clouddiensten gelden pas nadat bepaalde clouddiensten specifiek poortwachter worden aangewezen en de zes maanden implementatietermijn is verstreken.

Indien de clouddiensten AWS of Azure als poortwachters worden aangewezen, worden DMA-verplichtingen juridisch afdwingbaar. Zij zullen dan cloud switching en multi-cloud gebruik niet mogen belemmeren. Ook moeten zij dan interoperabiliteit faciliteren en oneerlijke contractuele drempels verwijderen.

Volgens analyses van de ACM en andere toezichthouders zou dit een belangrijke doorbraak betekenen in de afdwingbaarheid van cloud-portabiliteit, los van vrijwillige marktinitiatieven.

3.3.4 Cloud and AI Development Act levert mogelijk extra juridisch instrument

De Cloud and AI Development Act (CADA) bevindt zich nog in een voorbereidende fase en is op het moment van schrijven nog niet formeel gepubliceerd. De totstandkoming van het voorstel is meerdere malen uitgesteld, waardoor zowel de timing als de inhoud nog onzeker zijn.

Experts verwachten dat de Europese Commissie elementen uit bestaande initiatieven, zoals het Europees cloud-soevereiniteitskader (zie paragraaf 3.2.5 voor details), zal betrekken bij de verdere uitwerking van de CADA. Tegelijkertijd loopt er nog discussie over welke aspecten van soevereiniteit en controle passend zijn voor opname in regelgeving en welke beter via andere instrumenten kunnen worden uitgewerkt.

De CADA richt zich op het verkleinen van de achterstand van de EU ten opzichte van China en de Verenigde Staten op het gebied van cloud- en AI-infrastructuur, binnen bestaande informatiebeveiligings- en compliancekaders. Daarbij wordt ingezet op het versneld en verduurzaamd ontwikkelen van datacenters en digitale infrastructuren. Er wordt in dit kader gesproken over de dataverwerkingscapaciteit van de EU in de komende vijf tot zeven jaar te verdrievoudigen. (Deze tijdlijn staat niet in de verordening, maar is afgeleid uit beleidscommunicatie/-doelen.)

De CADA moet worden gezien als onderdeel van een bredere Europese strategie gericht op het versterken van digitale soevereiniteit. Het initiatief richt zich primair op het vergroten van het Europese aanbod van cloud- en AI-infrastructuur, onder meer door het stimuleren van investeringen in datacenters en rekenkracht. Hiermee beoogt de EU haar strategische afhankelijkheid van niet-Europese aanbieders te verkleinen en haar concurrentiepositie ten opzichte van China en de Verenigde Staten te versterken.

De nadruk van de CADA ligt daarmee op de aanbodzijde van de markt, en minder op het direct afdwingen van portabiliteit voor cloud-afnemers. Indirect kan de CADA bijdragen aan portabiliteit, doordat: 1) de beschikbaarheid van Europese alternatieven toeneemt; en 2) technische portabiliteit via (delen van) het EU soevereignty framework een vereiste kan zijn.

De CADA dient daarom in samenhang te worden gezien met andere Europese instrumenten. Waar de Data Act overstapmogelijkheden juridisch afdwingt, versterkt de CADA het aanbod van alternatieve voorzieningen, en dragen aanvullende kaders zoals het Europees cloud-soevereiniteitskader bij aan governance, controle en risicobeheersing.

Hoewel soevereiniteit een belangrijk beleidsmatig uitgangspunt vormt binnen de bredere Europese agenda, is deze in de context van de CADA vooralsnog vooral richtinggevend van aard. De nadruk ligt op het versterken van capaciteit en strategische autonomie van de markt, en minder op het direct afdwingen van controle of portabiliteit op het niveau van individuele cloudgebruikers.

3.3.5 Certification Scheme on Cloud Services werkt indirect via security (EUCS)

De European Cybersecurity Certification Scheme on Cloud Services (EUCS) bevindt zich in de eindfase van ontwikkeling. De bijdrage van de EUCS aan portabiliteit lijkt beperkt en meer indirect. De EUCS is een schema ontwikkeld door European Union Agency for Cybersecurity (ENISA) onder de European Cybersecurity Act (EUCSA). Hierna zal het tot een Europese standaard worden omgevormd, die nu als voornorm beschikbaar is onder CEN/TS 18026:2024. Het doel van de EUCS is het voorschrijven van certificeringsniveau's voor cybersecurity voor cloud services. De EUCS biedt certificeringen voor de gehele breedte van de cloud stack (SaaS, PaaS en IaaS). Cloudleveranciers kunnen een certificering bemachtigen voor één van de drie niveaus, die ze vervolgens kunnen gebruiken om te demonstreren dat ze de cloudservice die ze aanbieden voldoende veiligheid voor klanten garandeert.

De EUCS draagt niet direct bij aan cloud-portabiliteit door technische of juridische overstapverplichtingen op te leggen, maar verlaagt wél wezenlijke drempels voor overstappen door een geharmoniseerde beveiligings- en compliancebasis te creëren.

3.3.6 Digital Operational Resilience Act vereist cloud exit-strategie financiële sector

De Digital Operational Resilience Act (DORA) (Verordening (EU) 2022/2554) is sinds januari 2025 verplicht. Deze EU-verordening verplicht financiële instellingen (o.a. banken, verzekeraars) om aan te tonen dat zij ICT-verstoringen kunnen overleven.

De DORA creëert compliance standaardisatie en vraagt (eigenlijk) om cloud-portabiliteit, maar levert zelf geen technische standaarden om die portabiliteit te realiseren. Daardoor ontstaat een leemte tussen compliance-eisen van de DORA en de technische uitvoerbaarheid.

Cloud-portabiliteit komt daardoor indirect aan bod, vooral via exitstrategieën, contractuele eisen en continuïteit van dienstverlening. Drie Europese toezichthouders hebben meerdere RTS (Regulatory Technical Standards) en ITS (Implementing Technical Standards) opgesteld. Deze zijn inmiddels gepubliceerd en juridisch bindend. Er lijken weinig aanknopingspunten te zijn voor de meer technische portabiliteit standaarden die nog zijn voor cloud switching. Dus vooralsnog lijkt de DORA geen directe bron te zijn voor portabiliteit-standaarden.

In deze context is er ook het European Cloud User Coalition (ECUC); een initiatief van grote Europese banken dat gezamenlijke standaarden en best practices opstelt voor cloudproviders. Het doel is om minder afhankelijk te worden van specifieke technologiekeuzes van (niet-Europese) aanbieders. Het ligt meer op de GDPR (data protection) dan portabiliteit.

3.4 Europese en mondiale standaardisatie-initiatieven rond cloud-portabiliteit

De Europese regelgeving creëert directe vraag naar technische standaarden die cloud switching en cloud-portabiliteit praktisch uitvoerbaar maken. Dit heeft geleid tot een versneld en breed normalisatieprogramma binnen CEN, CENELEC, ETSI, en ISO/IEC. Naar verwachting van experts worden door deze initiatieven nieuwe standaarden ontwikkeld en/of voorgesteld die vervolgens verplicht kunnen worden voor cloud-aanbieders.

3.4.1 CEN-CENELEC JTC 25: Europese normontwikkeling voor cloud switching

In het kader van de Data Act heeft de Europese Commissie een formeel standaardisatieverzoek uitgezet voor interoperabiliteit en switching tussen data- en clouddiensten. Naar aanleiding hiervan is het gezamenlijke technische comité CEN-CENELEC JTC 25 - Data management, Dataspaces, Cloud and Edge opgericht in 2024. Dit comité fungeert als het centrale Europese technische vehikel voor de uitvoering van dit standaardisatiemandaat.

JTC 25 heeft als doel het ontwikkelen van Europese normen die cloud switching mogelijk maken door het wegnemen van technische en organisatorische belemmeringen. De kern van de standaardisatie-opdracht is gericht op:

- het verminderen van vendor lock-in;
- het ondersteunen van interoperabiliteit tussen data processing services (IaaS, PaaS, SaaS en edge-diensten);
- het mogelijk maken van portabiliteit van data en digitale assets tussen cloud-omgevingen;
- het aansluiten op de verplichtingen uit Hoofdstuk VI van de Data Act (artikelen 23–31);
- het bieden van een technische uitwerking, zonder nieuwe wettelijke verplichtingen te introduceren;
- het voortbouwen op bestaande internationale standaarden (zoals ISO/IEC);
- en het aanvullen van lacunes waar bestaande standaarden onvoldoende dekking bieden.

JTC 25 vormt een belangrijk Europees normalisatieplatform voor cloud-switching en portabiliteit in de context van de Data Act, en is belangrijk voor de ontwikkeling van cloud-portabiliteit standaarden. Het Forum Standaardisatie doet er goed aan om de ontwikkelingen rond JTC 25 te volgen, met name werkgroep 4 Cloud & Edge en werkgroep 2 Dataspaces:

JTC 25: Werkgroep 4 – Cloud en Edge

Binnen JTC 25 is Werkgroep 4 (Cloud & Edge) verantwoordelijk voor cloud-portabiliteit en cloud switching. Deze werkgroep ontwikkelt momenteel een Europese Technical Specification (TS) voor cloud computing – switching and interoperability in a European context. Volgens het openbare werkprogramma richt deze technische specificatie zich op:

- open interfaces en API's voor cloud switching;
- migratie van data en workloads tussen cloud-providers; en
- technische interoperabiliteitsprofielen ter ondersteuning van multi-cloudscenario's.

NEN coördineert de Nederlandse deelname en ondersteunt de Nederlandse afvaardiging, waaronder de WG4-rol.

De werkgroep ontwikkelt momenteel de Technical Specification: Cloud Computing – Switching and Interoperability in a European context. Dit document beschrijft een raamwerk voor het wisselen van cloud-leveranciers en voor interoperabiliteit tussen clouddiensten. Het raamwerk bevat concepten, aandachtspunten en praktische richtlijnen voor zowel afnemers van clouddiensten als cloud-leveranciers. Het bevat geen concrete technische portabiliteit-standaarden die in aanmerking zouden kunnen komen voor opname op de lijsten van Forum Standaardisatie.

JTC 25: Werkgroep 2 - Dataspaces en verbreding van portabiliteit

Naast werkgroep 4 is Werkgroep 2 (Dataspaces) relevant voor cloud-portabiliteit. Deze werkgroep ontwikkelt standaarden voor interoperabiliteit, governance en trust binnen datadeel-omgevingen (ofwel data spaces), waaronder afspraken over federatieve samenwerking en trusted data transactions.

Hoewel dataspaces primair gericht zijn op data-uitwisseling, raken deze activiteiten indirect aan cloud-portabiliteit: effectieve overstap tussen cloud-omgevingen vereist dat data en diensten ook na migratie binnen federatieve ecosystemen kunnen blijven functioneren.

Werkgroep 2 (Dataspaces) draagt indirect maar wezenlijk bij aan cloud-portabiliteit doordat zij waarborgt dat data en diensten na een cloud-switch hun semantiek, governance en federatieve werking behouden. Daarmee vormt werkgroep 2 een noodzakelijke aanvulling op technische cloud-portabiliteit-standaarden, door portabiliteit ook op ecosysteem- en dienstniveau uitvoerbaar te maken. Werkgroep 2 werkt direct en indirect o.a. aan:

- Behoud van databetekenis: standaarden die zorgen dat data haar semantiek en metadata behoudt na migratie, waardoor data ook ná cloud-switching bruikbaar blijft.
- Federatieve continuïteit: Dataspace-afspraken maken het mogelijk dat samenwerking tussen partijen blijft functioneren, ongeacht bij welke cloudprovider zij draaien.
- Ontkoppeling van cloud-infrastructuur: werkgroep 2 werkt zo aan scheiding tussen data-lagen en cloud-infrastructuur, wat vendor lock-in vermindert.
- Overdraagbaar vertrouwen: Standaarden voor identity, beleid en trusted data transactions maken het mogelijk om bij overstap governance en trust te behouden. (Meer over identiteit standaarden komt aan bod in hoofdstuk 7 waar experts dit thema tot aandachtsgebied hebben gedefinieerd.)
- Functionele portabiliteit: WG2 ondersteunt dat diensten na een cloud-switch blijven werken binnen ecosystemen, wat essentieel is voor 'geslaagde' portabiliteit volgens de Data Act.

3.4.2 ISO/IEC JTC 1/SC 38: Internationale cloud-standaardisatie

Op mondiaal niveau blijft ISO/IEC JTC 1/SC 38 (Cloud Computing and Distributed Platforms) het centrale forum voor cloud-standaardisatie. SC 38 werkt aan onderwerpen zoals interoperabiliteit, data- en workload-portabiliteit en multi-cloudbeheer. SC 38 heeft momenteel 33 standaarden gepubliceerd (waaronder ISO.IEC 19941:2017 en ISO/IEC 22123-1:2023), 15 standaarden in ontwikkeling[1] en circa 30 actieve deelnemende landen (waaronder Nederland).

Binnen SC 38 lopen nieuwe werkitems rond **multi-cloud** management, waaronder standaarden voor orchestratie en identity-management, die direct relevant zijn voor de probleemgebieden van portabiliteit.

JTC 25 – JTC 1 / SC 38 kruisverbanden

Opvallend is dat binnen SC 38 expliciet een samenwerkingsstructuur met CEN-CENELEC JTC 25 is ingericht, waarbij input vanuit JTC 25 wordt ingebracht in SC 38. Dit onderstreept dat Europese technische specificaties – met name rond cloud switching – in toenemende mate richtinggevend worden voor mondiale normontwikkeling. Er zijn twee JTC 1/SC 38 werkgroepen (WG 2 en WG 4) van waaruit de kruisverbanden met JTC 25 liggen:

1. Kruisverband met JTC 25 Dataspaces, Datamanagement, Cloud & Edge waar het gaat om WG 2 Dataspaces waar input van experts gevraagd is vanuit de technische commissie uit Europa aan de mondiale commissie:
    - ISO/IEC PWI 20151-2. Cloud computing and distributed platforms - Dataspaces - Part 2: Trust frameworks. WG 6
    - ISO/IEC AWI TR 25850. Information technology - Cloud computing and distributed platforms - Use cases for dataspaces. WG 6
    - ISO/IEC CD 11034.2. Information technology - Cloud computing - Trustworthiness in cloud computing. WG 5
    - ISO/IEC DIS 20151-1. Cloud computing and distributed platforms - Dataspaces -Part 1: Concepts and characteristics. WG 6
2. Kruisverband met JTC 25 Dataspaces, Datamanagement, Cloud & Edge waar het gaat om WG 4 Cloud & Edge waar input van experts gevraagd is vanuit de technische commissie uit Europa aan de mondiale commissie:
    - ISO/IEC PWI 26191. Information technology - Cloud computing and distributed platforms — Enabling AI systems on cloud computing and distributed platforms. WG 3
    - ISO/IEC DIS 19941-1. Cloud computing - Part 1: Interoperability and portability. WG 6
    - ISO/IEC PWI 19941-2. Cloud computing - Part 2: Guidelines for designing solutions to reduce switching costs of applications. WG 6

3.4.3 Study on the interoperability of data processing services – Wik Consult

Parallel aan de normontwikkeling heeft de Europese Commissie een grootschalig extern onderzoek uitgezet bij WIK-Consulting. Dit heeft de Study on the interoperability of data processing services opgeleverd in november van 2025. De resultaten dienen als input voor zowel de Data Act-standaardisatieverzoeken als het werk van JTC 25.

De studie identificeert verschillende open specificaties en standaarden die kansrijk lijken voor opname in het Europese standaardenregister, waaronder:

- API-management: OpenAPI (OAS), SECA
- Containerisatie & Orchestratie: OCI, TOSCA
- Datatransport en gegevensuitwisseling: XML, JSON

Voor relationele data noemt de studie SQL als potentiële kandidaat, maar concludeert zij dat hierover nadere analyse nodig is, onder meer vanwege verschillende versies en leveranciersspecifieke uitbreidingen. Verwacht wordt dat SQL mogelijk verder wordt onderzocht op Europees niveau.

Daarnaast zijn ook CSV en Apache Iceberg beoordeeld, maar deze zijn in de screening niet geheel geslaagd. Volgens de studie leveren deze standaarden in hun huidige vorm onvoldoende bijdrage aan de bredere eisen rond interoperabiliteit en cloud switching in de zin van de Data Act. Deze kunnen dragen bij wel enigszins bij aan portabiliteit.

De studie merkt daarbij expliciet op dat niet alle verzamelde kandidaat-standaarden al volledig zijn beoordeeld en dat voor aanvullende standaarden en specificaties verdere screening nodig is.

De bovengenoemde standaarden worden in hoofdstuk 5 tot en met 9 veder meegenomen en beoordeeld op hun relevantie voor opname op de lijsten van Forum Standaardisatie.

Methodiek: De studie heeft een tevens evaluatiemethodologie ontwikkeld die is gebaseerd op de CAMSS methode (zie paragraaf 3.4.4) en specifieke criteria die volgen uit de Data Act. Op basis van deze methodologie identificeert het onderzoek verschillende open specificaties die mogelijk in aanmerking komen voor opname in het Europese standaardenregister. Deze standaarden komen aan bod in hoofdstuk 6 en hoofdstuk 10.

3.4.4 EU CAMSS framework voor beoordeling standaarden

De EU heeft het Common Assessment Method for Standards and Specifications (CAMSS) framework ontwikkeld. CAMSS levert scenario's, beoordelingsvragen en een bibliotheek met uitgevoerde assessments die gebruikt kunnen worden bij selectie van standaarden voor architectuur en aanbesteding. CAMSS is een geharmoniseerde beoordelingsmethode voor ICT-standaarden en specificaties. Het biedt een neutrale, herbruikbare set criteria en tools om standaarden te evalueren op openheid, governance, IPR-voorwaarden en toepasbaarheid. CAMSS is ontwikkeld door en wordt onderhouden binnen EU-initiatieven (ISA² / Interoperable Europe). CAMSS is erkend als referentiemethode door EU-instanties en de Multi-Stakeholder Platform on ICT Standardisation.

CAMSS is specifiek ontworpen om standaarden scenario-gebaseerd te beoordelen op onder andere het risico op vendor lock-in. Daarmee is het mogelijk ook bruikbaar om portabiliteit te analyseren in concrete gebruikssituaties (bijvoorbeeld overstappen tussen cloudproviders, multicloud-gebruik of aanbestedingen). Mogelijk draagt CAMSS bij om inzichtelijk te maken waar een standaard cloud-portabiliteit ondersteunt of niet. CAMSS maakt die bijdrage expliciet door per scenario gerichte beoordelingsvragen te stellen. CAMSS is in dit onderzoek niet expliciet getoetst op fit en bruikbaarheid voor Forum Standaardisatie, maar de indruk is dat het relevant lijkt om dat verder te verkennen.

CAMSS kan door organisaties gebruikt worden om gebruiksscenario's systematisch door te lopen bij cloud-architectuurkeuzes en cloud-inkoop. Zo kan een beter en realistisch beeld verkregen worden van de bijdrage van standaarden aan cloud-portabiliteit (of interoperabiliteit). Het instrument kan mogelijk als aanvulling op de bestaande toetsingsprocedure van Forum Standaardisatie dienen daar waar verdieping nodig is.

3.5 Europese standaardenregister versus lijsten van Forum Standaardisatie

Het Europese standaardenregister en de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie zijn beide relevante instrumenten rond standaarden voor cloud-portabiliteit. Ze opereren op verschillende niveaus en met verschillende juridische werking:

- **Verschillen in voor wie de verplichting direct geldt:** De EU geharmoniseerde normen en common specifications onder de Data Act (het Europese standaardenregister) is gericht op marktregulering en brengt verplichtingen voor aanbieders van data processing services (waaronder cloud-aanbieders) met zich mee binnen de EU. De 'Pas toe of leg uit'-lijst is niet gericht op marktregulering, maar op inkoop en ontwikkeling door de Nederlandse overheid.
- **Verschillen in selectiecriteria voor standaarden:** Er is een verschil in beoordelingskader tussen rond het Europese standaardenregister en de 'pas toe of leg uit'-lijst van het Forum

Standaardisatie. Dit kan ertoe leiden dat standaarden die niet geschikt worden geacht voor opname in het Europese standaardenregister, wel in aanmerking komen voor opname op de 'Pas toe of leg uit'-lijst.

Een illustratief voorbeeld is ISO/IEC 19994: In de Study on the interoperability of data processing services van WIK-Consult is deze standaard niet door de screening gekomen omdat de documentatie uitsluitend tegen betaling beschikbaar is. Er wordt vereist dat standaarden royalty-free toegankelijk zijn, en wordt beschikbaarheid onder FRAND-voorwaarden als onvoldoende beschouwd.

(FRAND staat voor *Fair, Reasonable and Non-Discriminatory*: licentievoorwaarden waarbij gebruik van een standaard tegen redelijke vergoeding en zonder discriminatie wordt toegestaan (dus niet per se royalty-free), zie Regulation (EU) No 1025/2012.) De Data Act vereist het gebruik royalty-free standaarden. (In dat kader is er ook een recente rechtspraak van het Hof van Justitie (HvJ EU 5 maart 2024, C-588/21 P (ECLI:EU:C:2024:201)) dat wanneer EU-wetgeving verwijst naar geharmoniseerde normen, de inhoud daarvan vrij toegankelijk moet zijn.)

3.5.1 Wat zijn de Europese tijdslijnen rond standaarden?

Het Europese standaardenregister voor interoperabiliteit van zogenaamde *data processing services* (waaronder cloud-diensten) is juridisch voorzien in de Data Act, maar wordt op dit moment nog gevuld. Er zijn nog geen concrete, publiek vastgestelde tijdslijnen bekend voor de eerste volledige vulling van het register. De onderstaande punten zijn daarom aannames / indicatieve stappen om het verwachte proces te schetsen.

- 2024-01-11 – De Data Act is in werking getreden.
- 2025-09-12 – De Data Act is van toepassing geworden, inclusief de regels rond cloud switching en interoperabiliteit van data processing services
- 2025-07-01 – De Europese Commissie heeft het standaardisatieverzoek M/614 formeel vastgesteld als Commission Implementing Decision C(2025) 4135.
- 2025-07-07 – CEN en CENELEC hebben het standaardisatieverzoek M/614 officieel aanvaard; samen met ETSI werken zij dit verder uit, onder meer via JTC 25.
- 2025-11 / 2026-02 – De WIK-studie is opgesteld ter ondersteuning van de Europese Commissie bij het opzetten van het register en het voorbereiden van een eerste tranche open specificaties en geharmoniseerde standaarden; de studie is in november 2025 afgerond en op 23 februari 2026 gepubliceerd.
- 2026 Q3/Q4(?) – De Europese Commissie zal naar verwachting de aanbevelingen uit de WIK-studie betrekken bij de verdere vulling van het register. Het is nog niet publiek vastgesteld wanneer hierover formele besluiten worden genomen en of dit leidt tot aanvullende standaardisatieverzoeken. Experts vermoeden van wel.
- 2025–2027 (?) – In deze periode ligt het voor de hand dat tijd nodig is voor ontwikkeling, afstemming en validatie van standaarden en specificaties binnen de lopende Europese en internationale standaardisatietrajecten. De precieze doorlooptijd verschilt per standaard.
- 2027 (?) – Daarna kunnen standaarden of *common specifications* formeel worden vastgesteld, gepubliceerd en opgenomen in het centrale EU-register. Voor deze stap zijn de technische afronding en de onderliggende Europese besluitvorming bepalend.
- 2028–2029 (?) – Na plaatsing in het register geldt voor aanbieders van data processing services een implementatietermijn van 12 maanden om compatibiliteit te waarborgen. Pas na afloop van die termijn ontstaat de feitelijke verplichting voor aanbieders. Die termijn gaat lopen nadat de relevante standaard of common specification in het register is gepubliceerd én de onderliggende uitvoeringshandeling is vastgesteld.

De totale doorlooptijd per standaard blijft onzeker en is afhankelijk van het specifieke standaardisatietraject, de besluitvorming en de mate van marktvolwassenheid per standaard. Verwacht wordt (op basis van diverse aannames) dat de eerste standaarden niet eerder dan 2028 in

het Europese standaardenregister worden opgenomen en pas vanaf 2029 tot verplichtingen voor aanbieders zullen leiden.

Volgens experts is het aannemelijk dat in de eerste tranche vooral standaarden worden opgenomen die al breed geaccepteerd en toepasbaar zijn. Minder waarschijnlijk is dat juist de standaarden met de grootste potentiële impact op de kernproblemen van cloud-portabiliteit als eerste verplicht worden gesteld.

Omdat het EU-register nog in opbouw is en de eerste tranche pas na standaardisatie, publicatie en daarna nog eens 12 maanden implementatietijd effect krijgt, ligt het voor de hand dat Forum Standaardisatie niet wacht tot Europese verplichtingen ingaan. Het Forum kan in de tussentijd via de Aanbevolen-lijst, de 'Pas toe of leg uit'-lijst en eventueel streefbeeldafspraken al richting geven aan adoptie in Nederland.

3.5.2 Complementariteit en koppeling

Het Europese standaardenregister en de 'Pas toe of leg uit'-lijst van Forum Standaardisatie zijn dus twee complementaire instrumenten in het kader van cloud-portabiliteit standaarden. Afstemming tussen beide versterkt de samenhang tussen Europese verplichtingen voor cloud switching en nationale keuzes in standaardisatie, inkoop en cloud-architectuur binnen de publieke sector.

3.6 Internationale projecten rondom cloud-portabiliteit

3.6.1 Sovereign Cloud Stack

De Sovereign Cloud Stack (SCS) is een Duits initiatief dat een open-source referentie-architectuur biedt voor het inrichten en beheren van cloud-infrastructuur. SCS standaardiseert met name de infrastructuur- en operationele lagen, gebaseerd op technologieën als OpenStack (zie bijlage D) en Kubernetes. Het doel is om de cloud-stack transparant, reproduceerbaar en leveranciersonafhankelijk te maken.

In de praktijk richt SCS zich vooral op het uniformeren van de onderliggende cloud-infrastructuur. Daarmee sluit het primair aan op IaaS-vraagstukken. De bijdrage aan cloud-portabiliteit zoals in dit onderzoek gedefinieerd—dat wil zeggen: het verplaatsen van data en applicaties tussen clouddiensten—blijft beperkt. Portabiliteit speelt zich vooral af op PaaS- en SaaS-niveau en raakt data- en applicatie-portabiliteit, terwijl SCS zich concentreert op infrastructuurconsistentie.

SCS illustreert wel dat open-source tooling en uniforme orchestratielagen lock-in kunnen verminderen, maar dit ondersteunt vooral platformconsistentie binnen één stack. Het helpt niet automatisch bij het migreren van workloads tussen verschillende cloud-aanbieders, wat centraal staat in dit onderzoek. Daarom fungeert SCS vooral als architecturaal referentiepunt, maar kunnen er wel relevante cloud-standaarden in naar voren (gaan) komen.

3.6.2 Standard for Portability Across Cloud Environments (SPACE)

Het project SPACE (Standard for Portability Across Cloud Environments) ontwikkelt een open technisch raamwerk en automatiseringstools om vendor lock-in te minimaliseren en portabiliteit tussen cloud-omgevingen te garanderen. Het initiatief richt zich op technische specificaties voor architectuur, security, data-verplaatsing en API-abstracties, in aansluiting op de EU Data Act en doelstellingen rond digitale soevereiniteit. De focus ligt op herbruikbare, bij voorkeur open-source, bouwstenen voor veelvoorkomende overstap- en migratiescenario's.

Het is een project dat wordt gedreven door een consortium, maar de regie en het intellectuele startpunt liggen bij de private organisatie genaamd Data Éclosion. Dit sluit niet per se de relevantie van het initiatief uit voor de lijsten van open standaarden. Het is immers redelijk gangbaar hoe veel moderne standaarden beginnen: een privaat initiatief dat via een consortium naar een brede, open community-standaard groeit. De standaarden worden momenteel uitgewerkt. SPACE moet op dit moment dus worden beschouwd als een markt consortium-initiatief. Tastbaarheden moeten nog

worden vrijgegeven. Mogelijk ontstaan er in de toekomst wel nieuwe portabiliteit-standaarden vanuit SPACE.

3.6.3 CISPE Data Portability Initiative – toetsingskader voor portabiliteit

Het Cloud Infrastructure Services Providers in Europe (CISPE) Data Portability Initiative vertaalt de abstracte eisen van de Data Act Eisen naar een Cloud Switching Framework (toetsingskader), waarmee het bijdraagt aan het verminderen van vendor lock-in. De focus van CISPE ligt op IaaS. CIPSE wil fungeren als een praktische brug tussen Europese wetgeving (waaronder de Data Act) en de technische implementatie van cloud-portabiliteit. CISPE is een Europese brancheverenigingzonder winstoogmerk. Hoewel het een vorm van zelfregulering is, biedt het een toetsingskader voor de interoperabiliteit en portabiliteit van clouddiensten, wat publieke organisaties mogelijk kan helpen bij aanbestedingen.

3.6.4 SWIPO

SWIPO (Switching Cloud Providers and Porting Data) ontwikkelde in opdracht en onder facilitering van de Europese Commissie gedragscodes voor cloud switching en data-portabiliteit in het kader van Regulation (EU) 2018/1807 - Free Flow of Non-Personal Data Regulation (FFDR). Deze codes zijn vormgegeven als vrijwillige “codes of conduct” en richten zich primair op contractuele en organisatorische afspraken tussen cloudproviders en afnemers over exit-regelingen, data-export en migratieondersteuning. SWIPO heeft daarmee vooral een betekenis als ‘soft-law’ instrument dat de praktijk van cloud switching structureert en transparantie in exit-processen vergroot. De codes bevatten geen technische specificaties. Enkele experts stellen vraagtekens bij de onafhankelijkheid van non EU cloud-aanbieders rond SWIPO. In het kader van open standaarden voor cloud-portabiliteit is SWIPO daarom vooral minder relevant, maar mogelijk wel bij cloud switching.

3.6.5 De facto standaardisatie organen voor cloud

Naast formele standaardisatieorganisaties vormen internationale consortia (zoals W3C, IETF of OASIS) voor standaarden-ontwikkeling rond onder andere cloud. Ook open-source samenwerkingen, platformen en communities een belangrijke bron voor standaardisatie. Organisaties zoals de Cloud Native Computing Foundation (CNCF) (bijvoorbeeld Kubernetes), de Linux Foundation (onder andere OCI) en de Eclipse Foundation ontwikkelen specificaties en technologieën die breed worden toegepast in de praktijk. Deze functioneren vaak als de facto standaardisatieorganen, waarbij standaarden niet primair via formele procedures ontstaan, maar via brede adoptie en gebruik. Daarmee spelen zij een cruciale rol in de ontwikkeling van cloud-standaarden, al sluiten zij niet altijd direct aan op de formele criteria voor open standaarden zoals gehanteerd door bijvoorbeeld het Forum Standaardisatie.

3.7 Kernbevindingen rond ontwikkelingen

Deze paragraaf vat de belangrijkste bevindingen samen uit de analyse van de ontwikkelingen rond cloud-portabiliteit.

- **Cloud-portabiliteit verschuift van een primair technisch vraagstuk naar een beleidsmatig en strategisch thema, als randvoorwaarde voor meer soevereiniteit en autonomie.**
- **Verbeteren van cloud-portabiliteit is een noodzakelijke randvoorwaarde voor digitale soevereiniteit, effectieve marktwerking en het verminderen van cloud-leveranciersafhankelijkheid.** Ontwikkelingen rond cloud-portabiliteit spelen zich af tegen de achtergrond van een (op sommige terreinen) sterk geconcentreerde cloud-markt, waarin de afhankelijkheid van enkele leveranciers hoog is. Die afhankelijkheid wordt verder versterkt door zogenoemde ‘sticky features’; geïntegreerde diensten en koppelverkoop. Overstappen van cloud-leverancier blijft daarom complex en kostbaar.

- **Europese regelgeving maakt portabiliteit in toenemende mate afdwingbaar. De praktische uitvoerbaarheid daarvan blijft echter sterk afhankelijk van de beschikbaarheid en toepassing van open standaarden die nog achterblijft.**
- De Europese verordeningen markeren een duidelijke verschuiving van interoperabiliteit en vrijwilligheid, naar afdwingbare portabiliteit. Er ontstaat steeds meer spanning tussen beleidsambities, zoals digitale soevereiniteit, en de technische haalbaarheid van portabiliteit in de praktijk. Europese en nationale beleidsinitiatieven versterken de vraag naar portabiliteit, maar bevatten nog beperkte concrete technische uitwerking. De verordeningen lossen portabiliteit dus niet zonder meer op, maar vragen juist om meer open standaarden.
- **Dit benadrukt het belang van actieve regie door het Forum Standaardisatie op de selectie, verplichtstelling en toepassing van open standaarden voor overheidsinkoop en ontwikkeling**. Tevens zijn open standaarden voor portabiliteit van belang in de vormgeving van de NDS-prioriteiten soevereine clouddienst en een overheid cloud-marktplaats.
- **Het Europese standaardenregister ontwikkelt zich tot het normstellende kader voor leveranciers voor cloud-portabiliteit**. Het register is een aanvulling op de ‘Pas toe of leg uit’-lijst; het is een potentiële bron voor relevante open standaarden, maar geen vervanging. Dit biedt het Forum Standaardisatie ruimte om een proactieve rol te vervullen. In plaats van te wachten totdat standaarden volledig zijn uitgekristalliseerd en formeel worden opgenomen in het Europese register, kan zij ervoor kiezen om de adoptie van kansrijke, opkomende standaarden actief te stimuleren door deze vroegtijdig op de lijst te plaatsen
- **Het is onduidelijk welke tijdslijnen verwacht kunnen worden bij de internationale ontwikkeling van standaarden en verplichtstelling hiervan.** Per standaard kan de doorlooptijd vanaf het standaardisatiemandaat, de oplevering, en de plaatsing op Europees register wisselen. Daarnaast kent de verplichtstelling via het Forum Standaardisatie en OBDO nog een eigen tijdslijn. Daarnaast ontstaat er vanuit NDS architectuurontwikkeling en internationale communities mogelijk ook standaardisatie. Overzicht en regie zijn belangrijk, om de juist afwegingen te maken tussen aanjagen en afwachten.
- **De Europese Unie stuurt voor standaarden primair via standaardisatieverzoeken, waarbij de technische uitwerking wordt belegd bij normalisatieorganisaties.** Binnen deze context richt opdrachtnemer CEN/CENELEC JTC25 zich op cloud switching en operationaliseerbare portabiliteit. Daarnaast blijft ISO/IEC JTC1/SC38 aanvullend relevant. Er liggen relevante kruisverbanden tussen standaardisatie-initiatieven. De verwachting is dat er aanvullende standaardisatie-verzoeken zullen komen die ook aan cloud-portabiliteit raken. Deze gremia en NEN zijn relevante bronnen om goed aangehaakt te blijven op internationale ontwikkelingen rond standaarden voor cloud-portabiliteit.
- **Tijdslijnen voor Europese standaarden-ontwikkeling zijn moeilijk in te schatten, maar het is niet nodig om op de EU-standaarden te wachten.** Er zijn standaarden nu in ontwikkeling. Het is echter onduidelijk wanneer deze gereed zijn voor opname op nationale lijsten van Forum Standaardisatie of voor verplichtstelling via het Europese standaardenregister. Experts achten de kans klein dat binnen twee jaar volledig uitgekristalliseerde en breed verplichte standaarden beschikbaar zijn.
- **Binnen Nederland verandert de NDS prioriteitsverschuiving naar de ontwikkeling van een soevereine overheidscloud de stimulans voor open standaarden.** Waar een marktplaatsmodel inzet op marktwerking en interoperabiliteit, verschuift de nadruk nu naar architectuur en standaardisatie binnen één centraal model. Dit vergroot het risico op stack lock-in, waarbij afhankelijkheid verschuift van individuele leveranciers naar een dominant technologisch ecosysteem. Tegelijkertijd biedt centrale regie ook kansen om open standaarden expliciet af te dwingen en adoptie binnen de overheid te versnellen.

- **Zonder substantiële verbetering van data- en applicatie-portabiliteit tussen clouddiensten, bestaat het risico dat zowel de soevereine overheidscloud als Europese cloud-alternatieven onvoldoende worden benut.** De ambitie om tot een cloud-marktplaats te komen op termijn, staat ook onder druk. Portabiliteit vormt daarmee een randvoorwaarde voor het realiseren van digitale soevereiniteit in de praktijk.

4 Identificatie van aandachtsgebieden rond portabiliteit en standaarden

In dit hoofdstuk wordt de aanpak beschreven om te komen tot relevante cloud-portabiliteit-standaarden die mogelijk in aanmerking komen voor opname op de lijsten van Forum Standaardisatie.

4.1 Aanpak inventarisatie en analyse standaarden

De aanpak om standaarden te inventariseren en analyseren bestond uit drie stappen:

- Stap 1: Inventarisatie en longlist uit interviews en deskresearch
- Stap 2: Validatie bevindingen en duiding aandachtsgebieden met experts
- Stap 3: Verdieping op aandachtsgebieden met deskresearch en interviews

Deze stappen worden onderstaand toegelicht:

Stap 1: Inventarisatie en longlist. Hiervoor is een longlist (zie bijlage E) opgesteld van potentiële standaarden die relevant zijn voor de portabiliteit van data en applicaties tussen clouddiensten. Deze longlist is gebaseerd op interviews met stakeholders, experts en deskresearch. De geïdentificeerde standaarden zijn grofweg geordend naar cloud-stack laag en focusgebied.

De lijst is heterogeen van aard. De lijst bevat uiteenlopende typen items, variërend van internationale normen (gericht op definities en begrippen), open standaarden (waaronder standaarden op de ‘pas toe of leg uit’-lijst), tot open-source tooling, platformen, leverancier-specifieke oplossingen, methodieken en beschrijvingstalen.

Gedurende het onderzoeksproces is gebleken dat er aanzienlijke onduidelijkheid en interpretatieverschillen bestaan rond kernbegrippen zoals cloud en portabiliteit van data en applicaties, en de definitie en afbakening van (open) standaarden.

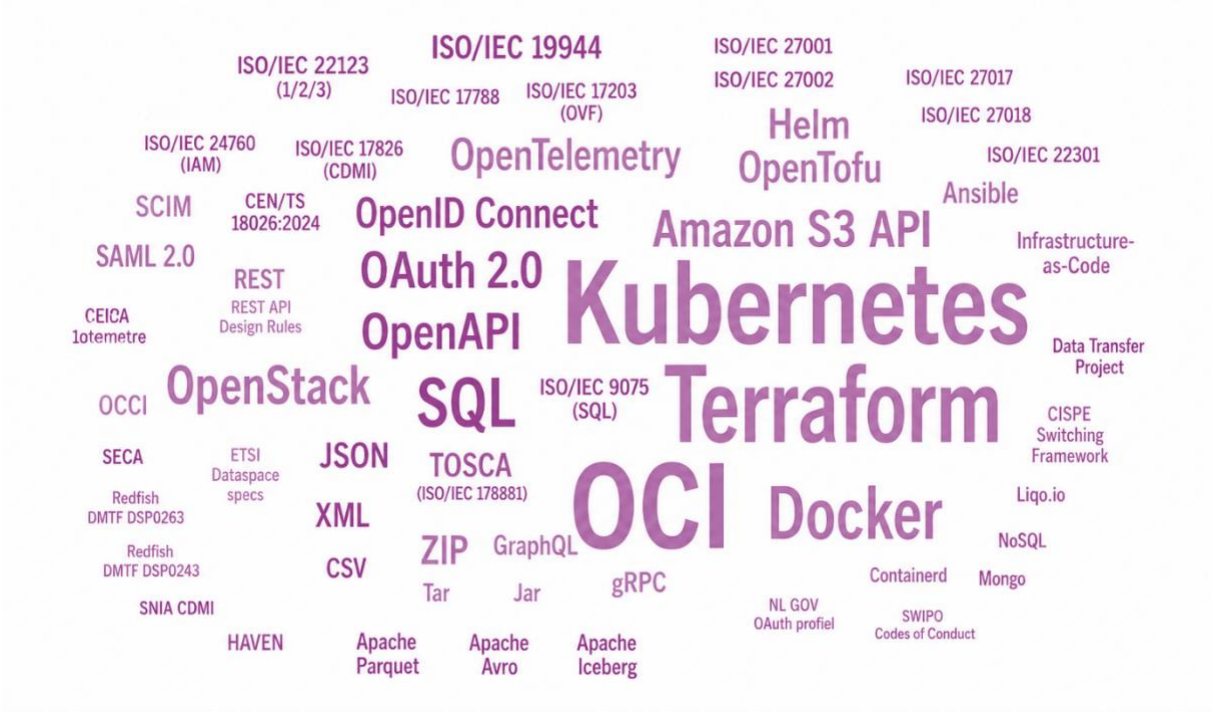
Daarnaast valt op dat de longlist relatief sterk is vertegenwoordigd door standaarden en technologieën in het PaaS-domein. SaaS-gerelateerde standaarden zijn beperkter aanwezig. Diverse items zijn niet specifiek voor cloudservice type of laag (ze zijn dwarsdoorsnijdend van aard).

Stap 2: Validatie bevindingen en duiding aandachtspunten met experts. Vervolgens zijn de tussentijdse bevindingen en geïdentificeerde aandachtspunten gevalideerd, aangescherpt en aangevuld in een expertsessie met betrokken deskundigen (zie bijlage A, paragraaf A.2).

Stap 3: Verdieping: In de daaropvolgende fase is aanvullend en verdiepend deskresearch uitgevoerd, specifiek gericht op de geïdentificeerde aandachtspunten en zijn enkele aanvullende interviews afgenomen. Per aandachtsgebied zijn de relevante standaarden op de lijsten van het Forum Standaardisatie in kaart gebracht, evenals de geïdentificeerde “witte vlekken”. Vervolgens zijn standaarden en initiatieven geïdentificeerd die mogelijk bijdragen aan het invullen van deze hiaten. Daarbij is tevens gekeken naar relevante (internationale) ontwikkelingen die in hoofdstuk 3 aan bod zijn gekomen binnen de betreffende aandachtsgebieden.

4.2 Longlist

Experts benoemden tijdens de interviews over cloud-portabiliteit een breed spectrum aan standaarden, specificaties, implementaties en cloud-native technologieën. De dominantie van implementaties en de facto standaarden illustreert dat portabiliteit in de praktijk vaak meer wordt gestuurd door ecosystemen en tooling dan door formele open standaarden.



Figuur 3 Woordwolk ter illustratie van de grote diversiteit van items op de longlist in bijlage E

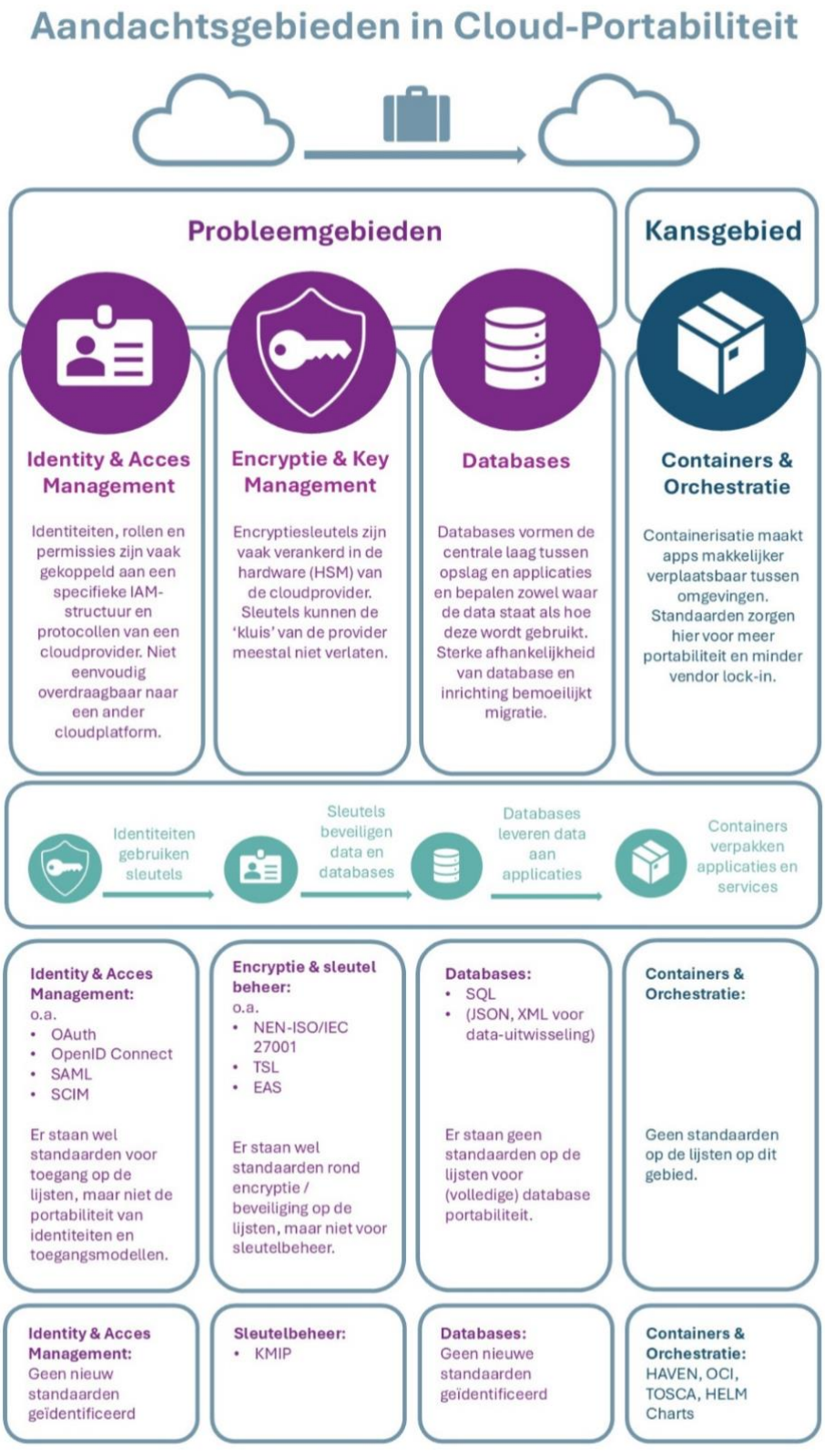
In bijlage E staat een tabel met items van de longlist opgenomen. De bovenstaande figuur geeft daar een grafische weergave van ter illustratie van de diversiteit aan items.

4.3 Door experts benoemde aandachtsgebieden in cloud-portabiliteit

Experts hebben tijdens de expertsessie de volgende aandachtsgebieden benoemd rond cloud-portabiliteit:

- **Identity & Access Management**: Identiteitsbeheer fungeert als een digitale paspoortcontrole. Omdat IAM-rollen en permissies vaak gebonden zijn aan de specifieke hiërarchie en protocollen van een cloud-leverancier, zijn deze rechten niet direct overdraagbaar naar een concurrerend platform.
- **Cryptografie & sleutelbeheer:** Beveiligingssleutels voor encryptie zijn vaak verankerd in de hardware (HSM) van de provider. Deze sleutels kunnen de "kluis" van de oorspronkelijke provider doorgaans niet verlaten, waardoor versleutelde data op een nieuwe locatie ontoegankelijk blijft zonder complexe migratiestrategieën.
- **Databases:** Databases vormen een centrale laag tussen opslag en applicaties, en voeren bewerkingen uit op data. Door deze combinatie bepalen databases niet alleen waar data staat, maar ook hoe data wordt gebruikt binnen een systeem. Hierdoor zijn applicaties vaak sterk afhankelijk van de gekozen database en de manier waarop deze is ingericht. Dit levert problemen op bij cloud-migraties.
- Naast de bovengenoemde aandachtpunten, vormt het domein **containerisatie & orchestratie** juist een gebied wat kansrijk is voor portabiliteit-standaarden.

Daarnaast zijn **cybersecurity en informatiebeveiligingsstandaarden** belangrijk en randvoorwaardelijk. In het kader van portabiliteit van data en applicaties zijn beveiligingsstandaarden echter niet als primair aandachtspunt bij cloud switching geduid tijdens de expertsessie. In hoofdstuk 9 komen deze nader aan bod.



Figuur 4 Visuele weergave van de aandachtsgebieden

De onderstaande tabel geeft weer waar elk aandachtsgebied zich bevindt in de verschillende Cloud Service Modellen. Dit geeft weer dat de belangrijkste knelpunten zich niet per se houden aan de indeling van servicemodellen IaaS, PaaS en SaaS.

Aandachtsgebied	Cloud Service Model
Containers & Orchestratie	Infrastructure-as-a-Service / Platform as a Service (afhankelijk van implementatie)
Encryptie- & sleutelbeheer	Dwarsdoorsnijdend (securityfunctie over alle lagen, vaak als PaaS)
Identity & Acces Management	Dwarsdoorsnijdend (identity- en toegangslaag, vaak als PaaS)
Databases	Platform as a Service

5 Aandachtsgebied 1: Containers en orchestratie

Tijdens de expertsessie is het domein ‘containers & orchestratie’ als aandachtsgebied aangewezen door experts. Zij geven aan dat portabiliteit-kansen zich juist voordoen in dit domein en dat er tevens kansen voor standaardisatie kunnen zijn.

Containerisatie is een manier om een applicatie samen met alles wat die nodig heeft (zoals instellingen en software) in één “pakketje” te zetten, zodat die overal hetzelfde kan draaien. Orchestratie zorgt ervoor dat al die pakketjes automatisch worden gestart, verdeeld en beheerd over meerdere systemen, zodat alles goed blijft werken en kan opschalen als dat nodig is.

Containerisatie heeft de portabiliteit van applicaties binnen cloud-omgevingen aantoonbaar verbeterd, maar lost die problemen in de aandachtsgebieden van hoofdstuk 6, 7 en 8 niet op. De huidige standaardisatiebasis (met name OCI, Kubernetes en aanverwante ecosystemen) is sterk op applicatie- en infrastructuurniveau. Het domein containers brengt daarmee ook vraagstukken naar voren over wat voor type items zich wel en niet lenen als open standaard; er is grijs gebied, zoals in dit hoofdstuk nader staat toegelicht.

5.1 Wat zijn containers?

Containerisatie is een technologie- en platformparadigma waarbij applicaties worden verpakt in gestandaardiseerde, geïsoleerde eenheden (containers) die onafhankelijk van onderliggende infrastructuur kunnen worden uitgevoerd. Het vormt de basis voor cloud-native architecturen. Containerisatie vermindert de afhankelijkheid van specifieke cloud-infrastructuur.

5.2 Containerisatie & portabiliteit

Containerisatie kan binnen het cloud-domein worden gezien als een relatief succesvol voorbeeld van portabiliteit. Het vermindert de afhankelijkheid van specifieke infrastructuur en maakt reproduceerbare uitvoeringen mogelijk over schillende cloudomgevingen (als ook naar on-premise infrastructuur).

5.3 Huidige lijsten van open standaarden en witte vlekken

Op de lijsten van Forum Standaardisatie staan geen open standaarden direct gericht op cloud containerisatie en de portabiliteit van de applicaties in die containers. Het ontbreekt aan open standaarden rond containerisatie van cloud-native platformcomponenten zoals container-orchestratie, containerformaten en workload-portabiliteit.

5.4 Welke standaarden zouden hiervoor invulling aan kunnen geven?

In het onderzoek zijn Kubernetes, HAVEN, OCI, TOSCA en Helm charts naar voren gekomen aan relevante standaarden rond containerisatie. Deze standaarden worden onderstaande nader toegelicht.

5.4.1 Kubernetes

Beschrijving: Kubernetes is een open-source containerorchestratieplatform dat functioneert wereldwijd als dé facto standaard voor het beheren van containerized workloads. Het biedt een gestandaardiseerde API en een breed ecosysteem.
Beheer: De specificatie en governance liggen bij een open-source gemeenschap en niet bij een formele standaardisatieorganisatie.

Cloud stack laag: primair Platform as a Service (PaaS), secundair: raakt IaaS (stuurt infrastructuur aan)
Formele status: geen formele status
Nederlandse betrokkenheid: onbekend
Adoptie en draagvlak: Internationaal en nationaal hoog; Kubernetes is de industriestandaard.

5.4.2 Open Container Initiative (OCI)

Omschrijving: Het Open Container Initiative (OCI) is een open governanceproject dat specificaties ontwikkelt voor containerimages, container runtimes en distributie. De OCI Image, Runtime en Distribution specifications definiëren een gestandaardiseerd formaat en uitvoeringsmodel voor containers, zodat containerimages consistent en overdraagbaar zijn tussen verschillende containerplatformen. De meest relevante technische specificaties van OCI zijn: OCI Image Specification, OCI Runtime Specification en OCI Distribution Specification.
Bijdrage aan portabiliteit: In combinatie met Kubernetes als de facto orchestratiestandaard ontstaat een gangbaar ecosysteem voor applicatie-portabiliteit.
Beheerorganisatie: OCI hangt onder de Linux Foundation.
Open beheer: Ja. OCI kent een open governance-model met brede wereldwijde deelname van leveranciers en gebruikers. De specificaties worden publiek ontwikkeld en zijn vrij implementeerbaar. Het heeft een vendor-neutraal governance model met brede industriële deelname.
Functioneel toepassingsgebied: Standaardisatie van containerimages, runtime-gedrag en distributie voor interoperabele containeruitvoering.
Bijdrage aan portabiliteit: OCI ondersteunt applicatie-portabiliteit door een gestandaardiseerd containerformaat en runtime-gedrag te definiëren. Hierdoor kunnen containerimages onafhankelijk van onderliggende infrastructuur worden uitgevoerd. De bijdrage is beperkt tot de container- en applicatiepakket-laag; data-, platform- en service-portabiliteit vallen buiten scope. Het ondersteunt geen data-, service- of platform-portabiliteit. Beperkt tot containerformaten en runtimes; geen ondersteuning voor applicatiemodellering, data-portabiliteit of platformdiensten.
Cloud stack laag: IaaS / PaaS (tussen infrastructuur en platform)
Formele status: Geen
Adoptie en draagvlak: Internationaal en nationaal hoog.

5.4.3 Haven

Omschrijving: Haven schrijft een specifieke configuratie voor van Kubernetes. Het definieert een uniforme set van infrastructuurcomponenten, deployment-patronen en configuratiestandaarden. Haven fungeert zo als een generieke laag die past binnen de diversiteit van IT-systemen. Deze laag maakt de verbinding tussen ontwikkelde applicaties en de infrastructuur (IaaS of on premise) die organisaties gebruiken. Hiermee zijn applicaties niet meer afhankelijk van één IT-infrastructuur. Applicaties kunnen overal gehost worden zonder ze aan te moeten passen aan de specifieke infrastructuur waarop ze moeten draaien. De Haven standaard bestaat momenteel uit 15 verplichte en 2 voorgestelde checks. Haven+ is een doorontwikkeling van Haven, waarbij de nadruk sterker ligt op praktische implementatie, opschaling en aansluiting op concrete overheidsomgevingen.
Bijdrage aan portabiliteit: Haven draagt bij aan platform-onafhankelijke cloud-infrastructuur. Een applicatie of website die op één Haven omgeving werkt, is herbruikbaar op alle Haven-omgevingen. Met Haven maakt het niet uit welke cloud- of on-premise oplossing er wordt gebruikt. Ook kan er

technisch gezien eenvoudig van leverancier worden veranderd. Migraties zijn veel simpeler. Haven heft de onderliggende verschillen in technische infrastructuur op. Haven standaardiseert niet het applicatiemodel zelf, maar het gebruik van onderliggende cloud-native technologieën. Daardoor ontstaat meer portabiliteit binnen het Haven-ecosysteem (migraties van de ene naar de andere Haven-omgeving).
Cloud stack laag: primair op de PaaS / container orchestratie-laag, boven infrastructuurdiensten (IaaS).
Beheerorganisatie: Vereniging van Nederlandse Gemeenten (VNG)
Open beheer: Ja. Haven kent een open, sectorale beheerstructuur onder regie van de VNG, waarbij gemeenten en enkele andere publieke organisaties betrokken zijn bij de ontwikkeling en toepassing.
Formele status: Haven is een VNG standaard voor platform-onafhankelijke cloud hosting. Het bestuur van de VNG heeft Haven op 25 maart 2022 tot standaard verklaard waarmee het de 'pas-toe-of-leg-uit'-status nu heeft.
Nederlandse betrokkenheid: Hoog.
Adoptie en draagvlak: Hoog. Haven wordt toegepast binnen een groeiend aantal Nederlandse gemeenten. Het is echter geen breed internationaal geadopteerde standaard. Haven kent referentie-implementaties van diverse toonaangevende leveranciers. Adoptie in de leveranciersmarkt is hoog alsook onder ODC Noord, Logius en DICTU.

5.4.4 TOSCA

Omschrijving: Topology and Orchestration Specification for Cloud Applications (TOSCA) is een standaard die een modelgedreven methode definieert voor het beschrijven van cloudapplicaties, inclusief hun componenten, afhankelijkheden en deployment- en orchestratieprocessen. De standaard scheidt applicatiemodel en infrastructuur-implementatie om platformonafhankelijke applicatiebeschrijvingen mogelijk te maken.
Bijdrage aan portabiliteit: TOSCA draagt bij aan portabiliteit door applicaties en hun deployment-logica onafhankelijk van specifieke cloud-leveranciers te modelleren. Hierdoor kan dezelfde applicatiebeschrijving in principe worden hergebruikt in verschillende cloud-omgevingen zonder volledige herimplementatie. De bijdrage van TOSCA is primair gericht op applicatie-portabiliteit en in beperkte mate op service-portabiliteit via expliciete modellering van afhankelijkheden en orchestratie.
Cloud stack laag: Primair op de PaaS-laag, als model- en orchestratielaag boven infrastructuurdiensten (IaaS).
Beheerorganisatie: OASIS (Organization for the Advancement of Structured Information Standards)
Open beheer: Ja. TOSCA wordt ontwikkeld binnen een open, multi-stakeholder standaardisatieproces met deelname van leveranciers en andere partijen.
Formele status: Internationale open standaard (OASIS Standard).
Functioneel toepassingsgebied: Modelgedreven beschrijving van cloudapplicaties, inclusief componenten, relaties, deployment- en orchestratieregels, ten behoeve van platformonafhankelijke applicatie-uitrol en lifecycle management.
Nederlandse betrokkenheid: Beperkt zichtbaar in directe standaardisatiebijdragen; toepassing in Nederland is voornamelijk experimenteel of academisch en niet breed ingebed in overheidscloudarchitecturen.

Adoptie en draagvlak: Internationaal erkend als formele OASIS-standaard, maar beperkte adoptie in cloud-native ecosystemen en beperkte ondersteuning door hyperscale cloud-leveranciers.

5.4.5 Helm charts

Omschrijving: Helm charts zijn een declaratieve configuratiespecificatie (in YAML-vorm) die in de open source tool Helm worden gebruikt. Ze beschrijven op een gestandaardiseerde manier hoe een applicatie opgebouwd is en hoe deze moet worden geïnstalleerd in een cloud-omgeving. Ze werken als een soort “recept” waarmee een applicatie inclusief alle onderdelen kan worden uitgerold. Toepassingsgebied: Beschrijven, installeren en beheren van applicaties in cloud-omgevingen
Bijdrage aan portabiliteit: Helm charts maken het mogelijk om dezelfde applicatie op een consistente manier te installeren in verschillende cloud-omgevingen. Hierdoor wordt het eenvoudiger om applicaties tussen omgevingen te verplaatsen. De bijdrage is vooral beperkt tot de manier van installeren; data, gebruikers en beveiliging worden niet automatisch meegenomen
Cloud stack laag: Platformlaag (PaaS), dicht bij de applicatie (deployment en orchestratielaag), met raakvlak naar de applicatielaag.
Beheerorganisatie: Cloud Native Computing Foundation (CNCF)
Open beheer: Ja. Helm wordt ontwikkeld binnen een open governance-model onder CNCF, met brede internationale bijdrage van leveranciers en gebruikers.
Formele status: Geen.
Nederlandse betrokkenheid: Niet specifiek zichtbaar op standaardisatieniveau; gebruik lijkt indirect hoog via Kubernetes-gebruik binnen overheid en markt.
Adoptie en draagvlak: Internationaal en nationaal hoog; Helm is de facto standaard voor packaging en deployment binnen Kubernetes-ecosysteem.
Conclusie: Helm charts zijn belangrijk in de praktijk voor portabiliteit, maar geen officiële standaard. Helm charts zijn nauw verbonden aan de open source tool Helm. Ook zijn Helm charts nauw verbonden aan het technologisch ecosysteem Kubernetes.

5.5 Container-tools en -platformen

Experts hebben meermaals diverse tools en platformen voor containerisatie genoemd als dé facto standaarden. Kubernetes en de OC-specificaties vormen vaak de basis van deze (open) tools/platformen. Met het veelgebruikte Docker en daarnaast Podman worden containers verpakt. Het is de "industrie-standaard" voor het werken met containers. CRI-O is een lichtgewicht alternatief dat specifiek is gebouwd voor Kubernetes. Containerd was oorspronkelijk onderdeel van Docker, maar nu een onafhankelijk project. Het is de standaardmotor voor de meeste moderne Kubernetes-omgevingen. Dergelijke tools/platformen gebruiken vaak de OCI-specificaties als standaard. Binnen dit ecosysteem speelt de tool Helm een belangrijke rol voor declaratief deployment. Helm maakt het mogelijk om applicaties en hun afhankelijkheden gestandaardiseerd te verpakken en uit te rollen binnen Kubernetes-omgevingen. Opname van dergelijke tools op de lijsten van Forum Standaardisatie lijkt minder voor de hand te liggen.

Daarnaast is er een nieuwe norm bij ISO/IEC JTC1/SC38 in ontwikkeling rond orchestratie.

5.6 Conclusie containers

Containerisatie draagt bij aan de portabiliteit van applicaties. Het is daarom van belang containerisatie te richten op open standaarden: hoe beter gestandaardiseerd, hoe hoger de

portabiliteit en hoe lager de overstapdrempels voor organisaties. **Het domein containerisatie is kansrijk voor verdere standaardisatie.**

Binnen dit domein zijn verschillende standaarden en technologieën geïdentificeerd die mogelijk invulling kunnen geven aan de witte vlekken op de lijsten van Forum Standaardisatie. In de praktijk vormen OCI, Kubernetes, Helm (Charts) en TOSCA samen een ecosysteem voor applicatie-portabiliteit op infrastructuur- en platformniveau. Echter lijken dat niet al deze oplossingen zich zonder meer lenen voor opname als open standaard op de lijsten van Forum Standaardisatie.

- Kubernetes is een technisch platform voor containerorchestratie; Haven is daarvan een implementatie- en configuratiestandaard die binnen Nederlandse gemeenten een uniforme inrichting voorschrijft en daarmee portabiliteit binnen dat ecosysteem vergroot.
- OCI bestaat uit drie technische specificaties (OCI Image, OCI Runtime en OCI Distribution) en vormt een geschikte kandidaat voor opname als open standaard, doordat het containerformaten en uitvoering vendor-neutraal standaardiseert.
- Helm is een open-source tool en daarmee minder geschikt voor opname als open standaard; de onderliggende Helm charts functioneren echter als een declaratieve specificatie en mogelijke standaard.
- TOSCA is een formele OASIS-standaard voor het modelleren van applicaties en hun afhankelijkheden en lijkt daarmee geschikt als open standaard, ondanks de beperkte adoptie.

5.6.1 Grijs gebied

Wat uit deze analyse naar voren komt, is dat het domein containerisatie zich bevindt in een grijs gebied tussen open standaarden, technologieën en implementaties. In de praktijk dragen juist de combinatie van tools, platforms en (de facto) specificaties het meest bij aan portabiliteit, terwijl het toetsingskader van Forum Standaardisatie primair is gericht op formele, stabiele en vendor-onafhankelijke standaarden. Dit roept fundamentele vragen op, zoals:

- Wanneer is iets een “standaard” en wanneer een technologie of platform?
- Zijn dé facto standaarden (zoals Kubernetes of Helm charts) voldoende stabiel en generiek voor normering?
- In hoeverre zijn implementatiestandaarden (zoals Haven) geschikt voor opname, gezien hun afhankelijkheid van specifieke technologie-stacks?

Daarbij geldt dat:

- open-source tooling op zichzelf doorgaans geen geschikte standaard is voor opname, omdat het geen formele specificatie betreft;
- platformen zoals Kubernetes wel sterk standaardiserend werken in de praktijk, maar niet als formele open standaard kwalificeren;
- technische specificaties (zoals OCI en TOSCA) het beste aansluiten bij het bestaande toetsingskader van Forum Standaardisatie;
- implementatiegerichte standaarden zoals Haven zich in een tussenpositie bevinden en daarmee casuïstisch beoordeeld moeten worden.

Het containerdomein laat zien dat de meest relevante bijdragen aan portabiliteit in de praktijk vaak afkomstig zijn uit een combinatie van standaarden, platforms en tooling, terwijl het huidige standaardisatiekader vooral gericht is op formele specificaties. Dit vraagt om een bewuste afweging van wat als open standaard wordt beschouwd, en mogelijk om verdere doorontwikkeling van het toetsingskader van Forum Standaardisatie.

6 Aandachtsgebied 2: Encryptie en sleutelbeheer

Tijdens de expertsessie is het domein ‘encryptie & sleutelbeheer’ als aandachtsgebied aangewezen door experts. Zij geven aan dat portabiliteit-problemen zich in de praktijk met name voordoen op het vlak van sleutelbeheer, ofwel key management.

6.1 Wat is encryptie en sleutelbeheer?

Encryptie beschermt data; en sleutelbeheer bepaalt wie toegang kan krijgen tot die data. Encryptie is het proces waarbij data wordt versleuteld zodat deze alleen leesbaar is met een bijbehorende cryptografische sleutel. Sleutelbeheer omvat het genereren, opslaan, distribueren, roteren en intrekken van deze cryptografische sleutels. In cloud-omgevingen wordt dit meestal uitgevoerd via Key Management Services (KMS), vaak aangeboden door cloudproviders. Deze systemen bepalen niet alleen de veiligheid van data, maar ook de afhankelijkheid van een specifieke cloud-omgeving.

6.2 Wat is de impact van encryptie & sleutelbeheer op portabiliteit?

Encryptie en sleutelbeheer hebben impact op cloud-portabiliteit, omdat data in veel gevallen versleuteld is opgeslagen, versleuteld wordt getransporteerd en alleen toegankelijk is via specifieke KMS-systemen. Versleutelde data kan niet worden gemigreerd zonder toegang tot de bijbehorende sleutels en het onderliggende key management systeem. Dit raakt aan applicatie-portabiliteit, met name applicatie-gedrag met raakvlakken met applicatie-beleid (zie ISO/IEC 19941).

Voorbeeld: Bij migratie van een gemeentelijk zaaksysteem van cloudprovider A naar B: data is versleuteld met provider-specifieke KMS-sleutels, sleutelmaterialen zijn niet direct exporteerbaar, her-encryptie is noodzakelijk, en audit- en compliance-ketens moeten opnieuw worden opgebouwd. Dit leidt tot hoge migratiekosten, risico op dataverlies of downtime en vendor lock-in op de beveiligingslaag.

6.3 Welke open standaarden staan er al op de lijsten van Forum Standaardisatie?

Relevante bestaande standaarden in het kader van encryptie & sleutelbeheer richten zich primair op de encryptie alsook transportbeveiliging, organisatorische security controls, zoals:

Pas toe of leg uit:

- NEN-ISO/IEC 27001 en 2 – managementsysteem voor informatiebeveiliging. Deze standaard is relevant als governancekader voor informatiebeveiliging, inclusief beleid rond cryptografie en sleutelbeheer.
- TLS – standaard voor beveiligde gegevensuitwisseling tussen clients en servers; relevant voor transportbeveiliging

Aanbevolen open standaarden:

- AES – aanbevolen standaard voor versleuteling van opgeslagen en verzonden data. AES is relevant als cryptografische techniek, maar zegt niets over het beheer of de overdraagbaarheid van sleutels.
- X.509 – aanbevolen standaard voor certificaten en PKI-gebaseerde authenticatie. X.509 is relevant voor certificaatgebruik en vertrouwen, maar biedt geen oplossing voor cloud-native key management-portabiliteit.

- IPsec – aanbevolen standaard voor beveiligde IP-verbindingen. Relevantie ligt vooral bij transport- en netwerkbeveiliging
- S/MIME – aanbevolen standaard voor beveiligde e-mail, inclusief gebruik van certificaten en encryptie. Relevantie is beperkt tot specifieke toepassingsdomeinen.
- SHA-2 – aanbevolen standaard voor authenticatie en integriteitscontrole. Deze ondersteunt beveiliging, maar niet de portabiliteit van sleutelbeheer.

6.4 Waar zitten de 'witte vlekken' rond encryptie & sleutelbeheer standaarden?

Experts geven aan dat het op de lijsten van Forum Standaardisatie ontbreekt aan open standaarden voor cloud-native Key Management Service (KMS)-portabiliteit. Ook de *Study on the interoperability of data processing services* (zie paragraaf 3.4.3) signaleert op dit vlak een standaardisatie-gap in het kader van de Data Act.

6.5 Welke standaarden zouden hier een oplossing voor kunnen zijn?

Tijdens de expertsessie zijn er geen nieuwe standaarden naar voren gekomen die de gaps rond key management zouden kunnen adresseren. In de deskresearch is wel Key Management Interoperability Protocol (KMIP) als mogelijk relevante standaard naar voren gekomen. Deze wordt hieronder nader toegelicht:

6.5.1 Key Management Interoperability Protocol (KMIP)

Omschrijving: KMIP is een protocol voor de communicatie tussen cryptografische clients en Key Management Systems (KMS). KMIP stelt verschillende systemen in staat om met elkaar te communiceren via een gestandaardiseerde interface.
Hoe draagt het bij aan portabiliteit: Het gebruik van KMIP helpt bij het voldoen aan eisen rond 'Bring Your Own Key' en 'Hold Your Own Key', waardoor organisaties de controle over hun cryptografische sleutels behouden. Door een gestandaardiseerde interface te bieden voor het beheer van cryptografische sleutels, maakt KMIP het technisch mogelijk om sleutels en versleutelde data te verhuizen naar conformerende omgevingen zonder dataverlies of de noodzaak voor her-encryptie. Hiermee wordt voorkomen dat een gebruiker gevangen zit in het ecosysteem van één specifieke hardware- of cloudleverancier.
Cloud stack laag: primair in de beveiligings- en platformdienstenlaag binnen PaaS.
Beheerorganisatie: OASIS
Open beheer: Ja. KMIP wordt ontwikkeld binnen een open, multi-stakeholder standaardisatieproces met deelname van leveranciers, gebruikers en overheidsorganisaties.
Formele status: Nee.
Nederlandse betrokkenheid: Onbekend/Geen directe betrokkenheid.
Adoptie en draagvlak: Internationaal breed erkend binnen enterprise security en storage-ecosystemen, maar beperkt geadopteerd in de hyperscaler markt. Het Duitse Sovereign Cloud Stack ondersteunt de integratie van systemen die gebruiken met name via ondersteuning van open source Key Management tools welke KMIP gebruiken, zoals OpenStack Barbican. Specifieke Nederlandse adoptie is niet bekend.
Potentie voor de Forum Standaardisatie lijst(en): Hoog, maar lage adoptie onder de hyperscalers die de markt domineren vormt een aandachtspunt.

6.6 Relevante ontwikkelingen

De *Study on the interoperability of data processing services* door Wik stelt dat verdere (Europese) harmonisatie en onderzoek naar cloud key management noodzakelijk is, zonder een concrete nieuwe standaard voor te stellen. KMIP wordt wel genoemd, maar heeft volgens de in dit onderzoek gehanteerde screeningsmethode een te lage adoptie op dit moment om in aanmerking te komen voor het Europese standaardenregister. Verwacht wordt dat in Europese standaardisatie-activiteiten mogelijk verder wordt voortgebouwd op de huidige KMIP-standaard om tot een standaard te komen die geschikt is voor het Europese standaardenregister.

Uit deskresearch blijkt dat binnen open-source initiatieven en de Sovereign Cloud Stack (SCS) ondersteuning voor het KMIP wordt gerealiseerd via open-source componenten en integraties. Ook de Franse cloud-aanbieder OVHcloud past KMIP toe in zijn cloud- en infrastructuurdiensten.

De meer prominente open-source KMIP-implementaties zijn PyKMIP, libkmip en kmip-go. PyKMIP wordt daarbij vaak gebruikt als een toegankelijke en goed gedocumenteerde implementatie van de OASIS-standaard, bijvoorbeeld voor ontwikkeling en testing. Andere implementaties, zoals libkmip en kmip-go, worden toegepast in uiteenlopende integratie- en productieomgevingen binnen cloud- en infrastructuurcomponenten.

De aanwezigheid van meerdere open-source implementaties van KMIP bevestigt de technische haalbaarheid, volwassenheid en openheid van de standaard. Dit ondersteunt de geschiktheid van KMIP als kandidaat voor opname op de lijsten van Forum Standaardisatie. Tegelijkertijd vormt de beperkte adoptie bij hyperscalers een aandachtspunt voor de uiteindelijke effectiviteit in de praktijk.

6.7 Conclusies Encryptie en sleutelbeheer

De grootste witte vlek op de lijsten van Forum Standaardisatie bevindt zich op het vlak van Key Management-portabiliteit. Momenteel domineren propriëtaire oplossingen van cloud-leveranciers keymanagement-systemen, wat een barrière vormt voor cloud switching. OASIS heeft hiervoor het KMIP ontwikkeld, maar deze standaard blijft in adoptie achter door met name de hyperscalers.

7 Aandachtsgebied 3: Identiteit & Toegang

Tijdens de expertsessie is het domein ‘Identiteit & Toegang’ (ofwel Identity & Access Management, IAM) als aandachtsgebied aangewezen door experts. Zij geven aan dat significante portabiliteit-problemen zich in de praktijk voordoen in dit domein.

7.1 Wat is Identity & Access Management?

Identity & Access Management (IAM) bepaalt wie toegang heeft tot welke cloudresources, onder welke voorwaarden en op basis van welke vertrouwensrelaties tussen organisaties en cloud-leveranciers. Het omvat het geheel aan processen, standaarden en technologieën voor het beheren van digitale identiteiten en het reguleren van toegang tot systemen en data. Dit betreft onder meer authenticatie (vaststellen van identiteit), autorisatie (toekennen van rechten), federatie (identiteiten over domeinen heen) en lifecycle management van gebruikers en entiteiten.

Ter achtergrond is ISO/IEC 24760-serie A Framework for Identity Management relevant.

7.2 Wat is de impact van IAM op portabiliteit?

Experts geven aan dat IAM een kritieke factor is voor cloud-portabiliteit, wat wordt bevestigd door de Europese studie van WIK-Consult. Identiteiten, toegangsrechten en vertrouwensrelaties zijn vaak diep verankerd in specifieke cloud-platformen. Hierdoor heeft IAM een directe impact op de applicatie-portabiliteit.

Applicaties zijn sterk afhankelijk van identity providers en authenticatiemechanismen van cloud-leveranciers. Hierdoor is hergebruik van identiteiten en toegangsrechten tussen verschillende cloud-omgevingen beperkt. Dit leidt in de praktijk tot beperkte overdraagbaarheid van gebruikers, rollen en governance-structuren tussen omgevingen. Identity- en accessmodellen worden bovendien vaak leveranciers-/platformspecifiek ingericht. Hierdoor zijn zij niet volledig gestandaardiseerd. Zonder dergelijke standaardisatie kunnen applicaties technisch worden gemigreerd, maar blijft functionele toegang na migratie problematisch. Het onderstaande voorbeeld illustreert dit.

Voorbeeld: Een ministerie migreert een applicatie van de ene cloud-leverancier naar een andere. De gebruikers, rollen en rechten zijn in de oorspronkelijke omgeving ingericht volgens platform-specifieke IAM-modellen en niet volledig gebaseerd op open standaarden. Na migratie herkent de nieuwe cloud-omgeving deze identiteiten niet direct, waardoor gebruikers opnieuw moeten worden ingericht en toegang tot de applicatie tijdelijk niet beschikbaar is.

7.3 Welke open standaarden staan al op de lijsten van Forum Standaardisatie?

De standaarden op de lijsten van Forum Standaardisatie die het duidelijkst naar voren komen zijn:

Pas toe of leg uit-lijst:

- NL GOV Assurance Profile for OAuth 2.0 moet worden toegepast bij applicaties waarbij gebruikers of ‘resource owners’ impliciet of expliciet toestemming geven aan een dienst van een derde om namens deze toegang te krijgen tot gegevens via een REST API waarvoor ze recht van toegang hebben.
- SAML 2.0 en OpenID.NLGov (OpenID Connect – OIDC, identiteitslaag boven OAuth 2.0) zijn samen verplicht op het vlak van (federatieve authenticatie en single sign-on): Deze authenticatie-standaarden moeten worden toegepast door aanbieders van identity-diensten, onder wie identity

providers en identity brokers/gateways, op hun externe koppelvlak aan serviceproviders (d.w.z. overheden met digitale diensten) voor federatieve toegang en voor de uitwisseling van attributen, waaronder identiteitsgegevens, zodat serviceproviders de keuze hebben tussen beide standaarden. De verplichting van OpenID.NLGov (het Nederlandse profiel) betekent dat het gebruik van de internationale standaard OpenID Connect (OIDC) verplicht is volgens de aanscherpende eisen uit het Nederlandse profiel.

Aanbevolen standaarden:

- OAuth 2.0 is een aanbevolen standaard op het gebied van autorisatie voor API-toegang.
- X509 / PKI-profielen (digitale certificaten en trust) is een aanbevolen standaard op het gebied van authenticatie van applicaties, gebruikers, systemen middels certificaten op het internet, zoals www, elektronische mail (beveiligd), gebruikers authenticatie en IPsec, SSL en TLS.
- SCIM (System for Cross-domain Identity Management). Deze standaard is gericht op het reduceren van kosten en complexiteit en het voorbouwen op bestaande protocollen: Geautomatiseerde uitwisseling van identiteitsinformatie van gebruikers tussen verschillende (cloud) systemen. SCIM heeft als doel om gebruikers snel, goedkoop en eenvoudig in, uit en tussen clouddiensten te brengen. SCIM zorgt ervoor dat identiteitsinformatie van gebruikers systeemoverstijgend op de juiste plek aanwezig is. Hierdoor kunnen gegevens die niet meer in systemen horen te staan, omdat een gebruiker bijvoorbeeld niet langer in dat systeem hoeft te zijn opgenomen, worden verwijderd. Doordat dit geautomatiseerd gebeurt is relatief weinig inspanning nodig om de gewenste toevoeging of verwijdering van gegevens te realiseren. SCIM heeft een relatie met JavaScript Object Notation (JSON) en Extensible Markup Language (XML), dit zijn formaten waarin gegevens (de identiteitsinformatie) worden opgenomen.

7.4 Waar zitten de ‘witte vlekken’ rond IAM?

Experts geven aan dat de huidige IAM-standaarden op de lijsten van het Forum Standaardisatie ondersteunen (federatieve) toegang (authenticatie en autorisatie), maar niet de portabiliteit van identiteiten en toegangsmodellen tussen cloud-omgevingen.

7.5 Welke standaarden zouden hier een oplossing voor kunnen zijn?

Op basis van de interviews, expertsessie en deskresearch zijn geen standaarden geïdentificeerd die de geïdentificeerde witte vlekken op het gebied van IAM kunnen invullen binnen de context van cloud-portabiliteit.

7.6 Oplossingen via tools en methoden

Geïnterviewde experts noemen dat **Infrastructure as Code** (IaC) bijdraagt aan applicatie-portabiliteit. Met IaC maakt men de configuratie los van de onderliggende interface van de cloud-provider, waardoor de drempel om over te stappen naar een ander platform aanzienlijk lager wordt. Met IaC-tools zoals Terraform, OpenTofu of Ansible (zie longlist bijlage E) kan namelijk de volledige configuratie van de IAM-oplossing vastgelegd worden in code. Hierdoor kan men dezelfde identiteitsomgeving snel opzetten in een andere cloud of op een lokale server. Diverse experts noemen open source tools voor identity-management als oplossingsrichting. Dit komt ook terug in het Duitse Sovereign Cloud Stack (zie paragraaf 3.6.1) bijvoorbeeld. Deze oplossingsrichtingen lijken niet geschikt als open standaarden.

Experts geven aan dat centrale IAM-voorzieningen (één identity-laag), ondersteund door (nieuwe) open standaarden, essentieel zijn voor cloud-portabiliteit. Door identiteiten en toegangsrechten los te koppelen van specifieke cloud-leveranciers ontstaat veel betere portabiliteit.

7.7 Relevante ontwikkelingen

- In de praktijk vormen SAML, OpenID Connect (OIDC) en OAuth 2.0 de kern van federatieve toegang tot clouddiensten. Voorbeelden zoals SURFconext en GovConext laten zien dat organisaties met één koppeling toegang kunnen regelen tot meerdere cloudservices op basis van deze open standaarden. Daarbij ondersteunt SAML vooral klassieke federatieve single sign-on, OIDC moderne identity federation, en OAuth 2.0 gedelegeerde autorisatie en veilige toegang tot API's. Deze standaarden maken interoperabiliteit van toegang goed mogelijk, maar lossen identity-portabiliteit — het meenemen van identiteiten, rollen, groepen en rechten tussen cloudomgevingen — nog niet volledig op.
- Internationaal wordt onder de subcommissie ISO/IEC JTC 1/SC 38 (Cloud computing and distributed platforms) gewerkt aan standaarden zoals de ISO/IEC AWI 10822-2 (Cloud computing — Multi-cloud management — Part 2: Identity management) standaard. Daarnaast is er ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection met onder andere WG 5 - Identity management and privacy technologies. Het accent van SC 27 ligt minder op cloud dan in SC 38. Voor cloud-portabiliteit van IAM lijkt SC 38 relevanter, dan SC 27.
- In de Study on interoperability of data processing services wordt aan de Europese Commissie geadviseerd om nieuwe standaardisatie-opdrachten te verstrekken aan Europese organisaties om de hiaten in standaarden die geschikt zijn voor het Europese standaardenregister te vullen. De studie stelt dat aanvullende standaarden nodig zijn die bovenop bestaande federatieve IAM-standaarden (zoals SAML, OAuth 2.0 en OpenID Connect) functioneren en specifiek gericht zijn op automatiserings- en migratievriendelijkheid.

  Hierbij wordt onder meer gewezen op API-gebaseerde provisioning en Infrastructure-as-Code-benaderingen (zoals SCIM-achtige modellen), zodat volledige IAM-omgevingen reproduceerbaar en overdraagbaar worden tussen cloudproviders. Concreet adviseert de studie de EC om te werken aan:

  - de ontwikkeling van een standaard voor IAM-portabiliteit en federatie over datadomeinen heen, inclusief mechanismen voor cross-trust identity exchange, policy enforcement en credential portability;
  - de definitie van Europese metadata- en ontologiemodellen voor IAM, ter ondersteuning van semantische interoperabiliteit en cross-domain discoverability van identiteiten, rollen en toegangsbeleid; en
  - ontwikkeling van interoperabiliteitsprofielen en conformance testprocedures, om daadwerkelijke uitwisselbaarheid tussen soevereine cloudomgevingen en hyperscaler-omgevingen te waarborgen.

Naar verwachting worden deze adviezen (grotendeels) overgenomen door de Europese Commissie. Najaar 2026 wordt dit advies naar verwachting behandeld.

7.8 Conclusies Identiteit & Toegang

De huidige IAM-standaarden op de lijsten van het Forum Standaardisatie ondersteunen interoperabiliteit tussen systemen, maar bieden onvoldoende ondersteuning voor portabiliteit van IAM. Dit wordt ook erkend in de Europese beleidsopgave, waarin niet het uitbreiden van authenticatiestandaarden centraal staat, maar het realiseren van volledige identity portabiliteit over cloud-omgevingen heen.

Adoptie van bestaande standaarden op de lijsten van Forum Standaardisatie is belangrijk om aankomende nieuwe portabiliteit-standaarden voor IAM goed op te laten functioneren.

8 Aandachtsgebied 4: Database portabiliteit

Tijdens de expertsessie is het domein als aandachtsgebied aangewezen door experts. Zij geven aan dat significante portabiliteit-problemen zich in de praktijk voordoen in dit domein.

8.1 Wat zijn databases?

Databases slaan data op. Ze zorgen ervoor dat gegevens bewaard blijven en later opnieuw gebruikt kunnen worden door applicaties. In cloud-omgevingen vormen databases daarom een centrale laag tussen opslag en applicaties.

Databases organiseren data ook zodat deze kan worden opgezocht, aangepast en gedeeld. Ze voeren ook bewerkingen uit op data. Door de combinatie van opslag en verwerking bepalen databases niet alleen waar data staat, maar ook hoe data wordt gebruikt binnen een systeem. Hierdoor zijn applicaties vaak sterk afhankelijk van de gekozen database en de manier waarop deze is ingericht.

Databases zijn zogenaamde ‘stateful’ systemen. Dat betekent dat ze altijd de huidige toestand van de data bewaren en deze toestand in de tijd verandert. Elke wijziging bouwt voort op eerdere data (historie).

8.2 Wat is de impact van portabiliteit van databases?

Portabiliteit van databases betekent dat data in databases en bijbehorende databasefunctionaliteit kan worden verplaatst tussen cloud-omgevingen, met behoud van betekenis, werking en beheerbaarheid. In de praktijk is dit complex.

Een database bestaat niet alleen uit data, maar kan ook informatie bevatten over de manier waarop die data wordt verwerkt en geïnterpreteerd. Hierdoor vereist migratie niet alleen het verplaatsen van data, maar ook het overdragen of heropbouwen van de context waarin die data functioneert.

Deze context bestaat onder andere uit schema’s, indexstructuren, transactiemechanismen, replicatie-instellingen en eventueel provider-specifieke uitbreidingen. Database-portabiliteit is daardoor geen eenvoudige dataoverdracht, maar eerder een herimplementatie van het dataverwerkings- en consistentiemodel. De staat van een database (statefulness) versterkt deze complexiteit. Een database bewaart een toestand die in de tijd verandert, waarbij elke wijziging voortbouwt op eerdere data. Daardoor is de actuele toestand en historie van het systeem direct onderdeel van de functionaliteit. Migratie kan hierdoor niet los worden gezien van deze bestaande toestand.

In de praktijk leidt dit vaak tot vendor lock-in. Cloudproviders bieden beheerde database-diensten die sterk geoptimaliseerd zijn voor hun eigen platform. Deze diensten bevatten vaak functionaliteit zoals automatische back-ups, schaalbaarheid, monitoring en integraties met identity- en toegangsbeheer. Een deel van deze functies is niet gestandaardiseerd en verschilt per provider. Deze zogenoemde ‘sticky features’ beperken de overdraagbaarheid van databases tussen cloud-omgevingen. Daardoor vereist migratie in veel gevallen meer dan een technische overdracht van data. Vaak is herconfiguratie of aanpassing van de database-architectuur nodig om compatibiliteit met een ander platform te realiseren.

De mate van portabiliteit verschilt bovendien per type data:

- Gestructureerde data is opgeslagen volgens een vast schema, zoals in relationele databases. Dit maakt uitwisseling relatief goed mogelijk, maar alleen binnen compatibele systemen en standaarden.

- Semi-gestructureerde data heeft een flexibele structuur, zoals bij documentgebaseerde NoSQL-systemen. Hoewel uitwisseling vaak technisch mogelijk is via formaten zoals JSON, ontbreekt regelmatig uniformiteit in semantiek en interpretatie tussen systemen.
- Ongestructureerde data (zoals bestanden en media) is technisch het meest overdraagbaar, omdat opslagformaten doorgaans onafhankelijk zijn van database-logica.

8.3 Welke open standaarden staan reeds op de lijsten?

Op de lijsten van het Forum Standaardisatie ontbreken specifieke standaarden voor portabiliteit van database management systems. Hierdoor ontstaan belangrijke witte vlekken op drie niveaus:

1. database-engine functionaliteit;
2. migratie van complete databases tussen cloud-leveranciers; en
3. de semantiek en operationele database-logica.

In de praktijk beperkt dit de database-portabiliteit. Standaarden reguleren wel hoe data wordt uitgewisseld en benaderd, maar niet hoe databases functioneren, worden beheerd en als geheel worden verplaatst tussen cloud-omgevingen. Daardoor blijft migratie van databases grotendeels afhankelijk van leveranciersspecifieke oplossingen.

De huidige standaarden op de lijsten richten zich met name op data-uitwisseling (JSON, XML), query-interactie (SQL) en API's (REST/OpenAPI). Daarmee ondersteunen zij de uitwisseling van data, maar niet de overdraagbaarheid van de onderliggende databasefunctionaliteit.

De lijsten bevatten vooral standaarden voor datamodellen, gegevensuitwisseling en toegangsinterfaces, maar geen standaarden die de portabiliteit van volledige database-omgevingen tussen cloud-leveranciers borgen. De bestaande open standaarden richten zich met name op data-interoperabiliteit (zoals SQL, JSON en XML) en op koppelvlakken en API's voor gegevensontsluiting, maar niet op de interne werking, het beheer of de migratie van databases zelf. Daardoor ontbreekt standaardisatie voor de overdraagbaarheid van complete database-omgevingen, inclusief bijbehorende functionaliteit en platformafhankelijkheden. De meest relevante standaarden zijn:

Pas toe of leg uit:

- (geen standaarden)

Aanbevolen open standaarden:

- **SQL (ISO/IEC 9075)** – relationele databases. Op de aanbevolen lijst. SQL standaardiseert de querytaal en het relationele datamodel en ondersteunt daarmee basisinteroperabiliteit tussen relationele databases. SQL maakt het mogelijk om gestructureerde data en basisquery's op een vergelijkbare manier te gebruiken binnen verschillende relationele databases in diverse cloud-omgevingen. Daarmee ondersteunt SQL vooral de uitwisselbaarheid van data en query-logica. Het standaardiseert echter niet het gedrag, beheer of de platformafhankelijke functies van databases, waardoor SQL geen volledige database- of cloud-portabiliteit borgt, maar slechts een deelaspect ervan.

8.4 Waar zitten de witte vlekken rond database-portabiliteit?

Experts geven aan dat op de lijsten van Forum Standaardisatie standaarden ontbreken voor de volledige database-omgeving: niet de data zelf, maar het gedrag, het beheer en de werking daaromheen van de database als compleet systeem.

8.5 Welke standaarden zouden dit kunnen invullen?

Er bestaat geen geïntegreerde open standaard die database-portabiliteit tussen cloud-leveranciers end-to-end afdekt. Dit wordt ook bevestigd door experts en in de WIK-studie. Bestaande

standaarden dekken slechts deelaspecten, met name op het niveau van datamodel, data-uitwisseling en opslagabstractie. Onderstaande staat een inhoudelijke verdieping hierop:

Voor relationele databases vormt ISO/IEC 9075 (SQL) de belangrijkste open standaard op de Aanbevolen-lijst van Forum Standaardisatie. SQL ondersteunt portabiliteit op het niveau van querytaal en het relationele model. Aanvullend kunnen ook generieke uitwisselstandaarden zoals CSV, XML en JSON helpen bij export en migratie van gegevens, maar deze dekken vooral de data zelf en niet het volledige gedrag van de database. De dekking van SQL blijft bovendien beperkt, omdat onderdelen niet volledig gestandaardiseerd zijn en per leverancier verschillen. SQL zorgt daarmee vooral voor syntactische portabiliteit (hoe je iets vraagt), maar niet voor functionele portabiliteit (hoe een database zich gedraagt). Daardoor blijft portabiliteit in de praktijk grotendeels beperkt tot data en basisquery's.

Voor semi-gestructureerde en NoSQL-databases ontbreken breed gedragen, vendor-neutrale standaarden voor schema's, semantiek en migratiegedrag. Wel zijn er standaarden en formaten die deelaspecten ondersteunen, zoals JSON voor gegevensuitwisseling, Apache Avro (zie ook hoofdstuk 9) voor schema-gedreven uitwisseling en schema-evolutie, en Protobuf voor efficiënte uitwisseling van gestructureerde berichten tussen diensten. Voor analytische of lakehouse-achtige omgevingen spelen daarnaast Apache Parquet en Apache Iceberg een rol (zie ook hoofdstuk 9). Iceberg ondersteunt met name portabiliteit van data lake-tabellen en metadata (zoals schema-evolutie, partities en versies), maar is gericht op een specifiek analytics-ecosysteem en geen algemene standaard voor database-portabiliteit. De WIK-studie bevestigt dit beeld: Iceberg scoort laag in de screening en wordt daarmee niet gezien als volwassen oplossing voor brede cloud-portabiliteit.

Voor ongestructureerde data **lijkt de situatie gunstiger, maar deze is in de praktijk vaak** niet leveranciersonafhankelijk. Hieromtrent zijn vooral de facto standaarden naar voren gekomen, zoals de Amazon S3 API**,** die brede praktische interoperabiliteit ondersteunen voor objectopslag, maar onder beheer staan van marktpartijen. Voor cloudopslag komt één open standaard naar voren, namelijk CDMI (ISO/IEC 17826). CDMI zit echter vooral op de opslaglaag, niet op het niveau van de database als functionele omgeving, dus het lost het probleem met database portabiliteit niet op.

8.6 Oplossingen in de praktijk voor database portabiliteit

In de praktijk zijn er verschillende (deel)oplossingsrichtingen, maar deze hebben beperkte potentie om als open standaard te worden opgenomen op de lijst van het Forum Standaardisatie. Het gaat hierbij vooral om technische benaderingen die slechts specifieke lagen van database-portabiliteit adresseren, zoals:

- Op infrastructuurniveau dragen cloud-native abstractielagen zoals Kubernetes en Infrastructure-as-Code bij aan reproduceerbare uitrol van database-omgevingen. Hierdoor wordt de inzetbaarheid tussen cloud-omgevingen vergemakkelijkt. Deze benadering standaardiseert echter niet de interne werking, semantiek of beheerlogica van databases.
- Daarnaast wordt in de praktijk vaak gebruikgemaakt van open-source database-engines zoals PostgreSQL, MySQL (Oracle) en MongoDB (MongoDB Inc.). Deze dragen bij aan overdraagbaarheid doordat implementaties breed beschikbaar zijn. Alleen PostgreSQL lijkt community-gedreven; andere systemen worden door commerciële partijen beheerd. Hoewel deze engines bijdragen aan praktische interoperabiliteit, vormen zij geen open standaard voor portabiliteit en blijven implementatieverschillen bestaan.
- Technieken zoals database-replicatie, abstractielagen (bijvoorbeeld ORM's) en containerisatie kunnen de portabiliteit verder ondersteunen. Deze technieken verminderen de afhankelijkheid van specifieke implementaties, maar nemen de fundamentele verschillen in database-engines, datamodellen en beheerdiensten niet weg.

8.7 Relevante ontwikkelingen rond databases

Op het gebied van database-portabiliteit zijn in het onderzoek slechts beperkte nieuwe ontwikkelingen geïdentificeerd. De belangrijkste ontwikkeling betreft verdere aandacht voor SQL als gestandaardiseerde basis voor relationele databases, waaronder de mogelijkheid dat SQL (ISO/IEC 9075) wordt opgenomen in het Europese standaardenregister.

8.8 Conclusies databases

Er staan geen standaarden op de ‘Pas toe of leg uit’-lijst. SQL (op de aanbevolen lijst) standaardiseert hoe data wordt bevraagd binnen relationele systemen, maar is geen standaard voor volledige database-portabiliteit.

9 Overige standaarden

In deze paragraaf worden diverse standaarden en thema's besproken die door experts zijn genoemd, evenals in eerder onderzoek in opdracht van Forum Standaardisatie en in de *Study on the interoperability of data processing services* in opdracht van de Europese Commissie. Deze standaarden vallen buiten de primaire aandachtsgebieden en zijn daarom slechts beperkt meegenomen in de analyse.

9.1 Standaarden op het gebied van beveiliging

Cybersecuritystandaarden en informatiebeveiligingsstandaarden dragen bij aan de mate van portabiliteit van databeleid en applicatiebeleid. Het tussen de twee type standaarden verschil zit vooral in waar in de keten zij ingrijpen en wat zij concreet mogelijk maken voor portabiliteit:

- **Cybersecurity-standaarden** (zoals NVN TS 18026:2024 EN) richten zich primair op de weerbaarheid en technische veiligheid van systemen. Hun bijdrage aan portabiliteit is voorwaardelijk: zij zorgen dat data en applicaties veilig kunnen worden verplaatst of beheerd (bijvoorbeeld veilige overdracht, identiteit- en toegangsbeheer, logging, continuïteit). Zij maken overstappen verantwoord en beheersbaar, maar bepalen niet hoe data of applicaties technisch overdraagbaar zijn. Cybersecurity-standaarden doorbreken dus geen lock-in en specificeren meestal geen uitwisselformaten, API's of migratiemechanismen. Tegelijkertijd vereisen vrijwel alle securitystandaarden een vorm van inventarisatie van middelen, identiteiten en rechten, wat direct relevant is voor het kunnen migreren van systemen en data tussen omgevingen. Zonder deze gestructureerde vastlegging is het niet mogelijk om een consistente en controleerbare overdracht van securitycontext te realiseren bij cloud-migraties.
- **Informatiebeveiligingsstandaarden** (zoals de BIO: ISO/IEC 27001 en ISO/IEC 27002) hebben een bredere bestuurlijke en organisatorische scope. Zij dragen sterker bij aan portabiliteit doordat zij eisen stellen aan databeleid en applicatiebeleid, zoals dataclassificatie, eigenaarschap, levenscyclusbeheer, exit-strategieën en verantwoordelijkheidsverdeling. Daarmee stimuleren zij voorwaarden voor keuzevrijheid en controle (wanneer, onder welke voorwaarden en door wie data/applicaties kunnen worden overgedragen), maar ook zij schrijven zelden concrete technische interoperabiliteitsstandaarden voor.

9.2 Standaarden uit andere cloud-portabiliteit onderzoeken

In deze paragraaf worden prominente standaarden uit twee onderzoeken rond cloud-portabiliteit nadere bekeken, te noemen 1) Standaarden en standaardisatieactiviteiten voor clouddiensten (E-Space, 2024); en 2) Study on the interoperability of data processing services (Wik, 2025).

9.2.1 Standaarden uit 'Standaarden en standaardisatieactiviteiten voor clouddiensten'

Het onderzoek Standaarden en standaardisatieactiviteiten voor clouddiensten benoemt daarnaast diverse open standaarden die relevant zijn voor data-portabiliteit en interoperabiliteit, waaronder Apache Parquet, Apache Avro, Apache Iceberg, GraphQL en gRPC. Deze dragen vooral bij aan data-portabiliteit en API-interoperabiliteit op data- en applicatieniveau. Zij leveren waarde op deelaspecten van portabiliteit (en interoperabiliteit), met name op het niveau van dataformaten en API-interacties.

9.2.2 Standaarden uit 'Study on the interoperability of data processing services'

De *Study on the interoperability of data processing services* staat in paragraaf 3.4.3 nader toegelicht. Uit deze studie komen de volgende standaarden prominent naar voren:

- OCI en TOSCA zijn al behandeld in hoofdstuk 5 bij het aandachtsgebied ‘Containers & Orchestratie’
- SQL is behandeld in hoofdstuk 8 bij het aandachtsgebied ‘Databases’.
- XML en JSON zijn ook al aan de orde gekomen, en niet als sleutelstandaard aangewezen voor van de aandachtsgebieden.
- SECA

De WIK-studie maakt onderscheid tussen enerzijds standaarden die reeds kansrijk worden geacht voor opname in het EU-repository (OpenAPI, SECA, OCI, TOSCA, XML en JSON), anderzijds standaarden die nog nadere beoordeling vereisen (zoals SQL), en daarnaast standaarden die voornamelijk deelaspecten van portabiliteit ondersteunen, zoals Parquet, Avro, GraphQL en gRPC.

Apache Iceberg is daarbij expliciet beoordeeld, maar niet geslaagd in de screening. Iceberg is volgens deze studie te smal / te specifiek voor het doel van de eerste tranche.
Het ondersteunt vooral lakehouse-/datalake-tabellen en metadata, maar werd door WIK niet gezien als voldoende brede oplossing voor interoperabiliteit en switching van data processing services in de zin van de Data Act. In de onderstaande tabel staan de bovengenoemde standaarden geordend.

Standaard	Status op de lijsten	Bijdrage aan portabiliteit	Duiding vanuit de WIK-studie	Cloud-stacklaag
Apache Parquet	Staat niet op de lijsten.	Open dataformaat voor overdracht en hergebruik van grote datasets, vooral in analytics- en data lake-omgevingen. Ondersteunt overdraagbaarheid van datasets tussen analysetools zonder conversie naar leverancier-specifieke opslagformaten.	Vooral een ondersteunende bouwsteen, geen sleutelstandaard voor cloudswitching.	PaaS (data/analytics), soms IaaS (opslag)
Apache Avro	Staat niet op de lijsten.	Open formaat voor schemagebaseerde data-uitwisseling en streaming. Ondersteunt overdraagbaarheid van datastromen en behoud van schema’s bij migratie tussen databases, dataplatformen en cloudomgevingen.	Vooral relevant als ondersteunende standaard voor data-uitwisseling en schema-evolutie.	PaaS (data pipelines, messaging)
Apache Iceberg	Staat niet op de lijsten.	Open tabel- en metadataformaat voor data lake- en lakehouse-omgevingen. Ondersteunt overdraagbaarheid van tabellen, schema’s en versies bovenop open dataformaten, maar is beperkt tot dit specifieke domein.	Volgens WIK geen kansrijke eerste repository-kandidaat voor brede cloud-portabiliteit of interoperabiliteit.	PaaS (lakehouse/analytics)

GraphQL	Staat niet op de lijsten.	Gestandaardiseerd API-query- en typesysteem. Vermindert afhankelijkheid van clients bij backendmigraties, maar draagt vooral bij aan interoperabiliteit op API-niveau.	Vooral een ondersteunende API-standaard.	PaaS / SaaS (API-laag)
gRPC	Staat niet op de lijsten.	Open protocol voor efficiënte service-tot-service-communicatie via Protobuf en HTTP/2. Ondersteunt interoperabiliteit tussen diensten, maar draagt slechts beperkt bij aan bredere cloudportabiliteit.	Vooral een technische bouwsteen voor service-interoperabiliteit.	PaaS (microservices / backend)
WebDAV	Aanbevolen standaard.	Ondersteunt uniforme toegang tot, en migratie van, documenten en bestandsstructuren via HTTP. Draagt bij aan overdraagbaarheid van bestanden in documentgerichte omgevingen.	Vooral ondersteunende standaard op applicatieniveau.	Primair SaaS (applicatielaag), secundair PaaS (API/integratie)
CalDAV	Aanbevolen standaard.	Ondersteunt gestandaardiseerde synchronisatie en overdracht van agenda's en afspraken tussen verschillende systemen, zonder leveranciersspecifieke exportformaten.	Vooral ondersteunende standaard op applicatieniveau.	Primair SaaS (applicatielaag), secundair PaaS (API/integratie)
OpenAPI (OAS)	Aanbevolen standaard.	Open specificatie voor het beschrijven van RESTful API's. Ondersteunt syntactische interoperabiliteit tussen diensten en vergemakkelijkt migratie of herimplementatie van applicaties die van API-koppelingen afhankelijk zijn.	Door WIK expliciet aanbevolen als kansrijke kandidaat voor de eerste tranche van het EU-repository. OpenAPI behaalde in de screening 100% op de toepasselijke criteria. Kansrijk voor EU verplichting.	PaaS / SaaS (API- en integratielaag)
Sovereign European Cloud API (SECA)	Staat niet op de lijsten.	Open specificatie voor interoperabiliteit tussen Europese cloud-omgevingen. Beoogt een uniforme API-laag voor	Door WIK expliciet genoemd als kansrijke kandidaat voor het EU-repository. Echter, de open governance lijkt	PaaS (platformdiensten / API-laag)

		basale platformdiensten, maar de bijdrage aan dataportabiliteit blijft beperkt.	nog minder uitgekristalliseerd dan bij formele standaarden en is bredere adoptie nog in ontwikkeling.	

De WIK-studie maakt een onderscheid tussen een beperkte eerste tranche kansrijke standaarden voor opname in het EU-repository (OpenAPI, SECA, OCI, TOSCA, XML en JSON), een categorie die nog nader onderzocht moet worden (zoals SQL), en overige standaarden die vooral deelaspecten ondersteunen, zoals Parquet, Avro, GraphQL en gRPC. Apache Iceberg is daarbij expliciet beoordeeld, maar niet geslaagd in de screening.

Voor opname in de eerste tranche moesten standaarden dus niet alleen “open” of technisch bruikbaar zijn, maar ook breed bijdragen aan cloud switching en interoperabiliteit tussen data processing services van hetzelfde type. Iceberg haalde dat volgens WIK onvoldoende.

9.3 Conclusies Overige standaarden

De in dit hoofdstuk besproken standaarden dragen vooral bij aan deelaspecten van portabiliteit, zoals data-uitwisseling, API-koppelingen en bestandsuitwisseling. Zij adresseren niet de belangrijkste lock-in problemen rond IAM, databases, sleutelbeheer en complete cloud-omgevingen.

10 Bevindingen standaarden analyse

Dit hoofdstuk vat de belangrijkste bevindingen uit hoofdstuk 5 tot en met 10 samen. Centraal staat de vraag in hoeverre bestaande en opkomende standaarden bijdragen aan cloud-portabiliteit en welke kansen er liggen voor opname op de lijsten van Forum Standaardisatie.

10.1 Rol van open standaarden bij portabiliteit

- Cloud-portabiliteit wordt in de praktijk niet opgelost door één standaard, maar door een stapeling van open specificaties, tooling, ecosystemen en operationele conventies.
- Standaarden laten zich in de praktijk niet per se eenduidig indelen naar één facet van data- of applicatie-portabiliteit zoals onderscheiden in ISO/IEC 19941 (hoofdstuk 3). Standaarden combineren ook elementen van syntactische, semantische en soms ook beleidsmatige aspecten. Zo bevatten standaarden soms zowel een gegevensformaat (syntax) als structuur of relaties (semantiek), en zijn zij in hun toepassing ingebed in bredere kaders zoals beveiliging, governance of compliance. Dit maakt dat hun bijdrage aan portabiliteit per geval meerdere facetten tegelijk kan beslaan.
- Veel bestaande standaarden ondersteunen deelaspecten van portabiliteit, maar er zijn weinig standaarden die de benodigde cloud-portabiliteit over data, applicaties, identiteiten, configuraties en platformdiensten heen adresseren. Uit de analyse van de aandachtsgebieden (hoofdstukken 5 tot en met 9) blijkt dat de grootste behoefte ligt bij standaarden die volledige overdraagbaarheid ondersteunen.

10.2 Algemene bevindingen

- Standaardisatie concentreert zich vooral op lagere lagen van de cloud stack, zoals dataformaten, API's en containertechnologie, terwijl de grootste knelpunten zich bevinden op hogere en dwarsdoorsnijdende lagen, zoals IAM, databases en key management.
- Gebruik van managed services van cloud-leveranciers vergoot het gebruiksgemak voor cloud-afnemers, maar beperken portabiliteit: bij migratie kan de dienst zelf niet worden meegenomen, alleen de data, vaak zonder volledige standaardisatie. Hierdoor wordt overstappen complex en herimplementatie noodzakelijk.
- De analyse laat zien dat cloud-portabiliteit in de praktijk voornamelijk wordt gerealiseerd via ecosystemen van open source tooling, cloud-native technologieën en de facto standaarden, in plaats van via geharmoniseerde normen of formele open standaarden.
- Dit leidt tot spanning met het huidige toetsingskader van Forum Standaardisatie, dat primair gericht is op formele, stabiele en vendor-onafhankelijke standaarden.
- In het cloud-native domein bevindt portabiliteit zich vaak in een grijs gebied tussen standaarden, specificaties, implementaties en tooling. Daardoor zijn juist de meest relevante oplossingen voor portabiliteit in de praktijk niet altijd direct te kwalificeren als formele open standaard, wat spanning geeft met het huidige toetsingskader van Forum Standaardisatie.
- interoperabiliteit ≠ overdraagbaarheid. Interoperabiliteit betekent dat systemen met elkaar kunnen communiceren en samenwerken, terwijl overdraagbaarheid ziet op het daadwerkelijk kunnen verplaatsen van data, applicaties of diensten tussen omgevingen. Interoperabiliteit is daarmee een voorwaarde voor portabiliteit, maar biedt geen garantie op portabiliteit.

10.3 Kansen voor open standaarden

De onderstaande tabel geeft een overzicht van kansen voor open standaarden.

Tabellegenda:

- Toepassingsgebied: het inhoudelijke domein waarop de standaard betrekking heeft.
- Cloud Service Model: de laag of lagen binnen het cloud-landschap waarop de standaard primair betrekking heeft (IaaS, PaaS, SaaS of dwarsdoorsnijdend).
- Standaarden op de lijsten: standaarden die reeds voorkomen op de lijsten van Forum Standaardisatie.
- Kansrijke standaarden: standaarden of specificaties die in dit onderzoek als potentieel relevant naar voren zijn gekomen voor opname op de lijsten of verdere verkenning.
- Relevante SOV-categorieën: verwijzing naar de mogelijk relevante SOV-categorieën uit het EU Cloud Sovereignty Framework, die aangeven aan welk aspect van soevereiniteit de standaard kan bijdragen (zie paragraaf 3.2.5 voor een toelichting). Dit betreft een schets en geen volledige analyse. Nadere analyse en mapping is nodig.

Toepassings-gebied	Cloud Service Model	Standaarden op de lijsten	Kansrijke standaarden	Mogelijke relevante SOV-categorieën (een schets)
Definities & Begrippen	Overkoepelend	-	ISO/IEC 19941 ISO/IEC 22123	SOV-6, SOV-4
Containers& Orchestratie	Infrastructure-as-a-Service / Platform as a Service (afhankelijk van implementatie)	-	HAVEN OCI TOSCA Helm Charts	SOV-6, SOV-4
Encryptie & Sleutelbeheer	Dwarsdoorsnijdend (securityfunctie over alle lagen, vaak als PaaS)	AES (encryptie)	KMIP (key management)	SOV-3, SOV-7
IAM	Dwarsdoorsnijdend (identity- en toegangslaag, vaak als PaaS)	OAuth, OIDC, SAML, SCIM	Nog geen concrete standaard geïdentificeerd; wel Europese standaardisatie in ontwikkeling.	SOV-3, SOV-4, SOV-6
Databases	Platform as a Service	SQL	Nog geen concrete standaard geïdentificeerd; SQL vraagt nadere beoordeling aldus Wik-studie	SOV-3, SOV-4
Dataformaten & Uitwisseling	Dwarsdoorsnijdend	o.a. JSON, XML, CSV	Apache Avro, eventueel Parquet (ondersteunend)	SOV-3, SOV-6
API & Integratie	Vooral PaaS / SaaS	o.a. OpenAPI (OAS)	SECA	SOV-4, SOV-6
Bestands- en documentuitwisseling	Vooral SaaS, deels PaaS	WebDAV, CalDAV	-	SOV 3, SOV 4
Overige ondersteunende bouwstenen	Vooral PaaS	-	GraphQL, gRPC, Apache Iceberg (beperkt / domeinspecifiek)	SOV 3, SOV 6

10.2.1 Definities en begrippen

Er bestaat geen breed algemeen geaccepteerde definitie van cloud-portabiliteit. In dit onderzoek zijn daarom expliciet keuzes gemaakt in de gehanteerde definities en begrippen. Internationale standaarden zoals ISO/IEC 19941 (interoperabiliteit en portabiliteit) en ISO/IEC 22123 (cloud computing concepten en terminologie) bieden richting en een gemeenschappelijk referentiekader. Deze standaarden dragen bij aan eenduidigheid in begripsvorming, maar hebben nog beperkt status binnen de Nederlandse overheid.

10.2.2 Containers en orchestratie

Containerisatie vormt het meest volwassen en kansrijke domein voor cloud-portabiliteit. Op de lijsten van Forum Standaardisatie staan momenteel geen open standaarden die zich direct richten op containerisatie.

Binnen het cloud-native domein vervagen de grenzen tussen standaarden, specificaties, implementaties en ecosystemen (zie ook paragraaf 5.6.1). Standaarden en initiatieven zoals OCI, TOSCA en Haven kunnen bijdragen aan het invullen van de huidige witte vlek op de lijsten. Kubernetes speelt hierin een centrale rol, maar geldt als de facto standaard en niet als formele open standaard.

- **OCI (Image, Runtime, Distribution)** is een duidelijke kandidaat voor opname als open standaard, vanwege de vendor-neutrale specificatie en brede adoptie.
- **TOSCA** biedt een formele standaard voor applicatiemodellering, maar kent beperkte adoptie.
- **Haven** is relevant in de Nederlandse context als implementatiestandaard, maar heeft een beperkter internationaal bereik.
- **Helm charts** vormen een breed toegepast declaratief packaging- en deploymentmechanisme binnen Kubernetes-ecosystemen. Zij zijn echter verbonden aan de open source Helm-tool. In hoeverre dit een status als open standaard in de weg zit, moet nader bekeken worden.

In hoofdstuk 5 staat het aandachtsgebied containers & orchestratie nader uitgewerkt.

10.2.3 Bevindingen aandachtsgebied encryptie en sleutelbeheer

Het domein encryptie & sleutelbeheer vormt een aspect van security. Het domein kent een duidelijke witte vlek op het gebied van key management-portabiliteit. Momenteel domineren propriëtaire oplossingen van cloudleveranciers Key Management Service. OASIS heeft hiervoor **het Key Management Interoperability Protocol (KMIP)** ontwikkeld, maar deze standaard blijft achter in adoptie, door met name hyperscalers. Deze standaard heeft hoge relevantie, maar opname vraagt Forum Standaardisatie om afweging tussen adoptie en strategisch belang.

In hoofdstuk 6 staat het aandachtsgebied sleutelbeheer nader uitgewerkt.

10.2.4 Bevindingen aandachtsgebied Identity & Access Management (IAM)

IAM is een kritische factor voor cloud-portabiliteit, zo bevestigen experts. Bestaande standaarden op de lijsten van Forum Standaardisatie ondersteunen interoperabiliteit, maar niet de overdraagbaarheid van identiteiten, rollen en toegangsmodellen tussen cloudomgevingen, zo wordt aangegeven.

Met name **OAuth 2.0** is essentieel voor autorisatie in cloud-omgevingen, maar lost het portabiliteitsvraagstuk niet op. Identiteiten en toegangsstructuren blijven in de praktijk sterk platformspecifiek ingericht, wat migraties complex maakt en portabiliteit beperkt.

Er ontbreken standaarden voor overdraagbaarheid van identiteiten, rollen en policies. Grote standaardisatiegap; kansen liggen vooral in toekomstige (Europese) standaarden, maar dergelijke standaarden zijn nog niet beschikbaar. Voor IAM is de adoptie van bestaande standaarden op de lijsten van belang als basis; Nieuwe Europese standaarden voor IAM-portabiliteit worden verwacht hierop voort te bouwen.

In hoofdstuk 7 wordt het aandachtsgebied IAM nader uitgewerkt.

10.2.5 Bevindingen aandachtsgebied databases

Database-portabiliteit vormt een belangrijke bottleneck voor cloud-portabiliteit. De huidige standaarden op de lijsten van Forum Standaardisatie (zoals **SQL** en **JSON**) ondersteunen data-uitwisseling, maar niet de overdraagbaarheid van volledige database-omgevingen. De afhankelijkheid ontstaat niet alleen door datastructuren, maar vooral door beheerdiensten, provider-specifieke extensies, replicatiemechanismen, performance-optimalisaties en geïntegreerde cloudservices.

Hierdoor blijven databases in de praktijk sterk afhankelijk van specifieke cloud-platformen, mede door beheerfunctionaliteit, configuraties en 'sticky features' van aanbieders. Migratie vereist vaak herimplementatie in plaats van eenvoudige overdracht. Er zijn geen specifieke Europese ontwikkelingen voor database-portabiliteit naar voren gekomen.

In hoofdstuk 8 staat het aandachtsgebied databases nader uitgewerkt.

10.2.6 Ondersteunende standaarden

- Samenvattend geldt dat de standaarden **Parquet, Avro, Iceberg, GraphQL en gRPC** technisch volwassen en breed toepasbare bouwstenen zijn, maar vooral bijdragen aan **deelaspecten van portabiliteit**, zoals data-uitwisseling, API-koppelingen en interoperabiliteit op applicatieniveau. Zij zijn daarmee ondersteunend van aard en niet richtinggevend voor de primaire aandachtsgebieden van cloud-portabiliteit in dit onderzoek. **Plaatsing op de Aanbevolen-lijst lijkt kan wel passend zijn voor deze standaarden, maar dit heeft nadere analyse en wellicht ook prioritietstelling nodig.**
- Voor de Aanbevolen standaarden **OpenAPI, XML, JSON** en mogelijk **SQL** ligt het, gezien hun positie in de WIK-studie en de verwachte Europese doorontwikkeling, voor de hand om de ontwikkelingen rond het Europese standaardenregister actief te volgen. Dat neemt niet weg dat het Forum Standaardisatie deze standaarden kan opwaarderen naar verplichte standaard voor inkopende overheden. Immers geldt het Europese standaardenregister-verplichting voor leveranciers (aanbodzijde).
- Ook **WebDav, CardDav** zijn reeds Aanbevolen standaarden. Eerder onderzoek in opdracht van het Forum Standaardisatie in 2024 adviseerde om deze standaarden op te waarderen naar verplicht. Het is zinvol om de praktische toegevoegde waarde van een opwaardering naar de 'Pas toe of leg uit'-lijst te valideren en (samen met de andere standaarden die in dit onderzoek naar voren komen te valideren bij experts.
- **SECA** verdient daarbij bijzondere aandacht: de standaard is beleidsmatig relevant en wordt in de WIK-studie prominent genoemd, maar kent vooralsnog beperkte adoptie en een nog onvoldoende uitgekristalliseerde open governance. Voor Forum Standaardisatie ligt hier daarom vooral een rol in **monitoring, selectieve erkenning en proritering**, in plaats van directe brede agendering als sleutelstandaarden.

10.2.7 Cybersecuritystandaarden en informatiebeveiligingsstandaarden

Cybersecuritystandaarden en informatiebeveiligingsstandaarden dragen bij aan de mate van portabiliteit van databeleid en applicatiebeleid. Zij vormen een belangrijk randvoorwaarde en dragen bij aan cloud-portabiliteit. In hoeverre de huidige beveiligingstandaarden op dit moment cloud-portabiliteit afdekken, is niet onderzocht.

10.4 Grijs gebied: containers en cloud-native standaarden

Het containerdomein laat een belangrijk grijs gebied zien tussen open standaarden, technologieën, platforms, open source tooling en methodieken. In de praktijk dragen juist combinaties van deze elementen het meest bij aan portabiliteit. Dit roept fundamentele vragen op, zoals: ***Wanneer is iets***

een standaard versus een technologie? Zijn de facto standaarden geschikt voor normering? Hoe beoordeel je implementatiegerichte standaarden zoals Haven?

Open-source tooling en platforms zijn essentieel in de praktijk, maar vallen vaak buiten het huidige toetsingskader. Het Forum Standaardisatie moet expliciet bepalen hoe om te gaan met dit grijze gebied: vasthouden aan formele standaarden, of ruimte creëren voor de facto standaarden en implementatieprofielen.

11 Conclusies en aanbevelingen

In dit hoofdstuk worden de conclusies en aanbevelingen van het onderzoek weergegeven.

11.1 Conclusies

Cloud-portabiliteit is niet alleen een technisch vraagstuk, maar een strategische randvoorwaarde voor digitale soevereiniteit. Juist daar schieten standaarden nu tekort. Cloud-portabiliteit is geen technisch detail, maar een strategische randvoorwaarde voor digitale autonomie, leveranciersonafhankelijkheid en keuzevrijheid. Zolang data, applicaties, identiteiten en configuraties niet voldoende overdraagbaar zijn tussen cloud-omgevingen, blijven organisaties in de praktijk afhankelijk van dominante aanbieders. Nieuwe soevereine of Europese cloud-alternatieven alleen zijn daarom onvoldoende; zonder lagere overstapdrempels blijven deze alternatieven structureel onderbenut.

Lage marktwerking en lock-in versterken elkaar

Lang niet alle cloud-gebruik leidt tot portabiliteit-problemen. De grootste problemen doen zich voor in delen van de cloud-markt waar de marktwerking beperkt is en leveranciers sterke lock-in kunnen opbouwen. Via koppelverkoop, managed services en ‘sticky features’ groeit de afhankelijkheid van één leverancier stap voor stap. Elke extra integratie verhoogt de overstapdrempel, waardoor migratie steeds complexer, kostbaarder en risicovoller wordt.

Te lage portabiliteit belemmert digitale soevereiniteit

Portabiliteit is een noodzakelijke randvoorwaarde voor het realiseren van beleidsdoelen rond digitale autonomie en soevereiniteit. Zolang portabiliteit beperkt blijft, kunnen organisaties in de praktijk moeilijk overstappen naar Europese of soevereine alternatieven. Daardoor dreigt het potentieel van nieuwe cloud-initiatieven, waaronder de soevereine overheidsclouddienst, structureel onbenut te blijven.

Open standaarden zijn nodig, maar marktadoptie blijft achter

De dominante marktpartijen passen bestaande open standaarden beperkt toe. Hierdoor ontstaat een vicieuze cirkel: zonder brede marktadoptie worden standaarden niet snel als volwassen gezien, maar zonder erkenning en stimulering blijft die adoptie ook uit. Bij te lage adoptie worden standaarden niet opgenomen in een Europees standaardenregister. Datzelfde geldt voor plaatsing op de lijsten van het Forum Standaardisatie. Het gevolg is dat standaardisatie achterblijft en bestaande afhankelijkheden in stand blijven.

Alternatieve oplossingen zijn tegelijk kans en risico

Cloud-portabiliteit wordt in de praktijk vaak gerealiseerd via open source tooling, de facto technologieën en architectuurkeuzes, in plaats van via formele open standaarden. Deze oplossingen dragen wezenlijk bij aan portabiliteit in de praktijk, maar vormen niet in alle opzichten een volwaardig alternatief voor open standaarden. Enerzijds kunnen zij de prikkel verminderen om formele standaarden te ontwikkelen en te adopteren. Anderzijds kunnen zij juist een bron vormen voor nieuwe standaarden en brede adoptie. Zonder gerichte regie bestaat echter het risico dat tooling en implementaties leidend worden, terwijl standaardisatie achterblijft.

Het huidige standaardenbeleid van Forum Standaardisatie is nog onvoldoende op portabiliteit gericht

De standaarden op de lijsten van Forum Standaardisatie zijn primair gericht op (cloud)interoperabiliteit en slechts in beperkte mate op portabiliteit in de zin van migratie en exit. Ook in de huidige beschrijvingen en toetsingssystematiek komt de bijdrage van standaarden aan portabiliteit nog beperkt tot uitdrukking. Hoewel het criterium leveranciersonafhankelijkheid al een

plaats heeft in de beoordeling, wordt portabiliteit als praktisch vermogen om over te stappen nog onvoldoende expliciet meegewogen.

Europa bouwt het juridische kader, maar de technische invulling loopt achter

De toenemende Europese regelgeving versterkt de juridische afdwingbaarheid van portabiliteit, maar de technische invulling via open standaarden loopt daar nog op achter. De Data Act vormt hierbij het belangrijkste kader. Daarnaast kan de Digital Markets Act, afhankelijk van de uitkomst van lopende Europese onderzoeken, een extra juridisch instrument worden richting dominante cloud-aanbieders. Daarmee groeit de druk op de markt om overstapbaarheid en interoperabiliteit beter te faciliteren.

Het Europese standaardenregister vergroot de urgentie van nationale sturing

De Europese Commissie werkt aan een centraal standaardenregister voor interoperabiliteit van *data processing services* (waaronder cloud-leveranciers) onder de Data Act. Wanneer dit register tot verplichte standaarden zal leiden, is nog onzeker; verwacht wordt dat dit niet vóór 2028 zal zijn. Dit betekent echter niet dat het Forum Standaardisatie de uitkomsten daarvan moet afwachten. Juist omdat Europese verplichtingen zich primair richten op aanbieders, blijft nationale sturing via de lijsten noodzakelijk om portabiliteit tijdig in de Nederlandse overheidspraktijk te borgen.

De rol van Forum Standaardisatie wordt daarmee belangrijker, niet kleiner

Het Europese standaardenregister neemt de rol van Forum Standaardisatie niet weg, maar onderstreept die juist. Door relevante standaarden en specificaties tijdig te agenderen en, waar passend, op te nemen op de lijsten, kan het Forum de adoptie van portabiliteit-bevorderende technologieën versnellen en richting geven aan de markt.

Standaarden-ontwikkeling in Europa komt op gang, maar blijft onzeker in tempo en uitkomst

De Europese Commissie stuurt via de Data Act en het bijbehorende standaardisatieverzoek op de ontwikkeling van standaarden voor cloud-portabiliteit. Dit gebeurt vooral via een geleidelijke en bottom-up benadering, waarbij Europese standaardisatieorganisaties zoals **CEN, CENELEC en ETSI** standaarden ontwikkelen, onder meer via **JTC 25**. Daarnaast blijft **ISO/IEC JTC 1/SC 38** een belangrijke internationale bron van cloud-standaarden. Tussen deze Europese en internationale trajecten bestaat duidelijke wisselwerking. NEN is hier goed op aangehaakt. Het blijft echter onzeker wanneer deze trajecten daadwerkelijk leiden tot breed toepasbare standaarden voor de praktijk. Verwachting is dat de eerste resultaten vanaf 2027 zichtbaar worden.

Ook buiten formele standaardisatie ontstaan relevante standaarden

Naast formele normalisatie spelen ook technische consortia en open source communities een belangrijke rol bij de ontwikkeling van cloud-standaarden. Organisaties zoals OASIS en de Linux Foundation ontwikkelen veelal de technische specificaties die in de praktijk het meest worden toegepast. Deze trajecten zijn vaak sneller, praktischer en innovatiever dan formele standaardisatie. Tegelijkertijd is hun output niet altijd direct geschikt voor opname op de lijsten van Forum Standaardisatie, bijvoorbeeld vanwege verschillen in governance, stabiliteit of formele status. Dit onderstreept de noodzaak voor het Forum om niet alleen standaarden te volgen, maar ook actief te beoordelen welke specificaties, profielen en implementatie-ecosystemen kansrijk zijn om door te groeien tot open standaard.

Standaarden: Aandachtsgebieden & Witte vlekken

Volgens experts bevinden de belangrijkste witte vlekken in cloud-portabiliteit zich op het vlak van: containerisatie, IAM, key management en databases. Op het vlak van containerisatie zijn de meest concrete kansen voor open standaarden.

I. Containerisatie draagt bij aan portabiliteit van applicaties. Standaarden zijn in opkomst. Hiervoor zijn HAVEN, OCI, Helm Charts en TOSCA kansrijk naar voren gekomen. Hoewel

HAVEN een implementatie is, lijkt deze toch kansrijk als open standaard, zeker gezien het reeds bestaande draagvlak ervoor. HAVEN is in 2024 al aangemerkt voor de lijst, maar is tot op heden niet aangemeld.

II. Key Management-portabiliteit is volgens experts een probleem. Er staan geen standaarden hiervoor op de lijsten van Forum Standaardisatie. OASIS heeft hiervoor haar Key Management Interoperability Protocol (KMIP) ontwikkeld, maar deze standaard blijft achter in adoptie door met name hyperscalers.

III. Database-portabiliteit is ook problematisch stellen experts. Er zijn geen (potentiële) open standaarden geïdentificeerd hiervoor, naast SQL (Aanbevolen standaard). Bestaande standaarden richten zich vooral op deelaspecten, data of toegang, maar niet op de database zelf als complete, functionele omgeving.

IV. De huidige IAM-standaarden op de lijsten van het Forum Standaardisatie (zoals SAML 2.0, OpenID Connect, OAuth 2.0 en SCIM) zijn essentieel voor authenticatie, autorisatie en federatieve toegang. Zij ondersteunen daarmee interoperabiliteit tussen systemen, maar bieden onvoldoende ondersteuning voor identiteit-portabiliteit. Deze lacune is ook op Europees niveau geïdentificeerd.

11.2 Aanbevelingen aan stakeholders

Het verbeteren van cloud-portabiliteit vraagt om samenhangende actie op het snijvlak van beleid, marktontwikkeling, architectuur, standaardisatie en toepassing in de praktijk. Geen enkele partij kan dit vraagstuk alleen oplossen. Onderstaande aanbevelingen richten zich daarom op de belangrijkste stakeholders die gezamenlijk voorwaarden kunnen scheppen voor meer overstapmogelijkheden, minder leveranciersafhankelijkheid en grotere digitale soevereiniteit en autonomie.

Aanbevelingen aan het Ministerie van Binnenlandse Zaken:

- **Breng migratiescenario's voor overheden in kaart**, zodat duidelijk wordt hoe organisaties daadwerkelijk kunnen overstappen van hun huidige cloudomgeving naar een gewenste Europese, soevereine of overheidscloudomgeving.
- **Stuur actief op het verlagen van overstapdrempels**, zodat beleidsdoelen rond digitale autonomie en soevereiniteit ook praktisch realiseerbaar worden.
- **Positioneer de overheid als launching customer** voor nieuw cloud-aanbod en stimuleer Europese alternatieven via vraagbundeling (zoals ACM ook adviseert). Richt je daarbij niet alleen op de soevereine overheidscloud, maar ook op de ontwikkeling van een gezondere markt waarin portabiliteit en concurrentie beter tot hun recht komen.

Aanbevelingen aan het Ministerie van Economische Zaken:

- **Stimuleer ontwikkeling en adoptie van open standaarden op de geïdentificeerde probleemgebieden** (IAM, databases, key management) door de markt via subsidies, innovatieprogramma's en publiek-private samenwerking.
- **Draag actief bij aan internationale standaardisatie-initiatieven** en versterk de betrokkenheid van Nederlandse partijen daarbij.
- **Bevorder concurrentie en marktwerking voor meer prikkel tot portabiliteit binnen cloud-markten**. Focus hierbij op domeinen met lage marktwerking (IAM, databases, key management).

Aanbevelingen aan het OBDO:

- **Agendeer cloud-portabiliteit expliciet als randvoorwaarde** voor digitale autonomie en soevereiniteit, en niet als losstaand technisch onderwerp.

- **Prioriteer niet alleen de ontwikkeling van een soevereine cloud, maar ook de mogelijkheid om daar naartoe over te stappen.** Zonder portabiliteit blijven nieuwe alternatieven in de praktijk onderbenut.

Aanbevelingen aan het NDS Aanjaagteam Cloud:

- **Borg samenhang tussen de NDS-cloudarchitectuur en het standaardenbeleid** op nationaal en Europees niveau. Hanteer daarbij open standaarden als norm en portabiliteit als expliciet ontwerpbeginsel. Zorg rond architectuur voor een goede wisselwerking en ordening tussen open standaarden, open source tools en methodieken zoals IaC.
- **Draag relevante IaaS- en PaaS-standaarden uit de soevereine cloudarchitectuur aan** voor opname op de lijsten van Forum Standaardisatie, en help bij het in kaart brengen van de bijbehorende beheer- en intermediaire organisaties.
- **Verken de meerwaarde van een portabiliteit-mapping** van de lijsten van Forum Standaardisatie en overige relevante standaarden op het EU Cloud Sovereignty Framework. Dit kan bijdragen aan de ontwikkeling van een concrete portabiliteit-baseline.
- **Breng samen met betrokken partijen in kaart** wat nodig is om overheden daadwerkelijk in staat te stellen hun rol als launching customer te vervullen.

Aanbevelingen aan Tiido (MIDO):

- **Ondersteun het Forum Standaardisatie bij het prioriteren van portabiliteit-standaarden** voor opname op de lijsten.
- **Verken samen met het Forum Standaardisatie de ontwikkeling van een portabiliteitsarchitectuur**, die iteratief en adaptief kan meebewegen met technologische, juridische en marktontwikkelingen.
- **Draag bij aan de ontwikkeling van een technische portabiliteit-baseline**, in samenhang met het NDS Aanjaagteam Cloud en soevereiniteitsmodellen zoals het EU Cloud Sovereignty Framework. Kijk hierbij niet alleen naar IaaS, maar juist ook naar PaaS en SaaS.
- **Faciliteer kennisdeling, vroegsignalering en praktijkinput**, onder meer door use cases, lessons learned en opkomende standaarden actief te delen met het Forum Standaardisatie.

Aanbevelingen aan overheidsorganisaties / cloud-inkopers:

- Eis open standaarden voor portabiliteit bij inkoop.
- Eis migratie en exit-mogelijkheden, met de Data Act als juridisch kader.
- Voorkom afhankelijkheid van platform-specifieke diensten via koppelverkoop.
- Neem portabiliteit mee in architectuurkeuzes en lifecycle management.

11.3 Aanbevelingen aan het Forum Standaardisatie

Voor Forum Standaardisatie ligt de kernopgave in drie samenhangende rollen:

1) portabiliteit explicieter verankeren in het standaardenbeleid,

2) kansrijke standaarden prioriteren en toetsen, en

3) toepassing in de praktijk actief stimuleren.

Algemeen:

1. **Stimuleer actief de adoptie van portabiliteit-standaarden**, in samenwerking met de bovengenoemde stakeholders. Wacht daarbij niet op brede adoptie door de grootste marktpartijen of opname in het Europese standaardenregister, maar geef nationaal richting door relevante standaarden tijdig te agenderen, op te nemen en waar nodig te verplichten.
2. **Veranker cloud-portabiliteit expliciet in de beoordelingssystematiek van het Forum Standaardisatie.** Concreet wordt geadviseerd om het toetsingscriterium 'Leveranciersonafhankelijkheid' te verdiepen met een (sub)vraag in het expertadvies-template over de bijdrage van een standaard aan migratie of exit. Verken of de Europese scenario-gebaseerde CAMSS-systematiek hier handvatten voor biedt.
3. **Stuur actief op het gebruik van concrete open standaarden naast open source tools en methodieken.** Voorkom dat tooling of implementaties feitelijk de plaats van standaarden innemen zonder dat daar expliciete regie op wordt gevoerd.
4. **Ontwikkel een aanvullend beoordelingskader voor cloud-standaarden.** Het huidige toetsingskader biedt nog onvoldoende houvast voor het beoordelen van implementaties, profielen, open source tooling en de facto standaarden. Een aanvullend kader moet onderscheid maken tussen formele standaarden, technische specificaties, implementaties, tooling en architectuurkeuzes, en duidelijk maken welke daarvan zich lenen voor opname op de lijsten.
5. **Faciliteer de toetsing van cloud-aanbestedingen op open standaarden.** Ondersteun inkopende overheden met gerichte adviezen over welke standaarden bijdragen aan portabiliteit van data en applicaties, zodat afhankelijkheden van leveranciers worden beperkt en keuzevrijheid wordt vergroot.

Informatie/kennis:

6. **Volg de Europese normalisatie- en standaardisatieactiviteiten rond cloud-portabiliteit actief**, met name de ontwikkeling van het Europese standaardenregister, het standaardisatieverzoek **M/614** en eventuele aanvullende of opvolgende Europese standaardisatieverzoeken. Deze trajecten bepalen in belangrijke mate de toekomstige technische standaarden voor cloud-portabiliteit en interoperabiliteit.
7. **Richt een dynamisch kennisplatform in, of draag eraan bij dat dit elders tot stand komt.** Naast dit rapport is behoefte aan een actuele, publiek toegankelijke kennisomgeving met nieuwe standaarden, juridische en technische ontwikkelingen, praktijkvoorbeelden, marktinnovaties en governance-inzichten.

Definities & begrippen:

8. **Stimuleer dat cloud-portabiliteit wordt opgenomen in het landelijke cloudbegrippenkader.** Verzoek het NDS Aanjaagteam Cloud om in een volgende versie van de *Cloud definities en begrippenlijst* expliciet aandacht te besteden aan portabiliteit, cloudswitching en migratie.
9. **Onderzoek of het cloudbegrippenkader geschikt is voor opname op de 'Pas toe of leg uit'-lijst**, of dat hiervoor een afgeleide standaard nodig is. Uniforme definities zijn randvoorwaardelijk voor inkoop, architectuur en marktwerking, en kunnen daarmee de werking van een toekomstige cloudmarktplaats versterken.
10. **Indien portabiliteit niet tijdig in het begrippenkader wordt opgenomen, verken dan opname van ISO/IEC 19941** als referentie voor definities rond interoperabiliteit en portabiliteit van clouddiensten.

Aanbevelingen rond de primaire cloud-portabiliteit aandachtsgebieden

Aanbevelingen rond containers en orchestratie:

1. Verzoek VNG Realisatie om HAVEN aan te melden voor opname op de 'Pas-toe-of-leg-uit'-lijst en toetst op HAVEN geschikt is als open standaard.
2. Vraag de experts rond HAVEN ook naar overwegingen aan mogelijke Nederlandse indieners om image-spec, runtime-spec en distribution-spec van Open Container Initiative (OCI) en TOSCA (Topology and Orchestration Specification for Cloud Applications) en Helm Charts toe te voegen aan de lijst.

Aanbevelingen rond database-portabiliteit:

3. Onderzoek experts de haalbaarheid en praktische toegevoegde waarde van het verhogen van de status van SQL (ISO/IEC 9075) van de Aanbevolen-lijst naar de 'Pas toe of leg Uit'-lijst. Neem in overweging dat SQL mogelijk ook in het Europese standaardenregister komt en mogelijk verplicht wordt voor leveranciers.

Aanbevelingen rond sleutelmanagement:

4. Onderzoek met experts de haalbaarheid om de OASIS-standaard Key Management Interoperability Protocol (KMIP) op te nemen op de 'Pas toe of leg uit'-lijst, met als doel het verminderen van afhankelijkheden van leverancier-specifieke key management oplossingen.

Aanbevelingen rond identiteit- en toegangsbeheer:

5. Houd internationale standaardisatie-initiatieven op het gebied van Identity and Access Management actief in de gaten, met name subcommissie ISO/IEC JTC 1/SC 38 (Cloud computing and distributed platforms) waarin wordt gewerkt aan standaarden zoals de ISO/IEC AWI 10822-2 (Cloud computing - Multi-cloud management - Part 2: Identity management) standaard.
6. Stimuleer en monitor de adoptie van bestaande standaarden, en met name OAuth, voor identiteit en toegangsbeheer die al op de lijsten van Forum Standaardisatie staan. Dit vraagt eraan bij dat nieuwe cloud-portabiliteit-standaarden binnen dit domein goed kunnen aansluiten op een bestaande, gestandaardiseerde basis en de samenhang en interoperabiliteit binnen het domein worden versterkt.
7. Onderzoek de mogelijkheid en praktische toegevoegde waarde voor cloud-portabiliteit om SCIM (System for Cross-domain Identity Management) te herzien van aanbevolen naar Pas toe of leg uit.

Aanbevelingen voor standaarden in overige domeinen:

8. Onderzoek met experts de haalbaarheid en vooral de praktische toegevoegde waarde om in de Europese Wik-studie (zie paragraaf 3.4.3 en 9.2.2) naar voren gekomen standaarden JSON, OpenApi (OAS), XML, (reeds aanbevolen standaarden), eventueel SQL, en daarnaast CalDAV en WebDAV te opwaarderen naar verplichte standaarden ten behoeve van hun bijdrage aan cloud-portabiliteit.
9. Onderzoek met experts de haalbaarheid en vooral de praktische toegevoegde waarde om Apache Parquet, Apache Avro, Apache Iceberg, GraphQL en gRPC (zie ook paragraaf 9.2.1) op te nemen in de Aanbevolen lijst. Deze standaarden liggen buiten de aandachtsgebieden en/of bieden deeloplossingen voor portabiliteit-problemen.
10. Houd ontwikkelingen rond Sovereign European Cloud API (SECA) in de gaten. Deze door Europese cloud-aanbieders ontwikkelde standaard is in de WIK-studie prominent naar voren

gekomen. Echter het beheer lijkt niet geheel open en de adoptie is nog laag. Toch krijgt SECA relatief veel beleidsaandacht in Europa.

11. Breng eerst prioriteit aan in de standaarden genoemd onder aanbevelingen 11 en 12. De verwachting is dat niet elke standaard eventueel praktijk-impact heeft op cloud-portabiliteit. Stem prioriteit tussen deze standaarden af met experts. Een enquête onder experts kan bijvoorbeeld snel een beeld geven.

Overzicht acties per standaard:

Cluster	Actie
Containers (HAVEN, OCI, TOSCA, Helm Charts)	Actief aanjagen en prioriteren voor toetsing/opname
Sleutelbeheer (KMIP)	Haalbaarheid opname toetsen
Databases (SQL)	Opwaardering onderzoeken
IAM (OAuth, OIDC, SAML, SCIM)	Adoptie versterken; SCIM-opwaardering verkennen
JSON, XML, OAS, CalDAV, WebDAV,	Praktische toegevoegde waarde ophalen bij experts om van Aanbevolen-lijst op te waarderen naar verplicht.
Parquet, Avro, Iceberg, GraphQL, gRPC, SECA	Selectief monitoren, prioriteren en waar passend opnemen op de Aanbevolen-lijst

Overzicht bijlagen

Bijlage A Betrokkenen

In deze bijlage wordt een overzicht gegeven van de bij dit onderzoek betrokken personen.

Sponsorgroep

Een afvaardiging van de Sponsorgroep Markt en (Cloud)standaarden is in de beginfase (interviews) en bij de verdiepingsfase (sessie met experts) betrokken geweest bij dit onderzoek.

Naam	Functie/Rol	Organisatie
Guido Bayens	Voorzitter Architectuurraad Digitale Overheid	BZK
Anton Grootendorst	Concernstrateeg Digitalisering & Informatievoorziening	Provincie Utrecht
Michiel Steltman	Project Lead	ECP | Platform voor de InformatieSamenleving
Geert-Jan van de Ven	Directeur	CIP
Gino Laan	Directeur	Stichting RINIS

Tabel A1: Betrokken sponsorgroepleden

Experts

Bij het onderzoek zijn leveranciers en (indirecte) gebruikers van cloud-standaarden en -initiatieven betrokken. Tabel 2 toont de experts die betrokken zijn geweest bij het onderzoek in de interviewronde. Tabel 3 toont de experts die hebben deelgenomen aan de expertsessie.

Naam	Functie/Rol	Organisatie/Gremium
Bijkerk, Marco	Leveranciersmanager Red Hat voor RWS	Strategisch Leveranciersmanagement Rijksoverheid
Brouwer, Jacco	Beleidscoördinator cloud	VNG Realisatie
Graziano, Renzo	Programmamanager	IT Platform Twente
Guijt, Terry	Sr. Consultant	NEN
de Jong, Bart	IT Strategist & IT Architect	Gemeente Hengelo & IT Platform Twente
Jongeleen, Lotte	Projectleider Ontwikkeling	De BedrijfsvoeringsPartner
Peters, Holger	Strategisch Informatiemanager	Gemeente Baarn, initiatiefnemer Open WebConcept
van der Pol, Idsard	Beleidsmedewerker	CIO Platform
Kerssen, Ruud	Lead Security Expert European Cybersecurity Certification	RDI
Lascu, Andreea	Medewerker Toezicht	ACM
Mahieu-Arons, Sandra	Enterprise Architect	Bureau MIDO, BZK
Mous, Fabrice	Sales & Marketingmanager Benelux	Next Cloud GmbH

Salters, Marijke	Adviseur Digitale Transformatie	CIO Platform
Stroeven, Marisa	Sr. Consultant	NEN
Ver Loren Themaat, Ywen	Toezichthouder Data Economie	ACM
Zuurmond, Arre	Adviseur IT & informatiebeveiliging	ICTU

Tabel A2 - Betrokken experts (interview- en afstemrondes)

Naam	Functie/Rol	Organisatie
Ahaloui, Redouan	Senior Adviseur Standaardisatie	Bureau Forum Standaardisatie
van Heijningen, Dian	Product owner cloud	Wigo4it
Bos, Willem	Business Development Manager	Previder
de Jong, Bart	IT Strategist & IT Architect	Gemeente Hengelo & IT Platform Twente
Koks, Gerco	Chief architect	Centric
Laagland, Hans	Senior Adviseur Standaardisatie	Bureau Forum Standaardisatie
Laan, Gino	Directeur	Stichting RINIS
Ormeling, Ferjan	Strategisch medewerker cloud	CIO-Rijk
van der Voort, Joël	Cloud Native Platform Engineer	Previder

Tabel x - Betrokken experts (expertsessie)

Gremia

Naam	Context	Type deelnemers
Tiido werkgroep	MIDO, BZK	>10 architecten van verschillende overheidsorganisaties
Bureau Forum Standaardisatie medewerkers en management	Forum Standaardisatie	Experts op het gebied van verschillende soorten open standaarden

Tabel A3 – Betrokken gremia

Bijlage B Definities & Begrippen

In deze bijlage staan begrippen rond cloud en rond (algemene) standaarden toegelicht.

B.1 Wat is cloud en cloud computing?

Cloud is eigenlijk een Containerbegrip dat zowel kan verwijzen naar het leveren van **clouddiensten** via een cloudmodel als naar een specifieke instantie daarvan ("een cloud").

Het draait om de levering van rekenkracht, opslag en software via het internet. In plaats van eigen servers, huurt de overheidsorganisatie digitale infrastructuur bij gespecialiseerde leveranciers. In dit model neemt de leverancier de verantwoordelijkheid voor het beheer van IT-middelen. Organisaties worden zo “ontzorgd” en betalen voor wat ze gebruiken. Overheden hebben niet meer het eigendom van alle IT-middelen, maar huren IT als dienst vaak aangevuld met bijbehorende IT-tools en IT-ondersteuning vanuit de leverancier.

Cloud computing is een model dat het mogelijk maakt om plaats- en tijdsonafhankelijk, op een gemakkelijke manier en op afroep, via een netwerk, toegang te krijgen tot een voortdurend beschikbare, gedeelde verzameling van configureerbare computing resources die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met de **cloud-leverancier**. Deze definitie voldoet aan vijf essentiële karakteristieken:

- Op afroep beschikbare self-service
- Breed beschikbare toegang via netwerken
- Gedeelde computermiddelen
- Gemeten dienstgebruik
- Snelle schaalbaarheid

Computing resources zijn bijvoorbeeld netwerken, servers, besturingssystemen, opslag, applicaties en andere hogere-orde diensten.

B.2 Cloud servicemodellen IaaS, PaaS en SaaS

Om cloud-computing aan te bieden of te gebruiken zijn er verschillen cloud service-modellen op de markt. Zo’n **cloud service-model** beschrijft welke onderdelen van de IT-omgeving door de **cloud-aanbieder** worden geregeld en welke door de **cloud-afnemer.** Cloud servicemodellen worden ook wel cloud-capabilities of cloud stack genoemd. Cloud-servicemodellen worden op hoofdlijnen onderverdeeld in drie lagen: **Infrastructure-as-a-Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS)**. Deze varianten verschillen in waar welke verantwoordelijkheden liggen; bij de cloud-leverancier of bij de overheidsorganisatie. Conform de vastgestelde definities in het OBDO in 2026, definieert dit onderzoek ze als volgt:

- **Infrastructure as a Service (IaaS)** Verzameling **clouddiensten** waarbij verwerking, opslag, netwerken en andere fundamentele computing resources worden aangeboden waarmee de klant willekeurige software kan implementeren en draaien, zoals operating systems en applicaties. De cloud-afnemer voert geen beheer op de onderliggende infrastructuur noch op de interne werking van de geleverde clouddiensten. De cloud-afnemer beheert de besturingssystemen, opslag en geïmplementeerde applicaties. De cloud-afnemer beheert daarnaast mogelijk een beperkt deel van de netwerkcomponenten (bijvoorbeeld: firewalls).
- **Platform as a Service (PaaS):** Verzameling van clouddiensten waarop de cloud-afnemer eigen gemaakte applicaties of aangekochte applicaties kan implementeren. De cloud-afnemer voert geen beheer op de interne werking van de clouddiensten zoals netwerk, servers, besturingssystemen of opslag. De cloud-afnemer heeft controle over de

geïmplementeerde applicaties en mogelijke configuratie-instellingen voor de applicatie hosting omgeving.

- **Software as a Service (SaaS):** Verzameling clouddiensten in de vorm van een of meer voor eindgebruikers van de afnemer. De applicaties zijn toegankelijk vanaf verschillende clientapparaten via een thin clientinterface, zoals een webbrowser (bijvoorbeeld webgebaseerde e-mail) of een programmainterface. De cloud-afnemer beheert of controleert de onderliggende infrastructuur niet, noch netwerk, servers, besturingssystemen, opslag of zelfs individuele applicatiemogelijkheden, met de mogelijke uitzondering van beperkte gebruikerspecifieke applicatieconfiguratie-instellingen.

De aankoop en afname van clouddiensten vereist een expliciete afweging tussen de voordelen van uitbesteding en de mate van leveranciersafhankelijkheid. De verdeling van verantwoordelijkheden tussen cloud-leverancier en cloud-afnemer verschilt per cloud servicemodel en bepaalt in belangrijke mate de mate van ontzorging, controle, risico en de effecten op portabiliteit.

In de praktijk worden deze cloud service model definities niet strikt gehanteerd. Ze fungeren namelijk tevens als marketingtermen van aanbieders. Ook zijn er meerdere subvarianten.

B.3 Cloud gerelateerde begrippen, definities en hun bronnen

*Afkomstig uit de door het OBDO vastgestelde Cloud definities en begrippenlijst V1.0 en de bronnen die daarvoor zijn gebruikt.

Term	Definitie	Bron
Cloud	Containerbegrip dat zowel kan verwijzen naar het leveren van Diensten via een cloudmodel als naar een specifieke instantie daarvan ("een cloud").	*
Cloud computing	Model dat het mogelijk maakt om plaats- en tijdsonafhankelijk (ubiquitous), op een gemakkelijke manier (convenient) en op afroep (on-demand), via een netwerk (network access), toegang te krijgen tot een voortdurend beschikbare, gedeelde verzameling van configureerbare computing resources die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met de cloudaanbieder. Deze definitie voldoet aan vijf essentiële karakteristieken: - Op afroep beschikbare self-service - Breed beschikbare toegang via netwerken - Gedeelde computermiddelen - Gemeten dienstgebruik - Snelle schaalbaarheid Computing resources zijn bijvoorbeeld netwerken, servers, besturingssystemen, opslag, applicaties en andere hogere-orde diensten.	* NIST 800-145 ISO/IEC 17788:2016 (R2021) ISO 22123-1:2023 NVN / CEN/TS 18026:2024 CSA Rijksbreed cloudbeleid 2022 RORA

Cloudaanbieder of Aanbieder, cloud provider (NIST), Cloudleverancier, Clouddienstverlener, Cloud Service Provider (ISO)	Rechtspersoon of onderdeel daarvan die Clouddienst(en) aanbiedt aan een Afnemer en daarmee een leveringsafspraak onderhoudt.	* Cloud supplier in NIST 800-145 en NIST 500-292
Cloudafnemer of afnemer, cloud consumer, service consumer	Rechtspersoon of onderdeel daarvan die Clouddienst(en) afneemt van een Cloudaanbieder en daarmee een leveringsafspraak onderhoudt.	* 'Cloud consumer in NIST 800-145, NIST 500-292
Cloud native	Zodanige toepassing van cloud technologie dat een workload schaalbaar kan draaien in moderne, dynamische omgevingen zoals publieke, private en hybride cloud.	* Cloud Native Computing Foundation (CNCF)
Cloud switching	het proces waarbij een gebruiker data, applicaties en/of diensten overdraagt van de ene cloudserviceprovider naar een andere, of terug naar een eigen (on-premise) omgeving.	Data Act + ISO/IEC19 94:2017
Cloud-portabiliteit	het vermogen om data, applicaties en diensten tussen cloudomgevingen of aanbieders te verplaatsen zonder substantiële aanpassingen, functionaliteitsverlies of afhankelijkheid van specifiek leveranciersgedrag.	ISO/IEC 1994:2017
Cloud-interoperabiliteit	het vermogen van clouddiensten, systemen of componenten om informatie uit te wisselen en deze informatie wederzijds te gebruiken	SO/IEC 19941 (Interoperability and portability) ISO/IEC 22123 (Cloud computing concepts and vocabulary)
Data-portabiliteit	het vermogen om data van het ene systeem of de ene omgeving naar een andere over te dragen en daar te gebruiken, met behoud van bruikbaarheid, structuur en betekenis.	ISO/IEC 1994:2017
Applicatie-portabiliteit	het vermogen om een applicatie van de ene omgeving naar een andere te verplaatsen en daar te laten functioneren, met minimale aanpassingen en zonder verlies van functionaliteit.	ISO/IEC 1994:2017

Cloud Servicemodel	Het cloud servicemodel (ook wel cloud stack) onderscheidt drie hoofdtypen van clouddiensten: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS), die elk een verschillend niveau van abstractie en beheer door de gebruiker vertegenwoordigen.	
Cloud stack	de cloud stack een technische lagenstructuur die beschrijft waarin die services (zie cloud services modellen) zich bevinden. (Vaak wordt de cloud service model terminologie hiervoor gehanteerd in de praktijk.)	
Multi-cloud	het gelijktijdig gebruik van clouddiensten van meerdere cloudserviceproviders binnen één organisatie.	
Publieke cloud of Public cloud, publieke cloudvoorziening	Verzameling clouddiensten die is ingericht voor open gebruik door het algemene publiek.	* RORA, NIST 800-145
Private cloud of Private cloudvoorziening	Verzameling clouddiensten die is ingericht voor exclusief gebruik door één organisatie die bestaat uit meerdere interne cloudafnemers.	* RORA, NIST 800-145
Infrastructure as a Service of IaaS	Verzameling Clouddiensten waarbij verwerking, opslag, netwerken en andere fundamentele computing resources worden aangeboden waarmee de klant willekeurige software kan implementeren en draaien, zoals operating systems en applicaties. De Cloudafnemer voert geen beheer op de onderliggende infrastructuur noch op de interne werking van de geleverde clouddiensten. De Cloudafnemer beheert de besturingssystemen, opslag en geïmplementeerde applicaties. De Cloudafnemer beheert daarnaast mogelijk een beperkt deel van de netwerkcomponenten (bijvoorbeeld: firewalls).	* NIST 800-145
Platform as a Service of PaaS	Verzameling van Clouddiensten waarop de Afnemer eigen gemaakte Applicaties of aangekochte Applicaties kan implementeren. De Afnemer voert geen beheer op de interne werking van de clouddiensten zoals Netwerk, Servers, besturingssystemen of Opslag. De Afnemer heeft controle over de geïmplementeerde	* RORA, NIST 800-145

	Applicaties en mogelijke configuratie-instellingen voor de applicatie hosting omgeving.	
Software as a Service of SaaS	Verzameling clouddiensten in de vorm van een of meer voor eindgebruikers van de Afnemer. De Applicaties zijn toegankelijk vanaf verschillende clientapparaten via een thin clientinterface, zoals een webbrowser (bijvoorbeeld webgebaseerde e-mail) of een programmainterface. De Cloudafnemer beheert of controleert de onderliggende infrastructuur niet, noch netwerk, servers, besturingssystemen, opslag of zelfs individuele applicatiemogelijkheden, met de mogelijke uitzondering van beperkte gebruikerspecifieke applicatieconfiguratie-instellingen.	* RORA, NIST 800- 145
On-premise	Op een fysieke locatie waar de afnemende organisatie controle heeft over de fysieke plaatsing en beveiliging van informatietechnologie(-apparatuur) voor verwerking, -opslag en netwerk.	* RORA
Workload	Binnen de context van cloud computing is dit een onderscheidbare capaciteit of eenheid van werk die clouddiensten benut, bijbehorende software en data omvat en specifieke non functional requirements kan hebben. Dit kan één applicatie zijn, een verzameling van applicaties of een andersoortige deel daarvan. Workloads zijn zeer divers in omvang, scope, tijd dat ze aaneengesloten draaien, ontwerp en in de eisen die ze stellen aan de clouddiensten die ze benutten. Ze worden dus vaak in groepen op basis van dergelijke aspecten gegroepeerd die samen vergelijkbare clouddiensten benutten of in een gezamenlijke landingszone draaien. Voorbeeld: Eindgebruiker applicatie, functionaliteit draaiend in één container, een clouddienst, eindgebruiker werkplek, compleet ERP pakket, een database	* IBM
Soevereine clouddienst	Verzameling clouddiensten binnen het eigen rechtsgebied die voldoet aan de eisen voor datalocalisatie en operationele autonomie. De soevereine cloud moet ervoor zorgen dat de data, activiteiten, infrastructuurcomponenten en technologie niet kunnen worden beïnvloed door andere rechtsgebieden en beschermd moeten worden tegen directe invloed of toegang door overheden uit derde landen	* Non paper EU

B.4 Standaarden, normen en geharmoniseerde normen

In de dagelijkse praktijk worden termen zoals standaard, specificatie of norm vaak door elkaar gebruikt. Juridisch en procedureel bestaan er echter belangrijke verschillen. Onderstaande zijn afkomstige uit: *De cloud en de Nederlandse rechtsorde: Groningse perspectieven*.

Wat zijn standaarden?

Een standaard is een regel, richtlijn of kenmerk die een bepaald doel dient en die vaak een technische implementatie kent. De term verwijst zowel naar het concept van uniformiteit als naar het document waarin de specificatie is vastgelegd. Volgens Verordening (EU) 1025/2012 beschrijft een technische ICT-specificatie de eisen waaraan een product, proces of dienst moet voldoen. In de context van cloudcomputing kan dit variëren van koppelvlakdocumentatie tot API-ontwerpregels zoals de REST API Design Rules.

Wat zijn normen?

Een norm is een standaard die is opgesteld door een erkende normalisatie-instelling (men noemt dit ook wel een Standards Developing Organization, ofwel SDO), zoals ISO (mondiaal), CEN/CENELEC/ETSI (Europees) of NEN (nationaal). Normen worden ook wel *formal standards* genoemd in het Engels. (Vandaar ook de begripsverwarring die kan optreden indien een Nederlander in een internationaal gezelschap spreekt over ‘standards’ in gevallen waarbij het juist niet gaat om een norm die afkomstig is van een erkende normalisatie-instelling.) Conformiteit met een norm biedt vaak een vermoeden van overeenstemming met wettelijke eisen, bijvoorbeeld onder de EU Data Act of de NIS2-richtlijn. Normen kunnen bovendien dienen als basis voor certificering.

Veel ICT-standaarden komen echter niet uit normalisatie-instellingen, maar uit internationale consortia zoals W3C, IETF of OASIS. Bekende voorbeelden zijn HTTPS en IPv6. Hoewel deze formeel geen norm zijn, hebben ze internationale marktimpact en kunnen ze worden opgenomen op de lijsten van Forum Standaardisatie.

Wat zijn geharmoniseerde normen?

Geharmoniseerde normen zijn Europese technische specificaties ontwikkeld door CEN, CENELEC en ETSI op verzoek van de Europese Commissie. Die specificaties vertalen een bestaande wettelijke eis naar meer concrete (technische) regels. Het opvolgen van zo’n specificatie zorgt voor een ‘vermoeden van overeenstemming’ met de na te leven wettelijke verplichting, waardoor de bewijslast af zal nemen.

Kortom: Elke geharmoniseerde norm is een norm. Elke norm is een standaard. Maar niet elke standaard is een norm, en niet elke norm is geharmoniseerd.

B.5 Wat zijn open standaarden?

Wanneer is een standaard een open standaard? Dat is een belangrijke vraag voor dit onderzoek, want het Forum Standaardisatie plaatst enkel open standaarden op haar lijsten.

Nederlandse definitie van open standaarden

Het Forum Standaardisatie hanteert binnen Nederland een eigen, duidelijk afgebakende definitie van een open standaard. Deze houdt nauw verband met de criteria binnen van het Europese CAMSS. Voor Nederland is de NORA het NIF. De mate van alignment tussen NORA en EIF is sterk en wordt jaarlijks gemonitord. Een standaard komt in aanmerking voor opname op de lijsten van Forum Standaardisatie wanneer: stakeholders voldoende inspraakmogelijkheden hebben bij de ontwikkeling of doorontwikkeling; het gebruik van de standaard niet is onderworpen aan octrooirechten of andere beperkende licentievoorwaarden; en de documentatie vrij of tegen een redelijke vergoeding beschikbaar is. Deze (toetsings-)criteria moeten voorkomen dat gebruikers afhankelijk worden van één leverancier of technologie.

De Nederlandse Overheid Referentie Architectuur (NORA) en de Wet digitale overheid (Wdo) benadrukken het belang van interoperabiliteit, openheid en het gebruik van open standaarden. De lijsten van Forum Standaardisatie vormen daarbij een belangrijk instrument om deze principes in de praktijk te brengen.

Ook in cloud-contracten is het gebruik van open standaarden daarom een belangrijke maatregel tegen vendor lock-in. Conformiteit met een proprietary standaard — zoals een specifieke API van een hyperscaler — kan lock-in juist versterken, terwijl open standaarden dit proberen te doorbreken.

Voorbeelden van items die zich niet lenen als open standaard voor toetsen op openheid volgens Forum Standaardisatie zijn de FAIR data principes en NL Design Systems. (Voor details zie onderzoek FAIR dataprincipes, 2020, InnoValor, i.o.v. Bureau Forum Standaardisatie.) Een standaard moet namelijk een technische specificatie zijn die concreet voorschrijft hoe iets werkt of moet worden geïmplementeerd. Dus:

- er moet een specificatiedocument zijn;
- met normatieve regels;
- die interoperabiliteit mogelijk maken; en
- die door meerdere partijen implementeerbaar zijn.

Als iets géén technische specificatie is, maar een principe, richtlijn, ontwerpfilosofie of governance-model, dan valt het automatisch buiten scope voor de lijsten van Forum Standaardisatie. De lijsten van Forum Standaardisatie bevatten uitsluitend technische specificaties, met normatieve inhoud, die interoperabiliteit bevorderen en die voldoen aan de open-standaardcriteria.

B.6 De facto of industrie-standaarden: standaard door gebruik

Een de facto standaard is een standaard die niet formeel is vastgesteld of goedgekeurd door een erkende standaardisatieorganisatie, maar die in de praktijk breed wordt toegepast en daardoor als standaard gaat functioneren. In het cloud-domein gaat het hierbij onder andere om open- en closed-source tools, softwareoplossingen, platformen en andere implementaties. Open-source implementaties kwalificeren daarbij niet automatisch als open standaard; dit dient per geval te worden beoordeeld, bijvoorbeeld op basis van governance, open beheer en beschikbaarheid van specificaties.

In het cloud-domein ontstaan veel technische specificaties binnen open-source communities en samenwerkingsverbanden rond platforms en ecosystemen. Door de vaak minder formele governance-structuren zijn deze lastiger te kwalificeren als standaard in juridische of beleidsmatige zin. Dit doet echter niets af aan hun praktische relevantie: juist deze technologieën spelen een belangrijke rol in interoperabiliteit en portabiliteit in de praktijk.

Voorbeelden hiervan zijn technologieën uit het CNCF-ecosysteem, zoals Kubernetes, Prometheus en Helm, en Apache-projecten zoals Kafka, Parquet en Avro. Deze functioneren in feite als de facto standaarden: hun status is niet gebaseerd op formele standaardisatie, maar op brede adoptie en gebruik in de markt.

Bijlage C Verdieping op facetten van portabiliteit

Deze bijlage biedt een nadere verdieping van de verschillende aspecten van portabiliteit zoals beschreven in ISO/IEC 19941:2017. Daarbij wordt zowel ingegaan op data-portabiliteit als applicatie-portabiliteit. Ter illustratie van de praktische betekenis en uitdagingen van portabiliteit worden daarnaast enkele (analyses op) praktijkvoorbeelden uitgewerkt.

C.1 Data portabiliteit

Facet 1: Data-syntax

Het syntactische facet (ofwel de structuur van data) betreft het kunnen overdragen van data door middel van machine-leesbare dataformaten die kunnen worden ontcijferd op het doelsysteem. Voorbeelden hiervan zijn gangbare en open bestandsformaten en packaging-formaten. Een open standaard voor bestandsformaten op de lijsten van Forum Standaardisatie is bijvoorbeeld CSV. Dit zijn veelgebruikte formaten voor het exporteren en importeren van gegevens tussen verschillende systemen. Ze worden breed ondersteund en maken het eenvoudig om gestructureerde gegevens te verplaatsen.

Dataformaten spelen een essentiële rol binnen het mogelijk maken van data-portabiliteit (zowel in de cloud of niet in de cloud), omdat het syntactisch mogelijk maken van data-portabiliteit een voorwaarde is voor het semantisch mogelijk maken van data-portabiliteit. Het is niet mogelijk om de betekenis van gemigreerde data te achterhalen als het dataformaat na migratie niet meer kan worden uitgelezen.

Voorbeeld: Een dataset met klantgegevens wordt geëxporteerd als CSV-bestand. Omdat CSV een open en gangbaar formaat is, kan het bestand zonder problemen worden ingelezen in een ander systeem. Als dezelfde data in een propriëtair of onbekend formaat zou staan, is het mogelijk dat het doelsysteem de data niet kan lezen. In dat geval kan de data technisch niet worden overgezet en gaat ook de betekenis van de gegevens verloren.

Facet 2: Data-semantiek

Het semantische facet (ofwel de betekenis van data) betreft het overdragen van data op zo'n manier dat de betekenis van de data wordt door het doelsysteem wordt begrepen. Dit wordt doorgaans weergegeven in een datamodel[2], waarin data-elementen, hun onderlinge relaties en logische structuren worden beschreven. Voorbeelden hiervan zijn semantische modellen en beschrijvingstalen zoals OWL (Aanbevolen standaard), evenals schema's zoals en OWMS of Dublin Core schema.

Voorbeeld: In een database is "klant_id = 123" gewoon een klantnummer. In een applicatie betekent dit dat het om een specifieke gebruiker gaat met bepaalde inlogrechten in het klantportaal. Op businessniveau staat hetzelfde nummer voor een klantrelatie, bijvoorbeeld een organisatie met een contract.

Semantische standaarden zijn echter niet in staat om deze betekenis volledig vast te leggen. De structuur en het gedrag van systemen, zoals SQL-databases of complexe XML-structuren, laten zich niet altijd volledig modelleren in een taal als OWL. Dit illustreert dat semantische interoperabiliteit slechts een deel van het portabiliteit-vraagstuk afdekt en nauw samenhangt met syntactische en structurele aspecten van data.

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

De manier waarop data wordt beschreven – het datamodel – verschilt per laag in de IT-architectuur, en daarmee ook de betekenis (semantiek) van die data. De IT-stack bestaat grofweg uit infrastructuur (servers, opslag), platform (middleware, databases), applicaties (SaaS-diensten) en de businesslaag (processen en informatie). Elke laag gebruikt data op een andere manier en hanteert eigen modellen en structuren.

In de praktijk kan semantiek (betekenis) en syntax (structuur) niet volledig los van elkaar worden gezien, zo is opgemerkt door één van de experts. Dat is ook merkbaar bij de ordening van standaarden: er zijn standaarden die combineren syntactische en semantische elementen. Zo beschrijft SQL niet alleen hoe data wordt opgeslagen, maar ook de onderlinge relaties en betekenis binnen het datamodel, terwijl XML via schema's (zoals XSD) eveneens structuur en deels betekenis vastlegt.

Facet 3: Data-beleid

Het beleidsfacet beschrijft dat het mogelijk is om data te migreren in overeenstemming met de geldende wettelijke, organisatorische en beleidsframeworks. Hierbij kan gedacht worden aan waar de data staat opgeslagen, wie er toegang tot heeft, of bepaalde informatiebeveiligingseisen.

Voorbeeld: Een organisatie wil klantdata migreren naar een andere cloud-omgeving. Technisch is dat mogelijk, maar een deel van de data mag volgens beleid alleen binnen de EU worden opgeslagen en is alleen toegankelijk voor geautoriseerde medewerkers. Als de nieuwe cloud-omgeving hier niet aan voldoet, kan de migratie niet worden uitgevoerd, ook al is deze technisch haalbaar.

C.2 Applicatie-portabiliteit

Facet 1: Applicatie-syntax

Applicaties moeten zodanig worden verpakt, overgedragen en geconfigureerd dat zij in een andere cloud-omgeving opnieuw kunnen worden ingezet zonder verlies van functionaliteit. Vergelijkbaar met syntactische data-portabiliteit betreft dit facet de wijze waarop een applicatie technisch wordt voorbereid voor overdraagbaarheid en heruitvoering in een doelsysteem.

Dit omvat onder meer de packaging van applicaties, maar ook de afhankelijkheden, configuraties en runtime-aspecten die nodig zijn om de applicatie opnieuw te kunnen uitvoeren. In moderne cloud-omgevingen spelen hierbij containerisatie en gestandaardiseerde deployment-mechanismen een belangrijke rol (zie hoofdstuk 6 voor meer informatie).

Voorbeelden van eenvoudige packaging-formaten zijn zip, tar of jar-bestanden, maar in de praktijk worden deze vaak aangevuld met meer geavanceerde mechanismen voor deployment en orchestratie. Hierbij zijn met name packaging, deliverY, OCI registries (image distribution) en security, ISO/IEC 27001 (informatiebeveiliging algemeen), container signing (bijv. Cosign in OCI ecosystem) relevant. Voor applicaties zijn bekende voorbeelden van packaging-formaten bijvoorbeeld zip, tar of jar.

Voorbeeld: Een applicatie wordt verpakt als een standaard ZIP- of containerbestand en bevat alle benodigde onderdelen. Hierdoor kan deze eenvoudig worden verplaatst en opnieuw worden gestart in een andere cloud-omgeving. Als de applicatie echter afhankelijk is van een specifiek platformformaat of beveiligingsmechanisme van één cloud-leverancier, kan het doelsysteem deze niet goed uitpakken of uitvoeren.

De grootste belemmeringen voor cloud-migraties liggen in de praktijk niet in de overdraagbaarheid van applicaties zelf, maar in het kunnen borgen van non-functionele eisen (NFR's) binnen een nieuwe cloud-omgeving, zo merken experts op.

Voorbeeld: Een organisatie kan de eis hebben om alle logginggegevens van de afgelopen 7 jaar beschikbaar te houden, bijvoorbeeld een loggingdatabase van 100 TB. Dit type eis heeft geen

betrekking op de functionaliteit van de applicatie zelf, maar op compliance, archivering en auditbaarheid. Bij migraties blijkt juist dit soort eisen vaak problematisch: het overzetten en opnieuw inrichten van zulke grote datasets is technisch complex en kostbaar. In de praktijk komt het voor dat dergelijke eisen in een noodsituatie (bijvoorbeeld een verplichte migratie) tijdelijk worden versoepeld of losgelaten, omdat zij migratie aanzienlijk bemoeilijken.

Facet 2: Applicatie-instructie

Applicatie-instructies moeten zo worden gespecificeerd en uitgevoerd dat de instructieset en orchestratiescripts op het bronsysteem ook functioneel equivalent uitvoerbaar zijn op het doelsysteem, ongeacht de onderliggende cloud-omgeving of infrastructuur. Het instructiefacet van applicatie-portabiliteit schrijft voor dat de instructieset van de applicatie op het bronsysteem ook uitvoerbaar moet zijn op het doelsysteem. De orchestratie-instructies moeten geïnterpreteerd kunnen worden en de scripts gerund, op een manier die functioneel equivalent is aan het bronsysteem. Deze applicatie-instructies worden omschreven in technische programmeertalen, zoals bijvoorbeeld C# of Java.

Voorbeeld: Een applicatie wordt uitgerold met behulp van deployment-scripts (bijvoorbeeld in Kubernetes of via Infrastructure-as-Code). Als deze scripts gebruikmaken van generieke en gestandaardiseerde instructies, kunnen ze ook worden uitgevoerd in een andere cloud-omgeving. Als de scripts echter afhankelijk zijn van specifieke functies of instellingen van één cloud-platform, moeten ze worden aangepast voordat de applicatie opnieuw kan worden ingezet.

Standaarden zoals OCI, Helm, TOSCA en Haven (zie ook hoofdstuk 6) adresseren verschillende facetten van applicatie-portabiliteit. Waar OCI zich primair richt op het packaging-aspect (syntaxis), richten Helm en TOSCA zich op de uitvoering en orchestratie van applicaties (instructie). Implementaties zoals Haven combineren deze facetten gedeeltelijk, maar tonen tegelijkertijd dat volledige portabiliteit in de praktijk afhankelijk is van een samenhangende toepassing van meerdere standaarden.

Facet 3: Applicatie-metadata

Applicatie-metadata moet zó worden gestructureerd en overgedragen dat informatie over de werking, afhankelijkheden en configuratie van de applicatie door het doelsysteem kan worden geïnterpreteerd en toegepast, zodat de applicatie in een nieuwe omgeving functioneel correct kan worden geïnitialiseerd en uitgevoerd. Metadata voor applicaties beschrijft de omgeving en werking van de applicatie. Ook deze metadata van een applicatie moet portabel zijn om een applicatie goed te laten werken in een nieuwe omgeving. Het facet metadata beschrijft dat de afhankelijkheden van de applicatie, zoals welke resources het gebruikt of hoe deze geïnitialiseerd moet worden, ook moet kunnen worden geïnterpreteerd door het doelsysteem. Metadata voor applicaties wordt vaak in XML, JSON of YAML-formaat (alle drie onderdeel van de lijsten van Forum Standaardisatie) gestructureerd.

Voorbeeld: Een gemeente draait een applicatie voor vergunningverlening. In de metadata is vastgelegd dat de applicatie een specifieke database gebruikt, verbinding maakt met een berichtenservice en bepaalde beveiligingsinstellingen nodig heeft. Deze informatie staat in een YAML-bestand. Als de gemeente overstapt naar een andere cloud-omgeving, kan het nieuwe platform deze metadata lezen en de juiste database, verbindingen en instellingen automatisch opnieuw configureren. Als deze metadata ontbreekt of alleen werkt voor één specifieke cloud-leverancier, moet de omgeving handmatig opnieuw worden ingericht, met risico op fouten en verstoringen van de dienstverlening.

Facet 4: Applicatie-gedrag

Het gedrag van een applicatie moet zo consistent en reproduceerbaar blijven dat de applicatie in een nieuwe omgeving functioneel hetzelfde resultaat oplevert als in de oorspronkelijke omgeving, waarbij ook test suites, applicatiecomponenten en ondersteunende services verplaatsbaar en uitvoerbaar zijn binnen de nieuwe context, zonder verlies van functionele gelijkwaardigheid. Applicatie-gedrag is

complex en in de praktijk vaak een probleem. De essentie is de applicatie zich hetzelfde moet gedragen en dezelfde resultaten moet kunnen opbrengen in een nieuwe omgeving. Voorbeelden van aspecten zijn dat test suites, applicatie- en ondersteunende services moeten mee-gemigreerd kunnen worden. De code waarin de applicatie geschreven is open moet zijn zoals C# of Java.

Voorbeeld: Een overheidsorganisatie draait een applicatie voor uitkeringsbeheer. Na migratie naar een andere cloud-omgeving moet het systeem dezelfde berekeningen uitvoeren, aanvragen op dezelfde manier verwerken en dezelfde uitkomsten geven. Hiervoor worden ook de testscripts en ondersteunende services (zoals berichtenverwerking en authenticatie) mee gemigreerd. Als deze niet goed werken in de nieuwe omgeving, kan de applicatie afwijkende resultaten geven of fouten veroorzaken, wat direct impact heeft op de dienstverlening aan inwoners.

Facet 5: Applicatie-beleid

Net als bij data-portabiliteit is het ook bij applicatie-portabiliteit van belang dat er rekening wordt gehouden met de geldende beleidsframeworks en verordeningen. Beleid en beleidskaders moeten zo worden meegenomen in applicatie-portabiliteit dat toepasselijke regelgeving, governance-vereisten en licentiebeperkingen - inclusief geografische restricties - in een nieuwe omgeving worden herkend en nageleefd, zodat de inzet van de applicatie in een andere cloud-omgeving juridisch en contractueel toegestaan blijft. Bij applicaties kan dit bijvoorbeeld ook slaan op licenties die niet afgegeven worden aan bepaalde landen.

Voorbeeld: Een overheidsorganisatie gebruikt een applicatie voor subsidieverlening die alleen mag draaien binnen de EU en waarbij specifieke licentievoorwaarden gelden voor gebruik van bepaalde softwarecomponenten. Bij migratie naar een andere cloud-omgeving moet worden gecontroleerd of deze omgeving binnen de toegestane regio valt en of de licenties daar geldig zijn. Als dat niet het geval is, mag de applicatie juridisch of contractueel niet worden ingezet, ongeacht of dit technisch mogelijk is.

C.3 Portabiliteit in de praktijk

Om het onderwerp concreter en herkenbaar te maken voor de praktijk binnen de overheid, worden in deze paragraaf enkele use-cases uitgewerkt. Deze zijn mede tot stand gekomen in samenwerking met het Tiido (MIDO).

In deze paragraaf worden drie praktijksituaties geschetst:

1. migratie naar een nieuw SaaS-HR-systeem;
2. migratie naar een aankomende soevereine overheidscloud; en
3. migratie van legacy-systemen naar de cloud.

Het doel van deze paragraaf is om het thema portabiliteit tussen clouddiensten te illustreren aan de hand van concrete en herkenbare voorbeelden uit de praktijk.

Praktijk: migratie naar een nieuw SaaS HR-systeem

De overheid koopt regelmatig nieuwe SaaS-diensten: Software as a Service. Voor diverse SaaS-applicaties, zoals HR-systemen en Content Management Systemen (CMS), is het reeds voor overheden gebruikelijk om eens in de paar jaar (einde aanbesteding) te migreren, een andere oplossing aan te besteden en in gebruik te nemen. Binnen deze pratijkcases brengen we data-portabiliteit en applicatie-portabiliteit naar voren:

- **Data-portabiliteit:** In de aanbesteding is er een ander merk HR-systeem geselecteerd. De cloud-afnemer (bijvoorbeeld een gemeente) wisselt dan van software. Daarbij moet de data uit het HR-systeem worden gemigreerd van SaaS-systeem A naar SaaS-systeem B. Vaak is het uitvoeren van de migratie van de data-onderdeel van de aanbesteding en wordt dit grotendeels uitgevoerd door de nieuwe SaaS-leverancier.

- **Applicatie-portabiliteit:** Een overheidsorganisatie besteedt een nieuwe HR SaaS-pakket aan; de software en het platform waar deze software op draait is onderdeel van de inkoop (net zoals in het voorbeeld hierboven). De overheidsorganisatie heeft echter de wens om het nieuwe HR-systeem niet meer bij een Amerikaans hyperscaler te laten draaien, maar wil het een nieuwe soevereine overheidscloud draaien. De oude SaaS-leverancier doet mee in de aanbesteding. Deze kan 1) de applicatie geheel opnieuw neerzetten op het platform(PaaS-laag) of 2) de bestaande HR-applicatie migreren naar de nieuwe soevereine overheidscloud. In dat laatste geval komt applicatie-portabiliteit (ook) naar voren. In deze situatie moet de HR SaaS-leverancier zijn eigen software op een ander cloud-platform gaan aanbieden om aan de eisen van de inkopende overheidsorganisatie te voldoen. Kortom, de HR SaaS-leverancier migreert de applicatie naar een andere clouddienst en/of ander platform.

Vaak wordt ondersteuning in de migratie mee aanbesteed, waarbij de nieuwe leverancier dit technisch uitvoert. Afhankelijk van de mate van portabiliteit rekent de leverancier lagere of hogere kosten hiervoor door. Ook is het mogelijk dat de oude leverancier kosten (egress fees).

Praktijkcase: migreren naar de aankomende soevereine overheids-cloud

In het kader van de NDS wordt de ontwikkeling van een soevereine overheidscloud als een strategische prioriteit aangemerkt. Voor het welslagen van dit initiatief is het essentieel dat overheidsorganisaties hun bestaande datasets en applicaties zonder belemmeringen kunnen migreren naar deze nieuwe omgeving. Hierbij speelt het thema portabiliteit een cruciale rol. De technische en financiële realiseerbaarheid van een overstap – de zogenaamde switch – bepaalt in aanzienlijke mate straks de effectiviteit van de soevereine cloud. Bij gebrek aan data en applicatie portabiliteit uit de huidige omgevingen ontstaat het risico dat de soevereine overheidscloud onderbenut blijft.

Cloud-soevereiniteit is immers alleen realiseerbaar wanneer zowel de onderliggende infrastructuur als de applicaties overdraagbaar zijn. Zolang applicaties niet eenvoudig kunnen worden gemigreerd, blijft de overstap naar soevereine cloud-omgevingen in de praktijk beperkt, ongeacht de beschikbaarheid van dergelijke infrastructuur.

Om de beoogde digitale soevereiniteit daadwerkelijk te effectueren, moet de portabiliteits-drempel voor uittreding uit commerciële cloud-omgevingen worden geminimaliseerd. Alleen wanneer portabiliteit als randvoorwaarde is geborgd, kan de soevereine overheidscloud optimaal worden ingezet voor de maatschappelijke opgaven waarvoor deze is bedoeld.

Praktijk: legacy systemen zijn een moderniseringsvraagstuk

Legacysystemen vallen buiten de scope van dit onderzoek. Dit onderzoek richt zich op cloud-native standaarden en toepassingen en de portabiliteit tussen clouddiensten. De migratie van legacysystemen is niet primair een vraagstuk van portabiliteit, maar vereist doorgaans een ingrijpende moderniseringsslag waarbij architectuur, technologie en processen fundamenteel worden aangepast. Hier komen mogelijk ook andere standaarden bij kijken.

In de praktijk is legacy echter zeer relevant. Experts geven aan dat het overgrote deel van overheids-IT draait in traditionele legacy-omgevingen of hybride. Hierdoor vormt legacy een belangrijke randvoorwaarde voor cloudk-euzes binnen de Nederlandse overheid. De vraag op welke wijze open standaarden kunnen bijdragen aan portabiliteit van deze legacy-systemen is daarmee zeker relevant in het kader van de beleidsdiscours op digitale autonomie, maar ligt buiten de scope van dit onderzoek.

Om cloud-portabiliteit te realiseren moeten data en systemen eerst cloud-native worden gemaakt. Dit vraagt om aanzienlijke inspanning van overheidsorganisaties. Het risico ontstaat daarmee dat de benodigde moderniseringsslag onvoldoende tempo heeft, waardoor cloud-portabiliteit in de praktijk niet wordt gerealiseerd, ongeacht de bijdrage van portabiliteit-standaarden en leveranciers-afhankelijkheden gewoon blijven bestaan.

Nieuwe technologische ontwikkelingen bieden inmiddels gedeeltelijke overbruggingsmogelijkheden. Zo maken oplossingen zoals virtualisatie op containerplatformen (bijvoorbeeld KubeVirt) het mogelijk om bestaande VM-gebaseerde applicaties te draaien binnen een cloud-native beheeromgeving. Hiermee kunnen legacy-systemen deels meebewegen richting cloudbeheer, zonder dat directe herbouw noodzakelijk is. Deze oplossingen bieden echter geen volledige cloud-native eigenschappen, zoals optimale schaalbaarheid en portabiliteit tussen platformen.

C.4 Hoe zou je cloud-portabiliteit kunnen meten?

Er is geen uniform meetmodel voor cloud-portabiliteit beschikbaar, maar er zijn wel relevante aanknopingspunten, zoals het EU Cloud Sovereignty Framework en mogelijk bestaande methoden voor het meten van business continuïteit. Deze modellen dekken het cloud-portabiliteit vraagstuk niet volledig, maar bieden een praktisch vertrekpunt om de portabiliteit van data en applicaties te duiden, te vergelijken en te beoordelen. Onderstaande schetsen we twee methodisch handvatten:

1. Binnen het Cloud Sovereignty Framework wordt de schaal wat explicieter gemaakt. Portabiliteit is daarin geen doel op zichzelf, maar een belangrijk onderdeel van meerdere soevereiniteitsdimensies. Het vermogen om data/workloads te migreren, systemen zelfstandig te exploiteren en afhankelijkheden van leveranciers te beperken, vormt daar een expliciet beoordelingscriterium. Hogere niveaus van soevereiniteit vereisen daarmee aantoonbaar hogere niveaus van portabiliteit. Het Cloud Sovereignty Framework komt nader aan bod in hoofdstuk 3 van dit rapport.
2. Daarnaast kan de mate van ‘cloud switch-baarheid’ mogelijk worden geobjectiveerd vanuit een business continuity-perspectief (aldus één van de betrokken experts in dit onderzoek). Waar traditioneel wordt gewerkt met indicatoren zoals Recovery Time Objective (RTO) en Recovery Point Objective (RPO), kan voor cloud-portabiliteit mogelijk een vergelijkbaar begrip worden geïntroduceerd: het Switch Time Objective (STO). STO beschrijft de tijd waarbinnen een organisatie daadwerkelijk moet kunnen overstappen naar een alternatieve cloud-leverancier om de continuïteit van dienstverlening te waarborgen. Dit zou onderdeel kunnen zijn van weerbaarheid- en cloud-exit strategieën. STO gaat echter breder dan de mate van cloud-portabiliteit, want STO gaat ook veel over hoe goede een organisatie bijvoorbeeld kennis en processen klaar heeft om te switchen als het moet. Ook lijkt is concept TSO meer gericht op crisismanagement, dan op switchen als onderdeel van normale inkoop en marktwerking.

Omdat de mate van portabiliteit sterk situatie-specifiek is, gaat dit onderzoek niet verder in op de meetbaarheid en schaal van portabiliteit.

C.5 Relaties met actuele thema’s

Deze paragraaf beschrijft hoe cloud-portabiliteit zich verhoudt tot open standaarden, cloud-interoperabiliteit, soevereine cloud, multi- en hybride cloud-strategieën en BIO-compliance. Dit schetst een beeld over hoe cloud-portabiliteit gepositioneerd kan worden tussen deze actuele thema’s.

Wat is de relatie tussen open standaarden en cloud-portabiliteit?

Open standaarden zijn een sleutelvoorwaarde voor cloud-portabiliteit. Zonder open standaarden zijn cloud-omgevingen vaak gebaseerd op leverancierssspecifieke technologieën en API’s. Dit maakt overstappen kostbaar en risicovol en leidt tot vendor lock-in. Open standaarden vergroten de technische portabiliteit, maar garanderen niet automatisch cloud-switching want daar komen bijvoorbeeld ook contractafspraken bij kijken.

Een standaard wordt in dit onderzoek relevant voor portabiliteit geacht wanneer zij concreet en direct bijdraagt aan het vermogen van de cloud-afnemer om technisch over te stappen naar een andere

cloud-leverancier. (Potentiële) open standaarden die niet specifiek aan cloud computing zijn gekoppeld, zijn slechts beperkt meegenomen.

Bijvoorbeeld: Toepassing van open en gestandaardiseerde dataformaten vergroten de kans dat data na import in een ander softwaresysteem correct en consistent blijft functioneren. Dit geldt ongeacht of de ontvangende applicatie als SaaS of via een andere leveringsvorm wordt afgenomen.

Wat is de relatie tussen cloud-interoperabiliteit en cloud-portabiliteit?

Cloud-interoperabiliteit garandeert geen cloud-portabiliteit. Gebruik van cloud-interoperabiliteit standaarden geeft dus ook geen garantie voor portabiliteit. Interoperabiliteit betekent dat cloud-systemen of clouddiensten met elkaar kunnen samenwerken. Interoperabiliteit maakt zo samenwerking mogelijk, maar het betekent niet automatisch dat verplaatsen ook eenvoudig is. Een applicatie kan bijvoorbeeld met meerdere cloud-omgevingen communiceren, terwijl deze toch afhankelijk blijft van leverancierspecifieke configuraties die migratie lastig maken.

Wat is de relatie tussen cloud-portabiliteit en de soevereine cloud?

Meer cloud-portabiliteit maakt het eenvoudiger om van cloud-aanbieder te wisselen, ongeacht of het gaat om een overstap tussen Amerikaanse cloud-leveranciers, naar on-premise, naar een Europese aanbieder naar een overheidsdatacentrum of soevereine cloud. Het doel van dit onderzoek is om al deze overstappen mogelijk te maken. Door cloud-portabiliteit te vergroten met behulp van open standaarden, neemt het vermogen van overheden wel flink toe om daadwerkelijk over te stappen naar een soevereine (overheids)cloud.

Wat is de relatie met multi-cloud en hybride-cloud strategieën?

Cloud-portabiliteit hangt samen met multi-cloud en hybride-cloudstrategieën, maar volgt daar niet automatisch uit. In de praktijk sluiten organisaties vaak meerdere cloudcontracten af, maar gebruiken zij per applicatie meestal slechts één cloudomgeving. Bij een multi-cloudstrategie gebruikt een organisatie meerdere cloud-aanbieders. Organisaties kiezen hiervoor om gebruik te maken van ‘best-of-breed’-diensten van verschillende cloud-leveranciers, voor hun verschillende applicaties. Dit betekent dat applicaties doorgaans niet zonder meer overdraagbaar zijn naar een andere aanbieder.

Het hebben van meerdere cloud-contracten kan het overstappen (cloud switching) wel eenvoudiger maken vanuit inkoop- en contractperspectief. Technisch blijft migratie echter even complex, omdat applicaties, data en configuraties vaak specifiek zijn ingericht voor één cloud-omgeving.

Experts schatten in dat slechts een zeer beperkt deel van de organisaties multi- of hybride cloud zodanig ingericht dat systemen daadwerkelijk tussen cloudomgevingen kunnen worden verplaatst. Echte portabiliteit vereist expliciete technische inrichting, ondersteund door open standaarden en leverancier-onafhankelijke architecturen.

Wat is de relatie met BIO-compliance, en regelt dat portabiliteit?

BIO-compliance ondersteunt cloud-portabiliteit, maar regelt deze niet automatisch. De (herziene) BIO stelt eisen aan onder meer beschikbaarheid, continuïteit, gegevensbescherming en exit-maatregelen, zoals het kunnen terughalen van data bij beëindiging van een contract. Dit draagt bij aan een gecontroleerde en veilige migratie. Het garandeert echter niet dat data, applicaties en functionaliteit eenvoudig naar een andere cloud-aanbieder kunnen worden overgezet.
BIO-compliance richt zich immers primair op risicobeheersing en continuïteit, en minder op technische overdraagbaarheid tussen omgevingen. Daarmee vormt BIO2 een noodzakelijke randvoorwaarde voor portabiliteit, maar geen voldoende garantie. Voor daadwerkelijke cloud-portabiliteit zijn aanvullende technische en architecturale maatregelen nodig, met name het gebruik van open standaarden en leverancier-onafhankelijke ontwerpen.

Bijlage D Beleids-stacks

Deze bijlage bevat overzicht van diverse ‘stacks’, zoals gevraagd in de opdracht voor dit onderzoek. De geïnventariseerde stacks zijn: Public Stack, Stackmodel Digitale Economie, Sovereign Cloud Stack, OpenStack en EuroStack. Voor elke stack wordt een beschrijving gegeven.

D.1 Overzicht stacks

Model	Type	Wat brengt het wel	Wat brengt het niet	Relevantie voor portabiliteit
Public Stack	Beleids-/maatschappelijk model	Benadrukt publieke waarden, openheid en afhankelijkheden	Geen standaarden, geen technische uitwerking	Indirect (agenderend)
IEM / Stackmodel Digitale Economie	Beleids-/economisch analysekader	Maakt marktmacht en afhankelijkheden zichtbaar	Geen technische standaarden of oplossingen	Indirect (analyse & beleid)
EuroStack	Strategisch EU-beleid	Positioneert autonomie en open standaarden als doel	Geen concrete standaarden of implementatie	Indirect (strategie)
Sovereign Cloud Stack (SCS)	Referentie-architectuur (open source)	Concrete open cloud stack (OpenStack/Kubernetes), standaardisatie infra	Geen generieke portabiliteit tussen clouds, beperkt hoger dan IaaS.	Ja. Primair relevant voor IaaS. Minder voor andere lagen.
OpenStack	Open-source platform	Open infrastructuur, API-gedreven, vendor-onafhankelijk	Geen standaard, geen end-to-end portabiliteit	Beperkt. Platform specifiek. Gericht op IaaS.

D.2 Public Stack

Beschrijving

De Public Stack is een conceptuele beleidsstack die gebruikt kan worden als leidraad bij het adopteren van open-source cloud-infrastructuur, specifiek binnen de publieke sector. Het is een beleidsstack die de burger en publieke waarden centraal stelt bij het ontwikkelen van technologie, waarbij het zinspeelt op ethics-by-design. Volgens PublicStack is het belangrijk dat er, voordat er een (cloud-)infrastructuur geïmplementeerd kan worden, aan bepaalde ‘bouwstenen’ wordt voldaan, zoals het democratiseren van de governance over digitalisering en het identificeren van alle stakeholders, maar ook het meenemen van burgers in het designproces. Public Stack wordt expliciet genoemd in het Plan van Aanpak Markt en Open (Cloud)standaardisatie van het Forum Standaardisatie. Het is een beleidsstack die met name focust op het centraal stellen van publieke waarden bij het designen van cloud-infrastructuur. Hierbij wordt benadrukt dat een open designproces en het gebruiken van open-source technologieën essentieel is. Data-portabiliteit hoort hier impliciet bij, maar wordt niet genoemd. De Public Stack is ontwikkeld door Waag binnen het onderzoeksproject Online European Public Spaces (OEPS), gefinancierd door de Adessium Foundation i.s.m. de European Cultural Foundation, en wordt gebruikt door de Gemeente Amsterdam en het initiatief Hollandse Luchten, en in opdracht van de RVO is PublicStack ook gebruikt om de publieke EV-laadinfrastructuur te analyseren.

Relaties met open standaarden

Public stack is echt een beleidsframework en schrijft dus geen concrete standaarden voor. Wel onderschrijft het in meer conceptuele vorm dezelfde waarden (portabiliteit, voorkomen van vendor lock-in), door de nadruk die ligt op het centraal stellen van de burger en democratisering van governance over digitalisering.

Relaties met andere stacks/ontwikkelingen

Public Stack is, net zoals EuroStack en het Stackmodel Digitale Economie, een analytisch beleidsmodel. Het is meer gericht op publieke waarden dan het Stackmodel Digitale Economie, dat meer focust op de economische positie die Nederland in kan nemen door het voeren van verschillende soorten beleid rondom Stacks. Het verschilt van het EuroStack-initiatief door het ontbreken van nadruk op Europese soevereiniteit. Er wordt nadrukkelijk gekeken vanuit het perspectief van de burger, in plaats van de (economische) positie van Nederland of Europa.

D.3 Stackmodel Digitale Economie

Beschrijving

Het Stackmodel Digitale Economie is een analytische beleidsstack. Het is een beschrijving van een technologische stack, met ‘daarbovenop’ nog 3 lagen die benadrukken hoe de digitale stack-technologieën onze samenleving transformeren. De cloud bevindt zich in de ‘zachte infrastructuur’ laag van het stackmodel. Voor deze laag worden decentralisering en data-liquiditeit (wat begrepen kan worden als data-portabiliteit) genoemd als voornaamste beleidsuitdagingen. Wat betreft decentralisering erkent het model dat gebruikers leveranciersafhankelijk zijn geworden. Als mogelijke oplossing hiervoor wordt Web3 genoemd, het gedecentraliseerde web. Web3 komt vanuit de cryptocurrency en heeft als doel om meer open-source te werken, maar bijvoorbeeld ook om block-chain beter te gebruiken. Wat betreft data-liquiditeit noemt het model dat data ongehinderd moet kunnen stromen naar de plekken waar het waarde kan creëren binnen de digitale economie. De huidige leveranciersafhankelijkheid wordt mede veroorzaakt door gebrek aan kennis, infrastructuur, afspraken en regelgeving van Nederlandse of Europese bodem. Meer algemeen benadrukt het model dat de manier waarop we digitaliseringsbeleid voeren (mission-oriented vs marktgericht) en de mate van adoptie (radicaal vs incrementeel) van invloed zijn op hoe Europa zich kan positioneren op de digitale economische markt. Het stellen van standaarden zoals bij dit onderzoek hoort bij een mission-oriented aanpak. Het Stackmodel Digitale Economie wordt expliciet genoemd in het Plan van Aanpak van het Forum Standaardisatie. Het is een brede beleidsstack die deels focust op decentralisatie en data-portabiliteit van de zachte infrastructuurlaag, waar de cloud onderdeel van is. Data-portabiliteit in het specifiek wordt niet genoemd. Het beheer wordt gedaan door het Ministerie van Economische Zaken en Klimaat, al is de Stack ontwikkeld door Freedom Lab.

Relaties met open standaarden

Omdat het Stackmodel Digitale Economie een beleidsstack is heeft het geen directe relatie met open standaarden op de Lijst, maar het onderschrijft wel het belang van datasoevereiniteit (en daarmee van data-portabiliteit).

Relaties met andere stacks/ontwikkelingen

Het Stackmodel Digitale Economie is, net zoals EuroStack en PublicStack, een analytisch beleidsmodel waarin digitale systemen worden ontleed in verschillende deeltechnologieën met als doel om de relatie ertussen te duiden. Het is dus niet zo concreet als OpenStack of Sovereign Cloud Stack. Het focust zich in het kader van decentralisatie voornamelijk op Web3, en in het kader van data-liquiditeit voornamelijk op Europese wetgeving.

D.4 Sovereign Cloud Stack

Beschrijving

Sovereign Cloud Stack (SCS) is een open-source, door Open Source Business Alliance e.V. ontwikkeld initiatief voor het definiëren van een open en transparant Europees cloudplatform waarbij interoperabiliteit en datasoevereiniteit centraal staan. Portabiliteit en leveranciersonafhankelijkheid zijn hierbij belangrijke speerpunten.

SSC bundelt en gebruikt een mix van open standaarden (zoals OCI, OVF, TOSCA), implementaties (OpenStack, Kubernetes), en tooling (Terraform, Ansible) om een Europese, veilige en portabele cloud stack te realiseren.

Het doel van SCS is tweeledig: enerzijds definieert het een set van 51 duidelijke om de bovengenoemde waarden te waarborgen (inclusief een certificeringsframework voor cloudproviders), anderzijds biedt SCS ook een referentie-implementatie aan, wat een voorbeeld is van een volledig cloudplatform die is samengesteld uit componenten (IaaS, containers, IAM en Ops) die allen voldoen aan de door SCS opgestelde standaarden. Deze referentie-implementatie wordt ook genoemd in de Domeininfrastructuur clouddiensten Digitale Overheid. Digitale soevereiniteit en het vermijden van leveranciersonafhankelijkheid zijn één de voornaamste speerpunten van Sovereign Cloud Stack. SCS waarborgt cloudinteroperabiliteit en -portabiliteit door het gebruiken van open-source technologieën van aanbieders als OpenStack en Kubernetes. SCS promoot een federatief cloudmodel, wat in lijn ligt met de Domeininfrastructuur clouddiensten Digitale Overheid. Het beheer van SCS wordt gedaan door het SCS projectteam, dat werkt voor het Open Source Business Alliance e.V., een verband dat wordt gefinancierd door het Duitse Ministerie voor Economie en Klimaatactie (BMWK). De standaarden zelf worden onderhouden en ontwikkeld door een actieve internationale community. Er zijn veel initiatieven die bepaalde standaarden van SCS gebruiken, zoals de Deutsche Verwaltungscloud, het cloudplatform dat wordt gebruikt door Duitse overheidsorganisaties. De referentie-implementatie van SCS wordt gebruikt in het GovStack infrastructuur bouwblok.

Relaties met open standaarden

De SCS-standaarden bevatten normatieve bepalingen voor API-beschrijving (OpenAPI), transportbeveiliging (TLS/HTTPS), DNS-functionaliteit en SSO-federatie, maar kiezen daarbij bewust voor minimale interoperabiliteitsafspraken en laten expliciete portabiliteit van IAM-modellen, DNSSEC en sleuteluitwisseling grotendeels open.

De standaarden die door SCS worden geformuleerd komen veelal overeen met standaarden op de ‘pas toe of leg uit’-lijst van het Forum. Sovereign Cloud Stack definieert 51 standaarden. Voor een aantal standaarden zijn er concrete overeenkomsten, zoals OpenAPI Specification (OAS) in scs-0402 *(Status page OpenAPI decision)* en TLS, HTTPS, HSTS in scs-0125 (Secure Connections). Specifiek rond de aandachtgebieden:

- IAM-standaarden In SCS:
    - scs-0300 - Requirements for SSO identity federation specificeert SSO-federatie-eisen. Het definieert eisen voor SSO-federatie en ondersteunt OIDC, OAuth 2.0 en SAML, met OIDC als primaire referentie-implementatie via Keycloak[3].
    - scs-0302- Domain Manager configuration for Keystone: Keystone is de Identity & Access Management (IAM)-dienst van OpenStack.

[3] Keycloak is een open-source Identity & Access Management (IAM)-platform dat wordt gebruikt voor authenticatie, autorisatie en Single Sign-On (SSO) voor applicaties en cloud-diensten.Het wordt veel ingezet in cloud-, Kubernetes- en OpenStack-omgevingen, waaronder binnen de Sovereign Cloud Stack.

Op het vlak van IAM kiest SCS niet voor normering van portabele IAM-modellen. Het blijft provider-/implementatie-specifiek. IAM wordt niet als zelfstandige interoperabiliteitsstandaard gedefinieerd. SCS veronderstelt IAM als randvoorwaarde binnen OpenStack/Kubernetes: RBAC is verplicht toegepast. Federatie/SSO wordt geaccepteerd, maar niet genormeerd (geen OIDC-profielen, geen portabele rollenmodellen).

- **Key management:** SCS lost sleutelbeheer binnen één cloud op, maar geen portabiliteit van sleutels tussen clouds; geen verplicht gebruik van KMIP of vergelijkbare inter-cloud protocollen. Gerelateerde scs-standaard:
    - SCS Key Manager Standard (scs-0116) verplicht de aanwezigheid van een Key Manager op IaaS-niveau. SCS schrijft functionele vereisten voor sleutelbeheer voor, waaronder: scheiding tussen KEK / Master-KEK, RBAC op sleuteltoegang, Bescherming van de Master-KEY (bij voorkeur HSM-backed), abstractie van backend-plugins. Referentie-implementatie: OpenStack Barbican (maar techniek is uitwisselbaar).
- **Databases:** Databases vallen buiten scope van SCS.
- **Containers & orchestratie: SCS definieert KaaS-standaarden** scs-0200 tot en met scs-0219, met onder andere verplichte Scs-201: CNCF Kubernetes conformance voor interoperabiliteit (cloud-providers kunnen aantonen dat hun KaaS API- en gedragscompatibel is. Essentieel voor portabiliteit van workloads.)
- gestandaardiseerde cluster-API's (Cluster API (CAPI), Cluster Stacks),voor uniforme lifecycle- en beheerafspraken.

Relaties met andere stacks/ontwikkelingen

Sovereign Cloud Stack is aanbieder van een volledig cloudplatform (referentie-implementatie) als een concreet standaardisatieframework. Het aanbieden van een *volledig* platform maakt het anders dan OpenStack, wat alleen IaaS aanbiedt. Het aanbieden van concrete standaarden inclusief certificering daarvoor maakt het anders dan pure beleidsstacks als EuroStack, PublicStack en het Stackmodel Digitale Economie.

D.5 OpenStack

Beschrijving

OpenStack is een open-source IaaS-platform dat organisaties in staat stelt om publieke, private en hybride clouds te bouwen. Het wordt beheerd door de non-profit organisatie Open Infrastructure Foundation, die inzet op open standaarden, interoperabiliteit en leveranciersonafhankelijkheid. OpenStack ondersteunt een modulaire architectuur met flexibele componenten en maakt gebruik van open API's voor resourcebeheer. OpenStack wordt wereldwijd vooral toegepast door grote bedrijven, telecomproviders en serviceproviders die behoefte hebben aan een robuuste cloudinfrastructuur die kan worden aangepast aan hun specifieke behoeften. OpenStack wordt vooral toegepast door grote organisaties omdat zij kunnen beschikken over de vereiste specialistische kennis en een eigen solide basisinfrastructuur. Bekende gebruikers binnen de Nederlandse en Europese overheid zijn ODC Noord, welke OpenStack met Ceph combineert voor schaalbare infrastructuur, maar ook in andere Europese landen als Frankrijk wordt OpenStack gebruikt binnen bijvoorbeeld het Ministerie van Binnenlandse Zaken.

Relaties met open standaarden

OpenStack maakt, als open-source technologie, veel gebruik van standaarden. Zo ondersteunt het standaarden als JSON, XML en CSV, en biedt het goede integraties met de facto industriestandaarden als Kubernetes, Docker en Ceph. Ook worden er open API's gebruikt voor resourcebeheer.

Relaties met andere stacks/ontwikkelingen

OpenStack is, in tegenstelling tot Eurostack, Public Stack en het Stackmodel Digitale Economie, geen beleidsinitiatief. Het is een IaaS-platform dat open source infrastructuurdiensten aanbiedt. Ook schrijft het niet, zoals Sovereign Cloud Stack, concrete standaarden voor. OpenStack implementeert juist de door initiatieven als Sovereign Cloud Stack voorgeschreven standaarden: de referentie-implementatie van Sovereign Cloud Stack gebruikt dan ook OpenStack in haar IaaS-toepassingen.

D.6 EuroStack

Beschrijving

EuroStack is een analytische bedrijfsstack. Het is eind 2024 ontwikkeld, en heeft als voornaamste doel om een soeverein, open en interoperabel Europees digitaal ecosysteem te ontwikkelen, om de gehele technologische stack heen. Op deze manier kan de Europese marktpositie ten opzichte van de VS en China versterkt worden. Eén van de manieren om dit te bereiken is bijvoorbeeld het 'Buy European' initiatief, waarbij bedrijven gestimuleerd worden om zich te committeren aan Europese leveranciers. Het uiteindelijke doel is om ook EuroStack-certificeringen uit te kunnen geven. De EuroStack bestaat uit drie brede levels, waarbij cloud zich op het middelste level bevindt. Het beheer van de EuroStack is in handen van een voor dat doel opgerichte stichting: EuroStack Initiative Foundation e.V.. Deze stichting, opgezet door Europese tech-CEO's (zoals die van Ecosia en Signal) is dan wel ontstaan uit een conferentie in het Europees Parlement, maar is dus geen formeel EU-orgaan.

Relaties met open standaarden

Omdat de EuroStack een beleidsstack is heeft het geen directe relatie met open standaarden op de Lijst, maar vanwege de nadrukkelijke focus op soevereiniteit en het vermijden van vendor lock-in kan worden gesteld dat deze waarden wel worden onderschreven. Bovendien wordt er wél expliciet verwezen naar frameworks als NIS2, die zouden kunnen optreden als handvaten voor de kopers van EuroStack-gecertificeerde initiatieven.

Relaties met andere stacks/ontwikkelingen

EuroStack is, net zoals het Stackmodel Digitale Economie en PublicStack, een pure beleidsstack. Er worden geen concrete standaarden voorgescheven, zoals bij Sovereign Cloud Stack, en er wordt geen concrete dienst geleverd, zoals bij OpenStack. Wel wordt de EuroStack vaak ook gelinkt aan Gaia-X, een eerder Europees initiatief (wel technologisch) dat specifiek gericht is op het realiseren van een meer soevereine Europese cloud. Dit initiatief wordt echter ook wel gezien als iets waar Big Tech toch zijn stempel op heeft kunnen drukken, en dus wordt EuroStack gezien als de doorstart daarvan.

Bijlage E Longlist standaarden

Deze bijlage bevat een overzicht van de verschillende soorten items die door experts zijn benoemd en in de deskresearch naar voren zijn. Het is een longlist met een ruwe ordening.

Legenda bij de tabel

Cloud Service Model:

- IaaS = Infrastructure as a Service
- PaaS = Platform as a Service
- SaaS = Software as a Service
- Dwarsdoorsnijdend / Anders = relevant over meerdere lagen heen of niet eenduidig aan één servicemodel toe te wijzen

Type & Status:

- Formele norm = norm van een formele normalisatieorganisatie (bijv. ISO/IEC, ETSI, CEN/CENELEC)
- Technische specificatie = open specificatie of standaard, vaak beheerd door een consortium of community
- Implementatie / platform / tooling = technische oplossing of softwareproject, geen formele standaard
- Methodiek / framework / gedragscode = ondersteunend instrument, geen technische standaard
- FS PTLU = staat op de 'Pas toe of leg uit'-lijst
- FS Aanbevolen = staat op de lijst Aanbevolen standaarden
- FS In procedure = in procedure voor opname / wijziging op de lijsten

Standaard / item	Cloud Service Model	Functioneel domein	Type & status
AES	Dwarsdoorsnijdend	Encryptie	Technische standaard – FS Aanbevolen
Amazon S3 API	IaaS / PaaS	Object storage / data-opslag	De facto specificatie / interface
Ansible	Dwarsdoorsnijdend	Configuratiebeheer / automatisering	Implementatie / tooling
Apache Avro	PaaS	Data-uitwisseling / schema-evolutie / streaming	Technische specificatie
Apache Iceberg	PaaS	Data lake-tabellen / metadata / lakehouse	Technische specificatie
Apache Parquet	PaaS / IaaS	Open dataformaat / analytics / data lakes	Technische specificatie
AsyncAPI	PaaS / SaaS	Eventgedreven API-beschrijving	Technische specificatie
CalDAV	SaaS / PaaS	Agenda-uitwisseling / synchronisatie	Technische specificatie – FS Aanbevolen
CEN/TS 18026:2024	Dwarsdoorsnijdend	Cloud cybersecurity	Technische specificatie – FS In procedure

CISPE Switching Framework	IaaS / PaaS	Cloud switching	Framework
CloudEvents	PaaS / SaaS	Event-interoperabiliteit	Technische specificatie
Containerd	PaaS	Container runtime	Implementatie / tooling
CSV	Dwarsdoorsnijdend	Gegevensuitwisseling	Technische specificatie – FS Aanbevolen
Data Transfer Project	SaaS	Data-overdracht tussen diensten	Technische specificatie
Docker	PaaS	Containers / packaging	Implementatie / tooling
ETSI Dataspace specifications	Dwarsdoorsnijdend	Dataspace-interoperabiliteit	Technische specificatie
FIDO	SaaS / Dwarsdoorsnijdend	Authenticatie	Technische specificatie
GraphQL	PaaS / SaaS	API-querylaag / interoperabiliteit	Technische specificatie
gRPC	PaaS	Service-tot-service communicatie	Technische specificatie
HAVEN	PaaS	Kubernetes-configuratie / portabiliteit / platformonafhankelijke hosting	Implementatiestandaard / profiel
Helm	PaaS	Kubernetes deployment / packaging	Implementatie / tooling
Helm Charts	PaaS	Declaratieve packaging- en deploymentbeschrijving	Specificatie / artefact (de facto)
Infrastructure as Code (IaC)	Dwarsdoorsnijdend	Herhaalbare infrastructuurconfiguratie	Methodiek
IPsec	Dwarsdoorsnijdend	Netwerkbeveiliging	Technische standaard – FS Aanbevolen
ISO/IEC 11179	Dwarsdoorsnijdend	Metadataregistratie / data-catalogi	Formele norm
ISO/IEC 17203 (OVF)	IaaS / PaaS	VM packaging / migratie	Formele norm
ISO/IEC 17788	Dwarsdoorsnijdend	Cloudterminologie	Formele norm
ISO/IEC 17826 (CDMI)	IaaS / PaaS	Cloudopslag / datamigratie	Formele norm
ISO/IEC 17888-1 (TOSCA)	PaaS	Applicatiedeployment / orchestratie	Formele norm / technische specificatie *(controleer exacte referentie)*
ISO/IEC 19941	Dwarsdoorsnijdend	Cloudinteroperabiliteit & portabiliteit	Formele norm

ISO/IEC 19944	Dwarsdoorsnijdend	Datastromen / datacategorieën	Formele norm
ISO/IEC 22123-1/2/3	Dwarsdoorsnijdend	Cloudbegrippen / referentiearchitectuur	Formele norm
ISO/IEC 22301	Dwarsdoorsnijdend	Continuïteit / uitwijk	Formele norm
ISO/IEC 24760 (reeks)	Dwarsdoorsnijdend	Identity & access management	Formele norm
ISO/IEC 27001	Dwarsdoorsnijdend	Informatiebeveiliging	Formele norm – FS PTLU
ISO/IEC 27002	Dwarsdoorsnijdend	Informatiebeveiliging	Formele norm – FS PTLU
ISO/IEC 27017	IaaS / PaaS / SaaS	Cloud security controls	Formele norm
ISO/IEC 27018	SaaS	Bescherming persoonsgegevens in de cloud	Formele norm
JAR	Dwarsdoorsnijdend	Packaging / overdracht	Technische specificatie
JSON	Dwarsdoorsnijdend	Data-uitwisseling / API's	Technische specificatie – FS Aanbevolen
KMIP	Dwarsdoorsnijdend / PaaS	Key management / sleutelbeheer	Technische specificatie (OASIS)
Kubernetes	PaaS	Containerorchestratie	De facto standaard / implementatie
Liqo.io	PaaS	Multicluster / Kubernetes-interoperabiliteit	Implementatie / tooling
MongoDB	PaaS	NoSQL-database	Implementatie / platform
NL GOV Assurance Profile for OAuth 2.0	SaaS	Publiek IAM-profiel / API-autorisatie	Technische specificatie – FS PTLU
NoSQL	PaaS	Niet-relationele databases	Categorie / implementatie-ecosysteem
OAuth 2.0	SaaS / PaaS	IAM – autorisatie / API-toegang	Technische specificatie – FS Aanbevolen
OAI-PMH	Dwarsdoorsnijdend	Metadata harvesting / data-catalogi	Technische specificatie
OCCI	IaaS	Cloud resource management	Technische specificatie
OData	PaaS / SaaS	API-bevraging / data-ontsluiting	Technische specificatie

Open Container Initiative (OCI)	PaaS	Container images / runtimes / distributie	Technische specificatie
OpenAPI Specification (OAS)	PaaS / SaaS	API-beschrijving / interoperabiliteit	Technische specificatie – FS Aanbevolen
OpenID Connect	SaaS / PaaS	IAM – authenticatie	Technische specificatie
OpenID.NLGov	SaaS / PaaS	Publiek IAM-profiel / authenticatie	Technische specificatie – onderdeel authenticatiestandaarden FS PTLU
OpenStack	IaaS	Cloudinfrastructuurplatform	Implementatie / platform
OpenTelemetry	Dwarsdoorsnijdend	Observability / logging / tracing	Technische specificatie / community-standaard
OpenTofu	Dwarsdoorsnijdend	Infrastructure as Code	Implementatie / tooling
Redfish DMTF DSP0243	IaaS	VM / hardware / resourcebeheer	Technische specificatie
Redfish DMTF DSP0263	IaaS	Cloudinfrastructuurbeheer	Technische specificatie
REST (architectuurstijl)	Dwarsdoorsnijdend	API-architectuur	Architectuurstijl / specificatie
REST API Design Rules	Dwarsdoorsnijdend	API-ontwerp / uniformiteit	Technische specificatie – FS PTLU
SCIM	SaaS / PaaS	IAM – identity provisioning	Technische specificatie – FS Aanbevolen
SCS-0116-v1 Key Manager Standard	PaaS / Dwarsdoorsnijdend	Key management	Technische specificatie / profiel
SCS-0125 TLS/HTTPS	Dwarsdoorsnijdend	Veilige verbindingen	Technische specificatie / profiel
SCS-0127 DNS	IaaS / Dwarsdoorsnijdend	Naamresolutie / netwerk	Technische specificatie / profiel
SCS-0201 Kubernetes Conformance	PaaS	Kubernetes-conformiteit	Technische specificatie / profiel
SCS-0300 SSO Federation (OIDC)	SaaS / PaaS	IAM / federatie	Technische specificatie / profiel
SCS-0402 OpenAPI	PaaS / SaaS	API-beschrijving	Technische specificatie / profiel
SECA	IaaS / PaaS	Europese cloud-API-laag	Technische specificatie
SHA-2	Dwarsdoorsnijdend	Authenticatie / integriteitscontrole	Technische standaard – FS Aanbevolen

S/MIME	SaaS / Dwarsdoorsnijdend	E-mailbeveiliging	Technische standaard – FS Aanbevolen
SNIA CDMI	IaaS / PaaS	Data-opslag / migratie	Technische specificatie
SQL (ISO/IEC 9075)	PaaS (DBaaS)	Relationele databases	Formele norm – FS Aanbevolen
SWIPO Codes of Conduct	SaaS / PaaS	Cloudswitching / exit	Gedragscode
TAR	Dwarsdoorsnijdend	Packaging / overdracht	Technische specificatie
Terraform	Dwarsdoorsnijdend	Infrastructure as Code	Implementatie / tooling
TLS	Dwarsdoorsnijdend	Beveiligde gegevensuitwisseling / transportbeveiliging	Technische standaard – FS PTLU
WebAuthn	SaaS / Dwarsdoorsnijdend	Authenticatie	Technische specificatie
WebDAV	SaaS / PaaS	Bestandsuitwisseling / documenttoegang	Technische specificatie – FS Aanbevolen
XML	Dwarsdoorsnijdend	Data-uitwisseling	Technische specificatie – FS Aanbevolen
ZIP	Dwarsdoorsnijdend	Data packaging / overdracht	Technische specificatie – FS Aanbevolen