DigiD / Solvinity / Kyndryl — Feitelijke Analyse

Stand van zaken april 2026 | J. Konstapel

---

1. De architectuur: wie doet wat

De publieke discussie is onnauwkeurig omdat de technische lagen door elkaar worden gehaald. De feiten zijn:

Laag	Eigenaar/beheerder	Wat het inhoudt
DigiD software & authenticatielogica	Logius (overheid)	Applicatiecode, BSN-koppeling, wachtwoorden, PIN-codes, authenticatieprotocollen
Applicatiebeheer	Logius	Gebruikersrechten en toegangscontrole op applicatieniveau; intellectuele eigendomsrechten bij de Staat
PICARD platform	Solvinity (technisch beheer)	IaaS + PaaS: virtuele machines, netwerken, disk storage, containers, object storage
Datacenter (housing)	Overheids Datacenter (odc)	Fysieke locatie — welk specifiek odc is nooit openbaar gemaakt door Logius

Kernpunt: Solvinity beheert uitsluitend de infrastructuurlaag. De applicatie, de authenticatielogica en de gebruikersdata zijn eigendom van en worden beheerd door de Nederlandse overheid. Solvinity heeft operationeel alleen toegang tot IP-adressen en e-mailadressen van DigiD-gebruikers — uitsluitend voor het technisch functioneren van het platform.

---

2. De contractuele situatie

- **Augustus 2020**: Logius gunt contract aan Solvinity voor bouw en beheer van PICARD (infrastructuurdiensten voor DigiD, MijnOverheid, Digipoort).
- **Initiële looptijd**: 4 jaar → einde eind 2024, daarna eerste verlengingsoptie van 2 jaar gelicht → loopt tot medio/eind **2026**.
- Er ligt nog een **tweede verlengingsoptie** (nogmaals 2 jaar → potentieel tot 2028). Of Logius deze heeft of zal lichten is onduidelijk.
- De **landsadvocaat** onderzoekt of contractontbinding op grond van wezenlijke wijziging (overname door buitenlandse partij) juridisch mogelijk is.
- Een **nieuwe aanbesteding** is in voorbereiding; publicatie was voorzien voor maart 2026.

Conclusie: het contract loopt in de tweede helft van **2026** af tenzij de tweede verlengingsoptie wordt gelicht. Het veelgenoemde getal "2028" is de maximale horizon bij volledige benutting van alle opties, niet de huidige contractuele einddatum.

---

3. De overname: tijdlijn en status

Datum	Feit
Vóór zomer 2025	Solvinity informeert Logius dat overname op handen is, zonder naam van koper

Datum	Feit
13 nov 2025	Solvinity maakt overname door Kyndryl publiek
Nov 2025	Melding bij BTI (Bureau Toetsing Investeringen)
12 jan 2026	Brandbrief coalitie burgers/organisaties naar BTI
23 jan 2026	BTI maakt bekend dat melding is ingediend onder Telecommunicatiewet (Wet ozt), niet Wet Vifo
26 feb 2026	ACM keurt overname goed — geen concurrentiebezwaren
Feb 2026	Brede Kamermeerderheid (incl. VVD, D66, CDA) keert zich tegen overname
Mrt 2026	Overname raakt meer ministeries dan alleen Logius: ook J&V, SZW, VWS, Financiën, Politie Nederland, Translink, Zorginstituut
April 2026	BTI-toetsing nog steeds lopend; geen definitief besluit

De overname is per april 2026 **niet definitief afgerond**. De beslissende toets ligt bij het BTI.

---

4. Wat Kyndryl zegt

- Kyndryl opereert via een **Nederlandse BV**, valt daarmee onder Nederlands en

Europees recht.

- Data van klanten blijft op **Europees grondgebied**; toegang is alleen mogelijk vanaf EU-grondgebied.
- Kyndryl stelt zich **maximaal te zullen verzetten** bij verzoeken van Amerikaanse autoriteiten om data, en klanten direct te informeren bij elk dergelijk verzoek.
- Reputatieargument: Kyndryl stelt dat het zijn complete Europese klantenportefeuille zou verliezen bij een dataschandaal.

---

5. Het juridische kernpunt: Cloud Act / FISA

Dit is het meest serieuze technische punt in de discussie.

De **CLOUD Act** (2018) verplicht Amerikaanse bedrijven om data die zij beheren op verzoek aan te leveren aan Amerikaanse autoriteiten, ook als die data op Europese servers staat. Een Nederlandse BV die eigendom is van een Amerikaans moederbedrijf valt hier in beginsel onder.

De eigen staatssecretaris erkende dit in Kamervragen expliciet: de drie genoemde Amerikaanse wettelijke instrumenten (CLOUD Act, FISA, EO 12333) maken het *"in ieder geval in theorie mogelijk dat autoriteiten in de VS toegang kunnen krijgen tot de gegevens die door Solvinity in opdracht van de Staat worden verwerkt, óók wanneer de gegevens zich bevinden onder een dochtervennootschap en op servers buiten de VS."*

- De CLOUD Act heeft een mechanisme voor conflicten met buitenlands recht (Art. 4a): een bedrijf kan uitstel verzoeken als voldoen in strijd is met buitenlandse wetgeving.
- De EU en VS onderhandelen over een bilateraal CLOUD Act Agreement dat dit spanningsveld moet oplossen.
- In de praktijk gaan CLOUD Act-verzoeken via rechterlijke machtiging en zijn gericht op specifieke verdachten, niet op bulkdata van miljoenen burgers.
- Solvinity heeft bij DigiD alleen toegang tot IP-adressen en e-mailadressen — niet tot BSN, wachtwoorden of authenticatiegeschiedenis.

Het woord "in theorie" in de uitspraken van de staatssecretaris is juridisch essentieel en wordt in de publieke discussie stelselmatig weggelaten.

---

6. Het continuïteitsrisico

Dit is het sterkste argument van de critici en het meest legitiem vanuit risicomanagementperspectief.

Als de VS sancties zou opleggen aan Nederland of specifieke Nederlandse entiteiten, zou Kyndryl als Amerikaans bedrijf de dienstverlening kunnen moeten staken. DigiD verwerkt jaarlijks **550 miljoen authenticaties** voor **16,6 miljoen gebruikers**. Een uitval treft de Belastingdienst, zorg, pensioenen, sociale zekerheid en gemeenten tegelijkertijd.

Kanttekening: dit risico is niet uniek voor Solvinity/DigiD. Het Rijk heeft talrijke andere kritieke afhankelijkheden van Amerikaanse technologiebedrijven — Microsoft 365, Cisco-netwerkhardware, diverse cloud-providers. De Solvinity-casus is exemplarisch voor een breder patroon, niet een geïsoleerd incident.

---

7. De PICARD-geschiedenis: de onbesproken achtergrond

Dit aspect verdient meer aandacht dan het krijgt, omdat het de huidige situatie in zijn juiste context plaatst.

Het Adviescollege ICT-toetsing (AcICT) concludeerde in **2023** al dat de migratie naar het PICARD-platform onhaalbaar was in de geplande tijd:

- PICARD werd na **een jaar vertraging** opgeleverd eind 2021.
- Bij de eerste migraties traden direct technische knelpunten op; migraties werden stilgelegd.
- Logius had bewust **niet** gekozen voor de door het AcICT geadviseerde tweestaps-aanpak (eerst basisinfrastructuur, dan cloud), waardoor de overgang met meer dan twee jaar vertraagde.
- Het AcICT sprak van een aanpak waarmee *"Logius, de leverancier en BZK zich hebben vertild."*

- Kostenoverschrijdingen: initiële raming 28 miljoen euro; werkelijke kosten significant hoger.
- Bovendien is onduidelijk in welk datacenter het DigiD-platform fysiek draait: Logius claimt een "overheids-datacenter", maar van de vier odc's zijn NorthC (Franse meerderheidsaandeelhouder) en Equinix (Amerikaans) geen overheidseigendom.

Structurele conclusie: de vendor lock-in bij Solvinity bestond al vóórdat Kyndryl in beeld kwam. De Solvinity/Kyndryl-overname heeft een reeds bestaand probleem zichtbaar en geopolitiek urgent gemaakt — zij heeft het niet veroorzaakt.

---

8. Escrow: de ontbrekende schakel

Er is geen bewijs van een robuuste, geteste **escrow-constructie** voor het PICARD-platform. Dit betekent:

- Als Solvinity/Kyndryl wegvalt, heeft Logius niet automatisch beschikking over alle configuraties, runbooks, Infrastructure as Code (IaC)-artefacten en operationele kennis die nodig zijn om elders door te draaien.
- Experts pleiten expliciet voor het verplicht deponeren van IaC-artefacten, CI/CD-pijplijnen en sleutelmateriaal bij contractstart en periodieke herstelbaarheidstoetsen — wat suggereert dat dit nu onvoldoende geregeld is.

- De landsadvocaat onderzoekt de mogelijkheden, maar zonder robuuste escrow is elke exitstrategie per definitie een meerjarig traject.

---

9. De politieke situatie

- **Brede Kamermeerderheid** (VVD, D66, CDA, GL-PvdA en meer) keert zich tegen de overname.
- **Motie aangenomen**: als overname doorgaat, het contract met Solvinity/Kyndryl bij afloop in 2026/2028 niet verlengen.
- **Motie aangenomen**: onderzoek naar staatsdeelneming of "gouden aandeel" in strategische IT-bedrijven als beschermingsmechanisme.
- **BTI** toetst onder Wet ozt (Telecommunicatiewet) — dit geeft minder transparantie naar burgers dan toetsing onder Wet Vifo, maar opent wel de deur voor ingrijpen op grond van nationale veiligheid.
- **Pieter van Oordt**, Centrale Privacy Officer van Logius, heeft publiekelijk gesteld dat de overname "bijzonder risicovol" is en bereidt een rechtszaak voor tegen de Staat om zijn positie als klokkenluider juridisch te beschermen. Dit is opvallend: een functionaris van Logius zelf neemt een positie in die afwijkt van zijn eigen opdrachtgever (BZK).

---

10. DigiD is technologisch achterhaald

Dit is het aspect dat in de politieke discussie volledig ontbreekt, maar het meest fundamenteel is.

DigiD doet in essentie maar één ding: een online bezoeker identificeren en het BSN doorgeven aan de dienstverlener. Altijd het volledige BSN — ook als dat voor de betreffende dienst helemaal niet nodig is. Het is een gecentraliseerde architectuur uit de vroege jaren 2000.

Ondertussen zijn er meerdere fundamenteel betere systemen operationeel:

Estland — X-Road / eID (operationeel sinds 2002) Het Estse systeem werkt op een gedistribueerd principe: er is geen centrale database die alles doorsluist. X-Road legt beveiligde verbindingen tussen bestaande databases wanneer dat nodig is — data blijft bij de bronhouder. Het systeem verwerkt bijna één miljard jaarlijkse queries (95% geautomatiseerd), bespaart 2% van het BBP per jaar, en biedt burgers volledige inzage in wie hun gegevens heeft opgevraagd. Estland biedt meer dan 600 e-diensten aan burgers en 2.400 aan bedrijven. Burgers kunnen er ook digitaal mee stemmen, contracten ondertekenen met wettelijke geldigheid, en zorgdossiers inzien — allemaal met dezelfde identiteitsinfrastructuur.

België — itsme Meer dan 80% van de volwassen Belgische bevolking gebruikt itsme actief, voor zowel overheidsdiensten als commerciële diensten. itsme neemt nu ook het Nederlandse iDIN over: vanaf juni 2026 kunnen Nederlandse consumenten met de itsme-app inloggen bij aangesloten diensten.

Nederland zelf — Yivi (TU Eindhoven) Yivi (voortgekomen uit het academische IRMA-project van de Radboud Universiteit / TU Eindhoven) werkt op basis van attributen en data-minimalisatie: de burger deelt alleen de specifieke eigenschap die relevant is voor de dienst ("ouder dan 18", "woonachtig in gemeente X") — zonder het BSN prijs te geven. Gemeente Nijmegen werkt er al mee. Het is open source en volledig in Nederlandse handen.

EU — EDI-wallet (verplicht eind 2026) Elke EU-lidstaat moet eind 2026 minstens één gecertificeerde European Digital Identity wallet aanbieden. De identiteitsgegevens staan op het apparaat van de burger zelf, niet centraal bij de overheid. Nederland ontwikkelt de NL-wallet. Dienstverleners die nu DigiD accepteren worden vanaf 2027 verplicht ook de EDI-wallet te accepteren.

Conclusie: de Solvinity-crisis is in feite de beste aanleiding om de fundamentelere vraag te stellen: waarom wordt DigiD in zijn huidige gecentraliseerde architectuur niet gewoon vervangen door iets dat al bestaat, beter werkt en geen infrastructurele afhankelijkheidsrisico's meebrengt? De technische alternatieven zijn beschikbaar. De politieke wil en bestuurlijke capaciteit om zo'n migratie goed te managen zijn dat vooralsnog niet.

---

11. Nuchter oordeel: wat klopt en wat niet

Claim	Oordeel
"DigiD komt in Amerikaanse handen"	**Misleidend.** De applicatie, software en gebruikersdata blijven eigendom van de Nederlandse overheid.
"Amerikanen kunnen je BSN en wachtwoord zien"	**Onjuist.** Solvinity heeft alleen toegang tot IP-adres en e-mailadres.
"Je kunt de beheerder gewoon vervangen"	**Technisch en contractueel te simpel.** PICARD is diep geïntegreerd; er is geen geteste escrow; migratie is minimaal een traject van 1-2 jaar.
"De CLOUD Act is een louter theoretisch risico"	**Onvolledig.** Theoretisch, maar reëel bij geopolitieke escalatie. De Staat erkent dit zelf in Kamerstukken.
"Het continuïteitsrisico is reëel"	**Correct.** Het sterkste argument, relevant vanuit standaard risicomanagementprincipes.
"Dit is uniek voor DigiD"	**Onjuist.** Het Rijk heeft talloze afhankelijkheden van Amerikaanse tech. Solvinity is exemplarisch, niet uitzonderlijk.
"Het contract loopt tot 2028"	**Onzeker.** Basiscontract loopt in 2026 af; de tweede verlengingsoptie is nog niet gelicht.

Claim	Oordeel
"DigiD is state of the art"	**Onjuist.** De architectuur dateert uit de vroege jaren 2000. Estland, België en zelfs Nederlandse alternatieven (Yivi) zijn technologisch significant verder.
"Er zijn geen alternatieven"	**Onjuist.** X-Road, itsme, Yivi en de Europese EDI-wallet zijn operationeel of imminently beschikbaar.

12. Het structurele probleem

De Solvinity/Kyndryl-casus is een symptoom van drie samenhangende structurele problemen:

1. **Uitbestedingsbeleid zonder exitstrategie:** de overheid heeft kritieke IT systematisch uitbesteed zonder adequate escrow, herstelbaarheidstoetsen en exit-clausules. PICARD is hiervan het meest recente voorbeeld.
2. **Technologische stilstand:** DigiD heeft in 20+ jaar geen fundamentele architectuurvernieuwing ondergaan, terwijl de wereld om het systeem heen is doorontwikkeld. De gecentraliseerde BSN-doorgeefdienst is inmiddels inferieur aan wat elders beschikbaar is.

3. **Ontbrekend strategisch kader**: Nederland heeft geen wettelijk kader dat bepaalt welke IT-leveranciers "vitaal" zijn en bescherming verdienen tegen ongewenste buitenlandse overname. Solvinity was op het moment van de overname formeel niet als vitaal aangemerkt, waardoor de reguliere marktmechanismen gewoon hun werk deden.

De korte-termijn oplossing is pragmatisch: contract in 2026 niet verlengen, nieuwe aanbesteding met strikte soevereiniteitsvoorwaarden en escrow-verplichtingen. De structurele oplossing is het vervangen van DigiD door een moderne, gedistribueerde identiteitsinfrastructuur — waarbij de al verplichte EU EDI-wallet het meest logische vehikel biedt.

Bronnen: Kamerstukken 2025-2026 nr. 764, officiële Kamervragen antwoorden staatssecretaris Van Marum (dec. 2025), Logius/DigiD.nl, ACM besluit 26-02-2026, AcICT adviesbrief 2023 (Tweede Kamer 2023D17688), Computable.nl, Taylor Wessing analyse april 2026, technische briefing Vaste Kamercommissie Digitale Zaken jan. 2026, Yivi.app, digitaleoverheid.nl (EDI-wallet), e-Estonia/verifyed.io.