CONCEPT Clusterplan regieraad Interconnectiviteit 2016

1. Inleiding

De voorzieningen die onder de regieraad Interconnectiviteit vallen vormen de basis voor de digitale overheid. Zonder fysieke netwerken, standaarden, architectuur en gegevensuitwisseling is er geen digitale overheid. En er is geen samenwerking zonder samenwerkingsafspraken, onder andere over de gebruikte standaarden voor informatieveiligheid en gegevensuitwisseling. De bijdrage van de producten en standaarden die in dit cluster vallen zijn vitaal voor Nederland. Dit brengt een grote verantwoordelijkheid met zich mee op onder andere het gebied van borging van continuïteit, informatieveiligheid, privacy maar ook door borging via wettelijke kaders en beleidsplannen.

GDI-voorzieningen binnen het cluster Interconnectiviteit

- Standaarden (incl. pas-toe-of-leg-uit-lijst);
- PKIoverheid;
- Digipoort: Overheidstransactiepoort (OTP), Procesinfrastructuur (PI) en Keteninformatiesystemen (KIS);
- Diginetwerk;
- Nederlandse Overheid Referentie Architectuur (NORA).

2. Terugblik

Terugblik op clusterplan 2015 en realisatie ervan.

- Financiering GDI-voorzieningen tot stand gebracht (via bestedingsplannen, ook voor het cluster Interconnectiviteit). Op Digipoort na zijn alle voorzieningen gefinancierd vanuit de begrotingen van de beleidsverantwoordelijken of door middel van doorbelasting naar de voorzieningen die gebruik maken van de desbetreffende voorziening.
- Governance op orde: uit het 'niets' een regieraad Interconnectiviteit in het leven geroepen. Die kent amper een jaar na dato een stabiele structuur. In de regieraad brede vertegenwoordiging, zeer goede opkomst, inhoudelijke discussies met resultaat (denk aan Digipoort en Diginetwerk, zie hieronder).
- Rollen en verantwoordelijkheden voor Digipoort en Diginetwerk belegd. Digipoort OTP is beleidsverantwoordelijk overgegaan van het ministerie van BZK naar het ministerie van EZ. Digipoort PI/KIS kende nog geen beleidsverantwoordelijke. Het ministerie van EZ heeft deze verantwoordelijkheid ook op zich genomen. Als gedelegeerd opdrachtgever fungeert de Belastingdienst. Het beheer blijft bij Logius.
- Ook Diginetwerk had geen beleidsverantwoordelijke. Deze verantwoordelijkheid is nu belegd bij het ministerie van EZ en het ministerie van BZK. Het beheer voor deze voorziening blijft bij Logius.
- Diginetwerk kende bovendien nog geen beleidskader. Aan de hand van een inhoudelijke discussies is gewerkt aan beleidsontwikkeling rondom Diginetwerk en zijn de eerste stappen gezet naar een dergelijk kader. Dit geeft duidelijkheid op de potentie van Diginetwerk en draagt bij aan betrouwbare informatie-uitwisseling tussen overheden.
- Informatieveiligheid is een onderwerp dat op de agenda staat en nu geconcretiseerd moet worden: gezamenlijk werken aan DDoS bestrijding, implementeren en naleven van normen enz. Dit vergt transparantie in plannen, delen van kennis en bundeling van resources: echte samenwerking van beleid, uitvoering en toezicht.
- Overige thema's zijn besproken maar moeten geconcretiseerd worden. Het gaat om de thema's vitale infrastructuur, toezicht op naleving afspraken rondom gebruik standaarden en voorzieningen, Europese koppelingen en gegevensuitwisseling en visie op aanpalende ontwikkelingen.

Kenmerkend aan de thema's die in 2015 zijn geagendeerd is dat deze niet tijdelijk zijn, maar een vaste plek op de agenda blijven houden.

3. Algemeen: thema's/ontwikkelingen die spelen in het cluster en die de voorzieningen raken

In het clusterplan van 2015 zijn thema's benoemd die van belang zijn voor de voorzieningen en standaarden die in het cluster Interconnectiviteit vallen. Dit zijn thema's die doorlopend aandacht behoeven en daarmee niet automatisch in 2015 als afgerond kunnen worden beschouwd. Tegelijk is het belangrijk om focus te hebben. Daarom worden voor de periode 2015/2016 onderstaande thema's als leidend voorgesteld.

Overheidsbreed nummerplan Internet Protocol versie 6 (IPv6)
Het Internet Protocol versie 6 (IPv6) zorgt voor het toewijzen van IP-adressen. Het is de opvolger van Internet Protocol versie 4 (IPv4) en is de tweede versie van het internetprotocol dat in gebruik is genomen. IPv6 is onder andere in het leven geroepen om het tekort aan beschikbare IP-adressen op te lossen. Om leveranciersonafhankelijkheid te bevorderen, fouten te voorkomen en migratiekosten te beperken, is onder regie van BZK een overheidsbreed nummerplan tot stand gekomen dat toewijzing van de nieuwe nummers in goede banen moet leiden. Digitale overheidsdienstverlening is niet denkbaar is zonder een stabiel en veilig internet. Dat maakt IPv6 en het nummerplan van evident belang voor datgene waar de GDI uiteindelijk toe dient: toegankelijke, betrouwbare en toekomstvaste overheidsdienstverlening.

Het internet der dingen (Internet of Things)
Met het internet der dingen wordt bedoeld dat alledaagse voorwerpen met het internet zijn verbonden en gegevens kunnen uitwisselen, en op die manier zaken monitoren en regelen[1]. Met de ingebedde informatie- en communicatietechnologie neemt de bruikbaarheid van objecten enorm toe. Hieruit kunnen nieuwe, persoonlijke diensten ontstaan, die het leven veraangenamen en veiliger maken. Ook in het publieke domein en bij overheidsdienstverlening zijn er vele toepassingen. Denk dan aan eHealth en de automotive industrie. Meer toegepast op de GDI en de regieraad Interconnectiviteit, hoort bij het internet der dingen ook een veilige netwerkomgeving voor dergelijke toepassingen. Hierbij kan gedacht worden aan de doorontwikkeling van Diginetwerk dat mobiele of vaste netwerken voor het internet der dingen ondersteunt met veilige koppelvlakken, standaarden en informatiebeveiliging. Met name dit laatste wordt algemeen geduid als een risico en aandachtspunt bij deze ontwikkeling.

Machine-to-Machine informatieuitwisseling (M2M)
Geautomatiseerde informatie uitwisseling tussen machines/systemen zonder menselijke tussenkomst wordt steeds belangrijker bij zowel bedrijfsleven als overheid. Bekeken moet worden in hoeverre de GDI en de daarmee verbonden dienstverlening aansluit op deze ontwikkeling. Hierbij zijn er relaties met thema's als het internet der dingen en IPv6.

Vitale infrastructuur en continuïteit
Delen van de GDI zijn vitale infrastructuur. Bezien moet worden welke dat precies zijn en hoe we continuïteit wordt gegarandeerd en/of welke acties daarvoor nodig zijn vanuit de governance van de Digicommissaris. Concrete voorbeelden binnen het cluster interconnectiviteit zijn Digipoort, Diginetwerk en PKIoverheid. Niet alleen vanuit het oogpunt van continuïteit, maar ook vanuit informatieveiligheid moeten dergelijke essentiële voorzieningen beschermd worden door helder beleid en bijbehorende wetten.

Informatieveiligheid en beveiligde koppelvlakken
Binnen dit cluster wordt aan het thema informatieveiligheid invulling gegeven door de beveiligde koppelvlakken die er zijn op Digipoort en Diginetwerk. Deze koppelvlakken zorgen voor een beveiligde verbinding tussen het bedrijfsleven en de overheid of tussen onbeveiligde (overheids) netwerken en beveiligde rijksnetwerken. De regieraad Interconnectiviteit ziet toe op juiste toepassing van de beveiligde koppelvlakken, opdat de informatieveiligheid ook op netwerk- en

[1] Een mooi achtergrondartikel is te vinden op:
http://www.mckinsey.com/insights/business_technology/an_executives_guide_to_the_internet_of_things

voorzieningniveau bij bedrijfsleven en overheid geborgd is. Naast deze inhoudelijke insteek wordt ook gewerkt aan het verbeteren van overheidsbrede sturing op informatieveiligheid. Met name door optimaal gebruik te maken van bestaande gremia, en die in hun kracht te plaatsen.

Toezicht
Een aantal standaarden (pas-toe-of-leg-uit-lijst) en voorzieningen is door de overheid verplicht in te zetten of te implementeren. Tot op heden is het toezicht op (juiste) implementatie van standaarden of gebruik van voorzieningen niet goed geregeld. De regieraad Interconnectiviteit stimuleert beleidsontwikkeling voor toezicht de juiste implementatie van standaarden en gebruik van voorzieningen. In een later stadium ziet de regieraad ook toe op het daadwerkelijk uit (laten) voeren van het ontwikkelde beleid.

Europese koppelingen en gegevensuitwisseling
Gegevensuitwisseling met Europese lidstaten en bedrijven is een belangrijk aandachtspunt. Met name ook een integrale benadering voor de overheid als geheel. De Regieraad Interconnectiviteit ziet toe op beleidsontwikkeling op dit vlak waarbij ook het sTESTA netwerk en relevantie Europese initiatieven worden betrokken. Hierbij hoort ook meer samenhang realiseren richting europa als 1 overheid.

Visieontwikkeling aanpalende domeinen
Binnen de overheid zijn tal van innovatieve projecten voor onder andere IPV6, Rijkscloud en Rijks DNS opgestart. De spin-off van deze projecten buiten de rijksoverheid is in potentie groot. De regieraad Interconnectiviteit volgt deze projecten en ontwikkelingen nauwgezet en ontwikkelt visie of en op welke wijze ze ook in aanpalende domeinen van waarde kunnen zijn.

4. Prioriteiten voor dit cluster voor 2016/2017

De GDI-voorzieningen binnen het cluster Interconnectiviteit dragen bij aan vrijwel alle andere onderdelen van de GDI die in de overige regieraden ter sprake komen. Voor de regieraad Interconnectiviteit is een aantal specifieke doelstellingen geformuleerd. Deze zijn mede afkomstig uit de workshops die in het kader van de voorbereiding van het eerste Nationale Beraad gehouden zijn. Naast de resultaten van de workshops zijn ook de doelstellingen, zoals geformuleerd in de opdrachtbrieven, van de voorzieningen opgenomen. Van de voor het Nationaal Beraad geformuleerde ambities[2] (d.d. 9 december 2014) zijn onderstaande doelstellingen het meest relevant voor de regieraad Interconnectiviteit. Per doelstelling wordt een voorstel gedaan wat de regieraad Interconnectiviteit hieraan in 2016 (en verder) concreet bijdraagt.

1. **Veilige en betrouwbare toegang tot de dienstverlening**

- De regieraad Interconnectiviteit vult voor deze doelstelling de randvoorwaarden in. Zonder beveiligde netwerken, beveiligde koppelvlakken en standaarden is er geen veilige en betrouwbare toegang tot dienstverlening. De regieraad Interconnectiviteit is primair de regieraad waar onderwerpen met betrekking tot de connectiviteit (infra), informatieveiligheid en continuïteit van dienstverlening primair aan de orde komen. De regieraad ontwikkelt concrete (beleids)plannen voor integrale continuïteit en veiligheid van de eOverheid en jaagt indien nodig de totstandkoming van wetgeving aan. Ketensamenwerking, ook in een publiek-private context, is essentieel om deze doelstelling te bereiken.

2. **Verhoging gebruik voorzieningen**

- De regieraad Interconnectiviteit brengt in kaart wat de belemmeringen zijn die grootschalig gebruik van de voorzieningen in het cluster tegenhouden en formuleert oplossingsrichtingen om deze belemmeringen weg te nemen. Hierbij kan worden gedacht aan het harmoniseren van beleid, instellen van wettelijke verplichtingen tot gebruik en het ontsluiten van nieuwe sectoren.

[2] http://www.digicommissaris.nl/nieuws-item/stukken-van-het-nationaal-beraad-openbaar

- Concreet voor de voorziening Digipoort betekent dit het vergroten van het gebruik door organisaties die reeds gebruikmaken. Dit door het verhogen van berichtvolumes en het initiëren van nieuwe berichtstromen. Verder wordt ingezet op het verhogen van de berichtstroom van overheid naar bedrijven en het inzetten van Digipoort in nieuwe sectoren (veiligheid, onderwijs) en waar nodig het uit de weg nemen van belemmeringen. Tot slot wordt onderzocht welke informatiestromen nu niet over Digipoort maar over andere voorzieningen gaan, en die vanuit het oogpunt van administratieve lastenverlichting voor het bedrijfsleven wel over Digipoort zouden kunnen lopen.

3. Getoetste standaarden en voorzieningen voor een doelmatige en veilige eOverheid overheidsbreed inzetten.

- De commissie Elias dringt aan op de daadwerkelijke toepassing van het pas-toe-of-leg-uit beleid van de Nederlandse overheid (aanbeveling 9), evenals de daaropvolgende motie Oosenbrug/Gesthuizen (voor eind 2015 correct omgaan met open standaarden bij aanbestedingen). Tezamen met het belang van standaarden voor de GDI en Digitaal 2017 (o.a. eenmalige gegevensverstrekking), betekent dit dat toezicht beter geregeld moet worden. Immers, het beleid is er al jarenlang, maar de daadwerkelijke adoptie van de verplichte standaarden (en GDI-voorzieningen) blijft achter.

---

5. Toelichting per voorziening

Standaarden (incl. pas-toe-of-leg-uit-lijst);

Standaarden bevorderen het uitwisselen van gegevens tussen overheidsorganisaties. Forum Standaardisatie beheert de 'pas toe of leg uit'-lijst met verplichte open standaarden die gelden voor de gehele publieke sector.

- Ten aanzien van de adoptie van informatieveiligheid-standaarden wordt aangegeven wanneer de adoptie bij de deelnemers aan het Nationaal Beraad snel genoeg gaat (tijdsplanning). De daadwerkelijke adoptie van deze standaarden wordt vier keer per jaar gemonitord.
- Onderdeel van de tijdsplanning is de adoptie van de verplichte standaarden van de lijst met verplichte standaarden[3] in de GDI-voorzieningen zelf. Dit wordt in samenhang met het wetgevingstraject eOverheid, dat o.a. het aansluiten op voorzieningen regelt, bezien.
- Daarnaast worden acties opgenomen die de leden van het Nationaal Beraad nemen, om het gebruik van standaarden actief te stimuleren.
  Adoptie van standaarden (met de nadruk op de standaarden rond informatieveiligheid) wordt het hoofdpunt van het Werkplan 2016 van het Forum Standaardisatie.
- Het Forum doet een kwaliteitstoets op de GDI-voorzieningen (twee reeds gedaan, twee worden momenteel uitgevoerd, in 2016 volgt opnieuw een aantal).

PKIoverheid

Digitale certificaten zijn nodig om de betrouwbaarheid van informatie-uitwisseling, via e-mail en websites en over netwerken, conform Nederlandse wetgeving te waarborgen. Een certificaat is als het ware een legitimatiebewijs van een website of ICT-systeem. PKIoverheid is het certificaat dat waarborgt dat een dienstafnemer met een officiële overheidsinstantie communiceert.

[3] Verplicht in de vorm van een 'pas-toe-of-leg-uit' regime.

- In 2016 zal het Agentschap Telecom het toezicht op het PKIoverheid-stelsel overnemen van Logius.

Digipoort (OTP, PI en KIS)

Digipoort regelt het berichtenverkeer tussen overheid en bedrijfsleven. Overheden kunnen Digipoort inzetten om bedrijfs- en ketenprocessen te automatiseren. Digipoort bestaat uit twee onderdelen: Digipoort OTP en Digipoort PI. OTP staat voor Overheidstransactiepoort en regelt basaal de logistieke kant van het berichtenverkeer. PI staat voor Procesinfrastructuur en kan ook berichten inhoudelijk 'uitlezen' en daarop controles uitvoeren.

- Voor 2016 staat de migratie van Digipoort OTP naar Digipoort KIS gepland.
- De sector handel en transport heeft veel raakvlakken met het thema duurzaamheid, bijvoorbeeld synchromodaal vervoer. De gegevensuitwisseling via Digipoort kan bijdragen aan het verhogen van duurzaamheid, bijvoorbeeld door betere achterlandverbindingen, gebruik van milieuvriendelijke vervoersmodaliteiten, en effectievere inspecties. Het gebruik wordt daarmee verbreed naar de sectoren veiligheid en duurzaamheid.
- Daarnaast hebben Justid en Logius, beide knooppunten in de e-overheid, afspraken gemaakt om intensiever met elkaar samen te werken. Als deze knooppunten met elkaar verbonden raken, heeft VenJ met Digipoot een vaste oplossing voor gegevensuitwisseling met partijen buiten justitie.
- Synergie met andere voorzieningen zoals Digilevering en de Berichtenbox voor Bedrijven wordt onderzocht. Dat vereist een investering, die zich terugbetaalt als blijkt dat er minder bouwstenen nodig zijn.
- Daarnaast wordt voor specifiek Digipoort een internationale rol geambieerd, mogelijk zelfs als eSens-bouwsteen.
- Bespreken verkenningen naar de mogelijkheden tot inbeheername van of regie op overheidsbreed gebruik van een tool (Ma3tch) en FIU.NET die geanonimiseerde matching van persoonsgegevens binnen een decentraal netwerk mogelijk maakt. Onderzoeken welke alternatieven er zijn voor Digipoort en mogelijke interventies hierop. Dit naar aanleiding van het kiezen door CIOT en TRIP voor alternatieve gegevensuitwisselingsystemen, in casu DJI/JUSTID.
- Onderzoek naar de haalbaarheid van de roep vanuit het bedrijfsleven en het Topsectoren beleid aan de overheid om informatie te delen met het bedrijfsleven (G2B) en gegevensuitwisseling tussen overheden onderling (G2G) om het logistieke proces te optimaliseren. Steeds meer overheidspartijen willen gegevens hergebruiken, om processen efficiënter uit te voeren en administratieve lasten te verlagen.

Diginetwerk

Diginetwerk is het besloten netwerk van de overheid. Diginetwerk maakt het uitwisselen van gegevens met een hoge mate van beveiliging mogelijk tussen overheden. Diginetwerk bestaat uit een aantal aan elkaar gekoppelde, specifieke, besloten overheidsnetwerken.

- Diginetwerk zal in 2016 in het teken staan van de bestendigen van de governance, het eenduidig beleggen van rollen, taken en verantwoordelijkheden voor deze voorziening.
- Het definiëren van een visie en beleidskader over de gewenste ontwikkelrichting van Diginetwerk en het verkrijgen van een trusted netwerk voor uitwisselen overheidsgegevens.
- De vraag naar meer netwerkcapaciteit van de overheid leidt tot forse investeringen in sneller, nieuwer en vooral uitgebreider netwerk. Een verkenning hiertoe is nodig om de juiste besluiten te kunnen nemen.
- Net als dat we het waterbeheer ondergebracht hebben bij de overheid moeten we ook het digitale netwerk onder brengen bij de overheid.
- In 2016 wordt onderzocht wat de invloed van het internet der dingen op Diginetwerk is en hoe eventuele koppeling met niet-fysieke, besloten netwerken op een veilige wijze tot stand gebracht kan worden.

Nederlandse Overheid Referentie Architectuur (NORA)

De Nederlandse Overheid Referentie Architectuur (NORA) bevat principes, beschrijvingen, modellen en standaarden voor het ontwerp en de inrichting van de elektronische overheid.

Het is een instrument dat door overheidsorganisaties kan worden gebruikt in de verbetering van de dienstverlening aan burgers en bedrijven. In 2009 is NORA door het kabinet vastgesteld als norm voor de overheid.

- Het stelsel van overheidsgegevens en uitwerking van het rotondemodel zullen hun beslag krijgen in de NORA zo dat deze ontwikkelingen zijn geborgd en voor iedereen helder zijn.
- De koppeling tussen NORA en Europese architecturen en raamwerken (EIRA/EIF) wordt onderzocht om zo een eenduidige aansluiting op Europa voor gegevensuitwisseling te bewerkstelligen.

Informatieveiligheid

- [input wordt door V&J aangeleverd].

- Het Digiprogramma biedt een kans om op het domein van informatieveiligheid een grote stap in de goede richting te zetten. Ten aanzien van de GDI is overheidsbrede samenwerken op gebied van informatieveiligheid een ontwikkelpunt. Gezamenlijk expertise opbouwen, gezamenlijk calamiteitenbeleid, ketenbrede calamiteit afhandeling, meld*wil* in plaats van meld*plicht*, samenwerking op preventie, detectie, analyse, aangiftes en het nemen van maatregelen om risico's voor de hele GDI af te dekken in plaats van per organisatie. Het is nodig de organisatiecompliance te laten vervangen door ketencompliance. Hierdoor wordt het ketenbelang om compliant te zijn van groter belang dan je eigen compliance in te richten. Hierbij kunnen ook efficiencyvoordelen worden behaald.

- Vanuit de opdracht van de Digicommissaris wordt bekeken hoe de overheidsbrede sturing op informatiebeveiliging meer samenhang maar ook meer doorzettingsmacht kan krijgen. Die is er veelal wel op organisatieniveau, maar nog niet in alle gevallen overheidsbreed. Ook moet de relatie met aanpalende thema's zoals rijks/overheidscloud worden geborgd.

6. SMART doelstellingen voor dit cluster

De SMART-doelstellingen voor 2016 die voortkomen uit het voorafgaande zien er als volgt uit.

1. Bestuurlijke geaccordeerde visie op Diginetwerk (Nationaal Beraad) inclusief planning van aansluiting/gebruik door overheidspartijen.

2. Verhoging gebruik Digipoort met nader vast te stellen meetbare doelstelling.
    a. Meer gebruik huidige stromen
    b. Nieuwe stromen/aansluitingen
    c. In kaart brengen van alternatieve voorzieningen waarover gegevensstromen lopen en mogelijke interventies hierop.

3. Getoetste standaarden en voorzieningen voor een doelmatige en veilige eOverheid overheidsbreed inzetten door inbreng in de governance
    a. Aan de hand van de nieuwe monitor standaarden worden concrete doelstellingen voor 2016 en verder geformuleerd.

7. Krachtenveld: wie heeft welke rol?

Het krachtenveld van de regieraad Interconnectiviteit kenmerkt zich door de notie dat elke overheidspartij gebaat is bij betrouwbare interactie met elkaar en met de private partijen, oftewel interconnectiviteit. De voorzieningen binnen dit cluster hier aan bij betrouwbaarheid. Of het nu gaat om de kabels in de grond (Diginetwerk), de fysieke machines (Digipoort) of de standaarden die de uitwisselingen allemaal mogelijk maken: het moet allemaal werken om dienstverlening

mogelijk te maken. Doordat de voorzieningen niet altijd eenduidig georganiseerd zijn of het vlak van beleid, uitvoering of toezicht kan de governance van de Digicommissaris bijdragen aan een gemeenschappelijke en generieke aanpak.
Op de voorzieningen is beleidsmatig het ministerie van Economische Zaken verantwoordelijk voor de standaarden en voor Digipoort. Een gedeelde verantwoordelijkheid heeft het met het ministerie van Binnenlandse zaken voor Diginetwerk. Dit ministerie is ook verantwoordelijk voor PKIoverheid en de NORA. Voor het thema cybersecurity en informatieveiligheid is het ministerie van Veiligheid en Justitie beleidsmatig verantwoordelijk.
Voor wat betreft het toezicht kan worden aangegeven dat een tal van organisaties zich hier vanuit diverse invalshoeken mee bezighoudt. Zo is er het Agentschap Telecom dat toezicht houdt op PKIoverheid en Diginetwerk en ??? op ???? [NCTV/NBV/NCSC???].
Het beheer van alle voorzieningen is belegd bij Logius. Hierbij wordt Logius aangestuurd door EZ, BZK en de Belastingdienst. EZ waar het gaat om standaarden en Diginetwerk, BZK voor PKIoverheid en Diginetwerk en de Belastingdienst in de rol van gedelegeerd opdrachtgever voor Digipoort, in naam van EZ.

Samengevat zijn in de regieraad de volgende rollen vertegenwoordigd:

- Beleidsverantwoordelijken (eigenaren van een voorziening)
- Opdrachtgevers van de GDI-elementen (Sturen op realisatie binnen de kaders van de beleidsopdracht)
- (vertegenwoordigers van) afnemers
- (vertegenwoordigers van) beheerders van GDI elementen
- (vertegenwoordigers van) leveranciers/marktpartijen (indien van toepassing)

Deze rollen corresponderen met de volgende organisaties binnen het cluster Interconnectiviteit:

Voorziening	Beleidsverantwoordelijk	Opdrachtgever	Beheerder
Digipoort	EZ	Belastingdienst	Logius
Diginetwerk	BZK/ EZ	BZK/ EZ	Logius
Standaarden	EZ	EZ	Logius
NORA	BZK	BZK	Logius
PKI Overheid	BZK	BZK	Logius
Informatieveiligheid en cybersecurity	VenJ	VenJ	Nvt

Daar waar het gaat om het ondersteunen van massale processen door interconnectiviteit zijn het vaak de grote uitvoeringsorganisaties die vooroplopen bij nieuwe ontwikkelingen en het volop digitaliseren van primaire processen. Enerzijds kunnen zij de rest van de overheid helpen tempo te maken met betrekking tot deze ontwikkelingen. Anderzijds zullen zij ook rekening moeten houden met het generieke en overheidsbrede karakter van voorzieningen. Dit spanningsveld is een blijvend punt van aandacht.