Rapportage Monitor Digitale Overheid 01 januari 2023

Inhoud Monitor

Wat is het doel van de Monitor?

Doel

- De Monitor geeft overzicht en inzicht in:
  - de governance;
  - de relevante wetgeving;
  - de belangrijkste thema's.

- De Monitor signaleert voor pensioenuitvoerders relevante ontwikkelingen bij de Digitale Overheid met als doel:
  - Tijdig te kunnen anticiperen op ontwikkelingen en kansen;
  - Waar relevant en mogelijk tijdig invloed te kunnen uitoefenen;
  - Impact voor pensioenuitvoerders te bepalen waar noodzakelijk.

Hoe kwam de Monitor tot stand?

Proces totstandkoming Monitor

- Via bureauonderzoek stelde SIVI de Monitor op. Hierbij is gebruik gemaakt van rapporten, verslagen die in het publieke domein beschikbaar zijn. Ook is gebruik gemaakt van de output van diverse overleggen waarin de pensioensector participeert.

- De Monitor is gedeeld met de stuurgroep DSO, de stuurgroep GZD, en de werkgroep IDP.

- Terugkoppeling is verwerkt van:
  - Ad van Leest (Strategisch Consultant APG, voorzitter werkgroep IDP);
  - Melanie Meniar (Beleidsadviseur Pensioenfederatie);
  - Jos Schaffers (Beleidsadviseur Verbond van Verzekeraars).

- Buiten de scope:
  - Prijsstelling diensten overheid: dit staat al volop in de aandacht van de Pensioenfederatie en het Verbond van Verzekeraars. Aandachtspunt is hier wel de prijsstelling van nieuwe erkende inlogmiddelen onder de WDO:
    - Moeten private dienstverleners hetzelfde doorbelasten als de overheid doet voor DigiD?
    - Mogen private dienstverleners maximaal hetzelfde doorbelasten als de overheid doet voor DigiD?

Wat zijn de belangrijkste bevindingen?

Impact EU - wetgeving

- Vanuit EU-wetgeving is in toenemende mate sprake van het reguleren van de marktmacht in het digitale domein en het nog sterker beschermen van de grondrechten van EU-burgers.
  - Doel is het inperken van de macht in Europa van Amerikaanse technologie reuzen, door het stimuleren van Europese alternatieven, bijvoorbeeld de EU ID-wallet.

- Evident is dat de wetgeving vanuit de EU steeds meer impact krijgt. De Tweede Kamer stelt veel in het werk om meer grip te krijgen op het onderwerp digitalisering.
  - De vaste commissie voor digitale zaken monitort digitalisering vanuit verschillende beleidsterreinen en richt zich tevens op de samenhang van verschillende digitaliseringsterreinen. De vaste commissie voor Digitale Zaken geeft in de tweede helft van 2022 prioriteit aan de volgende EU-voorstellen:
    - Dataverordening;
    - Verordening Europese digitale identiteit;
    - AI Verordening;
    - Europese wet Cyberweerbaarheid;
    - EU-interoperabiliteitsstrategie voor overheden.

Impact EU – ID-wallets

- In 2025 zijn één of meer nationale ID-wallets én andere Europees erkende ID-wallets in Nederland te gebruiken:
  - Daarmee kunnen burgers hun bronidentiteit (een digitale versie van de identiteitsgegevens die de overheid van burgers heeft geregistreerd) en bijbehorende gegevens en documenten gebruiken om digitaal zaken te doen in het publieke én het private domein.
  - Timing is afhankelijk van Europa.

  - Streven:
    - In 2023 is een eerste versie van een publieke open source voorbeeld ID-wallet beschikbaar.
    - In 2023 start NL met deelname enkele grensoverschrijdende Large Scale Pilots met ID-wallets.
    - In 2025 kunnen alle burgers en bedrijven gebruik maken van een hoogwaardige ID-wallet binnen het Europese digitale identiteit raamwerk.

- Deelnemers loggen vanaf 2025 met wallet in bij pensioenuitvoerders en kunnen de wallet bijvoorbeeld ook gebruiken om nog meer gegevens met pensioenuitvoerders te delen en documenten te ondertekenen.

- In Nederland bestaat veel aandacht voor de mogelijkheden en op te lossen issues.
  - Het Nederlandse IRMA liep in dit verband voor de troepen uit en staat model voor de EU ID-wallet.

Impact Wet Digitale Overheid is significant

- De WDO sluit aan bij Europese ontwikkelingen in digitale overheidsdienstverlening en inloggen bij de overheid. De toe te laten publieke en private inlogmiddelen moeten voldoen aan de Europese eisen aan inlogmiddelen (eIDAS-verordening). De eIDAS-verordening is niet nieuw, maar ontwikkelt wel door.

- De impact van de WDO voor pensioenuitvoerders is significant:
  - Ondersteuning erkende private middelen (naast DigiD).
  - Ondersteuning erkende bedrijfs- en organisatiemiddelen (naast eHerkenning).
  - Ondersteuning genotificeerde inlogmiddelen van andere EU-lidstaten.
  - Inregelen juiste betrouwbaarheidsniveau:
    - Zie conceptregeling betrouwbaarheidniveaus;
    - zie Regelhulp.
  - Zodra de onderliggende wetgeving gereed is en conform het aansluitschema in werking treedt, moeten publieke dienstverleners machtigingen accepteren bij diensten op betrouwbaarheidsniveau substantieel en hoog.
  - Voor diensten op niveau Substantieel of Hoog kunnen deelnemers niet meer met SMS-authenticatie inloggen.
  - Op termijn moeten pensioenuitvoerders naar verwachting ook wettelijke vertegenwoordiging ondersteunen.
  - Jaarlijks auditverklaring overleggen waaruit blijkt dat wordt voldaan aan de gestelde veiligheidsnormen. Deze audit geldt al voor DigiD maar is straks van toepassing voor het hele stelsel.

- Reden bestaat om vanuit de pensioenuitvoerders en verzekeraars vragen te stellen over de voorgestelde nieuwe architectuur die de WDO met zich meebrengt. Bijvoorbeeld:
  - De Makelaar krijgt een andere rol binnen het stelsel van Elektronische Toegangsdiensten. Wat is hiervan de impact?
  - Is voldoende rekening gehouden met ketenmachtigingen?

Externe bronnen

- Een aantal databronnen staat real-time raadplegen toe, maar dit is niet het ideaalplaatje. Dat zijn volgens technische experts API-koppelingen, althans daar waar real-time datauitwisseling voor de hand ligt. De KVK biedt een KVK-API, maar hier maken pensioenuitvoerders geen gebruik van. UWV werkt met configureerbare Webservices en de BRP experimenteert met API-koppelingen in een speciaal programma. Dit biedt toekomstperspectief voor pensioenuitvoerders.
  - Het programma Haal Centraal ontwikkelt API's waarmee gemeenten en andere overheidsorganisaties basisgegevens rechtstreeks bij landelijke registraties kunnen bevragen. Of en wanneer dergelijke API's voor pensioenuitvoerders beschikbaar komen is onbekend.
  - De toezichthouders stellen vast dat niet altijd sprake is van een goede AVG verwerkingsgrond voor het opvragen persoonsgegevens. Het Ministerie van Financiën gaat in 2023 hier wetgeving voor opstellen en consulteren.

- BRP/RNI
  - Systemen worden aangepast om de registratie van e-mailadressen en telefoonnummers van niet-ingezetenen mogelijk te maken. Het registreren start in oktober 2022.
  - Onderzoek is aanstaande of ook voor ingezetenen registratie van e-mailadressen en telefoonnummers zal worden ingevoerd. Hierbij zullen de ervaringen met de registratie van contactgegevens van niet-ingezetenen worden betrokken.
    - Eind 2022 is duidelijk dat het genoemde onderzoek niet in 2023 gaat plaats vinden.
  - De pensioensector heeft op basis van het huidige autorisatiebesluit nog geen rechten om deze gegevens te raadplegen.

Toezichthouders

- Datagedreven toezicht vormt steeds meer het uitgangspunt voor DNB. In bepaalde uitingen spreekt DNB zelfs van real-time toezicht en geeft aan de sector te betrekken. Datagedreven toezicht staat gepland om per 2025 in te gaan.

- De AFM dringt aan om rekening te houden met DORA, ook als het niet verplicht is (<250FTE).
  - DORA beoogt om de digitale weerbaarheid van financiële ondernemingen te vergroten om risico's te verminderen voor de financiële sector als geheel, voor individuele financiële ondernemingen en voor consumenten en beleggers.
  - De AFM stelt dat DORA ook als raamwerk kan dienen voor de (proportionele) inrichting van de ICT-beheersing van kleinere en daarmee alle ondernemingen.

- AI heeft een belangrijke plek op de strategische agenda van de Rijksinspectie Digitale Infrastructuur (voorheen Agentschap Telecom).

- De Autoriteit Persoonsgegevens is vanaf 1-1-2023 algoritmetoezichthouder.

Regie op gegevens

- Het overheidsprogramma Regie op Gegevens werkt aan een generiek sector-overstijgend kader dat veilige, betrouwbare en gebruiksvriendelijke digitale uitwisseling van gegevens tussen overheden, private en maatschappelijke organisaties mogelijk maakt.

- Belang:
  - Pensioenplanning is in toenemende mate onderdeel van financiële planning. Regie op financiële gegevens maakt het in toenemende mate mogelijk dat personen/huishoudens sneller en beter overzicht hebben over hun financiële positie en de data kunnen delen met dienstverleners (hypotheekadviseurs, pensioenadviseurs, financiële planners, schuldhulp verleners etc.). Naast versnelling van processen – een kickstart van het advies of de keuzebegeleiding - kunnen hierdoor ook de kosten en kwaliteit van financieel advies en keuzebegeleiding gunstig beïnvloed worden. Een dienst die integraal inzicht biedt in gegevens over betaalrekeningen (kosten van levensonderhoud), spaarrekeningen, schulden, hypotheken, verzekeringen, pensioenen, abonnementen, etc. ontbreekt momenteel nog.
  - Randvoorwaarden zijn
    - Voordelen voor de consument (gemak!);
    - Vertrouwen van de consument;
    - Eenvoudige systematiek voor toestemming;
    - Gegevens uit relevante databronnen in het publieke en private domein moeten hiertoe op gestandaardiseerde wijze beschikbaar komen. Denk hierbij aan API-koppelingen en een betrouwbare standaardwijze van inloggen.

- Vertrouwen van de consument maakt een andere voorwaarde noodzakelijk: toezicht op dienstverleners.

REGIE OP GEGEVENS
Zelf geregeld, veilig en betrouwbaar!

Levensgebeurtenissen

- https://www.rijksoverheid.nl/onderwerpen/levensgebeurtenissen/overzicht-levensgebeurtenissen

- Met pensioen: wat moet ik regelen?
  - Vul de vragen in en bekijk wat je moet regelen als je met pensioen gaat.
  - Na invullen vragen volgt afhankelijk van de antwoorden een actielijst.
  - De actielijst komt in PDF beschikbaar.

Met pensioen: wat moet ik regelen?

Regelen voordat u uw AOW-leeftijd bereikt

Hoogte pensioen bekijken

Doen nadat u uw eerste AOW-uitkering ontvangt

AIO-aanvulling aanvragen

Regelen voordat u (voor een deel) stopt met werken

Aanvullend pensioen aanvragen

Voor een deel blijven werken

Arbeidscontract beëindigen

Doen nadat u gestopt bent met werken

Toeslagen aanpassen of aanvragen

Toeslag wijzigen

Loonheffingskorting regelen

Loonheffingskortingen vergelijken

Middelingsregeling toepassen

Belasting terugkrijgen

Wijziging inkomen doorgeven voor uw Ziektewetuitkering

Voorlopige aanslag aanvragen of wijzigen

Voorlopige aanslag wijzigen

Regelen bij eerstvolgende belastingaangifte

Oudedagsreserve afrekenen

Pensioensector kan invloed uitoefenen via uiteenlopende gremia

Overlegorgaan	Vertegenwoordiger
Logius Klantenraad	Ad van Leest (APG, namens SDSO)
Programmeringsraad Generieke Digitale Infrastructuur (PGDI)	Edith Maat (Pensioenfederatie)
Programmeringstafel Interactie	Ad van Leest (APG, namens SDSO)
Programmeringstafel Toegang	Melanie Meniar (Pensioenfederatie)
Stakeholdergroep Federatief Berichtenstelsel (FBS)	Ad van Leest (APG, namens SDSO)
Gebruikersoverleg BRP	Melanie Meniar (Pensioenfederatie)
Werkgroep Ontwikkelingen BRP	Melanie Meniar (Pensioenfederatie)
Werkgroep Kwaliteit BRP	Eric Antwerpen (APG)
Afnemersoverleg Loonaangifteketen	Melanie Meniar (Pensioenfederatie)
Tactisch Beraad eHerkenning	Ad van Leest (APG, namens SDSO)
Strategisch Beraad eHerkenning	Jos Schaffers (Verbond van Verzekeraars)

Wat zijn onze conclusies en aanbevelingen?

Conclusies

- Het lijkt van belang - met name voor betrokkenen bij compliant pensioenuitvoering - dat overzicht en inzicht wordt gecreëerd voor wat betreft de samenhang tussen het digitale beleid op Europees en op nationaal niveau en de impact hiervan:
  - Wat betekent de overlap in wetten en regelingen?
  - Wat is vanaf wanneer van kracht en wat betekent het voor mijn organisatie?
- De EU ID-wallet biedt kansen, ook voor de pensioensector.
- De impact van de WDO is significant. Bij het denken over de toekomst houdt de overheid niet vanzelfsprekend rekening met private partijen met een publieke taak.
- De overheid heeft het voornemen BRP/RNI uit te breiden met contactgegevens. Dit is weliswaar een gunstige ontwikkeling voor pensioenuitvoerders met een hoog besparingspotentieel, maar meer tempo is gewenst.
- De DNB heeft vergaande plannen met datagedreven toezicht.
- In toenemende mate is het mogelijk voor een huishouden snel en laagdrempelig inzicht te krijgen in de financiële situatie nu en in de toekomst. Dit geeft kansen voor keuzebegeleiding en advies.

Aanbevelingen

- Speel in op de kansen die nationale ID-wallets bieden. Dit vraagt om samenwerking en onderzoek.
- Blijf invloed uitoefenen op het aansluitschema voor de Wet Digitale Overheid rekening houdend met de haalbaarheid voor pensioenuitvoerders/pensioenuitvoeringsorganisaties.
  - Denk hierbij onder meer aan het belang van routeringsvoorzieningen in het verlengde van de erkenning van private inlogmiddelen naast DigiD.
- Anticipeer tijdig op veranderingen rond eHerkenning, bijvoorbeeld de mogelijkheid dat eHerkenningsmakelaars een andere rol krijgen.
- De DNB heeft vergaande plannen met datagedreven toezicht. Het ligt voor de hand dit op kort op de bal te volgen.
- In toenemende mate is het mogelijk voor een huishouden snel en laagdrempelig inzicht te krijgen in de financiële situatie nu en in de toekomst. Dit geeft kansen voor keuzebegeleiding en advies. Samenwerking kan bijdragen deze kansen te benutten, bijvoorbeeld het gezamenlijk ontwikkelen van een data-aggregator.
- Verwijs als Pensioenuitvoerder in het eigen portaal naar de website over levensgebeurtenissen.

Dit is het einde.

Bijlagen

Bijlage Beleid & Wetgeving EU

Intro EU-wetgeving

- De EU-wetgeving omvat alle verdragen die betrekking hebben op de oprichting en werking van de Europese Unie (EU) en alle verordeningen, richtlijnen en besluiten die van toepassing zijn in de lidstaten van de EU.

- De meeste maatregelen van de EU worden genomen volgens de 'gewone wetgevingsprocedure'. Deze procedure bepaalt dat het Europees Parlement samen met de Raad (de regeringen van de EU-lidstaten) EU-wetsvoorstellen moet goedkeuren.

- De belangrijkste wetgevingsmaatregelen in de EU zijn verordeningen, richtlijnen en besluiten.
  - Verordeningen zijn bindend en rechtstreeks toepasselijk in de hele EU.
  - Richtlijnen zijn eveneens bindend wat betreft het beoogde resultaat, maar werken niet rechtstreeks als maatregel. Via richtlijnen worden de wetgevingen in de verschillende EU-lidstaten geharmoniseerd. De lidstaten mogen zelf regels vaststellen om de doelstellingen van de richtlijnen te bereiken. Elke richtlijn heeft een uiterste datum waarbinnen lidstaten de bepalingen moeten omzetten in nationale wetgeving.
  - Besluiten zijn specifieke maatregelen die alleen bindend zijn voor het EU-land of bedrijf tot wie zij zijn gericht.

EU Wetgeving

Data Governance Act

- Doel is de hoeveelheid gegevens die beschikbaar is voor hergebruik binnen de EU te vergroten door toe te staan dat overheidsgegevens worden gebruikt voor andere doeleinden dan waarvoor de gegevens oorspronkelijk zijn verzameld.
- Tevens voorstel om "gegevenstussenpersonen" op te richten, die het delen van gegevens door individuen, overheidsinstanties en particuliere bedrijven zullen afhandelen.
- Het wetsvoorstel beoogt ook sectorspecifieke dataruimten te creëren om het delen van data binnen een specifieke sector mogelijk te maken.
- Een European Data Innovation Board gaat toezicht houden op de dienstverleners voor het delen van gegevens (de data-intermediairs) en gaat advies geven over best practices voor het delen van gegevens.
- Deze verordening treedt naar verwachting op 24 september 2023 in heel Europa in werking.

Data Act

De Data Act is een voorstel voor een verordening tot harmonisatie van regels voor eerlijke toegang tot en gebruik van gegevens. Het zal een sleutelrol spelen in het digitale decennium en helpen de regels voor de digitale economie en economie vorm te geven. De Data Act verduidelijkt wie waarde kan creëren uit data en onder welke voorwaarden. Het zal ook regels introduceren met betrekking tot het gebruik van gegevens die worden gegenereerd door apparaten die zijn aangesloten op het internet der dingen.

Het voorstel voor de EU Data Act ('Data Act') ligt sinds 23 februari 2022 op tafel

Digital Markets Act

- Stelt een reeks nauwkeurig gedefinieerde objectieve criteria vast om een groot online platform te kwalificeren als een zogenaamde "poortwachter".
- Zo pakt de wet de problemen met grote, systemische onlineplatforms gericht aan.
- Poortwachters moeten bijvoorbeeld derde partijen in staat stellen in bepaalde specifieke situaties met de eigen diensten van de poortwachter samen te werken.
- De wet inzake digitale markten wordt begin mei 2023 van toepassing.

Digital Services Act

- De wet inzake digitale diensten omvat regels voor onlinetussenhandelsdiensten, die miljoenen Europeanen dagelijks gebruiken De verplichtingen van de verschillende onlinespelers passen bij hun rol, omvang en impact op het online-ecosysteem.
- De wet inzake digitale diensten betekent een aanzienlijke verbetering van de mechanismen voor het verwijderen van illegale inhoud en doeltreffende bescherming van de grondrechten van gebruikers, waaronder de vrijheid van meningsuiting. De wet leidt ook tot een sterker overheidstoezicht op onlineplatforms, met name op platforms die meer dan 10% van de EU-bevolking bereiken.
- De wet inzake digitale diensten zal 15 maanden na de inwerkingtreding of vanaf 1 januari 2024, indien dat later is, rechtstreeks van toepassing zijn in de hele EU. Dit moet leiden tot meer vertrouwen in de veiligheid van digitale producten en handelsplatformen.

European Digital Identity

- De Europese digitale identiteit zal beschikbaar zijn voor EU-burgers, inwoners en bedrijven die zich willen identificeren of bepaalde persoonlijke informatie willen bevestigen. Het kan worden gebruikt voor zowel online als offline openbare en particuliere diensten in de hele EU. Elke EU-burger en ingezetene van de Unie kan een persoonlijke digitale portemonnee gebruiken.
- Het idee van het European Digital Identity Framework is dat alle nationale overheden vanaf 2024 minimaal één wallet gaan uitgeven of erkennen

Herziening eIDAS-verordening van juni 2021

- Begin juni 2021 kondigde de Europese Commissie een revisie aan van de eIDAS regulering.
  - Europese Digitale Identiteit raamwerk (EDI), het wetsvoorstel Europese Commissie.

Raamwerk Europese Digitale Identiteit (EDI)

- Van:
  - eIDAS-verordening uit 2014, van toepassing vanaf september 2018 op:
    - Elektronische identiteiten (eIDs):

      NL eIDs (DigiD en eHerkenning) kunnen gebruikt worden bij andere Europese (semi-)overheden,

      eID's uit momenteel 15 andere EU-landen kunnen gebruikt worden bij NL (semi-)overheden (nu: ± 300).

      Nationale IT-voorzieningen voor grensoverschrijdende authenticatie onder beheer van BZK.
    - Trust Services = Vertrouwensdiensten:

      Elektronische handtekening, zegel en andere waarmerken voor gebruik bij (semi-)overheden, aangeboden vanuit commerciële sector.
- Naar:
  - Een of meer publieke en private 'wallets' voor burgers én bedrijven, met digitale identiteiten én andere gegevens, inclusief elektronische vertrouwensdiensten, voor gebruik in (semi-)overheid én in bedrijfsleven.
  - **Zie verder de aparte bijlage over de EU ID-wallet.**

EU ID-wallet

European Digital Identity – Wallet

- eIDAS betrouwbaarheidsniveau hoog.
- Wallet is gratis voor gebruiker.
- Voor burgers en bedrijven.
- Publieke en private sector.
- Algemene toepassingen, bijvoorbeeld:
  - Identiteit bewijzen (SCA = sterke klant authenticatie);
  - Elektronische documenten delen;
  - Documenten digitaal ondertekenen met een gekwalificeerde elektronische handtekening (QES);
    - https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+-+Get+started
    - https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+FAQ
  - Data delen.
- Specifieke toepassingen, bijvoorbeeld:
  - Openbare diensten zoals het opvragen van geboorteakten, medische attesten, het doorgeven van een adreswijziging;
  - Openen van een bankrekening;
  - Het doen van belastingaangiftes;
  - Solliciteren naar een universiteit, thuis of in een andere lidstaat;
  - Het bewaren van een medisch recept dat overal in Europa gebruikt kan worden;
  - Bewijs van leeftijd;
  - Auto huren met digitaal rijbewijs;
  - Inchecken in een hotel.

Een voorbeeld van een ID-wallet (Hong Kong)
https://www.singpass.gov.sg/main/

Wat verandert er?

Nu:

Wat regelt de huidige eIDAS-verordening voor eID's?

Betrouwbaar inloggen met elektronische identiteiten bij (semi)overheidsdiensten (over de grens).

Straks:

Wat regelt het voorstel voor een 'Europese Digitale Identiteit'?

- Alle lidstaten geven **verplicht één of meer wallets** uit.
- **Regie op gegevens**: Burgers en bedrijven kunnen hun digitale (bron)identiteit en gegevens, zoals diploma's, zelf delen via een wallet-applicatie op hun smartphone.
- **Gebruik in private sector**: Wallets kunnen gebruikt worden, niet alleen in het publieke domein, maar ook in het private domein, in het bijzonder op grote platforms (Google, Facebook, Amazon, etc.).
- **Gebruik is gratis** voor natuurlijke personen, wallet voldoet aan toegankelijkheidseisen en aan hoogste niveau van betrouwbaarheid bij uitgifte en gebruik.
- Wallets zijn geschikt voor **offline gebruik** zonder internet.
- Wallets moeten de vertrouwensdiensten **elektronische handtekening en zegel** bevatten (samenloop met beleidsterrein EZK). Daarnaast verplichte nationale certificering door in NL RDI (EZK).

Welke attributen in EU ID-wallet?

Overeenkomstig artikel 45 quinquies waarborgen de lidstaten dat er, indien die attributen gebruikmaken van authentieke bronnen binnen de publieke sector, maatregelen worden genomen zodat gekwalificeerde verleners van elektronische attesteringen van attributen op verzoek van de gebruiker langs elektronische weg aan de hand van de relevante authentieke bron op nationaal niveau of via op nationaal niveau erkende aangewezen intermediairs, overeenkomstig nationaal of Unierecht, de authenticiteit van de volgende attributen kunnen verifiëren:

1. **adres;**
2. **leeftijd;**
3. **geslacht;**
4. **burgerlijke staat;**
5. **gezinssamenstelling;**
6. **nationaliteit:**
7. **onderwijskwalificaties, -titels en -diploma's;**
8. **beroepskwalificaties, -titels en -licenties;**
9. **openbare vergunningen en licenties;**
10. **financiële en bedrijfsgegevens.**

Identificerende gegevens eIDAS

Vereisten betreffende het minimale pakket persoonsidentificatiegegevens dat een natuurlijke persoon of rechtspersoon op unieke wijze vertegenwoordigt, als bedoeld in artikel 11

1. Minimaal gegevenspakket voor een **natuurlijke persoon**

Het minimale gegevenspakket voor een natuurlijke persoon bevat al de volgende verplichte attributen:

a) huidige familienaam of familienamen;

b) huidige voornaam of voornamen;

c) geboortedatum;

d) unieke identificatiecode, door de lidstaat van verzending vastgesteld volgens de technische specificatie voor grensoverschrijdende identificatie, zodanig dat deze zo lang mogelijk stabiel blijft.

Het minimale gegevenspakket voor een natuurlijke persoon **kan** één of meer van de volgende aanvullende attributen bevatten:

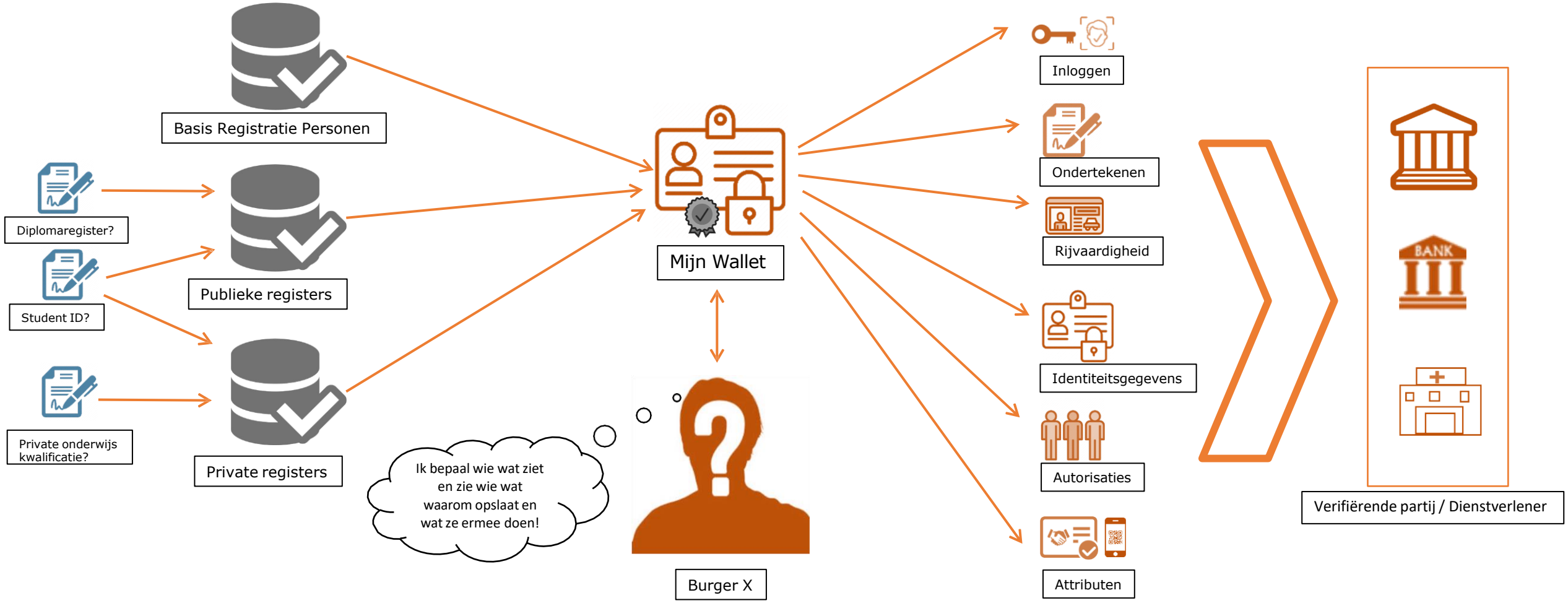
a) voornaam of voornamen en familienaam of familienamen bij geboorte;

b) geboorteplaats;

c) huidig adres;

d) geslacht.

Hoe werkt zo'n wallet?



Overheden en organisatie met publiekrechtelijke taken (‘openbare instanties’) = huidig eIDAS domein

Verplichte Acceptatie

Grote platforms als Facebook en Google.

Particuliere partijen die hoog niveau betrouwbaarheid eisen in onlinetransacties in o.a. vervoer, financiële dienstverlening, sociale zekerheid, gezondheidszorg, post, energie, telecom en onderwijs.

Vrijwillige Acceptatie

Particuliere partijen o.b.v. zelfregulerende gedragscodes.

Uitgegeven BZK
Gecertificeerd AT

Wallet-applicatie in Smartphone

eHandtekening
eZegel

Digitaal
NIK
Rijbewijs

Personal Identification Data (PID)
= Digitale Bron Identiteit (DBI)

Machtigingen
(vertegenwoordiging bedrijf of persoon)

Attributen
1.adres;
2.leeftijd;
3.geslacht;
4.burgerlijke staat;
5.gezinssamenstelling;
6.nationaliteit:
7.onderwijskwalificaties, -titels en -diploma’s;
8.beroepskwalificaties, -titels en -licenties;
9.openbare vergunningen en licenties;
10.financiële en bedrijfsgegevens.

Listed Trust Providers =
Private aanbieders
vertrouwensdiensten
Diverse partijen, onder toezicht EZK

Registers
Rijbewijzen-NIK
BZK/RvIG en
I&M/RDW

BRP en PIVA
BZK/RvIG

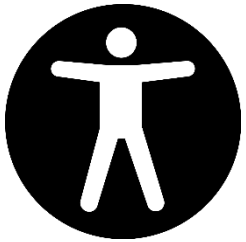
BRP, Handelsregister,
Machtigingenregisters.
Diverse beheerders

BRP, Handelsregister*
basisregistraties en
diverse andere
registers.
Diverse beheerders

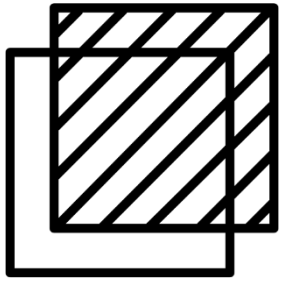
Principes EDI-Stelsel NL

Privacy en autonomie

Veiligheid en betrouwbaarheid



Inclusie en toegankelijkheid



Vertrouwen en transparantie

Uitgangspunten EDI-Stelsel NL

- Inrichting EDI-stelsel voor wallets waarin per medio 2025* één of meer nationale ID-wallets én andere Europees erkende wallets in Nederland te gebruiken zijn.
- Met deze ID-wallets kunnen burgers zelf beschikken over hun eigen identiteit en data en hier vaardig (bewust en bekwaam) mee omgaan**.
- Dienstverleners krijgen niet meer gegevens dan nodig zijn en de overheid organiseert toezicht zodat ID-wallets betrouwbaar en veilig te gebruiken zijn***.
- De ID-wallets kunnen zowel bij publieke als private dienstverleners worden gebruikt in lijn met de herziene eIDAS-verordening.
- De samenwerking aan deze ontwikkeling is open en transparant.

- * Timing afhankelijk van Europa
- ** Verder uitwerken + invullen
- *** Normering en regulering in te richten

Status EDI-Stelsel NL

- Programma EDI-Stelsel NL is in de maak (najaar 2022).
- Maatschappelijke Kosten-Baten Analyse (MKBA) loopt (najaar 2022).
- Streven
  - In 2023 een eerste versie van een publieke open source voorbeeld ID-wallet beschikbaar, ICTU ontwikkelt deze.
  - In 2023 start NL (indien EU gegund) met deelname enkele grensoverschrijdende Large Scale Pilots met ID-wallets.
    - NL gaat deelnemen in Potential, een Consortium van 19 lidstaten op initiatief van overheden

      Consortium Potential (digital-identity-wallet.eu).
  - In 2025 kunnen alle burgers en bedrijven gebruik maken van een hoogwaardige ID-wallet binnen het Europese digitale identiteit raamwerk.

- Op dit moment zijn er in totaal vier van de zes punten die Nederland heeft ingebracht verwerkt in de Europese raadsconclusie.
  - De verwerkte punten gaan over een hoog betrouwbaarheidsniveau voor uitgifte van de wallets, het voorkomen van één universeel persoonsnummer, het aanhouden van langere implementatietermijnen en de aanbeveling om broncode van een Wallet open source beschikbaar te stellen.

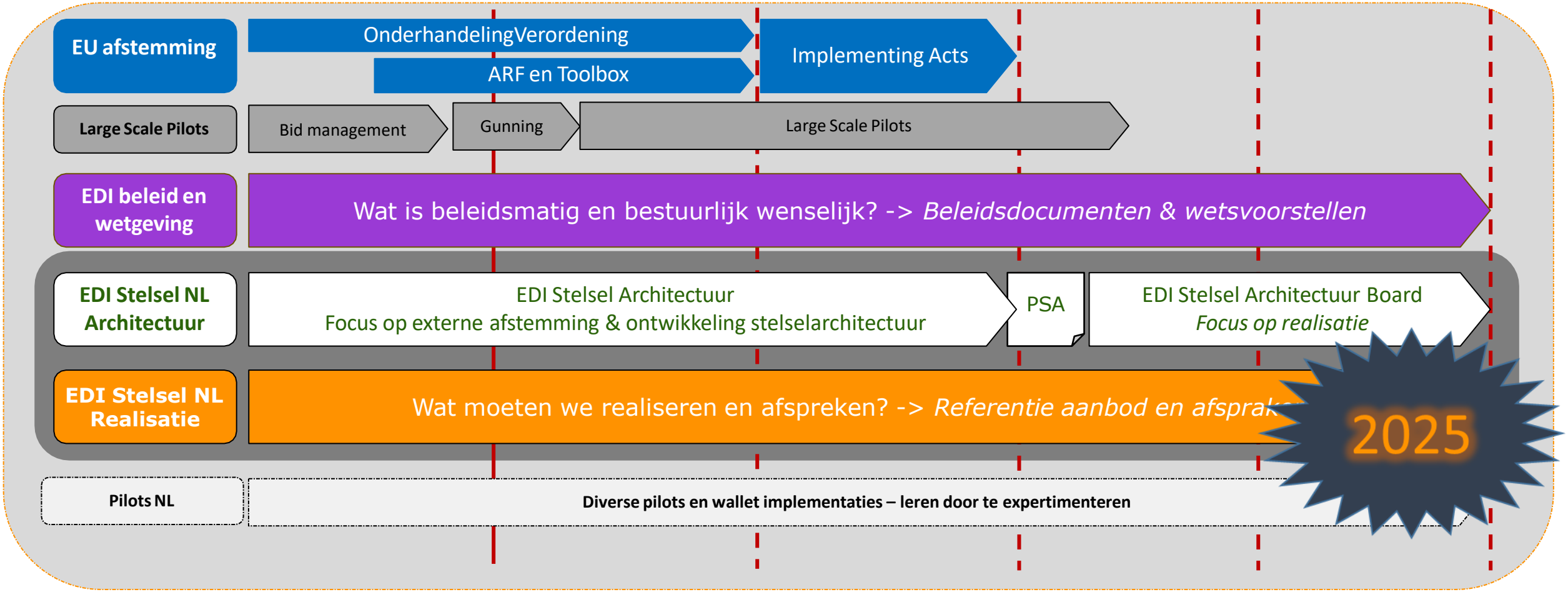
Belangrijke vraagstukken in NL

- In het EU-voorstel heeft de Europese Commissie in Bijlage VI een minimale lijst van attributen opgenomen die lidstaten uit authentieke bronnen ter beschikking zouden moeten stellen voor gebruik in portemonnees.
  - Dit betreffen adres, leeftijd, geslacht, burgerlijke staat, gezinssamenstelling, nationaliteit, onderwijskwalificaties, -titels en -diploma's, beroepskwalificaties, -titels en -licenties, openbare vergunningen en licenties en financiële en bedrijfsgegevens.
  - Het kabinet beraadt zich welke van deze attributen in welke volgorde in de Nederlandse portemonnee(s) dienen te worden opgenomen en op welke wijze.

- Risico op overvraging door dienstverleners.
- Overidentificatie: risico dat een persoon zich overal moet identificeren.
- Gedwongen gebruik: het uitgangspunt is dat het gebruik van wallets niet verplicht mag zijn.
  - Dus moet bij dienstverleners altijd een parallel proces in stand blijven.
- Controlesamenleving en uitsluiting: mensen die niet aan een bepaald profiel voldoen, zouden bijvoorbeeld uitgesloten kunnen worden van bepaalde diensten of meer moeten betalen.

Waarden, kansen en uitdagingen rond het Europese Digitale Identiteit raamwerk, Van Huffelen 26 juli 2022

Tijdslijnen NL



Bijlage FAQ EU ID-wallet

Wallets – basisvragen (1)

- Wat zijn wallets?
  - Een wallet, of digitale portemonnee, is een applicatie waarin een burger of onderneming zijn/haar identiteitsgegevens en officiële documenten elektronisch kan opslaan en beheren. Ook kan je jezelf er digitaal mee identificeren en online een handtekening kunnen zetten.
  - Wanneer je als Nederlandse burger in de toekomst een EDI-wallet wilt gebruiken, installeer je deze als app op je telefoon of een ander (draagbaar) apparaat. Je vult deze met door de overheid gewaarmerkte identiteitsgegevens. Vanaf dan kun je je online identificeren, bij alle overheidsdiensten in de lidstaten van de EU, bij private dienstverleners, zoals banken en verzekeraars, en bij grote online platforms. Ook kun je extra geverifieerde gegevens toevoegen aan de wallet, uit zowel publieke als private bronnen. Denk daarbij aan het rijbewijs, diploma's en certificaten, beroepskwalificaties, inkomensgegevens, maar mogelijk ook betaalpassen, de OV-chipkaart en festivaltickets.

- Zijn er in de toekomst meerdere wallets beschikbaar?
  - Ja, dat is de bedoeling. Nederland zal een publieke voorbeeldwallet beschikbaar stellen, waarvan de broncode hergebruikt kan worden voor wallets die aan willen sluiten op het stelsel. Binnen het stelsel kunnen wallets aansluiten die voldoen aan de waarden en principes die wij belangrijk vinden. De precieze invulling wordt momenteel nog vormgegeven en is mogelijk aan verandering onderhevig.

- Kunnen private partijen attributen op de wallet uitgeven?
  - Ja dat kan. De verordening wordt echter niet verplicht voor private organisaties, tenzij het gaat om private organisaties met een publieke taak die expliciet zijn opgenomen in de verordening. Op dit moment wordt erover gesproken om richting een open standaard te gaan, waarbij het een mogelijkheid wordt om extra bewijzen en attributen toe te voegen. Hierbij gaan dan wel vereisten gelden.

Wallets – basisvragen (2)

- Wat betekent 'verplichte acceptatie' door platformen als facebook of google?
  - Wanneer gebruikers hun wallet willen gebruik om bij grote platformen in te loggen, dan moeten deze grote platformen dat accepteren.

- Krijgt een bedrijf ook een ID-wallet?
  - De regeling voor ID-Wallets in het voorstel tot herziening van de huidige eIDAS verordening is gericht op natuurlijke personen en rechtspersonen. Beiden kunnen gebruikers van Europese ID-Wallets zijn.

- Wat is de implementatietermijn voor de LSP en de herziening van de eIDAS verordening?
  - De LSP's starten vanaf 2023 voor een periode van twee jaar. De herziening van de eIDAS verordening zal naar verwachting in het najaar van 2023 gepubliceerd worden. De termijn waarbinnen Europese ID-wallets na publicatie van de verordening door lidstaten uiterlijk uitgegeven moeten zijn, is op dit moment voorwerp van onderhandeling.

- Worden de kaders van open standaarden ook op Europees niveau geadresseerd?
  - De Europese Commissie ondersteunt een expertgroep van alle lidstaten die werkt aan een EDI toolbox. Het streven is dat de komende maanden een referentiearchitectuur wordt opgeleverd en dat er een toolbox komt van standaarden, afspraken en principes over de werking van alle nationale ID-wallets zodat ze grensoverschrijdend en interoperabel te gebruiken zijn.

Wat zijn Large Scale Pilots?

- De Europese Commissie heeft op 14 december 2022 alle voorstellen gegund die zijn ingediend voor een Large Scale Pilot met de European Digital Identity Wallet. Eerder werd bekend gemaakt dat Netcompany en Scytáles de EU voorbeeldwallet gaan ontwikkelen die in deze LSP's gebruikt zal gaan worden.

- Door vier consortia is een voorstel ingediend:
  - Potential. Hieraan nemen Nederlandse organisaties deel. Coördinerende lidstaten: Frankrijk en Duitsland. De use cases van dit consortium richten zich op simkaart e-registratie, openen bankrekening, e-rijbewijs, e-overheidsdienstverlening, elektronische handtekening, e-prescription.
  - DC4EU. Hieraan nemen Nederlandse organisaties deel. Coördinerende lidstaat: Zweden. Dit consortium richt zich op eID, diploma's en beroepskwalificaties en sociale zekerheid (PDA1, EHIC).
  - EU Digital Wallet Consortium. Hieraan nemen Nederlandse organisaties deel. Coördinerende lidstaat: Spanje. Dit consortium richt zich op e-commerce en reizen.
  - NOBID Consortium. Geen (directe) deelname Nederlandse organisaties. Coördinerende lidstaat: Noorwegen. Dit consortium gaat werken aan een use case voor grensoverstijgende betalingen met de wallet.

- Bureau LSP
  - Bureau Large Scale Pilots (BLSP) ondersteunt Nederlandse organisaties bij deelname aan de LSP’s. Ook coördineert het bureau de Nederlandse deelname aan consortium Potential.

Waarom Qualified Trust Service Providers?

- Nieuw is dat EU-burgers met hun wallet-ID in heel Europa niet alleen met overheden maar ook met gecertificeerde bedrijven zaken kunnen doen.

- Artikel 22 van de eIDAS-verordening verplicht de lidstaten om vertrouwenslijsten op te stellen, bij te houden en te publiceren. Deze lijsten moeten informatie bevatten met betrekking tot de gekwalificeerde vertrouwensdienstverleners waarvoor zij verantwoordelijk zijn, en informatie met betrekking tot de gekwalificeerde vertrouwensdiensten die door hen worden verleend. De lijsten worden op een beveiligde manier gepubliceerd, elektronisch ondertekend of verzegeld in een formaat dat geschikt is voor geautomatiseerde verwerking.

- Nationale toezichthouders moeten hun ‘zegen’ geven over publieke en private dienstaanbieders, die zich na certificatie ‘qualified trust service provider’ mogen noemen.

Wat zijn voorbeelden van vertrouwensdiensten?

Dienst	Burgers	Bedrijven
Elektronische handtekening Het is een manier om in elektronische vorm uit te drukken dat u instemt met de inhoud van een document. Deze functie zal in de portemonnee worden geïntegreerd.	U kunt er juridische documenten mee ondertekenen en verzenden, zonder iets te printen.	Is goedkoper en sneller dankzij gestroomlijnde procedures en stimuleert innovatie bij bedrijven.
Elektronische tijdstempel Het is een elektronisch bewijs voor het bestaan van een zekere reeks gegevens op een bepaald tijdstip.	Het bewijst bijvoorbeeld dat ik een concertticket heb gekocht.	Het maakt het traceren van documenten makkelijker en het zorgt voor meer verantwoordingsplicht.
Elektronisch identiteitsbewijs Bedrijven en consumenten kunnen hiermee hun identiteit elektronisch bewijzen.	Zo kunt u bijvoorbeeld in een ander land met uw eigen nationale identiteitskaart een bankrekening openen.	Verruimt uw markt, bespaart tijd en geld en maakt buitenlandse transacties betrouwbaarder.
Gekwalificeerd webauthenticatiecertificaat Garandeert dat websites veilig en betrouwbaar zijn.	Informeert u bijvoorbeeld als consument over de betrouwbaarheid en veiligheid van de websites en apps die u gebruikt.	Stimuleert het consumentenvertrouwen en helpt phishing te voorkomen, waardoor uw reputatie als ondernemer beschermd wordt.
Elektronisch zegel Garandeert de herkomst en integriteit van een document.	Bewijst bijvoorbeeld dat uw voetbaltickets echt zijn en geen namaak.	Is goedkoper en sneller dankzij gestroomlijnde procedures en stimuleert het vertrouwen in de herkomst van elektronische documenten.
Elektronische aangetekende zending Beschermt documenten tegen verlies, diefstal, beschadiging of wijziging tijdens verzending.	Garandeert bijvoorbeeld dat het verjaardagscadeau voor uw kind veilig aankomt.	Maakt documenten uitwisselen sneller, goedkoper, efficiënter, betrouwbaarder en beter te traceren.

Bijlage Beleid & Wetgeving Rutte IV

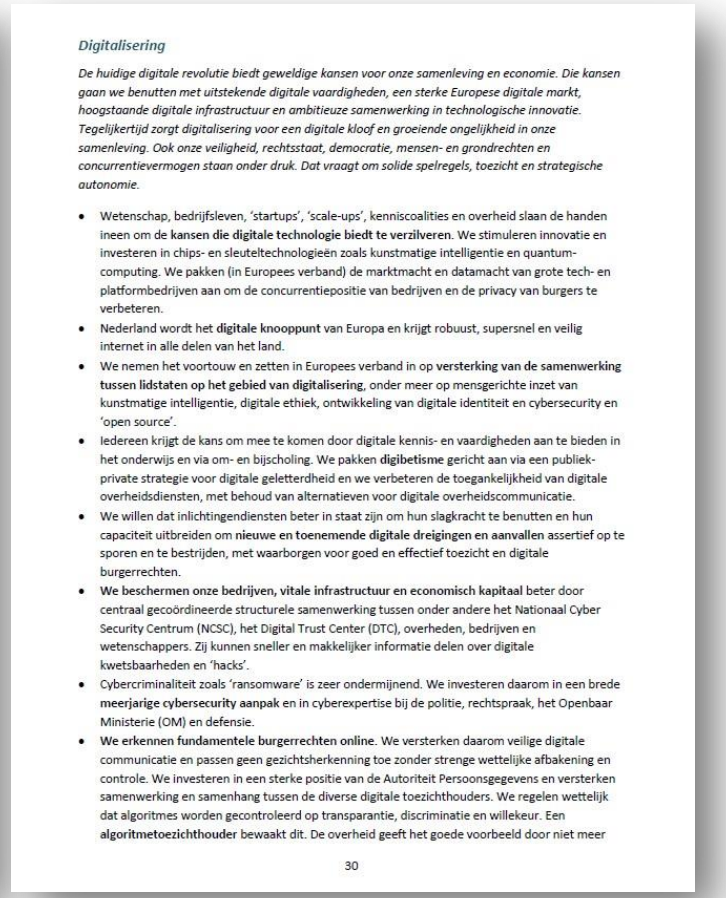
Rutte IV over Digitalisering

Omzien naar elkaar, vooruitkijken naar de toekomst

Coalitieakkoord 2021 – 2025

VVD, D66, CDA en ChristenUnie

15 december 2021

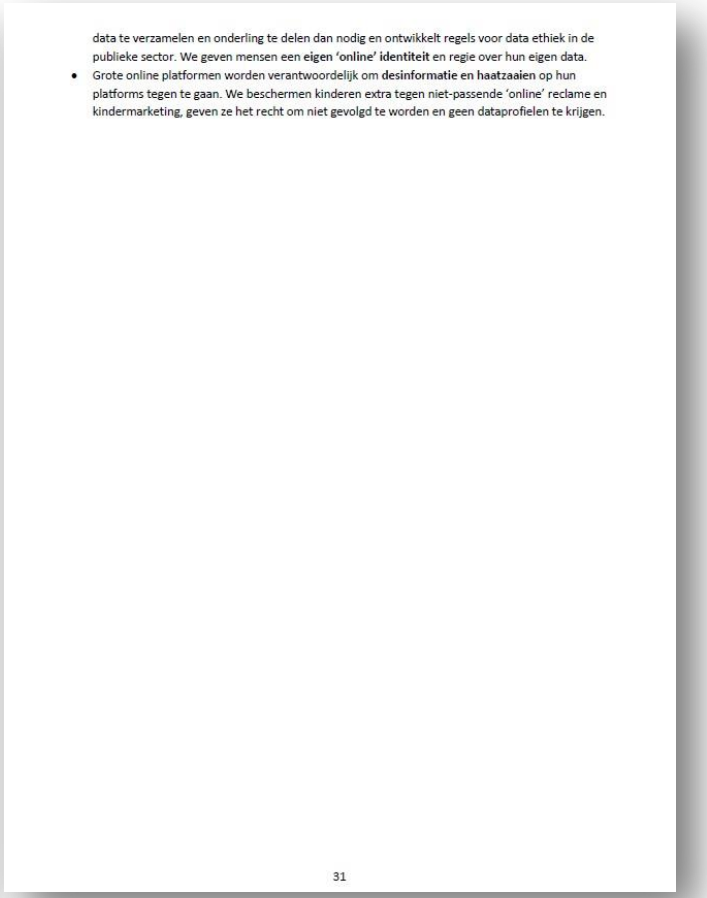


Digitalisering

De huidige digitale revolutie biedt geweldige kansen voor onze samenleving en economie. Die kansen gaan we benutten met uitstekende digitale vaardigheden, een sterke Europese digitale markt, hoogstaande digitale infrastructuur en ambitieuze samenwerking in technologische innovatie. Tegelijkertijd zorgt digitalisering voor een digitale kloof en groeiende ongelijkheid in onze samenleving. Ook onze veiligheid, rechtsstaat, democratie, mensen- en grondrechten en concurrentievermogen staan onder druk. Dat vraagt om solide spelregels, toezicht en strategische autonomie.

- Wetenschap, bedrijfsleven, 'startups', 'scale-ups', kenniscoalities en overheid slaan de handen ineen om de **kansen die digitale technologie biedt te verzilveren**. We stimuleren innovatie en investeren in chips- en sleuteltechnologieën zoals kunstmatige intelligentie en quantum-computing. We pakken (in Europees verband) de marktmacht en datamacht van grote tech- en platformbedrijven aan om de concurrentiepositie van bedrijven en de privacy van burgers te verbeteren.
- Nederland wordt het **digitale knooppunt** van Europa en krijgt robuust, supersnel en veilig internet in alle delen van het land.
- We nemen het voortouw en zetten in Europees verband in op **versterking van de samenwerking tussen lidstaten op het gebied van digitalisering**, onder meer op mensgerichte inzet van kunstmatige intelligentie, digitale ethiek, ontwikkeling van digitale identiteit en cybersecurity en 'open source'.
- Iedereen krijgt de kans om mee te komen door digitale kennis- en vaardigheden aan te bieden in het onderwijs en via om- en bijscholing. We pakken **digibetisme** gericht aan via een publiek-private strategie voor digitale geletterdheid en we verbeteren de toegankelijkheid van digitale overheidsdiensten, met behoud van alternatieven voor digitale overheidscommunicatie.
- We willen dat inlichtingendiensten beter in staat zijn om hun slagkracht te benutten en hun capaciteit uitbreiden om **nieuwe en toenemende digitale dreigingen en aanvallen** assertief op te sporen en te bestrijden, met waarborgen voor goed en effectief toezicht en digitale burgerrechten.
- **We beschermen onze bedrijven, vitale infrastructuur en economisch kapitaal** beter door centraal gecoördineerde structurele samenwerking tussen onder andere het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC), overheden, bedrijven en wetenschappers. Zij kunnen sneller en makkelijker informatie delen over digitale kwetsbaarheden en 'hacks'.
- Cybercriminaliteit zoals 'ransomware' is zeer ondermijnend. We investeren daarom in een brede **meerjarige cybersecurity aanpak** en in cyberexpertise bij de politie, rechtspraak, het Openbaar Ministerie (OM) en defensie.
- **We erkennen fundamentele burgerrechten online**. We versterken daarom veilige digitale communicatie en passen geen gezichtsherkenning toe zonder strenge wettelijke afbakening en controle. We investeren in een sterke positie van de Autoriteit Persoonsgegevens en versterken samenwerking en samenhang tussen de diverse digitale toezichthouders. We regelen wettelijk dat algoritmes worden gecontroleerd op transparantie, discriminatie en willekeur. Een **algoritmetoezichthouder** bewaakt dit. De overheid geeft het goede voorbeeld door niet meer

30



data te verzamelen en onderling te delen dan nodig en ontwikkelt regels voor data ethiek in de publieke sector. We geven mensen een **eigen 'online' identiteit** en regie over hun eigen data.

- Grote online platformen worden verantwoordelijk om **desinformatie en haatzaaien** op hun platforms tegen te gaan. We beschermen kinderen extra tegen niet-passende 'online' reclame en kindermarketing, geven ze het recht om niet gevolgd te worden en geen dataprofielen te krijgen.

31

"We geven mensen een eigen 'online' Identiteit en regie over hun eigen data." (p. 31)
https://www.kabinetsformatie2021.nl/documenten/publicaties/2021/12/15/coalitieakkoord-omzien-naar-elkaar-vooruitkijken-naar-de-toekomst

Hoofdlijnenbrief Digitalisering – Van Huffelen maart 2022

Kamerbrief hoofdlijnen beleid voor digitalisering

Staatssecretaris Van Huffelen (Koninkrijksrelaties en Digitalisering), minister Adriaansens (EZK) , minister Yeşilgöz-Zegerius (JenV) en minister Weerwind (Rechtsbescherming) sturen de Tweede Kamer een brief over de hoofdlijnen van het beleid van de digitale transitie van de samenleving voor deze kabinetsperiode .

Download 'Kamerbrief hoofdlijnen beleid voor digitalisering'

PDF document | 20 pagina's | 1 MB
Kamerstuk: Kamerbrief | 08-03-2022

Bijlagen

› Beslisnota behorende bij de Kamerbrief over Hoofdlijnen beleid digitalisering

Beslisnota bij Kamerbrief Hoofdlijnen beleid digitalisering. In een beslisnota staat achtergrondinformatie die bewindspersonen ...

Beleidsnota | 08-03-2022

"<u>Online identiteit en regie over eigen data</u>
Een andere cruciale voorwaarde is dat burgers in de digitale wereld autonoom kunnen zijn en zelf kunnen beschikken over hun eigen data en identiteit." (p. 7)

"(...) Een nieuwe privacy vriendelijkere manier van omgang met gegevens, waarbij burgers in staat worden gesteld echte keuzes te maken, ontstaat niet zomaar.
Daarom krijgen burgers een breed bruikbare digitale identiteit, zodat zij zich in de digitale wereld op veilige wijze kunnen identificeren en meer regie over eigen gegevens hebben zonder dat iemand over de schouders meekijkt – vergelijkbaar met het gebruik van een paspoort in de fysieke wereld." (p. 8)

Werkagenda | Prioriteiten

Fundament

1 "Iedereen kan meedoen in het digitale tijdperk"

1. Vergroten van digivaardigheden en kennis
2. Toegankelijke, hoogwaardige en proactieve dienstverlening
3. Impact online desinformatie verminderen
4. (EU) regelgeving en implementatie in samenhang ondersteunen

2 "Iedereen kan de digitale wereld vertrouwen"

1. Publieke waarden borgen
2. Borgen van privacy, verantwoord datagebruik en vergroten transparantie over gegevensverwerking en -uitwisseling
3. Anticiperen op nieuwe digitale technologie
4. Versterken cybersecurity

3 "Iedereen heeft regie op het digitale leven"

1. Regie op eigen gegevens
2. Hoogwaardig identiteitsstelsel waaronder inlogmiddelen en een wallet
3. Algoritmes reguleren

Overheid

4 "Een digitale overheid die waardengedreven en open werkt voor iedereen"

1. Verbeteren informatiehuishouding voor openbaarheid van bestuur
2. Verbeteren gegevenshuishouding voor burgers en organisaties
3. Versterken ICT-organisatie en -systemen van het Rijk

Caribisch deel koninkrijk

5 "Versterken van de digitale samenleving in het Caribisch deel van het koninkrijk"

5.1 Versterken van de digitale samenleving in het Caribisch deel van het Koninkrijk

Vaste commissie voor Digitale Zaken – EU rapporteurs

- Hoe werkt de Tweede Kamer in relatie tot Europa

- De vaste commissie voor Digitale Zaken is sinds 15 september 2021 verantwoordelijk voor het controleren van en richting geven aan de Nederlandse inzet in de Europese Telecomraad.
  - Deze Raad behandelt het Europese telecommunicatiebeleid en het beleid over informatie en communicatietechnologie (ICT), waaronder Kunstmatige Intelligentie (AI), Cybersecurity, Europese online identiteit, Data Governance, Open Data en Datadelen, Roaming en (e-)Privacy.

- De vaste commissie voor Digitale Zaken geeft in de tweede helft van 2022 prioriteit aan de volgende EU-voorstellen:
  - Dataverordening;
  - Verordening Europese digitale identiteit;
  - AI Verordening;
  - Europese wet Cyberweerbaarheid;
  - EU-interoperabiliteitsstrategie voor overheden;
  - (zie hier de volledige lijst met EU-prioriteiten van de Kamer).

- Regelmatig stellen Kamercommissies EU-rapporteurs aan voor een specifiek nieuw EU-dossier. Dit moet er toe bijdragen dat deze dossiers zo optimaal mogelijk worden behandeld in de Kamer en dat de informatiepositie van de Kamer wordt versterkt.
  - Rapportage over digitale identiteit;
    - Rapportage over digitale identiteit bevat interessante vraagsuggesties: zie Bijlage.
  - Rapportage over Digital Services Act en Digital Market Act.

WDO - kenmerken

- Het Stelsel Toegang maakt het mogelijk dat een burger voor zichzelf, voor een ander of voor een bedrijf zich digitaal kan authentiseren bij overheidsinstanties
  - Het doet dat door (tot het stelsel) toegelaten authenticatie- en machtigingsdiensten (zoals DigiD) en bedrijfsmiddelen (zoals eHerkenningsmiddelen) te verbinden met digitale diensten van de Nederlandse overheidsorganisaties, bijvoorbeeld bij de Belastingdienst of het UWV.
  - Door meerdere inlogmiddelen aan te bieden, borgt het stelsel de continuïteit van de toegang tot de digitale overheidsdienstverlening.

- De WDO treedt gefaseerd in werking
  - Het aansluitschema bevat een planning met data waarop de specifieke onderdelen van de wet voor welke instantie van kracht worden. De planning is dat het aansluitschema in 2023 op basis van de zogenaamde migratieadviezen wordt vastgesteld
    - De aansluiting van alle overheidsorganisaties op het nieuwe stelsel zal naar verwachting in de tweede helft van 2026 volledig afgerond zijn.
    - De overheid stelt het aansluitschema vast in overleg met de betrokken sectoren.
  - Zie ook overgangsrecht Wet digitale overheid.
  - De uitwerking van de WDO als kaderwet (piketpaal) vindt plaats in de lagere regelgeving.
  - Lagere regelgeving is op zijn vroegst pas vanaf 1 juli 2023 van kracht.

- De Eerste Kamer heeft op 29 november 2022 in een eerste termijn van de kant van de Kamer deze novelle en het oorspronkelijk wetsvoorstel gezamenlijk plenair behandeld, de tweede termijn van de behandeling WDO is op 21 februari 2023.

WDO – Impact voor pensioenuitvoerders

- Ondersteuning erkende private middelen (naast DigiD).
- Ondersteuning erkende bedrijfs- en organisatiemiddelen (naast eHerkenning).
- Ondersteuning genotificeerde inlogmiddelen van andere EU-lidstaten.
- Inregelen juiste betrouwbaarheidsniveau:
  - Zie conceptregeling betrouwbaarheidniveaus;
  - zie Regelhulp.
- Zodra de onderliggende wetgeving gereed is en conform het aansluitschema in werking treedt, moeten publieke dienstverleners machtigingen accepteren bij diensten op betrouwbaarheidsniveau substantieel en hoog.
- Voor diensten op niveau Substantieel of Hoog kunnen deelnemers niet meer met SMS-authenticatie inloggen.
- Op termijn moeten pensioenuitvoerders naar verwachting ook wettelijke vertegenwoordiging ondersteunen.
- Jaarlijks auditverklaring overleggen waaruit blijkt dat wordt voldaan aan de gestelde veiligheidsnormen.

Vooruitblik op tweede tranche Wet digitale overheid

- Voor de tweede tranche van de WDO komen de volgende onderwerpen in aanmerking voor wettelijke verankering. Dit zijn:
  - Het kader voor het verantwoord delen van digitale persoonsgegevens met partijen binnen en buiten de overheid (regie op gegevens);
  - Het beleggen van de verantwoordelijkheid voor het stelsel van basisregistraties en het bewaken van de werking daarvan, waaronder het correct (en verplicht) gebruik van authentieke gegevens in het stelsel;
  - Hoe kunnen in de WDO het burger- en bedrijvendomein verder naar elkaar toe groeien?

Authenticatiemiddelen - aandachtspunten

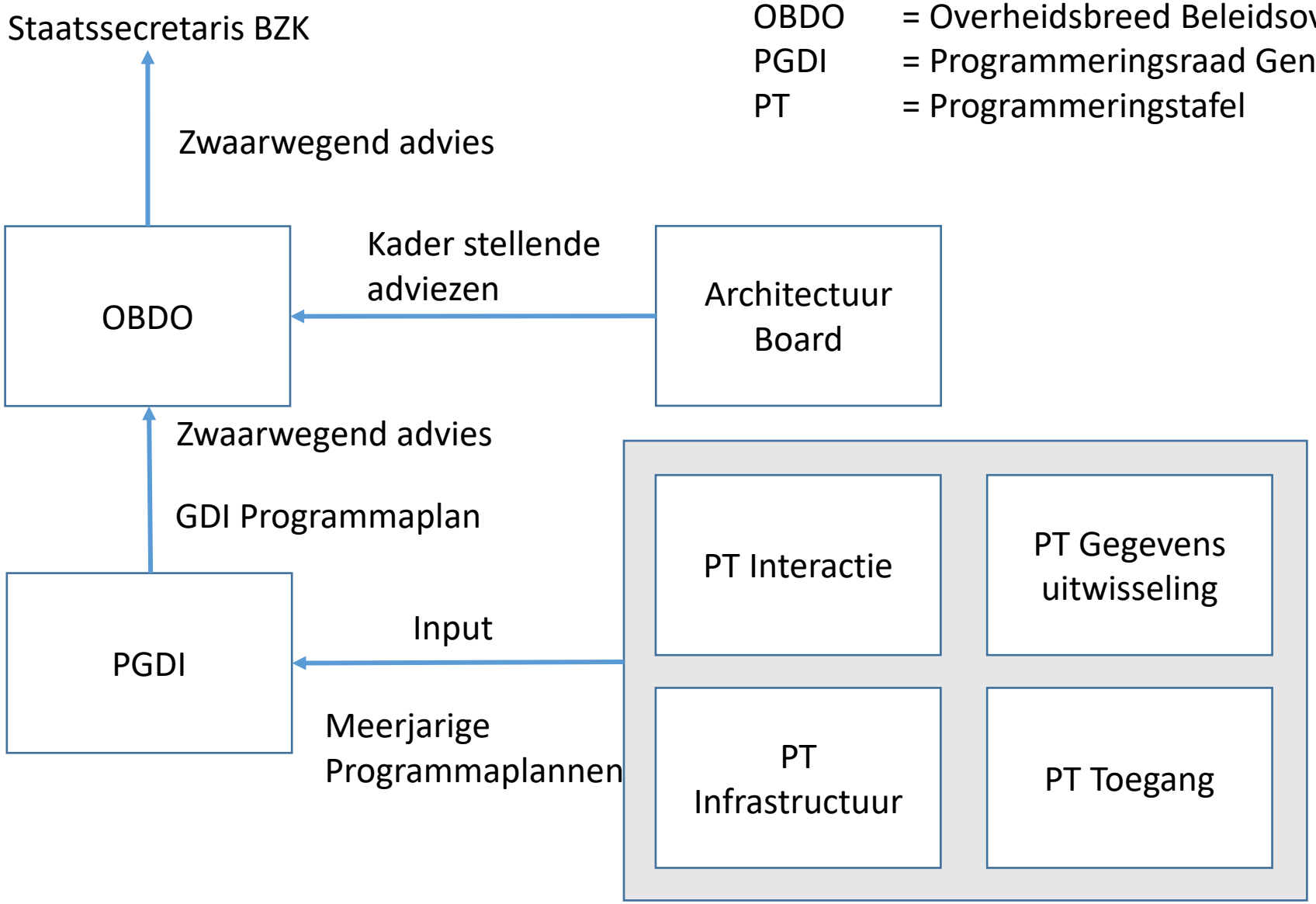
- Erkennen overige private middelen
  - Hoe zit het met de kosten voor pensioenuitvoerders? Denk hierbij vooral aan de kosten voor het inloggen bij pensioenuitvoerders.

- Het publieke middel
  - In de brief van 26 september 2022 – over de voortgang in het domein Toegang - van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties staat: ‘’Verder wordt gewerkt aan een kosteloos publiek middel voor het inloggen bij MijnBelastingdienst Zakelijk door enkelvoudig zelfstandig bevoegde bestuurders. De verwachting is dat dit middel in het voorjaar van 2023 in gebruik kan worden genomen. De eventuele bredere inzetbaarheid van dit publieke bedrijvenmiddel buiten de Belastingdienst vergt nadere besluitvorming.’’
  - In hoeverre gaat dit middel mogelijk concurreren met huidige middelen?

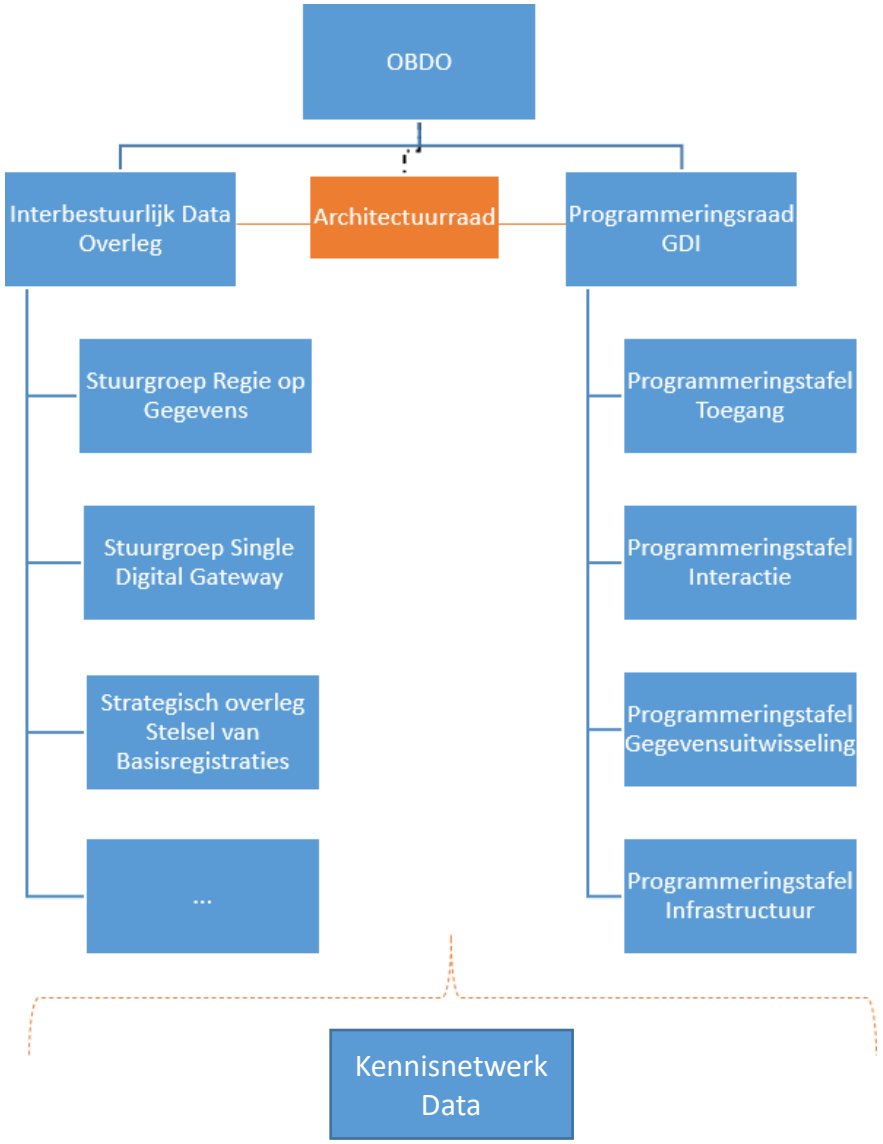
Bijlage Governance Digitale Overheid

Sturing Digitale Overheid (vereenvoudigde weergave)

OBDO = Overheidsbreed Beleidsoverleg Digitale Overheid
PGDI = Programmeringsraad Generieke Digitale Infrastructuur
PT = Programmeringstafel



Sturing Digitale Overheid (vereenvoudigde weergave)



Hier zit Pensioenfederatie aan tafel

Vanuit CBS, Kadaster en de VNG is voorgesteld om als invulling van het Public Ground3 initiatief een Kennisnetwerk Data in te richten. Dit netwerk kan op een gestructureerde manier de kennis leveren ter ondersteuning van datagedreven beleidsambities en de verschillende daarop gerichte (rijks)programma's.

Sturing Digitale Overheid

- Politiek Bestuurlijk Niveau
  - Staatssecretaris voert de regie op de (door)ontwikkeling.
  - Het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) adviseert haar daarbij.
  - Het OBDO geeft advies over het gebruik van digitale technologie om de modernisering van de overheid te stimuleren.

- Strategische niveau
  - Op strategisch niveau vindt afstemming plaats in het OBDO en de PGDI.
  - De Programmerings-raad GDI (PGDI) geeft het OBDO zwaarwegend advies over de prioritering en programmering van de GDI: hoe gaan we de doelen behalen. De PGDI overlegt met de partijen die de bouwstenen van de GDI ontwikkelen en beheren, zoals Logius, KOOP, RVO, KvK en RvIG. Daarnaast houdt de PGDI ook rekening met de wensen van afnemers van de bouwstenen.

- Tactisch Niveau
  - De PGDI krijgt input van de programmeringstafels. Voor elk GDI-domein is er een tafel waar ongeveer 12 personen aan deelnemen. De domeinen zijn:
    - Toegang;
    - Interactie;
    - Gegevensuitwisseling;
    - Infrastructuur.

Taken Vaste (kamer) Commissie Digitale Zaken

Samenstelling

Taken

1. Het voortouw nemen bij een coherente en integrale behandeling van commissie overstijgende digitaliseringsvraagstukken in de Tweede Kamer;
2. Het verkennen, doordenken en agenderen van huidige en toekomstige commissie overstijgende ontwikkelingen op het gebied van digitalisering;
3. Het controleren en behandelen van wetgeving van de bewindspersoon die verantwoordelijk is voor digitalisering of, in de afwezigheid daarvan, van de bewindspersoon tot wie de commissie zich primair verhoudt;
4. Het informeren van andere commissies in de Tweede Kamer over relevante ontwikkelingen op het gebied van digitalisering;
5. Het fungeren als aanspreekpunt voor digitaliseringskwesties voor zowel het kabinet als maatschappelijke groepen, bedrijfsleven, wetenschap en anderen.

- Kennisagenda voor het jaar 2022/2023:
  - Monitoren voortgang moties Marijnissen en Klaver;
  - Digitale toets;
  - Organiseren van (terugkerende) evenementen;
  - Quantum computing en gevolgen voor encryptie;
  - Algoritmes;
  - Artificiële intelligentie (AI);
  - Digitale weerbaarheid.

Sponsorgroep FBS

- Het opdrachtgeverschap gaat van de Programmeringsraad Logius (via de Sponsorgroep FBS) naar BZK DGDOO/Directie Digitale Samenleving (DS). Logius blijft opdrachtnemer.

- De Stakeholdergroep FBS geeft aan welke FBS-onderwerpen geagendeerd moeten worden bij de Programmeringstafel Interactie. De Programmeringstafel Interactie bepaalt welke onderwerpen door moeten naar de PGDI. Verdere escalatie is mogelijk via het OBDO en de DGDOO.

Overlegorganen met vertegenwoordiging pensioensector

Overlegorgaan	Vertegenwoordiger	Toelichting
Logius Klantenraad	Ad van Leest (APG, namens SDSO)	In de Klantenraad Logius wordt samen met stakeholders vooruitgekeken. De klantenraad geeft input en kan voorstellen doen voor (wijzigingen op) de Portfolio Roadmap. In deze roadmap worden de werkzaamheden tot twee jaar vooruit opgeschreven. Daarnaast wordt de samenhang op ontwikkelingen tussen de organisaties besproken om samen resultaten te behalen
Programmeringsraad Generieke Digitale Infrastructuur (PGDI)	Edith Maat (Pensioenfederatie)	De Programmerings-raad GDI (PGDI) geeft het OBDO zwaarwegend advies over de prioritering en programmering van de GDI: hoe gaan we de doelen behalen
Programmeringstafel Interactie	Ad van Leest (APG, namens SDSO)	Deze tafel geeft input aan de PGDI
Programmeringstafel Toegang	Melanie Meniar (Pensioenfederatie)	Deze tafel geeft input aan de PGDI
Stakeholdergroep Federatief Berichtenstelsel (FBS)	Ad van Leest (APG, namens SDSO)	Advies ten aanzien roadmap FBS

Overlegorganen met vertegenwoordiging pensioensector

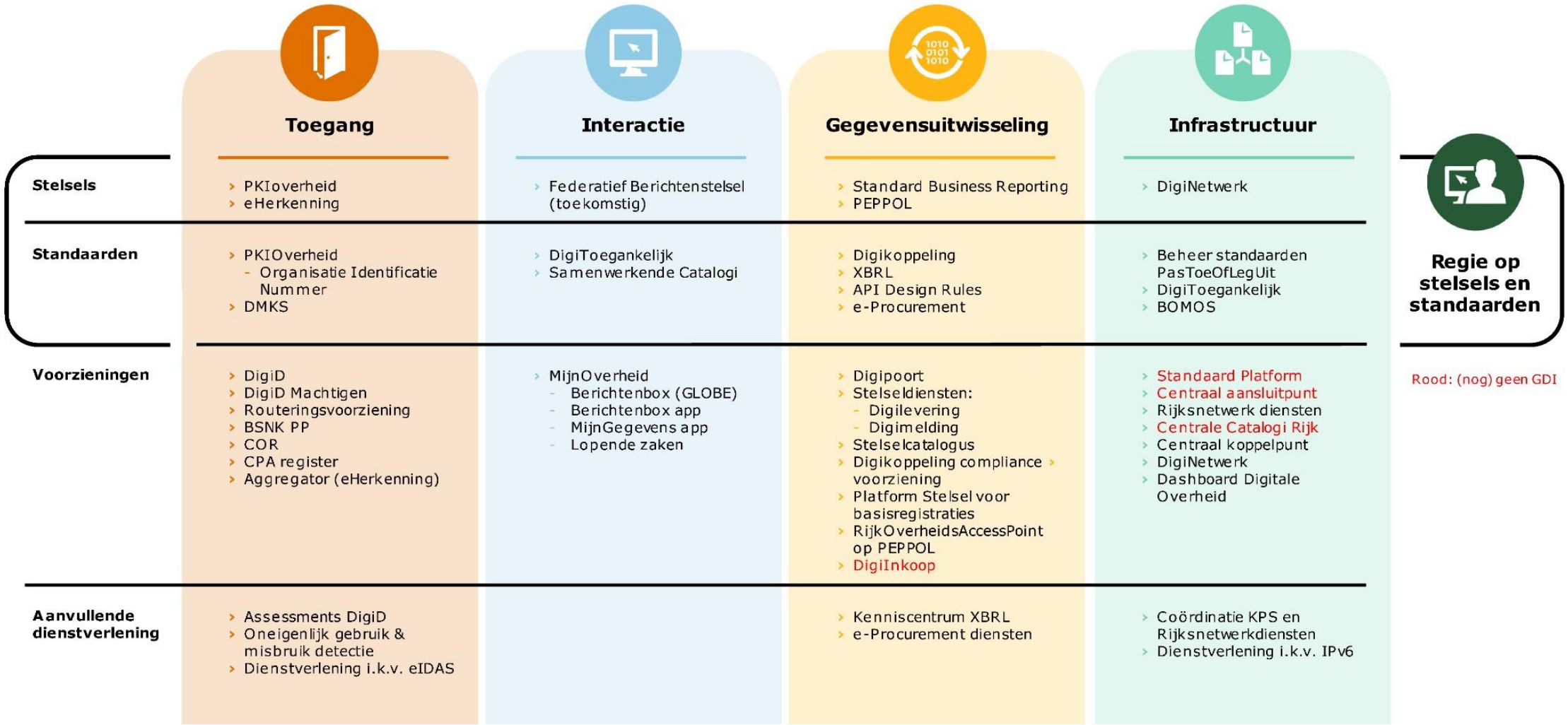
Overlegorgaan	Vertegenwoordiger	Toelichting
Gebruikersoverleg BRP	Melanie Meniar (Pensioenfederatie)	Richt zich op de belangen van afnemers van de BRP.
Werkgroep Ontwikkelingen BRP	Melanie Meniar (Pensioenfederatie)	Richt zich op de nieuwe ontwikkelingen rond de BRP.
WG Kwaliteit BRP	Eric Antwerpen (APG)	Richt zich op datakwaliteit van de BRP.
Afnemersoverleg Loonaangifteketen	Melanie Meniar (Pensioenfederatie)	Richt zich op de belangen van afnemers. Is betrokken bij de besluitvorming in de Loonaangifteketen daar waar het de samenstelling, de stabiliteit en de kwaliteit van de gegevensleveringen raakt. Bevordert het gebruik van zowel de collectieve als nominatieve gegevens uit de keten.
Tactisch Beraad eHerkenning	Ad van Leest (APG, namens SDSO)	Het Tactisch Beraad is verantwoordelijk voor: Inhoudelijke doorontwikkeling (tactisch beheer) van eHerkenning Besluiten over veranderingen en nieuwe functionaliteiten die worden voorgesteld door het Operationeel Beraad,
Strategisch Beraad eHerkenning	Jos Schaffers (Verbond van Verzekeraars)	Het Strategisch Beraad is verantwoordelijk voor de strategische visie en doorontwikkeling van eHerkenning,

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bijlage Dienstverlening Logius

Dienstverlening Logius

Dienstverlening Logius



Domein Toegang

DOMEIN TOEGANG - Het domein Toegang regelt voor publieke diensten via afspraken, standaarden en voorzieningen het kunnen vaststellen of een persoon bevoegd is om een bepaalde digitale dienst af te nemen.Tevens kan de bevoegdheid tot het digitaal handelen namens een persoon worden vastgesteld. Dit geldt zowelvoor natuurlijke- als voor niet-natuurlijke personen.

Interactiepatroon	Functie	Bouwsteen	Opmerking
Burger naar dienstverlener	Identificatie en authenticatie	DigiD	Afspraken, standaarden en voorzieningen, o.a. een app
		eIDAS	Europese verordening
		Identificatiemiddelen	In ontwikkeling in het kader van WDO
		Wallet	Onderwerp van eIDAS2
		Programma Toegang	Diverse bouwstenen
	BSN-uitgifte engebruik	BSNk-PP (polymorfepseudoniemen)	Standaard en voorziening
		BeheervoorzieningBSN	
	Machtigen en vertegenwoordigen	DigiD Machtigen	
		Machtigingenregister	
		Inzageregister (voor inzage in machtigingen)	In ontwikkeling
		Programma Toegang	Diverse bouwstenen
		Diverse oplossingenper dienstverlener	Machtigen met DigiD vaak nietmogelijk
Bedrijf naar dienstverlener	Identificatie en authenticatie	eHerkenning	
		Identificatiemiddelen	Wdo
		Wallet	eIDAS2
	Machtigen en vertegenwoordigen	eHerkenning	

Domein Interactie

DOMEIN INTERACTIE - Het domein Interactie gaat over afspraken, standaarden en voorzieningen ten behoeve van interactieverkeer met burgers en ondernemers. Als ook het digitaal ter beschikking stellen van officiële overheidspublicaties.

Interactiepatroon	Functie	Bouwsteen	Opmerking
Dienstverlener naarburger	Persoonlijke berichten aan burger	MijnOverheid Berichtenbox	
		Federatief Berichtenstelsel	In ontwikkeling
	Overzicht persoonsgebonden en gegevens	MijnOverheid	MijnOverheid PersoonlijkeGegevens
	Overzicht lopende zaken	MijnOverheid	MijnOverheid Lopende Zaken
Dienstverlener naarbedrijf	Algemene informatie verschaffen aanbedrijven	Digitaal Ondernemersplein	
		Antwoord voorOndernemers	
	Berichten aan en van bedrijf	Berichtenbox voorondernemers	2-weg berichtenverkeer
	Algemene Niet persoonsgebonden informatie verschaffen	Overheid.nl	
		Single DigitalGateway	Europese Unie

Domein Gegevensuitwisseling

DOMEIN GEGEVENS - Het domein Gegevensuitwisseling gaat over voorzieningen ten behoeve van geautomatiseerde gegevensuitwisseling tussen het bedrijfsleven en overheid en overheid onderling.

Interactiepatroon	Functie	Bouwsteen	Opmerking
Bedrijf naar dienstverlener	Aanleveren bedrijfsgegevens	Digipoort	Voorziening
	Aanleveren financiële bedrijfsgegevens	Standard BusinessReporting	Standaard
		XBRL	Standaard
Bedrijf als leverancier van overheid	Inkoop dooroverheid	Peppol	Standaarden voor inkoop
	Facturatie aanoverheid	e-Factureren	Standaarden en voorzieningenvoor facturering
Regie op gegevens	Regie op gegevens	Regie op gegevens	Een overheidsprogramma
	Burger of bedrijfnaar dienstverlener	Wallet	Onderwerp van eIDAS2
		Self SovereignIdentity	Internationale ontwikkeling
Gebruik van gegevens door burger, bedrijf, instelling, publiekedienstverlener en overheid	Authentiekebron	Basisregistraties	Wel GDI, sturing apart vanMIDO
	Overigebronnen	Diverse overheidsregistraties	
	Gegevenscatalogus	Stelselcatalogus	
		Dataregister van deNederlandse Overheid	Overzicht van datasets van overheidsinstellingen
	Gegevenslevering o.b.v. abonnementen	Digilevering	
Gegevenskwaliteit	Melding van gerede twijfel	Digimelding	Standaard en voorziening
	Corrigeren vanfouten	Meldpunt Fouten in Overheidsregistraties	Onderdeel van RvIG

Bouwstenen Logius

Bouwstenen	Toelichting
API-standaarden	Een werktitel van Logius voor API's. Maar de titel dekt niet de lading, zie API-standaarden | Logius Het ligt voor de hand dat API-standaarden een aspect is dat wordt beschreven bij het thema API. Evenals de afspraken over en de voorzieningen voor API's.
Beheervoorziening BSN	Een voorziening waarmee een éénduidige toekenning van een BSN kan worden gegeven aan burgers en aan buitenlanders die met Nederland te maken hebben en waarmee tevens toegang kan worden verkregen tot identificerende gegevens in de BRP, de achterliggende authentieke bron.
Berichtenbox voor bedrijven	Een voorziening waar overheidsorganisaties en bedrijvenop een veilige en vertrouwelijke manier digitale berichten met elkaar kunnen uitwisselen.
BOMOS	Een standaard model voor het beheer en ontwikkelenvan open standaarden. Dit model is ook toe te passen voor (referentie)architecturen, afsprakenstelsels en voorzieningen.
BSNk (Polymorfe Pseudonimisering	Een voorziening die het mogelijk maakt om publieke en private authenticatie- en machtigingsmiddelen met een hoog betrouwbaarheidsniveau te gebruiken in het publieke domein, waarbij de privacy en de veiligheid vande burger bij het inloggen wordt gewaarborgd.
Dataregister van de NederlandseOverheid	Een voorziening in de vorm van een publicatieplatform waarlangs overheidsorganisaties hun gegevens (data) in een voor hergebruik geschikte vorm beschikbaar stellen.
Developer.Overheid.nl	Een voorziening in de vorm van een publicatieplatformvan API's en Open Source repositories, waar software wordt getoond die is gepubliceerd onder verantwoordelijkheid van overheidsorganisaties.

Bouwstenen Logius

Bouwstenen	Toelichting
DigiD	Een voorziening waarmee overheidsorganisaties en publieke dienstverleners online de identiteit van burgers en kunnen vaststellen.
DigiD Machtigen	Een voorziening waarmee een burger een andere burger kan machtigen om namens hem zaken met de overheid te regelen.
Digipoort	Een voorziening waarmee bedrijven via 1 aanleverpunt(bulk)gegevens digitaal kunnen aanleveren bij de betreffende overheidsorganisatie(s). En ook andersom.
Digitaal Odernemersplein (DOP.nl)	Een voorziening in de vorm van een digitaal loket, een Digitaal Ondernemersplein (DOP), waar de dienstverlening van de overheid integraal voor bedrijven wordt ontsloten.
Digitoegankelijk	De wettelijke afspraak om websites en mobiele appstoegankelijk te maken voor mensen met een functiebeperking (zoals dyslectici, kleurenblinden, slechtzienden en blinden), door de standaard EN 301549 (WAGC 2.1) toe te passen en daar een toegankelijkheidsverklaring over te publiceren.
E-factureren	Een voorziening van de overheid waarmee facturen digitaal worden verzonden, ontvangen en verwerkt (in plaats van per brief en op papier).
eHerkenning	Een voorziening waarmee (medewerkers van) bedrijven zich veilig en betrouwbaar kunnen laten identificeren bij overheidsorganisaties.

Bouwstenen Logius

Bouwstenen	Toelichting
eIDAS	Een EU-afsprakenstelsel over begrippen, digitale identiteiten van burgers, betrouwbaarheidsniveaus en het onderlinge gebruik van digitale infrastructuren, waardoor Europese burgers en bedrijven met hun eigen nationale toegangsmiddel kunnen inloggen bij publieke dienstverleners van de andere Europese lidstaten.
Federatief Berichten Stelsel	Een voorziening waarmee overheidsorganisaties op eenvoudige en efficiënte wijze berichten kunnen sturen aan burgers en ondernemers. Hierbij verblijft de feitelijke informatie - de berichten en hun metadata t.b.v. het berichtenoverzicht - bij de bron en kunnen deze middels verschillende kanalen zichtbaar worden gemaakt: op MijnOverheid-web of -app, het mijn-portaal van de afzender, of misschien op termijn middels een systeem-naar-systeem koppeling (API) naar de toekomstige digital personal assistent van de individuele gebruiker.
Forum Standaardisatie (open standaarden)	Forum Standaardisatie is een adviescommissie met deskundigen uit diverse overheidsorganisaties, het bedrijfsleven en de wetenschap. De leden worden op persoonlijke titel benoemd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Het Forum wordt ondersteund door het Bureau Forum Standaardisatie (BFS). Dit bureau is gehuisvest bij Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
Identificatiemiddelen	Het programma Toegang realiseert bouwstenen ten behoeve van toegang tot overheidsdiensten geschikt voor publieke enerkende en genotificeerde inlogmiddelen.
Internet	Een wereldwijd openbaar netwerkvan computernetwerken. Zie ook de ontwikkeling van Solid (Social Linked Data), waarbij een gedecentraliseerd internet wordt opgebouwd met bescherming van de gegevens en privacy by-design.
Inzageregister (voor inzage inmachtigingen)	Via het inzageregister kan iedereen zelf zien welke middelen er aan zijn of haar BSN zijn gekoppeld. Als blijkt dat een onbekend middel is gekoppeld, dan kande persoon zelf actie ondernemen. Dit inzageregister wordt momenteel gebouwd door Logius.

Bouwstenen Logius

Bouwstenen	Toelichting
Machtigingenregister	In het machtigingenregister staat welke organisatie gemachtigd is voor het digitaal ophalen van berichten en gegevens voor een specifieke klant. In de praktijk zijn dit vaak intermediairs, die namens hun klanten berichten en gegevens uitwisselen met de Belastingdienst of het Uitvoeringsinstituut Werknemersverzekeringen (UWV). Logius beheert het machtigingenregister en maakt de juiste koppelingen.
Meldpunt Fouten in Overheidsregistraties	Een voorziening in de vorm van een meldpunt met ambtenaren en een platform, om burgers, bedrijven en overheidsorganisaties te helpen bij het laten corrigeren van fouten in overheidsregistraties.
MijnOverheid Berichtenbox	Een voorziening binnen MijnOverheid.nl waar overheidsorganisaties op een veilige en vertrouwelijke manier digitale berichten kunnen plaatsen voor burgers die dan per email worden geïnformeerd dat een bericht voor hen klaar staat.
MijnOverheid.nl	Een voorziening in de vorm van een digitaal loket, waarburgers op een veilige en gemakkelijke manier hun persoonlijke gegevens bij de overheid kunnen inzien, berichten van overheidsorganisaties digitaal kunnen ontvangen, en de status van lopende zaken en transacties kunnen volgen.
NLX	Een afsprakenstelsel met decentrale voorzieningen in devorm van open source software-modules, die samen zorgen voor snelle, veilige en AVG-proof gegevensuitwisseling binnen en tussen (overheids)organisaties.
NORA	Een afsprakenstelsel in de vorm van een (referentie)architectuur, dat inzicht geeft in de samenhang van “alles” wat voor de dienstverlening van de overheid nodig is: wet- en regelgeving, mensen,processen, gegevens, systemen e.d.

Bouwstenen Logius

Bouwstenen	Toelichting
Organisatie-identificatienummer	Het Organisatie-identificatienummer (OIN) is een uniek nummer dat Logius kan toekennen aan organisaties om zich te kunnen identificeren, authentiseren en of autoriseren bij digitaal berichtenverkeer binnen en met de overheid. Dit kunnen publieke en private organisaties zijn.
Overheid.nl	Een voorziening in de vorm van een website, waar de overheid informatie voor burgers en bedrijven publiceert, waaronder alle wet- en regelgeving en overheidsdienstenin Nederland.
Peppol	Standaarden voor het efficiënter communiceren van leveranciers met de verschillende Europese overheidsorganisaties bij inkoopprocessen.
PKIoverheid	Een voorziening voor de uitgifte van certificaten voor betrouwbare identificatie, digitale handtekeningen en veilige gegevensuitwisseling.
Programma Toegang	Het programma Toegang realiseert bouwstenen t.b.v. toegang tot overheidsdiensten.
Regie op Gegevens	Een programma dat een afsprakenstelsel met voorzieningen realiseert om burgers regie te kunnenlaten voeren op hun eigen persoonsgegevens bij de overheid, binnen de bestaande wettelijke kaders die daarvoor (gaan) gelden.
Register van Overheidsorganisaties	Een voorziening binnen Overheid.nl in de vorm van een digitale registratie, met een overzicht welke organisaties tot de overheid behoren en wat hun wettelijke taken en bevoegdheden zijn.
Routeringsvoorziening	Een voorziening waarop publieke dienstverleners zich éénmalig kunnen aansluiten en daarmee worden ontzorgd voor het afhandelen van alle toegelaten inlogmiddelen (authenticatiemiddelen) die burgers toegang verlenen om hun online zaken te regelen.
Samenwerkende catalogi	Een voorziening in de vorm van een verwijsmechanisme,waardoor een overzicht kan worden getoond van de overheidsdiensten die de ca. 1200 overheidsorganisaties afzonderlijk leveren.

Bouwstenen Logius

Bouwstenen	Toelichting
Sectorregistraties	Voorzieningen in de vorm van overheidsregistraties (niet zijnde Basisregistraties). Deze sectorregistraties kunnen dienen als authentieke bron voor de gegevens die nodig zijn voor de overheidsdienstverlening. En daarnaast als open data voor de samenleving.
Self Sovereign Identity	Een wereldwijd concept, in de vorm van een mogelijk afsprakenstelsel met standaarden en voorzieningen, voor regie op gegevens door (wereld)burgers.
Single Digital Gateway (SDG)	Een EU-afsprakenstelsel (EU-verordening) dat moet stimuleren dat alle burgers en bedrijven binnen de EU eenvoudig toegang kunnen krijgen tot overheidsdiensten van alle EU-lidstaten via een Single Digital Gateway in de vorm van de voorziening Your Europe (europa.eu).
Standaard Platform	Een voorziening in de vorm van clouddienstverlening die bestaat uit kant-en-klare werkomgevingen waarmee overheden zelf hoogwaardige digitale diensten als applicaties of websites kunnen ontwikkelen, testen en beheren.
Standard Business Reporting(SBR)	Een standaard voor het digitaal aanleveren van de financiële verantwoordingsinformatie van bedrijven en overheidsorganisaties aan de overheid c.q. het Ministerie van Financiën.
Stelselcatalogus	Een voorziening in de vorm van een registratie met daarin de betekenis van de gegevens in Basisregistraties.
Wallet	Een voorziening in de vorm van een online service of softwareprogramma dat vertrouwelijke gegevens kan bevatten, zoals persoonlijke attributen, identificatiegegevens, inloggegevens en bankpassen, en dat de bezitter in staat stelt digitale transacties uit te voeren, zoals aantonen van zijn identiteit, attributen verstrekken en betalingen te doen.
XBRL	eXtensible Business Reporting Language (XBRL) is een internationale open standaard om (financiële)bedrijfsgegevens op eenvoudige wijze uit tewisselen via het internet.

Bijlage Progammeringsraad GDI

Generieke Digitale Infrastructuur (GDI)

- De GDI is de set aan afspraken, standaarden en voorzieningen die overheidsorganisaties en dienstverleners met een publieke taak ondersteunt bij de inrichting van hun digitale dienstverlening aan burgers en ondernemers en bij hun onderlinge digitale samenwerking. Het perspectief van burgers en ondernemers is hierin leidend: de publieke digitale dienstverlening is voor burgers en ondernemers beschikbaar, veilig en gemakkelijk in gebruik. De GDI bevat de generieke bouwstenen die nodig zijn om dit te bereiken.

- De scope is beschreven in functionaliteiten die generiek bijdragen aan:
  - de digitale publicatie van wet- en regelgeving,
  - veilige digitale communicatie met de overheid,
  - veilige digitale toegang van burgers en ondernemers tot de overheid (identificatie en authenticatie).

- Daarnaast omvat de GDI:
  - de basisregistraties en
  - de afspraken, (open) standaarden en stelsel-voorzieningen die ervoor zorgen dat burgers en ondernemers met de overheid en overheden onderling met elkaar kunnen communiceren en samenwerken.

GDI-Programmeringsplan 2023

- Concreet wordt in 2023 het volgende opgeleverd:
  - GDI-architectuur Gegevensuitwisseling;
  - GDI-architectuur eIDAS2, wallet en Digitale Bronidentiteit;
  - GDI-architectuur Interactie;
  - Overkoepelende GDI-architectuur;
  - GDI-architectuur Data-domein;
  - GDI-architectuur Regie op Gegevens ;
  - Bijdrage aan GDI-afwegingskader;
  - Architectuurtoetsen en –adviezen;
  - Bijdrage aan het Programmeringsplan 2024;
  - Communicatie over de architectuur via infographics en presentaties.

- Het Jaarplan GDI-architectuur 2023 bevat een uitwerking hiervan, inclusief meer achtergrond over de samenhang van de GDI-architectuur met andere architecturen en de samenhang van GDI-bouwstenen.

GDI-Programmeringsplan 2023

- Berichtenbox
  - Maakt onderdeel uit van MijnOverheid.nl. Geen specifieke ontwikkeling opgenomen.

- Berichtenbox voor bedrijven
  - Het portaal voor digitale berichten aan ondernemers verkeert momenteel in de fase van visieontwikkeling. Deze visie wordt ontwikkeld door BZK in samenwerking met de uitvoeringsorganisaties die diensten verlenen aan ondernemers, zoals de KVK en RVO.

- Gegevensuitwisseling 2.0
  - Experimenteren met generieke manieren van gegevensuitwisseling onder regie van de burger op een hoog betrouwbaarheidsniveau (eIDAS), vooruitlopend op de komst van wallets of regietoepassingen.

- Zie verder Bijlage Toegang.

Bijlage Toegang

DigiD

- DigiD is een op BSN gebaseerde Authenticatiedienst. Elektronische authenticatie is het elektronisch vaststellen dat een persoon een bepaalde identiteit terecht claimt.

- Momenteel zijn er 17miljoen DigiD accounts waarvan 11 miljoen (ook) gebruik maken van de DigiD app. Daarvan zijn er 7 miljoen ID-gevalideerd. Op jaarbasis vinden er 600 miljoen DigiD inloggen plaats waarvan 300 miljoen zonder de DigiD app.

- DigiD wordt het publieke inlogmiddel in het in wording zijnde Toegang-stelsel onder de Wet Digitale Overheid. Hierdoor zullen nieuwe functies nodig zijn, en andere technische en beveiligingseisen worden gesteld aan de DigiD-authenticatievoorziening. Verder werkt de overheid aan het verbeteren van het aansluitproces zodat het sneller, eenvoudiger en minder arbeidsintensief is.

eIDAS

- eIDAS betrouwbaarheid wordt bepaald op de kwetsbaarheid van drie aspecten: uitgifteproces, inlogmiddel en infrastructuur. Als die bestand alle drie zijn tegen een aanvaller met een substantiële hoeveelheid tijd en middelen dan is het niveau Substantieel.

- De afgelopen jaren zijn er verschillende oplossingen ontwikkeld onder de noemer DigiD op drie betrouwbaarheidsniveaus: eIDAS laag, substantieel en hoog. Inmiddels beschikken veel mensen over een substantieel middel; hoog-middelen zijn in 2021 beschikbaar gekomen.

- DigiD is recent aangesloten te zijn op het Europese eIDAS netwerk, zodat een burger zijn DigiD ook bij buitenlandse dienstverlener kan gebruiken.

- eIDAS 2 moet weerwoord bieden aan “Big Five”. Een of meer publieke en private ‘wallets’ voor burgers én bedrijven, met digitale identiteiten én andere gegevens , inclusief elektronische vertrouwensdiensten, voor gebruik in (semi)overheid én in bedrijfsleven. Biedt de burger meer autonomie en Regie op Gegevens .

eIDAS – status implementatie (1 november 2022)

Erkend en actief in NL	Erkend niet actief in NL	In erkenningsproces
België (Belgische eCard, Itsme))	Frankrijk (LaPoste)	Positief oordeel lidstaten:
Denemarken (NemID)	Oostenrijk (Oostenrijkse eID)	Denemarken (MitID)
Duitsland (Duitse eID)	Tsjechië (MojeID, MEG)	Noorwegen(BankID, Buypass ID)
Estland (Ests eID-stelsel)		
Italië (SPID, CIE)		
Kroatië (eOI)		
Letland (Lets eID, eParaksts)		
Litouwen (ATK)		
Luxemburg (Luxemburgse eID)		
Malta (Malta eID, Malta e-RP kaart)		
Portugal (Portugese Nationale eID, CMD)		Nog geen oordeel lidstaten:
Slowakije (Slowaakse eID)		Bulgarije (Evrotrust eID)
Spanje (DNIe)		Liechtenstein (eID.li)
Tsjechië (Tsjechische eID-kaart)		Polen (Public Electronic Identification System)
Zweden (Zweeds eID)		

eIDAS – status implementatie (1 november 2022)

Organisaties	Aangesloten dienstverleners	Aangesloten diensten	Authenticaties oktober 2022
Belastingsamenwerking	4	4	
Gemeente	179	254	97
Omgevingsdienst	1	1	
Onderwijs	1	1	100
Overig	12	14	176
Pensioenuitvoerder	33	33	2.227
Provincie	9	16	
Rechtspraak	3	3	
Rijk	3	4	260
Uitvoeringsorganisatie (Klein Lef)	2	11	32
Uitvoeringsorganisatie (Manifestgroep)	12	24	6.756
Waterschap	10	17	
Zorg	6	8	637
Eindtotaal	275	390	10.285

Machtigen

- Machtigen is een vorm van autorisatie, op basis van vrijwilligheid, een eigen wilsbeschikking.

- Naast vrijwillig machtigen wordt in het programma Vertegenwoordigen aan de wettelijke variant gewerkt; ouderlijk gezag, bewindvoerders en curatoren, en bijvoorbeeld erven. Vanwege de verdeelde verantwoordelijkheden op dat gebied, verschillende regels voor verschillende zaken en het al dan niet bestaan van onderliggende registers zullen deze oplossingen meerdere jaren nodig hebben voordat ze volwaardig gerealiseerd en breed dekkend zijn.

- Eind 2021 waren er ruim 2mln machtigingen geregistreerd. Hiervan waren ongeveer 250.000 de belastingaangifte over 2020 en 1,5mln die van eerdere jaren.

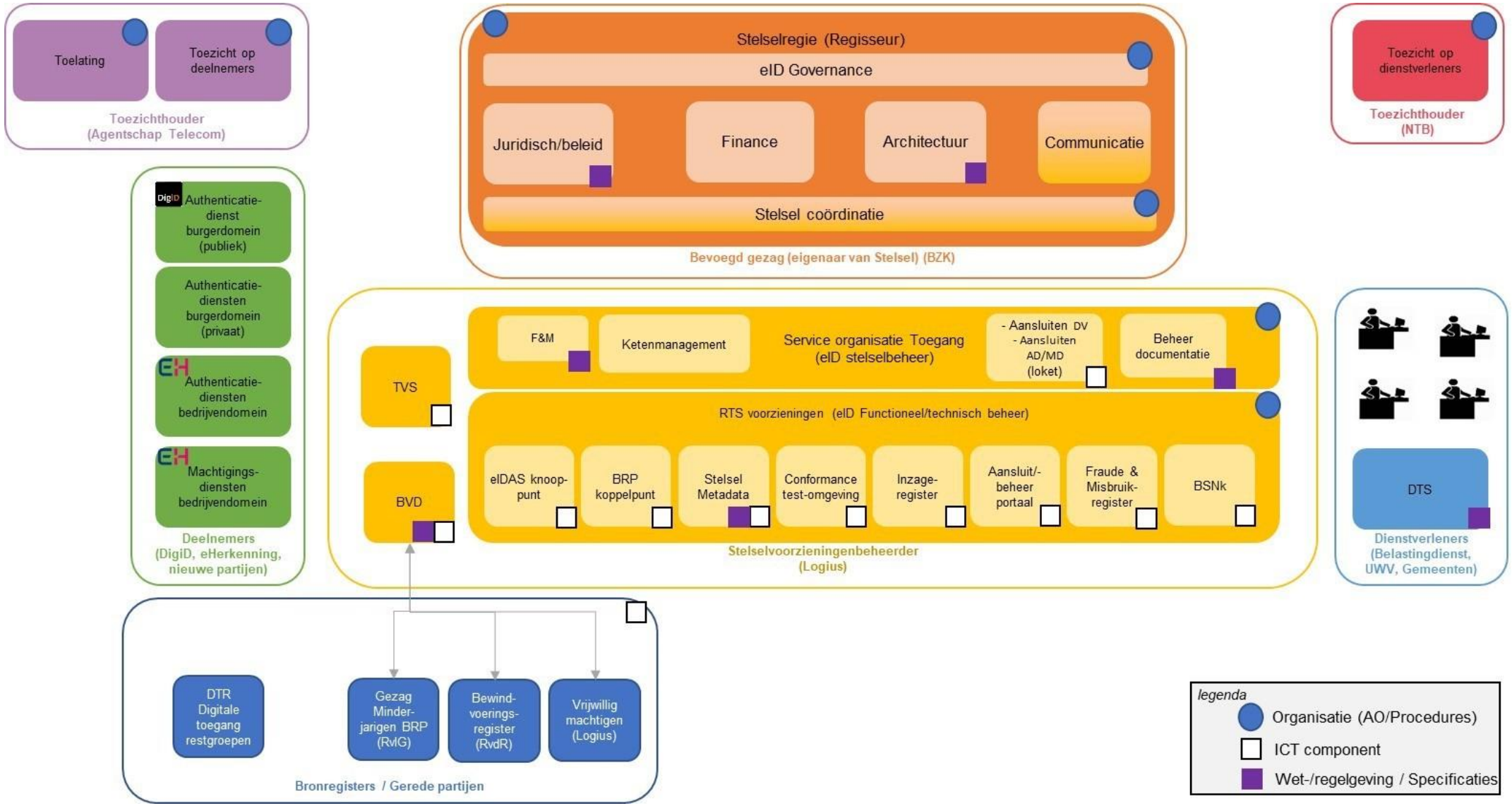
- In 2021 zijn de machtigingen ongeveer 13,4 mln. keer geslaagd getoetst op bestaan.

- Elke machtigingsregistratie bestaat uit de 3 componenten:
  - de machtigingsdienst (waarvoor is iemand gemachtigd);
  - de identiteit van de gemachtigde (actor);
  - de identiteit van de vertegenwoordigde (subject).

eHerkenning

- Marktwerking:
  - Iedere dienstverlener kan eigen makelaar kiezen;
  - Meerdere aanbieders van middelen,
- Brede inzetbaarheid.
- Dienstaanbieder bepaalt het betrouwbaarheidsniveau:
  - eH3 is norm in verzekeringsbranche.
- Ketenmachtiging.
- Landelijke dekking middel: onder druk van nieuwe wetgeving (Wet Digitale Overheid, eIDAS) is eHerkenningsmiddel straks overal te gebruiken. De facto landelijke standaard zakelijke authenticatie.
- Verzekeringsbranche als eerste private sector over op eHerkenning.
- Meer innovatie.
- Waar kunt u inloggen
- Makelaars
- Leveranciers middelen

Doelarchitectuur Toegang



Doelarchitectuur Toegang

- Strategisch Beraad eHerkenning, Doelarchitectuur Toegang, 27 september 2022
- De Doelarchitectuur Toegang is in juli 2022 in de DG Stuurgroep als uitgangpunt vastgesteld. Volledige realisatie van de doelarchitectuur zal gevolgen hebben voor het stelsel voor eHerkenning en hoe dienstverleners daar in de toekomst van gebruik maken.
- De belangrijkste (voornamelijk technische) gevolgen hebben in de praktijk de volgende (verwachte) effecten voor het stelsel en de aangesloten dienstverleners:
  - De Machtigingsregisters van eHerkenning zullen voortaan de samenvattende verklaring dat iemand is wie hij zegt dat hij is (de identiteit), en dat hij mag doen wat hij zegt dat hij mag doen (de machtiging of autorisatie), moeten gaan leveren in plaats van de Herkenningsmakelaars. Dit betekent een technische wijziging voor de eHerkenningsleveranciers waarvoor zij investeringen moeten doen.
  - De dienstverleners worden verantwoordelijk gemaakt voor de aansluiting op erkende bedrijvenmiddelen (zoals eHerkenning) in plaats van de Herkenningsmakelaars. De dienstverleners moeten óf zelf de aansluiting op de verschillende erkende bedrijvenmiddelen verzorgen, of gebruik maken van een interne ICT-leverancier, een publieke (de TVS) of een externe leverancier (Identitybrokers zoals KPN, Digidentity, Onewelcome bijv.) om aan te sluiten. Terwijl nu een aansluiting op en contract met een Herkenningsmakelaar onontbeerlijk is. Als gevolg hiervan en van de verandering onder 1) voorzien de Herkenningsmakelaars dat zij formeel geen deel meer uit zullen maken van het stelsel en derhalve niet meer onder de vlag van eHerkenning services zullen kunnen leveren. Het wordt onzeker of verschillende recente investeringen in de huidige Herkenningsmakelaar nog lonen.
  - Er zal een implementatie volgen van een nieuw onbeproefd technisch koppelvlak. Dit brengt een migratie voor dienstverleners met zich mee van hun aansluitingen op het huidige koppelvlak naar het nieuwe. De verwachting is dat dit niet in 1x gebeurd maar stapsgewijs. Dienstverleners zullen niet allemaal op het zelfde moment klaar zijn en in 1x over kunnen. Het lijkt dan tijdelijk noodzakelijk om aansluitingen op twee verschillende koppelvlakken in stand te houden en te ondersteunen. Ook het “oude” ETD-stelsel zal tijdelijk in stand gehouden en beheerd moeten worden. O.a. technische incidenten zullen nog steeds opgelost moeten worden. Hoe lang het migratietraject mag duren is onduidelijk.

eHerkenning en identificatieplicht

- Strategisch Beraad, Gebruik HRM Database, 26 juli 2022
  - Voor de uitgifte van inlogmiddelen vanaf niveau 2 mag volgens het Afsprakenstelsel voor de identiteitsverklaring worden gesteund op identiteitsgegevens uit de HRM-database van de werkgever. De werkgever heeft namelijk een plicht om bij indiensttreding de identiteit van werknemers te controleren aan de hand van het identiteitsdocument, en daar gegevens over vast te leggen in zijn/haar administratie, de HRM-database. Op niveau 4 dient de identiteit van de gebruiker evengoed gecheckt te worden via een fysieke controle. Het gebruik van de HRM-database maakt het mogelijk om snel veel inlogmiddelen te verstrekken tegen lagere kosten. Wel is het mogelijk dat er onjuiste identiteitsgegevens, bijvoorbeeld door handmatige fouten, in een HRM-database staan.
  - Of dit in het kader van de uitgifte van eHerkenningsmiddelen ook werkelijk fouten tot gevolg heeft of zelfs tot misbruik leidt, is niet bekend. Er zijn tot op heden geen concrete incidenten bekend met uitgegeven eHerkenningsmiddelen als gevolg van het gebruik van de HRM-database. Dat wil niet zeggen dat die onjuiste/onvolledige identiteitsgegevens er niet zullen zijn. Maar hoewel de kans aanwezig is, is het moeilijk in te schatten dat precies door die werknemers waarbij dit het geval is, ook een eHerkenningsmiddel wordt uitgegeven. En als dat wel gebeurt, dan is nog onbekend of dit bewust of onbewust tot stand gekomen is. Het gebruik van de HRM-database is nog maar van beperkte duur. De Wet digitale overheid (WDO) zal het gebruik ervan niet toe laten, is de verwachting.

- Deze situatie (die verborgen blijft in de uitingen van Logius) wordt gedoogd, maar is onhoudbaar. Een groot deel van de gebruikers van eHerkenning zal binnen afzienbare tijd zijn/haar middel moeten opwaarderen.

Agenda Toegang 2023

- DigiD:
  - Substantieel is de basis;
  - DigiD vernieuwt: eenvoudige herauthenticatie, ontwikkelingen rond afgifte Digitale Bronidentiteit, eventueel EU-wallet.

- DigiD Machtigen:
  - Meer vrijwillig machtigen (sneller, meervoudige machtigingen, inclusief voor niet-digivaardigen, onderzoek betrouwbaarheidsniveaus, balieprocessen).

- eHerkenning:
  - Doorontwikkeling eHerkenning: ketenmachtigingen en restgroepen.

Agenda Toegang 2023

- Elektronische Digitale Identiteit
  - Nederland moet per 2025 een raamwerk hebben staan om de Europese Digitale Identiteit (EDI)-verordening (de revisie van de eIDAS verordening) in te vullen. Daarbinnen kunnen burgers uit andere EU-landen met hun nationale EDI-wallet en Nederlanders met onze nationale EDI-wallet digitaal zichzelf identificeren, een elektronische handtekening zetten en gegevens en documenten delen in het publieke en het private domein. Dit programma gaat dit stelsel en de publieke voorbeeldwallet maken en de infrastructuur daaromheen inrichten.

- Integratie eIDAS wallet en de GDI
  - Het betreft een voorstel tot een onderzoek over hoe een nieuw te vormen wettelijke verantwoordelijkheid voor de burger als medeverantwoordelijke voor het bijhouden en de verstrekking van zijn eigen (persoons)gegevens vorm kan krijgen.
  - Eveneens wordt onderzocht hoe de burger betrouwbare verklaringen van derden kan gebruiken in het bijhouden van zijn eigen (persoons)gegevens. Daartoe is een onderzoeksopzet opgesteld met daarin een vooronderzoeksfase en een praktijkproef in een pilot. De uitkomsten zijn beschikbaar in 2025 en zijn ter ondersteuning van de beleidsvorming.

Stip op horizon: Digitale Bron Identiteit (DBI)

- Een door de overheid uitgegeven, erkende en in de wet en regelgeving verankerde, digitale identiteit voor gebruik in de publieke en private sector. Deze digitale bronidentiteit bevat een minimale set van identiteitsgegevens die nodig zijn in het maatschappelijk verkeer. De overheid creëert met de digitale bronidentiteit een ‘gezaghebbende bron’ van betrouwbare persoons identificerende gegevens.

- Onder een digitale identiteit wordt een verzameling gegevens verstaan, die een entiteit (persoon of organisatie) in het digitale domein representeert.

- Het toevoegen van biometrische gegevens vergroot de betrouwbaarheid van de DBI.

- Biometrie is momenteel de meest nauwkeurige en efficiënte technologie die beschikbaar is om grote populaties te ontdubbelen om statistische uniciteit te garanderen.

- De volgende modaliteiten lijken het best toepasbaar voor het ontdubbelen en het uitgeven van de DBI:
  - Vingerafdruk;
  - Gezicht;
  - Iris.

Bijlage Externe Databronnen

Gegevensuitwisseling Pensioenuitvoerders

Ontwikkelingen bronsystemen

Bron	Toelichting
UWV/Polisadministratie	UWV heeft een applicatie, configureerbare webservices (CWS), ontwikkeld waarmee ze realtime persoons- en Loonaangiftegegevens op maat kunnen leveren aan zowel interne als externe afnemers.
KVK - Handelsregister	KVK-API-service .
BRP	Het programma Haal Centraal ontwikkelt API's waarmee gemeenten en andere overheidsorganisaties basisgegevens rechtstreeks bij landelijke registraties kunnen bevragen. In verband met de bereikbaarheid van de pensioendeelnemers is een breed gedragen wens binnen de pensioensector dat contactgegevens (emailadres en mobiele telefoonnummer) aan de BRP worden toegevoegd. Dit is nog niet gerealiseerd.
CCBR	Centraal Curatele en Bewind Register, API beschikbaar, geen ondersteuning.

Bijlage bij Kamerbrief stand van zaken BRP 2022 - Ontwikkelagenda

- Opnemen digitale contactgegevens
  - De BRP bevat waar het gaat om gegevens waarmee contact gelegd kan worden met de burger alleen het fysieke adres waar post heen gestuurd kan worden of een huisbezoek kan worden afgelegd. Gegevens die gebruikt kunnen worden voor digitaal contact (e-mailadres, telefoonnummer) zijn niet opgenomen in de BRP, terwijl de overheid daar wel behoefte aan heeft, bijvoorbeeld om snel en op alternatieve wijze contact op te kunnen nemen met de burger. In het kader van de Ontwikkelagenda zal uitgewerkt worden hoe registratie, bijhouding en gebruik van digitale contactgegevens vorm kan krijgen. Een eerste stap wordt - vooruitlopend hierop - al gezet door digitale contactgegevens te registreren bij registratie van niet-ingezetenen in de BRP.

- Opgeleverd deelresultaat:
  - Systemen worden aangepast om de registratie van e-mailadressen en telefoonnummers van niet-ingezetenen mogelijk te maken. Het registreren start in oktober 2022.

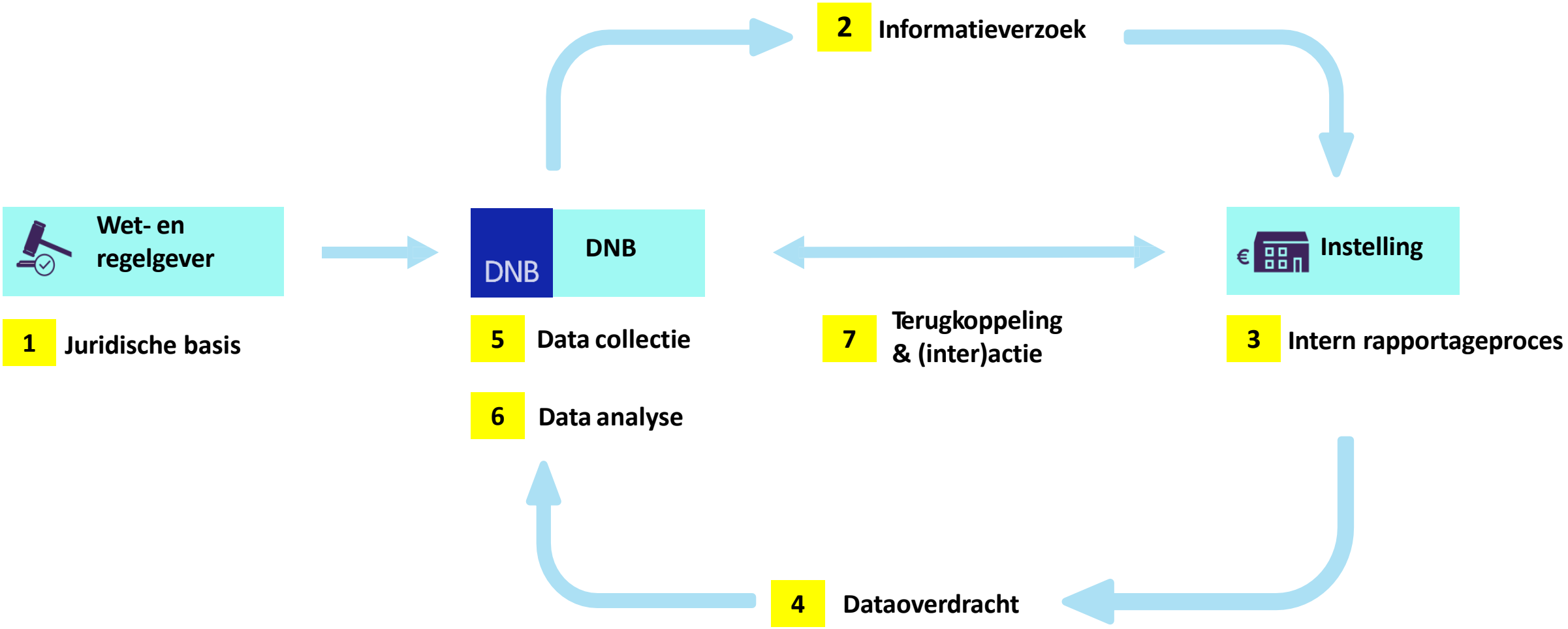
- In uitvoering, vervolgstappen in 2023/ (deel)resultaat verwacht in 2023:
  - Onderzoek of ook voor ingezetenen registratie van e-mailadressen en telefoonnummers zal worden ingevoerd. Hierbij zullen de ervaringen met de registratie van contactgegevens van niet-ingezetenen worden betrokken.

Bijlage: Toezichthouders

Waarnemingen

- Toezicht in Beeld, DNB december 2021
  - DNB zal in 2022 nader uitwerken hoe het toezicht zal houden op (de transitie naar) het nieuwe pensioenstelsel.
- Good Practice Robuuste Pensioenadministratie, DNB oktober 2021
  - Complexiteit in regelingen kan leiden tot een verhoogde kans op fouten in de berekening van pensioenaanspraken. De complexiteit leidt vaak ook tot hogere (uitvoerings)kosten, maakt de regelingen moeilijker uitlegbaar en bij aanpassingen in de regeling zijn er grotere operationele uitdagingen en risico's.
- Datagedreven toezicht vormt steeds meer het uitgangspunt voor DNB.
  - **Toezicht in beeld - november 2022**
  - De datagedreven aanpak in verschillende onderzoeken heeft bijgedragen aan scherpere onderzoeksbevindingen en gerichtere handhavingsmaatregelen. OSINT (Open Source Intelligence) onderzoeken maken een vast onderdeel uit van het instrumentarium dat wordt overwogen bij integriteitsonderzoeken. Met e-Discovery is verdere ervaring opgedaan.

Naar Real-Time Toezicht? Rapportageketen proces



Naar Real-Time Toezicht?

	Optimalisatie huidige rapportageketen	Verkenning innovatie rapportageketen
Experimenten	**Dataloop**: Hoe kunnen we het rapportage(analyse)proces efficiënter maken voor verzekeraars? **Slimme Integriteitsuitvraag (follow-up)**: Hoe kunnen we kwalitatieve uitvragen gebruikersvriendelijker maken voor instellingen?	**Real-Time Toezicht:** Wat zijn de technische en functionele wensen m.b.t. real-time toezicht?
Dialoog	**Real-Time Toezicht**: Waar zitten de grootste knelpunten in de huidige keten en hoe kunnen we die het beste adresseren? **Indirecte kosten:** Hoe kunnen we indirecte kosten minimaliseren?	**Real-Time Toezicht:** Hoe kan real-time toezicht voordelen opleveren voor de sector?

Marktindrukken AFM 2022 - Aandacht voor digitale weerbaarheid

- De Europese wetgever gaat verplichtingen opleggen aan grote(re) financiële ondernemingen die de digitale weerbaarheid moeten verhogen. Deze verplichtingen worden opgelegd in de Digital Operational Resilience Act (DORA), een verordening waarvan de definitieve tekst op korte termijn wordt verwacht. Als de wettekst definitief is, worden de verplichtingen op een aantal punten verder uitgewerkt in Regulatory Technical Standards.

- Hoewel DORA alleen van toepassing is op de grotere financiële dienstverleners met meer dan 250 fte's, is de AFM van mening dat DORA ook als raamwerk kan dienen voor de (proportionele) inrichting van de ICT-beheersing van kleinere en daarmee alle ondernemingen.

- DORA beoogt om de digitale weerbaarheid van financiële ondernemingen te vergroten om risico's te verminderen voor de financiële sector als geheel, voor individuele financiële ondernemingen en voor consumenten en beleggers. Om de digitale weerbaarheid te vergroten, bevat DORA verplichtingen over onderwerpen zoals het ICT Risk Management Framework, ICT-incidenten, het testen van de digitale weerbaarheid en de beheersing van uitbestede ICT-diensten en functies. Verder heeft DORA als doelstelling om bestaande wet- en regelgeving te harmoniseren.

Agentschap Telecom & AI

- Nieuwe naam vanaf 1 januari 2023: Rijksinspectie Digitale Infrastructuur.

- AI heeft een belangrijke plek op de strategische agenda van Agentschap Telecom:
  - Zij bekijken welke aspecten van kunstmatige intelligentie in de telecomsector belangrijk worden, en welke rol Agentschap Telecom hierin kan spelen.
  - Het onderzoek naar toezicht op gebruik artificiële intelligentie (AI) is inmiddels gepubliceerd.
    - Het doel van dit onderzoek was een overzicht te krijgen van het huidige gebruik van AI in de telecomsector, de verwachte ontwikkeling van het gebruik van AI in deze sector en de risico's ten aanzien van cyberveiligheid.
  - Daarnaast is een eerste schets gemaakt van hoe Agentschap Telecom als toezichthouder en uitvoeringsorganisatie kan bijdragen aan het beperken van die risico's.
  - Concrete invulling van het toezicht op artificiële intelligentie staat wereldwijd nog in de kinderschoenen, ook in ons land. Samenwerking tussen toezichthouders is essentieel om Nederland het vertrouwen te blijven geven in het veilig gebruik van AI. Agentschap Telecom neemt als autoriteit en toezichthouder in het digitale domein graag het voortouw in deze samenwerking. Zo werd samen met de Inspectieraad het initiatief genomen tot het oprichten van een brede werkgroep van toezichthouders op kunstmatige intelligentie, met als doel door onderlinge samenwerking en kennisuitwisseling de kwaliteit van het gezamenlijke toezicht door de toezichthouders op het terrein van AI in Nederland te vergroten. Lees meer over deze werkgroep in het artikel 'Algoritmen en Artificiële Intelligentie: hoe houd je daar toezicht op?' op Rijksoverheid.nl.

- Het Europese beleid over Artificial Intelligence is vastgelegd in verschillende actieplannen, richtsnoeren en voorgestelde wet- en regelgeving. Zo is de Europese benadering met betrekking tot AI beschreven in een Witboek. Hierin heeft de Commissie uiteengezet welke maatregelen het wil nemen voor het bevorderen van samenwerking en onderzoek naar AI tussen lidstaten. Verder zijn er ethische richtsnoeren voor Kunstmatige Intelligentie geformuleerd en heeft de Commissie in april 2021 een voorstel gedaan voor een nieuwe verordening voor AI.
  - De Artificial Intelligence Act (AI Act) is een voorstel voor een verordening van de Europese Commissie die tot doel heeft een gemeenschappelijk regelgevend en wettelijk kader voor kunstmatige intelligentie in te voeren .

Algoritmes – Autoriteit Persoonsgegevens

- Het Algoritmeregister van de Nederlandse overheid
  - Op deze website publiceren overheidsorganisaties de algoritmes die zij gebruiken in hun werk.
  - De overheid streeft om impactvolle algoritmes openbaar te maken. Zodat helder is hoe deze algoritmes werken en hoe deze ingezet worden.
  - Op dit moment kun je hier 109 algoritmes vinden.

- De AP is vanaf 1-1-2023 algoritmetoezichthouder.
  - Het gaat niet alleen om publieke maar ook om private algoritmen.

- Inrichtingsnota algoritmetoezichthouder, Brief Van Huffelen, 22 december 2022
- Beslisnota t.b.v. inrichting algoritmetoezichthouder, 14 december 2022
- Inrichting algoritmetoezicht, Scenario's korte en lange termijn, rapport Privacy Company, 5 december 2022

REGIE OP GEGEVENS
Zelf gegevens delen, veilig en betrouwbaar!

Bijlage Regie Op Gegevens

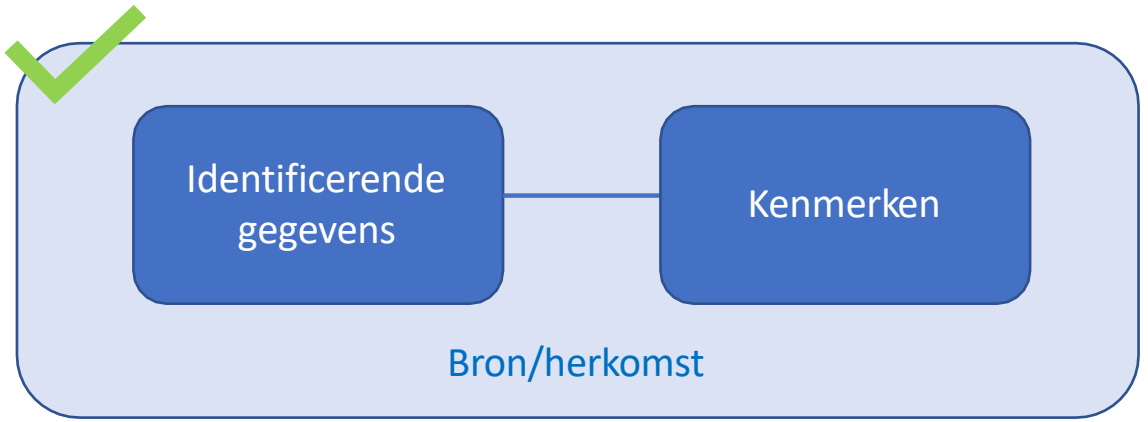
Regie op Persoonsgegevens (EU Datastrategie)

GDPR
(2016/679)

*bescherming van natuurlijke personen ivm de **verwerking persoonsgegevens** en het vrije verkeer van die gegevens*

Privacybescherming:
- *Dataminimalisatie*
- *Privacy-enhancing technologies*

Regiehandelingen:
1. *Inzien*
2. *Corrigeren*
3. *Delen (dataportabiliteit)*



eIDAS 1
(910/2014)

1. *Identificatie*
2. *Vertrouwensservices*

eIDAS 2
(amendement 2021)

1. *Kenmerken*
2. *e-Wallet:*
- *Alle regiehandelingen*
- *Erkenning wallet-providers*
- *Europees Keurmerk*

ePrivacy-verordening
Data verordening (DA)
Data Governance verordening (DGA)
Wet inzake digitale diensten (DSA)
Single Digital Gateway (SDG)
Sectoraal: European Health Data Space (EHDS)

NL: Wet Digitale Overheid

Regie op gegevens NL

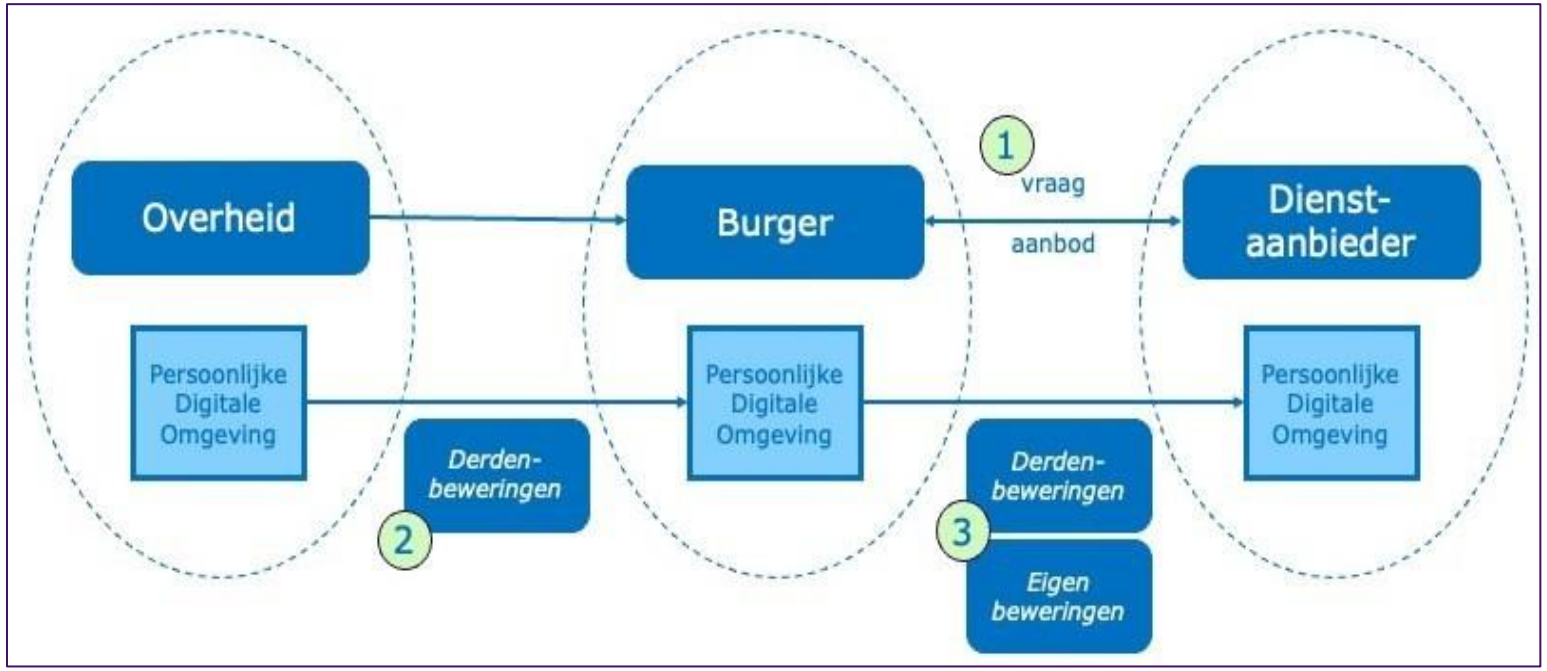
- Het programma Regie op Gegevens werkt aan een generiek sector-overstijgend kader dat veilige, betrouwbare en gebruiksvriendelijke digitale uitwisseling van gegevens tussen overheden, private en maatschappelijke organisaties mogelijk maakt.
  - Als onderdeel van de WDO werkt de overheid aan een juridisch kader voor het delen van gegevens.
  - De nationale ontwikkelingen op het terrein van regie op gegevens houden verband met Europese kaders. Met de Verordening Single Digital Gateway richt de EU zich op het vindbaar en toegankelijk maken van dienstverlening in lidstaten. Digitale uitwisseling van gegevens (digitaal bewijs) met andere lidstaten onder regie van de burger maakt hiervan deel uit. Om het mogelijk te maken om gegevens uit te wisselen met andere lidstaten is mogelijk een gezamenlijke aanpak gewenst.
  - Het voorstel voor wijziging van de eIDAS-verordening regelt het gebruik van een Europese Digitale Identiteit (EDI) binnen de interne markt en verplicht de lidstaten een ‘wallet’ uit te geven waarin onder de regie van de gebruiker gegevens (attributen) kunnen worden ontsloten voor overheden en ondernemers. Dit vraagt om het vindbaar en bruikbaar maken van deze gegevens, die uit de basisregistraties en andere overheidsregistraties zullen komen.

- Belang
  - Pensioenplanning is in toenemende mate onderdeel van financiële planning.
  - Regie op financiële gegevens maakt het in toenemende mate mogelijk dat personen/huishoudens sneller en beter overzicht hebben over hun financiële positie en de data kunnen delen met dienstverleners (hypotheekadviseurs, pensioenadviseurs, financiële planners, schuldhulp verleners etc.). Naast versnelling van processen – een kickstart van het advies - kunnen hierdoor ook de kosten en kwaliteit van financieel advies gunstig beïnvloed worden.
  - Randvoorwaarden zijn naast voordelen voor de consument (gemak!), vertrouwen van de consument en een eenvoudige systematiek voor toestemming. Een dienst die integraal inzicht biedt in gegevens over betaalrekeningen (kosten van levensonderhoud), spaarrekeningen, schulden, hypotheken, verzekeringen, pensioenen, abonnementen, etc. ontbreekt momenteel nog.

REGIE OP GEGEVENS
Zelf geregeld, veilig en betrouwbaar!

Zelf delen van gegevens*

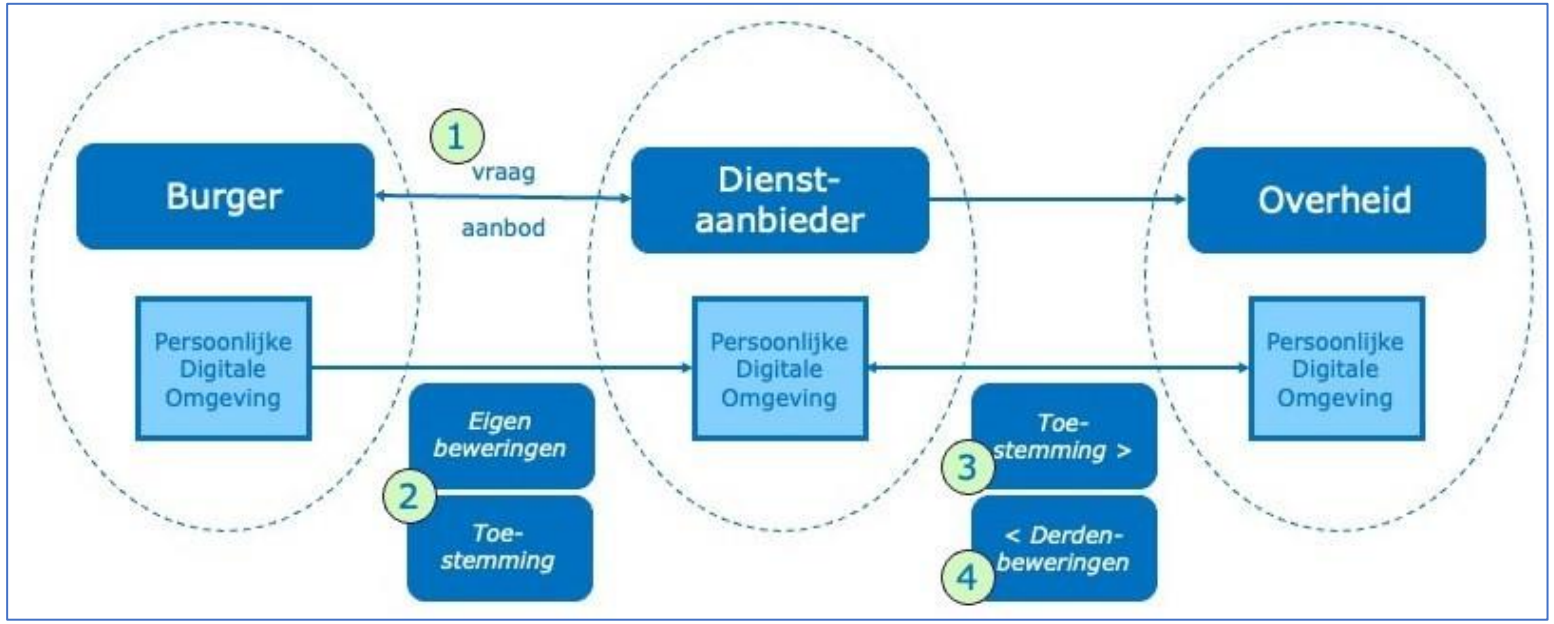
1. Burger wil een dienst afnemen, hiervoor zijn bepaalde gegevens nodig.
2. Burger haalt gevraagde gegevens op.
3. Burger levert de gegevens zodat de dienstaanbieder de dienst kan leveren.



***) Regie op Gegevens: 'Burger wint in."**

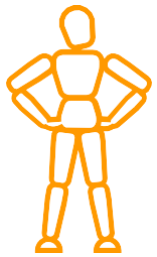
Machtigen van dienstaanbieder*

1. Burger wil een dienst afnemen, hiervoor zijn bepaalde gegevens nodig.
2. Dienstaanbieder biedt aan de gegevens op te halen.
3. Dienstaanbieder vraagt gegevens op.
4. Overheid levert de gegevens zodat de dienstaanbieder de dienst kan leveren.



***) Regie op Gegevens: 'Dienstaanbieder wint in."**

Functies worden geleverd door services



Identificatie & authenticatie

Gegevens produceren

Waarborgen (vertrouwen)

Gegevens leveren

proces

applicatieservices

IAM services

- Identificeren
- Authentiseren
- Autoriseren
- Machtigen
- Toestemmen

Data services

- Afleiden
- Vertalen
- Archiveren
- Verzamelen
- Filteren
- Samenstellen
- Opslaan
- Corrigeren
- Verwijderen

Trust services

- Waarmerken
- Dateren
- Elektronisch ondertekenen
- Versleutelen
- Verzegelen
- Aangetekende bezorging

Gateway services

- Inwinnen
- Verstrekken
- Adressering
- Verwijzen

Leerpunten

Bron: Barrières van digitaal persoonsgegevens delen door middel van regietoepassingen, rapportage van kwalitatief onderzoek, 18 augustus 2022

- Iedereen heeft zijn administratie online geregeld, want per post komt immers ook weinig meer binnen. Dat dit online staat 'opgeslagen' werkt meestal naar tevredenheid; gegevens zijn eenvoudig terug te vinden. Toch overschatten mensen op andere gebieden hun eigen digitale vaardigheden. In de realiteit zijn ze onzeker over hun eigen digitale kunnen en houden ze zich daarom liever vast aan wat ze kennen en voor hen goed werkt.
- Over het algemeen is iedereen goed op de hoogte van de gevaren van (online) gegevens delen. Dit komt zowel door negatieve ervaringen (zelf of uit de omgeving) als de 'opvoeding' door banken, nieuwsberichten en televisieprogramma's.
- Vooral ouderen zijn voorzichtiger in het delen van hun 'feitelijke' data, zoals NAW-gegevens, bankrekeningnummer etc. Terwijl jongeren zich meer zorgen maken om hun online identiteit (content op social media en digitale sporen die je achterlaat).
- Mensen treffen verschillende maatregelen om hun gegevens te beschermen, denk aan cookies niet of deels accepteren, niet klikken op linkjes in de e-mail en wachtwoorden regelmatig veranderen. Daarbij zijn er een aantal indicatoren die duiden op een ‘veilige’ omgeving, zoals slotje in de webbrowser, bekende afzender en DigiD.
- Motivatie om (online) gegevens te delen is voornamelijk: ‘ik heb niks te verbergen’, ‘je moet mee met de tijd’ en gemak.
- De overheid wordt gezien als een betrouwbare bron om (online) gegevens mee te delen. Er is een groot vertrouwen, omdat de overheid geen commerciële belangen heeft en er wordt verwacht dat strenge AVG wet- en regelgeving geldt. En net zoals in voorgaande onderzoeken naar regie op gegevens, speelt DigiD ook een belangrijke rol in het vertrouwen.
- DigiD wordt gezien als heel veilig en betrouwbaar door de twee-stapverificatie, is landelijk al jaren in gebruik (met Corona ook veelvuldig gebruikt) en er zijn goede ervaringen met de toepassing. Kortom, DigiD is een ‘heilige graal’ voor veilig inloggen en persoonsgegevens delen.
- Iedereen deelt wel (online) persoonsgegevens onder bepaalde voorwaarden.
- Mensen staan dan ook open voor het gebruik van regietoepassingen, maar er is wel een aantal drempels. De grootste drempel is het gebruik van een app.

SWOT

Bron: Barrières van digitaal persoonsgegevens delen door middel van regietoepassingen, rapportage van kwalitatief onderzoek, 18 augustus 2022

Sterkten

- Tijdbesparing ten opzichte van handmatig invullen
- Gemak ten opzichte van handmatig invullen
- Dataminimalisatie; geen onnodige informatie delen
- Toestemming geven voor tijdelijke/ eenmalige toegang
- Gebruik van DigiD
- Noodzaak van het regelen
- QR-code (gemak)

Zwakten

- Onbekende toepassing
- Er is nog veel uitleg nodig om het begrip van regietoepassingen te laten landen
- Een app als enige mogelijkheid om gebruik te maken van de toepassing
- Datacentralisatie; verhoogd risico alle belangrijke informatie bij elkaar
- Bewaartermijn van 90 dagen wordt ervaren als (te) lang
- QR-code (minder veilig/ onbekend)

Kansen

- Meer bekendheid van en uitleg over regietoepassingen; opvoeden burgers
- Positieve ervaringen van mensen uit de omgeving
- Overheidsbron als (mede-)afzender
- Alternatieven naast de app, zoals een webversie (in browser)
- Mogelijkheden tot (telefonisch) contact
- Routing richting regietoepassing: vanuit een bekende afzender/ omgeving (denk aan: website) doorgesluisd worden; keuze voor het blijven in 'vertrouwde omgeving', zoals de webbrowser.

Bedreigingen

- Digitale- en leesvaardigheid van burgers: weinig zelfvertrouwen; angst om het fout te doen.
- Digitale apparaten niet compatible/ up-to-date: weinig geheugen voor apps
- Technologie is ongrijpbaar en daardoor minder gevoel van controle
- Negatieve publiciteit rondom het delen van (online) persoonsgegevens (hacken, phishing, programma's zoals Kassa etc.)
- Routing: onbekend afzender in combinatie met doorkliklinkjes in e-mail

Vier verschillende houdingen t.a.v. digitaal gegevens delen

Bron: Regie op Gegevens – doelgroep analyse, MarketResponse 2022, Programma Mens Centraal

Afwijzers

- Controle over en bescherming van gegevens zijn cruciaal. Functionele uitwisseling is (daarmee) minder relevant.
- Barrières, bijvoorbeeld:
  - *Geen vertrouwen in de overheid op dit moment.*
  - *nog meer gegevens weg als het gehackt wordt en niet heeft iedereen een telefoon waar het op kan*
  - *Ik wil persoonlijk contact met de bank*

Wantrouwend

- Privacy is een meer manifest thema dan voor anderen.
- Controle over, bescherming van en vertrouwelijk omgaan met gegevens zijn belangrijk.
- Barrières, bijvoorbeeld:
  - *Omdat ik dan precies weet welke gegevens ik deel en met wie ik deze persoonlijk deel. Lekken zien we steeds meer vooral bij zulke apps*
  - *Ik blijf de veiligheid wantrouwen*
  - *het gevoel dat het buiten je om gaat*

Gematigden

- Meest gemiddelde groep als het gaat om belang van gemak en veiligheid
- Barrières, bijvoorbeeld:
  - *Hoe veilig is de digitale kluis, dat zou ik graag van security specialisten willen horen.*
  - *Ik heb liever zelf de touwtjes in handen, dan maar iets meer werk erin stoppen om uit te zoeken maar dan weet ik wel precies wat ik aanlever en op welke manier*
  - *Omdat niemand kan garanderen dat de bank de toegestuurde gegevens later vernietigd. Ook is het niet zeker dat de kluis de gegevens daadwerkelijk beschermt*

Enthousiasten

- Privacy en online criminaliteit zijn minder relevant dan gemiddeld (corona en klimaat juist wat relevanter).
- Sterk gericht op gemak – maar ook op veilige uitwisseling (functionaliteit). Veel minder op hoe controle op en gebruik van gegevens. Willen er niet te veel mee bezig zijn
- Barrières, bijvoorbeeld:
  - *Het laatste is een oude vertrouwde manieren om het te doen en daar ben ik gewoon meer naar toe geneigd.*
  - *Bij gegevens versturen weet ik echt niet wie achter het bureau zit en wie er meer bij kan kijken*
  - *de overheid misbruikt dikwijls de geheimhouding*

Projecten Programma Regie op Gegevens (ROG)

- Lopende Projecten ROG (najaar 2022):
  - De Referentie-architectuur Regie op Gegevens;
  - Voortgang pilot delen van gegevens voor de inkomenstoets woningcorporaties (met MijnOverheid);
  - Voortgang delen BRP-gegevens met maatschappelijk relevante organisaties;
  - MijnGegevens app (MijnOverheid);
  - Proeftuin ROG;
  - ROG community en kennisdeling (plannen kennis sessies, Pleio, etc);
  - Monitoren Europese Ontwikkelingen;
  - Landelijke uitrol algemene inzage.

- Afgeronde projecten in 2022:
  - De PoC inzage in geoorloofde verstrekkingen uit Basisregistraties;
  - Onderzoek eigenaarschap persoonsgegevens;
  - Verkenning vertrouwen en verantwoordelijkheden in Dataminimalisatie;
  - Gebruikersonderzoek toepassingen en pilots.

Bijlage
Levensgebeurtenissen

Levensgebeurtenissen

- https://www.rijksoverheid.nl/onderwerpen/levensgebeurtenissen/overzicht-levensgebeurtenissen

- Met pensioen: wat moet ik regelen?
  - Vul de vragen in en bekijk wat je moet regelen als je met pensioen gaat.
  - Na invullen vragen volgt afhankelijk van de antwoorden een actielijst.
  - De actielijst komt in PDF beschikbaar.

- Impact
  - Pensioenuitvoerder kan in eigen portaal naar website verwijzen.

Met pensioen: wat moet ik regelen?

Regelen voordat u uw AOW-leeftijd bereikt

Hoogte pensioen bekijken

Doen nadat u uw eerste AOW-uitkering ontvangt

AIO-aanvulling aanvragen

Regelen voordat u (voor een deel) stopt met werken

Aanvullend pensioen aanvragen

Voor een deel blijven werken

Arbeidscontract beëindigen

Doen nadat u gestopt bent met werken

Toeslagen aanpassen of aanvragen

Toeslag wijzigen

Loonheffingskorting regelen

Loonheffingskortingen vergelijken

Middelingsregeling toepassen

Belasting terugkrijgen

Wijziging inkomen doorgeven voor uw Ziektewetuitkering

Voorlopige aanslag aanvragen of wijzigen

Voorlopige aanslag wijzigen

Regelen bij eerstvolgende belastingaangifte

Oudedagsreserve afrekenen

Bijlage
Afkortingen - Verwijzingen

Afkortingen (1)

Afkorting	Betekenis
AFM	Autoriteit Financiële Markten
AI	Artificial Intelligence
AP	Autoriteit Persoonsgegevens
ARF	Architectural Reference Framework
AT	Agentschap Telecom
AVG	Algemene Verordening Gegevensbescherming
BRP	Basisregistratie Personen
BZK	Het ministerie van Binnenlandse Zaken
DGA	Data Governance Act
DGDOO	Directoraat-generaal Digitalisering en Overheidsorganisatie
DNB	De Nederlandse Bank
DSC	Data Sharing Coalition
DSO	Digitale Standaardisatie & Ontwikkeling
EC	Europese Commissie
EDI	Europese Digitale Identiteit
eID	Elektronische identiteit
eIDAS	Electronic Identities And Trust Services
EIOPA	European Insurance and Occupational Pensions Authority (EIOPA)
ESSIF	European Self-sovereign Identity Framework
ETD	Elektronische toegangsdiensten
EU	Europese Unie
FBS	Federatief Berichten Stelsel
GDI	Generieke Digitale Infrastructuur
GZD	Gezamenlijk Domein
IAK	Integraal Afwegingskader

Afkortingen (2)

Afkorting	Betekenis
ICTU	ICT Uitvoeringsorganisatie
IDP	Innovatie Digitale Pensioenuitvoering
LAK	Loonaangifteketen
LSP	Large Scale Pilot
MIDO	Meerjarenprogramma Infrastructuur Digitale Overheid
MKBA	Maatschappelijke Kosten Baten Analyse
MPO	MijnPensioenOverzicht
NORA	Nederlandse Overheid Referentie Architectuur.
NVB	Nederlandse Vereniging van Banken
OBDO	Overheidsbreed Beleidsoverleg Digitale Overheid
OOP	Only Once Principe
PGDI	Programmeringsraad GDI
PID	Personal Identification Data
PT	Programmeringstafel
RDI	Rijksinspectie Digitale Infrastrctuur
RINIS	Stichting Routerings Instituut (Inter)Nationale Informatiestromen
ROG	Regie Op Gegevens
RVO	Rijksdienst voor ondernemend Nederland
QES	Qualified Electronic Signature
SBR	Standard Business Reporting
SCA	Strong Customer Authentitication
SDG	Single Digital Gateway
SSI	Self Sovereign Identity

Afkortingen (3)

Afkorting	Betekenis
SVB	Sociale Verzekeringsbank
SWO	Softwareontwikkelaar
UWV	Uitvoeringsinstituut Werknemers Verzekeringen
VIA	Vooraf ingevulde Aangifte Inkomensheffing
vID	Virtueel identiteitsbewijs
WDO	Wet Digitale Overheid
WID	Wet op de Identificatieplicht
WRR	Wetenschappelijke Raad Regeringsbeleid

Verwijzingen

- Overzicht
  - Onderwerpen Digitale Overheid
- Europa
  - Europees beleid - Digitale Overheid
  - The Digital Europe Programme | Shaping Europe’s digital future
  - DiZa en Europa | Tweede Kamer der Staten-Generaal
- Politiek
  - Kennisagenda | Tweede Kamer der Staten-Generaal
- Voortgang
  - Documenten voor Monitoring - Digitale Overheid

Verwijzingen

- Wetgeving
  - Wetgeving
  - Nieuws
- AI
  - Nationale AI-cursus
  - WRR 2021: Opgave AI. De nieuwe systeemtechnologie
- Data
  - Federatief Datastelsel: ‘Het organiseren van vertrouwen’ - Digitale Overheid
- Ethiek
  - Toolbox Ethisch Verantwoorde Innovatie
- Standaarden
  - Standard Business Reporting (SBR)
  - Nederlandse Overheids Referentie Architectuur (NORA)
  - Lijst open standaarden

Verwijzingen

- Stelselplaat Infrastructuur
- Stelselplaat Basisregistraties

Bijlage Rapporten

Rapporten (1)

- **Onderzoek 'Algoritmes en grondrechten (Universiteit Utrecht), 17 september 2018**
  - De opkomst van algoritme-gedreven technologieën als Big Data, Internet of Things en Kunstmatige Intelligentie levert een breed scala aan nieuwe grondrechtelijke uitdagingen op. Dit juridische onderzoek brengt specifiek voor Nederland, in kaart wat de (potentiële) impact is van Big Data, het Internet of Things en Kunstmatige Intelligentie op vrijheidsrechten, gelijkheidsrechten, privacyrechten en procedurele rechten.

- **Quick scan AI in de publieke dienstverlening, 19 april 2019 | 35 pagina's**
  - Verkenning en categorisering van toepassingen van het gebruik van Artificial Intelligence (AI) in de publieke sector.

- **Strategisch Actieplan voor Artificiële Intelligentie, Beleidsnota | 08 oktober 2019**
  - Dit actieplan beschrijft de voornemens van het kabinet om de ontwikkeling van artificiële intelligentie (AI) in Nederland te versnellen en internationaal te profileren. Het gaat in op de AI-ontwikkelingen in Nederland, op de elementen die nodig zijn om AI-innovatie verder te stimuleren, en op het borgen van de publieke belangen bij AI-ontwikkelingen.

- **Beleidsbrief AI, publieke waarden en mensenrechten, 17 november 2019**
  - De beleidsbrief geeft een overzicht van de kansen en risico's van AI voor publieke waarden die voortkomen uit mensenrechten. Het beschrijft daarnaast bestaande en toekomstige beleidsmaatregelen om risico's voor deze fundamentele publieke waarden te adresseren.

- **Ethische richtlijnen voor betrouwbare AI , 8 april 2019**
  - Publicatie vanuit Europa, de High-Level Expert Group on AI Ethics Guidelines for Trustworthy Artificial Intelligence. Dit volgde op de publicatie van het eerste ontwerp van de richtlijnen in december 2018, waarop meer dan 500 opmerkingen werden ontvangen via een open raadpleging.

- **Toekomstverkenning Digitalisering 2030, Kamerstuk | 26 april 2021**
  - Een toekomstverkenning naar de belangrijkste trends en ontwikkelingen in de digitalisering richting 2030.

Rapporten (2)

- **Monitor Digitale Overheid 2021, 15 juni 2021**
  - De monitor geeft inzicht in de voortgang en implementatie van de voorzieningen en bouwstenen die gezamenlijk de digitale basis van de overheidsdienstverlening vormen op peildatum 31 december 2020.

- **Digitale Identiteit Verslag van rapporteur, 1 oktober 2021**
  - Tijdens de procedurevergadering van de vaste commissie voor Digitale Zaken (DiZa) van 9 maart 2022 is besloten mij een rapporteur aan te stellen als rapporteur voor het EU-voorstel voor een Verordening voor een raamwerk voor een Europese digitale identiteit (COM(2021) 281) en hoe het Nederlandse beleid daarop aansluit .

- **SSI Speelveldanalyse, oktober 2021**
  - Een verkenning van het Nederlandse SSI speelveld, toekomstige ontwikkelrichtingen, impact op publieke waarden en de rol van de Nederlandse overheid.

- **Eindpresentatie Project Vervolg Digitale Bronidentiteit, november/december 2021**
  - Exploratief gebruikersonderzoek met als centrale vraag: hoe komen we tot een vorm voor een digitale bronidentiteit die aansluit bij de belevingswereld van de burger?

- **Verkenning eWallets: Speelveldanalyse, 11 januari 2022**
  - Onderzoek naar het huidige speelveld van digitale identiteit wallets in Nederland en Europa.

- **GDI Meerjarenvisie 2022-2026, 14 januari 2022**
  - Visie over de Generieke Digitale Infrastructuur (GDI) voor de jaren 2022-2026.
  - ‘’We werken aan een publiek inlogmiddel voor bedrijven’’ (p.9)’.

Rapporten (3)

- **European Digital Identity Architecture and Reference Framework, 22 Februari 2022**
  - Dit overzicht geeft een beknopte beschrijving van het begrip van de eIDAS-expertgroep van het EUDI Wallet-concept. De eIDAS-expertgroep keurde het huidige document op 22 februari 2022 goed en besloot het te publiceren voor feedback van belanghebbenden.

- **Kamerbrief hoofdlijnen beleid voor digitalisering , 8 maart 2022**
  - Staatssecretaris Van Huffelen (Koninkrijksrelaties en Digitalisering), minister Adriaansens (EZK) , minister Yeşilgöz-Zegerius (JenV) en minister Weerwind (Rechtsbescherming) stuurden de Tweede Kamer op 8 maart 2022 een brief over de hoofdlijnen van het beleid van de digitale transitie van de samenleving voor deze kabinetsperiode.

- **Handreiking non-discriminatie by design, 1 april 2022**
  - Welke vragen en principes zijn leidend bij het ontwikkelen en implementeren van een AI-systeem met het oog op het discriminatieverbod? Deze handreiking behandelt dit vanuit zowel het juridische, technische, als organisatorische perspectief.

- **Rapportage over digitale identiteit, 22 mei 2022**
  - Rapportage vanuit de vaste commissie voor Digitale Zaken. Bevat diverse vraagsuggesties over de nieuwe Europese verordening.

- **Waarden, kansen en uitdagingen rond het Europese Digitale Identiteit raamwerk, Brief | 26 juli 2022**
  - Kijk van de staatssecretaris op de context, waarden, kansen en uitdagingen van wallets in het algemeen en het Europese Digitale Identiteit raamwerk in het bijzonder.

- **Voortgangsrapportage Europese Digitale Identiteit, 17 augustus 2022**
  - In deze brief informeert de staatssecretaris over de voortgang en te nemen stappen in het ‘Europese Digitale Identiteit raamwerk’ (EDI), het wetsvoorstel dat de Europese Commissie heeft ingediend op 3 juni 2021

Rapporten (4)

- **Monitor Digitale Overheid ,20 september 2022**
  - In deze monitor Digitale Overheid 2022 worden per voorziening de aansluitingen en het gebruik van de voorzieningen weergegeven. Voor deze monitor is de peildatum 31 december 2021 gehanteerd.

- **Beslisnota bij Kamerbrief over voortgangsrapportage domein Toegang, Beleidsnota | 21 september 2022**
  - Beslisnota bij Kamerbrief over voortgangsrapportage domein Toegang. In een beslisnota staat achtergrondinformatie die bewindspersonen gebruiken bij de besluitvorming over een Kamerstuk.

- **Voortgangsrapportage domein Toegang, Kamerstuk | 26 september 2022**
  - Staatssecretaris Van Huffelen (Koninkrijksrelaties en Digitalisering) informeert de Tweede Kamer over de voortgang van de aanpak in het domein Toegang.

- **Stand van zaken Basisregistratie Personen, kamerstuk | 27 september 022**
  - Staatssecretaris Van Huffelen (Digitalisering en Koninkrijksrelaties) informeert de Tweede Kamer over de Basisregistratie Personen (BRP) in het algemeen en over de stand van zaken rond de vernieuwing ervan.

- **Toelichting Ontwikkelagenda BRP 2022, Rapport | 27 september 022**
  - Toelichting over de voortgang van de doorontwikkeling van de Basisregistratie Personen (BRP).

Rapporten (5)

- **Nederlandse Cybersecuritystrategie 2022 – 2028, 10 oktober 2022**
  - Ambities en acties voor een digitaal veilige samenleving.

- **Actieplan Nederlandse Cybersecuritystrategie 2022 – 2023, 10 oktober 2022**
  - Ambities en acties voor een digitaal veilige samenleving.

- **Regie op gegevens - Welke burgers zien het digitaal delen niet zitten, en waarom niet, 13 oktober 2022**
  - Doel is om te achterhalen waarin nu de minder tot delen geneigde doelgroepen zich onderscheiden van de positiever, en welke indicaties er meer specifiek zijn van hun ervaren barrières tot het voeren van regie op gegevens in het digitaal delen met derden.

- **Verslag van een schriftelijk overleg over de voortgangsrapportage Europese Digitale Identiteit, 28 november 2022**
  - Beantwoording Kamervragen Voortgangsrapportage Europese Digitale Identiteit.

- **GDI Programmeringsplan, 2 december 2022**
  - Programmeringsplan dat richting geeft aan de ontwikkeling van de Generieke Digitale Infrastructuur (GDI) voor 2023. De GDI is de verzameling van voorzieningen, standaarden en afspraken(stelsels) die door alle publieke dienstverleners worden gebruikt voor hun digitale dienstverlening aan burgers en ondernemers.
  - Het plan is in december 2022 door staatssecretaris Van Huffelen naar de Tweede Kamer gestuurd.

Rapporten

- **Algoritmetoezicht**
  - Inrichting algoritmetoezicht, Scenario's korte en lange termijn, rapport Privacy Company, 5 december 2022
  - Beslisnota t.b.v. inrichting algoritmetoezichthouder, 14 december 2022
  - Inrichtingsnota algoritmetoezichthouder, Brief Van Huffelen, 22 december 2022