(76)

eHerkenning idensys

Retouradres Postbus 96810 2509 JE Den Haag

Ministerie van BZK
Directie Informatiesamenleving en Overheid (DIO)
[redacted]

Idensys | eHerkenning
Wilhelmina v Pruisenweg 52
2509 JE Den Haag

Postbus 96810
2509 JE Den Haag
[redacted]

Datum 28 maart 2017
Betreft Reactie ETD op wet GDI en Uniforme Set van Eisen

[redacted]

Naar aanleiding van de lopende consultatie heeft de governance Elektronische Toegangsdiensten (ETD) een impactanalyse uitgevoerd op de wet GDI en Uniforme Set van Eisen. Hierin is gekeken naar de gevolgen van het wettelijk kader voor de verschillende betrokkenen bij Idensys en eHerkenning, te weten: dienstverleners, leveranciers en eindgebruikers. Bijgaand treft u de input namens de leden van de governance.

De leden waarderen de inspanningen van het ministerie van BZK zeer, maar zien wel punten van aandacht en de noodzaak voor enkele concrete wijzigingen. Zonder bijstelling van de Wet GDI wordt de uitvoerbaarheid van de multimiddelenstrategie en daarmee ook de haalbaarheid van achterliggende beleidsdoelen belemmerd.

De leden van de governance hopen met de aandachtspunten en concrete adviezen een constructieve bijdrage te leveren aan de verdere ontwikkeling van het wettelijk kader. Wij zijn uiteraard bereid om desgewenst een nadere toelichting te geven op de bevindingen.

We kijken er naar uit de komende jaren een bijdragen te leveren aan een veiligere en betrouwbaardere inloginfrastructuur in Nederland.

Met vriendelijke groet,

Namens de leden van het Strategisch Beraad ETD,

[redacted]

1 Inleiding

In december 2016 zijn de concept wet Generieke Digitale Infrastructuur en de Uniforme Set van Eisen in publieke consultatie gegaan. Met het wettelijk kader streeft de overheid na dat elektronische dienstverlening in het BSN-domein naar een hoger plan wordt getild op het gebied van veiligheid, betrouwbaarheid, transparantie en gebruiksgemak. Doelen die ook door de governance van het stelsel Elektronische Toegangsdiensten (ETD) worden uitgedragen en vanzelfsprekend van harte worden gesteund.

Het ETD heeft een impactanalyse uitgevoerd op de wet GDI en Uniforme Set van Eisen 1.0 waarin hoofdzakelijk is gekeken naar werkbaarheid en uitvoerbaarheid. De analyse is uitgevoerd vanuit de verschillende perspectieven die verenigd zijn in ETD: eindgebruikers, dienstverleners en leveranciers. Insteek van de inbreng is een aantal praktische handvatten te bieden om de uitvoerbaarheid en maatschappelijke waarde van het wettelijk kader te vergroten en daarmee bij te dragen aan een succesvol eID-beleid.

In hoofdstuk 2 wordt allereerst gekeken naar de (invulling van) randvoorwaarden voor een succesvol eID-beleid vanuit de verschillende perspectieven die binnen ETD vertegenwoordigd zijn. Vanuit dit vertrekpunt wordt vervolgens in hoofdstuk 3 uiteengezet welke randvoorwaarden nadere invulling nodig hebben in de wet en het beleid. In hoofdstuk 4 wordt tot slot een aantal concrete adviezen gegeven ter verbetering van het wettelijk- en beleidskader.

Governance ETD: eHerkenning | Idensys
De governance ETD is een publiek-private samenwerking dat in opdracht van EZ reeds zes jaar werkt aan een betrouwbare, veilige en gebruiksvriendelijke inloginfrastructuur voor burgers en bedrijven, beter bekend als eHerkenning en Idensys. Het ETD wordt bestuurd door een samenwerking van leveranciers, publieke en private dienstverleners en eindgebruikers.

2 Een succesvol eID-beleid: drie perspectieven

In de governance ETD is een aantal belangrijke stakeholders van eID verenigd, te weten eindgebruikers, dienstverleners en leveranciers. Voor elk van hen gelden andere criteria voor een succesvol eID-beleid. De verschillende perspectieven worden hieronder toegelicht. Tevens wordt geschetst in hoeverre het huidige wettelijk kader en beleid hieraan invulling geven.

Eindgebruikers

Inloggen bij (overheid)dienstverleners is voor burgers en bedrijven een typische 'hygiënefactor'. Dat wil zeggen: het moet gewoon geregeld zijn en als gebruiker wil je hier zo min mogelijk moeite voor doen. Aangeboden middelen moeten betaalbaar zijn en makkelijk in gebruik. Ook is het van groot belang dat eindgebruikers vertrouwen hebben in de inlogmiddelen waaruit zij kunnen kiezen. De nagestreefde multimiddelenaanpak is wat dat betreft een stap in de goede richting; het geeft de eindgebruiker een keuze (mits er voldoende aanbod komt). De governance ETD is om dezelfde reden positief over de getoonde ambities op het gebied van betrouwbaarheid en privacybescherming. De introductie van

Polymorfe Pseudoniemen heeft breed draagvlak binnen het Strategisch Beraad omdat dit zorgt dat de privacy van de eindgebruiker optimaal gewaarborgd wordt. Nederland kan op dit gebied een voortrekkersrol gaan vervullen. Drempels voor de eindgebruiker lijken op dit moment vooral te zitten in de complexiteit van (uiteenlopende) aanvraagprocessen en de aanschafkosten van middelen. Onduidelijk is hoe voorlichting van eindgebruikers gaat plaatsvinden en of er budgettaire ruimte is om de uitrol van middelen te faciliteren. Het risico bestaat dat er bij ingang van de wet onvoldoende eindgebruikers zijn met een middel op het juiste betrouwbaarheidsniveau.

Dienstverleners

Er is bij dienstverleners, zowel publiek als privaat, een grote behoefte om het digitale dienstenaanbod uit te breiden en identiteitsfraude en gegevensdiefstal tegen te gaan. In dat licht is de stap naar hogere betrouwbaarheidsniveaus een positieve ontwikkeling. De multimiddelaanpak realiseert daarnaast terugvalopties zodat de beschikbaarheid van dienstverlening beter gegarandeerd is. Het is voor dienstverleners met name belangrijk dat zij voldoende tijd krijgen om de overstap te maken en dat zij betrokken worden bij de doorontwikkeling van het wettelijk kader om te zorgen dat deze uitvoerbaar blijft. Het migratiepad dat momenteel wordt voorgesteld vormt een immense uitdaging. Met name voor dienstverleners met diensten op niveau substantieel en hoog; zij moeten op 1 januari 2019 zonder overgangsregeling de overstap naar hogere betrouwbaarheidsniveaus hebben gemaakt. Dit vereist (ingrijpende) technische aanpassingen en uitfasering van bestaande oplossingen. Dienstverleners signaleren dat het op dit moment nog onvoldoende duidelijk is wat van hen wordt verwacht en wat de implementatielast en -kosten zullen zijn van het moeten aansluiten op alle erkende middelen. Voorzien wordt dat voor dienstverleners hoge initiële kosten gepaard gaan met de overstap van een laag betrouwbaarheidsniveau naar niveau substantieel en hoog (terwijl niet voor alle diensten een hoger betrouwbaarheidsniveau benodigd is).

Ook voor private dienstverleners brengt het eID-beleid onzekerheden met zich mee. Hoewel zij sinds vorig jaar buiten scope van het beleid zijn geplaatst, raken de beleidskeuzes deze partijen wel degelijk. Voor veel middelenleveranciers is het publieke domein de primaire en het private domein de secundaire focus, waardoor de verwachting is dat de variatie aan authenticatieoplossing dat beschikbaar komt voor commerciële dienstverlening afhankelijk zal zijn van het aantal partijen dat brood ziet in het BSN-domein. Private dienstverleners hebben de wens hun klanten meer dan één type inlogmiddel te bieden; dit vereist dat de BSN-markt aantrekkelijk genoeg is voor meerdere private leveranciers om op in te stappen.

Leveranciers

De leveranciers van eHerkenning en Idensys hebben de afgelopen jaren gewerkt aan een hoog betrouwbare authenticatie-infrastructuur ter ondersteuning van de digitale ambities van de overheid. eHerkenning en Idensys zijn beiden tot op het hoogste betrouwbaarheidsniveau doorontwikkeld, het stelsel wordt dit jaar Europaproof gemaakt (conform de eIDAS-verordening) en er wordt gewerkt aan de implementatie van het Polymorfe Pseudoniem om de identiteit van eindgebruikers optimaal te beschermen. Leveranciers zijn enthousiast over de getoonde ambitie in het eID-beleid en de kans die geboden wordt om private middelen voor zowel publieke als private diensten in te zetten; private

middelen worden hierdoor aantrekkelijker voor zowel gebruikers als dienstverleners. Desalniettemin is de multimiddelenmarkt binnen het huidige kader niet aantrekkelijk om op in te stappen. Er zijn met name zorgen over het ontbreken van een gelijkwaardige uitgangspositie tussen DigiD en iDIN enerzijds en andere private leveranciers anderzijds. Zowel DigiD als iDIN hebben, onder andere door hun hoge penetratiegraad, een voorsprong die tot gevolg heeft dat het uitermate lastig is voor concurrerende initiatieven om een rendabel marktaandeel te verwerven. Op dit moment is onzeker of de overheid bereid is maatregelen te treffen om een gelijkwaardig speelveld te creëren. Er zit daarnaast nog een aantal onzekerheden in het wettelijk kader en het beleid welke het lastig maken in te schatten wat de consequenties zijn van deelname aan de multimiddelenaanpak. Het betreft onder andere onzekerheid over de financiële gevolgen van deelname aan de multimiddelenaanpak, alsmede onzekerheid over de wijze waarop leveranciers inspraak krijgen in de verdere ontwikkeling van de uitvoeringsregelgeving. Zonder goede governance-structuur wordt leveranciers gevraagd te investeren in een product waarvan de besluitvorming over doorontwikkeling buiten de eigen invloedssfeer is belegd.

3 Randvoorwaarden voor uitvoerbaarheid

Op basis van de analyse signaleert de governance dat de volgende **randvoorwaarden** ingevuld moeten worden om een gezonde, werkbare en duurzame multimiddelenaanpak te realiseren:

1. Om eindgebruikers voor te bereiden op inloggen met hogere betrouwbaarheidsniveaus en het nut en de noodzaak ervan voor het voetlicht te brengen is gecoördineerde **communicatie naar eindgebruikers** noodzakelijk.
2. Om eindgebruikers (tijdig) te laten overstappen op hogere betrouwbaarheidsniveaus zijn **stimulerende maatregelen** vereist zodat er bij ingang van de wet voldoende middelen op niveau substantieel en hoog in omloop zijn.
3. Dienstverleners dienen **ontzorgd** te worden in de migratie van de huidige naar de nieuwe situatie. Het uitgangspunt moet zijn om de kosten en inspanning van de migratie zo laag mogelijk te houden terwijl de continuïteit van de dienstverlening blijft gewaarborgd.
4. Om een gezonde mix van private en publieke middelenleveranciers te bewerkstelligen moet een **level playing field** gecreëerd worden. Het speelveld moet in dusdanige gelijkwaardig zijn dat er voldoende commercieel perspectief wordt geboden aan een diversiteit aan private (middelen)leveranciers.
5. Er moet een overlegstructuur (**governance**) komen waarin dienstverleners, erkende leveranciers en eindgebruikers inspraak krijgen in de doorontwikkeling van de uitvoeringsregelgeving om te zorgen dat deze uitvoerbaar blijft en aansluit bij de laatste wensen en ontwikkelingen.
6. De eisen uit de Uniforme Set van Eisen moeten **rule based** worden opgelegd aan alle erkende leveranciers en niet principle based, zodat de vaststelling van identiteiten gebeurt op basis van specifieke voorschriften.
7. Er moet zo spoedig mogelijkheid **nadere invulling worden gegeven** aan de nog ontbrekende onderdelen in de Uniforme Set van Eisen (misbruikbestrijding, machtigingen, attribuutverstrekking en ondertekenen) en de AMVB's en ministeriële regelingen die voortvloeien uit de wet GDI. Bij de publicatie van nieuwe onderdelen moet er wederom een

consultatie plaatsvinden om stakeholders de kans te geven de uitvoerbaarheid en werkbaarheid te toetsen.

In het volgende hoofdstuk wordt voor de invulling van elk van deze randvoorwaarden een aantal concrete suggesties gedaan.

4 Adviezen en verzoeken

Communicatie naar eindgebruikers

1. Er moet een Rijksbrede publiekscampagne komen ter ondersteuning van de multimiddelenaanpak om eindgebruikers bewust te maken van het belang van hogere betrouwbaarheidsniveaus, zodat de vraag naar authenticatiemiddelen op niveau substantieel en hoog op gang wordt gebracht. Geadviseerd wordt bovendien om voor specifieke doelgroepen (denk bijvoorbeeld aan de zorg) maatwerkcommunicatie te bieden (publiekscampagnes afgestemd op een specifieke doelgroep en hun wensen, behoeftes en zorgen).
2. Er moet op het niveau van de multimiddelenaanpak een uniforme keuzehulp worden aangeboden om eindgebruikers te begeleiden naar een middel dat past bij hun gebruiksvoorkeur. Deze keuzehulp helpt de gebruiker bij het kiezen van een stelsel en vervolgens een middelenleverancier binnen dat stelsel welke het beste past bij zijn of haar situatie. Hiermee wordt bijvoorbeeld voorkomen dat er een middel op niveau substantieel wordt aangeschaft terwijl er (ook) een wens is om transacties op niveau hoog te doen. De keuzehulp moet onderdeel worden van de Uniforme Set van Eisen. Zie als voorbeeld de Gov.UK Verify keuzehulp: www.viewdrivingrecord.service.gov.uk/verify/start. *De governance ETD is bezig een keuzehulp voor Idensys te ontwikkelen die mogelijk als voorbeeld kan dienen voor de keuzehulp op het niveau van de multimiddelenaanpak.*
3. Het perspectief van de eindgebruiker moet te allen tijde prevaleren in de uitwerking van eisen. Dit betekent onder andere dat het polymorfe pseudoniem behouden moet blijven in de Uniforme Set van Eisen op zowel niveau substantieel als hoog.

Stimulerende maatregelen

4. Er moet in de voorloopfase (fase 1) een voorziening worden getroffen om de uitrol van middelen op niveau substantieel en hoog te stimuleren zodat er voldoende massa is op deze niveaus bij inwerkingtreding van de wet GDI (januari 2019).
5. Er moet in de Uniforme Set van Eisen een mogelijkheid worden opgenomen tot afgeleide identificatie (het aanvragen van een erkend middel met behulp van een ander erkend middel op hetzelfde betrouwbaarheidsniveau) om de kosten van uitgifteprocessen van middelen omlaag te brengen.

Ontzorging van dienstverleners

6. De Ontsluitende diensten (makelaars) die dienstverleners ontzorgen, moeten een verplichting krijgen om alle Erkende middelen te ondersteunen (ongeacht het koppelvlak). Daarbij moet worden voorkomen dat er een single point of failure ontstaat. Hoge kosten voor

dienstverleners om alle erkende middelen (en stelsels) te kunnen accepteren worden hiermee voorkomen.

7. De wet GDI moet het gebruik van het BSN als stamgegeven toestaan voor de uitgifte van middelen op niveau laag. De huidige wet dwingt op dit moment meerdere koppelvlakken/architecturen af voor dienstverleners en leveranciers die middelen op zowel niveau laag als substantieel/hoog aanbieden, wat leidt tot aanzienlijke kostenverhogingen. Dit raakt met name het private domein, waar niveau laag nog steeds de standaard is. Daarnaast raakt dit ook dienstverleners in het BSN-domein die tijdelijk niveau laag willen blijven accepteren in de overgangstermijn van 3 jaar na inwerkingtreding van de wet GDI.
8. Dienstverleners moet zekerheid worden geboden dat zij door de acceptatieplicht niet geconfronteerd gaan worden met niet-marktconforme prijzen.
9. Dienstverleners moeten zekerheid krijgen dat zij (doelgroep)specifieke oplossingen pas hoeven uit te faseren als hier alternatieven voor bestaan (continuïteit van dienstverlening).

Level playing field

10. Er moeten maatregelen worden getroffen om het commerciële perspectief van de multimiddelenaanpak voor private middelenleveranciers te vergroten, anders bestaat het risico dat er onvoldoende private middelen beschikbaar komen voor een gezonde, concurrerende markt. Dit zal ook verstrekkende gevolgen hebben voor de authenticatiemarkt in het private domein. Een ongezonde markt geeft een dreiging voor monopolies en kostenopdrijving.
11. De eisen uit de Uniforme Set van Eisen moeten voor alle partijen, publiek en privaat, op gelijke wijze gelden en op hetzelfde moment ingaan. Dat betekent bijvoorbeeld dat óók de publieke middelen aan de USvE moeten voldoen. Er moet daarnaast duidelijkheid komen over de implementatietermijn voor de gestelde eisen.
12. Er moet nog dit jaar duidelijkheid komen over de leges voor het publieke middel en de wijze waarop deze berekend worden.
13. Er moet duidelijkheid komen over het moment van en de voorwaarden voor uitrol van het publieke middel substantieel in fase 0. Voor een gelijkwaardig speelveld is het essentieel dat dit middel aan dezelfde beperkende voorwaarden is gebonden als de uitrol van private middelen op hetzelfde niveau.
14. Het moet in de wet mogelijk worden om naast individuele leveranciers ook Afsprakenstelsels te erkennen. Dit verlaagt de lasten die gepaard gaan met erkenning van partijen en gaat versnippering van het veld tegen.

Governance

15. Enkele jaren geleden is de overheid gestart met een publiek-private samenwerking gericht op de toekomst van eID, vanuit de gedachten dat de uitvoerbaarheid en gedragenheid van het beleid gebaat zou zijn bij directe betrokkenheid van de primaire stakeholders: eindgebruikers, dienstverleners en leveranciers. Met de ontwikkeling van de USvE is van deze constructie afgestapt, met als gevolg dat beschikbare kennis onvoldoende wordt benut en afwegingen in het beleid en de regelgeving onvoldoende transparant worden gemaakt. Er moet daarom opnieuw een overlegstructuur komen waarin dienstverleners, erkende leveranciers en

eindgebruikers inspraak krijgen in de doorontwikkeling van eID om te zorgen dat het beleid en de daaruit voortvloeiende uitvoeringsregelgeving uitvoerbaar blijven en aansluiten bij de laatste wensen en ontwikkelingen.

16. Er moet een verbinding komen tussen het beheer van de USvE en het beheer van erkende stelsels en middelen zodat afspraken gemaakt kunnen worden over de change- en releasecyclus.

Rule based kader

17. De Uniforme Set van Eisen is een normenkader met een mix van zowel rule based als principle based normen, waarbij de nadruk op rule based ligt. Het is essentieel dat de nadruk op rule based behouden blijft, zodat de vaststelling van identiteiten gebeurt op basis vans specifieke voorschriften. Alleen dan heeft het onderscheid tussen betrouwbaarheidsniveaus werkelijk waarde. Een principle based kader geeft wel richting maar schrijft niet voor hoe in specifieke situaties te handelen. Hierdoor wordt afbreuk gedaan aan de zekerheid over iemands identiteit, terwijl juist dit één van de belangrijkste drijfveren is van het huidige eID-beleid.

Duidelijkheid over nog ontbrekende passages

18. Er moet zo spoedig mogelijk, maar niet later dan eind 2017, duidelijkheid komen over de voorwaarden die aan leveranciers en dienstverleners worden gesteld in het kader van de wet. Dit betekent in ieder geval dat de nog ontbrekende hoofdstukken van de USvE, alsmede de AMvB's en ministeriële regelingen worden uitgewerkt.
19. De uitwerking van het machtigingen- en attributenvraagstuk is nog nauwelijks bekend; dit geldt ook in het domein van ondernemingen (en rechtspersonen). Echter in het wetsvoorstel wordt al wel een eerste kader neergelegd. Voorkomen moet worden dat dit te eng wordt geformuleerd. Want een zorgvuldige werking van machtigingenstructuren is essentieel voor een goede werking van de digitale infrastructuur.