DigiD

VERKENNING E•HERKENNING een andere opzet voor DigiD

Een verkennende studie naar de mogelijkheden van elektronische herkenning van bedrijven en burgers uitgevoerd door Innopay (Leendert Bottelberghs en Chiel Liezenberg). In opdracht van het Ministerie van Economische Zaken en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Ministerie van Economische Zaken

Ministerie van **Binnenlandse Zaken** *en* **Koninkrijksrelaties**

innopay

Inhoud

Voorwoord

Gebruikers en aanbieders van diensten op het internet moeten met zekerheid kunnen vaststellen met wie ze te maken hebben. Voor onze economie is dit een essentiële voorwaarde om beter elektronisch zaken te kunnen doen, ook internationaal.

De huidige manieren om contact te leggen tussen dienstenaanbieders en gebruikers beginnen te knellen. Er zijn te veel verschillende oplossingen, vaak onhandig, met een beperkt toepassingsgebied, moeilijk te onthouden of onvoldoende veilig. Deze onoverzichtelijke 'digitale sleutelbos' leidt tot problemen: fraude neemt toe, gebruikers worden wantrouwend, de veiligheid van het elektronisch verkeer neemt af. Dat remt een verdere ontwikkeling van het elektronisch verkeer. Dat kan en moet dus beter, slimmer. Het is tijd om nieuwe stappen te zetten.

Innopay presenteert in deze verkenning een aansprekende benadering. Mobiele telefoons, bankpassen en diverse bedrijfssystemen kunnen gebruikt worden om een belastingaangifte te ondertekenen, een vergunning aan te vragen of tal van andere zaken betrouwbaar via internet af te handelen. Innopay introduceert dus geen nieuwe toepassingen, maar stelt voor om bestaande middelen te gebruiken om transacties per internet veilig en betrouwbaar te laten verlopen. Bestaande oplossingen van diverse partijen kunnen zo via een 'open stelsel' aan elkaar worden gekoppeld.

Enkele jaren geleden hebben we DigiD geïntroduceerd. Dankzij dit ene authenticatiemiddel kan de overheid digitale diensten verlenen. Dat was een belangrijke stap. Maar wat nu? Met deze verkenning leveren de ministeries van Economische Zaken en Binnenlandse Zaken en Koninkrijksrelaties een bijdrage aan de discussie over de volgende stappen. Het is vooral voor het bedrijfsleven en grote overheidsdienstverleners urgent om breed toepasbare en breed gedragen oplossingen tot stand te brengen zodat ze weten met wie ze op internet te maken hebben. Deze uitdaging heeft voor ons hoge prioriteit.

Drs. F. Heemskerk
Staatssecretaris van Economische Zaken

Management Samenvatting

Herkenning van gebruikers in digitale omgevingen vormt een steeds grotere uitdaging. Al jaren wordt geworsteld met het ontbreken van voldoende beschikbare mogelijkheden voor digitale herkenning van gebruikers. Nu steeds meer transacties elektronisch worden afgewikkeld leidt dit tot problemen, zoals groeiende fraude, wantrouwen bij gebruikers en afname van veiligheid.

Voor het vertrouwen dat nodig is om elektronisch transacties te kunnen doen zijn betrouwbare mogelijkheden voor het herkennen van gebruikers in het elektronische domein noodzakelijk. Bedrijven hebben ondertussen eigen benaderingen voor deze problematiek. Goede voorbeelden hiervan zijn internetbankieren en iDEAL, waarvoor banken speciale middelen uitgeven om hun gebruikers op betrouwbare wijze te kunnen herkennen. Ook de overheid is bezig met eigen oplossingen. In 2003 is DigiD gelanceerd, een oplossing voor overheidsdiensten en uitgegeven aan burgers en bedrijven. Toepassing van deze oplossing door onder meer de Belastingdienst heeft voor een hoge penetratie gezorgd (ca. 6 miljoen burgers), maar deze oplossing wordt gemiddeld per gebruiker slechts 1,2 keer per jaar gebruikt. Veel gebruikers vergeten hun wachtwoord, hetgeen leidt tot hoge kosten en slechte gebruikersbeleving.

Het Ministerie van Economische Zaken en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzoeken graag de mogelijkheden om de herkenning van gebruikers in het elektronische domein naar een hoger niveau te brengen. Hiermee wordt de ontwikkeling van e-Overheid gestimuleerd en wordt een bijdrage geleverd aan de verdere ontwikkeling van de e-Economie ook buiten de overheid. Hiervoor is echter een andere benadering van het probleem nodig. De oplossing ligt in het gedeeld gebruiken van (bestaande) middelen om gebruikers elektronisch te herkennen (zogenaamde authenticatiemiddelen). Hierbij kan bijvoorbeeld gedacht worden aan middelen van financiële instellingen, de overheid en het notariaat. Herkenning van gebruikers in het elektronische overheidsdomein hoeft dan niet langer enkel op basis van door de overheid uitgegeven middelen. Iedere partij moet mee kunnen doen, zolang wordt voldaan aan non-discriminatoire kwaliteitscriteria. Daarbij kan ook de commerciële sector sterk profiteren van deze ontwikkeling en zijn partijen minder afhankelijk van het uitgeven van eigen authenticatiemiddelen.

Om partijen met elkaar te laten samenwerken is een 'open netwerk' nodig. Om een dergelijk netwerk goed te laten functioneren moeten afspraken worden gemaakt, zowel over techniek, toepassing alsook zakelijke aspecten. Afspraken in dit multidisciplinaire domein (standaarden) worden beschreven door middel van het concept van een zogenaamd 'scheme'. Een scheme gaat over het 'coöperatieve domein' tussen partijen en beschrijft o.a. rollen, techniek, toetredingsvoorwaarden, certificering en handhaving. Naast het 'coöperatieve' domein (waar samenwerking de boventoon voert) is er het competitieve domein, waarin marktpartijen hun eigen proposities en producten kunnen ontwikkelen (waar de concurrentie plaatsvindt). Door goed gebruik van een scheme ontstaan netwerkeffecten in combinatie met keuzevrijheid, marktwerking en vrije mededinging. Dit kan leiden tot snelle groei en een dynamische markt, zoals we hebben gezien bij iDEAL dat volgens het scheme concept is opgezet.

Bij de inrichting van DigiD volgens het concept van een 'scheme' speelt de overheid vooral een kaderstellende rol. Daarnaast kan de overheid zelf ook middelen blijven uitgeven, én tegelijkertijd afnemer zijn. Dit alles naast andere uitgevers van herkenningsmiddelen (zoals van banken, CA's, enzovoorts) en afnemers uit de commerciële sector.

Inleiding

2.1 Doel van deze verkenning

In het kader van de elektronische overheid is herkenning van gebruikers (burgers en bedrijven) in het elektronische domein een onmisbare schakel voor digitale dienstverlening. In dit kader was de komst van DigiD een goede springplank. Deze voorziening loopt momenteel echter tegen grenzen aan.

Het Ministerie van Economische Zaken en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties zien het als hun taak om de voorziening voor elektronische herkenning naar een hoger niveau te brengen. Daarbij ligt het voor de hand om zoveel mogelijk gebruik te maken van middelen die al voorhanden zijn. Het uitgangspunt is dat iedere partij die middelen voor herkenning aanbiedt kan aansluiten, mits zij aan non-discriminatoire kwaliteitscriteria voldoet. Zowel de dienstverlening rond uitgifte en beheer van deze middelen als het zekerheidsniveau van authenticatie moeten hiermee worden verbeterd.

Deze verkenning beschrijft een mogelijk nieuw concept voor DigiD, waarin marktwerking, mededinging en verbetering van de dienstverlening en het niveau van elektronische herkenning centraal staan. In dit oplossingsmodel, DigiD 'als scheme', treedt de Nederlandse overheid kaderstellend op en wordt de dienstverlening ingevuld door marktpartijen. Het doel van deze verkenning is een beeld te geven van wat een scheme is, hoe Digid 'als scheme' eruit kan zien en wat dit betekent voor de verschillende betrokken partijen.

2.2 Begripsbepaling

Dit rapport behandelt een onderwerp waarbinnen er veel verwarring bestaat over de gehanteerde begrippen. We geven daarom onze interpretatie van een aantal belangrijke begrippen die vaak in dit rapport terugkomen.

2.2.1 Identificatie

Identificatie is het koppelen van een set specifieke gegevens aan een persoon (gebruiker), waarmee deze kan worden onderscheiden van andere personen. Het kan hierbij gaan om zowel natuurlijke personen alsook rechtspersonen. De set specifieke gegevens die nodig is om een persoon uniek te identificeren hangt af van de context. Wanneer men bijvoorbeeld een burger uniek wil onderscheiden, dan wordt het BSN gebruikt. Voor een bedrijf geldt

in deze situatie dat het KvK-nummer uniek is en dit nummer kan bijvoorbeeld gebruikt worden in combinatie met een persooneelsnummer om werknemers van bedrijven uniek te kunnen herkennen.

2.2.2 Authenticatie en authenticatiemiddelen

Authenticatie is het verifiëren van een geclaimde identiteit, met als doel het kunnen herkennen van een gebruiker (bv. persoon of bedrijf). Middelen die hiervoor worden ingezet worden authenticatiemiddelen genoemd. Voorbeelden van authenticatiemiddelen in de fysieke wereld zijn het paspoort en rijbewijs. In de elektronische wereld worden andere middelen gebruikt, omdat personen hier door systemen moeten worden herkend. Voorbeelden van authenticatiemiddelen in het elektronische domein zijn bijvoorbeeld gebruikersnaam en wachtwoord, pinpas (token) en pincode. Maar er worden ook meer ingewikkelde methoden ingezet zoals zogenaamde PKI passen, die de betrouwbaarheid voor juiste herkenning van de gebruiker vergroten.

2.3 Document opzet

In hoofdstuk 3 wordt de achtergrond gegeven over DigiD en de huidige problematiek. In het volgende hoofdstuk worden de problemen geanalyseerd aan de hand van de DigiD dienstverlening en de organisatie hiervan. Uit deze analyse komt naar voren dat veel van de problematiek met een bestaand model – een scheme - kan worden opgelost. In hoofdstuk 5 wordt verder ingegaan op de scheme en op welke wijze de principes hiervan kunnen worden toegepast op DigiD. Hoofdstuk 6 geeft een voorbeeld van hoe DigiD er als scheme uit kan zien. In het laatste hoofdstuk worden aanbevelingen gedaan voor aandachtspunten en worden de vervolgstappen op een rij gezet.

Achterin het document zijn de definities, specifiek met betrekking op het fenomeen ‘scheme’ en online authenticatie, in deze verkenning toegelicht onder Terminologie.

Achtergrond

3.1 DigiD

3.1.1 De start

In 2003 is DigiD ontstaan uit de gezamenlijke behoefte van de manifestpartijen (een groep grote uitvoeringsorganisaties) aan één authenticatiemiddel waarmee de burger elektronisch diensten kon afnemen bij verschillende instanties. De dienstverlening van DigiD is daarna uitgebreid, zodat ook bedrijven konden worden herkend met dezelfde dienst. Begin 2006 is DigiD overgedragen aan de gemeenschappelijke beheerorganisatie GBO. Overheid. GBO.Overheid is onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. GBO.Overheid zorgt in samenwerking met de Belastingdienst voor het beschikbaar maken van DigiD aan het brede publiek.

3.1.2 Eén inlogcode voor de hele overheid

Burgers kunnen bij DigiD een gebruikersnaam met wachtwoord aanvragen, eventueel aangevuld met SMS authenticatie. De gebruikersnaam met wachtwoord is gekoppeld aan een uniek nummer (Burger Service Nummer). Er zijn momenteel ca. 6 miljoen DigiD accounts aan burgers uitgegeven.

Ook bedrijven kunnen een DigiD inlogcode aanvragen, die is gekoppeld aan hun KvK-nummer. Het gebruik van DigiD door bedrijven is op dit moment verwaarloosbaar.

In dit rapport worden burgers en bedrijven gezamenlijk beschouwd als 'gebruikers'. Met betrekking tot de authenticatiedienstverlening geen onderscheid gemaakt. Beide typen gebruikers verlangen in principe namelijk dezelfde functionaliteit: ze willen op betrouwbare wijze worden herkend via het internet.

3.1.3 DigiD dienstverlening

Voor overheidsinstellingen die hun klanten elektronische diensten willen aanbieden, vormt DigiD een welkome hulp omdat zij hiermee gebruikers eenvoudig kunnen herkennen. Een overheidsinstelling beschikt in één keer over een kant-en-klaar authenticatiesysteem dat snel aan haar website kan worden gekoppeld. Een ander voordeel voor overheids-

instanties is dat DigiD centraal wordt beheerd. Het uitgeven en beheren van authenticatiemiddelen (denk aan het doorvoeren van wijzigingen in gebruikersgegevens) is kostbaar en ingewikkeld en kan fors beslag kan leggen op de capaciteit van de overheidsinstelling. DigiD ontneemt de overheidsinstelling die last, zodat deze meer tijd overhoudt voor zijn kernactiviteiten. Ook voorkomt DigiD dat meerdere overheidsinstellingen een eigen systeem (moeten) ontwikkelen. Het belangrijkste voordeel is natuurlijk dat een overheidsinstelling zijn klanten met DigiD al op korte termijn het gemak kan bieden van dienstverlening via internet.

De gebruikers (burgers én bedrijven) hebben ook baat bij DigiD. De omvang van hun 'digitale sleutelbos' blijft beperkt doordat zij met één inlogcode bij alle overheidsinstanties terecht kunnen.

3.2 Problemen met DigiD

In de afgelopen jaren is DigiD voor burgers flink gegroeid en neemt een groot aantal overheidsorganisaties gebruik van de centrale dienstverlening. Met deze groei van het aantal gebruikers is ook een aantal uitdagingen naar voren gekomen. De belangrijkste worden hier toegelicht.

3.2.1 Navragen authenticatiegegevens

Een burger heeft maar een beperkt aantal contactmomenten met de overheid via online diensten, ongeveer 1,2 per jaar. Het authenticatiemiddel wordt zeer beperkt gebruikt. Dit kan er toe leiden dat de burger zijn gebruikersnaam en/of wachtwoord vergeet of kwijt raakt. Als dit gebeurt moet een nieuw DigiD account worden aangevraagd, waarbij het gehele registratieproces opnieuw moet worden doorlopen.

Dit zorgt voor extra werk voor de beheerorganisatie van DigiD, die nieuwe gegevens moet uitgeven voor dezelfde burgers. Verder is dit belastend voor de burger, omdat deze extra handelingen moet verrichten en moet wachten op zijn nieuwe gegevens. Het gebruiksgemak voor de burger neemt hierdoor af, en dit kan belemmerend werken voor afname van online diensten.

3.2.2 Kosten beheer en uitgifte

Het DigiD platform wordt centraal beheerd door GBO.Overheid. Dit betekent dat ook alle kosten centraal worden gedragen. Door het relatief lage aantal transacties en het grote aantal navragen op de authenticatiegegevens, is het lastig om deze organisatie

kostenefficiënt te laten opereren. Het ligt voor de hand dat hier synergievoordelen geboekt kunnen worden als gebruikers hun authenticatiemiddelen voor meer digitale dienstverlening kunnen gebruiken. De kosten per transactie kunnen omlaag.

3.2.3 Beperkte zekerheid basisniveau

Voor het basisniveau van authenticatie wordt nu gebruik gemaakt van een gebruikersnaam en wachtwoord combinatie. Het voordeel van dit authenticatiemiddel is dat het eenvoudig is in gebruik en beheer en daardoor lage kosten kent in vergelijking met meer geavanceerde middelen. Het nadeel is dat het zekerheidsniveau beperkt is en niet geschikt voor transacties waarbij meer zekerheid over de identiteit gewenst is. Door DigiD wordt ook de mogelijkheid geboden om de authenticatie uit te breiden met SMS. Dit verhoogt weliswaar het zekerheidsniveau, maar is voor de burger nog facultatief. Hierdoor biedt het geen garantie voor de dienstverlener. Voor het hoogste zekerheidsniveau wordt er in de toekomst een elektronische identiteitskaart voorzien. Het is echter nog onduidelijk wanneer deze zal worden geïntroduceerd.

In de markt wordt steeds meer gebruik gemaakt van *'two-factor*[1]*'* authenticatie voor betrouwbare dienstverlening. Door banken wordt veelal gewerkt met tokens, maar ook met gebruikersnaam en wachtwoord samen met SMS. De trend is dat deze middelen steeds geavanceerder worden, om mogelijke *phishing* en *man-in-the-middle*[2] aanvallen te kunnen weerstaan. Wanneer de overheid up-to-date wil blijven zullen de kosten voor uitgifte en beheer van authenticatiemiddelen zeker toenemen.

3.3 iDEAL als inspiratiebron

Door de overheid wordt – in het kader van online gebruikersherkenning - met grote interesse gekeken naar het succes van iDEAL. Deze Nederlandse internet-betaalstandaard is binnen 2 jaar de meest gebruikte methode voor het afrekenen van online aankopen. De belangstelling van de overheid is niet vreemd: in beide gevallen is digitale herkenning van de gebruiker nodig om een transactie te autoriseren.

1 Bij *two-factor* authenticatie wordt geverifieerd aan de hand van twee factoren: een kenniskenmerk (iets dat men weet) en een bezitskenmerk (iets dat men bezit). Een voorbeeld hiervan is een beveiligde pas in combinatie met een PIN code, die men beide nodig heeft om een transactie te kunnen doen.

2 Zie voor een uitgebreide uitleg over *Phishing* en *Man-in-the-middle* aanvallen de bijlage Terminologie.

Met iDEAL kan in principe iedere klant, die beschikking heeft over een internetbankier-product van een Nederlandse bank die de standaard ondersteunt, betalen bij een online winkelier die iDEAL accepteert. Miljoenen mensen in Nederland maken reeds gebruik van een internetbankier-product. Een verkoper die iDEAL betalingen accepteert heeft zo in één klap miljoenen potentiële klanten die realtime kunnen betalen in zijn online winkel.

Het succes van iDEAL is mede te danken aan het feit dat het voor consumenten herkenbaar is: ze doen de betaling in de vertrouwde omgeving van hun eigen bank. Hiervoor worden ook de authenticatiemiddelen van de eigen bank gebruikt. De overheid is dan ook met name geïnteresseerd in het (her-) gebruik van authenticatiemiddelen, die reeds op zeer frequente basis door consumenten worden toegepast. Dit kunnen zowel bestaande als nog in de markt te introduceren middelen zijn.

De sleutel voor dit succes zit achter de schermen: de afspraken die zijn gemaakt om alle Nederlandse banken toe te laten tot het scheme. Door samen het netwerk op te bouwen, in plaats van de concurreren met een eigen netwerk, profiteren zowel consumenten als online winkeliers en uiteindelijk ook de banken zelf.

3.4 Voorwaarden oplossing

Door de Ministeries van EZ en BZK wordt gekeken of de DigiD dienstverlening op de drie genoemde punten in paragraaf 3.2 kan worden verbeterd: (1) aantal navragen, (2) kosten voor beheer en uitgifte en (3) het niveau van authenticatie.

Bij het oplossen van de problemen staan derhalve de volgende punten centraal:

- Minder operationele beheersinspanningen voor de overheid.
- Er dient een betere kosten/baten verhouding te zijn voor de overheid.
- Het beveiligingsniveau van authenticatiemiddelen moet up-to-date zijn, minimaal vergelijkbaar met het niveau dat in de markt voor vergelijkbare toepassingen wordt gebruikt.

In de oplossing willen de Ministeries graag gebruik maken van de authenticatiemiddelen die reeds in de markt aanwezig zijn en door derde partijen worden beheerd en uitgegeven. Hiermee wil de overheid er ook aan bijdragen dat de digitale sleutelbos van de gebruiker beperkt blijft. Met een dergelijke oplossing kan de gebruiker zijn middel voor vele diensten inzetten.

4

Probleemanalyse

4.1 Typering DigiD dienstverlening

Het is belangrijk om de karakteristieken van de dienstverlening van DigiD goed te begrijpen om aan de eerder gestelde eisen te kunnen voldoen. Het product dat met de authenticatie-dienstverlening van DigiD wordt gevormd, is een zogenaamde *'two-sided market'*. Dit type markt, ook wel *'two-sided network'* genoemd, is een economische netwerken met twee verschillende typen gebruikers die elkaar netwerkvoordelen verschaffen. Voorbeelden van dit soort markten zijn credit cards (kaarthouders en acceptanten) en communicatiesystemen zoals internet (websites en bezoekers). In het geval van DigiD gaat het om de e-dienstverleners en burgers. Belangrijk is dat de dienstverlening naar deze twee groepen verschillend is. Dit in tegenstelling tot bijvoorbeeld een telefonienetwerk, waarbij elke gebruiker in principe dezelfde dienstverlening afneemt.

In een *two-sided* markt zijn er twee typen netwerkeffecten: *'cross-side'* en *'same-side'*. Een *'same-side'* netwerk effect verhoogt de waarde van de dienst wanneer meer gebruikers tot dezelfde kant van het netwerk toetreden, terwijl een *'cross-side'* effect juist de waarde van de dienst verhoogt bij het toetreden van gebruikers van de andere kant van het netwerk. Dit fenomeen zorgt ervoor dat beide groepen baat hebben bij de groei van het netwerk als geheel.

In het geval van DigiD gelden deze regels ook. De e-dienstverleners hebben er baat bij als de groep gebruikers die hun online diensten kunnen afnemen zeer groot is. Met andere woorden: zoveel mogelijk gebruikers moeten beschikken over de benodigde authenticatiemiddelen. Zoveel mogelijk potentiële gebruikers moeten over deze middelen beschikken.

Aan de andere kant geldt voor gebruikers hetzelfde: zij hebben er baat bij om met één authenticatiemiddel bij alle (overheids-) instanties terecht te kunnen. Wanneer er verschillende *'identity'* dienstverleners zijn waar gebruikers een uniek een account moeten hebben om per (e-Overheids)dienstverleners de online diensten af te kunnen nemen, dan zal deze methode van werken een drempel vormen voor de gebruiker. De gebruiker zal minder snel geneigd zijn de van de dienstverlening gebruik te maken vanwege de gebruiksonvriendelijkheid (digitale sleutelbos). De beide kanten van het netwerk kunnen elkaar versterken: er is hier duidelijk sprake van netwerkeffecten.

In de verdere analyse zullen we deze kenmerken van DigiD meenemen en de dienst beschouwen als een netwerk met twee groepen: de e-dienstverleners en de gebruikers.

4.2 Gebruiksfrequentie

Door de relatief lage gebruiksfrequentie en heeft DigiD een relatief lage relevantie voor gebruikers, ze gebruiken het amper. Dit gebrek aan relevantie kan op twee manieren worden aangepakt:

- Inzetten van beschikbare middelen die reeds frequent worden gebruikt door de burger. Een mooi voorbeeld hiervan zijn de authenticatiemiddelen die door banken worden uitgegeven en beheerd. Daarnaast is er natuurlijk ook ruimte voor andere (nieuwe) spelers in deze markt.
- Het vergroten van het toepassingsgebied om het authenticatiemiddel in te zetten. Momenteel kan DigiD alleen worden gebruikt door overheidsinstellingen. Het toelaten van meerdere e-dienstverleners (ook niet-overheidspartijen) tot het netwerk kan bijdragen aan een hogere gebruikersfrequentie.

De twee genoemde manieren – meer middelenaanbieders samenbrengen en middelen breder inzetbaar maken - sluiten elkaar niet uit en een combinatie van beide zou de relevantie van DigiD als authenticatiemiddel sterk kunnen vergroten. Het hergebruik van bestaande authenticatiemiddelen levert nog twee belangrijke voordelen op. De operationele belasting voor beheer en uitgifte liggen niet meer bij de overheid. Verder kan gebruik gemaakt worden van authenticatiemiddelen met een hoger zekerheidsniveau die reeds in de markt aanwezig zijn en op grote schaal gebruikt worden, dit kan onderdeel uitmaken van de afspraken.

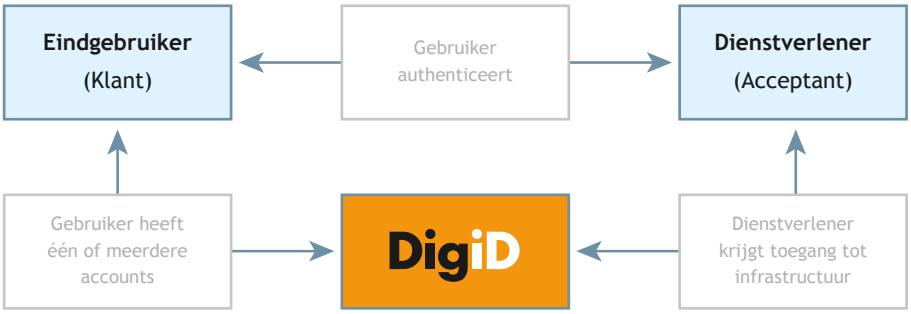
Vanuit het netwerkperspectief is het logisch het aantal e-dienstverleners dat gebruik maakt van het netwerk te vergroten. Dit levert de benodigde *'cross-side'* effecten op om het netwerk succesvol te maken. Gebruikers kunnen hierdoor hetzelfde authenticatiemiddel bij meer e-dienstverleners inzetten. En e-dienstverleners krijgen toegang tot een netwerk waarin al zeer veel gebruikers over authenticatiemiddelen beschikken.

4.3 Centraal platform: 3-partijen model

'DigiD' bestaat momenteel uit drie elementen:

- **Organisatie:** zorgt voor de uitgifte en het beheer van de DigiD accounts.
- **Platform:** de onderliggende infrastructuur (A-Select).
- **Authenticatiemiddel:** gebruikersnaam (of KvK nummer voor bedrijven) & wachtwoord, eventueel met SMS.

In de huidige opzet heeft DigiD een centrale positie in een zogenaamd 3-partijen model. Hierbij liggen businessmodel, merk, toepassing en infrastructuur allemaal in één hand en worden beide kanten van de markt (burgers en e-overheid) door dezelfde partij bediend. Dit houdt in dat deze partij beide kanten van het netwerk moet ontwikkelen en binnen dat netwerk een monopolistische positie opbouwt.



Figuur 4-1: 3-partijen model van huidig DigiD.

Een dergelijk model is niet open. Er is altijd één partij met een centrale positie in het netwerk. Wanneer men een dergelijk model in een vrije markt wil toepassen, kan dit op termijn problemen opleveren (mededinging), zoals dat bij het vroegere Interpay is gebeurd. Hier waren ook business, merk, toepassing en infrastructuur gecombineerd in één partij, die later is opgesplitst. In de nieuwe samenstelling (met onder andere Currence) zijn de rollen gescheiden waardoor meer marktwerking mogelijk is en mededinging beter tot zijn recht komt.

4.4 Trends in de markt

4.4.1 Ook vraag buiten de overheid

Overheidsinstanties zijn niet de enige partijen met een behoefte aan online authenticatie-diensten. Ook buiten de overheid bestaat er een grote behoefte aan betrouwbare authenticatie voor online dienstverlening. Dit kan in veel verschillende processen grote voordelen opleveren. Enkele belangrijke toepassingsgebieden zijn:

- **Veilige toegang tot informatie:** steeds meer bedrijven willen gebruikers (klanten) elektronisch toegang geven tot vertrouwelijke informatie. Denk bijvoorbeeld aan de zorgsector (patiëntendossier), verzekeringsmaatschappijen (polissen) en telecom-aanbieders (gebruikspecificaties).

- **Volledige elektronische afhandeling:** nog steeds komt er bij veel processen papier aan te pas, terwijl deze processen grotendeels zijn gedigitaliseerd. Enkele voorbeelden hiervan zijn het tekenen van een contract (bijv. mobiele telefonie), het indienen van een declaratie (verzekeringen), het afsluiten van een polis (verzekeringen), etc.
- **Betrouwbare online identificatie:** dit gaat enigszins vooraf aan de vorige twee voorbeelden, maar kan ook op zich worden beschouwd. Het betrouwbaar kunnen identificeren van een gebruiker leidt tot vermindering van risico's in de dienstverlening. In het economisch verkeer kan dit leiden tot vermindering van gegevensuitwisseling, doordat de gegevens zelf veel betrouwbaarder zijn. Een voorbeeld hiervan is achteraf betalen bij een online bestelling. Dit zal een webwinkelier niet doen als hij de consument op een later tijdstip niet kan aanspreken op zijn betalingsverplichting.

Voor de partijen bij wie deze behoefte leeft, bestaat er momenteel geen aanbod. Deze partijen vormen samen een onderdeel van één kant van een netwerk dat moet worden ingevuld. Er liggen grote kansen voor de verdere ontwikkeling van online dienstverlening wanneer deze behoefte op de juiste wijze wordt ingevuld.

4.4.2 Investering in authenticatie door banken

De banken moeten om hun vertrouwenspositie te bewaken blijven investeren in de beveiliging van hun online dienstverlening. Hiertoe wordt ook geïnvesteerd in de authenticatiemiddelen die hun klanten gebruiken. De kosten van deze investeringen kunnen worden gedeeld over het aantal transacties dat met deze authenticatiemiddelen wordt gedaan. Het ligt voor banken voor de hand om hun authenticatiemiddelen voor zoveel mogelijk soorten transacties in te zetten, wanneer deze bijdragen aan het terugverdienen van (een deel van) de investeringskosten en de operationele kosten.

4.5 Oplossingsrichtingen voor DigiD

De typering van DigiD als *'two-sided'* netwerk (een markt met twee verschillende typen partijen – gebruikers en e-dienstverleners) levert inzichten op in de netwerkeffecten die samengaan met dit type dienstverlening. Door het stimuleren van deze netwerkeffecten kan de dienst in volle potentie worden benut. We zien dat DigiD in zijn huidige vorm dergelijke netwerkeffecten binnen het eigen systeem belemmert. Aan de éne kant van het netwerk (de burgers/gebruikers) is de relevantie van de dienst te laag, doordat het aanbod aan de andere zijde van het netwerk (e-dienstverleners) beperkt blijft.

Wanneer we het vergroten van de gebruiksfrequentie als uitgangspunt nemen, zijn er drie oplossingsrichtingen:

- Overheid gebruikt marktmiddelen; DigiD koppelt authenticatiemiddelen van derde partijen (bijv. banken) op het centrale platform.
- Markt gebruikt overheidsmiddelen; DigiD wordt beschikbaar voor alle e-dienstverleners, niet alleen overheid.
- Markt en overheid werken samen in een open netwerk; Beide kanten van het netwerk kunnen door marktpartijen worden ingevuld en ontwikkeld. De overheid treed hier op in een kaderstellende rol, en als afnemer van authenticatie-dienstverlening.

In de eerste oplossingsrichting maakt DigiD gebruik van een deel van bestaande netwerken die door marktpartijen zijn ontwikkeld. Dit is een manier om één kant van het DigiD netwerk (de burgers) te 'ontwikkelen'. In dit geval zal DigiD zelf ook authenticatiemiddelen moeten blijven uitgeven, om niemand uit te sluiten van het netwerk. Het lastige van deze oplossing is dat de authenticatiemiddelen van de banken in principe niet als losse dienst te koop zijn. De overheid moet deze middelen bij o.a. de banken afnemen. Hiervoor moeten de overheid en aanbieders het wel eens worden onder welke voorwaarden dit gebeurt.

In de tweede oplossingsrichting blijft de DigiD dienst ook centraal beheerd, maar wordt de e-dienstverleners kant van het netwerk ontwikkeld. Door alle dienstverleners toe te laten kan een enorm netwerk ontstaan, met de beoogde positieve netwerkeffecten. Het zekerheidsniveau van de authenticatiemiddelen moet dan waarschijnlijk hoger om het volledige spectrum aan toepassingen af te kunnen dekken (bijv. met de e-NIK). Daarentegen kan het aantal transacties sterk toenemen en kunnen de kosten per transactie omlaag. Het is uiteindelijk afhankelijk van het business model waar de kosten terecht zullen komen. Wanneer de overheid de dienstverlening gratis ter beschikking stelt, komen alle kosten centraal te liggen. Bij een prijs-per-authenticatie kan een deel van deze kosten worden terugverdiend.

Op zich is dit een zeer goede oplossing, maar de haalbaarheid en houdbaarheid ervan hangt af van verschillende factoren. Wanneer vergelijkbare netwerken voor authenticatiedienstverlening in de markt ontstaan, zal de overheid hier onbedoeld mee gaan concurreren. Een andere belemmering is dat DigiD (voor burgers) gebruik maakt van het BSN. Het gebruik van dit nummer kent wettelijke beperkingen. Dit gebruik is kort

gezegd voorbehouden aan overheidsorganisaties (en onder bepaalde voorwaarden aan de zorgsector).

Bij de laatste oplossingsrichting worden de negatieve kanten van de beide hiervoor beschreven oplossingen verholpen door een open netwerk te creëren. In dit open netwerk kunnen partijen die authenticatiemiddelen uitgeven onder bepaalde voorwaarden deelnemen en kunnen transactieverwerkende partijen onder bepaalde voorwaarden de toegang voor e-dienstverleners verzorgen. Tevens kunnen naast overheidsinstanties ook bedrijven koppelen als e-dienstverlener en zo de authenticatiediensten afnemen van het netwerk. Het aantal authenticatie-transacties zal hierdoor sterk toenemen, waardoor bestaande authenticatiemiddelen van derde partijen effectief kunnen worden hergebruikt. Belangrijk is dat in dit netwerk marktwerking ontstaat, waardoor voor beide kanten van het netwerk keuzevrijheid geborgd wordt. Dit moet tevens leiden tot kostenverlaging voor alle gebruikers van het netwerk.

Een aandachtspunt in deze oplossing is dat de vertrouwelijkheid en privacy van de informatie die in het netwerk tussen verschillende partijen wordt uitgewisseld gewaarborgd blijft. De overheid moet in deze oplossing een kaderstellende rol vervullen, om ervoor te zorgen dat de markt onder de juiste condities opereert en belangen van verschillende partijen worden behartigd.

4.6 Keuze oplossingsrichting

In de verdere uitwerking van de oplossing is gekozen voor een open netwerk, omdat dit de meeste kansen biedt, gelet op de verschillende ontwikkelingen en omstandigheden. In een dergelijk netwerk moeten natuurlijk goede afspraken worden gemaakt om het goed te laten functioneren. Deze afspraken gaan over onder andere toetreding, handhaving, certificering, gebruik, aansprakelijkheid, techniek, etc. Deze afspraken moeten ervoor zorgen dat er een nieuwe markt ontstaat van mededinging, waarbinnen partijen met elkaar in concurrentie[3] kunnen treden. Een bestaand paradigma voor een dergelijke set afspraken heet een 'scheme'[4] en wordt in het volgende hoofdstuk verder gespecificeerd en geanalyseerd.

3 De overheid heeft hierin een speciale eigen positie ten opzichte van marktpartijen, en neemt deel om belangen van overheid en burger te behartigen.

4 Het gebruik van de term 'scheme' in dit verband komt uit de betalingswereld. Meer informatie en achtergrond van 'schemes' staat in hoofdstuk 5.

Verkenning oplossingsrichting: DigiD als 'scheme'

5.1 Wat is een scheme?

5.1.1 Oorsprong

De term 'scheme' is een oplossing uit de jaren '70 voor netwerk- en schaalproblemen bij wereldwijde betaalsystemen, speciaal voor *'two-sided'* markets. Met behulp van schemes werden wereldwijde netwerken van kaarthouders en acceptatiepunten tot stand gebracht. Deze modellen worden 'card schemes' genoemd en het succes ervan is groot.

De kracht van dergelijke schemes ligt in een zuivere scheiding van businessmodel, functionaliteit en infrastructuur (ook wel: *'infoculture', 'infostructure'* & *'infrastructure'* en vaak: *'business', 'application'* & *'infrastructure'*). Met deze scheiding zijn modellen te realiseren waarbinnen tot op zekere hoogte wordt samengewerkt maar ook concurrentie kan plaatsvinden, en die bovendien met een geschikt businessmodel netwerk-effecten kunnen sorteren.

Voorbeelden van internationale credit card schemes zijn Visa en MasterCard. Lokale Nederlandse schemes zijn bijvoorbeeld PIN voor debit card en iDEAL voor online betalen met behulp van internetbankieren.

5.1.2 Domeinscheiding: concurreren en samenwerken

In een scheme dient het netwerk twee doelen: enerzijds faciliteert het samenwerking tussen partijen door gebruik van een gezamenlijke infrastructuur. Dit *coöperatieve domein* zorgt voor een verlaging van verschillende kosten (o.a. ontwikkelings- en toetredingskosten) doordat partijen op dit terrein samenwerken. Anderzijds stimuleert het netwerk concurrentie op productniveau, waarmee marktpartijen mogelijkheden hebben zich te onderscheiden op toegevoegde waarde: dit is het *competitieve domein*.

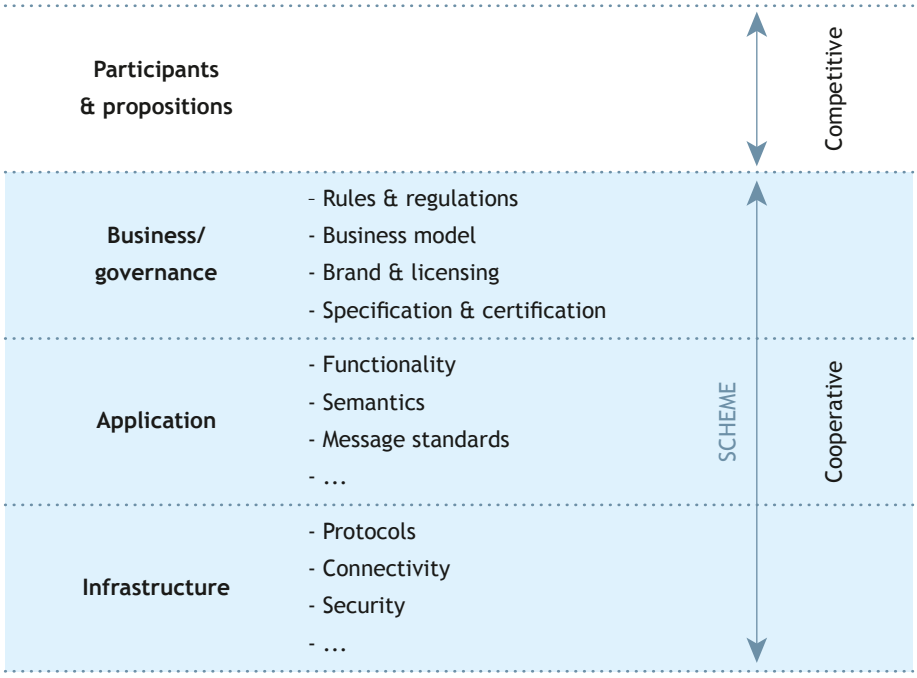
Met de scheiding van deze domeinen wordt voorkomen dat er wordt geconcurreerd op infrastructuur en dat partijen zich onderscheiden door de omvang van 'hun netwerk'. Concurrentie op het niveau van infrastructuur brengt extra kosten met zich mee, en levert geen extra voordelen voor de afnemers van de dienstverlening. Het scheiden van het coöperatieve en het competitieve domein is essentieel voor marktwerking en vrije mededinging.

5.1.3 Kernelementen van een scheme

Het coöperatieve domein van een scheme bestaat doorgaans uit drie kernelementen:

- **Business and Governance:** de commerciële laag, waarin afspraken worden gemaakt over hoe de participanten in de scheme met elkaar omgaan en welke rechten en plichten zij jegens elkaar en andere actoren in de scheme hebben;
- **Application:** de functionele laag, waarbinnen het toepassingsgebied en functionaliteit van het scheme worden gedefinieerd;
- **Infrastructure:** de ondersteunende laag, die ervoor zorgt dat verschillende partijen in het netwerk op een veilige en betrouwbare standaard manier met elkaar kunnen communiceren.

Bovenop dit coöperatieve domein kan het competitieve domein opereren zoals weergegeven in Figuur 5-1. In het competitieve domein kunnen de participanten in de scheme nu op basis van een '*level playing field*' proposities ontwikkelen voor de beoogde (2-zijdige) markt.



Figuur 5-1: Domeinscheiding in een scheme, opgedeeld in verschillende kernelementen.

5.1.4 Rollenscheiding

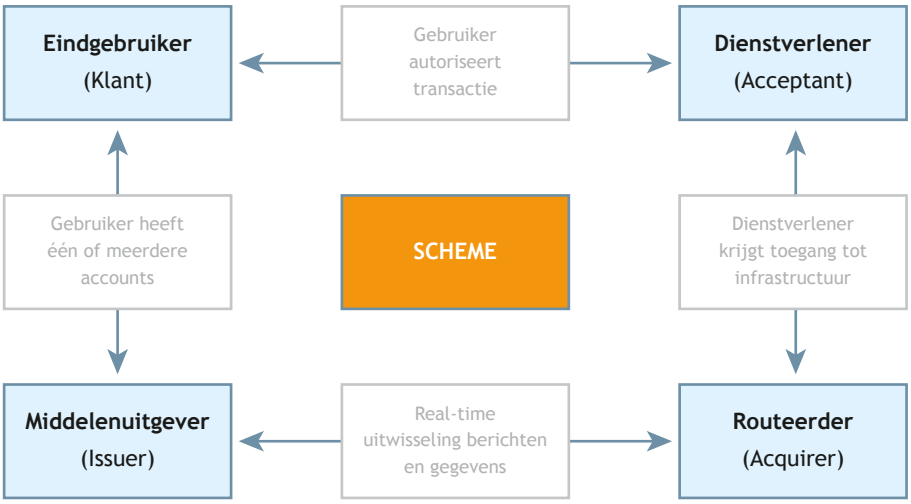
Een scheme kan worden vormgegeven in een zogenaamd 4-partijen model. Het 4-partijen model biedt belangrijke voordelen ten opzichte van een 3-partijen model. De rollen voor het bedienen van de twee verschillende kanten van het netwerk zijn uit elkaar getrokken: de Middelenuitgever (Issuer) bedient de Eindgebruiker, en de Routeerder (Acquirer) bedient de Dienstverlener (Acceptant); (zie Figuur 5-2). Deze twee rollen kunnen nu door verschillende partijen worden ingevuld. Zo wordt voorkomen dat er een centrale machtspositie ontstaat. Het is echter geoorloofd dat één enkele partij allebei de rollen vervult, daarom worden in de scheme duidelijke afspraken gemaakt over de rollen en verantwoordelijkheden.

In het 4-partijen model hebben alle actoren onderling zuivere bilaterale relaties en een duidelijk gedefinieerde rol in de keten:

- **Eindgebruiker en Dienstverlener:** de Eindgebruiker gaat met een dienstverlener een overeenkomst aan waarvoor authenticatie van de Eindgebruiker vereist is. Na de authenticatie wordt de overeenkomst als definitief beschouwd.
- **Dienstverlener en Routeerder:** de Routeerder biedt de Dienstverlener de mogelijkheid om authenticaties van klanten te verkrijgen, waartoe berichten en gegevens tussen beide worden uitgewisseld.
- **Routeerder en Middelenuitgever:** de Routeerder en de Middelenuitgever wisselen onderling in real-time berichten en gegevens uit.
- **Middelenuitgever en Eindgebruiker:** de Eindgebruiker heeft één of meer account(s) bij een Middelenuitgever (of accounts bij meerdere Middelenuitgevers). Elk account kan geselecteerd worden om een authenticatie mee uit te voeren. De Middelenuitgever biedt de Eindgebruiker de mogelijkheid zich te authenticeren bij de Dienstverleners.

De rollen en relaties worden schematisch weergegeven in Figuur 5-2 (*volgende pagina*).

Door het gebruik van het 4-partijen model is meer marktwerking mogelijk, doordat de dienstverlening richting beide kanten van het netwerk in concurrentie kan plaatsvinden. De afspraken in de scheme zorgen ervoor dat de belangen van de verschillende rollen elkaar versterken en niet tegenwerken. Het geheel bevordert schaalbaarheid van het netwerk, marktwerking en mededinging.



Figuur 5-2: Het '4-partijen' model in een scheme.

5.2 Toepassing op DigiD

Bij het toepassen van een scheme op de DigiD dienstverlening moeten de eerder gestelde uitgangspunten hun weerslag vinden in het coöperatieve domein van de scheme.

5.2.1 Mededinging

Om een markt met mededinging te laten ontstaan, moeten er heldere en eenduidige eisen zijn voor toetreding door marktpartijen. Deze non-discriminatoire regels zorgen ervoor dat in principe iedere partij kan toetreden die aan de gestelde eisen voldoet. Hierdoor ontstaat een zogenaamd *'level playing field'* waarin partijen dezelfde toetredings-drempels hebben moeten overwinnen.

5.2.2 Scope

Bij de transitie van DigiD naar een scheme met een open netwerk moet de scope opnieuw worden bekeken. Bij de afbakening moet de juiste ruimte worden gegeven aan de toepassingen. Mede bepalend hierbij is wie de DigiD dienst uiteindelijk zal afnemen: ook bij bedrijven bestaat er namelijk behoefte aan online authenticatie en zij hebben hierbij te maken met veel dezelfde problemen als de overheid. Een overweging bij het bepalen van de scope is daarom welke partijen afnemer kunnen worden. Daarnaast is het ook van belang wie de eindgebruikers zijn: alleen burgers, of ook bedrijven en

overheid. Afhankelijk van de combinatie afnemer – eindgebruiker zijn er verschillende toepassingen, met elk hun eigen behoefte aan functionaliteit en veiligheidsniveau. Het geheel van afnemers, eindgebruikers en toepassingen bepaalt uiteindelijk de scope.

AFNEMER (e-dienstverlener)	**EINDGEBRUIKER**	**TOEPASSING**
Overheid	Burgers ? Bedrijven ? Overheden ?	Aangifte / raadplegen belastingen Aanvragen visvergunning Vernieuwen paspoort Mestaangifte BTW aangifte ...
Bedrijven	Consumenten ? Bedrijven ? Overheden ?	Ondertekenen contract Afsluiten verzekering Afsluiten hypotheek ...

Tabel 5-1: Voorbeelden van combinaties Afnemer - Eindgebruiker - Toepassing.

De keuze van de scope werkt door op verschillende andere aspecten van het netwerk:

- Een te brede scope zorgt voor extra complexiteit in het netwerk. Wanneer er veel verschillende typen gebruikers en toepassingsgebieden zijn, moeten meer en complexere regels worden opgesteld om alles goed te kunnen beheersen. Dit kan van invloed zijn op de infrastructuur, maar ook op het *'level playing field'*.
- Een te nauwe scope belemmert het netwerkeffect. Hierdoor blijven de baten voor de participanten in het netwerk beperkt en zal het netwerk niet gaan groeien. Dit is van invloed op de business case.

Het soort toepassing is ook bepalend voor het benodigde zekerheidsniveau. Niet alle toepassingen vereisen hetzelfde beveiligingsniveau in authenticatie. De overheid moet – in samenwerking met marktpartijen – analyseren welke behoefte er bestaat bij de verschillende e-dienstverleners. Zodoende kan er differentiatie ontstaan in zekerheidsniveaus binnen de scheme, om binnen één netwerk te kunnen voldoen aan de verschillende eisen voor dienstverlening.

Bij het definiëren van een zekerheidsniveau moet zowel worden gekeken naar het authenticatiemiddel als de gehele administratieve organisatie van de middelenuitgever.

5.3 Conclusie

In de analyse van de mogelijkheden van DigiD als scheme komt naar voren dat de DigiD dienst zich zeer goed leent om in een dergelijke vorm te worden neergezet. Deze nieuwe dienst faciliteert het elektronisch herkennen van gebruikers, met behulp van middelen die door marktpartijen worden uitgegeven.

In deze nieuwe vorm kan een open netwerk worden gecreëerd waarin marktwerking en mededinging zijn geborgd. Essentieel voor het succes van de scheme is het netwerkeffect. Dit effect wordt voor een groot deel bepaald door de scope: voor welke toepassingen kan de DigiD dienst worden gebruikt. De scope bepaalt het potentieel van het netwerk in termen van aantal transacties, en is derhalve bepalend voor de business case op basis waarvan marktpartijen beslissen om toe te treden. Voordat de scheme verder wordt gespecificeerd moet daarom eerst in een scoping onderzoek de haalbaarheid ervan verder worden geanalyseerd.

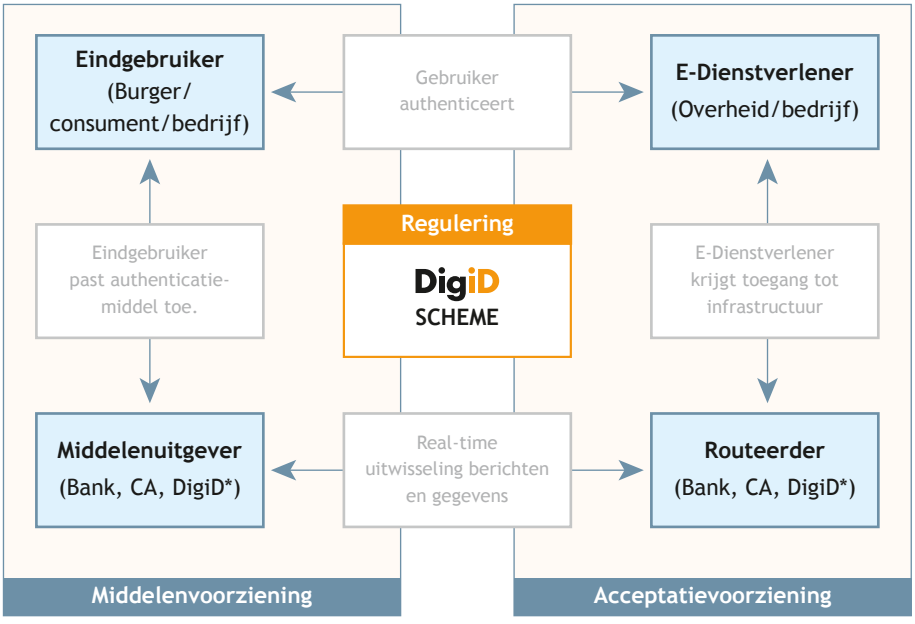
Voorbeeld DigiD als 'scheme'

6.1 Inleiding

Om een beeld te schetsen van hoe DigiD als scheme zal functioneren, beschrijven we een mogelijke invulling hiervan. Dit voorbeeld is niet definitief of bindend maar is bedoeld om meer gevoel te krijgen bij de rollen, actoren en processen die in de nieuwe situatie spelen.

6.2 4-partijen in de DigiD Scheme

Het huidige DigiD kan eenvoudig worden opgesplitst in twee rollen om van een 3-partijen naar een 4-partijen model over te gaan. Het DigiD onderdeel waar de authenticatie-middelen worden uitgegeven wordt de Middelenuitgever (issuer), het DigiD onderdeel dat de overheidsinstellingen aansluit wordt de Routeerder (acquirer). Het merk DigiD wordt onderdeel van de scheme-organisatie die ook de *'rules & regulations'* beheert. Op deze manier is er direct een invulling van een 4-partijen model gerealiseerd om het model te kickstarten. Marktpartijen kunnen dan worden uitgenodigd om binnen de scheme vergelijkbare rollen te vervullen, door te voldoen aan de *'rules & regulations'* van het DigiD scheme waardoor verder netwerkeffecten worden gerealiseerd.



Figuur 6-1: Invulling van 4 partijen bij DigiD als scheme.

De overheid speelt in deze scheme een initiërende en kaderstellende rol, maar hoeft niet als enige partij 'eigenaar' te zijn van het scheme. Er zijn verschillende mogelijkheden om de stakeholders een belang te geven in de organisatie die de scheme beheert, om te zorgen voor een breed draagvlak. Deze organisatie heeft naast het beheren en eventueel doorontwikkelen van de scheme ook andere taken: zij licentieert participanten en certificeert partijen die daarvoor in aanmerking komen door aan de vereisten te voldoen.

De volgende uitgangspunten kunnen worden gehanteerd voor 'DigiD als scheme':

- Belangrijke stakeholders worden gezamenlijk scheme eigenaar, en zien toe op naleving van de scheme *'rules & regulations'* door gecertificeerde participanten.
- De scheme wordt initieel ontwikkeld voor Nederlandse overheidsinstellingen en een aantal commerciële partijen, en wordt op termijn breder maatschappelijk toegepast.
- Het systeemmodel is open, bilateraal opgebouwd in een 4-partijen model en gedecentraliseerd.
- De implementatiecomplexiteit voor de acceptant dient geminimaliseerd te worden met inachtneming van de vereiste beveiliging.
- Alle communicatie verloopt via internet.

6.3 Gebruiker

Een gebruiker, die een account heeft bij een DigiD Middelenuitgever (bijvoorbeeld de DigiD authenticatiemiddelendienst of een bank die DigiD ondersteunt binnen het internetbankier-product), beschikt over de mogelijkheid om DigiD authenticaties af te geven.

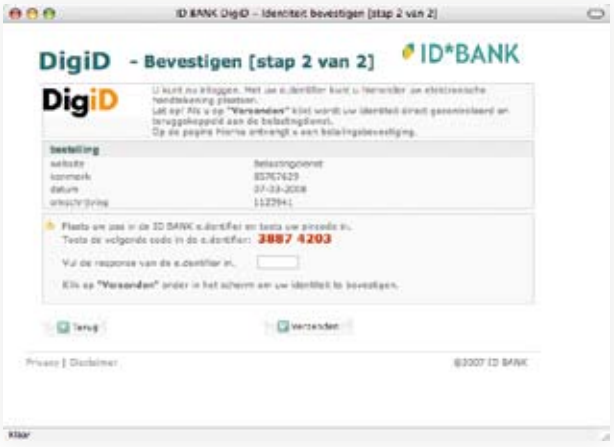
Een DigiD authenticatie afgeven vertaalt zich in handelingen die uitgevoerd moeten worden op internetpagina's die aan de klant worden getoond. We tonen hier een voorbeeld waarbij een burger online zijn belastingaangifte doet en deze ondertekent met DigiD via een bank.

De gebruiker (burger) vult zijn belastingaangifte in bij de E-Dienstverlener (Belastingdienst). Wanneer deze compleet is, kiest de gebruiker voor het ondertekenen van de aangifte met DigiD.

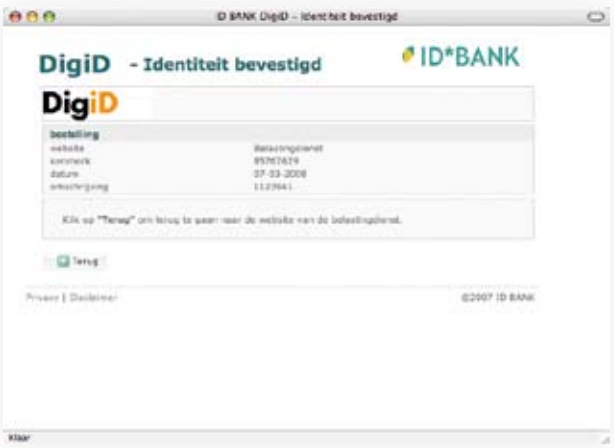
De gebruiker kan nu kiezen uit de lijst met Middelenuitgevers (Issuers) die DigiD ondersteunen. In dit geval kiest de gebruiker voor de bank waarbij hij internetbankiert, maar er kunnen meerdere soorten middelenuitgevers zijn die voldoen aan de scheme vereisten voor deze rol.

Het DigiD authenticatieverzoek en de gebruiker worden nu van de E-Dienstverlener (Belastingdienst) via de Routing Service (Acquirer) gerouteerd naar het login scherm van de geselecteerde Middelenuitgever (hier een bank). Hier volgt de gebruiker de gebruikelijke inlog-procedure van zijn bank.

De Middelenuitgever toont het betreffende authenticatieverzoek aan de gebruiker. De gebruiker wordt geauthenticeerd m.b.v. de methode die daarvoor bij de Middelenuitgever gebruikelijk is. Indien de authenticatie succesvol is wordt hier een bericht voor opgesteld en...



...wordt dit bevestigd aan de gebruiker. De gebruiker kan nu terugkeren naar de website van de E-Dienstverlener (Belastingdienst).



De E-Dienstverlener (Belastingdienst) haalt het resultaat van het authenticatieverzoek online op, via de Routeerder, direct nadat dit door de Middelenuitgever (bank) is bevestigd aan de gebruiker. Wanneer de gebruiker terugkeert naar de E-Dienstverlener (Belastingdienst), controleert deze de integriteit van het ontvangen transactieresultaat (de authenticatie), slaat dit op en bevestigt de aangifte aan de gebruiker.

Het hierboven beschreven proces is slechts een voorbeeld van een toepassing van DigiD. Voor andere online dienstverlening zal het proces er voor de gebruiker er echter grotendeels hetzelfde uitzien.

6.4 E-Dienstverlener

Een e-dienstverlener (acceptant), die DigiD authenticaties wenst te accepteren, dient zich aan te melden bij een routeerder (acquirer) die DigiD aanbiedt. Na aanmelding (en nadere verificatie en risico-analyse) wordt de e-dienstverlener door de routeerder aangesloten op het systeem van de routeerder. Hiervoor zal de e-dienstverlener een 'plug-in' moeten integreren in zijn website/e-dienstverlening applicatie. Hulpmiddelen en ondersteuning daarbij worden verzorgd als onderdeel van de dienstverlening van de routeerder.

Eenmaal aangesloten, kan de e-dienstverlener DigiD authenticaties van gebruikers accepteren en verwerken. De e-dienstverlener wordt geacht voor elk ingestuurd authenticatieverzoek direct na afhandeling door de gebruiker het transactieresultaat bij zijn routeerder op te halen. Bij een succesvolle transactie is dit de realtime authenticatie.

De e-dienstverlener kan informatie ontvangen op individueel authenticatieniveau en daarnaast gebruik maken van aanvullende dienstverlening van de routeerder.

E-Dienstverleners hebben in principe de mogelijkheid om aansluiting op meerdere routeerders te realiseren. Dit kan interessant zijn om meerdere redenen, onder andere risicospreiding (redundantie) en tariefoptimalisatie.

6.5 Routeerder

Een routeerder (acquirer) die tot DigiD scheme wenst toe te treden en DigiD routeringsproducten wenst te ontwikkelen en aan te bieden, dient zich te registreren bij de scheme eigenaar en een routeerder-licentie te verkrijgen. Hierbij ontvangt de routeerder een uniek DigiD routeerderID dat gebruikt wordt in het DigiD 'netwerk'.

Een routeerder biedt routeerderproducten aan acceptanten. De routeerder geeft zelf invulling aan de routeerderproducten, maar dient hierbij minimaal te voldoen aan alle voorwaarden zoals beschreven in de DigiD scheme documentatie.

De routeerder heeft de mogelijkheid de uitvoering van bepaalde taken te beleggen bij een externe partij (bijvoorbeeld een Acquiring processor[5]).

Afhankelijk van het businessmodel van de DigiD scheme zal een routeerder bilateraal met alle DigiD middelenuitgevers commerciële en operationele bilaterale afspraken moeten maken of zullen dergelijke afspraken centraal bij de scheme zijn vastgelegd.

6.6 Middelenuitgever

Een middelenuitgever die tot de DigiD scheme wenst toe te treden en authenticatie-producten wenst te ontwikkelen en aan te bieden, dient zich te registreren bij de scheme-eigenaar en een middelenuitgever-licentie te verkrijgen. Hierbij ontvangt de middelen-uitgever een uniek middelenuitgeverID dat gebruikt wordt in het DigiD 'systeem'.

Een middelenuitgever biedt producten aan klanten, in dit geval authenticatiemiddelen. De middelenuitgever geeft zelf invulling aan deze producten, maar dient hierbij minimaal te voldoen aan alle voorwaarden zoals beschreven in de DigiD scheme documentatie.

Afhankelijk van het businessmodel van de DigiD scheme zal een middelenuitgever bilateraal met alle DigiD routeerders commerciële en operationele bilaterale afspraken moeten maken of zullen dergelijke afspraken centraal bij de scheme zijn vastgelegd.

6.7 Schemeperspectief

De DigiD scheme beheert de *'rules & regulations'*, *'brand & licenses'* en specificaties.

De DigiD scheme certificeert deelnemende middelenuitgevers en routeerders en kent deze gebruikslicenties met unieke DigiD actor IDs toe. Hiermee zijn middelenuitgevers en routeerders herkenbaar in het DigiD netwerk.

Afhankelijk van het businessmodel kan de DigiD scheme centrale commerciële afspraken vastleggen en eventueel de onderlinge verrekeningen verzorgen.

De DigiD scheme werkt als bemiddelaar in de disputen tussen middelenuitgevers en routeerders indien deze zich voordoen en de betrokken partijen onderling geen overeenstemming konden bereiken.

5 Zie voor uitleg Acquiring processor de bijlage Terminologie.

6.8 Merkaspecten

De DigiD authenticatiemethode wordt herkenbaar als een merk gericht op de gebruiker. Niet alleen het logo, maar ook de initiatiedialoog van een authenticatieverzoek (via de e-dienstverlener) is gestandaardiseerd. Op deze manier is het starten van een DigiD authenticatie gelijk bij alle e-dienstverleners. De dialoog voor het authenticeren en het bevestigen van de authenticatie is afhankelijk van de methode van de middelenuitgever, maar voor een individuele gebruiker is dit altijd hetzelfde en daarmee een integraal onderdeel van de gebruikersbeleving van DigiD.

Het bestaande DigiD logo kan gewoon gebruikt worden. Wel is een nieuwe governance structuur nodig om merkmisbruik te voorkomen en een minimale kwaliteitsbeleving te borgen.

Aandachtspunten & vervolg

In de voorgaande hoofdstukken is een beeld geschetst van hoe DigiD kan worden verbeterd door als scheme te worden opgezet. In de voorbeelden die we hebben gegeven zijn we omwille van het doel van dit document niet ingegaan op alle aspecten en details. In de verdere uitwerking van DigiD als scheme is het essentieel hier gedegen inzicht in te krijgen. In dit laatste hoofdstuk nemen we een voorschot op enkele aandachtspunten die reeds door de markt over dit onderwerp naar voren zijn gebracht. Tevens geven we aan welke vervolgstappen nodig zijn om DigiD volledig om te vormen tot scheme.

7.1 Aandachtspunten

7.1.1 Pricing model en business case

Om de scheme succesvol te maken moet het voor middelenuitgevers en routeerders aantrekkelijk zijn om deel te nemen. Deze – commerciële – partijen zullen hiertoe in eerste instantie hun eigen business case opstellen. Twee belangrijke factoren die hierin meespelen zijn omvang van de markt (hoeveel transacties/authenticaties worden er per jaar gedaan) en het potentiëel aandeel (welk deel van de markt kan een partij maximaal verwerven).

Deze factoren worden bepaald door keuzes in het scheme, waaronder:

- **Pricing model:** op welke manier kan er in het scheme worden verdiend? Door de marktketen in het scheme en de afhankelijkheid die hiermee tussen partijen ontstaat moeten afspraken worden gemaakt over hoe deze partijen onderling de kosten mogen verrekenen. Het pricing model is daarmee van invloed op de pricing model.
- **Scope:** voor welke toepassingen en door welke afnemers kan DigiD worden gebruikt? De scope bepaalt de potentiële omvang van de markt en is dus ook van grote invloed op de business case.
- **Risico's en liability:** hoe worden risico's en aansprakelijkheid verdeeld tussen de verschillende partijen? Het risico is mede afhankelijk van het type transactie (dat weer wordt bepaald door de scope). Het risico dat een partij draagt wordt meegewogen in de business case.
- **Positie overheid:** treedt de overheid op als één afnemer of opereert iedere instantie voor zich? Dit maakt het verschil tussen één klant en vele honderden potentiële klanten voor een acquirer en is dus van grote invloed op de business case.

7.1.2 Waarborgen mededinging & kwaliteit

Bij het creëren van een open netwerk moet het onbetwistbaar zijn dat marktpartijen kunnen toetreden onder non-discriminatoire voorwaarden. Tegelijkertijd willen dezelfde partijen ook dat de kwaliteit van de dienstverlening in het gehele netwerk eenzelfde minimaal niveau heeft, om hun eigen positie te beschermen. Hierbij speelt mee dat het operationele risico van de dienstverlening wordt bepaald door het geheel van organisatie, platform én authenticatiemiddel. Bij het handhaven van de kwaliteit moeten al deze aspecten worden meegenomen.

7.1.3 Zorgvuldige verweking van gebruikersgegevens (privacy)

In het proces van authenticatie worden gegevens over de gebruiker uitgewisseld tussen verschillende partijen. Het is noodzakelijk dat hier zorgvuldig mee wordt omgegaan, en dat er niet meer gebruikersgegevens worden uitgewisseld dan nodig is. In de uitwerking van het uiteindelijke model dient hier ruim aandacht voor te zijn.

Een ander aandachtspunt is het nummer dat momenteel door DigiD wordt gebruikt voor het herkennen van gebruikers. Bij het herkennen van burgers wordt hiervoor het BSN gebruikt. Het gebruik hiervan kent veel voordelen: het is een unieke code die door alle overheidsinstanties wordt gebruikt (een zogenaamde *common identifier*). Het gebruik van dit nummer is gebonden aan wettelijke beperkingen. Het is kort gezegd alleen aan overheidsinstanties toegestaan om dit nummer te gebruiken (het gebruik moet wettelijk geregeld zijn), commerciële organisaties mogen dit niet (tenzij er een wettelijke grondslag is). Hiervoor moet een oplossing worden gevonden die regelt dat het BSN niet wordt verwerkt tenzij hier een wettelijke grondslag voor is, en dat er voldoende mogelijkheden zijn om dit effectief te controleren.

7.2 Inbreng van marktpartijen

De markt zal een belangrijke rol spelen in het vervullen en verbeteren van de DigiD dienstverlening. Een belangrijke groep in deze markt wordt gevormd door de banken. Hun bijdrage aan de nieuwe vorm van DigiD:

- Ervaring met verschillende rollen in schemes (o.a. PIN, iDEAL, credit cards);
- Efficiënt in het verwerken van transacties. In 2007 werden er ca. 2 miljard PIN transacties en 16 miljoen iDEAL transacties verwerkt.
- Hergebruik van bestaande authenticatiemiddelen voor internetbankieren. Door het hoog-frequente gebruik door burgers dragen deze bij aan het succes.

Uit informele gesprekken met verschillende banken is reeds naar voren gekomen dat er zeker bereidheid is om deel te nemen in een DigiD scheme. Een goede business case is echter wel een belangrijke voorwaarde.

7.3 Vervolgstappen

Om DigiD uit te werken tot een volledig scheme is nog een aantal vervolgstappen nodig. Er kan worden begonnen met een pilot om enkele aspecten van het scheme, bijvoorbeeld het opsplitsen van de centrale organisatie in twee rollen die door verschillende partijen worden ingevuld. Ook zouden enkele technische aspecten kunnen worden onderzocht en uitgewerkt in een pilot fase. Hiermee kan de haalbaarheid op organisatorisch en technisch gebied worden getoetst.

Ten tweede wordt de economische potentie van het scheme onderzocht. Het moet voor een marktpartij aantrekkelijk zijn om als participant (middelenuitgever of routeerder) in het scheme deel te nemen. De totale marktomvang (bijvoorbeeld uitgedrukt in aantal authenticatie-transacties) en de scope van de toepassing (welke afnemers, soort transacties) zijn noodzakelijke inzichten om een goede business case op te baseren.

Wanneer er voldoende potentie is voor het scheme en er is een coalitie van partijen die bereid zijn te starten, kunnen de details van het scheme worden uitgewerkt. Het uitwerken van de afspraken moet gebeuren over alle lagen: business & governance, applicatie en infrastructuur.

Tot slot wordt het scheme 'in bedrijf' genomen. Hiertoe moeten de deelnemende partijen migreren naar de nieuwe infrastructuur. Tevens worden de DigiD dienst, het platform en de organisatie 'unbundled' en opgesplitst in de twee rollen.

Terminologie

N.B. Het gebruik van de termen met de toelichting zoals in onderstaande tabel weergegeven, is beperkt tot dit document.

TERM	TOELICHTING
Acceptant	De partij die bij een Acquirer een contract heeft afgesloten om DigiD authenticaties te kunnen accepteren.
Account	Het account aangehouden bij een Issuer respectievelijk Acquirer welke wordt gebruikt voor verwerking van de Authenticaties.
Acquirer	Een instelling die een DigiD licentieovereenkomst heeft getekend en bij wie Acceptanten een Account aanhouden en een DigiD product afnemen, waarmee Klanten DigiD authenticaties uitvoeren ten behoeve van die Acceptanten.
Acquiring processor	De partij die, in het kader van DigiD, transactie-verwerkende taken geheel of gedeeltelijk van de Acquirer kan overnemen, onder eindverantwoordelijkheid van de Acquirer.
Authenticeren (Klant)	Het vaststellen door de Issuer van de geclaimde identiteit van de Klant.
Common Identifier	Een unieke code of nummer, dat door verschillende partijen gezamenlijk wordt gebruikt om een gebruiker te herkennen.
Issuer	Een instelling die een DigiD licentieovereenkomst heeft getekend en bij wie Klanten een Account aanhouden en een DigiD product afnemen, waarmee Klanten zich kunnen authenticeren bij Acceptanten.

TERM	TOELICHTING
Klant	De partij met een Account bij een Issuer en een authenticatie-product van die Issuer om DigiD authenticaties mee te kunnen doen. Dit kan in principe zowel een particulier (burger/consument) als een bedrijf zijn.
Licentienemer	Een instelling die een issuing respectievelijk acquiring licentie op de DigiD scheme heeft en daarop gebaseerde issuing respectievelijk acquiring producten kan ontwikkelen.
Man-in-the-middle attack	Een aanval die op het internet plaatsvindt, waarbij een crimineel zich positioneert tussen bijv. een klant en een bank. Hierbij onderschept de crimineel alle gegevens van beide partijen, manipuleert deze en stuurt het weer door. Hierbij heeft de klant de indruk dat hij met zijn eigen bank communiceert, terwijl de crimineel de gegevens gebruikt om transacties te doen in de bankieromgeving van de klant.
Phishing	Phishing is een poging om op criminele en frauduleuze wijze gevoelige informatie, zoals wachtwoorden of credit card gegevens, van personen te ontfutselen door zich voor te doen als een betrouwbare entiteit.
Scheme	Het geheel aan spelregels waarbinnen Issuers en Acquirers DigiD diensten kunnen ontwikkelen en vermarkten.
Service Provider (SP)	Een partij die (diverse) methoden ontsluit aan een Acceptant en mogelijk aanvullende dienstverlening op de verwerkte transacties verleent.

Colofon

Een uitgave in opdracht van het
Ministerie van Economische Zaken en
het Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties.

Auteurs
Innopay
Leendert Bottelberghs, Chiel Liezenberg

Ontwerp en opmaak
www.**myriad**design.nl

Papier
Deze uitgave is gedrukt op Olin;
mixed-sources FSC-papier.