Bijlage II: De werking en de stapsgewijze uitrol van de multimiddelenaanpak

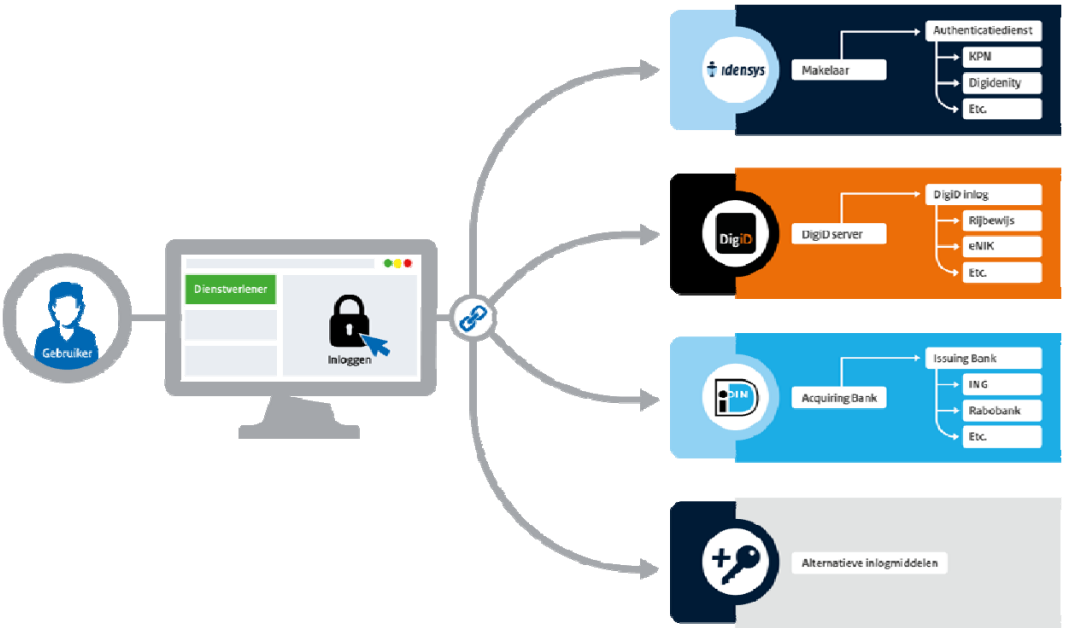
In deze bijlage wordt de werking van de multimiddelenaanpak in het BSN-domein geschetst. Daarna wordt de uitrol van de multimiddelenaanpak beschreven aan de hand van 3 stappen.

De werking van de multimiddelenaanpak

De situatie die het kabinet wil realiseren werkt als volgt. In de toekomst kan iemand die een digitale dienst wil afnemen bij dienstverleners in het BSN-domein zelf kiezen, met welk toegelaten inlogmiddel hij zich identificeert. Zo kan hij één inlogmiddel of een beperkt aantal inlogmiddelen gebruiken voor veilig online zaken doen met meerdere organisaties. In tegenstelling tot nu hoeft het middel niet langer DigiD te zijn, maar dat mag wel.

Als de multimiddelenaanpak in het BSN-domein gerealiseerd is, weet een organisatie niet van te voren met welk inlogmiddel iemand zich meldt. Dit is vergelijkbaar met betalen via internet: de webwinkel weet ook niet van te voren via welke methode en via welke bank een klant zal betalen. Om de organisatie te ontzorgen en om het de gebruiker gemakkelijk te maken zijn er verschillende functies om dit te bewerkstelligen. Net zoals bij internetbetalen kennen de verschillende landschappen een makelaarsfunctie met een scrollmenu waarbinnen je als gebruiker je inlogmiddel kunt kiezen.

Figuur 1: Eindsituatie voor publieke dienstverleners.



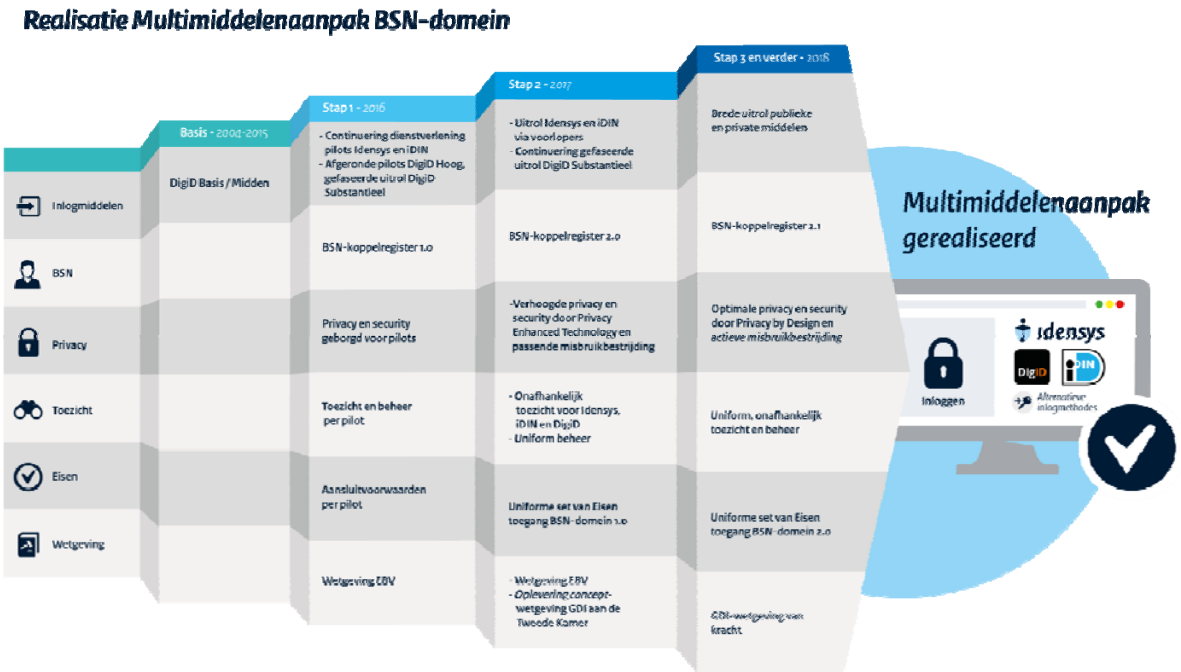
De uitrol van de multimiddelenaanpak: 3 stappen
Het kabinet wil de multimiddelenaanpak geleidelijk invoeren, met oog voor de technische mogelijkheden, de dienstverlenende organisaties en de burgers. Uitgangspunt bij de gefaseerde uitrol van hoogwaardige authenticatiemiddelen is dat organisaties en gebruikers zoveel mogelijk ontzorgd worden. Door goed aan te sluiten bij de uitrolbehoefte van dienstverlenende organisaties is er tijd en ruimte om in een natuurlijk tempo te werken aan het steeds breder beschikbaar komen van hoogwaardige authenticatiemiddelen. Het kabinet streeft daarbij binnen de mogelijkheden tevens naar een zo snel mogelijke realisatie van versterkte beveiliging.

De behoefte aan hoogwaardige authenticatie is een behoefte die publieke en private organisaties met elkaar delen. Voor de gebruiker is veel te winnen bij effectieve samenwerking. Gebruikers die dat willen kunnen in de toekomst bij steeds meer organisaties terecht met hetzelfde inlogmiddel. Als binnen de private sector gekozen wordt voor de private inlogmiddelen die zijn toegelaten in het publieke domein (bijvoorbeeld Idensys of iDIN), kunnen gebruikers die over deze middelen beschikken hiermee ook inloggen bij deze private organisaties. De groep gebruikers die liever zaken doet met de overheid via een publiek uitgegeven middel, kan dat doen door daarvoor bijvoorbeeld DigiD Hoog te gebruiken.

Dat houdt dat het kabinet de realisatie verdeelt in drie stappen, te weten:

- *Stap 1: Continuering huidige dienstverlening*
- *Stap 2: Aansluiten nieuwe organisaties op basis van eerste uniforme toelatingseisen*
- *Stap 3: Structurele uitrol multimiddelenaanpak*

Figuur 2: Stappenplan invoering multimiddelenaanpak



Stap 1: Continuering huidige dienstverlening

Voor de organisaties die als pilotdeelnemer een nieuwe hoogwaardige manier van inloggen uittesten, is het van belang dat zij zo mogelijk niet terug hoeven naar de 'oude situatie' van voor de pilots. Zij hebben de benodigde veranderingen deels al doorgevoerd en kunnen hun collega's helpen om hetzelfde te doen. In deze fase, die start na politieke besluitvorming in de Kamer, wordt de dienstverlening uit de pilotfase, met uitzondering van het publieke middel, gecontinueerd. Dat betekent dat de hoogwaardige authenticatiemiddelen beschikbaar blijven voor gebruikers, onder de huidige pilotcondities. En tegelijkertijd kan het aantal gebruikers nu nog uitgebreid worden naar de limiet die gesteld is voor de pilotsituatie. Mensen die een dienst willen afnemen met een hoogwaardig middel, kunnen daarvoor terecht bij de erkende middelenverstrekkers. De pilotorganisaties helpen hen hierbij.

Kenmerkend voor deze stap is: het aantal gebruikers wordt uitgebreid tot het maximaal aantal gebruikers voor de pilotsituatie. De uitgifte van inlogmiddelen is gebaseerd op de huidige pilotcondities.

Privacy

De opzet van de architectuur van het introductieplateau is geschikt voor het doen van pilots. Een verdere groei in aantal organisaties is niet verenigbaar met de verantwoordelijkheden van BZK op onder meer het gebied van bescherming van privacy. Om aan deze privacyeisen tegemoet te komen wordt privacy-enhancing-technology (PET) ingezet in de volgende stap. Deze technologie wordt voorgeschreven in de uniforme toelatingseisen en zal in de zomer van 2016 beproefd worden middels proof-of-concepts (PoC) tot acceptatieomgeving.

Stap 2: Aansluiten nieuwe organisaties op basis van uniforme toelatingseisen

Voor nieuwe organisaties die aan willen sluiten, biedt stap 2 mogelijkheden. Nieuwe dienstverleners in het BSN-domein geven aan dat zij graag op beperkte schaal willen starten met diensten waarvoor hoogwaardige authenticatie een voorwaarde is. Daarvoor is een aanpassing nodig, omdat stap 1 alleen bedoeld is voor de bestaande groep dienstverleners. Om tegemoet te komen aan de wens van deze organisaties, wordt bezien hoe de overheid nieuwe pilots kan inrichten, als opmaat naar de inwerkingtreding van de wet GDI (eind 2017) en de eIDAS-verordening (september 2018). Op deze wijze kunnen organisaties verder met de verbetering en innovatie van hun digitale dienstverlening.

In deze pilots zouden de uniforme toelatingseisen voor het BSN-domein leidend zijn. Leveranciers van toegangsdiensten die hieraan gaan voldoen, zouden dan hoogwaardige authenticatiediensten kunnen leveren aan nieuwe organisaties in het BSN-domein. Deze 'voorlopers' zijn dan de eerste organisaties in het BSN-domein die onder een eerste versie van de uniforme toelatingseisen bediend worden. Zij kunnen in deze stap gebruik maken van zowel private middelen als van DigiD substantieel.

Het verschil ten opzichte van de eerste fase is dat er extra waarborgen zijn op het gebied van privacy- en informatiebeveiliging. Dit is dan in ieder geval gebeurd door privacy by design in te bouwen bij de publieke voorziening: het BSN-koppelregister. Het BSN-koppelregister (BSNk) kan dan niet meer zien waar de gebruiker naar toe gaat. Daarnaast wordt er passende misbruik- en

fraudebestrijding toegepast. Hiermee worden inhoudelijke bezwaren welke doorgroei van het introductieplateau blokkeerden, gemitigeerd.
Bezien zal worden of middels de aansluitvoorwaarden van het BSNk conformiteit met de Uniforme toelatingseisen kan worden getoetst en toelating tot het publieke domein kan worden geregeld. Deze aansluitvoorwaarden zijn uniform en gelden voor alle partijen die toegang willen hebben tot het BSN-domein. De huidige wet EBV is de juridische basis voor deze stap.

Met de groei van het aantal organisaties, moet ook de groei van nieuwe gebruikers(groepen) worden toegestaan. Deze 'nieuwe' gebruikers moet vanuit gebruikersgemak ook terecht kunnen bij de dienstverleners van het Introductieplateau; doordat de mitigerende maatregel van beperking van dienstverleners voor deze versie behouden blijft, bestaan hiervoor geen bezwaren.

Deze stap is mogelijk in Q3 2017.

Stap 3: Brede uitrol multimiddelenaanpak

In stap 3 kunnen burgers kiezen uit verschillende inlogmiddelen en deze gebruiken bij publieke organisaties. Het idee is dat eind 2017 een natuurlijke overgang plaatsvindt naar een structurele situatie, omdat er dan een verankering van de uniforme toelatingseisen plaatsvindt in de wet GDI. In de loop van 2018 is het mogelijk om structureel uit te rollen.

Eind 2018 is het mogelijk om alle organisaties in het BSN-domein aangesloten te hebben op de tot het BSN-domein toegelaten 'authenticatiediensten'.

In de loop van 2018 is privacy by design bij alle partijen verplicht volledig doorgevoerd, waarmee de privacy en veiligheid van de gebruiker maximaal geborgd is.

Eind 2019 zouden alle dienstverleners in het BSN-domein hun diensten op het passende betrouwbaarheidsniveau via de multimiddelenaanpak ontsloten kunnen hebben.

Ook is het BSN-koppelregister dan alleen nog voor de eerste aanmelding van een middel voor een gebruiker nodig, maar tijdens alle gebruik niet meer. Dit betekent dat het BSNk dan ook in het gebruiksproces geen single-point of failure meer is.

<u>Noodzakelijke Toepassingen</u>

Naast het mogelijk maken van online identificeren op hoog betrouwbaarheidsniveau, worden in dezelfde periode ook andere, noodzakelijke, digitale toepassingen gerealiseerd.
Het gaat onder meer om:

- Digitaal ondertekenen van stukken.
- Iemand machtigen om namens jou zaken te doen (bijvoorbeeld voor minder digivaardigen).
- Machtigen voor onder gezag, curatele of voogdij staande personen en de vertegenwoordiging van rechtspersonen.

Dit zijn functionaliteiten die voortkomen uit wettelijke verplichtingen.

Aanvullende toepassingen

De Impuls eID wil dat het mogelijk wordt voor mensen om naast hun persoonsgegevens meer informatie mee te sturen over henzelf, zoals hun BIG-registratie of BAR-registratie, of een ander gegeven waarbij de basisregistraties mogelijk een rol spelen.

Andere kanalen kunnen worden ingezet bij digitaal inloggen. Vanuit technisch perspectief wordt het inzetgebied uitgebreid door ondersteuning van additionele kanalen naast het webkanaal (A2A/M2M) waarmee de Multi-channel strategie ondersteund zal worden. Als laatste is er ruimte voor innovatie als “mobile” en “apps”.

Invulling

Bovenstaande 3 stappen en de functionele doorontwikkeling vinden plaats binnen de eisen die het ministerie van BZK stelt aan het verlenen van authenticatiedienstverlening binnen het publieke domein en zal daarmee kaders kennen op gebieden als privacy, misbruikbestrijding, betrouwbaarheid en interoperabiliteit.

Publiek

De scope van de publieke activiteiten zijn gekenmerkt door het beleidsuitgangspunt ‘privaat wat kan, publiek wat moet’[1]. Hiertoe bestaat het publieke landschap uit voorzieningen die reeds hun counterpart kennen in het private domein, alsmede ook generieke technische overheidsvoorzieningen.

Publieke inlogmiddelen

DigiD blijft, naast de private alternatieven, bestaan als authenticatiedienst. Hiermee pakt het kabinet zijn verantwoordelijkheid om zorg te dragen dat authenticatie in publieke domein mogelijk blijft. Zo wordt op DigiD Hoog de burger in staat gesteld om te authenticeren zonder dat DigiD weet bij welke organisatie de burger inlogt. Voor gevoelige diensten wordt hiermee voor de burger een basis garantie te geven dat hij zich altijd bij een dienstverlener kan identificeren zonder dat er een andere partij hier kennis van hoeft te hebben. De verantwoordelijkheid van DigiD ligt bij het kabinet, waar onderliggend de RvIG en RDW als de middelenuitgevers voor respectievelijk de eNIK/Paspoort en het eRijbewijs hun eigen verantwoordelijkheden hebben met betrekking tot uitgifte en revocatie.

Aanvullend zal vanuit de overheid ook ondersteuning voor digitaal minder vaardigen blijven worden gefaciliteerd door de continuering van DigiD Machtigen. Waar toegewerkt wordt naar convergentie van de initiatieven in het publieke domein moet deze meer gezien worden als GDI-Bouwblok daar deze ook interoperabel is met de private authenticatiediensten in het publieke domein.

Technische overheidvoorzieningen

Als ondersteuning voor de authenticatiedienstverlening in het publieke domein zullen er technische overheidvoorzieningen komen welke mogelijk maken dat maatregelen voor privacy, informatiebeveiliging en misbruikbestrijding worden afgedwongen. Dit is het BSN-koppelregister.

[1] Brief van 19 december 2013, TK 26 643 nr. 299 Invoering eID stelsel en DigiD kaart

Privaat

Zoals aangegeven is het voor de private markt interessant om dienstverlening in het publieke domein te mogen vervullen. Voor de markt ontstaat hiermee een grotere afzetmarkt en toegang tot de technische overheidsvoorzieningen.

Voor de gebruiker betekent dit gebruiksgemak en verbeterde beveiliging, omdat hetzelfde inlogmiddel dan overal gebruikt kan worden; bij de overheid, webwinkels, verzekeraars etcetera. Voor de overheid wordt hiermee de multimiddelenaanpak gerealiseerd en een impuls gegeven aan innovatie. Binnen de private partijen zijn in ieder geval iDIN (vanuit de banken), en andere private partijen die onder Idensys vallen (het stelsel elektronische toegangsdiensten), voorlopers in het bieden van deze diensten.