



Whitepaper
Zo verbeter je de online
dienstverlening in de publieke
sector met nieuwe eID-middelen

Inhoudsopgave

Inleiding	1
Gemiste kansen	2
De 6 manieren om je online- dienstverlening te verbeteren met nieuwe eID-middelen	3
1. Burgers zelf de keuzevrijheid te geven over hun eigen ID-middelen	3
2. Alleen relevante ID-gegevens uitvragen	3
3. De kans op datalekken reduceren	4
4. Alles beheren vanuit één omgeving	4
5. Decentrale infrastructuur	4
6. Naast DigiD ook andere middelen kunnen aanbieden	4
Hoe helpt SIDN?	5

[Klik op een van de hoofdstukken om direct naar de bijbehorende pagina te gaan.](#)



Inleiding

Digitale identiteiten worden steeds belangrijker in de moderne maatschappij, zeker in de publieke sector. Elke burger heeft er geregeld mee te maken. Denk bijvoorbeeld aan het inloggen met DigiD om de jaarlijkse belastingaangifte in te vullen. Of om berichten van je pensioenfonds, het UWV of je zorgverzekeraar te bekijken.

Burgers meer regie geven over het beheren, organiseren en delen van hun persoonlijke gegevens is een van de speerpunten van het eID-beleid vanuit de overheid. In het kader van het programma Regie op Gegevens heeft de publieke sector veel kennis verzameld over de juridische kaders en noodzakelijke spelregels rondom de regie over gegevens. Ook vanuit Europa leeft de wens om te komen tot digitale eID-wallets die in de hele EU te gebruiken zijn.

De overheid kan ook een actieve rol spelen in het uitgeven van identiteitsgegevens, gezien zij bronhouder is van veel gegevens. Ook kan ze met een modern eID-middel als IRMA (in principe al een praktische uitwerking van de wallet-app waar de EU naartoe wil) de brug slaan tussen het publieke en private domein, waardoor het beheren van digitale identiteiten voor de eindgebruikers ook veel gemakkelijker wordt.

Hoewel de digitale identiteit dus belangrijk is en je met de nieuwste generatie eID-middelen steeds meer kunt, halen organisaties binnen de publieke sector nog lang niet altijd het optimale rendement uit eID-middelen. Lees verder om erachter te komen hoe je hier als organisatie in het publieke domein verandering in brengt door met de nieuwste generatie eID-middelen makkelijke, veilige en publieksvriendelijke online-diensten aan te bieden.

Gemiste kansen

Veel organisaties in de publieke sector worstelen nog met het in de praktijk brengen van de zogenoemde Self-Sovereign Identity (SSI). Met dit begrip bedoelen we dat de burger zelf de regie voert over het gebruiken van de middelen die deel uitmaken van zijn eID-wallet. SSI maakt de decentralisatie van gegevens mogelijk en biedt zo innovatiekansen.

De eigenaar van de persoonlijke gegevens-kenmerken kan meerdere waarheden over zichzelf ontvangen en gebruiken in betere, betrouwbare authenticatieprocessen. Als je het goed uitvoert, is SSI privacy by design en maakt de oplossing de regie over gegevens mogelijk.

Maar veel publieke instanties lopen op dit vlak nog achter de muziek aan. We zien bijvoorbeeld nog vaak dat burgers of klanten verschillende apps of accounts nodig hebben om zich te kunnen identificeren. De ene keer moet je inloggen met je DigiD, terwijl je voor een andere dienst weer een alternatieve combinatie van een gebruikersnaam en wachtwoord moet gebruiken.

Ook herkenbaar: iemand belt om antwoord te krijgen op een belangrijke vraag, maar moet elke keer opnieuw een waslijst aan vragen beantwoorden om zichzelf te identificeren. Dit is niet alleen omslachtig voor de gebruiker, maar zadelt de beheerder op met extra beheerposten en -kosten.

Een ander veelvoorkomend probleem is dat publieke organisaties complete profielinfo hebben die helemaal niet nodig is voor het uitvoeren of faciliteren van een bepaalde dienst. Dit vertraagt niet alleen de klantreis, maar vergroot ook de veiligheidsrisico's.

Een van de hoofdoorzaken voor het **recente GGD-lek** was dat te veel medewerkers inzage hadden in complete profielen van mensen. Wordt een profiel of dienst gehackt? Dan heeft de dief direct toegang tot de volledige profielinformatie van het slachtoffer. Het beveiligen van overbodige data kost publieke instellingen handenvol tijd en geld.

Nederland is er de afgelopen jaren niet in geslaagd om tot een nationale digitale identiteit te komen. Natuurlijk, we hebben het op zich succesvolle DigiD. Maar die ID-tool werkt alleen binnen het overheidsdomein, is eenzijdig gericht op de (semi)publieke sector en aan modernisering toe. Ontwikkelingen op gebied van de Wet Digitale Overheid (WDO) sturen bovendien richting oplossingen die volledig open source zijn, terwijl ook de EU actief streeft naar het gebruik van Europabreed bruikbare eID-wallets.

Veel organisaties in de publieke sector worstelen nog met het in de praktijk brengen van de zogenoemde Self-Sovereign Identity (SSI).



De 6 manieren om je online- dienstverlening te verbeteren met nieuwe eID-middelen

Gelukkig schept de nieuwste generatie eID-middelen volop kansen om de SSI-belofte waar te maken. Wij tonen je hoe.

1. Burgers zelf de keuzevrijheid te geven over hun eigen ID-middelen

De nieuwste eID-middelen geven elk individu de controle over zijn of haar persoonlijke informatie. Dit zorgt voor een stuk gebruiksgemak. SSI gaat hand in hand met zogenoemde 'identity wallets'. Dit zijn apps waar de gebruiker meerdere kenmerken, formulieren en/of digitale documenten in kan opslaan. Hij of zij kan de juiste informatie bovendien snel, eenvoudig en veilig vrijgeven als een instantie ernaar vraagt. Daarmee heeft de burger zelf de regie.

Het voordeel van dit stukje eigen regie is dat er geen derde partij is die continu over de schouder van de gebruiker meekijkt (wat bij DigiD bijvoorbeeld wel het geval is) en inzicht heeft in het complete online-profiel van een burger. Dat minimaliseert ook de risico's binnen de digitale informatieketen.

2. Alleen relevante ID-gegevens uitvragen

Alleen relevante ID-gegevens uitvragen is ook een manier om eID-diensten te verbeteren. Het komt nu nog veel voor dat burgers verplicht zijn om een compleet profiel aan te maken, terwijl je als uitvoerende instantie eigenlijk alleen een postcode of geboortedatum hoeft te weten. Denk bijvoorbeeld aan anoniem stemmen.

Alleen tonen wat nodig is maakt het leven van beide partijen makkelijker. De burger deelt alleen de informatie die nodig is voor een proces of aanvraag, terwijl jij als publieke dienstverlener alleen te zien krijgt wat je nodig hebt. Het resultaat? Snellere en gebruikersvriendelijke klantreizen en een kleinere kans op hacks of het lekken van volledige gegevensprofielen.

3. De kans op datalekken reduceren

Door het systeem de identiteiten te laten verifiëren in plaats van dit te doen door individuele medewerkers, verklein je de kans op datalekken. Neem het voorbeeld van iemand die een COVID-vaccinatieafpraak wil maken. De eID-applicatie verwerkt de BSN-gegevens van die persoon automatisch.

Vervolgens geeft ze alleen aan de callcenter-medewerker door dat de persoon die inbelt zichzelf geïdentificeerd heeft met een BSN-nummer. De medewerker hoeft het BSN-nummer dus niet uit te vragen of na te gaan. Het systeem weet al genoeg. Zo voorkom je ook situaties als het datalek bij de GGD, dat eerder dit jaar groot nieuws was op internet en veel krantenkolommen haalde.

Zo voorkom je ook situaties als het datalek bij de GGD, dat eerder dit jaar groot nieuws was op internet en veel krantenkolommen haalde.

4. Alles beheren vanuit één omgeving

Een goede SSI-oplossing biedt overheden en gebruikers één centrale omgeving waarin ze alle losse profielgegevens kunnen beheren en oproepen. Bovendien is het mogelijk om naar behoefte losse ID-kenmerken uit te vragen. Je past dus probleemloos hetzelfde eID-middel toe voor diverse diensten met verschillende veiligheids- en betrouwbaarheidsniveaus. Hierdoor kun je met hetzelfde inlogmiddel meerdere diensten probleemloos ontsluiten.

5. Decentrale infrastructuur

Maak gebruik van een decentrale infrastructuur. Dit betekent dat er geen centrale partij is die persoonsgegevens beheert en deelt uit naam van een gebruiker. Dat doen gebruikers namelijk zelf. Het profileren van eindgebruikers wordt hierdoor een stuk lastiger. Er is geen centraal zicht op waar gebruikers inloggen en welke gegevens met wie gedeeld worden.

6. Naast DigiD ook andere middelen kunnen aanbieden

In de publieke sector wordt nu met name DigiD als inlogmiddel gebruikt. Door ook andere middelen toe te passen, behoudt de consument zelf de keuze en bepaalt hij of zij op welke manier wordt ingelogd.

Hoe helpt SIDN?

SIDN, de partij achter .nl, borgt de betrouwbaarheid van IRMA, een ID-oplossing die uitermate geschikt is voor diverse publieke diensten. Met IRMA profiteer je onder meer van de volgende diensten en voordelen:

- Gebruikers krijgen de volledige regie over hun eigen gegevens en privacy. De ID-informatie staat en blijft op hun telefoon en wordt niet beheerd door derde partijen.
- Je controleert eenvoudig een specifiek identiteitskenmerk van een gebruiker, bijvoorbeeld of iemand 18 jaar of ouder is. Het voordeel: je verwerkt als publieke organisatie geen onnodige persoonsgegevens, zoals een geboortedatum of BSN-nummer.
- Belt iemand met IRMA? Dan heeft die persoon zich al geïdentificeerd, waardoor jij geen extra controlevragen meer hoeft te stellen.
- Gebruikers kunnen al hun ID-informatie beheren en aanroepen vanuit één centrale omgeving.
- IRMA is beveiligd met de juiste cryptografische protocollen en ISO-gecertificeerd. De oplossing beantwoordt aan het principe van 'privacy by design' en wordt geregeld op veiligheid getoetst. Hiermee voldoe je als overheidsinstantie makkelijk aan alle Nederlandse regels en wetten op het gebied van privacy- en databescherming. Omdat IRMA open source is, kan bovendien iedereen de broncode bekijken.
- De plannen van de EU voor het creëren van een Europese eID-wallet zijn volledig in lijn met het IRMA-gedachtegoed.

- Inloggen bij de Nederlandse overheid kan, als de WDO van kracht wordt, alleen met inlogmiddelen die open source zijn. Vooralsnog voldoet alleen IRMA aan die eis.
- IRMA is het enige eID-middel dat in Nederland zowel publiek als privaat wordt gebruikt.

Je IRMA-server, het onderhoud en de ondersteuning: SIDN regelt het voor je en ontzorgt jou zo op alle gebieden. SIDN is bovendien onderdeel van een rijk ecosysteem dat diverse uitgevers en aanbieders herbergt. SIDN Business levert ook support voor publieke dienstverleners en verzorgt de implementatie van IRMA.

Meer informatie

Wil je ook profiteren van de kracht en het gemak van de nieuwe generatie eID-middelen? En ben je benieuwd naar wat IRMA jou te bieden heeft? Neem dan gerust vrijblijvend contact met ons op voor meer informatie.

Meer weten? Neem contact op met:

Alex van Wijhe (SIDN)
alex.vanwijhe@sidn.nl
+31 (0)6 824 339 92

