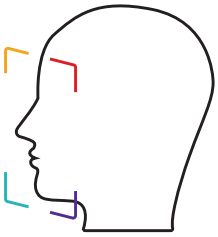
wegingskader digitale identiteit

waag technology & society

Kun je online kenbaar maken wie je bent en wat je wilt? Dat begint met een goede oplossing voor digitale identiteit. Maar welke? Hoe onderzoek je dat? Wat is belangrijk? Welke vragen stel je daarover? Welke technologie gebruiken we daarvoor? Staan publieke waarden op het spel of kunnen die juist versterkt worden? Het wegingskader biedt een kader voor een gesprek tussen burgers, beleidsmakers, bestuurders, experts en ontwikkelaars.



Nieuwe oplossingen voor digitale identiteit

balans tussen gemak, zorgplicht en autonomie

Diensten moeten toegankelijk en begrijpelijk zijn. Maar technologie is ingewikkeld en autonomie vereist juist begrip en handelingsperspectief. Dit spanningsveld stelt hoge eisen, vooral aan ontwerpers van architectuur en interfaces.

dataminimalisatie door attributen

Dataminimalisatie is door de AVG verplicht middels het concept 'Attribute Based Credentials'. Per context en transactie wordt alleen gerichte en gevalideerde informatie gevraagd. Die data is (door de burger) eenvoudig tussen contexten te delen.

decentraliseren van risico en verantwoordelijkheid

Spreid verantwoordelijkheid en risico: in beheerstructuur, architectuur en dataopslag. De burger heeft zoveel mogelijk zelf juridische én technische controle.

voorkomen van surveillance

Geen van de betrokken partijen kan ongewenst het gebruik van de andere partijen in het systeem in kaart brengen. In de architectuur is geen tussenpersoon zoals makelaar of broker nodig voor een transactie.

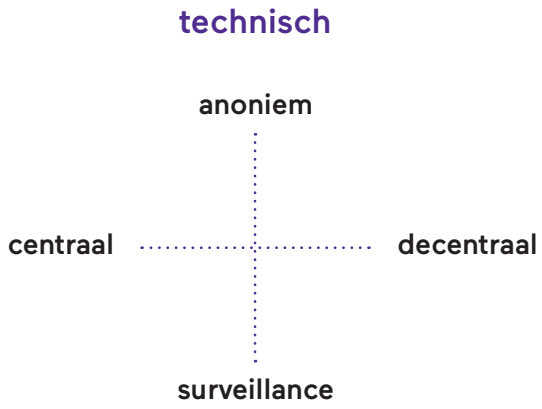
niet wachten op de markt maar regie nemen

In de digitale wereld vervagen de scheidslijnen tussen private, publieke en overheidscontexten nog sneller. Dat vereist nieuwe manieren voor beleidsontwikkeling en -implementatie. Meer spelers, diversere use-cases, en het infrastructurele maatschappelijke belang vragen om een andere rol van de overheid.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

VNG Vereniging van Nederlandse Gemeenten

decode



1 van transparantie naar dialoog

Is de applicatie open of is het een *black box*? Kun je vragen stellen, bellen of langsgaan? Is de aanbieder en het verdienmodel transparant?

Kortom: is een gesprek zinvol en gelijkwaardig? Kun je in beroep?

gesloten — *open*

2 vergroot het begrip

Is authenticatie verborgen en ongemerkt ('magische interactie' of gezichtsherkenning)? Of worden via gebruikersinteractie en communicatie rechten en transactie verduidelijkt? Wordt controle expliciet gemaakt en technologisch burgerschap gefaciliteerd?

afhankelijk — *autonoom*

maatschappelijk

3 spreid verantwoordelijkheid en risico

Central point of failure of resilience by design? Zijn er meerdere aanbieders, met een federatieve opzet? Is de gebruiker een essentiële stap in verstrekking?

Is de verstrekking gescheiden van het gebruik van gegevens? Wordt data gecentraliseerd of blijft het bij de bron?

centraal — *decentraal*

4 niet traceerbaar voor derden

Wordt elke activiteit gevolgd of traceer je *alleen* waar zorgplicht, fraudebestrijding of dienstverlening dit vereisen? Gebruik je daarvoor *pseudonieme attributen*? Is het altijd mogelijk een niet identificerend attribuut te delen? Kunnen er beperkingen gesteld worden aan het hergebruik (zoals bij BSN)?

surveillance — *anoniem*

technisch

5 regie en democratische controle

Digitale Identiteit is te beschouwen als een nutsvoorziening: dat vereist borging in zowel representatieve als maatschappelijke democratie.

Om belang en impact van infrastructuur te begrijpen hebben burgers een kader nodig waarmee zij op het ontwerp en werking kunnen reflecteren.