Identiteit transparant en decentraal

06-05-2020

Author: Tom Demeyer

service kunnen gaan aanbieden, en naar voorwaarden publiek maakt, gaat het behoorlijk mis.

Online identificeren

Om je online te identificeren was er met DigiD in het overheidsdomein al veel mogelijk. Deze vorm van digitale identiteit werd geïntroduceerd in 2003 als 'Burgerpin'. Maar breder bestaat er op dit moment, na 25 jaar internet, nog steeds geen alternatief dat echt betrouwbaar, veilig en privacy-vriendelijk is. De overheid wil nu de mogelijkheid bieden voor private partijen om hun diensten en middelen voor burgers beschikbaar te maken waarbij, indien wettelijk toegestaan, het Burgerservicenummer (BSN) kan worden gebruikt. Deze koppeling met het BSN, en daarmee ook met een aantal basisregistraties van de overheid, kan de kwaliteit van de identificatie en authenticatie aanzienlijk verhogen. Daarnaast is dit nodig om te kunnen voldoen aan Europese regelgeving. Een goed startpunt, zou je kunnen betogen.

Het toetsingskader

Daar waar private aanbieders diensten of middelen willen leveren, zullen ze worden getoetst voor ze worden toegelaten tot het proces. Het zogeheten 'toetsingskader', de regels waaraan een aanbieder moet voldoen, is nu ter consultatie aangeboden door het ministerie van Binnenlandse Zaken. Dit toetsingskader baart ons grote zorgen. Het beschermt de burger niet voldoende tegen ondoorzichtige businessmodellen noch tegen datacentralisatie en zet daarmee de digitale soevereiniteit van alle Nederlanders op het spel.

Vertrouwen door transparantie

digitaal gefaciliteerd, ook belangrijke levensmijlpalen waar in emotionele context administratieve processen moeten worden doorlopen (huwelijken, scheidingen, overlijden etc.). Vertrouwen in een digitale oplossing voor dit soort momenten is de sleutel en wordt dus alleen maar belangrijker. Zo'n fundamentele dienst en infrastructuur dient volledig transparant geëxploiteerd te worden. Hier zijn gedeelde of onduidelijke belangen van de aanbieder absoluut niet op hun plaats.

Daarnaast dient de broncode van de geleverde oplossingen open-source te zijn, zodat verbeteringen aan veiligheid, functionaliteit en gebruiksgemak niet afhankelijk worden van een enkele dominante partij. Iedereen moet dit kunnen controleren en waar nodig aan bij kunnen dragen. In het licht van het fundamentele karakter van deze toepassingen voor de samenleving is deze aanvullende eis onontkoombaar.

Centrale opslag is onnodig

Het gebruik door aanbieders van *centrale opslag* van persoonsgegevens aan de éne kant en gebruiksgegevens aan de andere kant wordt in het toetsingskader **niet** uitgesloten; dit is uiterst problematisch. Centrale opslag levert per definitie meer en grotere risico's op het gebied van beschikbaarheid, aanvallen en misbruik, en is **niet** nodig voor een goed functionerend en veilig middel. Dit bewijzen onder meer IRMA en Sovrin.

Dataminimalisatie

Daarnaast is een centrale data-architectuur niet in lijn met de AVG-eisen ten opzichte van dataminimalisatie. Deze eisen stellen dat dataminimalisatie waar mogelijk zal worden toegepast. De persoons- en

drankwinkel, etc.) een mannetje over de schouder mee zou kijken en aantekeningen zou maken over de tijd, plaats en gebruikte gegevens, dan zouden we dit lacherig afdoen als een idiote fantasie. Waarom wordt dit in het digitale domein als acceptabel ervaren? Als iets technisch haalbaar is, betekent dat zeker niet dat we dit ook moeten doen, en sowieso niet dat er juridische grond is.

'Privacy by design'

Een belangrijk deel van de toelichting van het ministerie gaat in op situaties die alleen voorkomen bij een centraal georganiseerd systeem. Bij een decentraal georganiseerd middel is fraude alleen mogelijk met het fysieke middel, het niveau van de gebruiker zelf. Dit beperkt zich dus tot één enkel middel per keer. Het loont zich derhalve nooit voor grotere, georganiseerde aanvallers of staten. Veiligheid en privacy zijn dan 'ingebouwd' in de architectuur. Dat is precies wat de AVG met 'privacy by design' beoogt. Zo realiseer je de verplichte scheiding van gegevens van gebruikers en gebruik. Je hoeft bij decentrale dataopslag geen extra regels te stellen aan het personeel dat toegang heeft tot de gegevens. Dit gebeurt automatisch. Er is immers geen sprake van een centrale database (anders dan bij de gebruiker zelf).

Het gebruik van gegevens voor commerciële toepassingen wordt door de Wdo uitgesloten. Maar het concept besluit is veel minder stellig in het vasthouden aan de specifieke doelbinding. Daar waar opslag van gegevens nodig geacht wordt voor het specifieke doel van 'herstelvermogen' is een aanvullende eis noodzakelijk dat de daarvoor benodigde gegevens versleuteld zijn opgeslagen en **uitsluitend** door de eindgebruiker kunnen worden ontsleuteld en gebruikt. Ook is het volledig onduidelijk hoe toezicht en handhaving wordt georganiseerd,

De Wet digitale overheid is een goede stap in de richting van een veilig en democratische digitale toekomst. Maar op het gebied van de bescherming van onze digitale identiteit worden een aantal kernvoorwaarden gemist qua transparantie en dataopslag. Voorwaarden die cruciaal zijn in het uitvoeren van de kerntaak van de overheid: het beschermen en waarborgen van de nationale en individuele soevereiniteit van alle Nederlanders.

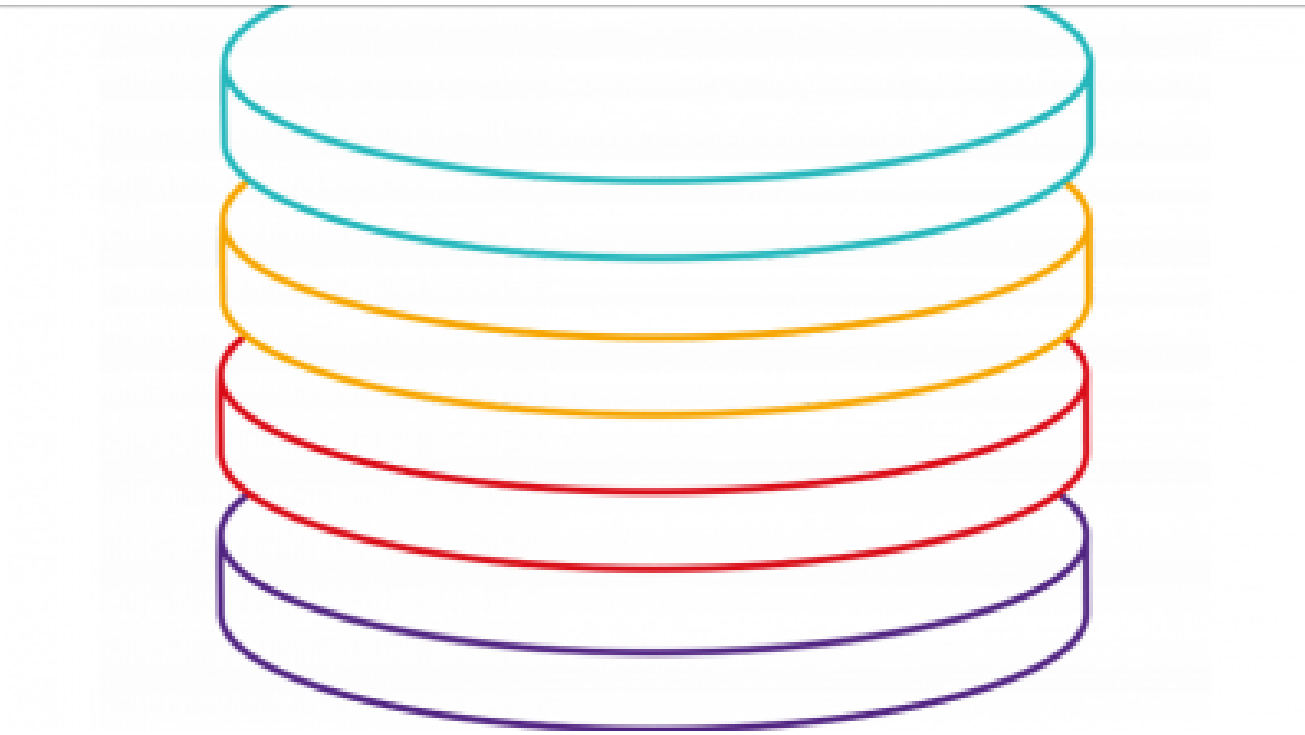
Tags

public domain

Over de auteur

Tom Demeyer

Tom Demeyer is hoofd technologie bij Waag.



we code future internet lab 30-03-2020

Public Stack: het alternatieve internet

Het internet is stuk, maar er zijn inmiddels veel alternatieven beschikbaar. De verzameling van deze open, eerlijke en veilige alternatieven noemen...
project

Postadres
Sint Antoniesbreestraat 69
1011 HB Amsterdam

Schrijf je in voor onze nieuwsbrief

abonneer >