Gemeente Amsterdam

Bezoekadres
Amstel 1
1011 PN Amsterdam

Postbus 202
1000 AE Amsterdam
Telefoon 14 020
Amsterdam.nl

Retouradres: Postbus 202, 1000 AE Amsterdam

Datum	12 mei 2020
Ons kenmerk	
Uw kenmerk	
Behandeld door	Mark Fonds – Mark.Fonds@amsterdam.nl
Kopie aan	
Bijlage(n)	
Onderwerp	Reactie Internetconsultatie Besluit identificatiemiddelen voor burgers Wet Digitale Overheid

Geachte heer Knops,

Het Ministerie van Binnenlandse Zaken heeft een internetconsultatie uitgezet ten behoeve van het besluit rondom identificatiemiddelen voor burgers in het kader van de Wet Digitale Overheid. Namens de gemeente Amsterdam en de gemeente Nijmegen, doen wij u hierbij onze reactie toekomen.

Allereerst willen we onze dank uitspreken voor de voortvarendheid waarmee de regelingen en besluiten in het kader van de Wet Digitale Overheid worden vormgegeven. De maatschappelijke behoefte aan veilige digitale identificatie- en authenticatiemiddelen is groot. De overheid heeft de taak om de digitale rechten van onze inwoners te beschermen waaronder het recht op privacy en zeggenschap over hun eigen data. Meerdere gemeenten hebben afgelopen periode gezamenlijk positieve ervaring opgedaan met een decentraal alternatief voor authenticatie, waarbij de burger regie heeft op zijn eigen gegevens. Dit is momenteel niet mogelijk doordat de huidige digitale identiteit, DigiD, gebruik maakt van alleen het BSN, waarvan het gebruik wettelijk is beperkt. DigiD is gebouwd op het gebruik van BSN, waardoor gemeenten verplicht zijn onnodig achterliggende persoonsgegevens te raadplegen. We zien uit naar authenticatiemiddelen die dit overbodig maken.

Aangezien we als gemeentelijke overheid verplicht zijn alle toegestane authenticatie middelen te accepteren, zowel publieke als private, brengen wij graag onderstaande technische en ethische aandachtspunten onder uw aandacht ten behoeve van de nadere uitwerking van het toelatingsmechanisme voor private inlogmiddelen onder de Wet Digitale Overheid.

Samenvattend:

1. Transparantie van het systeem (open source, inclusief uitlegbaar) is een vereiste.
2. Kies voor een decentrale opslag - gebruik de devices van inwoners als dragers van de ondertekende afschriften uit registers (zoals het paspoort een drager is van persoonsgegevens).
3. Voorkom en verbied ongewenste surveillance en andere 'function creep'.
4. Expliciteer bewaartermijnen en stel eisen aan dataminimalisatie.
5. Expliciteer dat het systeem de eindgebruiker in staat moet stellen om op een gebruiksvriendelijke transparante manier keuzes te maken.
6. Stel toegankelijkheidseisen op (minimaal de toegankelijkheid standaarden van de overheid), inclusief gebruikerstests op basis van gebruikerscentrale ontwerpprincipes.
7. Maak duidelijk wat met 'herstelvermogen' bedoeld wordt en zorg dat alleen de eindgebruiker zijn herstelde gegevens kan ontsleutelen.
8. Organiseer fraudebestrijding niet centralistisch (maar bij de eindgebruiker).
9. Draag zorg voor het risico dat fraudebestrijding niet als excuus gebruikt kan worden om eindgebruikers systematisch te surveilleren.
10. Werk beveiligingsmaatregelen verder uit en gebruik een gespecialiseerde partij voor toetsing hiervan. Toets jaarlijks in plaats van een driejaarlijkse audit.
11. Betrek de uitkomsten en leerpunten van het landelijk projectteam digitale identiteit in de totstandkoming van het kader.

Vertrouwen en transparantie

Identiteitsdiensten zijn onderdeel van een basisvoorziening en de infrastructuur daarvoor dient volledig transparant geëxploiteerd te worden. Gedeelde of onduidelijke belangen van aanbieders van digitale identificatiemiddelen staan haaks op zaken als transparantie en privacy by design. We zien graag een duidelijke waarborg van die, voor het vertrouwen noodzakelijke transparantie. Vertrouwen is niet gebaseerd op wie je 'moet' vertrouwen, maar *hoe* je elkaar kunt vertrouwen. Het lijkt ons daarom een logische eis dat de broncode open source en openbaar is.

Veiligheid en systeemprincipes

Om innovatie op technologisch gebied te stimuleren, wordt voorgesteld om geen beperking of voorkeuren te geven voor wat betreft de technologische inrichting van een identiteitsmiddel. We denken dat daarmee te makkelijk voorbij wordt gegaan aan bekende kwetsbaarheden in systeemarchitectuur. Het stellen van voorwaarden aan architectuurkeuzes en systeemprincipes sluit innovatieve technologie niet uit.

Het is algemeen bekend dat centralistische systemen waarin persoonsgegevens en authenticatiepogingen via centrale plekken gerouteerd en opgeslagen worden, onnodig kwetsbaar en doelwit van cybercriminaliteit zijn. Opslag bij één aanbieder maakt het systeem kwetsbaar voor cybercriminaliteit. Decentrale systemen zijn daarin minder kwetsbaar. We zien graag dit systeemprincipe in het kader opgenomen.

Function creep

De opslag van authenticatiegegevens en van gegevens over gebruik van het identificatiemiddel bij aanvrager, heeft het risico van 'function creep'. Dit knelt met het doelbindingsprincipe in de Algemene Verordening Gegevensbescherming (AVG).

Opslag van authenticatie- en gebruikersgegevens bij aanvragers kan leiden tot controles door een aanvrager in de publieke sector en ook dat aanvragers in de private sector analyses uitvoeren, al dan niet op basis van geanonimiseerde data. Het gevolg kan zijn dat de opgeslagen persoonsgegevens aangewend worden voor andere doeleinden dan waarvoor deze oorspronkelijk waren bedoeld. De eisen in artikel 2.29 van het kader bieden hier op dit moment onvoldoende waarborg tegen. Dit hangt ook samen met de genoemde onderwerpen in artikel 2.20 lid 1 onder c en h (traceerbaarheid of herstelvermogen, het herkennen van misbruik of fraude) van de in het kader aangekondigde ministeriële regeling, die de mogelijkheid bieden tot een (te) ruime interpretatie van het begrip 'authenticatiediensten'.

Dataminimalisatie
Het is onduidelijk welke eisen aan de opslag van persoons-en gebruiksgegevens door publieke of private aanvragers worden gesteld. Genoemd is weliswaar in artikel 2.2. lid 1 sub f van het kader dat aanvrager gegevens over een gebruiker van een middel verwerkt op een wijze die is afgescheiden van gegevens over het gebruik van dat middel door die gebruiker. Deze passage is echter niet aangevuld met concrete eisen waaraan aanvrager moet voldoen. Zo worden er bijvoorbeeld geen eisen gesteld met betrekking tot onderwerpen als dataminimalisatie, versleuteling en er ontbreken bewaartermijnen (privacy by design). Dit lijkt ons op gespannen voet staan met de AVG. Deze zaken moeten geëxpliciteerd worden. Decentrale middelen tonen aan dat het mogelijk is om in een digitale identiteit te voorzien waarbij de aanbieder van de app de persoonsgegevens van de gebruiker niet verwerkt. Ook de verwerking van gebruiksgegevens kan worden geminimaliseerd of voorkomen.

Regie op gegevens
De mogelijkheid voor de eindgebruikers om regie te voeren op de eigen gegevens wordt niet uitgewerkt. Regie op gegevens betekent dat mensen inzicht hebben in welke gegevens de overheid van hen heeft, maar ook dat mensen kunnen kiezen welke van hun persoonsgegevens ze tonen en delen. Er zijn transacties waarbij de eigenaar van de persoonsgegevens bepaalde gegevens rechtmatig moet geven, maar daar waar er keuzemogelijkheid is, moet een systeem van identiteitsmanagement de eigenaar in staat stellen die keuzes actief te maken. We zien dat aspect graag als onderdeel van het kader.

Inclusiviteit en gebruiksgemak
Als gemeenten zorgen we voor maximale inclusiviteit voor onze inwoners. We zorgen dat minder digivaardigen niet buiten de boot vallen. Kwetsbare groepen zijn vaak de dupe van slecht ontworpen systemen. Gebruikersgemak is integraal onderdeel van de nieuwe Wdo. Er wordt echter nergens uitgelegd wat daarmee wordt bedoeld of hoe dat wordt vastgesteld. We stellen voor op dit punt minimaal de toegankelijkheidseisen van de overheid te hanteren (zie: https://www.digitoegankelijk.nl/onderwerpen/themas/eenvoudige-uitleg).

Graag voegen we daaraan toe dat diensten vanuit een gebruikersperspectief zijn ontworpen en via gebruikerstests getoetst zijn, waarmee een adequaat niveau van gebruiksgemak wordt

aangetoond. We willen voorkomen dat er een middel wordt toegelaten dat niet door iedereen te gebruiken is, zoals nu met DigiD Machtigen. Juist de groep die het meest kwetsbaar is en machtigen nodig heeft, kan een functionaliteit als machtigen niet gebruiken. Voor zoiets fundamenteels als een inlogmiddel achten we een mate van toetsing op inclusiviteit noodzakelijk.

Herstelvermogen
Er is wat onduidelijkheid over wat 'herstelvermogen' inhoudt. Dat gaat volgens ons over de situatie waarbij iemand diens digitale identiteit kwijt is en wil herstellen. Het lijkt ons een situatie die overeenkomt met een paspoort kwijt zijn. Men moet dan het oude paspoort ongeldig laten verklaren en een nieuwe aanschaffen. Dat is een heel gedoe en dat is maar goed ook. Daarmee wordt een identiteit waardevol. Ditzelfde geldt volgens ons voor een digitaal identiteitsmiddel. We zien geen aanleiding om een kopie van gegevens en transacties centraal op te slaan voor dat doel. Een digitaal identiteitsmiddel herstellen betekent dan dat je bij iedere bron waar je je persoonsgegevens ondertekend ophaalt, opnieuw moet aankloppen voor een gesigneerd afschrift. Daar waar herstelvermogen zou leiden tot versleutelde opslag van gegevens, vinden we het belangrijk dat de ontsleuteling exclusief bij de eindgebruiker ligt. We zien dat graag opgenomen in de voorwaarden.

Fraudebestrijding
Veel van wat in het huidige voorstel wordt beschreven om fraudebestrijding te kunnen uitvoeren, gaat alleen op voor een centralistisch systeem. Door een voorkeur uit te spreken voor een decentraal georganiseerd middel is de kans op massale identiteitsdiefstal vele malen kleiner omdat de persoonsgegevens als afschrift alleen op de devices van de eindgebruikers staan. Op die wijze beperkt fraude zich, voor wat betreft het ontfutselen van die gegevens, tot één enkel middel per keer. Aanvallen moeten dan ook zeer gericht worden uitgevoerd, wat de drempel voor cybercriminelen hoger maakt. Door de logging van het gebruik van een digitaal identiteitsmiddel decentraal, bij de gebruiker zelf vast te leggen, heeft de gebruiker maximale regie over de gegevens en kan deze de fraude ook zelf aangeven bij de handhavende instantie.

Fraudebestrijding geen excuus voor surveillance
Fraudebestrijding mag geen reden zijn voor het legitimeren van surveillance. Het is mogelijk om fraudebestrijding uit te voeren via kundige bestaande recherche en de daarvoor geldende rechtsmiddelen. We zien graag dat voor een eerste implementatie van de Wdo en de private middelen die worden toegestaan, ervaring wordt opgedaan met het soort en de mate van fraude, voordat er ingrijpende keuzes worden gemaakt die met zich meebrengen dat derden en/of de overheid onder het mom van fraudebestrijding systematische surveillance kunnen doen.

Beveiliging en controle
Qua beveiliging leunt het voorstel zwaar op de ISO27001 certificering. Zo'n certificering richt zich op een gedocumenteerd Information Security Management System (ISMS) van een organisatie, maar zegt niets over de beveiligingsmaatregelen. Wij missen dat aspect.

Er wordt gesproken over "een verklaring van een geaccrediteerde certificerende instelling wordt overhandigd, waaraan het vermoeden kan worden ontleend dat aan de eisen die voor dat middel

gelden is voldaan". Het "vermoeden" klinkt vrijblijvend, zo'n certificering lijkt ons bedoeld om aan te tonen dat de organisatie daadwerkelijk voldoet.
Het Agentschap Telecom wordt aangemerkt om een toetsing uit te voeren. Gezien de onderwerpen die hierbij worden benoemd, is het de vraag of Agentschap Telecom hiervoor is geëquipeerd. Er is geen enkele relatie met het Telecom-werkveld. Wij stellen voor dat hier specifieke expertise voor wordt ingehuurd. Indien ervoor gekozen wordt om het Agentschap alsnog als toetsingsgremium in te stellen, zien we ook graag dat zij hiervoor voldoende middelen ter beschikking krijgen om deze taak uit te voeren.

We missen de relatie tussen ISO 27001 en de BIO. Overheidsorganisaties moeten voldoen aan de eisen in de BIO. Indien de aanbieder van een identiteitsmiddel de eisen uit de BIO niet meeneemt dan levert dat een probleem op bij alle overheidsorganisaties die dit middel gaan inzetten. Het voldoen aan de eisen uit de BIO, moet aan de aanbieder worden opgelegd.

Er wordt aangegeven dat een driejaarlijkse audit wordt uitgevoerd. Dit is gezien het belang van het identificatiemiddel, geen goede frequentie. Er is minimaal een jaarlijkse audit / Third Party Memorandum (TPM) nodig waarin over opzet, bestaan en werking van beheersmaatregelen wordt gerapporteerd.

Landelijk projectteam Digitale Identiteit
De afgelopen jaren heeft het Ministerie van Binnenlandse Zaken en Koningsrelaties in samenwerking met de VNG, Waag society en meerdere gemeenten waaronder de gemeente Amsterdam en Nijmegen via het landelijk overleg digitale identiteit proeven gedaan en studies verricht om tot kwalitatief hoogwaardige inzichten te komen, juist voor het beslissen over de toelating van private inlogmiddelen. We zien graag dat de waardevolle inzichten en lessen die daar ontstaan zijn in het kader worden verwerkt.

Ter afsluiting

Als gemeenten kijken we uit naar middelen die ons gaan helpen om onze processen conform de AVG uit te voeren en inclusief te maken. We hopen van harte dat dit besluit de kaders gaat bieden om dit ook mogelijk te maken.

Hoogachtend,
Namens de gemeente Nijmegen en de gemeente Amsterdam,

Touria Meliani
Wethouder ICT en Digitale Stad
Gemeente Amsterdam

Renske Heimer-Englebert
Wethouder werk, inkomen en armoedebestrijding, ICT en faciliteiten
Gemeente Nijmegen