Het ministerie ontvangt graag uw inhoudelijke reactie op de conceptregeling en -toelichting, u kunt reageren op alle onderdelen daarvan.

Inzender :Burgerrechtenvereniging Vrijbit
Contactpersoon: J.M.T.Wijnberg- bestuur@vrijbit.
Betrokkenheid:

Burgerrechtenvereniging Vrijbit zet zich, namens haar leden èn uit oogpunt van het algemeen belang, in voor het behoud van respecteren van de fundamentele rechten op bescherming van het privéleven. zie http://www.vrijbit.nl

Een korte opsomming van de belangrijkste kritiekpunten staat hieronder:

Fundamenteel

Het uitgangspunt dat het openstellen van overheidsdienstverlening via automatisch zou leiden tot een veiliger systeem van i/e-overheids functioneren, vanwege de diversiteit, doet geen recht aan de ervaringen ten aanzien van de doorgeschoten privatisering binnen de publieke sector. Niet aan de inmiddels bekende nadelen ten gevolge van de vermenging van privaat-publieke taken op gebied van rechtszekerheid, aansprakelijkheid, toepasselijkheid van wetgeving en mogelijkheden voor toezicht op publieke belangen. Nog los van het feit dat dit ook een rare manier vormt van het ministerie om zich bij voorbaat indekken voor toekomstige overheids ICT-debacles, kan men met een dergelijk taalkundige formulering geen rechtvaardiging leveren voor een beleid wat voortgaat op het doodlopende pad van een verdere uitbouw van de privatisering in het publieke terrein.

De hele conceptopzet met betrekking tot het openstellen van overheidsdienstverlening via private authenticatiediensten ademt een ongewenste onderdanigheid uit van de overheid ten opzicht van de belangen -en lobby- vanuit het bedrijfsleven. Belangen die men zwaarder laat wegen dan de taak tot optreden van de overheid als bewaker van de nationale en individuele veiligheid en soevereiniteit van alle Nederlanders.
Dat betreft in concreto:

A- Het feit dat er geen principiële keuze wordt gemaakt voor het uitsluiten van authenticatie systemen die niet gebaseerd zijn op een centraal georganiseerd systeem. Een vorm van negeren van de principes van privacy-in- ontwerp-archItectuur ten faveure van bedrijven die wel brood zien in een verdere uitbouw van hun systemen voor private dienstverlening en gebruik van biometrische identificatiesystemen. Een inzet kortom die niet kiest voor een aanpak waarbij het mogelijk misbruik van het e-ID-middel tot het gebruik daarvan beperkt blijft maar uitnodigt voor het grootschalige vormen van (georganiseerde) criminaliteit via de dataopslag. De hele opzet met zogenaamde waarborgen via een papieren randvoorwaarde dat een gescheiden opslag van gebruikersgegevens en gebruiksgegevens geëist wordt is een gotspe. Immers omdat de praktijk uitwijst dat ‘function creep’ bij een schat aan data altijd op de loer ligt, nauwelijks- en dan nog

altijd enkel achteraf- te bestrijden valt en domweg met een andere opzet voorkomen kan worden.

B- Het voornemen om geen systemen uit te sluiten die gebouwd worden op grond van bedrijfsgeheimen in plaats van principieel enkel op 'open source' principes gebaseerde systemen te accepteren.

Waardoor de mogelijkheden tot bescherming van iemands digitale identiteit tot een wassen neus verworden, voor zowel de burger zelf, als de verantwoordelijke en betrokken overheidsdiensten.

De overweging om het gebruik van het Burgerservicenummer (BSN)open te stellen voor private partijen introduceert een ongekend veiligheidsrisico voor iedere burger op misbruik van iemands identiteit en/of data die aan dit unieke persoonsregistratienummer gekoppeld zijn.

Dat het wetsvoorstel digi overheid(34.972)hiervoor een grondslag beoogt te introduceren, kan niet door de beugel. En zal als het goed is ook een struikelblok vormen voor het aannemen van de wet omdat het BSN uitsluitend bedoeld is voor het verkeer tussen de overheid en de burger.

Private partijen- waarvan bij voorbaat nota bene al bekend is dat ze met behulp van dit 'core ID' een business model voor zich zien *'waarbij er ruimte komt voor alternatieve middelen die bij voorkeur ook buiten de publieke sector gebruikt kunnen worden'* behoren geen toegang/ beschikking te krijgen tot de data van het Nederlandse Bevolkingsregister en het BSN. Waar het BSN als koppelnummer de toegang vormt voor alle gegevens over een burger waarover de overheid beschikt, is het onacceptabel dat een minister zelfs maar overweegt om het gebruik hiervan toe te staan aan anderen dan overheidsdiensten, instellingen in zorg en onderwijssector voor zover zij dat nodig hebben voor de uitoefening van hun publieke taak en de betrokken burger zelf.

Ook hier geldt dat het hele issue niet van toepassing is als men kiest voor een decentraal authenticathie systeem (waarbij specifieke persoonsgegevens- waaronder het BSN, naam of geboortedatum verstrekt worden door de overheid en afhankelijk van de context door de burger zelf onthuld kunnen worden).

Praktisch

Ook in geval van het ontwikkelen van authenticatiesystemen geldt het devies: 'beter voorzichtig zijn dan achteraf spijt krijgen'. Het heilige geloof in het onbezorgd inzetten op ruime holle kaderwetgeving ten behoeve van de mogelijke AMvB invulling *met het oog op de verwachtingen van toekomstige innovatieve van technologische ontwikkelingen*, is daarmee in strijd. Dat het stellen van degelijke, transparante en te handhaven voorwaarden aan architectuurkeuzes en systeemprincipes innovatieve technologie zou uitsluiten is natuurlijk onzin.

Daarbij willen we speciaal ook aandacht vragen voor de gemakzuchtigheid waarmee het concept schermt met de ISO27001 certificering alsof dit een daadwerkelijk garantie zou

bieden voor de feitelijke beveiliging en controle van de authenticatiesystemen. Waarbij de overheid- gezien de ervaringen met Diginotar- toch inmiddels ook wel het besef hoort te hebben dat certificeringen in feite rekenkundige modellen betreffen en geen garantiebewijzen.

Hoe men zich dat verder voorstelt om toezicht te kunnen houden op internationale bedrijven die vanuit andere lidstaten een authenticatiedienst gaan exploiteren waarbij de Nederlandse overheidsdiensten toegang gaat worden verplicht, is ons ook een raadsel. Waar we nu al te maken hebben met nationale organisaties- zoals de zorgverzekeraars- die toezicht op hun publieke taak via jarenlange juridische procedures over een correcte omgang met persoonsgegevens kunnen frustreren met beroep op bedrijfsvertrouwelijke processen, valt niet in te zien waarom de overheid zelfs maar een deur op de kier zet voor commerciële partijen die wensen te kunnen beschikken over zowel de opslag van authenticatiegegevens als over de gegevens over gebruik van het identificatiemiddel.

Gewoon niet aan beginnen is ons advies. Geen mogelijkheid voor scheppen bij wet en AMvB maatregelen voorkomt dat er überhaupt toezicht zou moeten worden uitgeoefend om te controleren of bedrijven die gegevens wel gescheiden bewaren *En hoe dan? En wie heeft toegang tot de bestanden, hoe zijn personeelsleden daartoe geautoriseerd, hoe wordt toegang tot gebruiksgegeven gelogd? In hoeverre zijn er uitzonderingen op analyse van- en controle op gebruiksgegevens in het kader van fraudebestrijding?* Deze opsomming is niet compleet, maar geeft wel een indicatie van onze ongerustheid t.a.v. zelfs maar de mogelijkheden van toezicht kúnnen houden nog los van de capaciteit en capabiliteit van de dienst die dit zou moeten gaan uitvoeren.