

Verzoek IRMA als standaard

Aan: College van Dienstverlening (samenorganiseren@vng.nl)

Afzender: De gemeenten Alblasserdam, Amersfoort, Arnhem, Boekel, Cuijk, Dordrecht, Emmen, Grave, Groningen, Haarlemmermeer, Harderwijk, Hardinxveld-Giessendam, Hendrik-Ido-Ambacht, 's-Hertogenbosch, Leiden, Lingewaard, Meierijstad, Mill, Nijmegen, Papendrecht, Sliedrecht en Zwijndrecht

Geacht college,

In het CIOberaad 100.000+ van 12 september 2019 heeft u de CIO's van gemeenten opgeroepen om te komen met voorstellen tot standaarden voor gemeenten. Graag geven wij gehoor aan deze oproep en zouden dan ook het volgende willen voorstellen in de categorie 'Standaarden voor informatiekundige vraagstukken':

Stel IRMA vast als standaard voor authenticatie bij de gemeentelijke overheid met de mate van verbindendheid: niet vrijblijvend 'pas toe of leg uit'-principe

In dit memo zullen we allereerst ingaan over digitale identiteit in zijn algemeen, vervolgens zullen de inhoudelijke vragen die zijn voorgeschreven in het proces standaardverklaring¹ worden behandeld waarna ten slotte de gedegen formulering gedaan zal worden op de punten zoals in het proces is aangegeven.

Digitale identiteit

Februari 2018 heeft de VNG een position paper digitale identiteit² uitgebracht waarin gesteld wordt dat een digitale identiteit noodzakelijk is die:

1. Identificatie en authenticatie in alle contexten en langs alle kanalen mogelijk maakt;
2. gebruikt kan worden voor accordering en ondertekening van stukken of transacties, zodat deze rechtsgeldig en voldoende betrouwbaar tot op het hoogste niveau zijn en
3. de inwoner of het bedrijf regie geeft op de eigen gegevens.

Met de Wet Digitale Overheid³ op komst is wordt het voor private partijen mogelijk om zich aan te melden als inlogmiddel voor de overheid. De kaders hiervoor worden bepaald in een nog niet gedefinieerde algemene maatregel van bestuur. Om hier op voorbereid te zijn is het voor gemeente verstandig om nu al een standaard te hebben, zodat zij de wet eenvoudig kunnen implementeren.

Privacy

De Wet Digitale Overheid wordt behandeld als 'technische' wetgeving. De concept wetteksten zijn zo geschreven dat er geen onnodige technische complicaties kunnen optreden bij de uitvoering van de

¹

https://vng.nl/sites/default/files/brieven/2018/attachments/08_notitie_proces_standaardverklaring_versie_cie_i_en_bestuur.pdf

² <https://vng.nl/nieuws/vng-position-paper-digitale-identiteit>

³

<https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A34972#activity-2019a03950>

wet. Ook Expertsessies voor de implicatie van de wet worden louter techneuten uitgenodigd. Met de komst van de Algemene Verordening Gegevensbescherming (AVG) en de steeds verder opkomende discussie over het gebruik van data is het noodzakelijk dat ook de maatschappelijke impact deze nieuwe wet wordt meegenomen in de uitvoering. De Raad van State wijst hier in haar advies over deze wet ook expliciet op⁴.

Hierop is het wetsvoorstel deels gewijzigd en is er geen sprake meer van een aanbesteding van private middelen, maar van een certificering door het ministerie. Echter, ook hier heeft de Raad van State nog de nodige kanttekeningen bij⁵.

Zover momenteel te overzien is, is er slechts één authenticatiemechanisme beschikbaar de AVG eigenschap 'Privacy by Design' in zich geeft: IRMA.

IRMA, I Reveal My Attributes

Aan de Radboud Universiteit is sinds 2008 onderzoek gedaan naar een veilig en privacy vriendelijke wijze van authenticatie⁶. Hieruit is een 'attribuut gebaseerd' decentraal model van authenticatie ontwikkeld dat in de kern neerkomt op de volgende eigenschappen:

- een identiteit wordt opgeknipt in zo klein mogelijke stukjes, attributen;
- deze attributen worden zo decentraal mogelijk opgeslagen, bij de gebruiker zelf;
- de attributen worden cryptografisch ondertekend door degene die hiervoor verantwoordelijk is;
- een partij die wil authenticeren kan zo de minimaal benodigde gegevens opvragen bij de gebruiker en door middel van de ondertekening controleren of ze 'echt zijn'.

Deze werkwijze is lastig commercieel te maken aangezien het door de decentrale opzet niet mogelijk is om een bedrag te vragen per authenticatie, zoals bij iDIN en DigiD, of een abonnementsmodel, zoals bij Itsme, op te zetten.

Om deze reden hebben de onderzoekers van deze authenticatiewijze een stichting opgezet om de onderzoeken om te zetten in de praktijk, de stichting Privacy by Design⁷. Inmiddels is ook de continuïteit van de Stichting geborgd doordat Stichting Internet Domeinnaamregistratie Nederland (SIDN), deze garandeert.

Meer informatie over IRMA is te vinden op de sites <https://www.irma.app> en <https://www.privacybydesign.foundation>.

Inhoudelijke vragen

In het proces standaardverklaring worden een vijftal vragen voorgeschreven om vast te stellen of het onderwerp in aanmerking komt om tot standaard te worden verheven.

Betreft het een beleidsarm onderwerp en is het een aangelegenheid voor gemeenten?

⁴ <https://www.tweedekamer.nl/downloads/document?id=008f1bf9-0484-4c6a-a6a5-20ee6a0139a2&title=Advies%20Afdeling%20advisering%20Raad%20van%20State%20en%20Nader%20rapport.pdf>

⁵ <https://www.tweedekamer.nl/downloads/document?id=3945b6a0-8fd6-472d-9415-c6676deeb415&title=Advies%20Afdeling%20advisering%20Raad%20van%20State%20en%20Nader%20rapport.pdf>

⁶ <https://privacybydesign.foundation/publicaties/>

⁷ <https://www.kvk.nl/orderstraat/product-kiezen/?kvknummer=67144128>

Alle gemeenten hebben diensten waarvoor inwoners en bedrijven zich moeten authenticeren. Denk hierbij onder andere aan het doorgeven van een adreswijziging, het aanvragen van een subsidie of het aanvragen van een vergunning maar ook bij het melden van een ongemak in de openbare ruimte is een vorm van authenticatie wenselijk. Momenteel is de gemeente hierbij afhankelijk van één centraal middel per groep: DigiD voor inwoners en eHerkenning voor bedrijven. Valt deze dienst uit, dan is er geen digitale dienstverlening mogelijk bij alle gemeenten. Daarnaast is deze vorm van authenticatie in sommige processen veel te zwaar, er wordt om een BSN gevraagd terwijl een postcode en huisnummer kan volstaan, zoals bijvoorbeeld bij een melding openbare ruimte.

Authenticatie is in alle processen een randvoorwaarde, een no-brainer voor beleidsmedewerkers. Dat maakt authenticatie een beleidsarm onderwerp voor gemeenten.

Is het nut van en behoefte aan de standaardvoldoende aangetoond en is deze in de praktijk beproefd?

Zoals eerder in deze memo behandeld heeft de VNG een position paper digitale identiteit⁸ opgesteld. In 2018, uitlopend begin 2019, is in het identiteitslab onderzocht aan welke randvoorwaarden de digitale identiteit zal moeten voldoen. Waag heeft in het kader hiervan een wegingskader⁹ uitgebracht waarin de belangrijkste eisen en waarden voor een digitale identiteit zijn beschreven.

De gemeente Nijmegen verstrekt in het kader hiervan sinds september 2018 gegevens uit de basisregistratie personen aan inwoners via IRMA¹⁰ en wordt daarbij ondersteund door 30 andere gemeenten. Bijna 8.000 personen hebben, zonder storing, van deze service gebruik gemaakt. Hierdoor is het mogelijk geworden dat zorgverzekeraar VGZ¹¹, een huisartsenpost in Uden¹² en een professioneel huisartsenportaal¹³ IRMA inmiddels in de praktijk gebruiken.

Gemeenten staan in de startblokken om IRMA te gaan gebruiken in de dienstverlening. De gemeente Buren is in afwachting van goedkeuring van een leverancier. De gemeenten Almere, Amsterdam, Haarlem en Leiden doen proeven in het kader van NLdigibeter en de gemeenten Groningen en Emmen beproeven samen met het ministerie Binnenlandse Zaken digitale democratie met IRMA, de gemeente Enschede laat mensen met een wisselend laag inkomen hun inkomstgegevens doorgeven via IRMA en de gemeenten Arnhem en Nijmegen starten op korte termijn een proef om persoonlijke telefonische dienstverlening mogelijk te maken via IRMA.

Wat is de noodzaak en/of meerwaarde van standaardisatie ten opzichte van de huidige situatie? (Welk probleem blijft bestaan als we niets doen? Is standaardisatie een passende oplossing voor dit probleem?)

Er zijn een aantal 'problemen' die opgelost worden als IRMA een gemeentelijke standaard kan worden:

1. *De afhankelijkheid van één centraal authenticatiemiddel neemt af.* DigiD is een goed middel om digitaal te authenticeren bij de overheid. Het is echter centraal van opzet waardoor een storing bij DigiD zorgt voor het dichtzetten van alle overheidsdienstverlening. Logius doet er

⁸ <https://vng.nl/nieuws/vng-position-paper-digitale-identiteit>

⁹ <https://digitaleidentiteit.waag.org/artikel/wegingskader/>

¹⁰ <https://services.nijmegen.nl/irma/gemeente/start>

¹¹ <https://www.vgz.nl/irma#/>

¹² <https://medipark.hix365.nl/Authentication/Authenticate?zpauth=Irma>

¹³ <https://helder.health/>

alles aan om dit tot een minimum te beperken, maar de afgelopen tijd nemen de storingen toe. Ditzelfde geldt voor eHerkenning voor bedrijven.

2. *Er komt een oplossing voor 'minimale authenticatie'.* Met DigiD geeft een inwoner zijn BSN aan de gemeente, die vervolgens via de BRP de overige gegevens van de inwoner bevestigt. Voor een groot aantal processen is dit een overtrokken vorm van authenticatie. Voor het aanvragen van een zoutkist, is de straat van de inwoner meer dan voldoende. Voor toegang tot de milieustraat is zelfs alleen van toepassing of iemand in de betreffende gemeente woont. Met IRMA is het mogelijk om alleen deze gegevens te verstrekken om aanspraak te maken op de door de gemeente geleverde dienst.
3. *Persoonlijke dienstverlening door de telefoon is mogelijk.* Op dit moment is het niet mogelijk om persoonlijke dienstverlening te bieden via de telefoon. Het is immers nooit zeker wie er aan de andere kant van de lijn is. Met IRMA kan de identiteit wel via de telefoon worden vastgesteld, waardoor er een extra volwaardig dienstverleningskanaal ontstaat.

Momenteel worstelen bijna alle gemeenten met bovenstaande problemen en kunnen er geen keuzes worden gemaakt, omdat er geen standaard is voor de problemen. Door middel van het standaard verklaren van IRMA hebben gemeenten houvast om op deze problemen aan te pakken.

Past het onderwerp binnen de GGU kaders die vastgesteld zijn in de Algemene Ledenvergadering?

Digitale identiteit is één van de 9 prioriteiten (A2) die de algemene ledenvergadering heeft vastgesteld.

Wordt de voorgestelde standaard niet al door een andere / hogere instantie of orgaan (bijvoorbeeld het Forum voor Standaardisatie) vastgesteld?

Momenteel ligt een expertadvies aan het Forum voor Standaardisatie voor om 'OpenID connect' voor te leggen voor standaardisering¹⁴. Het gaat hier echter om de eerste stap in het standaard, de routeringsvoorziening. Met IRMA expliciteren we dit naar het middel waarmee bij de gemeentelijke overheid geauthentiseerd kan worden.

Binnen de overheid geldt DigiD als 'standaard'. Zoals eerder gesteld is dit een risico doordat de centrale opstelling hiervan kan leiden tot onbereikbaarheid van gemeenten, daarnaast is het geen oplossing voor ondertekening, minimale authenticatie en telefonie.

De Wet Digitale Overheid maakt het mogelijk dat ook private partijen een authenticatiedienst aanbieden. Dit levert het maatschappelijke risico op dat er middelen beschikbaar komen die minder privacy vriendelijk zijn. Door als VNG een privacy vriendelijk alternatief als standaard te verklaren, beschermen we inwoners tegen dit privacy risico.

Motivering

Naast de vaststellingvragen, heeft het college ook vragen gesteld waarmee de argumentatie tot het nut van de standaardisering duidelijk wordt. Hieronder worden deze vragen beantwoord.

Wie zijn de stakeholders, wat is hun rol en hoe zijn ze betrokken?

Binnen het veld van authenticatie zijn veel stakeholders te benoemen. Waar het gaat om authenticatie middels IRMA bij binnen de overheid zijn er vier belangrijke stakeholders te benoemen:

- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Gemeenten

¹⁴ <https://www.forumstandaardisatie.nl/sites/bfs/files/Expertadvies%20OpenID%20Connect%201.0.pdf>

- Stichting Privacy by Design
- Stichting Internet Domeinnaamregistratie Nederland (SIDN)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Het ministerie is momenteel bezig met het wetgevingstraject rond de 'Wet Digitale Overheid'¹⁵, welke volgens ambtelijke planning medio 2020 in werking moet treden. De Wet is momenteel aangemeld voor plenaire behandeling. In deze wet is opgenomen dat buiten DigiD er andere identificatiemiddelen toegelaten kunnen worden tot het stelsel.

In voorbereiding hierop heeft het ministerie de Stichting Privacy by Design (uitleg zie hieronder) benaderd om mee te werken aan de nieuwe versie van DigiD¹⁶. Hierin wordt DigiD gepositioneerd als 'kernidentiteit', met daarin dezelfde gegevens als het paspoort¹⁷, met de mogelijkheid om deze gegevens door te geven aan een 'wallet' waarin de paspoortgegevens verwerkt kunnen worden met andere gegevens, zoals het adres. IRMA wordt gezien als eerste 'veilige wallet' die gebruik kan maken van deze functionaliteit.

Het ministerie is niet voornemens om extra gegevens buiten de 'paspoortgegevens' op te nemen in de nieuwe versie van DigiD. Gegevens als 'woonplaats', 'adres' en andere voor gemeente van toepassing zijnde gegevens moeten op een andere wijze worden opgehaald. IRMA wordt door het ministerie gezien als heel geschikte partij hiervoor.

Gemeenten

Zoals eerder in deze brief aangegeven zijn er veel gemeenten betrokken bij ontwikkelingen rond IRMA. Zowel bij de uitgifte van attributen als het maken van toepassingen. Binnen Common Ground lijkt IRMA op dit moment al de standaard te zijn bij toepassingen. Ieder project bevat wel een IRMA component.

Stichting Privacy by Design

De Stichting Privacy by Design is de ontwikkelaar van IRMA. Zij steunen dit voorstel voor standaardisering, uiteraard, en helpen momenteel de diverse gemeenten bij implementaties en passen de code aan op wens van de gemeenten.

SIDN

Stichting Internet Domeinnaamregistratie Nederland beheert sinds september 2019 de enige centrale component van IRMA, de keyshare server waar waar de helft van een wachtwoord wordt opgeslagen een deel van de wachtwoorden opgeslagen staat en de toegang tot 'mijnirma' in is gerealiseerd.

SIDN heeft een overeenkomst met het Ministerie van economische zaken waarin bevestigd wordt dat zij een cruciale schakel zijn in het internetverkeer in Nederland zijn en bij dreiging tot rechtsbeëindiging, door faillissement of andere redenen, worden 'gered' door het ministerie.

Ook SIDN is op de hoogte van dit voorstel en steunt dit van harte.

Wat is het draagvlak (hoe krijg je het, hoe meet je het en wanneer is het voldoende?)

¹⁵ <https://zoek.officielebekendmakingen.nl/dossier/34972>

¹⁶ https://digibeter-di.slack.com/files/UQ2NKH214/FQAKROYB0/20191106_informatieblad_pilot_inlogmiddelen.pdf

¹⁷ Paspoortgegevens: pasfoto, naam, BSN, geboortedatum

Dit voorstel wordt ingediend door 21 gemeenten variërend in grote. Deze gemeenten¹⁸ zien een groot belang in een standaard voor authenticatie naast DigiD en in lijn met de voorwaarden voortvloeiend uit de position paper digitale identiteit en het wegingskader van WAAG.

Ook buiten deze 21 gemeenten is er veel interesse om IRMA te gebruiken. De VDP en DIMPACT propageren IRMA bij hun leden en bijeenkomsten die worden georganiseerd rond IRMA worden door gemiddeld 40 gemeenten bezocht. Op congressen voor de digitale overheid (Zaakgericht werken, Congrestival, Overheid360 etc.), maar ook buiten de overheid (Eidentity, tweakers events) wordt de stichting of gemeenten die actief zijn met IRMA structureel gevraagd om een keynote of een groot side event te verzorgen.

Binnen de projecten in Common Ground is IRMA de facto de standaard gezien het open source karakter van de applicatie.

Door het decentrale karakter is het moeilijk te volgen hoe succesvol IRMA is. Wel kan het aantal gebruikers van IRMA worden gemeten door de stichting¹⁹ en weet de gemeente Nijmegen hoeveel BRP attributen zijn verstrekt. Het aantal implementaties en authenticaties is door de opzet niet te meten.

Wat zijn de uitvoeringsconsequenties voor gemeenten, ketenpartners, leveranciers, etc.?

De consequentie voor gemeente door de standaardisering van IRMA is dat zij, naast DigiD, een middel hebben dat het mogelijk maakt om inwoners te authenticeren. Leveranciers hebben zo duidelijkheid in de wens van gemeenten bij processen waar DigiD niet is toegestaan en ketenpartners hebben een extra middel om via de inwoner gegevens uit te wisselen.

PinkRocade is momenteel reeds bezig om IRMA te implementeren in haar software, maar voelt enige terughoudendheid door het ontbreken van een standaard.

In de zorg is IRMA reeds groeiend in gebruik. Diverse persoonlijke gezondheidsomgevingen passen IRMA toe en de grootste leveranciers van software in de zorg, Nedap en Chipsoft, hebben reeds werkende applicaties.

In plaats van beperkende consequenties, die zijn er niet, geeft standaardisering van IRMA juist duidelijkheid en richtinggevende consequenties.

Welke gradatie van verbindendheid wordt voorgesteld en in welk tempo en/of fases is implementatie wenselijk?

De eerste stap die voorgesteld wordt is de standaardiserende stap, pas toe of leg uit. Dit aangezien deze gradatie een vorm van urgentie en duidelijkheid uitspreekt naar leveranciers en gemeenten. Momenteel willen zowel leveranciers als gemeenten wel met IRMA werken, maar voelen een drempel. De standaardisatie kan deze drempel wegnemen.

Het tempo van de implementatie van de standaard wordt idealiter afgestemd met de invoering van de Wet Digitale overheid, welke vermoedelijk medio 2020 wordt vastgesteld. Na de invoering van deze wet is er ook een rijkskader waarin strakkere eisen worden gesteld aan authenticatie bij overheden. Een gemeentelijke standaard helpt gemeenten om deze wet soepel te implementeren.

IRMA is momenteel de enige applicatie die operationeel is en binnen deze kaders gaat passen. De mogelijkheid bestaat dat er in de toekomst meerdere decentrale oplossingen komen om veilig om te

¹⁸ Met in totaal 1.8 miljoen inwoners

¹⁹ <https://metrics.privacybydesign.foundation/grafana/d/000000011/irma-dashboard?orgId=1>

gaan met persoonsgegevens en authenticatie op hoog niveau mogelijk maakt. Op dit moment zien wij deze ontwikkelingen echter niet.

Ons voor stel is dan ook om bij de standaardisering direct een evaluatie in te plannen na 2 jaar. Op dat moment kan gekeken worden of er andere, betere, alternatieven zijn of dat IRMA een verplichtend karakter moet gaan krijgen.

Wat zijn de bij beheer-en handhavingsconsequenties? Inclusief financiële (incidenteel en structureel) gevolgen en de benodigde dekking daarvan.

Gezien het decentrale karakter van IRMA²⁰ zijn er geen structurele beheerkosten op korte termijn te voorzien voor de VNG, anders dan het op te nemen in de communicatiecampagne rond Samen Organiseren.

De benodigde IRMA server kan door de VNG meegeleverd worden in standaardsoftware die momenteel binnen Common Ground wordt ontwikkeld voor gemeenten. Het beheer van de software blijft echter bij de stichting Privacy by Design liggen.

Verstrekking BRP gegevens

Mocht blijken dat de gegevens uit de BRP verstrekt moeten blijven worden door gemeenten, dan is het denkbaar dat VNG realisatie deze verstrekkingen op zich neemt. De gemeente Nijmegen heeft ervaring in het implementeren van deze verstrekkingen. De kosten die hieruit voortvloeien worden geschat op:

Eenmalig	
Inrichting	€50.000,-
Structureel	
Per verstrekking	€0,22 ²¹

De eenmalige kosten bestaan uit het veilig, zowel technisch als juridisch, implementeren van een IRMA server die BRP gegevens uitgeeft namens gemeenten. De structurele kosten bestaan uit twee componenten:

- DigiD kosten. Momenteel bedragen de kosten voor een authenticatie binnen DigiD €0,14. Het is nog onduidelijk wat de kosten zullen zijn van het overnemen van de gegevens uit de nieuwe variant van DigiD zullen zijn.
- GBA-v kosten. Gemeenten nemen de GBA-v af via één van de vier BRP leveranciers²². De kosten voor het raadplegen van de GBA-v zijn momenteel ongeveer €0,08

Indien de VNG, of VNG realisatie zullen deze kosten gedekt moeten worden door het GGU fonds. In de huidige opzet zijn paspoortgegevens 5 jaar geldig en adres gegevens 1 jaar geldig. Indien IRMA evenveel gebruikers heeft als DigiD²³ zijn de kosten voor IRMA per jaar €1,25 miljoen²⁴.

²⁰ <https://irma.app/docs/what-is-irma/>

²¹ De kosten per verstrekking bevatten een DigiD component (momenteel 0,14) en een GBA-v component (€0,08)

²² Centric, PinkRoccade, Procura en compeT&T

²³ Momenteel ongeveer 14 miljoen

²⁴ $(14 \text{ mlj} * 0,22) + (14 \text{ mlj} * 0,08 * 4) / 5 = 1.243.200$

Afsluitend

Alvast hartelijk dank voor het in behandeling nemen van dit verzoek. We lichten het verzoek graag toe in uw overleg.

Met vriendelijke groet,

Ronald Mons
CIO Drechtsteden

Constance Boogers
CIO gemeente Nijmegen