IRMA Manifest

Digitale identiteiten voor digitale zekerheden

Een oproep om die zekerheden samen te organiseren

Prof. Bart Jacobs,
namens de stichting Privacy by Design

irma@privacybydesign.foundation

twitter.com/IRMA_privacy

Versie van 10 april 2019

De 6 belangrijkste punten

1. De digitale wereld is ons leven diep binnengedrongen, maar kent nog veel onzekerheden, bijvoorbeeld bij online kopen en verkopen: met wie heb ik van doen, hoe worden mijn gegevens beschermd, hoe kan ik anderen ergens aan houden?

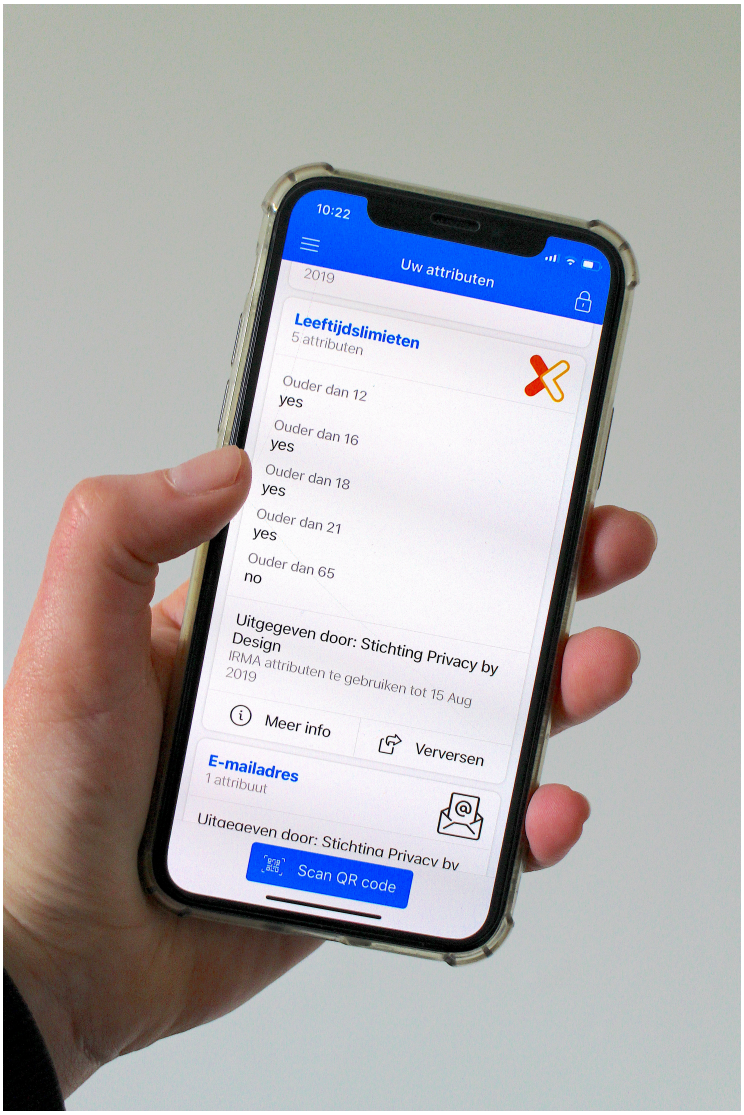
2. Voor het verkrijgen van zulke zekerheden spelen digitale eigenschappen van mensen (attributen) een grote rol: is zij een dokter, woont hij op dat adres, is dat haar telefoonnummer of e-mailadres, is hij wel ouder dan achttien?

3. Digitale zekerheden zijn gebaseerd op technieken voor authenticatie, versleuteling en ondertekening. Het is nodig deze drie technieken op een begrijpelijke wijze te combineren en voor iedereen makkelijk en gratis beschikbaar te maken.

4. Het is de rijksoverheid en het bedrijfsleven om allerlei redenen tot nu toe niet gelukt om zulke digitale identeiten op een open wijze te realiseren, zodat de hele samenleving er van kan profiteren en er ook aan bij kan dragen.

5. IRMA biedt nu wel zulke digitale identiteiten, via een onafhankelijke stichting. IRMA is van ons allemaal: het is open source, gratis beschikbaar voor eindgebruikers, privacy-vriendelijk en kan op steeds meer plaatsen gebruikt worden.

6. Onze digitale identiteit moeten we niet laten bepalen door internationale ICT-giganten. Met IRMA kunnen we het samen organiseren. Bedrijven, overheden en burgers: doe vooral mee en draag bij, vanuit ieders eigen rol, ten behoeve van onderlinge zekerheid en vertrouwen in de digitale samenleving.



De geopende IRMA app op een smartphone, met mapjes met verschillende attributen. Het mapje met leeftijdsgrenzen is geopend.

Overzicht

Dit manifest beschrijft een brede, samenhangende visie op de strategische rol die digitale identiteiten spelen in het maatschappelijke verkeer: ze bieden zekerheden om op een vertrouwde wijze digitaal te kunnen handelen. Dit manifest bestaat ruwweg uit drie delen: eerst wordt de rol van digitale identiteiten bij authenticatie, digitale ondertekening en versleuteling uiteengezet. Vervolgens wordt beschreven hoe IRMA een 'Zwitsers zakmes' voor digitale identiteiten is en nu reeds de gevraagde zekerheden op een open manier kan leveren. Ten slotte komt aan bod hoe IRMA verder uitgebouwd kan worden als *community effort* en wordt een oproep gedaan om deze *community* breder te steunen, zodat Nederland een internationaal leidende positie op kan bouwen met een duurzame en betrouwbare digitale infrastructuur.

Identiteiten en attributen, voor 'toe's'

Een groot deel van ons dagelijkse leven vindt plaats in de digitale wereld. Daarbij spelen digitale identiteiten een grote rol. We willen daarbij niet behandeld worden met kille administratieve persoonsnummers, maar met persoonlijke eigenschappen (attributen): ik ben Nederlander, woon in Nijmegen, op daten-dat adres, ik ben ouder dan 16, ik gebruik die-en-die e-mailadressen, ik heb dit burgerservice nummer (BSN) en dat verzekeringsnummer, enzovoort. Met zulke attributen kan ik, afhankelijk van de situatie, een relevant deel van mijn identiteit laten zien en gebruiken.

Dit gebruik omvat vele vormen van 'toe', zoals:

- **toegang**, bijvoorbeeld om bij mijn eigen bankrekening te kunnen of om mijn eigen telefoon te kunnen ontgrendelen en gebruiken;
- **toedekking**, bijvoorbeeld om de e-mails met mijn eigen huisarts vertrouwelijk te houden;
- **toestemming**, bijvoorbeeld voor als ik meedoe aan orgaandonatie;
- **toezegging**, bijvoorbeeld dat ik daadwerkelijk iets zal leveren via Marktplaats;
- **toeschrijving**, bijvoorbeeld van een politieke boodschap op sociale media.

AVO: Authenticatie, Versleuteling en Ondertekening

De zekerheden die met deze vijf toe's gepaard gaan hangen samen met de identiteiten van de betrokkenen: het moet duidelijk zijn *wie* toegang krijgt, voor *wie* iets wel of niet toegedekt wordt, *wie* toestemt of iets toezegt, en aan *wie* iets toegeschreven kan worden. De realisatie van die zekerheden maakt gebruik van de volgende drie technische basisbegrippen: authenticatie, versleuteling, en ondertekening. Ze worden hier gezamenlijk met de afkorting AVO aangeduid.

1 **Authenticatie** staat voor bewijzen wie je bent, of beter: het bewijzen van relevante persoonlijke eigenschappen in een bepaalde situatie. Een eenvoudige vorm van authenticatie is het aantonen dat je ouder dan 16 bent, voor het spelen van een (heftige) online game. Of: om aan je gemeente te melden dat er tegels losliggen in jouw straat is inloggen met je BSN veel te zwaar: het volstaat als je kunt laten zien dat je in de buurt woont (via je

postcode) en toont wat je e-mailadres is, zodat de gemeente op je melding kan reageren. Authenticatie vormt de basis voor het regelen van **toegang**, die alleen verleend moet worden aan personen die daar recht op hebben. Authenticatie vereist niet dat je overal altijd hetzelfde van jezelf laat zien, zoals de gegevens in je paspoort. Integendeel, breed bruikbare authenticatie is divers en kent veel vormen, zodat je in iedere situatie juist die persoonlijke eigenschappen (attributen) van jezelf aantoont die daar noodzakelijk zijn om toegang te krijgen. Authenticatie is belangrijk om zekerheid te hebben over 'wie aan de andere kant van de lijn zit', maar moet niet verworden tot privacy-onvriendelijk overvragen; dan worden veel te veel persoonsgegevens opgeëist, bijvoorbeeld voor het maken van uitgebreide profielen. De nieuwe privacywet — de Algemene Verordening Gegevensbescherming (de AVG) — verbiedt zulk overvragen en eist dat alleen minimale, relevante gegevens gevraagd worden voor toegang.

2 **Versleuteling** is het mechanisme om de inhoud van berichten op zo'n manier te verhullen dat alleen de juiste ontvanger erbij kan. Versleuteling kan het beste gekoppeld worden aan een uniek attribuut van de ontvanger, zoals een e-mailadres, telefoonnummer, een burgerservice nummer (BSN), of een zorgverlener-registratie nummer (BIG). Met zulke versleuteling kan alleen de persoon met dat unieke attribuut het bericht ontsleutelen. Door versleuteling zijn berichten vertrouwelijk, zoals bij Whatsapp. Versleuteling zorgt voor bescherming, niet alleen van persoonlijke informatie, maar ook van gevoelige informatie bij bedrijven of bij overheden. Versleuteling vormt de basis voor wat hierboven **toedekking** genoemd is. Versleuteling is een onmisbare beschermingstechniek in de digitale wereld die op veel verbindingen gebruikt wordt, bijvoorbeeld bij websites die beginnen met `https`, met een '`s`' voor 'secure'. Toedekking van persoonsgegevens wordt vereist in de AVG als een van de standaard beschermingstechnieken. Versleuteling kan zulke bescherming bieden tegen gericht of ongericht afluisteren, bijvoorbeeld door al te nieuwsgierige bedrijven, door cybercriminelen of door minder-bevriende landen. Dat laatste maakt versleuteling van nationaal belang. Zoals veel technieken heeft versleuteling ook een keerzijde: het kan gebruikt worden om zaken toe te dekken die het daglicht niet kunnen verdragen. Daardoor kunnen mensen misschien wegkomen met onwettig gedrag of kunnen aanslagen moeilijker voorkomen worden. De *bad guys* maken nu al gebruik van allerlei vormen van versleuteling. Dat is geen reden om het de *good guys* te onthouden. Brandkasten zijn ook vooral nuttig. Toch wil je er in noodgevallen bij kunnen. Met IRMA kan dat, zoals later beschreven wordt.

3 Digitale **ondertekening** speelt eenzelfde rol als gewone ondertekening, via een handtekening onder een brief of een formulier: de persoon die ondertekent legt zich vast (commiteert zich), vanuit een bepaalde rol, aan de inhoud van een (digitale) boodschap. De ontvanger van de ondertekende boodschap krijgt zo zekerheid over wie de afzender is, in welke rol, maar ook over waartoe de ondertekenaar zich precies verplicht. Digitale ondertekening is een krachtige techniek die gebruikt kan worden voor **toestemming**, **toezegging** en voor **toeschrijving** (of **toerekening**).

Wanneer een verkoper op Marktplaats digitaal ondertekent dat hij zal verkopen en leveren voor een bepaalde prijs, kan hij daar aan gehouden worden. En wanneer een medisch recept digitaal ondertekend wordt door een arts, kan de administratieve afhandeling met de juiste autorisaties en zekerheden uitgevoerd worden.

De combinatie van deze 'AVO' mechanismen — Authenticatie, Versleuteling en Ondertekening — vormt de basis voor een betrouwbare ICT-infrastructuur, niet alleen voor burgers, maar ook voor bedrijven en overheden. We zijn allemaal gewend onszelf dagelijks te authenticeren, tegenover onze eigen computer of telefoon, of op allerlei websites. Versleuteling is een veel gebruikte techniek in de ICT, op belangrijke verbindingen, maar wordt in het dagelijkse leven niet vaak actief gebruikt: slechts weinig mensen versleutelen hun e-mail zelf, ook al kan dat al lang, bijvoorbeeld met PGP. Deze techniek is niet heel gebruiksvriendelijk — vooral omdat het moeilijk is om zelf met cryptografische sleutels om te gaan. Digitale ondertekening bestaat als techniek al tientallen jaren, maar is ook nauwelijks doorgedrongen tot het grotere publiek, niet alleen vanwege gebrek aan gebruiksgemak en ondersteuning, maar ook vanwege de hoge kosten die er vaak mee gepaard gaan.

Het goede nieuws is dat AVO-technieken snel en breed beschikbaar zijn voor dagelijks gebruik, via IRMA!

Openheid

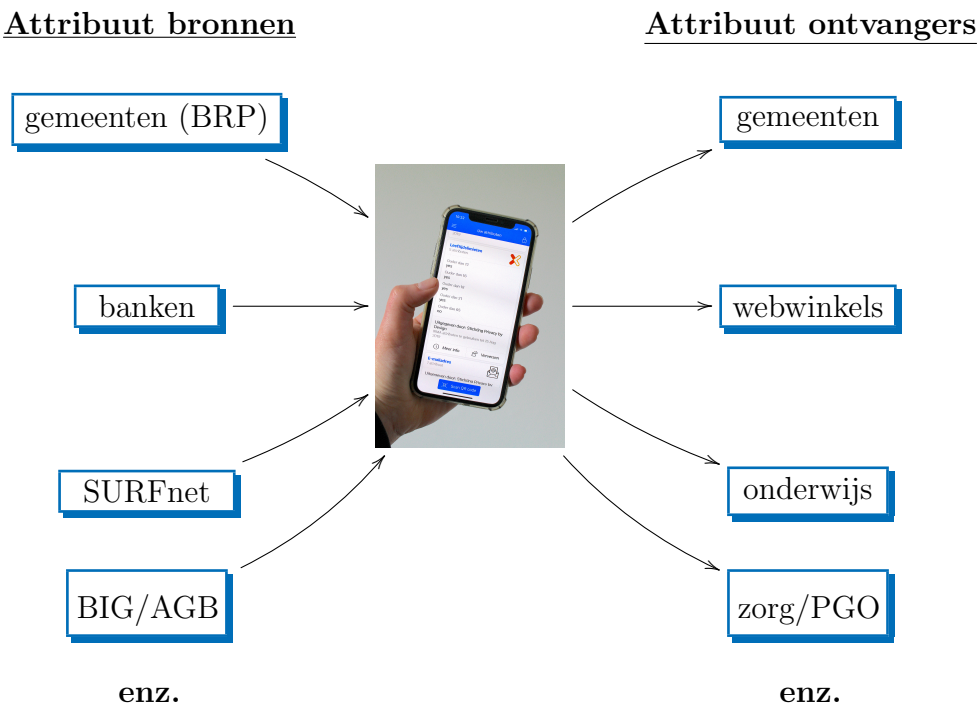
Authenticatie, Versleuteling en Ondertekening (AVO) zijn dus belangrijk voor digitale zekerheden. Deze technieken vergen onderlinge samenwerking en afstemming, zodat wat de ene partij bewijst, versleutelt of ondertekent, door de andere partij goed begrepen, vertrouwd en gebruikt kan worden. Hier zijn 'open' technieken voor nodig, die iedereen kan gebruiken en waar iedereen op kan vertrouwen. Deze technieken zijn zo belangrijk, dat hier internationale open standaarden voor zijn, zodat we niet van één organisatie of bedrijf afhankelijk hoeven te zijn, zodat er geen monopolie ontstaat, en we eenzijdig afhankelijk worden.

Deze gewenste openheid omvat een aantal punten.

- De AVO-functionaliteit moet in principe voor iedereen beschikbaar zijn, zonder kosten voor individuele gebruikers, en moet gebruiksvriendelijk zijn.
- Hoe het werkt moet duidelijk en begrijpelijk zijn, waarbij in het bijzonder helder moet zijn welke partijen welke (persoons)gegevens verwerken, bij authenticatie, versleuteling en bij ondertekening.
- De techniek moet gebruikt kunnen worden in andere ICT-systemen, zodat AVO-functionaliteit als los bouwsteentje (module) ingepast kan worden voor allerlei andere diensten.

In de praktijk worden deze eisen het beste gerealiseerd via systemen die *open source* zijn, zodat iedereen zekerheid kan krijgen over de gebruikte software en cryptografie. Met zulke openheid worden lastige discussies vermeden — zoals nu bij sommige Chinese leveranciers — over de mogelijke aanwezigheid van achterdeurtjes in de geheime software die heimelijk misbruikt kunnen worden.

Inderdaad, IRMA heeft een transparante werkwijze en gebruikt open source software.



Aan de linkerkant beschrijven de pijlen het ophalen van attributen uit vertrouwde bronnen in de IRMA-app. Aan de rechterkant staat hoe deze attributen vervolgens selectief getoond kunnen worden voor authenticatie, bij verschillende ontvangende partijen. De IRMA-app is het eigen knooppunt waar de eigen gegevens samenkomen.

De IRMA-oplossing

Hierboven is een visie geschetst op de maatschappelijke rol van digitale identiteiten, via authenticatie, versleuteling en ondertekening (AVO). De vraag rijst hoe deze rol het beste gerealiseerd kan worden. De Nederlandse stichting Privacy by Design biedt hiervoor het identiteitsplatform IRMA. Dit platform is voortgekomen uit wetenschappelijk onderzoek aan de Radboud Universiteit en is sinds 2016 ondergebracht bij een onafhankelijke stichting, zonder winstoogmerk. Deze stichting werkt aan de verdere ontwikkeling en uitrol van IRMA, via open source software. IRMA is beschikbaar via een gratis app, voor Google (Android) en Apple (iOS), waarin gebruikers een eigen 'paspoort' kunnen samenstellen met persoonlijke attributen, zoals voornaam, achternaam, huisadres, e-mailadres(sen), geboortedatum, telefoonnummer(s), bankrekening(en), BSN, medische BIG/AGB-registraties, inschrijvingen als student, enzovoort. Deze lijst van beschikbare attributen groeit voortdurend.

AVO met IRMA

Authenticatie, Versleuteling en Ondertekening (AVO) hangen nauw met elkaar samen binnen IRMA, omdat al deze technieken gebruik maken van persoonlijke attributen op de smartphone van de gebruiker. De uitleg daarvan hieronder is soms een beetje technisch, maar is bedoeld om een beeld te geven van nieuwe mogelijkheden. In het kort: authenticatie en ondertekening is nu mogelijk via IRMA, en wordt ook gebruikt; versleuteling via IRMA is nog in ontwikkeling.

Authenticatie met IRMA werkt met attributen (persoonlijke eigenschappen). Deze kan ik als gebruiker zelf in mijn IRMA-app verzamelen, vanuit verschillende betrouwbare bronnen. Zo heeft IRMA een koppeling met de Basisregistratie Personen (BRP), waardoor ik (een deel van) de officiële gegevens die de overheid van mij heeft in mijn IRMA-app kan zetten. Daarmee kan ik vervolgens op overtuigende wijze aantonen waar ik woon, bijvoorbeeld bij een webwinkel (voor de bezorging), of bij het openen van een bankrekening of verzekering, of bij een andere dienst. Om die attributen te tonen, moet ik een QR-code op een website scannen met mijn telefoon, en kan ik in de IRMA-app toestemming geven om de gevraagde attributen te onthullen. Ook kan ik zo via IRMA aantonen wat mijn BSN is en daarmee inloggen op websites van de overheid, in de zorg, of in het onderwijs. Iemand met een medisch beroep kan met IRMA aantonen wat zijn/haar BIG-nummer en medische specialisatie is, en vanuit die rol inloggen op een medisch systeem en berichten digitaal ondertekenen. Met zulke attributen kan ik afhankelijk van de context alleen die persoonlijke eigenschappen tonen die op dat moment van belang zijn. Hiermee bescherm ik mijn privacy en heb ik regie over mijn eigen gegevens.

Deze IRMA-attributen worden alleen in mijn eigen smartphone opgeslagen, en nergens anders. Deze attributen staan dus niet in de cloud en ook niet bij de stichting achter IRMA. Dat is net als bij een paspoort, waarbij ik mijn gegevens zelf in de hand heb. Het betekent wel dat ik op een nieuwe telefoon, in principe, de eigen attributen opnieuw moet verzamelen. De stichting Privacy by Design maakt het binnenkort echter mogelijk om zelf een beveiligde back-up te maken van reeds verzamelde attributen. Zo'n back-up kan dan op een nieuwe telefoon overgezet worden.

Dat is een voorbeeld van gestage verbetering van een open systeem als IRMA, in overleg met gebruikers.

Ondertekening van korte boodschappen is mogelijk via de IRMA-app. De boodschap verschijnt dan in het scherm op mijn telefoon, met daaronder een aantal van mijn persoonlijke eigenschappen. Die attributen bepalen de rol waarin ik de handtekening zet. Dat kan gewoon mijn naam zijn, maar ook mijn naam samen met een BSN of BIG-nummer, waardoor ik als burger of als arts onderteken — als ik tenminste arts ben. De gebruiker kan binnen de IRMA-app besluiten om het getoonde bericht wel of niet met die attributen te ondertekenen.

Digitale handtekeningen vormen het perfecte middel om **toestemming** vast te leggen, bijvoorbeeld wanneer ik besluit om mijzelf als orgaandonor te registreren, wanneer ik bepaalde gegevens beschikbaar stel voor medisch onderzoek of voor marketing, of wanneer ik iemand anders machtig om namens mij te handelen. De AVG vereist dat verwerking van mijn gegevens (bijna altijd) alleen met mijn toestemming mag plaatsvinden. Een digitale handtekening is daarvoor zeer geschikt. Een digitale handtekening is ook het juiste middel voor het vastleggen en het **toerekenen** van allerlei beroepsmatige handelingen, zoals het uitschrijven van een medisch recept, het accorderen van een financiële overschrijving, of het sluiten van een contract. Digitale handtekeningen kunnen het vertrouwen in digitale transacties sterk vergroten. Om dit daadwerkelijk mogelijk te maken moet echter nog veel werk verzet worden, zodat alledaagse computersystemen met digitale handtekeningen kunnen omgaan. Daarmee worden dan ook nieuwe innovatieve toepassingen mogelijk, zoals betrouwbaar, *anoniem solliciteren*. De sollicitant zet dan een digitale handtekening op zijn/haar sollicitatiebrief, waarbij de gebruikte attributen wel de behaalde opleiding omvatten, maar niet de eigen naam. De ontvanger weet dan dat de brief afkomstig is van iemand met die opleiding, maar weet niet de bijbehorende naam (en identiteit).

De stichting Privacy by Design voorziet een groots toekomstig gebruik van digitale handtekeningen bij het tegengaan van nepnieuws en van *deep fakes* — waarbij men iemand een willekeurige uitspraak kan laten doen door video en audio te manipuleren. Stel je voor dat er een video in omloop komt waarop premier Rutte zomaar hele negatieve dingen zegt over de Koran. Dan wil je snel kunnen vaststellen of zo'n video echt vanuit de overheid komt. Dat kan met digitale handtekeningen. Als voorlichters van ministeries, online kranten, en allerlei andere media organisaties hun berichten, foto's en video's systematisch voorzien van digitale handtekeningen, kunnen ongetekende berichten afgedaan worden als onbetrouwbaar. Dit vergt een enorme omslag, die heel hard nodig is om nepnieuws en deep fakes effectief tegen te gaan. Het is belangrijk te benadrukken: het gaat hierbij niet om het vastellen van de *waarheid* van media-uitingen — heel glad ijs — maar om het vaststellen van de *herkomst* ervan (d.w.z. de authenticiteit), via digitale ondertekening.

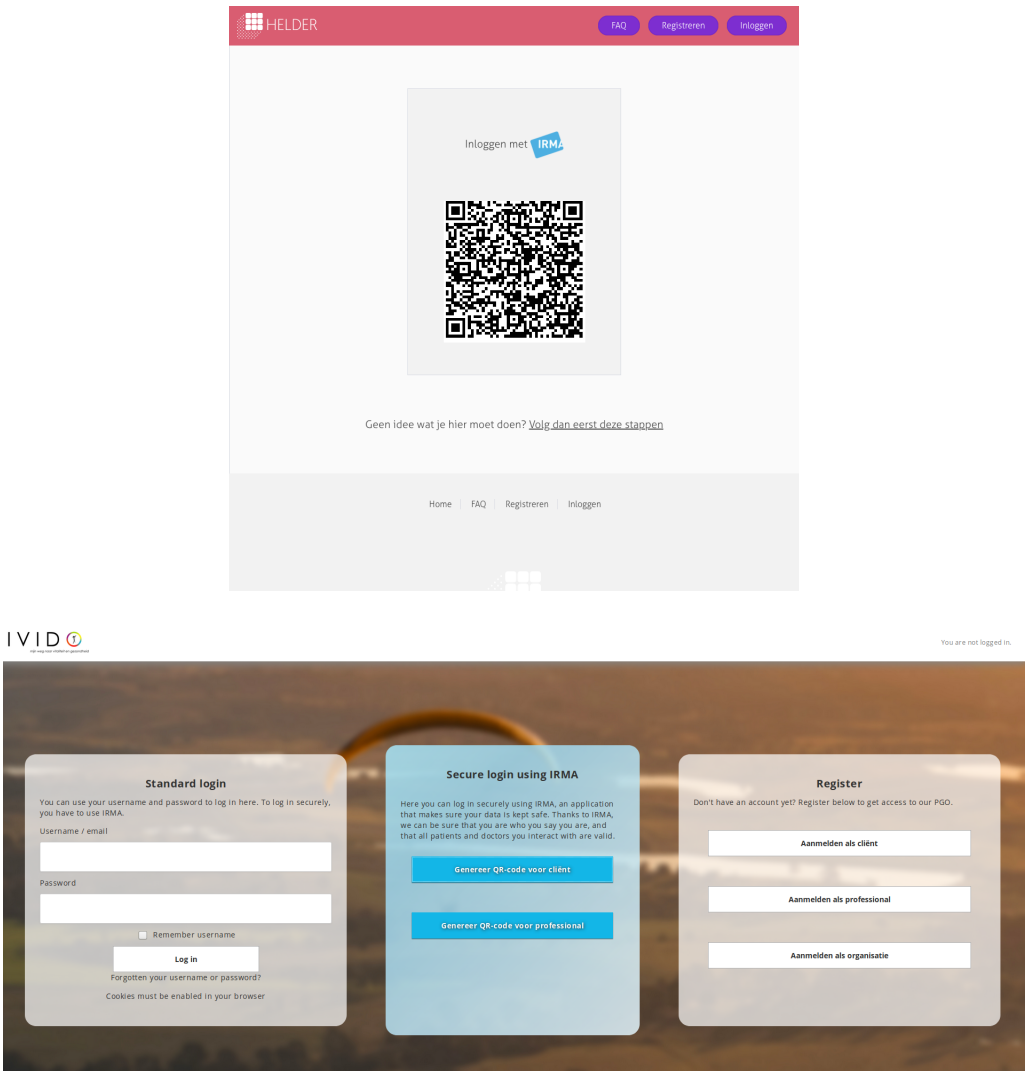
In het algemeen kunnen digitale handtekening zekerheden bieden in de vluchtige digitale wereld. Systematisch gebruik van digitale ondertekening is een middel tegen wat wel *context collapse* genoemd wordt, waardoor we niet goed zien waar berichten vandaan komen. Van belangrijke waarschuwing willen we zeker weten dat die bijvoorbeeld van de politie of brandweer af-

komstig zijn. Ook zouden gebruikers hun instemming met de voorwaarden van digitale platformen en van andere dienstverleners kunnen vastleggen via een digitale handtekening; dan wordt het minder eenvoudig die voorwaarden eenzijdig te wijzigen. Met zulke eenzijdige wijzigingen worden we helaas allemaal regelmatig geconfronteerd.

Versleuteling van berichten en teksten is op dit moment nog niet mogelijk met de IRMA-app. Er bestaan wel gedetailleerde plannen voor zo'n uitbreiding, gebaseerd op een techniek die identiteitsgebaseerde versleuteling (*Identity Based Encryption*) genoemd wordt. Daarbij kan de verzender een bericht versleutelen op basis van een uniek identificerend attribuut van de ontvanger. Zo'n attribuut kan bijvoorbeeld een e-mailadres zijn, een telefoonnummer, een BSN of een BIG-nummer. De ontvanger heeft een eigen geheime cryptografische sleutel nodig voor de ontsleuteling. Die sleutel kan opgehaald worden bij een vertrouwde partij — een *Trusted Third Party* of TTP — na een bewijs van bezit van dit unieke persoonlijke attribuut. Voor deze authenticatie stap wordt IRMA zelf gebruikt. Op deze wijze zijn ook versleuteling en authenticatie in IRMA geïntegreerd.

De genoemde vertrouwde partij, de TTP, speelt hierbij een zeer gevoelige rol. Deze partij maakt immers voor iedereen sleutels — in een eigen streng beveiligde omgeving (een *hardware security module*) — en kan met die sleutels, in principe, ieders berichten lezen. Mensen die geen sleutels via die ene TTP willen kunnen natuurlijk zelf andere systemen voor versleuteling gebruiken, zoals PGP. De beoogde versleuteling met IRMA is bedoeld voor dagelijks gebruik, zodat mensen op eenvoudige wijze versleuteld met hun huisarts, gemeente of advocaat kunnen e-mailen, over persoonlijke zaken. Dat zal het basisniveau van beveiliging aanzienlijk verhogen.

Tevens zorgt de aanwezigheid van de TTP ervoor dat de autoriteiten — alleen met de juiste wettelijke vereisten — de geheime sleutel van een verdachte kunnen opeisen, om diens communicatie te kunnen ontsleutelen. Daarmee biedt versleuteling met IRMA enerzijds laagdrempelige bescherming in lijn met vereisten van de AVG, en anderzijds de mogelijkheid om met wettelijke waarborgen (versleutelde) informatie te verzamelen voor strafrechtelijke vervolging of voor inlichtingendoelen. Zulke versleuteling met IRMA biedt wel de voordelen maar niet de nadelen: de angel wordt daarmee uit de discussie over de maatschappelijke wenselijkheid van versleuteling gehaald.



Twee voorbeelden van inloggen met IRMA in de zorg: bij het portaal ‘Helder’ van Nedap, voor artsen om toegang te krijgen tot de dossiers van hun patiënten (boven), en bij het portaal van Ivido voor patiënten en voor zorgverleners (onder).

IRMA in beweging

Eenmaal hier aangekomen in dit verhaal rijst de vraag: hoe krijgen we die digitale identiteiten goed van de grond, voor de digitale mogelijkheden en zekerheden die we zo hard nodig hebben?

Zonder overdrijving: IRMA is het meest geavanceerde platform voor digitale identiteiten in Nederland (en daarbuiten), met de meeste attributen. IRMA kan nu direct gebruikt worden, zonder kosten voor eindgebruikers, voor authenticatie en voor digitale ondertekening, en wordt de komende tijd uitgebouwd om ook versleuteling te ondersteunen. Rond IRMA heeft zich een ecosysteem gevormd van partijen — bijvoorbeeld in de zorg en in het locale bestuur — die de functionaliteit en stabiliteit van IRMA willen verbeteren en het gebruik willen vergroten. Binnen dat ecosysteem versterken partijen elkaar en kunnen ze profiteren van elkaars bijdragen. IRMA heeft nu, begin april 2019, zo'n 5500 geregistreerden in Nederland. Inloggen met IRMA komt nu van de grond, vooral in de zorg en bij locale overheden. Het gebruik van IRMA groeit gestaag, maar misschien is een versnelling nodig.

Wie moet het doen?

De rijksoverheid heeft al jaren grote ambities op het gebied van digitale identiteiten, voor de uitvoering van overheidstaken en voor de digitale toegang van burgers tot de overheid. Dit gaat alle departementen aan. Toch moeten we feitelijk constateren dat de rijksoverheid er in de afgelopen jaren niet in geslaagd is om een leidende rol in dit dossier te spelen en een verantwoordelijkheid te nemen voor de gehele samenleving, zowel publiek als privaat. De rijksoverheid heeft zich de laatste jaren beperkt tot het zorgen voor de eigen behoeften, waarvoor één attribuut volstaat, namelijk het BSN. Dit attribuut wordt enkel gebruikt voor authenticatie, met DigiD; voor versleuteling of ondertekening is geen aandacht. De niet-publieke sector mag dit BSN-attribuut niet gebruiken en heeft dus geen baat bij wat de overheid op dit gebied ontwikkelt.

Vanuit het bedrijfsleven zijn verschillende initiatieven naar voren gekomen, ook gericht op authenticatie, bijvoorbeeld vanuit de banken (met iDIN) of vanuit de telecom sector (bijvoorbeeld met Mobile Connect of Itsme). Daarbij moet voor iedere authenticatie betaald worden (in de orde van dubbeltjes), wordt maar een beperkt aantal attributen ondersteund, en is privacybescherming een ondergeschoven kind: deze partijen gebruiken een 'centrale' architectuur waarbij alle authenticaties via hun systemen verlopen. Daarmee kunnen ze niet alleen voor iedere authenticatie laten betalen, maar kunnen ze ook precies bijhouden wie waar op welk moment inlogt, en kunnen ze uitgebreide gebruikersprofielen opbouwen. We moeten constateren dat geen van deze commerciële initiatieven in Nederland al echt van de grond gekomen is, waarschijnlijk door een gebrek aan functionaliteit, vertrouwen en (privacy-)garanties. Ook bestaat er angst voor een mogelijk commercieel monopolie waardoor de prijzen alleen maar hoger worden.

Nu het zowel de rijksoverheid als het bedrijfsleven niet echt lukt om breed gebruik van digitale identiteiten te realiseren is het misschien de beurt aan de non-profit sector. Daarmee komen identiteiten buiten de handel te staan. Dat is niet zo'n vreemde gedachte. Nu reeds worden strategische taken in de Nederlandse digitale infrastructuur op non-profit basis uitgevoerd: de Stich-

ting Internet Domeinregistratie Nederland (SIDN) geeft bijvoorbeeld de .nl-webadressen uit, naar volle tevredenheid. In de Verenigde Staten geeft de organisatie *Let's Encrypt* (zie letsencrypt.org) gratis certificaten uit voor het beveiligen van internetverbindingen (voor de bekende groene slotjes in de adresbalk van browsers). Deze organisatie levert op betrouwbare wijze wat iedereen nodig heeft en wordt daarvoor ondersteund door zo ongeveer alle grote IT-bedrijven. Hiermee is *Let's Encrypt* in korte tijd een grote en gewaardeerde strategische leverancier geworden.

Het IRMA-ecosysteem

Rond IRMA groeit nu een gemeenschap, juist vanwege het non-profit, niet-monopoliserende, open karakter van de technologie. Zo hebben inmiddels meer dan twintig zorg-ICT leveranciers hun handen ineengeslagen onder de vlag van nuts.nl, om een gezamenlijke open infrastructuur op te zetten, waarbij IRMA een verbindende factor is. IRMA wordt daarbij gebruikt om in te loggen, waardoor patiënten toegang krijgen tot hun eigen medische gegevens en artsen toegang krijgen tot de gegevens van hun patiënten. Binnen de context van nuts.nl worden zogenaamde AGB-codes — voor declaraties in de zorg — aan zorgverleners uitgegeven, als IRMA attributen. De stichting Privacy by Design (achter IRMA) is bij deze uitgifte niet betrokken, en kan (en wil) niet zien welke zorgverlener zulke attributen in de eigen IRMA app heeft staan. Dit regelen de partijen in het veld allemaal zelf.

Een veertigtal gemeenten in Nederland ondersteunt het gebruik van IRMA, via uitgifte van IRMA-attributen vanuit de Basisregistratie Personen (BRP). Bij de daadwerkelijke uitgifte van deze attributen is de stichting Privacy by Design niet betrokken. Het hierbij, ondere andere, uitgegeven BSN-attribuut kan door burgers gebruikt worden om bij overheden, in de zorg, of in het onderwijs in te loggen, of om een belastingformulier of vergunningsaanvraag digitaal te ondertekenen. Ook worden hierbij leeftijdsgrenzen (zoals: ouder dan 16) als attributen uitgegeven, die gebruikt kunnen worden bij controle op (online) gokken en gaming en bij gereguleerde aankopen, zoals van alcoholische dranken. De uitgifte en het gebruik van IRMA-attributen door gemeenten is in februari 2019 juridisch getoetst door het befaamde advocatenkantoor Pels Rijcken & Droogleever Fortuijn, met als conclusie "dat er geen wezenlijke belemmeringen zijn". Die formulering klinkt zuinig, maar is van groot belang.

Andere sectoren dan de zorg of de (locale) overheid kunnen IRMA gebruiken en er hun voordeel mee doen. Zo is IRMA erg geschikt voor toepassingen in de financiële sector, bijvoorbeeld voor nieuwe PSD2-diensten: authenticatie met IRMA om in te loggen op een financiële app, of ondertekening met IRMA om toestemming te geven aan je bank om gegevens vrij te geven aan zo'n app, of om je opdracht tot overschrijving van een bedrag vast te leggen. Zo'n ondertekend bericht geeft zekerheid, voor alle betrokken partijen, inclusief toezichthouders. Maar IRMA is ook nuttig voor de banken, bijvoorbeeld om bij het openen van een rekening zekerheid te krijgen over de nieuwe rekeninghouder (KYC: *know-your-customer*), via de BRP-attributen op diens telefoon.

Zo vervullen de verschillende spelers in het IRMA-ecosysteem ieder een eigen (decentrale) rol, voor zichzelf en ook voor anderen. De stichting Privacy by Design heeft

enkel de taak om de IRMA-infrastructuur te garanderen. Die garanties worden overigens in samenwerking met SIDN gerealiseerd.

Alternatieven

Natuurlijk, er kan eindeloos verder gepraat worden over allerlei aspecten van digitale identiteiten: moet er nu wel of niet biometrie bij, of moeten de plaatjes in de app er zus of zo uitzien. We moeten ons daar niet door laten verlammen. Er wordt in Nederland al meer dan tien jaar gepraat over een nationaal systeem voor digitale identiteiten, als opvolger van het inmiddels verouderde DigiD. Ondanks vele pogingen is er niks écht van de grond gekomen. Met IRMA bestaat er nu een privacy-vriendelijk en veilig alternatief, met veel functionaliteit en sterke garanties (via *zero knowledge proofs*), dat de komende jaren door het open (source) karakter verder verbeterd kan worden, via bijdragen en ideeën vanuit de gemeenschap. Laten we daarmee aan de slag gaan, van onder op, *by creating facts on the ground*. IRMA is van ons allemaal. IRMA past in een bredere beweging voor een duurzame ICT-infrastructuur die gebaseerd is op publieke waarden, zie ook het Nederlandse initiatief *Public Spaces* (publicspaces.net) dat IRMA gaat gebruiken, en zie ook het internationale project Solid (solid.inrupt.com) van internet pionier Tim Berners-Lee.

Mogelijk komt er over een aantal jaren een beter systeem, dat de AVO-functionaliteit (en mogelijk meer), op een betere manier verschaft, met sterkere garanties. Dan moeten we daar op dat moment vooral op overstappen. Tot die tijd echter heeft IRMA de beste papieren en de meeste kans op brede acceptatie, juist vanwege het open non-profit karakter, zonder monopolisering. IRMA komt van onderop, vanuit onze eigen *civil society*, en onderscheidt zich juist door de inzet, de deskundigheid en het enthousiasme van de vele betrokkenen. Doe mee, *join the team!* Hiermee kan Nederland (en Europa) zich met waarden-gedreven ICT onderscheiden van Amerikaanse en Chinese benaderingen, die gericht zijn op dominantie, door grote ICT-bedrijven of door de staat. Als we hier dingen anders willen, zullen we daar wel zelf in moeten investeren.

Binnen Europa wordt vaak naar Estland gekeken als het gaat om digitale identiteiten. Estland kent een eigen digitale traditie die zich echter niet laat vertalen naar Nederland: in Estland heeft iedere burger een persoonlijk nummer, dat zowel in de publieke als in de private sector gebruikt kan worden. Alle online diensten zijn rond dit ene attribuut/nummer georganiseerd. Daarmee kunnen alle online handelingen onderling gekoppeld worden. Het resulterende gebrek aan privacy wordt gecompenseerd met transparantie: Estse burgers kunnen in detail zien wie wanneer wat met hun gegevens heeft gedaan. Estland heeft last van de 'wet van de remmende voorsprong'. De gebruikte één-attribuut benadering past niet in andere landen — zoals Nederland of Duitsland — en past ook niet bij moderne attribuut-gebaseerde benaderingen waarmee we in verschillende online situaties verschillen eigenschappen van onszelf willen laat zien.

IRMA is overigens internationaal beschikbaar en bruikbaar, maar de uitrol richt zich allereerst op Nederland. Als we het hier goed van de grond gekregen hebben, komen andere landen vanzelf wel kijken.

IRMA komt vanuit de gemeenschap

Jouw identiteit bepaal je voor een groot deel zelf. Maar je bent daarbij wel afhankelijk van anderen. Zo moet het digitaal ook werken, als de digitale wereld aan wil sluiten bij bestaande gebruiken en ervaringen. Met IRMA stel je ook zelf je identiteit samen, door zelf attributen over jezelf te verzamelen. Voor die attributen ben je afhankelijk van vele anderen, die fungeren als betrouwbare bronnen van attributen. Daarmee is IRMA een gezamenlijk project: een *community effort*, van ons allemaal. De overheid is daarbij een belangrijke speler, als verschaffer van een *bron*-identiteit — via de BRP, of via een paspoort, rijbewijs of ID-kaart. Maar de overheid is zeker niet de enige bron van jouw identiteit.

Verschillende partijen doen nu al mee met de ontwikkeling van het ecosysteem van IRMA. Maar nog veel meer partijen zouden zich aan kunnen sluiten, zoals: de Kamer van Koophandel voor het uitgeven van bedrijfsgegevens (inclusief wettelijke vertegenwoordiging) als IRMA-attributen, telecoms voor abonnement/contactgegevens, de belastingdienst voor inkomenscategorieën, DUO voor diploma's, Studielink voor digitale collegekaarten, verzekeraars voor verzekeringsbewijzen, supermarkten en andere winkels voor klant-/kortingskaarten, Marktplaats voor reputatie attributen voor verkopers, enzovoort, enzovoort. Wanneer wij burgers op eenvoudige wijze toegang kunnen krijgen tot zulke attributen over onszelf, kunnen wij die in allerlei situaties (selectief) gebruiken voor authenticatie, ondertekening, en zelfs versleuteling. Door het open (source) karakter van IRMA kunnen allerlei organisaties er gratis gebruik van maken: niet alleen ziekenhuizen en webwinkels, maar ook de locale schaak- of voetbal-club. De daaruit voortvloeiende mogelijkheden en zekerheden versterken het onderlinge vertrouwen en dragen bij aan de (digitale) samenleving en economie.

Oproep

Dit manifest eindigt met een algemene oproep — aan wie dit leest — om de verdere ontwikkeling van het IRMA-ecosysteem te ondersteunen en er aan bij te dragen. Digitale identiteiten kunnen we samen organiseren. IRMA is een gedistribueerd systeem, waarbij het juist niet de bedoeling is om te gaan wachten tot overheden of de Google's of Baidu's van deze wereld besluiten dat onze digitale identiteiten er zo-en-zo uit zullen gaan zien, vooral om hun eigen belangen te dienen. IRMA komt van onderop, en ontleent haar kracht aan de deelname van vele betrokkenen: hoe meer partijen attributen uitgeven, hoe rijker onze IRMA-identiteiten zijn. Tegelijkertijd is het bij IRMA geen anarchistische chaos, want IRMA heeft een wel-doordachte cryptografische basis waarin alleen vertrouwde bronnen digitaal getekende attributen uitgeven, waarop anderen kunnen vertrouwen.

Deze oproep richt zich op organisaties en op individuen.

Organisaties kunnen op verschillende manieren vorm geven aan hun steun, onder andere via:

1. operationele steun, via het integreren van IRMA-functionaliteit in de eigen diensten en/of producten, zowel voor het controleren als voor het uitgeven van attributen;
2. actieve steun, via het mee-ontwikkelen van open source software voor het IRMA-platform en via het beschikbaar stellen van ontwikkelcapaciteit;

3. financiële steun aan de stichting Privacy by Design, via een donatie, niet alleen voor het versnellen van de verdere ontwikkeling van IRMA, bijvoorbeeld voor versleuteling of andere uitbreidingen, maar ook voor het onderhouden en uitbouwen van de IRMA infrastructuur;

4. inhoudelijke ondersteuning van deze visie, bijvoorbeeld via publieke onderschrijving en verdere verspreiding via de eigen publicitaire kanalen (waaronder sociale media).

In ieder van deze gevallen kan contact opgenomen worden via het e-mailadres

irma@privacybydesign.foundation

voor de verdere bespreking van de gewenste betrokkenheid.

Individuen kunnen een bijdrage leveren aan de verdere ontwikkeling van het IRMA-ecosysteem, via:

1. het verspreiden van dit manifest via de eigen sociale media (Twitter, Facebook, Instagram, ...), voorzien van eigen inzichten, verklaringen en oproepen, bijvoorbeeld aan bedrijven of politici;

2. het zelf installeren van de IRMA-app en het verzamelen van eigen attributen, om daarmee de bekendheid met de technologie te vergroten;

3. het aansporen van de eigen organisatie / werkgever, of van organisaties waarmee samengewerkt wordt, om IRMA te steunen, langs hierboven genoemde lijnen;

4. voor open source ontwikkelaars en ontwerpers: meewerken aan de ontwikkeling van het IRMA-platform, aan het (meer) gebruiksvriendelijk maken, en aan de integratie van IRMA in andere software omgevingen — tekstverwerkers, mailclients, browsers, enz. — bijvoorbeeld via nieuw te ontwikkelen plugins.

Ook geïnteresseerde individuen kunnen natuurlijk contact opnemen via het bovengenoemde e-mailadres.