E - DEM

Digitale participatietools voor lokale overheden

Authenticatie, autorisatie en verificatie in platforms voor participatieve democratie.

DOOR TOM DEMEYER, WAAG SOCIETY

Inleiding

In de titel van deze notitie komt het woord identificatie niet voor. Dat is om een reden. Identificatie is een lastig begrip doordat identiteit op verschillende manieren te definiëren is die elk nooit geheel bevredigend zijn. Bij de geboorte wordt ons door de overheid een burgerservicenummer (BSN) verstrekt. Dit is de minimaalste wettelijk-bureaucratische definitie. Correct uiteraard, maar niemand identificeert zich met zijn of haar BSN. De meest brede definitie is de culturele betekenis van identiteit. We kunnen identiteit ook biologisch benaderen, bijvoorbeeld met biometrie of als een collectie van alle persoonlijke data. Voor sommigen zal identiteit het antwoord zijn op de vraag 'wie ben je?'

In overheidscontext is het duidelijk, het BSN levert een wettelijke mogelijkheid tot identificatie en bewijs van identiteit. Maar dit betekent niet dat we daarmee een algemeen antwoord hebben op wat we eronder verstaan; daarvoor is het begrip identiteit te afhankelijk van de context en het doel van de interactie.
Soms is directe koppeling met het BSN noodzakelijk, maar in de digitale werkelijkheid zijn er vele scenario's waarin het niet nodig of wenselijk is mensen op dit niveau te authentiseren. Bovendien, het gaat in de onderhavige context vaak ook om (e-)dienstverlening tussen (groepen van) burgers onderling, of tussen burgers en instellingen anders dan de overheid; in deze gevallen is het gebruik van BSN wettelijk ook niet mogelijk.

Identificatie is overigens zelden nodig. Er zijn weinig situaties waarin we werkelijk vast moeten stellen wie iemand is. Uiteraard wel bij de huisarts, of in het ziekenhuis, wanneer we het identiteitsbegrip biologisch benaderen. Maar in verreweg de meeste gevallen gaat het om de autorisatie om een recht uit te oefenen. Deze autorisatie aantonen (bewijzen) vereist in veel gevallen een mechanisme dat we authenticatie noemen. In het algemeen wordt dit omschreven als verificatie van identiteit, maar hier omschrijven we het simpelweg als verificatie van autorisatie. Strikter, verificatie van autorisatie om een recht te consumeren.

In Nederland zijn het paspoort, de identiteitskaart en het rijbewijs geldige identiteitsdocumenten die gebruikt kunnen worden bij een veelheid van authenticatievraagstukken. Digitaal hebben we DigiD (en voor beperkte toepassingen iDIN). Authenticatie kan echter ook op veel andere manieren, denk aan een zwempas, klantenkaart, pinpas. Deze authenticatiemiddelen autoriseren een bepaalde actie of transactie, tonen lidmaatschap aan of meer algemeen een recht. We verwachten niet voor alles het volle gewicht van een paspoort, maar leiden authenticatiemiddelen hieruit af, legitimeren een middel of verlenen autorisatie op een andere manier. Digitaal, online, hebben we buiten overheids- (en zorg-) context geen enkele optie die formeel, wettelijk, stand kan houden doordat er een koppeling is met ons BSN en daarmee met onze wettelijke persoon.

Deze notitie gaat over de eisen aan authenticatie in de context van (online, digitale) participatieve democratie, en over de mogelijkheden de noodzakelijke mechanismen hiervoor op een gedifferentieerde en privacy-beschermende manier vorm te geven.

Eisen aan authenticatie, relatie met STORK[1] raamwerk

In dienstverlening op het gebied van participatieve democratie is vertrouwen en transparantie cruciaal. Of het platform nu door de overheid gefaciliteerd wordt als bijvoorbeeld Stem van West[2], of door grass-roots initiatieven als Hallo IJburg[3].

Eén van de bronnen van dat vertrouwen is dat we ervan uit kunnen gaan dat deelnemers, op momenten dat het er toe doet, niet kunnen acteren vanuit niet bestaande of verzonnen kwalificaties. Wanneer dit van belang is, op wélke momenten, is toepassingsspecifiek.

De eisen die we stellen aan de hiervoor nodige authenticatie zijn dynamisch en veranderen per activiteit, en per rol die men daarin neemt. Wanneer de overheid initiatiefnemer is kunnen formele kwalificaties als leeftijd of inwonerschap na authenticatie via DigiD worden geverifieerd. Meer informele kwalificaties, of die voor gebruik in grass-roots platforms, hebben andere mechanismen nodig.

In overheidscontext wordt de kwaliteit van de authenticatie beschreven in het STORK-raamwerk. In deze context zijn vooral de STORK-niveaus twee en drie interessant. In participatieve platforms zien we nog een extra niveau tussen de niveaus een en twee. STORK-niveau één stelt weinig specifieke eisen en behoeft niet veel discussie, en iets dat vergelijkbaar is met STORK-2 is buiten overheidscontext lastig te realiseren. STORK-kwalificaties zijn niet van toepassing zijn op andere dan overheidsdiensten, ze leveren echter een bruikbare referentie op wanneer we spreken over vereisten die gelden voor authenticatie voor Platforms voor Participatieve Democratie (PPD). In het vervolg gaan we uit van wat we de “PPD indeling” noemen, naar analogie met de STORK-classificatie:

- PPD-1: Vergelijkbaar met STORK-1, behoeft weinig discussie en is in veel platforms op dit moment het niveau waarop wordt geauthentiseerd. In principe zou je kunnen zeggen dat de deelnemer hier zelf de verantwoording neemt voor de correctheid van haar claims. Soms is het een bewijs van controle over een e-mailadres, soms wordt er via standaard mechanismen (OAuth) een derde partij gebruikt zoals Google of Facebook. Dit laatste is redelijk betrouwbaar in het (her-)authentiseren van personen wanneer ze eenmaal ‘in het systeem’ bekend zijn, de moeilijkheid (het gebrek aan verificatie-mogelijkheid) zit in de eerste stap, wanneer de persoon zich aanmeldt.

- PPD-2: Dit is het meest interessante niveau; het levert meer garanties dan PPD-1, maar voert niet noodzakelijkerwijs direct terug op een wettelijk mechanisme. Hier zullen we later uitgebreid op terugkomen, dit is feitelijk het onderwerp van deze notitie.

- PPD-3: Hier hanteren we hetzelfde kwaliteitsniveau als STORK-2. De wettelijke basis wordt ontleend aan het feit dat de authenticatie op enigerlei wijze terug te voeren is op DigiD of een ander formeel geldend (toekomstig) eID mechanisme.

- PPD-4: Hier geldt eenzelfde niveau van zekerheid als bij STORK-3. Daar waar er grote belangen op het spel zouden staan, waar toekomstige platforms bijvoorbeeld lokale verkiezingen zouden faciliteren, zijn cryptografische mechanismen nodig zoals die ook bij diensten op niveau van STORK-3 worden gehanteerd. Dit niveau laten we in deze notitie grotendeels buiten beschouwing, maar is met de groeiende digitalisering van de democratische processen in toenemende mate relevant en interessant.

ZKP - Zero Knowledge Proof

Privacy is een groot goed en staat steeds meer onder druk. Bij het gebruik van platforms voor participatieve democratie is aandacht voor privacy en anonimiteit extra belangrijk. Met de aanstaande GDPR4 privacy wetgeving vanuit Europa, maar ook onder de huidige wetgeving, is zorgvuldige omgang met persoonsgegevens een belangrijke eis aan iedere digitale dienst. Bij vraagstukken rond authenticatie en identificatie gaat het bij uitstek om persoonsgegevens. Daar waar we gebruik of opslag van persoonsgerelateerde gegevens kunnen vermijden of minimaliseren, minimaliseren we ook de verantwoordelijkheid en aansprakelijkheid als ‘data processor’ zoals geformuleerd in de GDPR.

Een belangrijke technische mogelijkheid die de noodzaak van gebruik of opslag van persoonsgegevens beperkt is de zero knowledge proof (ZKP - een vertaling in het Nederlands klinkt erg onhandig). Hierbij stelt men de gebruiker in staat een “verklaring” (claim) te bewijzen zonder verder iets te hoeven prijsgeven. Een bewijs van inwonerschap, van leeftijd kan worden geleverd zonder enig ander persoonskenmerk prijs te geven. “Ik kan bewijzen dat ik ouder ben dan 18 zonder mijn leeftijd of geboortedatum te onthullen.” Hierdoor ontstaat

bijvoorbeeld de mogelijkheid van anoniem gebruik van een buurtplatform waar men gebruikers van buiten de buurt niet of anders wil laten deelnemen. Van de geverifieerde inwoner van de buurt weten we mogelijk verder niets, geen naam, geen adres; toch weten we onomstotelijk dat zij in de buurt woont.

Implementaties van deze technologie zijn bewezen en beschikbaar. We gaan ervan uit dat authenticatie-, autorisatie- en verificatiemechanismen in goede PD-platforms zodanig worden ingezet dat ze voldoen aan de privacy by design principes zoals die worden vereist door de GDPR. Een robuust systeem met fijnmazige ZKP-verificatie werkt ook bevordering van vertrouwen in de hand, zowel ten aanzien van datamanagement als in functionele zin. Men weet met grote betrouwbaarheid 'met wie men van doen heeft' in een bepaalde situatie, maar zonder noodzaak te weten wie het is. Vertrouwen is gebaseerd op veel meer dan op technologie alleen, maar een goede en bewezen technische implementatie is in dit kader wel een belangrijke voorwaarde.

Een ander voordeel van het gebruik van deze technologie om specifieke eigenschappen van deelnemers afzonderlijk te authentiseren en verifiëren is dat het de verscheidenheid aan mogelijke (innovatieve) diensten, gefaciliteerd door verschillende fijnmazige samenstellingen van eigenschappen, enorm vergroot.

Binnen het EU project DECODE[5] wordt er op het moment gewerkt aan een infrastructuur waarin deze en andere mechanismen ter beschikking komen, met een pilotimplementatie onder andere in de ppd platforms Decidim[6] en Gebied Online[7]; hierin zijn ook de steden Barcelona en Amsterdam partner.

PPD-2 gedifferentieerde authenticatie en verificatie

Wanneer we het idee van identificatie loslaten, en ons beperken tot verificatie van claims ("verklaringen") zijn we flexibeler in het antwoord op de vraag wie nu eigenlijk een bepaalde claim moet verifiëren. Wanneer het gaat om mijn claim dat ik auto mag rijden moet de RDW dat kunnen verifiëren (mogelijk via een tussenstap, een authenticatiemiddel, zoals een rijbewijs). Wanneer ik claim dat ik een middenstander ben in de Kinkerbuurt in Amsterdam, is het logisch dat de lokale Kamer van Koophandel deze claim kan verifiëren. In dit laatste voorbeeld is er 'verifier' nog steeds een min of meer officiële instantie met een wettelijke taak. De vraag is of dat wel altijd nodig is. Hierover later meer. Laten we eerst eens kijken naar die middenstander, actief op een hypothetisch platform waarop lokale democratie wordt bedreven. Het is goed om te begrijpen hóe zo'n claim kan worden geverifieerd.

In een toekomst, waarin er in het KvK-register (dat dan vanzelfsprekend open te raadplegen is) een publieke sleutel is opgenomen van de onderneming, kan hiermee een token worden versleuteld dat alleen degene die de onderneming beheert kan lezen. Als de 'claimer' vervolgens de inhoud van dit token terugkoppelt aan degene die (of het systeem dat) om verificatie vraagt, is bewezen dat deze claimer, vertegenwoordigd door die digitale entiteit op het platform, de privésleutel van de onderneming beheert, en dus ook de registrant is van dat KvK-record. Het proces is hier versimpeld weergegeven, maar in essentie loopt het zo. Let wel, dit gebeurt natuurlijk 'achter de schermen' op het platform zelf, of in een infrastructuur zoals die wordt voorzien in DECODE.

Op het moment dat een platform zo'n claim geverifieerd heeft kan dit natuurlijk (met een bepaalde geldigheidsduur) worden hergebruikt zonder de 'omweg' via de KvK te hoeven maken. De meeste van de actoren in de lokale democratie (buiten de individuele burger: denk aan sportverenigingen, VvE's, middenstanders, buurthuizen, bibliotheken etc.) staan geregistreerd bij de KvK. De hierboven besproken technieken met betrekking tot zero knowledge proof bouwen onder andere op deze PKI (public key infrastructure) verificatiemechanismen. We zien dus dat we hiermee (anoniem, en zonder verdere informatie uit te wisselen) bijvoorbeeld een voorzitterschap van een VvE kunnen aantonen en verifiëren. Dat kan in bepaalde activiteiten op het platform erg nuttige informatie zijn. Er zou bijvoorbeeld bij discussie of stemmingen meer gewicht kunnen worden toegekend aan direct betrokkenen bij het onderwerp dan aan zijdelings of niet betrokkenen, en dat zonder de 'identiteit' van de betrokkenen te hoeven kennen. Die anonimiteit is natuurlijk geen vereiste, er kan te allen tijde ook een naam gekoppeld worden aan de deelnemer, of een adres. Wat hier het beleid is, is een ontwerpkeuze van het specifieke platform, en wordt ingegeven door de diensten die het verleent.

Hiermee hebben we enig inzicht in hoe het zou kunnen werken voor veel van de betrokkenen in een context van lokale democratie, maar nog niet over de individuele burger. Ook is de KvK niet open te raadplegen, en is PKI (public key infrastructure) geen onderdeel van de registratie bij de KvK. Helaas. Wat we concluderen is dat we kunnen denken over gedifferentieerde authenticatie. Wanneer we, op welke manier dan ook, de lokale sportvereniging hebben gekoppeld aan een digitale representatie in het platform (aan de user "AFC IJburg") kunnen we het bewijs van lidmaatschap van een individu natuurlijk aan deze user 'AFC IJburg' overlaten, dat vinden we logisch. Maar dat lidmaatschap van een VvE een bewijs van inwonerschap van een bepaalde buurt kan leveren is wellicht iets minder vanzelfsprekend, omdat inwonerschap een 'officiële' kwalificatie is die in het algemeen een uittreksel uit het de GBA vooronderstelt. De vraag is of we voor dit soort toepassingen wel een PPD-3 (STORK-2) authenticatie nodig hebben, of dat een PPD-2 niveau voldoende is?

In de context waarover we spreken is de stelling dat we met PPD-2 het overgrote deel van de gebruiks-scenario's afdekken. Dit wil niet zeggen dat de we autoriteit van PPD-2 claims niet kunnen (of zouden moeten) opschroeven.

Zoals hierboven al is onderkend zit de crux van het vraagstuk bij de 'binnenkomst' van een gegeven in het systeem. Wanneer een gegeven eenmaal binnen is, zijn er, bijvoorbeeld met een infrastructuur als DECODE, betrouwbare uitspraken te doen en

zijn afgeleide of geaggregeerde eigenschappen verifieerbaar. Komt een gegeven binnen met een authenticatie op PPD-3 kwaliteitsniveau dan blijven uitspraken (voor de geldigheidsduur van de verklaring) beschikbaar met die specifieke zekerheid. Met meer PPD-3 geauthentiseerde gegevens is het mogelijk een systeem te versterken; op PPD-2 niveau leidt dat dan tot voldoende waarborgen voor de toepassingen waar de platforms zich mee bezig houden.

Zoals boven beschreven kunnen bedrijven en verenigingen een bijdrage leveren aan dit bootstrap proces, via lidmaatschap of inwonerschap. Individuele burgers kunnen dit ook. Ouders zijn (voor de meeste toepassingen) autoriteit genoeg om de leeftijd van hun kinderen te verifiëren, buren kunnen bevestigen dat iemand op hun trap woont, of in hun blok. We benadrukken nogmaals dat we het hier hebben over geautomatiseerde processen waar handelingen van de deelnemers zelf in de meeste gevallen niet nodig zijn. Bij uitstek in buurtplatforms lijken de mogelijkheden van sociale, of peer2peer authenticatie relevant en interessant. Waarbij wel moet worden opgemerkt dat wanneer het té gemakkelijk is endorsements te geven, en zeker wanneer deze anoniem kunnen worden gegeven, de betrouwbaarheid van uitspraken daarmee dramatisch zakt. Een zekere drempel is nodig, financieel, mogelijkerwijs, of bijvoorbeeld via platform credits die 'op kunnen' en weer moeten worden verdiend.

Portabiliteit en soevereiniteit van "identiteiten"

Wanneer we zien dat verschillende samenstellingen van eigenschappen ons verschillende rechten geven is de stap naar meerdere identiteiten niet zo'n grote. Een bepaalde collectie van eigenschappen kunnen we zien als een afzonderlijke entiteit, ook wel een 'nym' genoemd. De nym waarmee ik deelneem in een discussie over groenvoorziening is wellicht een andere dan die waarin ik deelneem aan een initiatief rond criminaliteitsbestrijding. In de 'echte' maatschappij ben ik op mijn werk niet dezelfde persoon als diegene die op het voetbalveld zijn zoon aanmoedigt; in de digitale wereld is het natuurlijk net zo.

Nu is dit niet de plek om digitale identiteit in z'n algemeenheid te bespreken, de onderhavige vraagstelling heeft hier natuurlijk wel alles mee te maken. Wat we uit die algemenere discussies minimaal willen meenemen zijn de begrippen "self-sovereign" en "portable". Met self-sovereign identity wordt bedoeld dat het beheer van de collectie van 'nyms' (van de identiteit, zo men wil) volledig bij de gebruiker zelf ligt, en dat deze onafhankelijk van enige (centrale) instantie eigenschappen ter verificatie kan overleggen. De verificatie kan vervolgens natuurlijk door derden worden gedaan, door de staat (BSN) of RDW (rijbewijs) of sportclub (lidmaatschap), maar óf en wanneer dit gebeurt is zaak van de houder van die eigenschappen. Het gebruik van deze nyms laat ook geen sporen achter in enig centraal systeem, tenzij de betreffende af te nemen dienst dit expliciet vereist, natuurlijk.

Een portable identiteit is een identiteit (in de zin van een collectie van eigenschappen) die niet afhankelijk is van, of technisch gekoppeld is aan, één enkel platform of één enkele instantie. Stel, ik woon in Amsterdam West, en ik ben vanuit mijn werk in Gouda actief in het platform Gouda Bruist. In Stem van West (een initiatief van Amsterdam) ben ik actief als bewoner. Veel overlap hoeft er niet te zijn tussen deze twee nym's, maar mocht ik ooit in Gouda Bruist willen kunnen aantonen dat ik bijvoorbeeld een forens uit Amsterdam ben, hoewel anoniem, dan kan ik dat bewijzen (zonder iets anders prijs te geven) doordat ik in Stem van West ooit geauthentiseerd ben met mijn DigiD, en aangetoond inwoner van West (Stem van West gebruikt DigiD op het moment niet, maar als overheidsplatform heeft het de mogelijkheid). Dit beperkt zich natuurlijk niet tot participatieplatforms, maar zal uiteindelijk van betekenis zijn in alle digitale (online) interactie. Dit is een goed voorbeeld waaruit blijkt dat afzonderlijke, geverifieerde claims op niveau PPD-3 helpen claims in andere context te verstevigen, zonder dat er opnieuw interactie plaatsvindt op PPD-3 niveau.

Conclusie & aanbevelingen

Authenticatie- en verificatievraagstukken in platforms voor participatieve democratie worden nu in de meeste gevallen op een per platform basis opgelost, zonder interoperabiliteit tussen die platforms. Er wordt in het algemeen geen rekening gehouden met de variëteit aan belanghebbenden en de verschillende 'identiteitsbehoeften' van de deelnemers. DigiD of e-Herkenning (eID voor bedrijven) worden niet gebruikt, ook niet waar dit wel nuttig zou zijn, wegens wettelijke en technische beperkingen.

De kwaliteit van authenticatie die nodig is varieert per gebruiksscenario; een gedifferentieerd systeem van authenticatie en verificatie levert meerwaarde in functionaliteit, veiligheid, dataminimalisatie en vertrouwen.

Digitale authenticatie in platforms voor participatieve democratie moet de complexiteit van het begrip identiteit in de fysieke wereld kunnen faciliteren op een manier die individuele zelfbeschikking vergroot. De deelnemer moet niet worden geconfronteerd met een veelheid aan verschillende diensten op het gebied van authenticatie.

Van belang voor inclusieve platforms is dat alle relevante lokale actoren kunnen deelnemen onder gelijke voorwaarden en met gelijke zekerheden, rechten en plichten. Een invoering van een sleutel-infrastructuur voor ingeschreven ondernemingen bij KvK, vanzelfsprekend via een open en gratis index te gebruiken, is dringende noodzaak.

Stimulering en uitvoering van pilots en tests met niet-propriëtaire, innovatieve identiteitsmanagementoplossingen helpt de problematiek te onderzoeken en te relateren aan ontwikkelingen rond digitale identiteit in het algemeen, aan overheidsdienstverlening en aan toekomstige eID-oplossingen.

Referenties:

1. Overheidsclassificatie van betrouwbaarheid van authenticatiemiddelen, zie:
   https://www.forumstandaardisatie.nl/sites/default/files/atoms/files/HR-Betrouwbaarheidsniveaus-v3-2014.pdf
2. http://stemvanwest.amsterdam.nl
3. http://halloijburg.nl
4. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
5. https://www.decodeproject.eu
6. https://www.decidim.barcelona
7. https://gebiedonline.nl