Hoe creëer je online vertrouwen?

Rowdy Chotkan

April 2021

1 Introductie

Self-Sovereign Identity (SSI) wordt gezien als dé opvolger van digitale identificatie middelen. Rowdy Chotkan heeft in het kader van zijn Master scriptie hier onderzoek naar gedaan bij de Rijkdienst voor Identiteitsgegevens. In deze blogpost bespreekt hij wat dit concept inhoudt en wat jij er aan hebt.

2 Digitaal vertrouwen

Het Internet is ontworpen zonder een notie van vertrouwen. De technologie die wij *het Internet* noemen, is op zeer kleine schaal begonnen zonder directe gedachten van mogelijk misbruik. Met het gevolg dat elke online service zijn eigen identificatie mechanismen heeft ontworpen. Dit is dan ook een van de voornaamste redenen dat wij wel tientallen verschillende inloggegevens dienen te onthouden. Vaak heb je voor elke online dienst waarvan je gebruik maakt, aparte inloggegevens nodig. Dit is voor gebruikers niet alleen vervelend, maar kan ook een grote impact op bijvoorbeeld privacy hebben.

Online identificatie heeft al meerdere fasen doorgaan. Op dit moment zitten wij in, waarnaar de wetenschap refereert als, de derde fase van digitale identiteit. Deze derde fase wordt de *gebruikersgerichte identiteit* genoemd. De primaire elementen uit deze fase zijn *gebruikers toestemming* en *interoperabiliteit*. *gebruikers toestemming* houdt in dat de gebruiker zelf toestemming kan geven met wie zijn of haar gegevens worden gedeeld. *interoperabiliteit* houdt in dat zulke identificatiesystemen kunnen samen werken met andere diensten. Hoewel zulke systemen bestaan, wordt een groot deel van digitale identiteiten nog steeds gedomineerd door centrale partijen. Denk hierbij aan de knoppen op websites en apps als “Sign in with Facebook”. Aangezien zulke partijen commercieel zijn, kan privacy in het gering raken én kunnen zij geen legale digitale identiteiten verschaffen.

Qua privacy kunnen deze partijen nog meer over hun gebruikers leren door de koppelingen met andere diensten. Ook is het vaak nodig dat gebruikers voor extra zekerheid een kopie van hun identificatiebewijs of paspoort moeten verschaffen. Dit is nodig omdat het anders simpelweg niet mogelijk is om iemand

digitaal te kunnen identificeren op persoon. Maar het grootste gevaar zit in het machtsverschil: doordat deze commerciële partijen jouw identiteit beheren voor talloze services, hebben zij tevens de mogelijkheid om deze af te pakken. Het gevolg hiervan is dat jij mogelijk de toegang tot talloze services kwijtraakt, indien jij bijvoorbeeld iets tegen hun service-voorwaarden in doet.

3 De volgende stap

Om de hiervoor benoemde knelpunten te doorbreken, is er een volgende fase nodig. Deze fase wordt *Self-Sovereign Identity* (SSI) genoemd, wat letterlijk vertaald *zelf-soevereine identiteit* betekent. Het voornaamste principe achter SSI wordt reeds duidelijk uit de naam: de zelf-soevereine aard van SSI plaatst de gebruiker in het midden van zijn of haar digitale identiteit. Dit houdt in dat geen centrale partij—oftewel autoriteit—jouw identiteit in handen heeft, maar dat jij zelf de regie neemt. Over het algemeen worden de volgende tien principes aan SSI gelinkt:

- **Bestaan**: gebruikers bestaan los van elkaar. Een digitale identiteit is persoonsgebonden.
- **Controle**: gebruikers hebben controle over hun identiteit.
- **Toegang**: gebruikers hebben toegang tot hun informatie.
- **Transparantie**: systemen en algoritmes (speciale berekeningen over informatie) moeten open zijn. Dit houdt in dat het duidelijk is hoe zij werken.
- **Volharding**: identiteiten moeten langdurig zijn.
- **Draagbaarheid**: informatie over identiteiten moet draagbaar zijn. Dit houdt in dat zij nooit vaststaan bij een derde partij.
- **Interoperabiliteit**: identiteiten moeten met zoveel mogelijk systemen samen kunnen werken.
- **Toestemming**: gebruikers moeten toestemming geven hoe hun identiteit wordt gebruikt.
- **Minimalisatie**: er moet nooit meer informatie worden gedeeld dan nodig is. Dit met het oog op privacy.
- **Beveiliging**: de rechten van gebruikers moeten worden beschermd. Dit principe zorgt ervoor dat de gebruikers het belangrijkst zijn.

Uit deze principes wordt het duidelijk dat een digitale identiteit persoonsgebonden is. Deze identiteit dient volledig te worden beheerd door de gebruiker zelf. De gebruiker is dan ook het belangrijkste in heel het systeem. Tevens moeten de technologieën zogenoemde *open standaarden* hebben en kunnen communiceren

met andere systemen. Wij kunnen hieruit concluderen dat SSI gericht is op de gebruiker en niet op de diensten om men te identificeren.

Om een beter beeld te kunnen geven aan hoe zo een identiteit werkt, zullen wij eerst wat nodige concepten doornemen. Wij zullen nu eerst de termen *blockchain* technologie en *attesten* kort behandelen.

3.1 Blockchain

Om de macht van centrale partijen weg te nemen, is er een digitale infrastructuur nodig die niet rust op deze partijen. Daarmee bedoel ik het opslaan van informatie en de benodigde servers—een dienstverlenende computer die bij deze partijen beheerd zou worden. In de meeste ontworpen SSI systemen, wordt er gebruik gemaakt van zogeheten *blockchain* technologie. Blockchain technologie kan worden gezien als een groot opslag-mechanisme. Waarbij miljoenen computers het eens worden over wat voor informatie opgeslagen wordt. Dit opslaan gebeurt pas indien de meerderheid van de computers het eens is over de informatie. Elke computer slaat uiteindelijk dezelfde informatie op. Dit resulteert in een groot netwerk van machines die het eens zijn over dezelfde informatie. Een ieder kan potentieel deelnemen aan dit netwerk. Aangezien hier geen commerciële partijen voor nodig zijn, in combinatie met het vorige punt, maakt dat blockchain technologie uitermate geschikt om SSI te realiseren.

3.2 Attesten

Nu wij een manier hebben om data op te slaan zonder dat dit kan worden aangetast door centrale partijen, is er een manier nodig om digitale identiteiten te vertrouwen.

Een belangrijk aspect van SSI zijn zo genoemde *attesten*—oftewel getuigenissen. Het idee achter attesten is dat een bepaalde autoriteit, bijvoorbeeld de overheid, bepaalde informatie digitaal ondertekent. Hierna kan een ieder verifiëren dat deze informatie juist is, omdat de overheid deze heeft ondertekend. Dit is zichtbaar in Figuur 1. Hierin kun je zien dat een *Autoriteit* digitaal ondertekent dat Alice daadwerkelijk Alice is. Hierna kan Alice deze ondertekende digitale informatie doorsturen naar Bob, die vervolgens kan verifiëren dat Alice is wie ze zegt dat zij is. De verificatie kan plaats vinden door middel van speciale cryptografische berekeningen waardoor Bob kan verifiëren dat het ondertekend is door de *Autoriteit*.

3.3 De identiteit

Nu wij een manier hebben om zonder derde partijen informatie te kunnen opslaan en verifiëren, hebben wij de fundamenten van SSI. Indien overheden en andere partijen jouw informatie digitaal ondertekenen, kun jij zelf de baas blijven over jouw (digitale) identiteit. Immers staat het jou nu zelf vrij met wie jij deze data deelt. Jij hebt zelf de keuze om de data met Bob te delen of

niet. Ook kan een autoriteit niet meer jouw identiteit gemakkelijk afpakken, aangezien deze staat opgeslagen op bijvoorbeeld de blockchain.

4 Use-cases

Nu wij weten wat zelf-soevereine identiteit inhoudt, wordt het wellicht al duidelijk dat er veel meer mee kan worden gedaan dan het inloggen op een website. Het heeft de mogelijkheid om alle belangrijke informatie te digitaliseren en wereldwijd geldig te laten zijn.

Het inschrijven bij een buitenlandse universiteit kan bijvoorbeeld instantaan. Dit zou kunnen door een digitaal ondertekend eerder diploma en de digitaal ondertekende identiteit. Maar ook zaken als leningen aanvragen kunnen gemakkelijker. Zo kan bijvoorbeeld de waarde van je jaarlijkse inkomsten worden ondertekend door de belasting of nog openstaande schulden. Maar ook actuelere problemen als digitale COVID-19 vaccinatie-passporten. Dit zou triviaal zijn om met SSI te realiseren. Indien bijvoorbeeld de gehele EU de technologie aanneemt, is het simpel om een attesten voor COVID-19 vaccinaties te maken. Deze zouden dan gelijk in heel Europa verifieerbaar zijn.

Een geheel andere use-case voor SSI is het gebruik in derdewereldlanden. SSI kan ook een introductie voor identiteit in derdewereldlanden zijn. Door het gemis van valide identiteiten worden inwoners van zulke landen uitgesloten van bepaalde diensten. Dit wordt ook wel het gemis van *economische inclusie* genoemd. SSI kan men in derdewereldlanden een valide identiteit verschaffen. Hierdoor hebben zij een grotere kans om hun leven te verbeteren.

5 Tot slot

De technologie is er, echter wordt het nog niet toegepast. Hoe komt dat? Dit komt vooral doordat SSI op grote schaal moet worden gebruikt voordat het een reëel alternatief wordt. Naar mijn mening kan dit alleen gerealiseerd worden door de introductie vanuit overheden. Immers moet er een verifieerbare link zijn tussen een persoon en zijn digitale identiteit. Aangezien de overheid dit reeds bijhoudt, is het een logische stap dat jouw digitale identiteit ook door hen wordt ondertekend. Het grote verschil, natuurlijk, is dan dat zij niet jouw identiteit zal beheren. Zij zal deze alleen attesteren.

Gelukkig worden hierin op Europees niveau al vele stappen gemaakt. Er is reeds een framework voor SSI vanuit de Europese Unie gecreëerd. Ook vanuit Nederland worden hier actief stappen voor gezet. Dus wellicht is het voor ons allen binnenkort mogelijk om óók online vertrouwen te creëren.

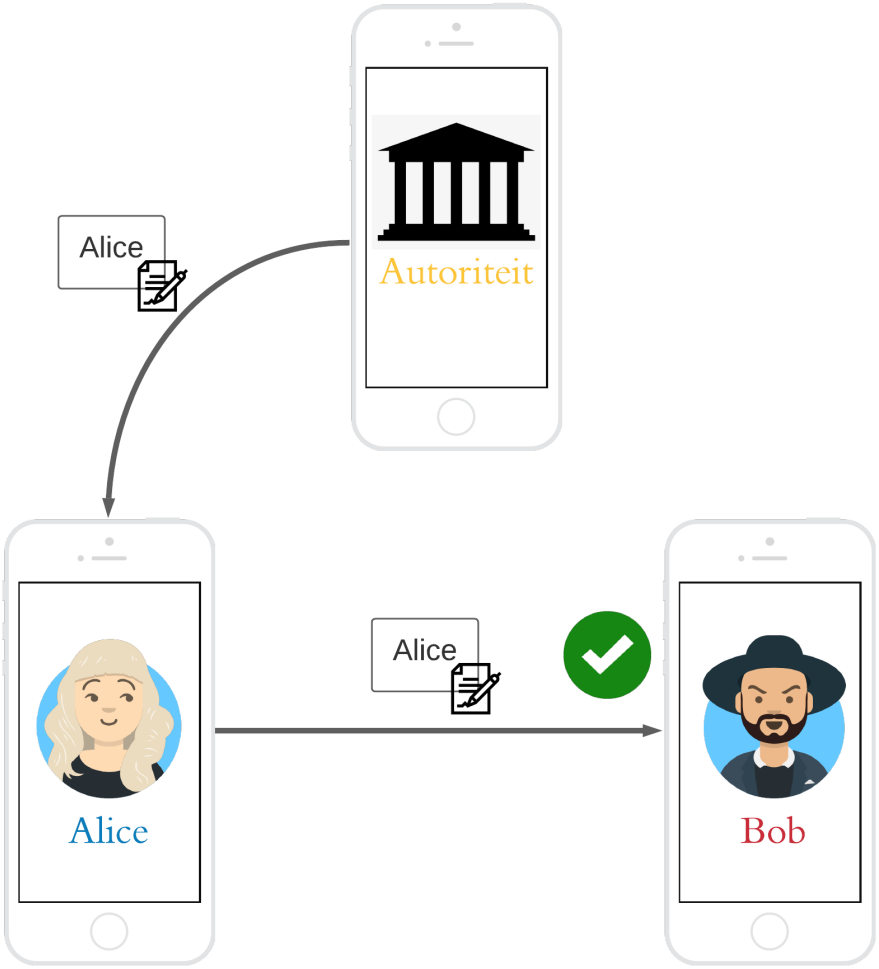

Figure 1: Attesten