Use-cases

Status:
Ter bespreking met de werkgroep op 17 april 2018.

1) De online kansspelaanbieders moeten eerst controleren of een speler is wie hij zegt te zijn en vervolgens controleren in een register of hij wel online mag gokken.

De kansspelaanbieders mogen geen gebruik maken van BSN. Hoe kunnen zij aan hun verplichting voldoen? Ook willen zij in principe niet weten wat de echte naam of woonplaats is van een speler: ze willen alleen aan hun wettelijke verplichtingen voldoen.
In ons model zou je het volgende pad moeten kunnen zien: de overheid stelt (bv. via DigiD) de identiteit vast van iemand die online wil spelen en maakt het mogelijk dat de betreffende burger de door de overheid verstrekte attributen kan verstrekken aan een kansspelaanbieder.
De online speler mag in het ideale geval best een fake-naam of adres verzinnen en hoeft geen BSN te verstrekken. Als hij maar kan aantonen, dat achter zijn spelers-identiteit een persoon schuil gaat die de Nederlandse overheid kent en die niet in een kansspel-register staat.
De online kansspelaanbieder moet echter wel fraude kunnen constateren: dat is ook in het belang van betrokken burger, bijvoorbeeld bij misbruik en identiteitsfraude. Zijn dat geen tegenstrijdige eisen?
Blockchain zou hier een rol in kunnen spelen: de speler plaatst een door hem zelf en de overheid digitaal ondertekende "geen probleem"-verklaring op de blockchain, die geraadpleegd kan worden door de partij die de speler daarvoor toestemming geeft. Als er een probleem wordt geconstateerd, zoals identiteitsfraude, kan, op basis van de digitale ondertekening, achterhaald worden wie wanneer die data op de blockchain heeft gezet, wat de herkomst is en wie de data heeft geraadpleegd.

2) In de bouwsector is de aannemer, die een bouwproject heeft aangenomen, verantwoordelijk, wanneer er mensen op de bouwplaats werken geen deugdelijke werkvergunning hebben en geen sociale lasten afdragen.

Er zijn veel onderaannemers bij bouwprojecten en vaak veel ZZP-ers. Ook uitzendbureau's en andere intermediairs brengen werknemers aan. Vaak worden buitenlandse werknemers ingevlogen, uit andere Europese lidstaten.
Identificatie , authenticatie en autorisatie (bv. toegang tot de digitale systemen op de bouwplaats) en de communicatie daarover, is een groot/kostbaar probleem: het identificatie-proces gaat nog grotendeels op papier en vindt iedere keer opnieuw plaats: er is geen mogelijkheden om de identificatie die een uitzendbureau heeft uitgevoerd, te

hergebruiken op de bouwplaats zelf. Bij een groot bouwproject zijn ondertussen talloze ordners gevuld met gegevens die moeten aantonen dat een werknemer mag werken.
Als een buitenlandse werknemer eerst een digitale identiteit moet aanvragen bij de overheid, ontstaan hoge kosten en ook wachttijden: een aanvraagproces duurt lang. Vaak heeft de overheid geen locatie in de buurt van de bouwplaats. Bovendien kan een onderaannemer of uitzendbureau, dat heeft vastgesteld dat een werknemer aan alle eisen voldoet, dat niet op een goede (dwz. met waarborgen op authenticiteit/integriteit) doorgeven aan andere partijen in de keten.
Een tweede aspect van de problematiek is de logistiek rond een bouwplaats: wie mag waar aanwezig zijn. Wie mag een bepaalde vrachtzending accepteren (en vaststellen dat de goederen aan de specificaties voldoen), of vaststellen dat iemand zijn werk goed heeft uitgevoerd.
Omdat dit soort zaken iedere keer weer opnieuw geregeld moeten worden, draagt het bij aan de faalkosten in de bouw.

In het architectuurmodel zou helder moeten worden op welke manieren en onder welke voorwaarden partijen elkaars checks rond identificatie en authenticatie mogen hergebruiken. Het gaat om het doorgeven van attributen met (digitale) echtheidskenmerken en gegevens die bewijzen dat een attribuut bij een fysieke persoon hoort. Bij incidenten moeten betrokkenen kunnen worden getraceerd.
Een zelfde probleem speelt in de landbouw en logistieke branche. In de logistiek mag een chauffeur een aantal ritten uitvoeren in een andere Europese lidstaat. Controle van de identiteit en zaken als vergunningen, (be)keuringen, rusttijden e.d. vergen ook identificatie. De logistieke sector heeft een eigen Europees identificatie-systeem.

3) In het onderwijs hebben kinderen recht op onderwijs, ongeacht de vraag waar ze vandaan komen en wie hun ouders zijn.

Onderwijs is een mensenrecht: omdat je kind bent, ook al ben je hier illegaal, heb je recht op onderwijs.
Kan het architectuurmodel het proces beschrijven waarin dergelijke kinderen een identiteit krijgen?

4) Webwinkels moeten voor verkoop van alcohol of bepaalde producten controleren of de klant 18+ is.

Fysieke winkels en bij bijvoorbeeld festivals (waar vele honderden mensen komen) moet dit ook. Tegelijkertijd is het niet nodig dat de winkel de naam van de klant registreert of de precieze geboortedatum.
Er zijn verschillende dienstverleners actief, die bijvoorbeeld een 18+ verklaring geven op basis van een scan en een aantal online controles van een identiteitskaart. De klant krijgt dan een kaart waarop staat dat hij of zij 18+ is, op basis van zijn identiteitskaart. Bij controle kan de verkoper van het product aantonen dat hij de controles heeft uitgevoerd, zonder allerlei persoonsgegevens te hoeven registreren en checks te hoeven doen.

5) IRMA, https://privacybydesign.foundation/irma/

IRMA staat voor I Reveal My Attributes (Bart Jacobs, Universiteit Nijmegen) en is een kaart (of telefoon) die (door de overheid) gevalideerde attributen verstrekt aan de partijen die gemachtigd zijn die attributen in te zien, zonder identiteit te onthullen. IRMA plaatst een geldigheidsduur bij het attribuut en, omdat een pincode vereist is, kan het attribuut niet anders dan bij de persoon horen die de kaart of de telefoon kan ontsluiten. Attributen worden geladen en voorzien van echtheidskenmerken, maar de server registreert niet wie wanneer welke attributen heeft gedownload en op welk middel. De ontvanger kan alleen die attributen inzien waartoe hij gerechtigd is, of een verklaring krijgen of een attribuut positief of negatief is.

Kan het architectuurmodel beschrijven hoe IRMA omgaat met sporen en of/waar IRMA een probleem heeft bij het signaleren en aanpakken van identiteitsfraude?
Kunnen volledige geanonimiseerde systemen (zoals IRMA) identiteitsfraude detecteren en aanpakken?

6) Gemeente Den Haag: hondenbelasting, https://formulier.denhaag.nl/Tripleforms/formulier/nl-NL/DefaultEnvironment/sc_08_Aangifte_Hondenbelasting.aspx/fIntro_08

De gemeente ontdekte dat veel burgers hun hond niet opgeven omdat ze hun DIgiD kwijt zijn. Daarom kun je in den Haag online aangeven dat je een hond hebt en belasting wilt betalen, ook zonder DigiD. Je geeft wel je adresgegevens op en uiteindelijk moet je ook nog een BSN opgeven op het aanvraagformulier. Maar je hoeft je niet met DigiD te identificeren. Als je maar betaalt (wellicht).
Ook bij de Belastingdienst is identiteit (misschien) minder belangrijk: als de belastinginkomsten maar kloppen. Wie betaalt doet er uiteindelijk niet toe. Wellicht dat vanuit fraudeopsporing identificatie wel belangrijk is.
Kan ons model deze situatie beschrijven?

7) NotarisID, https://www.knb.nl/nieuwsberichten/eerste-notarisid-uitgereikt-op-jaarcongres-notariaat

Notarissen hebben een hoog niveau eID ontwikkeld. Zij hebben wettelijk de mogelijkheden om een aantal daarvoor noodzakelijke controles uit te voeren zoals het controleren van de basisadministraties (bijvoorbeeld of iemand Nederlands staatsburger is, geregistreerde adresgegevens) en notarissen mogen/kunnen identificatie doen. De digitale NotarisID kan in de toekomst (is de bedoeling) in allerlei contexten gebruikt kan worden: voor online identificatie bij de bank, belastingaangifte, in de zorg, onderwijs. Maar wellicht ook voor allerlei overheidsdienstverlening (aanvragen van subsidies, sociale domein).
Kun je de NotarisID misschien op den duur gebruiken voor het online aanvragen van paspoort of identiteitskaart? Of voor het activeren van een SIM-kaart op je telefoon? En is deze eID in Europa geldig.
Het architectuurmodel zou op die vragen antwoord moeten kunnen geven.

Kan de NotarisID gebruikt worden om andere hoog-niveau eID's te activeren, zonder face-to-face controle?

8) QiY, https://www.qiyfoundation.org/

Qiy wil een portal ontwikkelen waarin mensen (gevoelige) gegevens kunnen beheren en gecontroleerd ter beschikking kunnen stellen aan derden. QiY waarborgt de authenticiteit en integriteit van data. Bijvoorbeeld (op den duur): wanneer adresgegevens recent door PostNL nog zijn bevestigd (omdat aan de betrokkene op dat adres een pakketje is afgeleverd) kun je die data via QiY aan een webwinkel verstrekken. Of wanneer iemand financiële gegevens verstrekt via QiY, is duidelijk dat die gegevens direct bij de betrokken bank vandaan komen. Ook kenmerken als leeftijd of werkhistorie kunnen op den duur via het QiY-portaal worden verstrekt.
QiY werkt nauw samen met pensioenwereld, energiesector, sociale verzekeringsinstellingen en banken: QiY verzamelt geen data, maar stelt de data-eigenaar in staat om data op te halen bij de bron (dat lijkt in elk geval de filosofie, maar er zijn ook andere berichten) en die data vervolgens te integreren en aan dienstverleners te verstrekken. Bijvoorbeeld met de vraag er diensten op te verlenen.

9) DigitalMe, https://digital-me.nl/digital-me/

Hier is nog geen use-case voor uitgewerkt, maar duidelijk is wel dat deze invalshoek verder verkend moet worden.

10) Self Sovereign Identities, https://sovrin.org/

Hier is nog geen use-case voor uitgewerkt, maar duidelijk is wel dat deze invalshoek verder verkend moet worden. Ook in relatie tot Blockchain.