Idensys lijkt op sterven na dood. Lang leve eiD?

September 11, 2018

Jaap-Henk Hoepman

1 Inleiding

De overheid is al jaren bezig met het invoeren van een nationaal elektronisch identiteitsstelsel (eID stelsel). Dit is belangrijk om een aantal redenen. Ten eerste wordt het steeds belangrijker om ook in de digitale wereld mensen betrouwbaar te kunnen identificeren. Ook is het niet fair dat in de fysieke wereld mensen moeten aantonen dat ze ouder zijn dan 18, terwijl de webshop dat niet hoeft te doen omdat ze dat niet *kan* doen. De vraag rijst dan of een paspoort of ID kaart ook voor digitaal gebruik geschikt gemaakt kan worden. Zo zou DigiD veiliger gemaakt kunnen worden. Tenslotte is de afhankelijkheid van DigiD een groot probleem: als DigiD uitvalt of gehackt wordt zijn alle digitale overheidsloketten waar burgers moeten inloggen onbereikbaar geworden.

Maar al die jaren is de overheid geen stap verder gekomen. Het laatste miljoenen project, Idensys, lijkt op sterven na dood. Na uittreden van een aanbieder zijn er nog maar drie aanbieders over, waarvan KPN tijdelijk geen middelen uitgeeft. Uit arren moede (zo lijkt het) is maar besloten om DigiD iets veiliger te maken door het uitbrengen van een DigiD app (ter vervanging van het steeds onveiligere SMS authenticatie). Alleen iDIN, het authenticatiemiddel van de banken, lijkt nog enig leven beschoren.

Maar een nationaal eID stelsel lijkt verder weg dan ooit. En dat terwijl de noodzaak alleen maar is toegenomen.

Naar mijn mening is Idensys mislukt omdat de overheid teveel aan de markt heeft willen overlaten. Voor succesvolle invoering van een nationaal eID-stelsel zal de overheid de regie moeten nemen. Maar dan rijst de vraag: welke keuzes heeft de Nederlandse overheid als het gaat om het invoeren van een nationale elektronische identiteit (eID)? Welke beslissingen moet de overheid nemen? En wat moet ze zelf doen, en wat moet ze aan anderen overlaten?

2 Kader

Een elektronische identiteit moet het Nederlandse burgers mogelijk maken om ook online hun identiteit (en wellicht meer eigenschappen over henzelf) aan anderen aan te tonen. Om helder te krijgen wat dit precies betekent moeten we aantal begrippen definiëren. Dus volgt eerst een korte uitleg over de belangrijkste begrippen in wat wel 'identity management' wordt genoemd.

Daarbij is het belangrijk om ons te realiseren dat we het hier over een zeer restrictieve interpretatie van het concept 'identiteit' hebben. We hebben het nadrukkelijk niet over de sociaalwetenschappelijke interpretatie van identiteit, of de expressie van iemands identiteit door middel van zijn of haar Facebook profiel, om maar eens een voorbeeld te noemen.

In de context van identity management is identiteit een verifieerbare eigenschap van een natuurlijk persoon die van belang is in de interactie tussen die persoon en een andere partij[1]. In de fysieke wereld is dat bijvoorbeeld de vraag of iemand zijn rijexamen gehaald heeft. In dit geval kan ik mijn rijbewijs gebruiken om dit aan een politieagent aan te tonen. Of is het de vraag wie ik ben. In dat geval kan ik mijn paspoort (of ook weer mijn rijbewijs) gebruiken om aan te tonen dat ik Jaap-Henk Hoepman heet.

Een *eigenschap* (ook wel attribuut genoemd) is een willekeurig kenmerk die een natuurlijk persoon zou kunnen betreffen, bijvoorbeeld naam, burgerservicenummer, leeftijd, kredietwaardigheid, lidmaatschap van het zwembad, toegang tot een Facebook account, etc.

Iemands identiteit is in deze context meer dan alleen zijn/haar naam, maar bestaat in feite uit de collectie van al zijn/haar eigenschappen.

Een *bewering* (ook wel claim genoemd) wijst, via een *identifier*, een bepaalde eigenschap toe aan een natuurlijke persoon. De bewering wordt gedaan door een *bron*. Een *identifier* is hier een unieke referentie die

[1] Soms worden systemen voor identity management ook gebruikt om de identiteit van niet-natuurlijke personen, of van computer systemen, vast te stellen. Denk bijvoorbeeld aan de public key infrastructure die is opgetuigd om de identiteit van websites met zekerheid vast te stellen. Maar dat valt buiten de scope van dit stuk.

naar een natuurlijk persoon verwijst. Dit kan een naam zijn (als die maar uniek is), een burgerservicenummer, of een pseudoniem[2].

Een bewering heeft dus altijd de volgende vorm:

(bron B) zegt dat (identifier I) de volgende (eigenschap E) heeft.

Een voorbeeld van zo'n bewering is een certificaat of diploma, waarmee een onderwijsinstantie (de bron) aangeeft dat een bepaalde met naam genoemde persoon (de identifier) de opleiding succesvol heeft afgelegd (de eigenschap). In het digitale domein is een zogenaamd attribuut certificaat een voorbeeld van zo'n bewering.

De bron is een persoon of entiteit die geacht wordt deze eigenschap te kennen en deze beweringen alleen te doen voor die personen waarvoor de eigenschap geldt. Zo kunnen vrienden beweringen doen over mijn betrouwbaarheid, de bank over mijn kredietwaardigheid, en de overheid over mijn leeftijd en staatsburgerschap. Mijn vrienden kunnen ook wel iets beweren over mijn leeftijd, maar dat is waarschijnlijk minder overtuigend dan als de overheid beweert dat ik ouder dan 50 ben.

Beweringen worden gebruikt door *acceptanten*, zoals online dienstaanbieders (die een naam willen weten), winkels (die de leeftijd van alcohol kopende klanten moet controleren), e.d. De *acceptant* bepaalt welke bronnen hij voor welke beweringen vertrouwt.

De *betrouwbaarheid* van de bewering wordt bepaald door

- de betrouwbaarheid van de bron (op welke manier deze controleert of de eigenschap van toepassing is),
- de betrouwbaarheid van het proces van uitgifte van de bewering (op welke manier de eigenschap aan de identifier wordt toegewezen), en
- de betrouwbaarheid van de *drager* waarop de bewering is vastgelegd (in hoeverre bijvoorbeeld de bewering veranderd kan worden door onbevoegden).

In het geval van een diploma gaat het dus om de betrouwbaarheid van de onderwijsinstelling (is dat het VMBO in Maastricht, Inholland, of de Radboud Universiteit ;-), de vraag hoe er voor wordt gezorgd dat de naam op het diploma overeenkomt met de persoon die daadwerkelijk gestudeerd heeft, en tenslotte of het diploma van de juiste handtekeningen en

[2] In een meer technische setting kan een identifier ook (de hash van) een cryptografische sleutel onder beheer van de natuurlijke persoon zijn.

stempels en echtheidskenmerken is voorzien (of dat het diploma in een online register gecontroleerd kan worden).

Om een vervolgens bepaalde eigenschap *aan te tonen* (hetzij aan een fysiek loket, dan wel online) moet een persoon een bewering kunnen overleggen die deze eigenschap aan hem of haar toewijst. Bovendien moet de persoon kunnen aantonen dat hij of zij de persoon is waar de bewering de eigenschap aan bindt.

De betrouwbaarheid van dit proces als geheel hangt (dus) af van

- de betrouwbaarheid van de bewering, en
- de mate van zekerheid of de bewering inderdaad deze natuurlijke persoon betreft.

In de fysieke wereld betekent de tweede eis dat je moet kunnen controleren of de persoon die voor je staat ook inderdaad diegene is waar de bewering naar verwijst. In het digitale domein betekent de tweede eis dat de website moet kunnen (laten) controleren of de persoon die op dit moment ergens met zijn of haar browser de website bezoekt inderdaad diegene is waar de bewering naar verwijst.

We hebben dus, naast een betrouwbare bewering, ook een betrouwbaar *authenticatiemiddel* (kortweg *middel* genoemd) nodig dat een natuurlijk persoon koppelt aan een identifier (en daarmee aan de beweringen over deze persoon). Zo'n authenticatiemiddel wordt gemaakt door een *uitgever* en heeft dus de vorm

> *(uitgever U) zegt dat (natuurlijk persoon NP) de volgende (identifier I) heeft.*

Een voorbeeld in het fysieke domein van zo'n authenticatiemiddel is een paspoort of identiteitskaart. In het digitale domein zijn wachtwoorden, biometrisch kenmerken, of smartcards voorbeelden van authenticatiemiddelen. Merk op dat vooral in het digitale domein waarin de uiteindelijke acceptant de persoon niet fysiek voor zich heeft staan, die koppeling tussen natuurlijke personen en identifiers niet zo sterk is: iemand kan er voor kiezen zijn smartcard met iemand anders te delen, of voor iemand anders te gebruiken. En sommige systemen voor identity management besteden deze controle uit aan (vertrouwde) derde partij.

Er kan overigens ook voor gekozen worden om een eigenschap direct aan een natuurlijke persoon te koppelen. Dan vallen de bewering en het middel samen en krijgen we iets van de vorm

(uitgever/bron UB) zegt dat (natuurlijk persoon NP) de volgende (eigenschap E) heeft.

Een voorbeeld hiervan is een toegangspasje voor het zwembad waar enkel de foto van de houder ter authenticatie op staat. (Ook het paspoort is hier overigens een voorbeeld van omdat dit onder meer ook de geboortedatum bevat).

Bovenstaand kader is belangrijk omdat we traditioneel de hierboven beschreven begrippen niet altijd duidelijk onderscheiden, wat tot verwarring kan leiden. Juist omdat in het digitale domein deze begrippen volledig los van elkaar (kunnen) bestaan.

Zo is een paspoort zowel een authenticatiemiddel als een drager van een bewering, en maken we dus geen onderscheid tussen de uitgever (van het middel) en de bron (van de bewering). Hetgeen zou kunnen leiden tot het misverstand dat dragers en authenticatiemiddelen onlosmakelijk met elkaar verbonden zijn.

Niet is minder waar! In het digitale domein kunnen het middel en de bewering los van elkaar bestaan. Ook kan een middel drager zijn van meerdere beweringen, die niet noodzakelijkerwijs door de uitgever van het middel gedaan worden. In de traditionele wereld kennen we hier overigens ook een voorbeeld van: papieren visa die bij uitgifte in het paspoort van de houder worden geplakt.

3 Keuzes

Gegeven dit kader kunnen we de volgende vragen stellen, waarop de Nederlandse overheid een antwoord moet geven. Waarbij zij dus een keuze moet maken.

1. Moet het eID stelsel voor publiek en/of privaat gebruik open staan? M.a.w. wie zijn de acceptanten?

   Mogen alleen publieke partijen, de overheid zelf dus, het eID stelsel gebruiken om veilige toegang te verlenen tot de digitale dienstverlening aan haar burgers? Of mogen ook private partijen hiervan gebruik maken?

   Vooral in dat laatste geval spelen privacy issues een rol. Bijvoorbeeld:

- hoe voorkom je 'overidentificatie' (dat je overal en nergens met je eID moet inloggen, en e.g. Facebook de eID gebruikt om haar real name policy af te dwingen), of
- hoe voorkom je dat burgers kunt volgen bij het gebruik van verschillende diensten, via een vaste identifier.

Ook maakt privaat medegebruik het stelsel groter wat (vanwege een grotere kans op incidenten) kan leiden tot een lager vertrouwen in het eID stelsel. Daarnaast dreigt het risico dat vanwege de te grote groep stakeholders aan tafel de belangen te ver uit elkaar liggen en het wensenlijstje te groot wordt, waarmee het project dus onbeheersbaar wordt. Dit hebben we gezien bij Idensys.

2. Wie mag er allemaal beweringen doen? M.a.w. wie zijn de bronnen?

   Mag alleen de overheid beweringen doen (en is dat één overheidsdienst, of zijn dat meerdere onafhankelijke diensten)? Of mag een beperkte, vooraf bekende, verzameling van private partijen ook beweringen doen? Of is het een open stelsel waar (eventueel na ballotage) willekeurige bronnen bij aan kunnen sluiten die allemaal beweringen mogen doen?

   Ook hier geldt weer dat een groter stelsel tot een lager vertrouwen leidt, en de ontwikkeling van zo'n stelsel onbeheersbaar wordt vanwege de (te) grote groep stakeholders.

3. Hoeveel authenticatiemiddelen moeten er zijn? En wie mag er allemaal authenticatiemiddelen uitgeven?

   Is er maar één authenticatiemiddel, uitgegeven door de overheid? (Is dit überhaupt een taak van de overheid?) En wat als dat middel niet meer werkt, of gehackt wordt? Dan zou de volledige digitale dienstverlening die van dit middel afhangt stilvallen. En dat was nu juist één van de belangrijkste tekortkomingen van DigiD die we wilden herstellen. Of moeten er meerdere middelen zijn? Mogen die dan uitgegeven worden door publieke én private partijen? En is het dan de bedoeling dat burgers meerdere middelen bezitten?

   Belangrijk issue hier is de veiligheid van het hele systeem. Die staat of valt met de veiligheid van de authenticatiemiddelen. Die koppelen immers natuurlijke personen aan beweringen (en dus hun eigenschappen). Een zwak middel draagt het risico in zich dat iemand zich de eigenschappen van iemand anders kan toe-eigenen. Zogenaamde

gefedereerde systemen (waarbij verschillende partijen middelen uitgeven die door anderen geaccepteerd worden) zijn riskant.

Als alleen de overheid uitgever is dan zal er maar een beperkt aantal middelen zijn (ID, paspoort, rijbewijs). Echter...

4. Is de koppeling van traditionele identiteitsbewijzen en een elektronisch identiteitsstelsel nodig?

   M.a.w. is een ID kaart, paspoort of rijbewijs überhaupt noodzakelijk of gewenst als middel? Of moeten we eerder denken aan (een app op een) smartphone of USB token (zoals de YubiKey) als authenticatiemiddel? Merk op dat het erg moeilijk is om een fysiek paspoort te integreren in een online authenticatieproces, achter een PC of met je smartphone. Aan de andere kant geef je zo als overheid de controle over de (voor jou essentiële) authenticatie middelen uit handen.

5. Over welke eigenschappen moeten beweringen mogelijk zijn?

   Zijn we alleen geïnteresseerd in identiteit, i.e. eigenschappen zoals naam, burgerservicenummer, of (dienst specifieke) pseudoniemen? Willen we ook beperkte, vooraf beschreven, verzameling aan eigenschappen ondersteunen? Of moet op een willekeurig moment besloten kunnen worden dat beweringen over een nieuwe eigenschap nodig zijn? (Bijvoorbeeld: lidmaatschap van de Papiermolen, een zwembad hier in Groningen.)

6. Moet er onderscheid gemaakt worden tussen betrouwbaarheidsniveaus? Zo ja, welke?

   Idensys onderscheidde de volgende betrouwbaarheidsniveaus: basis, midden, substantieel, en hoog. (Een vergelijkbaar onderscheid wordt ook in internationale standaarden en de Europese eIDAS verordening gemaakt).

   Een hoog betrouwbaarheidsniveau is lastig te realiseren en dus kostbaar. En de vraag is of je veel verschillende niveaus naast elkaar moet laten bestaan: waarom zou je met een lager niveau inloggen als een hoger niveau beschikbaar is (en net zo makkelijk is).

7. Hoe privacyvriendelijk moet het eID stelsel zijn, en hoe garanderen we dat?

   Een alomtegenwoordig, nationaal, eID stelsel kan een grote bedreiging vormen voor de privacy, als het stelsel het mogelijk maakt om

iedereen overal te identificeren, en zo een extreem gedetailleerd profiel te maken van wanneer ieder van ons gebruik maakt welke digitale diensten.

8. Welke juridische kaders gaan er gelden? Wie is er aansprakelijk voor wat binnen het eID stelsel?

   Naar mate het eID stelsel toegang gaat verlenen tot steeds hoogwaardiger, gevoeliger, diensten (denk aan toegang tot je medische dossier, of je bankrekening), wordt de mogelijke schade als gevolg van incidenten ook groter. Wie is daar aansprakelijk voor? En wat betekent dat voor de kosten voor het (gebruik van het) eID stelsel?

9. In hoeverre sluiten we aan bij internationale standaarden, zoals FIDO? Hoe gaan we om met internationale afspraken en regels, zoals de eIDAS verordening?

10. En als laatste (juist omdat het zo belangrijk is): welke rol/speelruimte heeft de burger binnen het eID stelsel.

Welke keuzes kan de burger maken? Hoeveel controle, inzicht krijgt de burger over de constructie van en het gebruik van zijn 'identiteit'? (Sommigen noemen dit self-sovereign identity.)

Grof gesteld gaat het dus om de vraag hoe open het eID stelsel moet/kan zijn (gegeven bepaalde eisen m.b.t. veiligheid, beschikbaarheid en privacy), hoe sterk de rol van de overheid binnen dit stelsel is, en hoeveel vrijheid de burger krijgt in de constructie van zijn eigen 'identiteit'.

Meer over deze, en andere zaken, is overigens ook te lezen in een serie eerdere blog posts:

- The Identity Crisis (1): Membership vs Ownership
- The Identity Crisis (2): What is identity?
- The Identity Crisis (3): Trust
- The Identity Crisis (4): Security

Zie ook het wetenschappelijke paper waar deze serie blog posts op gebaseerd is:

- Gergely Alpár, Jaap-Henk Hoepman, Johanneke Siljee: "The Identity Crisis. Security, Privacy and Usability Issues in Identity Management".

4 Mijn voorkeuren

Welke keuzes zou ik zelf maken?

Gezien de geschiedenis, zou ik klein en simpel beginnen. Maar daarbij wel, voor zover mogelijk, al rekening houden met de mogelijkheid om door te groeien naar een groter, veelomvattender eID systeem.

Het eID systeem moet een substantieel of hoog nivo van betrouwbaarheid garanderen. En goede privacy bescherming is essentieel.

De overheid moet zelf het primaire authenticatiemiddel uitgeven. Dat kan geïntegreerd zijn in het paspoort of identiteitskaart. (Een rijbewijs is een rijbewijs en zou geen identificatiemiddel moeten zijn.) Het authenticatiemiddel moet fysiek zijn. Dat is vaak minder gebruikersvriendelijk, maar de enige manier om een hoog betrouwbaarheidsniveau te garanderen. Welke vorm er ook gekozen wordt, integratie in alle vormen van online gebruik zal lastig zijn (vanwege de grote diversiteit aan systemen die mensen gebruiken: PC, laptop, tablet, smartphone).

Ik zie geen rol voor andere, private, partijen als uitgever van authenticatiemiddelen. (Tenzij er een volledig onafhankelijk, open, platform ontstaat voor het doen en verifiëren van beweringen, zie onder.)

Naast puur identificerende gegevens (naam, BSN) zou het eID systeem ook een beperkt aantal eigenschappen moeten ondersteunen, zoals leeftijd en nationaliteit.

Qua gebruik in een private context zou ik onderscheid maken tussen

- het vaststellen van de identiteit met een hoge mate van betrouwbaarheid, vanwege juridische eisen (denk aan “know your customer” eisen die worden gesteld aan banken e.d.
- het vaststellen van eigenschappen met een lage mate van betrouwbaarheid, zoals het vaststellen of iemand ouder is dan 18 bij een online drankenhandel

Het gebruik van het eID stelsel voor het eerste zou ik alleen openstellen aan een beperkte groep, betrouwbare, private partijen. Het gebruik voor het tweede zou ik openstellen aan alle private partijen (die aan niet al te strenge toelatingseisen hoeven te voldoen), voor zover dat de privacy niet schaadt: m.a.w.: deze private partijen moeten kunnen aantonen dat ze de eigenschap inderdaad moeten kunnen vaststellen voor het aanbieden van de dienst.

Gekeken moet worden of ondersteuning van een beperkt aantal eigenschappen zodanig geïmplementeerd zou kunnen worden dat dit op een later moment opengesteld kan worden voor derden. Dan zouden ook andere partijen als bron van bepaalde beweringen geaccepteerd kunnen worden, en zou er een open platform voor het doen en verifiëren van beweringen kunnen ontstaan. Omwille van de algehele betrouwbaarheid van het hele eID stelsel kan het echter verstandig zijn dit open platform zo veel mogelijk los te zien van het strikt publieke stelsel met een hoog niveau van betrouwbaarheid.