VERTROUWEN EN AUTHENTICATIE

B.P.F. (Bart) Jacobs[1]

Weten met wie of wat voor persoon men van doen heeft, draagt in het algemeen bij aan het vertrouwen in de onderlinge omgang tussen personen en organisaties. In de digitale wereld heeft zich een eigen discipline ontwikkeld die zich richt op het beheren en controleren van identiteiten en eigenschappen van mensen, namelijk *identity management*. Dit is een onderdeel van mijn eigen vakgebied computerbeveiliging. De moderne mens komt, bewust of onbewust, dagelijks in aanraking met identity management, bij het inloggen op de eigen computer met een gebruikersnaam (en een wachtwoord), bij het lezen van een online krant via een *Facebook* login, bij het gebruikmaken van een bedrijfspas, of bij het contact opnemen met de overheid via DigiD. In dit artikel zal verkend worden welke aanknopingspunten er in het recht gevonden kunnen worden voor identity management. Deze verkenning is zeer beperkt en vooral anekdotisch van aard, maar richt zich op een onderwerp dat systematische juridische aandacht verdient, om de wet niet te ver uit de pas te laten lopen bij technische en maatschappelijke ontwikkelingen.

Identificatie en authenticatie

Ieder vak kent zijn eigen beroepsdeformaties. Zo diagnosticeren artsen of psychologen vaak hun medereizigers in de trein. Ook ik heb zo mijn eigen beroepsgerelateerde eigenaardigheden. Een jaar of tien geleden waren mijn vrouw en ik bij een notaris voor de aankoop van ons huidige huis. Op een goed moment vroeg de notaris – omdat de wet dit vereist – om onze identiteitsdocumenten. Na overhandiging van onze paspoorten vroeg ik de notaris of hij maar wilde bewijzen dat hij notaris is. De beste man keek mij eerst verbaasd aan, ging toen achterover zitten en staarde een minuut lang stilzwijgend naar het plafond. Toen merkte hij droog op "dat is een hiaat in de wet!", en vervolgde zijn werkzaamheden.

---

1 Prof. dr. B.P.F. (Bart) Jacobs is Professor of Software Security and Correctness, Sectie Digital Security, Institute for Computing and Information Sciences, Radboud Universiteit.

Binnen het vakgebied computerbeveiliging wordt onderscheid gemaakt tussen *identificatie* en *authenticatie*. Identificatie is *vertellen* wie je bent, bijvoorbeeld door het geven van je loginnaam of het tonen van je burgerservicenummer (BSN) of bankrekeningnummer (via je betaalpas). Authenticatie is *bewijzen* wie je bent, bijvoorbeeld door het geven van het juiste wachtwoord of de juiste PIN. Binnen identity management kan identificeren ook ruimer opgevat worden als het tonen van relevante persoonlijke eigenschappen (attributen), zoals het feit dat je notaris bent. Wat precies je 'identiteit' is, is complex en niet zo eenvoudig te tonen, maar 'attribuut' is een veel flexibeler en bruikbaarder begrip; dit wordt later verder uitgewerkt.

In een juridische context wordt het woord legitimeren vaak gebruikt voor identificeren. Bij de notaris moesten mijn vrouw en ik ons legitimeren, zodat de notaris onze identiteit vast kon stellen, maar hoefde de notaris zelf niks te bewijzen. Men spreekt van *one-way authentication*.

Ik gebruik het bovenstaande notaris verhaal soms in colleges bij het uitleggen van deze basisbegrippen. Ooit kwam een week daarna een student in de pauze naar me toe met het volgende verhaal. Hij woonde in een studentenflat waar de verwarming het de voorafgaande week begeven had. Er kwamen reparateurs over de vloer, die door hem aangesproken werden met de vraag: wie bent u eigenlijk? De mannen keken elkaar verbaasd aan en antwoordden: wij zijn van het installatiebedrijf. Waarop deze student keurig vroeg: kunt u dat ook bewijzen? Een van de mannen hief een bahco en riep: zal ik jou eens iets bewijzen!

Onze notaris had meer gevoel voor deze materie.

Volgens art. 2 van de Wet op de Identificatieplicht heeft eenieder van 14 jaar of ouder een toonplicht tegenover bijvoorbeeld een politieambtenaar – wanneer daar een goede reden voor is. Dit klinkt als authenticatie in één richting. Echter, in jurisprudentie is vastgesteld dat de toonplichtige van de ambtenaar mag verlangen dat die zichzelf eerst legitimeert.[2] Het kan wel carnaval zijn! Feitelijk is hier dus sprake van *two-way authentication*. Ik heb daar zelf praktische ervaring mee.

2 Zie bijv. www.rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/wie-mag-vragen-naar-mijn-identiteitsbewijs-en-wanneer.

Waarom is er sprake van het door onze notaris geconstateerde hiaat in de wet? Ik denk omdat de wetgever uitgaat van de gewone, niet-digitale wereld waarin de context van onze handelingen een belangrijke impliciete rol speelt bij authenticatie. Het tekenen van de relevante notariële akten vond plaats in een kantoor waarop het woord 'notaris' prijkt. Wij werden opgehaald uit de wachtkamer met de mededeling: de notaris kan u nu ontvangen. De betreffende persoon stelde zichzelf voor als notaris en gedroeg zich ook zoals je van een notaris verwacht. Echter, in de digitale wereld ontbreekt zo'n betrouwbare context. Zeker, op een webpagina kan ook 'notaris' staan. Maar zo'n tekst kan iedereen maken. De juistheid ervan is moeilijker te controleren. Net zo goed wordt een persoon met een witte jas in de context van een ziekenhuis snel gezien als lid van de medische staf. Evenzo dacht de wetgever bij het schrijven van de Wet op de Identificatieplicht waarschijnlijk dat het uniform van een politieambtenaar een voldoende betrouwbare context gaf om slechts een eenzijdige authenticatieplicht op te leggen.

Er zijn digitale technieken ontwikkeld om online, op het web, meer zekerheid te krijgen. De belangrijkste is het gebruik van 'https' in plaats van 'http' in de adresbalk van een webbrowser. De eerste afkorting 'https' eindigt met een extra 's' van 'secure'. Bij websites met 'https' is vaak een gedeeltelijk groene tekst zichtbaar in de adresbalk, met een gesloten slotje. Als u daar op klikt krijgt u cryptografisch gegarandeerde zekerheid over de herkomst van de website. Maar dat zegt nog niet heel veel. U weet nog steeds niet of bijvoorbeeld de informatie op www.thuisarts.nl daadwerkelijk van (deskundige, gekwalificeerde) artsen afkomstig is. Op dit inhoudelijke probleem wordt verderop nader ingegaan.

De juridische praktijk is opmerkelijk informeel, althans in mijn ogen. De strafrechter begint typisch met de vraag aan de verdachte: bent u inderdaad persoon X, geboren te Y op datum Z. De rechter is tevreden met een simpel 'ja'. De verdachte hoeft zich niet te authenticeren – en de rechter zelf trouwens ook niet. Er is voor bezoekers meer controle bij de ingang van de rechtbank – met scanners en controle van identiteitsbewijzen – dan voor verdachten tegenover een rechter. Ook zijn civiele rechters, bijv. in descente, snel tevreden met constateringen: u bent dus X en u bent Y.

Zwakke authenticatie leidt tot problemen: in 2006 rapporteerde[3] Grijpink dat 46 van 700 onderzochte gevangenen onder een valse naam vastzaten.

3 J. Grijpink, Identiteitsfraude en overheid, Justitiële verkenningen, jrg. 32, nr. 7 2006.

Kennelijk konden veroordeelden hun straf makkelijk door een ander laten uitzitten. Sindsdien is de identiteitsvaststelling in de strafrechtsketen verbeterd, bijv. met de invoering van het strafrechtsketennummer (SKN), zie art. 27b Wetboek van Strafvordering, ihb. lid 1: "Onze Minister van Veiligheid en Justitie kent aan de verdachte na de vaststelling van zijn identiteit een strafrechtsketennummer toe. (…)" Dit nummer dient (enkel) in de gehele strafrechtketen gebruikt te worden ter identificatie en dient geverifieerd te worden op "contactmomenten". Relevante gegevens worden opgeslagen in de strafrechtsketendatabank (SKDB).[4]

Met de uitvoering van het programma Kwaliteit en Innovatie rechtspraak (KEI) worden procedures in de rechtspraak stapsgewijs gedigitaliseerd. In het huidige kader ben ik vooral geïnteresseerd in de identiteitsvaststelling van de verschillende deelnemers. Die vindt elektronisch plaats via het webportaal[5] 'Mijn Rechtspraak' waar natuurlijke personen zich authenticeren met DigiD, bedrijven met eHerkenning en advocaten met een advocatenpas. Hierover schrijft Wefers Bettink:[6] "Deze identificatiemiddelen voldoen aan de vereisten die art. 3:15a lid 4 van het Burgerlijk Wetboek (BW) stelt aan de elektronische handtekening". Hier zien we dat niet alleen identificatie en authenticatie verward worden, maar ook dat aan authenticatiemiddelen eisen gesteld worden voor een elektronische handtekening – waarmee ook authenticatie en ondertekening verward worden.

Authenticatie en ondertekening

Zoals eerder genoemd draait authenticatie om *bewijzen* wie je bent. Ondertekening is wezenlijk anders. Een ondertekenaar committeert zich aan een bepaalde verklaring door het daaraan verbinden van een persoonlijk onderschrift: de wilsverklaring van art. 3:33 BW. De verklaring zelf wordt daarmee onloochenbaar. In het Engels spreekt men van *non-repudiation* (onloochenbaarheid) als belangrijkste eigenschap van een (al of niet digitale) handtekening. DigiD is een systeem voor authenticatie, en niet voor onloochenbaarheid. DigiD wordt daar echter wel vaak voor

4 Informatie over de praktijk is te vinden in: "Protocol identiteitsvaststelling (strafrechtsketen) 2013", zie: www.rijksoverheid.nl/documenten/brochures/2011/12/22/protocol-identiteitsvaststelling.

5 Zie de webpagina: www.rechtspraak.nl/Paginas/Inloggen-Rechtspraak.aspx.

6 In: H.W. Wefers Bettink, Digitalisering van de civiele procedure: gevolgen voor de procespraktijk, *Tijdschrift voor Civiele Rechtspleging*, 2015/1.

misbruikt, bijvoorbeeld door de Belastingdienst bij het afsluiten van de digitale belastingaangifte. Daar wordt de burger gevraagd zich nogmaals te authenticeren, hetgeen geïnterpreteerd wordt als ondertekening. In dit geval is er echter geen onlosmakelijke koppeling met de aangifte, hetgeen art. 3:15a lid 2 sub b BW van de elektronische handtekening vereist: "(…) zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord". Een kwaadwillende systeembeheerder of hacker zou de inhoud van de aangifte op enig moment kunnen veranderen, terwijl de vereiste extra authenticatie als losstaande handeling gewoon in het systeem van de Belastingdienst geregistreerd blijft.

Er zijn weliswaar al decennia lang elektronische technieken voorhanden voor het zetten van elektronische handtekeningen, met *private keys* en PKI-certificaten, maar van deze technologie wordt in de praktijk slechts beperkt gebruik gemaakt. De hoge kosten spelen daarbij een belangrijke rol. Ook is er discussie[7] over de precieze mate van controle die individuen moeten hebben, zoals in art. 3:15a lid 2 sub a BW vereist van de handtekening: "(…) zij is op unieke wijze aan de ondertekenaar verbonden". Authenticatie is in de praktijk belangrijker dan ondertekening en daardoor grootschaliger beschikbaarheid. Dat is echter geen argument om het een tot het ander te reduceren.

Identiteitsfraude en attributen

In het voorafgaande zijn situaties beschreven waar partij A zich authenticeert tegenover partij B, zodat partij B meer vertrouwen krijgt. Het is echter van belang ook de positie van de zich authenticerende partij A zorgvuldig te bekijken. Typisch onthult partij A enige gegevens (eigenschappen) van zichzelf om B te overtuigen. Hierbij maakt A zich kwetsbaar: de getoonde gegevens zouden door B misbruikt kunnen worden om zichzelf als A voor te doen. Ook kan een kwaadwillende die toegang weet te verkrijgen tot de relevante (authenticatie) gegevens identiteitsfraude plegen. Authenticatie door A vereist vertrouwen vooraf van A in B en in de gebruikte authenticatiemethode. Hiervoor zou B zich eerst moeten authenticeren. In de praktijk wordt dit kip-en-ei probleem doorbroken door de regel dat de sterkere partij zich eerst moet authenticeren. Dit

7 Zie: F. van den Broek en E. Poll, Digitale handtekeningen: nieuwe technologie & nieuwe wet- en regelgeving, *Privacy & Informatie*, 2014/1.

wordt toegepast bij het online inloggen bij een bank of bij de overheid (via https) of bij de toonplicht tegenover een autoriteit.

Identiteitsfraude is een van de grote plagen van ons digitale tijdperk. Het kost slachtoffers vaak grote moeite om schade hersteld te krijgen ("u was het toch zelf!") of om van een gecompromitteerde identiteit af te komen.[8] Kopieën van identiteitsbewijzen zijn vaak een bron van identiteitsfraude, omdat ze bijvoorbeeld gebruikt kunnen worden om een lening of een telefoonabonnement af te sluiten. Desondanks worden zulke kopieën in de rechtspraktijk veelvuldig gebruikt, bijvoorbeeld door notarissen.

In het vakgebied identity management is een zekere verbreding zichtbaar, van het gebruik van identiteiten naar het gebruik van attributen. Sommige attributen zijn identificerend, bijvoorbeeld een BSN of een bankrekeningnummer, terwijl andere attributen ook voor meerdere personen kunnen gelden, zoals 'man' of 'inwoner van Nijmegen' of 'hoogleraar burgerlijk recht' of 'rector'. In digitale vorm hebben zulke attributen een geldigheidsduur en zijn ze voorzien van een digitale handtekening van een uitgevende partij. Voor veel contacten en transacties zijn slechts enkele eigenschappen (attributen) van betrokkenen van primair belang. In het ziekenhuis is het voor mij van groter belang om te weten dat mijn behandelaar een gekwalificeerd geneeskundige is dan om diens precieze naam te kennen. Die naam is vooral nuttig voor beleefde communicatie en voor eventuele klachtbehandeling. Nieuwe attribuut-gebaseerde technologieën[9] bieden enige bescherming tegen identiteitsfraude omdat een identiteit niet gestolen kan worden wanneer slechts enkele niet-identificerende attributen relevant en vereist zijn, zoals 'ouder dan 16' bij het spelen van een online spel.

Attributen kunnen vertrouwen en zekerheden geven in de zich snel ontwikkelende digitale rechtspraktijk. De verschillende rollen (rechter, officier, advocaat etc.) kunnen vastgelegd worden als digitale attributen, en daarmee de basis vormen voor betrouwbare authenticatie. In de digitale wereld bestaat het onderscheid tussen *reputation* en *regulation*. Bij veel moderne diensten, zoals de veilingsite eBay of de taxidienst Uber,

8 Het bekendste slachtoffer van identiteitsfraude is Ron Kowsoleea, die in 2009 publiekelijk excuses kreeg van toenmalig minister van Justitie Hirsch Ballin vanwege de eindeloze onterechte controles en de trage correctie in justitiële systemen.

9 Deze attribuut-gebaseerde technieken zijn ook een onderzoeksonderwerp van mijzelf, in het bijzonder in het zogenaamde IRMA systeem.

worden aanbieders continu beoordeeld door gebruikers. Zo bouwen ze een reputatie op, waar andere deelnemers zich weer op baseren. Zulke *reputation-based* systemen kunnen in de praktijk goed functioneren en gebruikers voldoende vertrouwen geven. Bij een *regulation-based* aanpak moeten aanbieders op een of andere wijze 'gecertificeerd' zijn. Hier kunnen digitale (ondertekende) attributen de benodigde mate van vertrouwen en rechtszekerheid geven.

In zijn algemeenheid kun je stellen dat *reputation* tot meer gebruiksvriendelijkheid leidt dan *regulation*. Aanbieders die eenmaal 'gecertificeerd' zijn, behoren tot een eigen (gesloten, elite) groep en gedragen zich vaak arroganter dan aanbieders die continu door gebruikers beoordeeld worden. In zijn algemeenheid geldt ook dat Amerikanen opener staan voor *reputation* dan Europeanen. Wij zijn minder geneigd om het 'ware' of 'juiste' te vereenzelvigen met aantallen 'likes'. Het spanningsveld tussen deze twee aanpakken wordt zichtbaar wanneer traditioneel gereguleerde beroepen, bijvoorbeeld in het onderwijs of in de gezondheidszorg, blootgesteld worden aan beoordelingen: de 'professionals' uit deze sectoren houden daar vaak niet van. Ook zie je dat incidenten met zichzelf organiserende *reputation-based* aanbieders leiden tot ingrijpen van autoriteiten en tot afgedwongen *regulation*. Concreet: wanneer Uber taxi chauffeurs te veel brokken maken, zullen er competentie eisen komen.

Conclusies

In deze 'schets met een brede kwast' is beschreven hoe identity management in de rechtspraktijk traditioneel weinig aandacht kreeg – en misschien ook niet echt vereist was. Deze aandacht is wel toegenomen, door aangetoonde onduidelijkheden in de gevangenispopulatie, maar vooral door digitalisering van juridische handelingen. Daarbij wordt de technische terminologie (met name: identificatie, authenticatie, ondertekening) slechts in beperkte mate gevolgd, hetgeen tot misvattingen en onduidelijkheden aanleiding geeft. Ook is er vooralsnog weinig aandacht voor de risico's van het gebruik van authenticatiemiddelen (zoals kopie paspoort). Nieuwe ontwikkelingen, zoals formele vertrouwensgaranties via attribuut-gebaseerde authenticatie en informele vertrouwensopbouw via *reputation*, vragen om begrip en aandacht vanuit systematisch juridisch perspectief.[10]

10 De auteur dankt Ybo Buruma, Janita Hofman, Corjo Jansen en Tim Walree voor hun suggesties en commentaar.