COLUMN DAAN KALMEIJER

De Dikke Nora

De laatste tijd stel ik – bij wijze van experiment – aan al mijn cursisten de volgende vraag: "Wie heeft er in het afgelopen jaar een document van meer dan honderd bladzijden volledig doorgelezen?". En wat blijkt; velen kunnen zich niet eens herinneren wanneer ze voor het laatst zo'n dik document gelezen hebben – ikzelf ook niet. Allemaal ervaren en verstandige IT-architecten, projectleiders en IT-managers. Ze lezen gewoonweg géén dikke documenten. Een leuk leesboek van honderden pagina's is geen enkel probleem. Maar: elk projectplan, architectuurdocument, visiedocument,... wordt direct opzij geschoven zodra het dikker is dan een pagina of honderd. Mocht u nu bezig zijn met het schrijven van zo'n dik document; houd er maar rekening mee.
Tijd voor een dappere daad! Ik moest maar eens zo'n document gaan lezen. Hoe moeilijk is dat nu helemaal? Kom, het kost je maar een paar uur! Ik koos voor de NORA – de Nederlandse Overheid ReferentieArchitectuur. Je zou het bijna als je burgerplicht kunnen zien om die NORA een keer te lezen, het gaat tenslotte om onszelf als burger en om de manier waarop de overheid met ons wil omgaan. Nogal belangwekkende materie. Bovendien is de NORA 'door architecten en voor architecten', en daarmee blijkbaar ook voor mij bedoeld. De NORA is een pak papier van 283 pagina's. Van al mijn geënquêteerden hadden maar een paar personen de NORA volledig uitgelezen. Velen gaven aan dat "ze ongeveer wel wisten wat er in

We worden gegrepen door een visie, niet door richtlijnen en kaders

stond" – ze hadden het dus niet meer dan doorgebladerd. De NORA wordt ondertussen meegestuurd bij elke offerteaanvraag van een gemeente. Zouden de gemeenteambtenaren het wél gelezen hebben? "Wij voldoen ongeveer wel aan de NORA", is een veelgehoorde opmerking bij leveranciers van overheden. Hebben zij het gelezen?

Hierbij mijn verslag van het doorlezen van 283 bladzijden referentiearchitectuur. Allereerst zal ik het document zichzelf laten verklaren. Soms geeft een beetje statistiek veel inzicht: Het woord 'architectuur' komt gemiddeld twee keer per pagina voor. 'Principe' lees je op elke tweederde pagina. Woorden als 'afspraak' en 'regel' komen één keer per twee pagina's voor. 'Richtlijn' doet het ook goed. Aan de andere kant komt het woord 'visie' maar één keer per twintig pagina's voor. Wat mij betreft is dat een prima samenvatting van wat ik gelezen heb. Een grote verzameling zeer verstandige richtlijnen, normen en kaders. Helemaal niets tegen in te brengen. En toch is er iets mis. Van de eerste tot de laatste bladzijde wordt er uitgelegd hoe de 'elektronische overheid' beter en efficiënter moet, hoe overheidsinstanties beter moeten samenwerken via standaard afspraken en protocollen. Nergens wordt verteld hoe een 'elektronische overheid' ons leven gaat veranderen. Hoe gaan de democratie of de transparantie van overheden veranderen met een elektronische overheid? Wat betekent de elektronische overheid voor mijn verantwoordelijkheden, mijn integriteit, mijn veiligheid, mijn privacy? Problemen rondom vergrijzing en zorgkosten zouden een plaats kunnen krijgen in de elektronische overheid. Kortom, hoe gaat de elektronische overheid de wereld verbeteren?

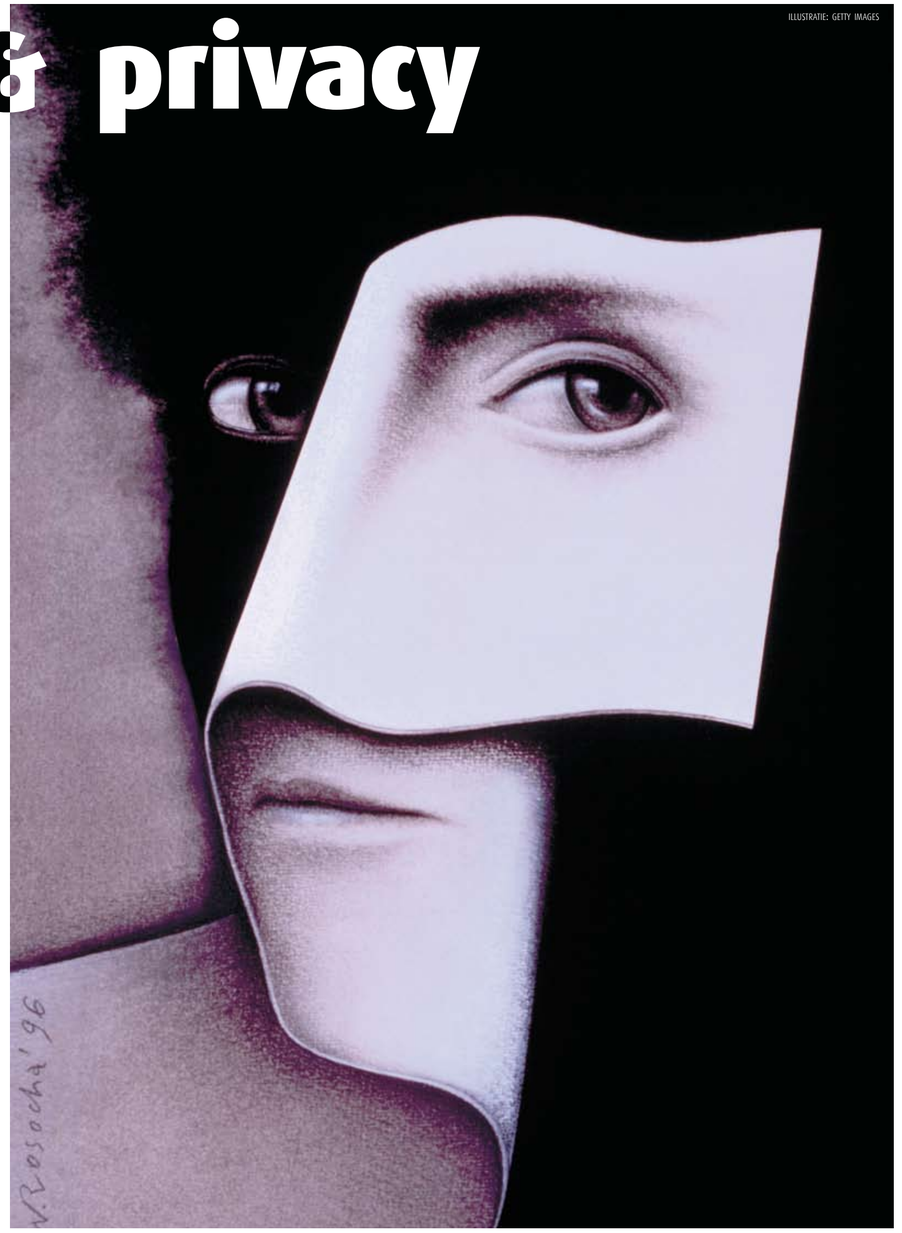
Misschien vindt u het een beetje overdreven, dat ik zou willen lezen hoe de elektronische overheid mijn leven ingrijpend gaat verbeteren. Het probleem is dat 'verstandige dingen', de NORA staat er bol van, ons gewoon niet genoeg boeien. Wij herkennen ons niet in 'verstandige dingen'. We worden gegrepen door een visie, niet door richtlijnen en kaders. Ik weet ook wel dat de makers van de NORA zich óók bezig houden met een heuse visie op de elektronische overheid – in aparte documenten. Maar, zolang die visie niet via elke bladzijde van de NORA aan mij opgedrongen wordt, blijf ik mij afvragen of dit wel de architectuur is waar ik achter sta. Ik ben bang dat gemeenteambten en leveranciers van die gemeenten ook zo in elkaar steken. Blijft buiten kijf dat de NORA gewoonweg verstandig is. Verstandig én dik. Daan Kalmeijer

Daan Kalmeijer is senior adviseur / docent bij DNV-CIBT.

Aanvraag- en activeringsproced ures zijn te zwak

DigiD & privacy

De Wet Bescherming Persoonsgegevens verplicht tot het nemen van passende maatregelen om persoonsgegevens te beveiligen. De bij DigiD getroffen beschermingsmaatregelen, zeggen **Bart Jacobs** en **Marc Jochems**, zijn onder de maat. De organisatorische maatregelen bijvoorbeeld bieden onvoldoende bescherming tegen identiteitsfraude.



ILLUSTRATIE: GETTY IMAGES

De publieke dienstverlening van rijk, provincies en gemeenten wordt steeds meer aangeboden via het internet, vanuit de 'Soft Sister'-rol van de overheid. Hierbij moet de burger zijn privacy deels opgeven ten behoeve van gebruiksgemak. Gaat het hier om gemak voor de burger of voor de overheid? Het opslaan en toegankelijk maken van persoonsgegevens (via één persoonsnummer) vergemakkelijkt namelijk niet alleen allerlei administratieve processen, maar ook koppelingen en toezicht van de overheid in haar rol als Big Brother, die de burger controleert.
DigiD (digitale identiteit) is de centrale authenticatievoorziening die door verschillende landelijke en lokale overheidsinstellingen wordt gebruikt. DigiD is een op Kerberos en A-select gebaseerd authentica-

Per post versturen van activeringscode biedt geen garantie

tiesysteem waarbij de authenticatiemiddelen zijn losgekoppeld van de toepassing waarvoor authenticatie vereist is. Deze middelen worden onderverdeeld in drie zekerheidsniveaus: basis, midden en hoog. Op het basisniveau maakt DigiD gebruik van een gebruikersnaam met wachtwoord. Het middenniveau behelst ook een eenmalige transactiecode (of wachtwoord) die wordt verzonden via sms naar de gebruiker. Het hoogste zekerheidsniveau moet in de toekomst worden ingevuld door de elektronische Nederlandse Identiteitskaart (eNIK). De overheidsinstelling die een bepaalde elektronische dienst aanbiedt, bepaalt zelf het bijbehorende zekerheidsniveau. Momenteel is dit in bijna alle gevallen het basisniveau. Vanaf 2008 gaat de belastingdienst gebruik maken van zekerheidsniveau 'midden' bij de vooraf ingevulde belastingaangifte.

Een omschrijving van privacy die aansluit bij artikel 10 van de Nederlandse Grondwet is: Privacy is het recht van een individu om te bepalen welke informatie over hem of haar mag worden verstrekt aan anderen. Privacy is noodzakelijk voor de verscheidenheid aan rollen die mensen vervullen in diverse sociale relaties. Privacy maakt het mogelijk informatie te beperken tot een bepaalde rol en is daarom ook van wezenlijk belang in situaties waarin men niets te verbergen heeft. Identiteitsfraude is een sterk groeiende vorm van misdaad waarbij iemand bewust en met kwade bedoelingen de schijn oproept van de identiteit van iemand anders. Identiteitsfraude is van alle tijden, zoals het gebruik van een vals kenteken of paspoort. Als gevolg van de toenemende elektronische interactie en opslag van persoonsgegevens in centrale databanken, vaak gekoppeld aan het internet, groeit identiteitsfraude sterk.
De Wet Bescherming Persoonsgegevens verplicht de verantwoordelijke, die bij elke verwerking van persoonsgegevens wordt aangewezen, tot het nemen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Bij DigiD zijn de getroffen beschermingsmaatregelen uitsluitend zogenaamde 'algemene PET-maatregelen'. Hiermee is onvoldoende krachtig gehoor gegeven aan de door de overheid zelf gestelde richtlijnen met betrekking tot het gebruik van Privacy Enhancing Technologies (PET). Binnen DigiD is het goed mogelijk gebruik te maken van effectievere vormen van scheiding van gegevens, waardoor informatie uit verschillende overheidsdomeinen moeilijker met elkaar te combineren zijn, zodat gegevens behorende bij verschillende rollen, die de mensen mogelijk gescheiden wensen te houden, ook daadwerkelijk gescheiden blijven.

De getroffen organisatorische maatregelen bieden onvoldoende bescherming tegen identiteitsfraude. Om een DigiD aan te kunnen vragen moet men beschikken over de juiste combinatie van een burgerservicenummer, geboortedatum, postcode en huisnummer. Adresgegevens kunnen doorgaans probleemloos worden gevonden in een telefoongids en ook een geboortedatum is vaak eenvoudig te vinden op het internet, bijvoorbeeld op netwerksites als hyves of myspace. Het burgerservicenummer is minder eenvoudig te verkrijgen, maar dit is niet onmogelijk. Door het groeiende gebruik ervan vermelden steeds meer organisaties, zoals de belastingdienst, werkgevers en zorgverzekaars, het burgerservicenummer in hun correspondentie. Bovendien staat dit nummer ook op paspoort, identiteitsbewijs en zorgverzekeringspas en wordt er in diverse alledaagse situaties gevraagd om één van deze documenten te tonen of af te geven, zoals bijvoorbeeld in het ziekenhuis, bij de tandarts, bij het inchecken in een hotel of bij het kopen van een telefoonabonnement. De door DigiD gebruikte aanvraagprocedure biedt daarom onvoldoende zekerheid over de identiteit van de aanvrager.
Hiermee wordt tevens de mogelijkheid tot een Denial of Service aanval geboden. Op het moment van aanvragen komt namelijk een eventuele reeds bestaande DigiD te vervallen en kan pas een nieuwe worden aangevraagd nadat de activeringscode is verlopen, twintig dagen na het versturen ervan.
Ook de activeringsprocedure is te zwak. Het per post versturen van een activeringscode biedt namelijk geen garantie dat deze de geadresseerde bereikt. Een onrechtmatige aanvrager die erin slaagt de activeringsbrief te onderscheppen heeft de beschikking over een DigiD waarmee hij zich kan voordoen als een ander persoon. De Postbank, die voor het internetbankieren een vergelijkbare aanvraagprocedure gebruikt, onderkent dit risico. Waar men in het verleden de gebruikersnaam, het wachtwoord en de activeringscode die hiervoor benodigd zijn alle per post verstuurde, in drie verschillende brieven, ontvangt de aanvrager tegenwoordig een bericht dat hij zijn wachtwoord kan komen ophalen op het postkantoor. Hij moet zich hierbij legitimeren.
Op het moment dat men onvoldoende zekerheid heeft over de identiteit van de persoon die een DigiD heeft aangevraagd en geactiveerd, biedt een hoger zekerheidsniveau geen enkele extra garantie over de identiteit van de gebruiker van de DigiD. Het mobiele telefoonnummer waarnaar de eenmalige inlogcode wordt verzonden is immers bij aanvraag zelf op te geven. Zekerheidsniveau 'midden' biedt dus ook nauwelijks extra zekerheid ten opzichte van zekerheidsniveau 'basis'. Iemand die erin slaagt de gebruikersnaam en het wachtwoord van iemand anders te bemachtingen – bijvoorbeeld via phishing of door onachtzaamheid of slordigheid van de betreffende persoon – kan hiermee sms-authenticatie aanvragen op een mobiel telefoonnummer naar keuze. Deze wordt weliswaar pas geactiveerd na invoering van een per post verstuurde activeringscode, maar hierboven is al aangegeven dat dit geen garantie biedt dat deze code de geadresseerde bereikt. Zolang de huidige aanvraag- en activeringsprocedures niet worden verbeterd, biedt een hoger zekerheidsniveau dus geen meerwaarde.

Bart Jacobs (bart@cs.ru.nl) is hoogleraar computerbeveiliging aan de Radboud Universiteit Nijmegen en aan de Technische Universiteit Eindhoven. Marc Jochems is pas afgestudeerd in Nijmegen als informatiekundige. Zijn scriptie 'DigiD en Privacy' is beschikbaar op: www.cs.ru.nl/onderwijs/afstudereninfo/scripties/2007/MarcJochemsScriptie.pdf.

Voor reacties en nieuwe bijdragen van deskundigen: h.ester@sdu.nl / 070-3780397

ZEKERHEID

Hoe werkt DigiD?

Alvorens een burger zichzelf kan authenticeren met behulp van zijn DigiD moet hij deze eerst aanvragen op de website van DigiD: www.digid.nl. Tijdens het aanvraagproces moet de burger een aantal verplichte gegevens invullen, namelijk zijn sofinummer, geboortedatum, postcode en huisnummer, evenals een gebruikersnaam en wachtwoord. Tevens heeft hij de mogelijkheid een huisnummertoevoeging, e-mailadres en een mobiel telefoonnummer op te geven. Vervolgens wordt in de landelijk raadpleegbare deelverzameling van de gemeentelijke basisadministratie gekeken of de combinatie van sofinummer, geboortedatum, postcode en huisnummer correct is. Zo ja, dan wordt per post een activeringscode verzonden naar de aanvrager. Na invulling daarvan op de website van DigiD is zijn DigiD bruikbaar.

Op dit moment zijn uitsluitend overheidsdiensten aangesloten, maar volgens de huidige wetgeving zou het voor private organisaties die een publieke taak hebben, mogelijk moeten zijn om gebruik te maken van DigiD, mits zij bevoegd zijn om het burgerservicenummer te gebruiken en te verwerken. Op het moment dat een burger kiest voor een overheidsdienst waarvoor authenticatie vereist is, wordt hij automatisch doorgestuurd naar de – met ssl beveiligde – website van DigiD en moet hij zijn gebruikersnaam en wachtwoord invoeren. Indien een burger zich authenticeert op zekerheidsniveau 'midden' dan moet hij tevens een eenmalige inlogcode, die hij per sms ontvangt, invoeren. Als hij alle gegevens correct invult, wordt hij teruggestuurd naar de overheidsinstelling en ontvangt deze het burgerservicenummer behorende bij de zojuist geauthenticeerde DigiD. Impliciet krijgt de overheidsinstelling ook de verzekering, te maken te hebben met de burger met dat burgerservicenummer. Op basis hiervan kan de overheidsinstelling besluiten de gevraagde dienst te verlenen. Op deze manier verloopt enkel de authenticatie door DigiD en blijven alle persoonsgegevens die nodig zijn voor de gevraagde diensten bij de betreffende overheidsinstelling.

VERIFICATIE

Drie aanbevelingen ter verbetering van DigiD

Allereerst is het binnen DigiD goed mogelijk de identificerende persoonsgegevens te scheiden per domein. Hiertoe dient een burger binnen DigiD te worden geïdentificeerd door een nieuw, uniek nummer, dat uitsluitend bekend is bij DigiD en de burger die eerdoor geïdentificeerd wordt. De overheidsdiensten die voor authenticatie gebruik maken van DigiD worden ingedeeld in verschillende sectoren, die elk een eigen sectoraal identiteitsnummer gebruiken om een burger te identificeren. Per sector is er één vertrouwde partij die zowel het algemene identiteitsnummer als het identiteitsnummer behorende bij de eigen sector kent.

Deze partij fungeert in de communicatie tussen overheidsdiensten en DigiD als tolk. Op deze wijze wordt het leggen van koppelingen bemoeilijkt en wordt de reikwijdte van eventuele identiteitsfraude beperkt. Op het belang daarvan is eerder ook door anderen gewezen: de hoogleraren Corien Prins (Tilburg) en Jan Grijpink (Utrecht).
Een tweede verbetering betreft de aanvraagprocedure. In de huidige situatie is deze gebaseerd op persoonsgegevens die relatief eenvoudig te verkrijgen zijn. In plaats hiervan kan men kiezen voor de combinatie van het nummer van een legitimatiebewijs (paspoort, identiteitsbewijs, rijbewijs of verblijfsvergunning) en de geldigheidsdatum ervan. Ook voor deze gegevens geldt dat externe partijen ze in handen kunnen krijgen, bijvoorbeeld wanneer zij bevoegd zijn te vragen om (een kopie van) het legitimatiebewijs, maar hier is aanzienlijk moeilijker aan te komen dan aan een burgerservicenummer.
Ten slotte dient de activeringsprocedure aangescherpt te worden. Bij dienstverlening aan het loket van een overheidsinstantie, moet een burger zich legitimeren door het tonen van zijn paspoort of identiteitskaart. Bij het aanvragen van een DigiD wordt wel gevraagd om een aantal identificerende persoonsgegevens, maar ontbreekt de verificatie met de pasfoto, zodat DigiD het qua betrouwbaarheid altijd zal afleggen tegen de traditionele manier van authenticatie. Een oplossing hiervoor is het versturen van een afhaalbericht voor de activeringscode in plaats van de code zelf.