

Zelf beheren identiteitsinformatie  
cruciaal.



Een privacyvriendelijke IDM oplossing vraagt niet meer dan nodig. Nu vragen veel dienstverleners vanuit een soort reflex vaak om gegevens die niet strikt noodzakelijk zijn om iemand te identificeren. Om je leeftijd aan te tonen bijvoorbeeld is je geboortedatum nodig, niet je naam en adres.

Voor de ontwikkeling van privacyvriendelijke IDM systemen waarbij de gebruiker centraal staat, is het van belang te weten wat de wensen van de gebruiker zijn, wat het begrip identiteit voor hem betekent en hoe hij daarmee omgaat. Hetzelfde geldt voor privacy: wat wordt onder privacy verstaan. Welke afweging wordt gemaakt tussen gemak, veiligheid en privacy? Met de komst van nieuwe technologieën zal de maatschappij blijven veranderen. Dit brengt ook verandering teweeg ten aanzien van het begrip en de verwachtingen over privacybescherming bij gebruikers. Dit heeft ook gevolgen voor de manieren waarop privacy wordt gereguleerd en de rol die aan de ene kant overheid en toezichthouder, en aan de andere kant bedrijfsleven en gebruiker innemen.

#### Conclusie

TNO ziet het als haar verantwoordelijkheid om overheid en dienstverleners te overtuigen dat het spanningsveld tussen privacy, veiligheid en gemak te overbruggen is. Het is mogelijk om hiervoor nieuwe concepten op technologisch en beleidsmatig gebied te ontwikkelen en bestaande en nieuwe methoden in de praktijk toe te passen.

#### TNO Informatie- en Communicatietechnologie

TNO Informatie- en Communicatietechnologie helpt overheden en bedrijven in uiteenlopende sectoren succesvol te innoveren. Dit kan een nieuw product of dienst opleveren, een compleet nieuwe werkwijze of een nieuwe strategische visie op de toekomst.

Marc van Lieshout

Brassersplein 2  
Postbus 5050  
2600 GB Delft

marc.vanlieshout@tno.nl  
www.tno.nl

T 015 285 71 25



# Privacy en identiteit in de informatiesamenleving



*Nu ICT vrijwel met alle facetten van ons leven verweven raakt, vervagen de grenzen tussen wat wij offline en online doen steeds meer. Hoewel we veel gemak hebben van de nieuwe diensten die ons worden aangeboden, laten wij zo ook continu en overal digitale sporen achter die meer impact op onze persoonlijke levenssfeer hebben dan we zouden willen.*

#### Privacy

Nieuwe technologieën als datamining, kunstmatige intelligentie en RFID creëren steeds meer mogelijkheden voor het verzamelen en analyseren van (persoonlijke) data. Aan de andere kant biedt diezelfde technologie ook nieuwe mogelijkheden om juist gebruikers meer zeggenschap te geven over hun identiteit en hoe, en aan wie, zij hun persoonsgegevens kenbaar willen maken. De vraag hoe privacy en identiteit in de toekomst vormgegeven en gewaarborgd kunnen worden, staat dan ook hoog op de agenda: in de media, de Tweede Kamer, bij bedrijven en overheidsinstellingen.

Het spanningsveld tussen privacy, veiligheid en gemak is te overbruggen.



## Maatschappelijke veiligheid

Ook maatschappelijke veiligheid staat, gevoed door de hedendaagse angst voor terrorisme en criminaliteit, hoog op de politieke agenda. Burgers verwachten een daadkrachtige overheid. Hierbij speelt ICT een cruciale rol, bijvoorbeeld door de mogelijkheid gegevens over burgers te koppelen en hun gedrag te monitoren. Dit gebeurt steeds meer d.m.v. inijkoperaties, tappen en dergelijke, zeker na de aanslagen in de VS op 9/11. De roep om telecomgegevens (ook internetverkeersgegevens) voor langere tijd op te slaan en te kunnen raadplegen bij incidenten vindt hier ook zijn oorsprong. Voorstellen voor maatschappelijke veiligheid staan echter op gespannen voet met de privacybescherming van de burger.

*ICT speelt een cruciale rol.*

### Het spanningsveld tussen security & privacy

Overheden en bedrijven willen enerzijds efficiënte en hoogwaardige diensten leveren. Anderzijds worstelen ze met de grote hoeveelheid gegevens en de bedreiging van de persoonlijke levenssfeer. We vinden dat de overheid door uitwisseling van gegevens tussen de gezinsvoogd, het Bureau Jeugdzorg, de Raad voor de Kinderbescherming en het Advies- en Meldpunt Kindermishandeling een drama als het overlijden van de kleuter

Savanna had moeten voorkomen, maar we worden boos als een politieagent onterecht in ons dossier snuffelt of een zorgprofessional dat zonder toestemming in ons toekomstig elektronisch patiëntendossier zou doen.

Het belang van privacy staat in deze discussie stelselmatig onder druk. Het recht op bescherming van de persoonlijke levenssfeer is bij wet vastgelegd. Maar dat is geen absoluut recht, zoals al te fanatieke privacybeschermers soms stellen. Die gedachte is net zo fout als de veronderstelling van security-adepten dat veiligheid boven alles gaat. De vraag is of een verhoging van de veiligheid altijd een aantasting van de privacy moet betekenen. En andersom, of iedere verbetering van de privacy altijd leidt tot een aantasting van de veiligheid. Volgens TNO is het zeer wel mogelijk om privacy en security tegelijkertijd te

## Het belang van privacy

verbeteren. TNO heeft de kennis en kunde in huis om beide aspecten goed in de architectuur van een ICT-systeem (bijvoorbeeld rekeningrijden, paspoortcontrole, identiteitsmanagement), te verankeren. Dit kan bereikt worden door middel van zogenaamde revocable privacy technieken. Systemen met revocable privacy verzamelen slechts (persoonlijke) gegevens van die gebruikers die *van te voren afgesproken* regels overtreden. Deze regels worden dus vooraf, in overleg, vastgelegd, en kunnen naderhand niet meer worden veranderd.

### Identiteit en identiteitsmanagement

Boeken bestellen, kleding kopen of het aanvragen van een vergunning bij de gemeente, en vele andere vormen van dienstverlening, gebeurt steeds vaker via het internet. Voor het verlenen van al deze online diensten speelt het elektronisch kunnen vaststellen en herkennen van de identiteit van de burger of klant een belangrijke rol; zo heeft bijvoorbeeld niet iedereen recht op een uitkering, of het recht om alcoholische drank te kopen. Voor innovatieve ICT-dienstontwikkeling in zowel de private als publieke sector, is een veilige, makkelijke en effectieve manier van identificatie van gebruikers dan ook essentieel. Het gebruik van identiteitsmanagement (IDM) oplossingen vormt dan ook een steeds belangrijker

onderdeel van onze informatiemaatschappij. Deze oplossingen zijn echter niet altijd veilig en vaak ook niet privacyvriendelijk. Bovendien richten ze zich vaak op authenticatie en autorisatie van gebruikers, en niet op het ondersteunen van het eigen beheer van allerlei identiteitsgegevens. Nog steeds moet een gebruiker bij iedere website opnieuw zijn naam en adresgegevens invullen en allerlei additionele gegevens opgeven die zijn identiteit uitdrukken.

### Visie

In onze visie is het mogelijk dat de gebruiker zijn identiteitsinformatie zelf beheert, en moet het identiteitsmanagementsysteem er zorg voor dragen dat deze informatie automatisch bij de juiste dienstverlener terechtkomt, natuurlijk alleen als de gebruiker daar expliciet toestemming voor geeft.