

Framing works! *Ident*

De CIO, de informatiemanager en de informatie-architect spelen een belangrijke rol bij het initiëren, stuwende waarde als men de juiste uitgangspunten kiest. Dit artikel behandelt die uitgangspunten met een verge-

Op het gebied Identity Management (IdM) bestaan verschillende raamwerken. Deze komen voort uit een visie van een productleverancier van IdM-hulpmiddelen (Microsoft), zijn opgezet door een samenwerkingsverband van bedrijven (Oasis), komen uit de universiteitswereld (zoals PRIME) of zijn gepubliceerd door informatiekundig ontwerpers en architecten (zie het kader 'iDNA'). In dit artikel worden een aantal van die raamwerken behandeld, waarna ze op punten worden vergeleken. Wat zegt het raamwerk over het delen van gegevens? Wie is de eigenaar van gegevens? Hoe gaat men om met overdracht van verantwoorde-

lijkheid? Het doel is te komen tot een aanbeveling: waar moet een Identity Management systeem aan voldoen om van (strategische) waarde te zijn voor een organisatie?

Voor de totstandkoming van dit artikel ben ik schatplichtig aan Pieter Wisse en Paul Jansen, die in mei 2006 hun paper 'Identity management distilled: a comparison of frameworks' publiceerden.¹ In dat paper wordt door hen onderzocht wat de strategisch politieke implicaties van diverse Identity Management raamwerken zijn.

In dit artikel wordt de volgende definitie van raamwerk gebruikt: "Een elementair denkbeeld dat aannames, concepten, waardes en richtlijnen vastlegt, en daarbij instructies geeft voor de implementatie." ² Een raamwerk kan daarmee gebruikt worden voor de selectiefase van producten die in een Identity Management project worden ingezet. Daarnaast is het nuttig als toetsingskader voor de visie op Identity Management en ter controle tijdens de ontwerp- en ontwikkelfase.

Opzet

Achtereenvolgens worden de raamwerken PRIME, de 'Laws of Identity', de BurgerServiceCode en iDNA behandeld, waarna ze op hoofdpunten worden vergeleken.³ In de kaders wordt ingegaan op de definitie van raamwerken, de verwarring rond éénmalige gegevensverstrekking en Identity Management in relatie tot het BSN.

Raamwerken: PRIME

De afkorting PRIME staat voor *Privacy and Identity Management for Europe*.⁴ Dit project is in 2004 gestart met

als doel een werkend prototype te beschrijven en te maken van een privacy-enhanced Identity Management systeem. De achtergrond van het project is te vinden in de toename van online diensten die op enige wijze om persoonlijke informatie van de gebruiker vragen.

Op dergelijke transacties is nationale en internationale wetgeving van toepassing. Het is echter niet eenvoudig om aan die wetgeving te voldoen. Goede hulpmiddelen (systemen) zijn noodzakelijk. Verder onderkent PRIME het belang van persoonlijke gegevens. In hun visie wordt die omschreven als: "Personal data is an essential asset because it represents power. It is therefore essential to protect this asset to preserve the individual's autonomy."

De uitgangspunten voor het PRIME-systeem zijn tweeledig: enerzijds dient de gebruiker van een online dienst volledige controle over de persoonlijke levenssfeer (gegevens) te houden, anderzijds dienen de aanbieders van online diensten te voldoen aan de wettelijke vereisten. Door specifiek aandacht te besteden aan de client side en ook richtlijnen voor de gebruikers interface voor te schrijven, wordt geprobeerd het werken met persona's te vereenvoudigen.

PRIME vergelijkt deze manier van werken met de intuïtieve wijze waarop mensen in het dagelijkse leven met hun persoonlijke gegevens omgaan. Bijvoorbeeld de beslissing om de eigen naam te zeggen bij een ontmoeting. Het idee is dat een online systeem die intuïtieve manier van handelen op gelijksoortige wijze moet bevatten. In het kader 'PRIME' worden de ontwerp-principes van PRIME behandeld.

PRIME

De ontwikkeling van PRIME is betaald met geld van de Europese Unie en het Zwitserse Ministerie van Onderwijs. Aan het project zijn bedrijven als IBM, T-Mobile en Hewlett-Packard verbonden. Ook wordt door een aantal universiteiten medewerking verleend, zoals de Technische Universiteit Dresden, de Rotterdamse Erasmus Universiteit en de Universiteit van Tilburg.

De principes die PRIME hanteert zijn achtereenvolgens: 1) Het systeemontwerp dient te starten vanuit maximale privacy bescherming; 2) Systeemgebruik wordt nadrukkelijk gestuurd door privacy bescherming; 3) Navolging van regels voor privacy bescherming moet worden afgedwongen; 4) Privacybescherming moet te vertrouwen zijn; 5) Gebruikers moeten gemakkelijk en op intuïtieve wijze verschillende verzamelingen van privacy gevoelige gegevens kunnen gebruiken; 6) Privacybescherming dient een geïntegreerde aanpak te hebben; 7) Privacybescherming moet geïntegreerd zijn in applicaties.

PRIME presenteert een technisch architectuurontwerp voor een IdM-systeem dat holistisch is van opbouw.

Identity Management Frameworks

ren en ontwerpen van een Identity Management project. Een dergelijk project krijgt alleen strategische lijking van een aantal Identity Management frameworks of raamwerken. LEON KUUNDERS

Laws of Identity

Microsoft is de bekendste speler in automatiseringsland. Deze fabrikant van ICT-software (en inmiddels ook hardware) speelt alleen daarom al een belangrijke rol bij het ontwerpen en gebruiken van Identity Management systemen. Een bekend IdM-systeem dat Microsoft heeft geïntroduceerd is het Passport-systeem. Dit systeem was gebaseerd op het *one-size-fits-all* paradigma: als iedereen maar gebruik zou maken van Microsoft Passport dan werd het vanzelf succesvol en zouden de beloftes worden ingewilligd. Vreemd genoeg gebruikte nagenoeg niemand het systeem, waardoor Microsoft in januari 2005 besloot het niet langer te promoten.⁶

In mei 2005 werd door Microsoft's Kim Cameron de 'Laws of Identity' gepubliceerd.⁷ Deze richtlijnen voor het ontwerp van een IdM-systeem zijn het resultaat van uitgebreide discussies gevoerd met experts op het gebied van internet-technologieën en ICT-toepassingen. In deze 'Laws' vinden we ook de reactie op Microsoft Passport terug:

"Internet users saw Passport as a convenient way to gain access to MSN sites

[... but] it did not make sense to most non-MSN sites for Microsoft to be involved in their customer relationships [.. or to have ..] a single Microsoft identity service to be aware of all [users] Internet activities."

Passport mislukte omdat gebruikers én bedrijven niet gelukkig waren met de gedwongen relatie met Microsoft die voor gebruik van het systeem noodzakelijk was. De 'Laws of Identity' zijn bedoeld als ontwerprichtlijnen voor een Identity metasysteem. Zo'n systeem kan dan *de identity-laag* van het Internet vormen. Want het Internet, en dan met name het daar gebruikte netwerkprotocol TCP/IP, heeft als ontwerp-principe dat onbekend is met wie en wat een verbinding wordt gelegd. Die flexibiliteit heeft voordelen, maar voor bijvoorbeeld e-mail (spam) en gebruikersdiensten ook grote nadelen. Het resultaat is dat organisaties eigen oplossingen hebben ontwikkeld voor dit specifieke probleem. Zo heeft elke bank zijn eigen manier om internetbankieren veilig te maken. En hoewel ze bijna allemaal OTP's gebruiken (zie het artikel 'Afscheid van OTP tokens'⁸), komen die van verschillende fabrikanten en zijn niet wederzijds bruikbaar.

Een ander belangrijk punt dat in de 'Laws of Identity' wordt besproken is het verschil tussen 'claims' en 'assertions'. Een claim is een *betwistbare aanspraak op iets*, een *bewering*. In de context van de 'Laws' is dit bijvoorbeeld een aanwijzing voor een bepaalde identiteit, zoals een Windows-gebruikersnaam (bijvoorbeeld T-ID\Leon). Door de betwistbaarheid van de claim dient deze geëvalueerd te worden en bevestigd. Volgens de 'Laws' is er een groot ▶

Laws of Identity

De regels die door de 'Laws of Identity' worden gedicteerd zijn de volgende: **1) User Control and Consent** - De gebruiker bepaalt zelf welke gegevens worden gebruikt; **2) Minimal Disclosure for a Constrained Use** - Alleen de minimaal noodzakelijke identificerende gegevens worden gebruikt; **3) Justifiable Parties** - Uitsluitend partijen die binnen een transactie betrokken moeten zijn, worden erbij betrokken. Dus geen intermediair of identiteitenverschaffer die kan meekijken; **4) Directed Identity** - De digitale identiteit wordt niet rondgedeeld. De gebruiker deelt zijn identiteit alleen zelf mee aan een bepaalde ontvanger; **5) Pluralism of Operators and Technologies** - Iedereen kan zelf bepalen welk product of hulpmiddel wordt ingezet. Dat betekent dat een framework daadwerkelijk uit open standaarden moet bestaan; **6) Human Integration** - De mens maakt een ondeelbaar onderdeel uit van het metasysteem. Dat betekent dat er ook eenvoudige hulpmiddelen moeten bestaan om de mens bij het identificatieproces te ondersteunen; **7) Consistent Experience Across Contexts** - Het metasysteem moet eenduidig zijn. Het moet op ongeveer dezelfde manier werken bij zowel het browsen als het verwerken van transacties of chatten.²⁰

De regels zijn te interpreteren als normen. Een IdM systeem dat niet aan deze normen voldoet kan uiteindelijk geen succesvol Identity Management-systeem zijn.

▶ 1 Zie <http://primavera.fee.uva.nl/PDFdocs/2006-10.pdf>

▶ 2 Deze definitie is afkomstig uit de presentatie 'Modellen, Raamwerken en Methodes' http://leon.kuunders.info/ib-modellen-raamwerken-methodes_v2.pdf

▶ 3 Het ISO werkt aan een 'Framework for Identity Management' onder nummer 'ISO/IEC 24760' en richt zich daarmee op bescherming tegen misbruik van gegevens en privacy. Verder is het framework van de Liberty Alliance bekend. Voor de laatste: zie http://en.wikipedia.org/wiki/Liberty_Alliance.

▶ 4 Zie <http://www.prime-project.eu>

▶ 5 Het Latijnse woord 'persona' betekent masker, en wordt hier gebruikt als verwijzing naar de gewoonte om verschillende, mogelijk fictieve, persoonsgegevens te gebruiken.

▶ 6 Zie <http://www.zdnet.co.uk/comment/other/0,39020682,39183062,00.htm>.

▶ 7 Zie http://www.identityblog.com/?page_id=352.

▶ 8 Zie 'Afscheid van OTP Token', Infosecurity.nl nr. 3, oktober 2006 <http://leon.kuunders.info/InfoSec-3-2006-AfscheidOTPTokens.pdf>.

▶ 20 Voor de toelichting is gebruik gemaakt van de tekst op Wikipedia, zie http://nl.wikipedia.org/wiki/Laws_of_Identity

◀ verschil tussen claims en 'assertions', een term die bekend is uit de specificaties van SAML.⁹ Met die laatste term wordt een vaststaand feit bedoeld. In de wereld van het Internet, gedistribueerd en *loosely coupled*, zijn feiten echter niet voorhanden. *Trust but verify*, is het devies. Het kader 'Laws of Identity' bevat een overzicht van de richtlijnen, of wetmatigheden.

BurgerServiceCode

Door 'burger @ overheid' is in november 2005 de BurgerServiceCode v2.1¹⁰ uitgebracht. Deze code is bedoeld als

normeringskader voor digitale contacten tussen burger en overheid. De normen die in de code staan vermelden telkens een recht van de burger met de daarbij passende verplichting van de overheid. Het is een sympathieke poging om richting te geven aan e-overheid initiatieven die de achter ons liggende kabinetten met wisselend succes hebben gelanceerd. Het ontbreken van een gebruiksverplichting van deze normen maakt de naleving ervan wel erg vrijblijvend. Door de specifieke context - 'burger @ overheid' lijkt vaak op 'burger voor overheid', is het uitgangspunt, anders dan de naam doet vermoeden, niet des burgers. In het kader 'BurgerServiceCode' worden de normen genoemd.

Het iDNA manifest

Er is een groot verschil tussen de gebruiker van informatie, de beheerder van informatie, de distributeur van informatie en de informatie-eigenaar. Waar dit op andere vlakken goed is geregeld (bijvoorbeeld de auteurswet die het eigendomsrecht, gebruiksrecht

Verantwoord gebruik, Kwaliteit en Vertrouwensrelaties. In het kader iDNA manifest wordt iDNA gedetailleerder behandeld.

Vergelijking

Tussen de verschillende raamwerken zitten grote verschillen. Die zijn voornamelijk te wijten aan de context waarbinnen ze zijn opgesteld en de belangen die er mee worden gediend. Het meest opvallende verschil betreft het eigendomsrecht van persoonlijke gegevens. Drie van de vier raamwerken behandelen dit punt niet. Het iDNA manifest neemt het daarentegen als uitgangspunt, en verwoordt het op duidelijke wijze. Waar komt die verwarring, als het zo genoemd mag worden, rond eigendomsrecht vandaan? Waarom is het geen uitgangspunt van alle architecturen?

Over eigendomsrecht van persoonsgegevens schreef Henk Bos¹² in zijn boek 'Privacy begint in je genen' dat "rekening en regie begint bij het persoonlijk beschikkingsrecht van persoonlijke gegevens."¹³ "Het individu

BurgerServiceCode

De normen uit de BurgerServiceCode zijn de volgende: **1) Keuzevrijheid contactkanaal** - De burger kan zelf kiezen, de overheid stelt contactkanalen beschikbaar (balie, brief, telefoon, e-mail, internet); **2) Vindbare overheidsproducten** - De burger weet waar deze terecht kan, de overheid treedt op als één concern; **3) Begrijpelijke voorzieningen** - De burger weet onder welke voorwaarden er recht is op bepaalde voorzieningen, de overheid maakt die rechten permanent inzichtelijk; **4) Persoonlijke informatieservice** - De burger heeft recht op juiste, volledige en actuele informatie, de overheid levert die actief en gepersonaliseerd; **5) Gemakkelijke dienstverlening** - De burger hoeft gegevens maar één keer aan te leveren en kan gebruik maken van pro-actieve diensten. De overheid maakt inzichtelijk wat zij van mij weet en gebruikt mijn gegevens niet zonder mijn toestemming; **6) Transparante werkwijzen** - Als burger kan ik gemakkelijk te weten komen hoe de overheid werkt. De overheid houdt mij op de hoogte van het verloop van de procedures waarbij ik ben betrokken; **7) Digitale betrouwbaarheid** - Als burger kan ik ervan op aan dat de overheid haar digitale zaken op orde heeft. De overheid garandeert vertrouwelijkheid van gegevens, betrouwbaar digitaal contact en zorgvuldige elektronische archivering; **8) Ontvankelijk bestuur** - Als burger kan ik klachten of meldingen en ideeën voor verbeteringen eenvoudig kwijt. De overheid herstelt fouten, compenseert tekortkomingen en gebruikt klachten om daarvan te leren; **9) Verantwoordelijk beheer** - Als burger kan ik prestaties van overheden vergelijken, controleren en beoordelen. De overheid stelt de daarvoor benodigde informatie actief beschikbaar; **10) Actieve betrokkenheid** - Als burger krijg ik de kans om mee te denken en mijn belangen zelf te behartigen. De overheid bevordert participatie en ondersteunt zelfwerkzaamheid door de benodigde informatie en middelen te bieden.

Controle wordt verloren als eigendomsrecht op persoonlijke informatie niet is geregeld

en distributierecht voor informatie in woord, beeld en geluid regelt) ontbreekt dergelijke wetgeving voor de e-overheid. Dat het ontbreken van dergelijke wetgeving voor onduidelijkheid zorgt blijkt onder meer uit de discussies die in de Tweede Kamer zijn gevoerd over het burgeridentificatienummer BSN.¹¹

Als uitgangspunt voor de normen in dit raamwerk is het *eigendomsrecht van persoonsgegevens* gekozen. Dit uitgangspunt vinden we bij geen ander raamwerk terug. De normen uit het iDNA-manifest zijn verdeeld over vijf categorieën; Algemeen, Gebruiksrechten,

moet eigenaar worden van zijn gegevens. [...] Het individu heeft dus een soort auteursrecht of beeldrecht nodig over zijn digitaal portret. Voor het gebruik van de gegevens is de toestemming van de eigenaar nodig."¹⁴ Henk Bos is niet de enige die verwijst naar het beeldrecht in relatie tot persoonsgegevens. Voor hem zijn traditionele juridische concepten als 'eigendom' en 'privacy' voor het uitoefenen van controle te herleiden tot een vorm van 'toegang tot informatie', met *access- en use scenario's* tot gevolg.¹⁵ Het iDNA manifest kiest daar tegenover voor het

▶ 9 Zie <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.

▶ 10 Zie http://www.burger.overheid.nl/wat_wij_doen/burgerservicecode.

▶ 11 Zie daarvoor onder meer het becommentarieerde stenogram dat op http://www.cvib.nl/cvib-new/2006/09/jij_ik_en_het_b.php is te vinden.

▶ 12 Henk Bos is de architect van de informatiestrategie van gemeente Den Haag, zie zijn site <http://www.informatiehuis.nl/index.php?id=37> voor een overzicht van publicaties.

▶ 13 Zie 'Privacy begint in je genen - Cookies van eigen deeg voor de burger', ISBN 90-76249-86-5, november 2002, pagina 20.

▶ 14 Idem, pagina 58.

▶ 15 Idem, pagina 91.

◀ uitgangspunt dat zonder het regelen van het eigendomsrecht op persoonlijke informatie de burger de controle juist verliest. De redenering is dat goed beschreven toegangsregels (bijvoorbeeld door middel van RBAC) zonder eigendomsrecht holle frasen blijven.

Eigendom van persoonsgegevens is dus een ondergeschoven kindje in de raamwerken PRIME, Laws of Identity en BurgerServiceCode. PRIME noemt het wel maar slechts als moeilijk probleem¹⁶, de andere twee noemen het he-

lemaal niet. Zeker het ontbreken van dit onderwerp in de BurgerServiceCode is zorgelijk. Die code behandelt enkel het eigenaarschap van bestanden en dan alleen nog vanuit het oogpunt van een beheerder. Daarmee neemt het impliciet aan dat de overheid de eigenaar is van uw persoonsgegevens. In het kader over PIP is te zien waartoe dit leidt.

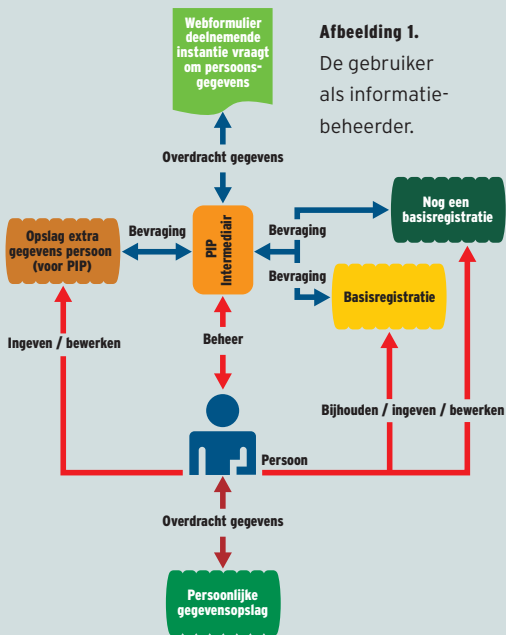
Waarom is eigenaarschap zo belangrijk? Wat voorbeelden om dit te verduidelijken, vanuit de context Identity- & Access Management: de beschermingslagen rond informatie stoppen bij de fysieke grens, in de regel de firewall met daarachter het Internet. Toegang tot die informatie is vervolgens (onder meer) afhankelijk van wie je bent. In organisaties is dat een *claim* die lokaal wordt gecreëerd. Normaliter gebruikersnaam en wacht-

Een ander voorbeeld betreft het gebruik van persoonlijke apparaten. Nu is dat veelal nog beperkt tot PDA's en *smart phones* en is het aantal medewerkers dat met de eigen laptop komt werken minimaal. Die laatste categorie bestaat meestal ook nog uit consultants die worden ingehuurd. Maar ook hier zien we snelle veranderingen. Techniek past in een vingerhoed en wordt meer en meer persoonlijk. Het afsluiten van het netwerk voor alles wat *niet in eigendom* is van de organisatie kan allang niet meer. Het is belangrijk om de implicaties hiervan te overdenken zodat dit de juiste weerslag krijgt in de Identity- en Access management infrastructuur.

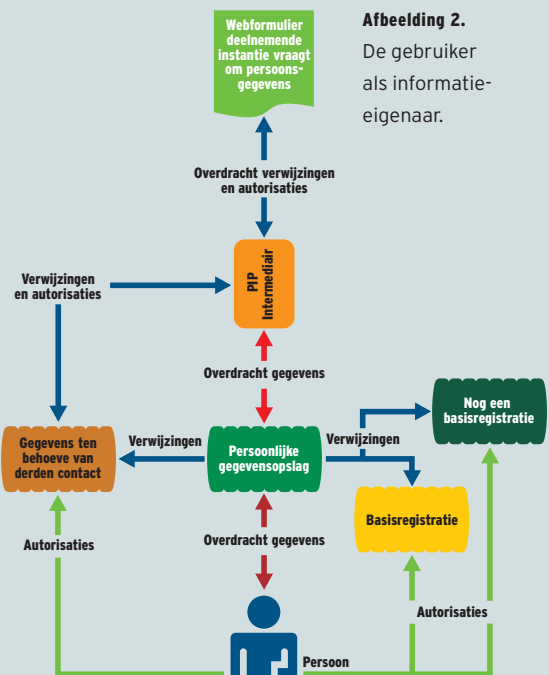
Rondom het *delen van gegevens* zijn de raamwerken specifiek. PRIME gaat daar uitgebreid op in en geeft

PIP versus iDNA

Afbeelding 1.
De gebruiker als informatie-beheerder.



Afbeelding 2.
De gebruiker als informatie-eigenaar.



In onsuccessvolle Identity Management projecten leren organisaties niet fietsen maar pleisters plakken

woord. Maar wat gebeurt er als een medewerker uit dienst gaat en weer in dienst komt? Of op contractbasis opnieuw wordt ingehuurd? Dit zijn alledaagse gebeurtenissen waarmee organisaties te maken krijgen. Nu gebeurt dat door netwerkaccounts aan te maken, te beheren, te wijzigen en in te trekken. Deze tussenlaag van accounts levert extra beheer op, terwijl het in alle gevallen persoonsgegevens zijn waarmee wordt gewerkt. Huidige Identity & Access Management systemen richten zich op het automatiseren van dit beheerproces. Ze plakken doorlopend leuke banden, maar leren de organisatie niet fietsen. In een omgeving waarin het eigendomsrecht van informatie goed is vastgelegd wordt de gebruiker zelf de leverancier van die *claim* en valt het verschil tussen medewerkers die in dienst zijn, uit dienst, of worden ingehuurd, weg. De gebruiker houdt het eigendom over de persoonsgegevens en geeft het *gebruiksrecht* aan de organisatie om een substraat ervan in te zetten voor de eigen systemen.

voorbeelden van concepten die rond het delen van gegevens van belang zijn. Het werken met persona's, subsets van (geanonimiseerde) data, is in de gebruikersinterface van PRIME ingebakken. Ook de 'Laws' is duidelijk en noemt controle over het delen van gegevens in haar eerste wet. De BurgerServiceCode bekijkt het 'delen' vanuit de moeite die het de burger kost om telkens dezelfde gegevens op een overheidsformulier in te vullen. iDNA is op het punt zeer duidelijk en geeft heldere normen voor de wijze waarop dit onderdeel moet worden ingericht. iDNA maakt daarmee effectieve controle op gebruik en misbruik van persoonsgegevens mogelijk. Met het iDNA raamwerk creëert men ruimte voor een transactie-gerelateerd factureringsmodel.

Rond het *overdragen van verantwoordelijkheden* schrijft iDNA onder meer een kwaliteitsnorm voor: als een persoon gebruiksrecht heeft verleend op informatie en een signaal krijgt dat die informatie niet correct is, dan be-

◀ 16 Zie v1.0 van het "Framework V2 for the PRIME project."

◀ staat de verplichting die informatie te verbeteren. De andere raamwerken gaan niet in op het overdragen van verantwoordelijkheden, anders dan met betrekking tot de zorgvuldigheid waarmee gegevens behandeld dienen te worden.

iDNA manifest

De normen uit het iDNA-manifest zijn onderverdeeld in vijf categorieën: Algemeen, Gebruiksrechten, Verantwoord gebruik, Kwaliteit en Vertrouwensrelaties. De eerste categorie **Algemeen** bevat één norm, die meteen het belangrijkste onderscheidingspunt ten opzichte van de andere normen en kaders is: 1.1. Informatie over de individuele (rechts)persoon is eigendom van diezelfde (rechts)persoon.

De categorie **Gebruiksrechten** bevat vijf regels: 2.1 De persoon kan gebruiksrechten op zijn persoonsinformatie verlenen aan andere partijen in maatschappelijk verkeer; 2.2 De persoon bepaalt in een overeenkomst voor een specifiek gebruiksrecht ofwel informatiemachtiging tenminste a. de andere partij; b. het gebruiksdoel en; c. de deelverzameling van persoonsinformatie; 2.3 Tot een gebruiksrecht kan behoren dat de andere partij beheer voert over – een afschrift van, ongeacht het medium – persoonsinformatie; 2.4 Verleende gebruiksrechten zijn onlosmakelijk onderdeel van persoonsinformatie; 2.5 Een overheidsinstelling krijgt een gebruiksrecht niet onmiddellijk door de persoon verleend. Dat gebruiksrecht is bij wet vastgesteld.

In de categorie **Verantwoord gebruik** zijn de regels terug te brengen tot: 3.1 Recht van inspectie en beheer; 3.2 Verantwoording per transactie in een vastgestelde rapportagetermijn; 3.3 Verantwoordingsplicht over het beheer; 3.4 Verantwoordingsplicht voor een overheidsinstelling is bij wet vastgesteld. Daarna volgt in **Kwaliteit**: 4.1 De persoon is verantwoordelijk voor de kwaliteit van informatie waarop verleende gebruiksrechten betrekking hebben; 4.2 Op melding door de andere partij van foutieve persoonsinformatie is de persoon verplicht tot correctie per omgaande.

Tenslotte handelt **Vertrouwensrelaties** over: 5.1 Beperking beschikkingsrecht van de persoon over eigen persoonsinformatie kan – met het oog op voldoende waarborg voor maatschappelijk verkeer – beperkt zijn. Zulke beperking heeft altijd een wettelijke grondslag; 5.2 De persoon wijst zijn vertrouwenspartij aan voor beheer over bedoelde informatie. Zo'n vertrouwenspersoon is voor die intermediaire rol gecertificeerd (als neerslag van vertrouwen in maatschappelijk verantwoord optreden in die rol); 5.3 Bij handelingsonbevoegdheid van de persoon zelf vervallen de rechten en plichten aan de wettelijke vertegenwoordiger(s) van die persoon.

Een voorbeeld: PIP

Door ICTU wordt op dit moment gewerkt aan de Persoonlijke Internet Pagina (PIP).¹⁷ Deze website moet als informatiemakelaar voor overheidsgegevens en transacties gaan dienen. Gebruikers zijn burgers, privé en zakelijk. Bij de beschrijving van de functionaliteiten van PIP wordt uitgebreid verwezen naar de BurgerServiceCode. Een achterliggend concept is de 'digitale kluis', zoals deze door Berenschot in april 2004 werd beschreven.¹⁸

PIP is eigenlijk een website zonder inhoud. De PIP is ook een webservice. PIP integreert diensten en gebruikt gedistribueerde opslag, PIP ondersteunt het aanmaken en toekennen van taken. In PIP kan de gebruiker extra gegevens opslaan, die derden geautoriseerd kunnen bekijken. Voor de dienstverlening is ze afhankelijk van de aangesloten bronnen en webservices. Die bronnen zijn (op termijn) onder meer de basisregistraties. PIP gebruikt DigID als *authenticatiehub*.¹⁹

In het volgende voorbeeld wordt aangetoond hoe de werking van PIP kan wijzigen indien het iDNA-raamwerk als ontwerpuitgangspunt wordt genomen. Om PIP te kunnen gebruiken moet PIP gegevens kunnen distribueren. Die worden gehaald uit

base. Maar dit proces kan ook anders (zie *afbeelding 2*). Ditmaal zien we de persoon als een informatie-eigenaar, die gebruiksrechten verdeelt om persoonsinformatie te gebruiken.

De persoon deelt autorisaties uit aan verschillende instanties om bepaalde persoonsgegevens te gebruiken. De gegevens worden niet gedistribueerd, alleen de verwijzing ernaar en de autorisatie, het gebruiksrecht. Op die manier wordt de eigendom van persoonlijke informatie als basis genomen voor het systeem. Aan de lezer de vraag: welk systeem is efficiënter?

Conclusie

De verschillende raamwerken hebben ieder hun eigen toegevoegde waarde. Ze kunnen dan ook voor specifieke doeleinden ingezet worden. Een combinatie van meerdere raamwerken is een krachtiger leidraad dan een enkel raamwerk. Door hun verschillende achtergrond kunnen ze (ten dele) in verschillende fases van een IdM-traject worden gebruikt om *visie, ontwerp, ontwikkeling* en *beheer* te toetsen. Directe toegevoegde waarde is in de visie/initiatie-fase te halen uit iDNA, in de ontwerp fase uit iDNA en PRIME, tijdens het managen van ontwikkeling en beheer uit de 'Laws

In onsuccesvolle Identity Management projecten leren organisaties niet fietsen maar pleisters plakken

aangesloten diensten als de DigID-database, de basisregistratie of de GBA. De PIP maakt van de gebruiker daarmee een informatiebeheerder. In afbeelding 1 is te zien dat er ook diverse informatie-eigenaren zijn: de basisregistraties, PIP, de deelnemende instantie en de persoon. De persoon beheert via de PIP interface de aangesloten bronnen en vergelijkt die gegevens met die uit de eigen data-

of Identity' en in wat mindere mate uit de BurgerServiceCode. De raamwerken zijn dus zinvolle hulpmiddelen voor een IdM traject. Gebruik ze dus, en zet ze in op die momenten dat het kan.

Leon Kuunders (leon@nedidm.nl) is Senior Identity Management consultant bij NedIDM, een onderdeel van de NedSecure Group.

▶ 17 Zie v1.0 van het "Framework V2 for the PRIME project."

▶ 18 Zie <http://www.e-overheid.nl/sites/pip/>

▶ 19 Zie <http://www.minbzk.nl/contents/pages/960/digitalekluisberenschot.pdf>

▶ 20 Deze informatie is afkomstig uit het globale ontwerp van PIP.

▶ 21 Meer daarover in het artikel 'De CD rom voorbij', Infosecurity.nl nr. 3, oktober 2006, <http://www.lar-gos.nl/docs/Identity%20Management%20-%20De%20CD%20voorbij.pdf>

IdM en administratieve lastenverlichting

In discussies over administratieve lastenverlichting wordt eenmalige gegevensverstrekking gezien als een wondermiddel. Burgers en bedrijven hoeven nooit meer twee maal dezelfde gegevens opnieuw op te geven bij contact met de overheid. Als de éénmalige gegevensverstrekking is ingevoerd dan komt alles goed, zo beweren de heren en dames politici. Het project heeft alleen nog een druppeltje Haarlemmerolie nodig, in de vorm van een algemeen identificatienummer. Doelstelling is daarmee een betrouwbare sleutel voor bestanden op te bouwen; met een compleet overzicht van alle identificeerbare personen en objecten als gevolg.

Nu is dat voor een organisatie een zeer valide doelstelling. Er zijn meerdere argumenten aan te dragen voor zo'n administratie, niet in de laatste plaats de verwachte betere controle op naleving van de Wet Bescherming Persoonsgegevens en het Informatiebeveiligingsbeleid. Maar het opzetten van zo'n administratie is geen sinecure. De algehele betrouwbaarheid van gegevens neemt af naarmate ze uit meer bronnen afkomstig zijn. Cijfers uit een project bij een van de grootste ministeries van Nederland laten dat zien: de centrale adresgids bevat 4000 medewerkers meer dan de centrale HR-database die op zijn beurt slechts 30% van de gebruikersobjecten bevat die in de directory's zijn opgenomen. Wie en wat hoort bij wat en wie? Het opzetten van een betrouwbare identiteitenadministratie en het invoeren van Identity Management is dus een hele klus. Het vraagt om integratie van techniek en organisatie en verandering van mensen en processen.²¹

De gedachte dat de Nederlandse overheid als één concern dient op te treden lijkt aantrekkelijk. In de BurgerServiceCode wordt daar zelfs expliciet aan gerefereerd. Dit is om verschillende redenen wel erg simpel gedacht, ook in relatie tot eenmalige gegevensverstrekking. Want het proces waarmee dat moet worden bereikt is lang en moeizaam en vraagt om veranderingen in die hele overheid, in alle processen, bij alle ambtenaren. In verkiezingsprogramma's wordt al tientallen jaren geroepen om veranderingen bij de overheid. Het geeft te denken over de te verwachten doorlooptijd van een dergelijk project.

Daarmee zijn direct de grootste bezwaren tegen dat concerndenken zichtbaar. Als eerste weten we namelijk niet wat de toekomst ons brengt. Een algemeen identificatienummer heeft als nadeel dat het voor algemene identificatie gebruikt gaat worden. Ook waar en wanneer dat niet wenselijk is. De geest kan dan echter niet meer terug in de fles. Ten tweede zit niemand te wachten op een project zonder einde. Dat soort sprookjes horen thuis in de Efteling en niet op de rijksbegroting.



gevraagd

Consultants

Ter versterking van ons team, zoeken wij ervaren consultants. Je bent in staat zelfstandig uitvoering te geven aan projecten op het gebied van informatiebeveiliging, zowel een technisch als organisatorisch. Denk hierbij aan:

- onderzoeken naar de status van informatiebeveiliging;
- het uitvoeren van risico-analyses;
- ontwikkelen van beleid en procedures;
- het uitvoeren van reviews, audits en penetratie-testen, zowel op netwerk en systeem gebied als in applicaties.

Met jouw expertise help je onze klanten in de financiële en overheidssector om de beveiliging van de informatievoorziening effectief en efficiënt op het juiste niveau te brengen én te houden.

Je sollicitatie met uitgebreide CV zien wij graag tegemoet via een e-mail aan remco.bakker@irc2.com

over irc2

Information Risk Control is een onafhankelijke adviesorganisatie. Als erkend specialist op het gebied van informatiebeveiliging voorzien wij organisaties binnen zowel de overheid als het bedrijfsleven van onafhankelijk advies. Wij ondersteunen opdrachtgevers bij het inrichten van de informatiebeveiliging, zowel op het gebied van techniek/ICT, als op organisatorisch vlak. Kernbegrippen zijn: kwaliteit, integriteit, nuchterheid en praktische toepasbaarheid.

contact

Perkinsbaan 17b
3439 NB Nieuwegein
+31(0)30 - 600 10 90

www.irc2.com