DigiD en Privacy

Masterscriptie Informatiekunde

Auteur: Marc Jochems
E-mail: M.Jochems@hccnet.nl
Studentnummer: 9705791
Afstudeernummer: 58 IK
Afstudeerbegeleider: Prof. dr. B.P.F. Jacobs

Voorwoord

Ter afsluiting van de Master Informatiekunde aan de Radboud Universiteit Nijmegen heb ik een onderzoek uitgevoerd naar de mate waarin de beveiligingsmaatregelen, binnen het door de Nederlandse overheid gebruikte authenticatiesysteem DigiD, de privacy van de burger waarborgen. Deze scriptie is hiervan het resultaat.

Graag wil ik een aantal mensen bedanken voor de bijdrage die zij hebben geleverd aan het tot stand komen van deze scriptie. Allereerst gaat mijn dank uit naar mijn afstudeerbegeleider Bart Jacobs voor de constructieve en prettige gesprekken die we gevoerd hebben tijdens het verloop van het onderzoek en voor zijn goede begeleiding en feedback.
Verder ben ik Michiel Schoo, beleidsmedewerker bij de Directie Innovatie en Informatiebeleid Openbare Sector van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Bart Kerver, manager Middleware Services bij SURFnet zeer erkentelijk voor de tijd die zij hebben vrijgemaakt om mij uitgebreid te woord te staan over de beleidsmatige en technische invulling van DigiD.

Marc Jochems
Nijmegen, augustus 2007

Samenvatting

DigiD, dat staat voor Digitale Identiteit, is een authenticatievoorziening die door verschillende Nederlandse overheidsinstellingen gebruikt wordt bij de elektronische dienstverlening. Een dergelijk systeem kent grote uitdagingen en risico's op het gebied van privacy van de burger. Ook kan het leiden tot identiteitsroof. Aan de hand van een literatuurstudie en interviews met medewerkers van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, SURFnet en GBO.Overheid is onderzoek gedaan naar de mate waarin de privacy van de burger wordt gewaarborgd binnen DigiD. Bescherming van de privacy is in de Nederlandse Grondwet verankerd en nader uitgewerkt in de Wet Bescherming Persoonsgegevens. Deze laatste wet verplicht de verantwoordelijke tot het nemen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Technische maatregelen die kunnen worden ingezet ter bevordering van de privacy kunnen worden gebundeld onder de verzamelnaam Privacy Enhancing Technologies (PET). Er worden vier hoofdvormen van PET onderscheiden. In oplopende volgorde van effectiviteit zijn dit algemene PET-maatregelen, scheiden van gegevens, privacymanagementsystemen en anonimiseren van persoonsgegevens. De technische maatregelen die binnen DigiD zijn getroffen om te voorkomen dat onbevoegden toegang kunnen krijgen tot met behulp van DigiD verwerkte persoonsgegevens zijn algemene PET-maatregelen. Deze maatregelen zijn versleuteling van het opgeslagen wachtwoord, het over SSL tunnelen van de communicatie tussen de burger en de DigiD server en het tekenen van de communicatie tussen de DigiD server en de overheidsdienst waarvoor authenticatie vereist is op basis van een gedeelde sleutel. Al in 1999 is kamerbreed een motie aangenomen waarin de regering onder andere wordt verzocht te bevorderen dat de overheid het voortouw zal nemen bij de inzet van PET bij haar eigen verwerking van persoonsgegevens. Aan dit verzoek is onvoldoende gehoor gegeven bij de ontwikkeling van DigiD door geen gebruik te maken van één of meer effectievere hoofdvormen van PET-maatregelen, namelijk scheiden van gegevens, privacymanagementsystemen en anonimiseren.

Organisatorische maatregelen die binnen DigiD zijn getroffen om de privacy van de burger te waarborgen zijn het onderscheiden van verschillende zekerheidsniveaus, het controleren van de bij aanvraag van een DigiD opgegeven persoonsgegevens met behulp van de landelijk raadpleegbare deelverzameling en het per post versturen van een activeringscode.

Verder zijn maatregelen getroffen om het achterhalen van een gebruikersnaam en wachtwoord te bemoeilijken en mag een mobiel telefoonnummer maximaal aan één DigiD gekoppeld zijn. Tenslotte worden alle transacties met behulp van DigiD gelogd. Deze maatregelen bieden echter onvoldoende bescherming tegen identiteitsroof, omdat de huidige procedures voor aanvraag en activering geen garantie bieden dat de persoon die een DigiD heeft aangevraagd en geactiveerd ook daadwerkelijk de burger is met het sofinummer behorende bij deze DigiD. Bovendien kan uitsluitend op basis van een gebruikersnaam en wachtwoord een DigiD, worden uitgebreid met sms-authenticatie op een mobiel nummer naar keuze, indien de per post verstuurde activeringscode wordt onderschept. De extra zekerheid die het niveau midden zou moeten brengen, wordt hierdoor niet of nauwelijks geboden.

Een aanbeveling voor een extra technische maatregel om de privacy van de burger te waarborgen is gebruikmaking van de tweede hoofdvorm van PET-maatregelen, namelijk scheiding van gegevens. Hierbij wordt de burger binnen DigiD geïdentificeerd door een uniek, identificerend nummer dat niet bekend is bij de diverse overheidsdiensten die voor authenticatie gebruik maken van DigiD. In plaats hiervan worden deze diensten ingedeeld in verschillende sectoren, waarbij elke sector een eigen sectoraal identiteitsnummer gebruikt 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 en in de communicatie tussen de overheidsdienst en DigiD als tolk fungeert. Uitsluitend de burger beschikt over alle sectornummers.

Ter verbetering van de organisatorische maatregelen wordt met name versterking van de procedures voor aanvraag en activering aanbevolen. De persoonsgegevens op basis waarvan men een DigiD kan aanvragen zijn te eenvoudig te achterhalen door derden en bieden daarom onvoldoende bescherming tegen fraude. In plaats van het sofinummer kan beter gekozen worden voor bijvoorbeeld de combinatie van het nummer van een paspoort, identiteitsbewijs, rijbewijs of verblijfsvergunning en de geldigheidsdatum van dit document. Ook de huidige activeringsprocedure biedt onvoldoende bescherming tegen identiteitsroof. Door de activeringscode niet langer per post te versturen, maar deze pas na legimitatie te overhandigen op het gemeentehuis, krijgt men meer zekerheid over de identiteit van de gebruiker van een DigiD. Wanneer ook bij wijziging of toevoeging van een mobiel telefoonnummer een activeringscode na legitimatie wordt overhandigd op het gemeentehuis, biedt een hoger zekerheidsniveau ook daadwerkelijk meer zekerheid over de identiteit van de gebruiker.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Eind december 2003 presenteerde het kabinet het programma Andere Overheid. Dit programma had tot doel het verbeteren van de kwaliteit van publieke dienstverlening, met name door meer en beter gebruik te maken van ICT. Een streven hierbij was dat in 2007 65 procent van de publieke dienstverlening van rijk, provincies en gemeenten plaats kan vinden via het internet. Bij de elektronische dienstverlening maken de verschillende overheidsinstellingen gebruik van een centrale authenticatievoorziening: DigiD.

De overheid kent twee belangrijke rollen. Enerzijds moet zij als Big Brother toezien op het controleren van de burgers. Anderzijds is zij ook de Soft Sister die de burger tot dienst is. Tussen beide rollen heerst een duidelijk spanningsveld. In haar communicatie naar buiten toe wijst de overheid bij het gebruik van DigiD hoofdzakelijk op haar rol als Soft Sister. De dienstverlening moet vereenvoudigd worden en de administratieve lasten verlaagd. Dit wordt onder meer gerealiseerd door toepassing van het principe van eenmalige gegevensverstrekking. Dit betekent echter wel dat de verstrekte gegevens op een bepaalde manier moeten worden bewaard, zodat de verschillende overheidsinstellingen hier toegang toe hebben. Hierdoor bestaat het gevaar dat de burger zijn privacy deels moet opgeven ten koste van gebruiksgemak. Bovendien kan men zich de vraag stellen of het hier gaat om gebruiksgemak voor de burger of voor de overheid. Het opslaan en toegankelijk maken van persoonsgegevens vergemakkelijkt namelijk ook het toezicht van de overheid in haar rol als Big Brother. Binnen deze rol van de overheid bestaat een spanningsveld tussen de privacy van de burger en de veiligheid van zowel de burger als zijn omgeving.

Een elektronische overheid kent dus grote uitdagingen en risico's op het gebied van privacy van de burger. Dit maakt het zinvol om te onderzoeken in hoeverre de privacy van de burger wordt gewaarborgd binnen DigiD. Dat de beveiliging van DigiD daadwerkelijk een relevant, actueel onderwerp is, is gebleken uit de aandacht van diverse media. Zo kopte het NRC Handelsblad half april 2006 op de voorpagina: *'Beveiliging DigiD te zwak voor belastingaangifte'*. In het bijbehorende artikel was te lezen dat het Genootschap van Informatiebeveiligers (waarbij onder andere Cap Gemini, CMG, KPMG en PricewaterhouseCoopers zijn aangesloten) het gekozen zekerheidsniveau, bestaande uit een gebruikersnaam en wachtwoord, te zwak achtte om er de belastingaangifte mee te ondertekenen.

Begin april 2007 was er veel ophef over het advies van de informatienummers van de Belastingdienst om de DigiD van iemand anders te gebruiken voor de belastingaangifte indien men de eigen DigiD kwijt was of niet op tijd had aangevraagd. Met dit advies zet de overheid zelf aan tot identiteitsfraude en haalt zij de eigen identiteitsinfrastructuur onderuit.

Een ander actueel probleem is identiteitsroof. Volgens Avivah Litan, vice-president en onderzoeksdirecteur bij Gartner, waren in 2004 naar schatting zo'n 9,4 miljoen Amerikaanse burgers op een of andere manier slachtoffer van identiteitsdiefstal. Uit een onderzoek van consumentenorganisatie Which? in 2005 bleek dat één op de vier Engelsen ooit het slachtoffer is geworden van een vorm van identiteitsroof.

Tenslotte staat als gevolg van de antiterrorismewetgeving het privacyvraagstuk nadrukkelijk op de agenda. Hierbij staat de vraag centraal of persoonlijke vrijheid en privacy moeten worden opgegeven in ruil voor meer veiligheid in de vorm van preventie en bestrijding van terrorisme. De Amerikaanse Patriot Act, voluit de "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" is een bekend voorbeeld van een dergelijke wet. Deze wet, die een directe reactie is op de aanslagen van 11 september 2001, heeft als doel meer mogelijkheden te geven aan de Amerikaanse overheid om informatie te vergaren over en op te treden in geval van mogelijk terrorisme.

1.2 Onderzoeksvraag

DigiD reguleert de toegang tot diverse verzamelingen persoonsgegevens. Voorbeelden hiervan zijn gemeentelijke registers en belastinggegevens. Het aantal overheidsinstanties aangesloten op DigiD is groeiende en hiermee ook de hoeveelheid persoonsgegevens waartoe door middel van DigiD toegang verkregen kan worden. De wijze waarop deze toegang is gereguleerd, moet voldoen aan het recht op privacy, zoals dat wordt voorgeschreven door de Wet Bescherming Persoonsgegevens. In mijn onderzoek wil ik achterhalen of de getroffen beveiligingsmaatregelen dit recht op privacy waarborgen. Ik richt me hierbij op de beveiligingsaspecten confidentialiteit en integriteit en onderscheid twee categorieën van maatregelen: technische en organisatorische.
De onderzoeksvraag luidt:
In welke mate voldoen de technische en organisatorische maatregelen, die zijn getroffen om confidentialiteit en integriteit van persoonsgegevens te garanderen bij het reguleren van de toegang tot persoonsgegevens door DigiD, aan de eisen die de Wet Bescherming Persoonsgegevens stelt en op welke wijze kunnen of moeten deze maatregelen verbeterd worden?

Deze hoofdvraag wordt beantwoord met behulp van een aantal deelvragen:

1. *Welke eisen stelt de Wet Bescherming Persoonsgegevens aan het verwerken van persoonsgegevens?*
2. *Tot welke persoonsgegevens reguleert DigiD toegang?*
3. *Waar worden deze persoonsgegevens opgeslagen, door wie gebeurt dit en hoelang blijven deze persoonsgegevens op deze plaats opgeslagen?*
4. *Wie behoren op welk moment toegang te hebben tot (een deel van) deze gegevens op grond van de Wet Bescherming Persoonsgegevens?*
5. *Welke technische en organisatorische maatregelen zijn getroffen om te reguleren dat uitsluitend toegang wordt verschaft tot gegevens waartoe men volgens de Wet Bescherming Persoonsgegevens gerechtigd is en in welke mate bereiken deze maatregelen het gestelde doel?*
6. *Op welke wijze is identiteitsroof mogelijk met DigiD?*
7. *Welke technische en organisatorische maatregelen zijn getroffen om identiteitsroof te voorkomen en in welke mate bereiken deze maatregelen het gestelde doel?*

1.3 Aanpak

Het door mij verrichte onderzoek is een gevalsstudie. Ik heb één specifiek geval bestudeerd, namelijk de authenticatievoorziening DigiD en dit heb ik in zijn geheel bestudeerd, zonder een deel(aspect) hiervan kunstmatig te isoleren. Zoals gebruikelijk voor gevalsstudies betrof het een kwalitatief onderzoek. De dataverzameling met betrekking tot verkenning van het onderzoeksterrein, vergaren van achtergrondinformatie en het afbakenen van de scope van het onderzoek vond hoofdzakelijk plaats door middel van literatuurstudie. De informatie die specifiek betrekking had op DigiD, is verkregen door middel van een aantal interviews. Het eerste interview vond plaats met Michiel Schoo, die werkzaam is als beleidsmedewerker bij de Directie Innovatie en Informatiebeleid Openbare Sector van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De nadruk lag bij dit interview op beleidsmatige keuzes en beslissingen die zijn genomen bij de ontwikkeling en het in gebruik nemen van DigiD. Vervolgens heb ik Bart Kerver, manager Middleware Services bij SURFnet, geïnterviewd over de technische invulling van DigiD. Tenslotte heeft de Serviceorganisatie GBO.Overheid mij voorzien van informatie met betrekking tot enkele operationele kwesties, met name op het gebied van opslag van persoonsgegevens en loggen van transacties.

1.4 Opbouw

Deze scriptie bestaat uit een zevental hoofdstukken. Het eerste hoofdstuk vormt een introductie op het onderzoek. Hoofdstuk 2 beschrijft de ontwikkeling en achtergrond van DigiD. Hoofdstuk 3 gaat nader in op het begrip privacy. Naast een definitie van de betekenis hiervan in de context van mijn onderzoek, wordt ingegaan op de noodzaak van privacy, de wijze waarop het recht op privacy in de Nederlandse wetgeving wordt beschermd en op Privacy Enhancing Technologies. Hoofdstuk 4 geeft een beschrijving van het gebruik van DigiD en van de maatregelen die zijn getroffen om de privacy van de burger te waarborgen. In hoofdstuk 5 volgt een kritische beoordeling van DigiD. Hierbij wordt in het bijzonder gekeken naar het risico op identiteitsroof. Hoofdstuk 6 geeft de conclusies van het onderzoek weer, evenals een aantal aanbevelingen die moeten zorgen voor meer privacy voor de burger en identiteitsroof moeten bemoeilijken. Tenslotte volgt in hoofdstuk 7 een overzicht van de bij het onderzoek gebruikte literatuur.

2 Achtergrond DigiD

2.1 Inleiding

Dit hoofdstuk handelt over de achtergrond van DigiD. Paragraaf 2.2 begint met een beschrijving van het actieprogramma Andere Overheid. Hierna wordt in paragraaf 2.3 nader ingegaan op de elektronische dienstverlening door de diverse overheidsinstanties. Vervolgens komt in paragraaf 2.4 de rol die authenticatie bij deze diensverlening speelt aan bod. Paragraaf 2.5 handelt tenslotte over het burgerservicenummer.

2.2 Andere overheid

Veranderende maatschappelijke omstandigheden zijn voor de overheid de afgelopen decennia steeds de aanleiding geweest om zich te bezinnen op haar rol, taken en werkwijze. Dit leidde in de jaren zeventig tot het versterken van het sturende vermogen van de overheid, in de jaren tachtig gevolgd door een financiële herbezinning met grootscheepse privatiseringen en verzelfstandigingen. In de jaren negentig werd de nadruk gelegd op marktwerking en efficiency, waardoor overheidsorganisaties steeds meer als bedrijven werden beschouwd, zij het zonder concurrentie of alternatieven voor de burger. Het actieprogramma Andere Overheid stelt dat de overheid in het huidige millennium steeds meer is beland “in de rol van ‘albedil’ die eigenhandig alle kleine en grote problemen in de samenleving moest en ook wilde oplossen.” De ingrepen die zij hiertoe neemt, dringen diep in de samenleving door. Er zijn steeds meer en gedetailleerdere regels bijgekomen, die steeds moeilijker te handhaven zijn. Bovendien is gebleken dat meer regels, meer voorschriften, meer agenten en meer toezichthouders niet leiden tot het daadwerkelijk oplossen van de maatschappelijke problemen. Hierdoor is het besef ontstaan dat een andere koers nodig is. Deze andere koers wordt verwoord in het actieprogramma Andere Overheid, dat in januari 2004 van start is gegaan en moet leiden tot een afnemende overheidsbemoeienis met minder regels en minder administratieve lasten.

Centraal in het programma Andere Overheid staat dat de overheid zich beperkt tot haar kerntaken en deze eenvoudiger, efficiënter en effectiever uitvoert. Het programma heeft betrekking op diverse lagen van de overheid: het rijk, uitvoeringsorganisaties, provincies en gemeenten. Andere Overheid omvat verbeteracties en initiatieven rond de thema’s: betere dienstverlening, minder bureaucratie, slagvaardige organisatie en andere werkwijze.

De overheid wil de kwaliteit van de publieke dienstverlening voornamelijk verbeteren door meer en beter gebruik te maken van ICT. Overheidsdienstverlening zal steeds vaker verlopen via een elektronisch loket dat 24 uur per dag en 7 dagen per week, thuis of onderweg, open en bereikbaar is. In de private sector is dit al heel gebruikelijk. Hierbij valt te denken aan e-business en telebankieren. Het kabinet streeft er naar dat in 2007 65 procent van de publieke dienstverlening (van rijk, provincies en gemeenten) plaats kan vinden via het internet. Het voornemen van het kabinet om de administratieve lasten voor burgers en bedrijven met een kwart te verminderen vormt een extra prikkel om deze doelstelling te realiseren.

2.3 Elektronische overheid

Mettau (2005) noemt vier stadia van ontwikkeling die kunnen worden onderscheiden bij digitale communicatie in de samenleving: informatie, interactie, transactie en transformatie.
Een website die zich in de informatiefase bevindt, biedt slechts informatie aan die voorheen in folders of publicaties verstrekt werd. Interactie vindt plaats op het moment dat een gebruiker ook een mail kan sturen via de website. Bij transactie is de website ingericht op voortdurende communicatie met gebruikers. Bij transformatie tenslotte wordt de communicatie dynamisch en volgt de interactie niet meer de structuur van de website en de door de site vertegenwoordigde instanties, maar andersom.

Mettau (2005) beschrijft onder andere de volgende drie strategische verschuivingen in de oriëntatie van de overheid op het functioneren van publieke uitvoeringsorganisaties:

1. Vraaggerichte dienstverlening waarbij aandacht is voor maatwerk
2. (G)één loket, waardoor de burger niet meer van het kastje naar de muur wordt gestuurd
3. Het door de overheid mogelijk maken van proactieve dienstverlening

Vraaggerichte dienstverlening
Vraaggerichte dienstverlening betekent dat de organisatie zich richt op de behoeften van de omgeving en niet alleen op de behoeften van beleidsmakers of politici. De focus komt te liggen op vraagpatronen van burgers en niet op de inrichting van het openbaar bestuur als gevolg van wet- en regelgeving. De overheid probeert hierbij haar focus te verleggen naar maatwerk in dienstverlening.

(G)één loket
Het klantcontactpunt, vooral de balie en de telefoon, wordt gezien als een vangnet voor burgers die niet op een andere, snellere, en voor de overheid vaak goedkopere manier van de dienstverlening gebruik kunnen maken. Gestreefd wordt naar een minimale telefonische en papieren bereikbaarheidsbehoefte. Uitgangspunt bij de (g)één loket gedachte is dat de burger niet meer van het kastje naar de muur wordt gestuurd, maar bij één contactpunt geholpen wordt. Dit houdt in dat overheidsloketten alle voor de burger relevante diensten aanbieden op een bepaald vraagpatroon, niet alleen de dienst waar de achterliggende organisatie primair voor is ingericht.

Proactieve dienstverlening
Een overheid die proactief werkt, neemt zelf het initiatief om diensten aan te bieden, zonder dat daar een expliciete vraag van de burger aan vooraf is gegaan. Er is sprake van dienstverlening op maat, waarbij de overheid het dienstverleningsproces start op basis van de informatie die zij van de klant heeft.

ICT speelt een grote rol bij het realiseren van deze strategische verschuivingen. Dé overheid als consistent geheel bestaat niet, maar is een verzameling van een grote hoeveelheid verschillende overheidsorganisaties. Het internet maakt het echter mogelijk deze aan elkaar te koppelen tot één portal, waar de burger voor alle overheidsdiensten terecht kan. Een belangrijk uitgangspunt dat hierbij gehanteerd wordt, is het principe van eenmalige gegevensverstrekking. Dit wil zeggen dat aan burgers geen gegevens worden gevraagd die al binnen de overheid beschikbaar zijn.
Bovendien moet de elektronische overheid een hoog ontwikkelingsstadium bereikt hebben. Voor een vraaggerichte dienstverlening die uitgaat van één elektronisch loket is het stadium transactie noodzakelijk. Om proactieve dienstverlening aan te kunnen bieden is het stadium transformatie vereist.

2.4 Authenticatie

In de vorige paragraaf is beschreven dat de overheid streeft naar digitale communicatie met de burgers volgens een hoog ontwikkelingsstadium, waarbij het principe van eenmalige gegevensverstrekking wordt gehanteerd. Dit is niet mogelijk zonder digitale identificatie (Prins & De Vries, 2003). De verstrekte gegevens moeten worden bewaard en gekoppeld aan een digitale identiteit van de burger. Om te voorkomen dat onbevoegden toegang hebben tot deze gegevens is een authenticatiesysteem vereist. De Nederlandse overheid heeft hierbij gekozen voor DigiD.

DigiD staat voor Digitale Identiteit. Het is een inlogcode voor transacties met de overheid. Burgers kunnen met behulp van DigiD terecht bij elektronische diensten van een toenemend aantal overheidsinstellingen. Deze overheidsinstellingen kunnen op hun beurt met DigiD de identiteit controleren van klanten die gebruik maken van hun elektronische diensten. DigiD ondersteunt het gebruik van drie verschillende zekerheidsniveaus: basis, midden en hoog. Elk zekerheidsniveau heeft zijn eigen authenticatiemethodes. Op het basisniveau maakt DigiD gebruik van een gebruikersnaam met wachtwoord. Op het middenniveau maakt DigiD gebruik van een gebruikersnaam met wachtwoord én een transactiecode via sms. Het is de bedoeling dat het hoogste zekerheidsniveau in de toekomst wordt ingevuld door de elektronische Nederlandse Identiteitskaart (eNIK).

De overheidsinstelling die een bepaalde elektronische dienst aanbiedt bepaalt zelf welk zekerheidsniveau voor deze dienst gewenst is. In de meeste gevallen zal dit het basisniveau zijn. In 2005 waren onder andere diverse gemeenten, de Sociale Verzekeringsbank en het Centrum voor Werk en Inkomen aangesloten op DigiD. Sinds 15 februari 2006 is ook de Belastingdienst toegetreden, waardoor het ook mogelijk werd de belastingaangifte te doen met behulp van DigiD. Inmiddels kan elektronische belastingaangifte uitsluitend nog met behulp van DigiD. In 2007 maakten hier bijna 2 miljoen mensen gebruik van.

2.5 Burgerservicenummer

DigiD is gekoppeld aan een uniek identificerend persoonsnummer. Na een geslaagde authenticatie door een burger, die van een overheidsdienst gebruik wil maken, ontvangt de bijbehorende overheidsinstelling dit persoonsnummer. Momenteel wordt hier het sofinummer voor gebruikt, maar dit zal op korte termijn worden vervangen door het burgerservicenummer. De invoering hiervan stond aanvankelijk gepland voor 2006, maar de wet Burgerservicenummer is pas op 11 juli 2007 goedgekeurd door de Eerste Kamer. Het burgerservicenummer is getalsmatig gelijk aan het sofinummer, maar de nummers verschillen wat betreft beheer, juridische grondslag en gebruik. Zo zal het burgerservicenummer gebruikt gaan worden in de gehele publieke sector, terwijl het sofinummer uitsluitend betrekking heeft op het sociaal/fiscaal domein. Door persoonsgegevens van de burger te koppelen aan het burgerservicenummer, zijn deze eenvoudig uitwisselbaar tussen verschillende overheidsinstellingen. Dit maakt het principe van eenmalige gegevensverstrekking mogelijk.

3 Privacy

3.1 Inleiding

Dit hoofdstuk, dat theoretisch van karakter is, begint in paragraaf 3.2 met een definitie van het begrip privacy. Vervolgens wordt in paragraaf 3.3 het belang van privacy aangegeven. Paragraaf 3.4 handelt over de wijze waarop privacy gewaarborgd wordt in de Nederlandse wetgeving, waarna in paragraaf 3.5 wordt aangegeven hoe Privacy Enhancing Technologies kunnen worden toegepast om persoonsgegevens te beschermen. Tenslotte sluit paragraaf 3.6, die handelt over identiteitsroof, dit hoofdstuk af.

3.2 Definitie van privacy

Er bestaat geen algemeen geaccepteerde definitie van het begrip privacy. Wel bestaat er onder deskundigen overeenstemming over het feit dat dit begrip betrekking heeft op de bescherming van de persoonlijke levenssfeer. Schoeman (1984) verdeelt de definities die door diverse auteurs zijn voorgesteld in drie categorieën. De eerste categorie ziet privacy als het recht van een individu om te bepalen welke informatie over hem of haar mag worden gecommuniceerd naar anderen. Volgens de tweede categorie is privacy de mate van zeggenschap die een individu heeft over informatie met betrekking tot hem- of haarzelf, vertrouwelijkheid van persoonlijke identiteit of wie zintuiglijke toegang heeft tot hem of haar (Gavison, 1984). De derde categorie tenslotte stelt dat privacy de toestand van beperkte toegang tot een persoon is.

Om onduidelijkheid te voorkomen heb ik in deze scriptie gekozen voor de eerste categorie. Hiermee wil ik geenszins beweren dat de twee andere visies onjuist zijn, maar deze zijn uit praktisch oogpunt minder geschikt voor de reikwijdte van mijn onderzoek, dat handelt over de verspreiding van persoonsgegevens.
Wanneer ik in deze scriptie spreek over privacy, bedoel ik hiermee dus *het recht van een individu om te bepalen welke informatie over hem of haar mag worden gecommuniceerd naar anderen*.
Deze definitie sluit goed aan bij artikel 10 van de Nederlandse Grondwet, waarin privacy wordt omschreven als het recht op eerbiediging van de persoonlijke levenssfeer.
Blok (2002) stelt dat privacy een subjectief recht is. Dit houdt in dat een individu in beginsel zelf mag uitmaken of hij zijn persoonlijke levenssfeer verborgen wil houden.

3.3 Noodzaak van privacy

Het belang van privacy wordt treffend beschreven door Rachels (1984). Hij stelt dat privacy noodzakelijk is voor de verscheidenheid aan sociale relaties die mensen willen onderhouden. Elke relatie kent zijn eigen karakteristieke gedragspatronen, die samenhangen met de rol die men in deze relatie vervult. Door invloed uit te kunnen oefenen op het type en de mate van kennis die anderen van ons hebben, zijn we in staat om ons in het bijzijn van bepaalde personen te gedragen op de wijze die past bij de sociale relatie die we met hen hebben, zonder afbreuk te doen aan andere sociale relaties die een ander gedragspatroon kennen. Om een variëteit aan sociale relaties te kunnen onderhouden, is het noodzakelijk de toegang tot persoonlijke informatie te kunnen reguleren. Een feit over onszelf gaat uitsluitend iemand iets aan, wanneer er een specifieke sociale relatie is tussen ons, die hem of haar recht geeft het te weten (Rachels, 1984).

Privacy is dus ook van wezenlijk belang in situaties waarin men niets te verbergen heeft, want het maakt het mogelijk een scheiding te maken tussen verschillende rollen. Het geeft iemand het recht om informatie te beperken tot een bepaalde rol. Het koppelen van informatie uit verschillende domeinen moet met de grootst mogelijke terughoudendheid gebeuren, omdat er mogelijk gegevens uit rollen gekoppeld worden, die betrokkenen gescheiden wensen te houden (Jacobs, 2007).

3.4 Privacy in de Nederlandse wetgeving

In Nederland handelen twee wetten over privacy. Allereerst komt de bescherming van de persoonlijke levenssfeer ter sprake in artikel 10 van de Grondwet dat luidt:

1. *Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.*
2. *De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.*
3. *De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.*

Een wet die zich geheel richt op het waarborgen van privacy is de Wet Bescherming Persoonsgegevens, ook wel de privacywet genoemd. Deze wet is op 1 september 2001 van kracht geworden, als uitvloeisel van de op 24 oktober 1995 vastgestelde Europese richtlijn inzake de bescherming van persoonsgegevens.

De Wet Bescherming Persoonsgegevens is van toepassing op verwerkingen van persoonsgegevens. Een persoonsgegeven is in deze wet gedefinieerd als elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Hierbij moet het gaan om levende personen. Het begrip verwerking heeft een zeer ruime strekking. Iedere handeling vanaf de verzameling en opslag van een persoonsgegeven tot de verwijdering en vernietiging ervan dient te worden opgevat als een verwerkingshandeling. De Wet Bescherming Persoonsgegevens is van toepassing indien sprake is van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. Tevens is de wet van toepassing indien sprake is van niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen. Onder een bestand wordt een al dan niet langs geautomatiseerde weg gevoerde verzameling van persoonsgegevens verstaan (Berkvens & Prins, 2004).
De verwerking van persoonsgegevens moet eerlijk, rechtmatig en doelgebonden zijn. Persoonsgegevens mogen niet voor andere doelen gebruikt worden dan waarvoor ze verkregen zijn. Ook moet degene wiens gegevens verwerkt worden op de hoogte zijn van de verwerking, het doel ervan, de herkomst van de gegevens en de ontvangers van de verwerkte gegevens. Bovendien heeft iedereen het recht om onjuiste of onvolledige registratie van de eigen gegevens te laten corrigeren of verwijderen (Overbeek, Lindgreen & Spruit, 2005).

De Wet Bescherming Persoonsgegevens richt zich primair op de verantwoordelijke. Bij elke verwerking van persoonsgegevens kan deze worden aangewezen. Bij het bepalen wie als verantwoordelijke moet worden aangemerkt, wordt gekeken wie doel en middelen van een verwerking vaststelt. De verantwoordelijke bepaalt of er gegevens worden bewerkt, welke gegevens er worden bewerkt, welke bewerking wordt toegepast en op welke wijze dat gebeurt en voor welk doel (Berkvens & Prins, 2004). Artikel 13 van de Wet Bescherming Persoonsgegevens stelt dat de verantwoordelijke passende technische en organisatorische maatregelen moet nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen moeten, rekening houdend met de stand van de techniek en de kosten van de maatregelen, een passend beveiligingsniveau garanderen. Artikel 14 stelt dat deze eis ook geldt als de verwerking van de persoonsgegevens is uitbesteed (Overbeek, Lindgreen & Spruit, 2005).

De Wet Bescherming Persoonsgegevens kent een aantal verplichtingen om de betrokkene te informeren over diverse aspecten van de informatieverwerking. Op de eerste plaats geldt de verplichting van artikel 33 om bij het verzamelen van gegevens bij de betrokkene zelf, deze voorafgaand aan het moment van verkrijging nader te informeren over onder meer de identiteit van de voor de verwerking verantwoordelijke, de doeleinden van de gegevensverwerking, de ontvangers en een eventuele overdracht naar derde landen. In de praktijk zal deze plicht veelal vorm krijgen door de betreffende informatie te vermelden op een bij verkrijging te overhandigen standaardformulier. Mededeling is niet nodig indien de betrokkene op de hoogte is van de verkrijging van de gegevens door het bedrijf of de organisatie die de gegevens verwerkt (Berkvens & Prins, 2004).
Wanneer de gegevens op een andere wijze worden verkregen gelden de bepalingen van artikel 34. In deze gevallen dient de informatie aan de betrokkene te worden verstrekt op het moment van vastlegging dan wel uiterlijk op het moment van de eerste verstrekking aan een derde indien de gegevensverwerking daartoe bestemd is. Ook hier is mededeling niet nodig indien de betrokkene op de hoogte is van de verkrijging van de gegevens door het bedrijf of de organisatie die de gegevens verwerkt. Tevens gelden in deze situatie aanvullende uitzonderingen: het informeren van de betrokkene blijkt onmogelijk, de mededeling kost een onevenredige inspanning of de verstrekking is bij of krachtens de wet voorgeschreven. Deze laatste situatie vormt de uitzonderingsgrond voor vele verwerkingen door de overheid en betekent dat betrokkenen in vele gevallen niet zullen worden geïnformeerd over gegevensverwerkende processen bij de overheid. (Berkvens & Prins, 2004)

In aanvulling op de voornoemde actieve informatieplichten van de verantwoordelijke kan men bij een verantwoordelijke informeren of hem of haar betreffende gegevens worden verwerkt. Artikel 37 schrijft voor dat de verwerker de benodigde informatie dient te verstrekken, waarbij hij zich overigens dient te vergewissen van de identiteit van de betrokkene.

3.5 Privacy Enhancing Technologies

De koers die de overheid heeft ingezet op het gebied van elektronische dienstverlening heeft een grote invloed op het spanningsveld tussen privacy en gebruiksgemak dat de overheid als dienstverlener bij de burger opwerpt. Het door de overheid mogelijk maken van proactieve dienstverlening leidt tot aanzienlijk meer gebruiksgemak voor de burger, maar heeft ook een direct effect op zijn privacy.

Door uit te gaan van het principe van eenmalige gegevensverstrekking, kan de overheid in haar communicatie met de burger optreden als één partij, in plaats van de verschillende overheidsorganisaties die erachter schuilgaan. Hierbij moet echter goed in het oog worden gehouden dat men ook tegenover de overheid verschillende rollen speelt (Jacobs, 2007). Bij het koppelen van informatie vanuit de verschillende overheidsorganisaties moet dus rekening worden gehouden met de rol waarbij bepaalde informatie hoort. Technische hulpmiddelen die kunnen worden ingezet ter bevordering van de privacy worden gebundeld onder de verzamelnaam Privacy Enhancing Technologies (PET). Hieronder vallen alle ICT-middelen die kunnen worden gebruikt om persoonsgegevens te beschermen.

PET-maatregelen kunnen worden ingedeeld in vier hoofdvormen. In oplopende volgorde van effectiviteit zijn dit algemene PET-maatregelen, scheiden van gegevens, privacymanagementsystemen en anonimiseren (Koorn et al., 2004). Deze vormen zullen hieronder nader worden beschreven.

Algemene PET-maatregelen

Algemene PET-maatregelen betreffen voornamelijk versleuteling van gegevens, identificatie, authenticatie en autorisatie. Deze algemene beveiligingsmaatregelen, die door veel organisaties worden toegepast, hebben bij het juiste gebruik ook een privacyverhogende functie. Authenticatie en autorisatie vormen een voorwaarde voor het effectief functioneren van veel andere PET-maatregelen. Wanneer ongeautoriseerde personen onrechtmatig toegang verkrijgen tot bepaalde persoonsgegevens, wordt het voordeel van deze andere maatregelen tenietgedaan. Iemand dient uitsluitend toegang te krijgen tot de gegevensverzameling die hoort bij de functie of rol die deze persoon vervult. Daarom staat een betrouwbaar authenticatie- en autorisatieproces veelal aan de basis van een succesvolle PET-implementatie (Koorn et al., 2004).

Een andere algemene PET-maatregel is gegevensminimalisatie. Hierbij worden de persoonsgegevens getransformeerd tot gegevens, waaruit de identiteit niet direct herleidbaar is. Dit kan gebeuren door bepaalde gegevens (deels) te verwijderen, zoals bijvoorbeeld de laatste 3 tekens van een postcode, wanneer niet het gehele adres van een persoon benodigd is, maar uitsluitend een indicatie van de buurt waarin hij woont. Ook kan gekozen worden voor het categoriseren van bepaalde gegevens. Een voorbeeld hiervan is het uitsluitend aangeven of iemand wel of niet meerderjarig is in plaats van het geven van de geboortedatum of leeftijd.

Scheiding van gegevens

Een belangrijke vorm van PET betreft de scheiding van gegevens in meerdere domeinen. De identificerende persoonsgegevens worden hierbij losgekoppeld van de overige persoonsgegevens. Om dit te realiseren worden twee of meer domeinen gecreëerd: een identiteitsdomein met daarin de identificerende persoonsgegevens en één of meer pseudo-identiteitsdomeinen waarin overige gegevens worden verwerkt. De scheiding tussen deze domeinen wordt aangebracht en beheerd door een identiteitsbeschermer. Deze zet de echte identiteit om in een pseudo-identiteit, meestal door het toekennen van niet-herleidbare identificatiecodes. Alleen met behulp van de identiteitsbeschermer kan de koppeling tussen de verschillende domeinen worden gelegd. Indien er sprake is van meer dan één pseudo-identiteitsdomein, dient elk een andere pseudo-identiteit te gebruiken, om te voorkomen dat de ware identiteit alsnog achterhaald kan worden. Gezien de belangrijke functies van de identiteitsbeschermer is een goed systeem van autorisatie en authenticatie van essentieel belang bij deze vorm van PET. Maximale gegevensbescherming wordt gerealiseerd wanneer de identiteitsbeschermer wordt beheerd door de persoon wiens gegevens zijn vastgelegd. Alleen hij bepaalt dan wanneer en aan wie zijn ware identiteit wordt bekendgemaakt (Koorn et al., 2004).

Privacymanagementsystemen

Privacymanagementsystemen zorgen voor de geautomatiseerde toepassing van privacybeleid. Het systeem ligt als een soort schil om de persoonsgegevens heen en toetst alle transacties die plaatsvinden met deze gegevens automatisch aan elektronisch vastgelegde privacyregels, die zijn afgeleid uit het privacyreglement voor het betreffende informatiesysteem. Men start met het invoeren van het vastgestelde privacybeleid van de organisatie in het privacymanagementsysteem. Vervolgens wordt dit systeem geïntegreerd met de verwerkingsprocessen. Wanneer nieuwe verwerkingsprocessen of gegevens worden ingevoerd, analyseert het systeem automatisch of het verwerkingsproces wordt gedekt door een vastgelegde norm of regel die voortvloeit uit het privacybeleid en stelt het vast of de verwerkingsprocessen van de verschillende organisatieonderdelen consistent zijn.

Anonimiseren
Het anonimiseren van persoonsgegevens is de ultieme vorm van PET. Het kan op twee manieren worden toegepast. In het eerste geval worden geheel geen persoonsgegevens verwerkt. Deze oplossing is alleen mogelijk indien voor het doeleinde van de dienstverlening het verwerken van persoonsgegevens niet noodzakelijk is. In het tweede geval worden de persoonsgegevens direct na verwerking vernietigd of losgekoppeld van de overige gegevens. Dit vernietigen of loskoppelen moet onomkeerbaar zijn, omdat de persoonsgegevens anders alsnog gekoppeld kunnen worden zodat de anonimiteit tenietgedaan is (Koorn et al., 2004).

Koops en Lenes (2005) stellen dat de overheid een belangrijke taak heeft bij het zorgen voor toepassing van PET. De Tweede Kamer heeft in 1999 de motie van Nicolaï c.s. aangenomen, waarin de regering wordt verzocht "te bevorderen dat de ontwikkeling en gebruik van PET krachtig ter hand wordt genomen en te bevorderen dat de overheid als innovatieve aanbesteding het voortouw zal nemen bij de inzet van PET bij haar eigen verwerking van persoonsgegevens." In 2004 heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties het boek Privacy Enhancing Technologies – Witboek voor beslissers uitgebracht. Dit boek dient als richtlijn voor overheidsorganisaties bij het toepassen van PET.

3.6 Identiteitsroof

Identiteitsroof vormt een groeiende bedreiging voor de privacy. De Federal Trade Commission schat dat jaarlijks 9 miljoen Amerikanen het slachtoffer worden van deze vorm van identiteitsfraude. Volgens het onderzoeksbureau Javelin Strategy & Research leidde dit in 2006 in Amerika tot een schade van 49,3 miljard dollar. Van identiteitsfraude is sprake wanneer iemand met kwade bedoelingen bewust de schijn oproept van een identiteit die niet bij hem hoort, daarbij gebruikmakend van de identiteit van iemand anders of van een niet-bestaande persoon (Grijpink, 2003). In het eerste geval, dus bij identiteitsfraude waarbij gebruik gemaakt wordt van de identiteit van een bestaand persoon, gaat het om identiteitsroof (Koops & Leenes, 2006).

Identiteitsfraude is van alle tijden. Voorbeelden ervan zijn het gebruik van een valse kentekenplaat of paspoortfraude. Om identiteitsroof te kunnen plegen moet men beschikken over identificerende persoonsgegevens van iemand anders. Dit kan bijvoorbeeld een naam, sofinummer of creditcardnummer zijn. Aangezien steeds meer persoonsgegevens worden opgeslagen in centrale databanken, vaak gekoppeld aan het internet, is identiteitsfraude een sterk toenemende vorm van misdaad (Jacobs, 2007).

4 Gebruik van DigiD

4.1 Inleiding

Dit hoofdstuk beschrijft de werking van DigiD. Het is puur descriptief van aard, een kritische beoordeling volgt in het volgende hoofdstuk. Paragraaf 4.2 behandelt de aanvraag van een DigiD. In paragraaf 4.3 wordt beknopt weergegeven hoe een authenticatie met behulp van DigiD verloopt. Paragraaf 4.4 beschrijft vervolgens eenzelfde authenticatie technisch bezien. In paragraaf 4.5 komt logging aan bod, waarna het hoofdstuk in paragraaf 4.6 wordt afgesloten met problemen die kunnen optreden bij het gebruik van DigiD.

4.2 Aanvragen 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. Deze website wordt gehost door de Gemeenschappelijke Beheer Organisatie (GBO.Overheid). Dit is een directie binnen het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, die op 1 januari 2006 is ingesteld voor het beheer en de verdere ontwikkeling van een aantal overheidsbrede ICT-voorzieningen, waaronder DigiD.

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. Na invulling van deze gegevens wordt in de landelijk raadpleegbare deelverzameling gekeken of de combinatie van sofinummer, geboortedatum, postcode en huisnummer correct is. De landelijk raadpleegbare deelverzameling is een voorziening voor online bevraging van persoonsgegevens. Deze bevat een beperkt gedeelte van de persoonsgegevens uit de gemeentelijke basisadministratie en fungeert als tijdelijke oplossing tot een volledige online gemeentelijke basisadministratie beschikbaar is. Indien de combinatie van gegevens correct is bevonden, wordt per post een activeringscode verzonden naar de aanvrager. Wanneer de aanvrager deze code en zijn gebruikersnaam en wachtwoord invult op de website van DigiD, is zijn DigiD geactiveerd en kan hij deze gebruiken om zich te authenticeren bij aangesloten overheidsdiensten.

De door de burger bij zijn aanvraag opgegeven persoonsgegevens worden opgeslagen in een database bij DigiD. Hierbij wordt het wachtwoord zodanig versleuteld, dat dit niet meer leesbaar gemaakt kan worden. Volgens welke methodiek dit gebeurt, wordt vanuit veiligheidsoverwegingen niet openbaar gemaakt door GBO.Overheid. Het burgerservicenummer, nu nog sofinummer, fungeert als databasesleutel. De postcode, het huisnummer en de geboortedatum worden na het aanvragen nog 10 weken bewaard in de database ten behoeve van het versturen van de activeringsbrief. Na deze periode worden ze verwijderd uit de database van DigiD. Het burgerservicenummer, de gebruikersnaam, het wachtwoord en indien opgegeven het e-mailadres en het mobiele telefoonnummer blijven net zo lang bewaard als de DigiD bestaat. Dit is in principe onbeperkt, maar indien een DigiD anderhalf jaar niet gebruikt is, vervalt deze en worden de bijbehorende persoonsgegevens verwijderd uit de database van DigiD.

GBO.Overheid is formeel en juridisch verantwoordelijk voor het beheer van de DigiD database. Zij voeren dit beheer niet zelf uit, maar hebben het uitbesteed aan de belastingdienst.

Om een DigiD aan te kunnen vragen moet men staan ingeschreven in de gemeentelijke basisadministratie. Hieruit wordt namelijk het adres gehaald waarheen de activeringsbrief verstuurd wordt. Bij de aanvraag wordt ook getoetst of de aanvrager dit adres correct heeft opgegeven. Nederlanders die in het buitenland wonen en mensen die uitsluitend een postbus hebben, kunnen dus geen DigiD aanvragen.

4.3 Authenticatie met DigiD

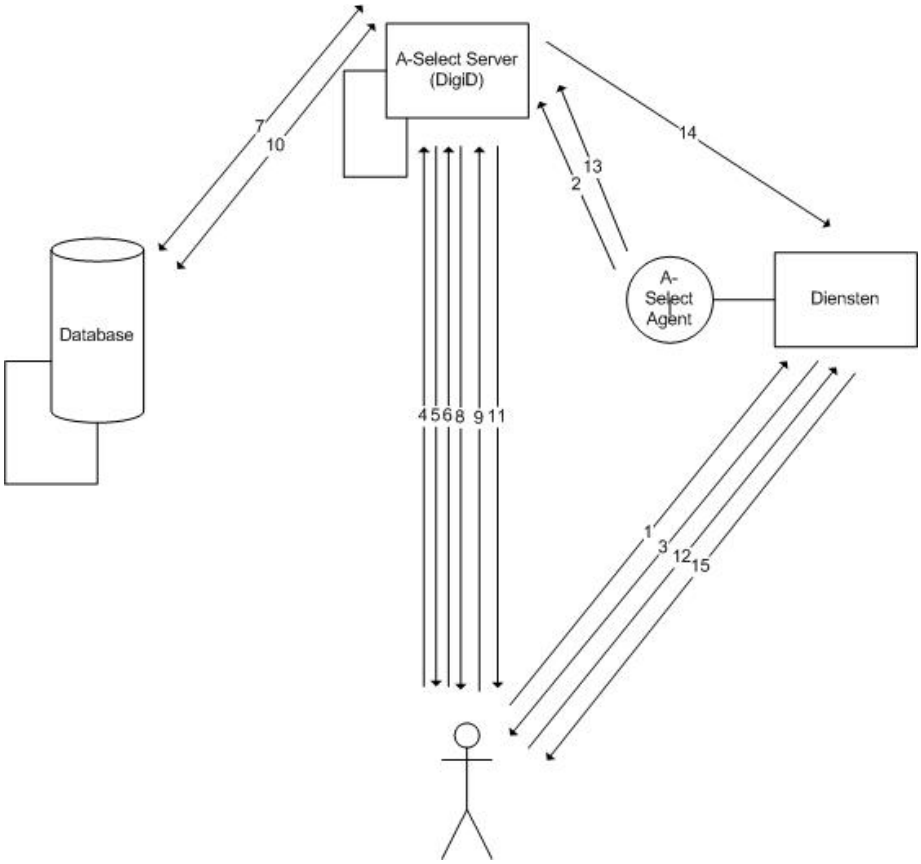
Een authenticatie met behulp van DigiD begint met het afnemen van een dienst bij een aangesloten instelling. Op dit moment zijn uitsluitend overheidsdiensten aangesloten, maar volgens de huidige wetgeving zou het voor private organisaties die een publieke taak hebben, mogelijk moeten zijn om gebruik te maken van DigiD, mits zij bevoegd zijn om het sofinummer, of in de toekomst het burgerservicenummer, te gebruiken en te verwerken.
Voorbeelden van dergelijke diensten zijn het online aanvragen van een vergunning bij de gemeente waar men woont en het aanvragen van een uittreksel uit het bevolkingsregister. Op het moment dat een burger kiest voor deze dienst wordt hij automatisch doorgestuurd naar DigiD en moet hij zijn gebruikersnaam en wachtwoord invoeren. Als hij deze correct invult, wordt hij teruggestuurd naar de gemeente en ontvangt de gemeente het sofinummer of burgerservicenummer behorende bij de zojuist geauthenticeerde DigiD. Op basis hiervan kan de gemeente besluiten de gevraagde dienst te verlenen.

In dit voorbeeld authenticeert de burger zich met zijn gebruikersnaam en wachtwoord. Deze authenticatiemethode wordt gebruikt voor diensten met een authenticatie van zekerheidsniveau basis. Processen die als gevoeliger beschouwd worden, kunnen een hoger zekerheidsniveau vereisen. DigiD ondersteunt het gebruik van drie verschillende niveaus, waarvan er momenteel twee actief zijn. Zekerheidsniveau midden vereist naast een gebruikersnaam en een wachtwoord ook een eenmalige inlogcode die verzonden wordt via sms. Een burger kan hiervan dus uitsluitend gebruik maken, indien hij in het bezit is van een mobiele telefoon en zijn nummer heeft bekendgemaakt aan DigiD. Bovendien mag dit telefoonnummer slechts door één DigiD gebruikt worden. In het verleden heeft men het plan opgevat het middenniveau uit te breiden met bestaande middelen in de markt. Hierbij werd vooral gekeken naar de authenticatiemiddelen die banken gebruiken bij het internetbankieren, zoals de challenge response systemen van de ABN Amro. Dit kreeg echter vanuit ambtelijk niveau geen prioriteit, waardoor momenteel het middenniveau uitsluitend wordt ingevuld met sms-authenticatie.
Het hoogste zekerheidsniveau is nog niet in gebruik. De bedoeling is dat dit in de toekomst ingevuld gaat worden door de elektronische Nederlandse Identiteitskaart (eNIK).

4.4 Authenticatie met DigiD technisch bezien

DigiD is gebaseerd op het standaardproduct A-Select, dat is ontwikkeld door SURFnet. Op dit moment maakt DigiD gebruik van A-Select versie 1.4.2. A-Select is een op Kerberos gebaseerd authenticatiesysteem waarbij de authenticatiemiddelen, zoals de combinatie van een gebruikersnaam en wachtwoord, losgekoppeld zijn van de toepassing waarvoor authenticatie vereist is, zoals bijvoorbeeld een stemapplicatie. Dit maakt het mogelijk eenvoudig authenticatiemiddelen toe te voegen of te verwijderen, zonder dat hiervoor aanpassingen hoeven te worden verricht aan de toepassingen die gebruik maken van deze middelen. A-Select kent enkele standaardcomponenten die ook in DigiD aanwezig zijn. Centraal staat de A-Select server. DigiD heeft een aantal redundante A-Select servers, die zorgen dat er voldoende capaciteit beschikbaar is om authenticatie op een deugdelijke manier snel uit te kunnen voeren. Deze servers zijn gezamenlijk te beschouwen als de component DigiD server. Een tweede component van DigiD is de database, die ook redundant is uitgevoerd. Zoals eerder in dit hoofdstuk al is aangegeven, bevat deze database onder andere de persoonsgegevens die nodig zijn bij de authenticatie.

Verder kent DigiD aangesloten diensten, die door overheidsinstellingen worden aangeboden. De communicatie tussen deze diensten en de DigiD server verloopt grotendeels via een vierde component, de A-Select agent, die namens de dienst communiceert met de DigiD server. In de onderstaande afbeelding zijn deze componenten en de communicatie die ertussen plaatsvindt weergegeven.



Zoals in de vorige paragraaf is aangegeven, wordt een authenticatie geïnitieerd op het moment dat een burger gebruik wil maken van een dienst waarvoor authenticatie vereist is. Als voorbeeld werd onder andere het online aanvragen van een vergunning bij de gemeente genoemd. Uitgaande van dit voorbeeld gaat burger B, met burgerservicenummer, nu nog sofinummer, BSN_B met zijn internetbrowser naar de dienst vergunning aanvragen op de website van de gemeente waar hij woont. In de afbeelding is dit transactie 1. Nadat die dienst tot de conclusie komt dat de burger zichzelf nog niet heeft bekendgemaakt, komt de A-Select agent in actie. De A-Select agent stuurt een bericht naar de DigiD server, waarin hij aangeeft dat iemand spoedig contact gaat opnemen met de DigiD server om in te loggen. Tevens reserveert de A-Select agent een sessie, een rid geheten, bij de DigiD server (transactie 2).

De A-Select agent stuurt de burger nu via de dienst naar de DigiD server (transactie 3 en 4). Hierbij geeft de burger het rid mee, zodat de DigiD server weet dat dit dezelfde burger is over wie de A-Select agent hem zojuist heeft verteld. De DigiD server stuurt een bericht terug naar de burger, waarin hij vraagt om zijn gebruikersnaam (transactie 5), waarop deze antwoordt met gebruikersnaam B (transactie 6). Vervolgens neemt de DigiD server contact op met de database om te kijken welke authenticatiemiddelen bekend zijn voor burger B. (transactie 7) De DigiD server vraagt nu om het wachtwoord van de burger (transactie 8) en ontvangt dit (transactie 9). Hierna wordt dit wachtwoord geverifieerd in de database (transactie 10). Indien bovendien een mobiel telefoonnummer van burger B bekend is in de database, worden transactie 8 tot en met 10 herhaald voor het verifiëren van de eenmalige inlogcode die per sms verzonden wordt.
De DigiD server stuurt de burger vervolgens terug naar de dienst waarvan hij gebruik wil maken (transactie 11 + 12). Hierbij wordt een afgeleide van een ticket granting ticket meegestuurd. Dit ticket granting ticket geeft aan dat het inderdaad de burger met burgerservicenummer BSN_B betreft en op welk niveau hij zich heeft geauthenticeerd. De dienst stuurt via de A-Select agent het ticket granting ticket door naar de DigiD server en vraagt of dit inderdaad door hem is uitgegeven (transactie 13). De DigiD server bekijkt vervolgens het ticket granting ticket en controleert of hij het ticket zelf heeft afgegeven, het geldig is en een voldoende hoog zekerheidsniveau heeft. Als dit het geval is stuurt hij een bevestigend antwoord naar de dienst (transactie 14). De dienst geeft de burger tenslotte een applicatieticket, waarmee hij gebruik kan maken van de gewenste dienst (transactie 15). Dit applicatieticket wordt afgegeven voor een bepaalde tijd. Bij alle vervolgverzoeken vanuit burger B naar die dienst wordt automatisch het applicatieticket meegestuurd, zodat hij toegang krijgt tot deze dienst zolang het applicatieticket geldig is. Het meesturen van het applicatieticket gebeurt in de vorm van een memory based cookie.

Binnen DigiD zijn een aantal maatregelen genomen om de transacties die plaatsvinden af te schermen voor eventueel meeluisterende externe partijen. Alle communicatie die plaatsvindt tussen de burger en de DigiD server en tussen de burger en de overheidsdienst wordt getunneld over SSL. De communicatie tussen de DigiD Server en de dienst waarvoor authenticatie vereist is, wordt getekend. Over het totale bericht wordt een MD5 hash berekend, die versleuteld wordt met een gedeelde sleutel.

4.5 Logging

Alle authenticatiepogingen die worden ondernomen met behulp van DigiD worden opgeslagen. Dit geldt zowel voor de geslaagde pogingen als voor de mislukte. Ditzelfde geldt voor alle aanvragen, activeringen en opzeggingen van DigiD en de wijzigingen in persoonlijke gegevens, die door burgers worden doorgegeven. De gegevens die worden gelogd zijn het burgerservicenummer of sofinummer van de burger in kwestie, de actie die door hem is uitgevoerd en het tijdstip en de datum waarop deze actie plaatsvond. Tevens wordt het IP-adres waar het verzoek vandaan is gekomen opgeslagen, evenals de dienst waarbij de actie is uitgevoerd. Deze logs worden opgeslagen en beheerd door GBO.Overheid en zijn uitsluitend toegankelijk voor de functioneel beheerder van de serviceorganisatie van GBO.Overheid. Overigens kunnen politie en inlichtingendiensten op basis van de Wet Bevoegdheden Vorderen Gegevens in bepaalde situaties ook aanspraak maken op inzage van deze logs.

De logs blijven 3 maanden bewaard op de productieomgeving van DigiD om ondersteuning te kunnen bieden aan burgers. Om statistieken te kunnen uitvoeren over een afgelopen periode en om prognoses te kunnen maken voor de toekomst, worden deze logs voor langere tijd op een apart Management Informatie systeem versleuteld opgeslagen. Om wat voor periode het hier gaat, heb ik ondanks herhaald aandringen niet kunnen achterhalen.
Voor eventuele audit trails, zoals bijvoorbeeld fraudeonderzoeken, worden de logs voor langere tijd versleuteld op tape bewaard bij GBO.Overheid.

4.6 Problemen en misbruik

In dit hoofdstuk is beschreven hoe een succesvolle aanvraag en activering van een DigiD verlopen en hoe een succesvolle authenticatie met behulp van DigiD in zijn werk gaat. Deze paragraaf richt zich op transacties die anders verlopen dan gewenst door de eigenaar van de DigiD. Dit kan bewust zijn, wanneer iemand misbruik wil maken van de DigiD van iemand anders, maar er zijn ook diverse situaties waarin er onbewust of onbedoeld iets misgaat.

Als een activeringscode verlopen is, voor deze gebruikt is, moet een nieuwe DigiD worden aangevraagd. Hierna ontvangt de aanvrager per post een nieuwe activeringscode. Ook wanneer iemand zijn gebruikersnaam of wachtwoord vergeten is, moet hij een nieuwe DigiD aanvragen. DigiD verstrekt uit veiligheidsoverwegingen namelijk geen van beiden aan gebruikers. Als de oude DigiD nog niet was geactiveerd, moet hij bovendien eerst wachten tot de activeringscode verlopen is. Deze vervalt 20 dagen na de aanvraag. Bij het aanvragen van de nieuwe gebruikersnaam, vervallen de oude gebruikersnaam en het oude wachtwoord automatisch. Wanneer een burger wiens mobiele nummer nog niet bekend is bij DigiD gebruik wil maken van een dienst waarvoor zekerheidsniveau midden vereist is, moet hij eerst zijn DigiD uitbreiden met sms-authenticatie. Hiervoor moet hij opnieuw dezelfde persoonsgegevens invullen, die hij ook heeft opgegeven bij het aanvragen van zijn DigiD. Ook ontvangt hij opnieuw per post een activeringscode die hij moet invoeren alvorens hij gebruik kan maken van sms-authenticatie. Wanneer een burger zich 3 maal op rij probeert te authenticeren met een verkeerd wachtwoord, wordt zijn DigiD 10 minuten geblokkeerd. Bij volgende foutieve pogingen loopt deze blokkade op tot 24 uur.

Ook kan het zo zijn dat een burger vermoedt dat iemand anders misbruik maakt van zijn DigiD. Dit vermoeden kan bijvoorbeeld veroorzaakt worden door een geblokkeerde DigiD zonder dat de eigenaar ervan verkeerde gegevens heeft ingevuld of doordat hij gevolgen ondervindt van een transactie die niet door hem is uitgevoerd. Van dit laatste geval kan bijvoorbeeld sprake zijn wanneer zijn persoonlijke gegevens gewijzigd zijn of wanneer hij een schriftelijke bevestiging ontvangt van een actie waar hij niet om gevraagd heeft. In dergelijke gevallen kan hij contact opnemen met de helpdesk van DigiD om dit (mogelijke) misbruik te melden. Afhankelijk van de ernst van de situatie kan geadviseerd worden een nieuwe DigiD aan te vragen of besloten worden tot directe opheffing van de bestaande DigiD. Dit laatste gebeurt uitsluitend via de Servicedesk van DigiD, waarnaar de helpdesk kan besluiten iemand door te sturen. In zeer uitzonderlijke situaties kan bovendien worden overwogen hiervan melding te maken bij de politie.

5 Beoordeling DigiD

5.1 Inleiding

Dit hoofdstuk geeft een kritische beoordeling van DigiD. Allereerst wordt in paragraaf 5.2 aangegeven op welke wijze iemand identiteitsroof kan plegen met behulp van DigiD. Vervolgens wordt in paragraaf 5.3 de authenticatie met behulp van DigiD geëvalueerd. Tenslotte wordt in paragraaf 5.4 specifiek gekeken naar de wijze waarop binnen DigiD met de persoonsgegevens van de burger wordt omgegaan.

5.2 Identiteitsroof met behulp van DigiD

Van identiteitsroof met behulp van DigiD is sprake wanneer iemand beschikt over de DigiD van een ander persoon. Er zijn grofweg twee manieren om identiteitsroof te plegen met behulp van DigiD. De eerste methode is het aanvragen van een DigiD op basis van de gegevens van een andere persoon. De tweede methode is het in gebruik nemen van een reeds bestaande DigiD behorende bij een andere persoon.

5.2.1 Onrechtmatig aanvragen van een DigiD

Bij het aanvragen van een DigiD wordt in de landelijk raadpleegbare deelverzameling getoetst of de door de aanvrager opgegeven combinatie van sofinummer, geboortedatum, postcode en huisnummer correct is. Indien iemand identiteitsroof wil plegen door een DigiD aan te vragen voor een andere persoon, moet hij dus in ieder geval over deze gegevens van de andere persoon beschikken.

Wanneer iemand een DigiD behorend bij een persoon die hij kent wil aanvragen, beschikt hij mogelijk al over diens geboortedatum en adresgegevens. Als hij deze echter niet heeft of een DigiD aanvraagt behorend bij een persoon die hij niet kent, zijn deze gegevens doorgaans redelijk eenvoudig te achterhalen. De meeste Nederlanders hebben geen geheim telefoonnummer en staan met naam en adres in de telefoongids. Achternaam en woonplaats kunnen al voldoende zijn om de postcode en het huisnummer te verkrijgen. Indien er meerdere mensen met dezelfde achternaam in een stad of dorp wonen, volstaan dikwijls de voorletters en/of een indicatie van de wijk waar iemand woont.

Een korte rondgang op internet leert dat het niet moeilijk hoeft te zijn om iemands geboortedatum te verkrijgen. Een groot aantal mensen vermeldt deze pontificaal op de persoonlijke website of bij het eigen profiel op netwerksites als hyves en myspace. Even op Google zoeken op iemands naam leidt dikwijls tot heel wat persoonsgegevens van de persoon in kwestie. Een andere, meer gewiekste, manier om te proberen iemands geboortedatum te achterhalen wordt geboden door de website www.jarig.nl waar mensen online een verjaardagskalender bij kunnen houden. In het geval men de exacte datum van iemands verjaardag niet weet, biedt deze website de mogelijkheid een mailtje te sturen naar de persoon in kwestie waarin om de geboortedatum gevraagd wordt. De aanvrager kan zich hierbij voordoen als een bekende, zonder dat degene die het mailtje krijgt kan zien van wie het verzoek om zijn geboortedatum afkomstig is.

Stel dat een kwaadwillende erin is geslaagd de hierboven genoemde adresgegevens en geboortedatum van iemand anders te achterhalen, dan heeft hij alleen nog diens sofinummer nodig om een DigiD voor hem of haar aan te kunnen vragen. Het sofinummer is minder eenvoudig te verkrijgen dan de hierboven genoemde gegevens, omdat mensen dit doorgaans niet op hun website zullen plaatsen en ook minder snel zullen verstrekken aan iemand die zich voordoet als een bekende. Er is immers geen enkele noodzaak voor een bekende om dit nummer te kennen. Toch is het bepaald niet onmogelijk om iemands sofinummer in handen te krijgen. Door het groeiende gebruik van het sofinummer vermelden steeds meer organisaties het in hun correspondentie. Naast de belastingdienst en werkgevers geldt dit bijvoorbeeld ook voor de Informatie Beheer Groep en zorgverzekeraars. Dit aantal zal bovendien fors stijgen na invoering van het burgerservicenummer, wanneer de gehele publieke sector dit nummer gaat gebruiken. Een kwaadwillende kan proberen dergelijke correspondentie te onderscheppen voor deze de geadresseerde bereikt, door deze te ontvreemden uit de brievenbus, van de postbode of uit het postkantoor. Ook kan hij het oud papier van de persoon wiens sofinummer hij wil achterhalen doorzoeken op dergelijke correspondentie.

Hierboven werd de situatie beschreven, waarin iemand op zoek is naar het sofinummer van een vooraf bepaalde persoon. Het omgekeerde kan ook voorkomen, wanneer men begint bij het sofinummer en de hierbij behorende persoon wil achterhalen. Formeel wordt het sofinummer geacht een inhoudsloos nummer te zijn, dat niet te herleiden is tot beschrijvende informatie over de persoon bij wie het hoort. In de praktijk hoeft dit echter lang niet altijd het geval te zijn.

In diverse alledaagse situaties wordt gevraagd om het tonen of afgeven van (een kopie van) het paspoort, identiteitsbewijs of zorgverzekeringpas, zoals bijvoorbeeld bij de receptie van het ziekenhuis, bij de tandarts, bij het inchecken in een hotel, bij het inschrijven bij een uitzendbureau of bij het kopen van een telefoonabonnement. In al deze gevallen beschikt de ontvanger direct over de naam, geboortedatum en sofinummer van de persoon in kwestie.

Naast de reeds beschreven manieren om de benodigde persoonsgegevens te verkrijgen kan men ook gebruik maken van phishing, social engineering en keyloggers. Hierop kom ik in de volgende paragraaf, die handelt over het in gebruik nemen van een bestaande DigiD, terug.

Stel nu dat een kwaadwillende, bijvoorbeeld door gebruikmaking van één of meer van de hiervoor genoemde methoden, de beschikking heeft gekregen over een combinatie van een sofinummer, een geboortedatum, een postcode en een huisnummer, dan kan hij hiermee een DigiD aanvragen. Hij kan hierbij zelf een gebruikersnaam en wachtwoord kiezen en tevens zijn eigen mobiele telefoonnummer opgeven. Alvorens hij de DigiD kan gebruiken, dient hij deze eerst te activeren. Hiervoor moet hij echter wel over de activeringscode beschikken, die per post wordt verstuurd naar het adres waarop de persoon op wiens sofinummer de DigiD is aangevraagd staat ingeschreven in de gemeentelijke basisadministratie. Hij zal deze dus moeten onderscheppen alvorens de geadresseerde hem ontvangt, door hem te ontvreemden uit de brievenbus, van de postbode of uit het postkantoor.
Indien hij hierin slaagt, heeft hij de beschikking over een DigiD waarmee hij zich kan voordoen als een ander persoon, zonder dat die persoon daar op het moment van activeren weet van heeft. De rechtmatige eigenaar van de DigiD, dat wil zeggen de persoon op wiens sofinummer de DigiD is aangevraagd, zal de identiteitsroof pas in de gaten krijgen op het moment dat hij gevolgen ondervindt van door de identiteitsrover aangevraagde diensten of op het moment dat hij zelf een DigiD wil aanvragen. In dit laatste geval krijgt hij namelijk de melding dat er reeds een DigiD in omloop is voor het betreffende sofinummer. Ook als de kwaadwillende er niet in slaagt de activeringscode te onderscheppen, weet de ontvanger dat iemand anders heeft geprobeerd op zijn naam een DigiD aan te vragen.

5.2.2 Onrechtmatig gebruiken van een bestaand DigiD

In de vorige paragraaf heb ik beschreven hoe iemand een DigiD kan aanvragen op basis van de persoonsgegevens van iemand anders. Ik heb daarbij buiten beschouwing gelaten of de persoon wiens identiteit geroofd wordt al over een DigiD beschikte. Dit maakt echter niets uit voor het aanvragen van een DigiD. Ook als er al een DigiD in omloop was, kan men er opnieuw één aanvragen op basis van dezelfde persoonsgegevens. Hier is voor gekozen omdat DigiD geen gebruikersnaam of wachtwoord verstuurt naar gebruikers. Daarom kan een gebruiker die (één van) beide is vergeten een nieuwe DigiD aanvragen. Direct gevolg van deze keuze is echter wel dat ieder ander ook een nieuwe DigiD kan aanvragen voor elke persoon van wie hij sofinummer, geboortedatum en adres kent. Zodra de nieuwe gebruikersnaam is aangevraagd (dus nog voor de DigiD is geactiveerd), vervallen de bestaande gebruikersnaam en wachtwoord. Een eerste verschil met de situatie waarin er nog geen DigiD in omloop was, is dat de rechtmatige eigenaar de identiteitsroof nu ook opmerkt als hij gebruik wil maken van zijn DigiD en zijn gebruikersnaam en wachtwoord niet geaccepteerd worden. Een tweede verschil is dat het ook mogelijk is de DigiD aan te vragen zonder de intentie te hebben om er daadwerkelijk gebruik van te maken, maar uitsluitend om de rechtmatige eigenaar ervan te treiteren door middel van een Denial of Service aanval. Deze kan immers geen gebruik maken van zijn DigiD en geen nieuwe aanvraag indienen zolang de huidige aanvraag niet geactiveerd is of de activering verlopen is. (Deze verloopt 3 weken na het aanvragen.)

Het is ook mogelijk om de bestaande DigiD van iemand anders te gebruiken, zonder een nieuwe aan te vragen. In dit geval moet men de combinatie van gebruikersnaam en wachtwoord zien te achterhalen. Beiden zijn door de aanvrager zelf gekozen en hebben een variabele lengte. De gebruikersnaam is minimaal 4 tekens lang en mag bestaan uit hoofdletters, kleine letters, cijfers en de tekens ‘-‘ en ‘_’. Het wachtwoord is minimaal 8 en maximaal 32 tekens lang, mag zowel uit letters, cijfers als speciale tekens bestaan, en moet minimaal één cijfer en één letter bevatten. Deze eisen en het gegeven dat op 3 foute pogingen het DigiD 10 minuten geblokkeerd wordt, maken de kans op het toevallig raden van gebruikersnaam en wachtwoord aanzienlijk kleiner.

De zwakste schakel blijkt echter doorgaans de gebruiker zelf te zijn. Hoewel DigiD de gebruikers nadrukkelijk adviseert zorgvuldig om te gaan met hun gebruikersnaam en wachtwoord en deze nergens op te schrijven, is het maar de vraag hoeveel personen dit advies ook daadwerkelijk opvolgen. Iemand die denkt zijn DigiD maar één keer per jaar te gebruiken, bijvoorbeeld voor de belastingaangifte, en er weinig voor voelt elk jaar een nieuwe DigiD aan te vragen, zal al snel geneigd zijn dit toch op te schrijven. De strenge eisen die aan het wachtwoord gesteld worden en de grote hoeveelheid aan overige wachtwoorden waar de gemiddelde internetgebruiker mee te maken heeft, vergroten de kans op vergeten ervan immers fors. Het opschrijven van deze gegevens brengt het risico met zich mee dat deze in verkeerde handen vallen.

Een kwaadwillende kan bovendien proberen de gebruikersnaam en het wachtwoord te achterhalen door middel van phishing. Hiervan is sprake als mensen onder valse voorwendselen gelokt worden naar een website waarvan zij ten onrechte denken dat deze betrouwbaar is bijvoorbeeld omdat het een kopie is van de website van DigiD. Wanneer zij hier hun gebruikersnaam en wachtwoord invullen, zijn zij in de veronderstelling die naar DigiD te sturen, maar in feite verschaffen zij deze aan de oplichter.
Een andere manier om door middel van misleiding de beschikking te krijgen over de gebruikersnaam en het wachtwoord is social engineering. In dit geval kan iemand zich bijvoorbeeld voordoen als een medewerker van DigiD en de gebruiker proberen over te halen deze gegevens af te staan.
Tenslotte kan een kwaadwillende ervoor kiezen een keylogger te installeren of te verspreiden met behulp van kwaadaardige software. Deze keylogger registreert alle ingevoerde waarden, dus ook gebruikersnamen en wachtwoorden van diverse authenticatievoorzieningen, waaronder DigiD.
Zoals reeds aangegeven in de vorige paragraaf kunnen phishing, social engineering en keyloggers ook gebruikt worden om de voor aanvraag van een DigiD benodigde persoonsgegevens te verkrijgen.

Wanneer men eenmaal beschikt over de gebruikersnaam en het wachtwoord is het ook zonder de mobiele telefoon te stelen van de rechtmatige eigenaar van de DigiD mogelijk om toegang te krijgen tot diensten die authenticatie op zekerheidsniveau midden vereisen. Met enkel de gebruikersnaam en het wachtwoord kan men namelijk sms-authenticatie aanvragen op een mobiel telefoonnummer naar keuze, indien dit nog niet was aangevraagd. Indien dit wel al was aangevraagd kan men, wederom met enkel de gebruikersnaam en het wachtwoord, de optie tot sms-authenticatie opzeggen en vervolgens opnieuw aanvragen voor een mobiel telefoonnummer naar keuze.

Wel geldt in beide gevallen dat eerst een activeringscode, die per post verstuurd wordt naar het adres waarop de rechtmatige eigenaar van de DigiD staat ingeschreven in de gemeentelijke basisadministratie, moet worden ingetoetst alvorens sms-authenticatie op het nieuw opgegeven telefoonnummer mogelijk is. Deze activeringscode moet dus, net als bij het onrechtmatig aanvragen van een DigiD, onderschept worden door de identiteitsrover voor deze de geadresseerde bereikt.

5.2.3 Kritiek

In de vorige paragrafen is aangetoond hoe iemand identiteitsroof kan plegen met behulp van DigiD. In het geval van phishing, social engineering, keyloggers of het onzorgvuldig omgaan met gebruikersnaam en wachtwoord ligt de verantwoordelijkheid hiervan bij de burger. De overheid is echter wel verantwoordelijkheid voor een aantal andere zaken die identiteitsroof mogelijk maken. Deze zaken komen hieronder aan bod.

Bij het plegen van identiteitsroof met behulp van DigiD is een cruciale rol weggelegd voor de activeringsprocedure. Allereerst kan men een (op)nieuw aangevraagde DigiD pas gebruiken wanneer deze geactiveerd is. Bovendien kan men na activering gebruik maken van sms-authenticatie op een zelfgekozen mobiel telefoonnummer, wanneer men de gebruikersnaam en wachtwoord van een andere gebruiker heeft weten te achterhalen. Het is dan ook kwalijk dat bij de activeringsprocedure op geen enkele wijze gecontroleerd wordt wie deze procedure uitvoert. Zowel de aanvraagprocedure van DigiD als de gebruikte authenticatiemiddelen lijken erg op de door de Postbank voor het internetbankieren gebruikte aanvraagprocedure en authenticatiemiddelen. Bij de Postbank kan de aanvrager echter niet zelf een gebruikersnaam en wachtwoord kiezen, maar krijgt hij beide toegewezen. In het verleden werden de gebruikersnaam, het wachtwoord en de activeringscode alle per post verstuurd, in drie verschillende brieven. Klaarblijkelijk vond men dit toch de nodige risico's met zich meebrengen, want tegenwoordig wordt het wachtwoord niet langer per post verstuurd. In plaats hiervan ontvangt de aanvrager een bericht dat hij zijn wachtwoord kan komen ophalen op het postkantoor. Hij moet zich hierbij legitimeren. De activeringsprocedure binnen DigiD kan op dezelfde wijze worden ingevuld, door de burger een activeringscode te laten ophalen op het gemeentehuis, waarbij hij zich dient te legitimeren.

Een tweede kwalijk punt is het gemak waarmee iemand een DigiD kan aanvragen op basis van persoonsgegevens van iemand anders. Extra kwalijk hierbij is dat een dergelijke nieuwe aanvraag automatisch leidt tot het vervallen van de bestaande gebruikersnaam en wachtwoord, ook als de nieuwe aanvraag niet geactiveerd wordt. De overheid zou ervoor kunnen kiezen de bestaande gebruikersnaam en wachtwoord pas te laten vervallen op het moment dat de nieuwe aanvraag geactiveerd is. Een betere oplossing is echter te kiezen voor een aanvraagprocedure op basis van moeilijker te achterhalen persoonsgegevens. In plaats van het sofinummer zou bijvoorbeeld gekozen kunnen worden voor de combinatie van het nummer van een paspoort, identiteitsbewijs, rijbewijs of verblijfsvergunning en de geldigheidsdatum van dit document.

Tenslotte heeft een hoger zekerheidsniveau geen enkele meerwaarde als men dit vanuit het basisniveau kan toevoegen of wijzigen. Wel is het zo dat de toevoeging van sms-authenticatie eerst geactiveerd moet worden. Zolang deze activeringsprocedure echter niet wordt verbeterd, bijvoorbeeld op de manier zoals hierboven is voorgesteld, biedt deze weinig zekerheid.

Het wijzigen van een mobiel telefoonnummer is zeer merkwaardig ingevuld. Met de oorspronkelijke activeringscode die is verkregen bij het toevoegen van de sms-authenticatie kan men het opgegeven telefoonnummer wijzigen in een nieuw nummer. Om deze reden wordt in de brief met activeringscode vetgedrukt opgedragen deze brief goed te bewaren. Men draagt de burger dus enerzijds op zijn gebruikersnaam en wachtwoord, die hem toegang geven tot zekerheidsniveau basis, in geen geval op te schrijven om te voorkomen dat deze in verkeerde handen vallen. Anderzijds verwacht men wel dat diezelfde burger de activeringscode, waarmee het telefoonnummer kan worden opgegeven waarop de codes worden doorgegeven die toegang geven tot zekerheidsniveau midden, schriftelijk bewaart.
Overigens is het ook mogelijk het telefoonnummer te wijzigen zonder in het bezit te zijn van de oorspronkelijke activeringscode. In dat geval dient men eerst de sms-authenticatie op te heffen. Hiervoor zijn alleen de gebruikersnaam en wachtwoord benodigd. Vervolgens kan men sms-authenticatie weer toevoegen met opgave van het nieuwe nummer. Hierbij wordt een nieuwe activeringscode verzonden en geldt hetzelfde als in de eerstgenoemde situatie.

5.3 Authenticatie met behulp van DigiD

Bij authenticatie is een gouden regel dat de sterkste partij als eerste (een deel van) zijn identiteit prijsgeeft (Jacobs, 2007). Authenticatie met DigiD voldoet aan deze regel, doordat gebruik wordt gemaakt van een ssl-certificaat. Alvorens een burger zijn gebruikersnaam doorgeeft, kan hij aan het certificaat zien dat hij daadwerkelijk met DigiD communiceert. Vervolgens kan de burger zich authenticeren door gebruikmaking van het authenticatiemiddel behorend bij het gewenste zekerheidsniveau. De gekozen zekerheidsniveaus komen overeen met een veelgebruikte indeling van authenticatietechnieken. Deze indeling kent drie categorieën:

- authenticatietechnieken gebaseerd op iets wat een persoon weet
- authenticatietechnieken gebaseerd op iets wat een persoon heeft
- authenticatietechnieken gebaseerd op iets wat een persoon is

De meestgebruikte authenticatiemethode op basis van iets wat een persoon weet is het wachtwoord. DigiD gebruikt deze methode om zekerheidsniveau basis in te vullen.

Authenticatietechnieken gebaseerd op iets wat een persoon heeft, maken gebruik van een fysiek instrument. Dit kan bijvoorbeeld een smartcard zijn, of in het geval van DigiD een mobiele telefoon. Omdat dergelijke instrumenten vatbaar zijn voor diefstal, dienen zij altijd in combinatie te worden gebruikt met een andere authenticatietechniek (De Boer, 2004). Zekerheidsniveau midden van DigiD vult dit in door een eenmalige code die naar de mobiele telefoon van de burger gestuurd wordt te combineren met gebruikmaking van het wachtwoord bekend van zekerheidsniveau basis. De combinatie van verschillende authenticatietechnieken maakt deze categorie van technieken sterker dan de eerstgenoemde categorie.

De derde categorie van authenticatietechnieken maakt gebruik van fysieke- of gedragskenmerken van de persoon die zich authenticeert. Dit wordt geacht de sterkste categorie te zijn omdat deze uitgaat van unieke, onveranderlijke kenmerken die een persoon heeft. De bedoeling is dat het hoogste zekerheidsniveau van DigiD zal worden ingevuld met een authenticatiemiddel behorende tot deze categorie, namelijk de elektronische Nederlandse Identiteitskaart (eNIK) die gebruik gaat maken van biometrie. Momenteel is dit zekerheidsniveau echter nog niet beschikbaar.

Na afloop van een geslaagde authenticatie met behulp van DigiD ontvangt de overheidsdienst waar een burger gebruik van wil maken het bericht dat burger B met burgerservicenummer BSN_B zich succesvol heeft geauthenticeerd op een bepaald zekerheidsniveau. De overheidsdienst behoort er nu met een bepaalde mate van zekerheid, afhankelijk van het gekozen zekerheidsniveau, vanuit te kunnen gaan dat de persoon die de dienst aanvraagt inderdaad de persoon met dit burgerservicenummer is.
Idealiter wordt deze mate van zekerheid in het geval van niveau basis uitsluitend ingeperkt door het risico dat iemands wachtwoord in verkeerde handen valt. In het geval van niveau midden bestaat de onzekerheid idealiter uitsluitend uit het risico dat een buitenstaander niet alleen het wachtwoord van iemand anders weet te achterhalen, maar ook diens mobiele telefoon in handen krijgt. In de praktijk ligt het echter anders.

Om de risico's te beperken tot de bovengenoemde gewenste waarden, dient men er allereerst zeker van te zijn dat een DigiD behorend bij burgerservicenummer BSN_B uitsluitend wordt uitgereikt aan de persoon met burgerservicenummer BSN_B. Hoewel dit vanzelfsprekend klinkt, is dit momenteel niet het geval. Ik heb eerder in dit hoofdstuk al aangegeven dat het mogelijk is het DigiD behorend bij het burgerservicenummer van iemand anders aan te vragen en te activeren. Ik heb daarbij als oplossing aangedragen een aanvraagprocedure gebaseerd op moeilijker te achterhalen persoonsgegevens dan sofinummer, geboortedatum en woonadres, aangevuld met een activering op basis van een activeringscode die op het gemeentehuis wordt overhandigd na legitimatie. Op deze wijze kan zekerheidsniveau basis ook daadwerkelijk de gewenste zekerheid bieden.

Ten tweede dient men er zeker van te zijn dat het mobiele telefoonnummer dat wordt gebruikt voor sms-authenticatie van de DigiD behorende bij burgerservicenummer BSN_B daadwerkelijk het telefoonnummer is van de persoon met burgerservicenummer BSN_B. Dit telefoonnummer kan bij de aanvraag van de DigiD worden opgegeven, het kan ook later worden toegevoegd of gewijzigd met behulp van de gebruikersnaam en het wachtwoord. In beide gevallen is een activeringscode vereist alvorens sms-authenticatie mogelijk is. Door deze activeringscode ook bij wijziging of toevoeging van een mobiel telefoonnummer op het gemeentehuis te overhandigen na legitimatie, kan men ook op zekerheidsniveau midden het gewenste niveau van zekerheid bereiken.

5.4 Persoonsgegevens

Wanneer iemand een DigiD aanvraagt worden de door hem opgegeven persoonsgegevens opgeslagen in een centrale database. De adresgegevens en de geboortedatum worden 10 weken na het aanvragen van de DigiD uit de database verwijderd. De overige persoonsgegevens, namelijk het burgerservicenummer, de gebruikersnaam, het wachtwoord en eventueel het mobiele telefoonnummer en e-mailadres, blijven bewaard gedurende het bestaan van de DigiD. Aangezien de DigiD database uitsluitend door de burger opgegeven persoonsgegevens bevat, bepaalt de burger zelf welke gegevens van hem worden opgeslagen. Bovendien is hij zelf de initiatiefnemer, omdat de gegevens pas worden opgeslagen als hij zelf een DigiD aanvraagt. Op het moment dat een burger zich succesvol heeft geauthenticeerd met behulp van DigiD wordt het burgerservicenummer behorende bij de gebruikte DigiD verzonden naar een overheidsdienst waar deze burger gebruik van wil maken. De burger neemt hiertoe zelf het initiatief door de overheidsdienst te benaderen en vervolgens zichzelf te authenticeren. Zowel bij opslag als verwerking van de persoonsgegevens is de burger dus de initiatiefnemer.

Het beheer van de hierboven beschreven persoonsgegevens ligt niet bij de burger, aangezien deze gegevens centraal worden opgeslagen in een database bij DigiD. GBO.Overheid is formeel en juridisch verantwoordelijk voor het beheer ervan, maar heeft de uitvoering uitbesteed aan de belastingdienst. De beheerder van de persoonsgegevens bepaalt niet alleen de wijze en locatie van opslag, maar reguleert ook de toegang tot deze gegevens. GBO.Overheid is dus bij zowel de opslag als de verwerking van de persoonsgegevens de verantwoordelijke. De keuze voor één centrale database met daarin zowel de identificerende persoonsgegevens als de authenticatiemiddelen (gebruikersnaam, wachtwoord en eventueel mobiel telefoonnummer), heeft als gevolg dat iemand die toegang weet te krijgen tot deze database direct de beschikking heeft over de complete verzameling gegevens.
In plaats van een centrale database had men ook voor een compleet tegenovergestelde benadering kunnen kiezen, namelijk een decentrale invulling waarbij de regie in handen van de burger is. Door de burger zijn eigen persoonsgegevens te laten beheren, bepaalt hij niet alleen zelf of en wanneer hij deze wil delen met iemand anders, maar ook welke persoonsgegevens hij wil delen met anderen. In deze benadering is de burger de verantwoordelijke bij de opslag en de verwerking van zijn eigen persoonsgegevens.

In een eerder hoofdstuk heb ik al aangegeven dat mensen verschillende rollen vervullen en dat privacy het mogelijk maakt een onderscheid te maken tussen deze rollen. Het koppelen van informatie uit verschillende domeinen, brengt het risico met zich mee dat gegevens gekoppeld worden uit rollen die de betrokkenen gescheiden wensen te houden. Ook tegenover de overheid speelt een burger verschillende rollen. Deze verschillende rollen worden binnen DigiD echter niet onderkend. Voor DigiD vervult iemand die een overheidsdienst wil afnemen in alle gevallen dezelfde rol, namelijk de eigenaar van een bepaald sofinummer.

DigiD maakt dus geen gebruik van scheiding van gegevens, terwijl deze vorm van PET uitstekend is in te passen binnen het gebruikte systeem.
Ik zal hieronder een invulling van DigiD geven, waarbij de identificerende persoonsgegevens worden gescheiden per domein. Binnen DigiD kan een persoon worden geïdentificeerd door een uniek nummer, dat uitsluitend bekend is bij DigiD en de burger die erdoor geïdentificeerd wordt. Dit moet dus een nieuw nummer zijn, omdat het sofinummer dusdanig veel gebruikt wordt, dat hiervan niet langer kan worden verondersteld dat buitenstaanders hier niet over kunnen beschikken. De overheidsdiensten die voor authenticatie gebruik maken van DigiD worden ingedeeld in verschillende sectoren, waarbij elke sector een eigen sectoraal identiteitsnummer gebruikt om een burger te identificeren. Deze sectorale nummers komen uiteraard niet overeen met het door DigiD gebruikte identiteitsnummer. 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.
Wanneer een burger gebruik wil maken van een overheidsdienst waarvoor hij zich moet authenticeren met behulp van DigiD, verandert er voor de burger niets. Hij geeft nog steeds zijn gebruikersnaam en wachtwoord op, eventueel vergezeld van zijn mobiele telefoonnummer, en kan na een succesvol verloop gebruik maken van de overheidsdienst. De overheidsdienst communiceert nu niet langer met DigiD, maar met de partij die als tolk optreedt. Indien de authenticatie succesvol verloopt, stuurt DigiD het algemene identiteitsnummer naar de tolk. Deze vertaalt dit naar het sectorale identiteitsnummer en stuurt dit vervolgens door naar de overheidsdienst. Deze beschikt dus niet over het globale identiteitsnummer en kan dan ook geen koppeling leggen met gegevensverzamelingen uit andere domeinen.

Ook bij dit systeem is het mogelijk te kiezen voor een decentrale oplossing. In dat geval is de burger de enige die in staat is de koppeling te leggen tussen sectorale nummers behorende bij verschillende sectoren. Grijpink (2006) stelt dat de bestrijding van identiteitsfraude een gedifferentieerd persoonsnummerbeleid vereist, waarbij een aantal verschillende en onafhankelijk van elkaar beheerde sectornummers worden gebruikt. Ook stelt hij dat een algemeen persoonsnummer niet verplicht of openbaar mag zijn en niet mag worden verspreid of gebruikt voor externe communicatie. Een systeem zoals hierboven voorgesteld voldoet aan deze eisen, mits het globale identiteitsnummer pas wordt gecreëerd op het moment dat iemand zich aanmeldt bij DigiD en het dus geen algemeen toegewezen nummer is.

6 Conclusies

6.1 Inleiding

In dit hoofdstuk wordt met behulp van de eerder beschreven onderzoeksresultaten een antwoord gegeven op de onderzoeksvraag. Eerst wordt in paragraaf 6.2 per deelvraag een antwoord geformuleerd en vervolgens wordt in paragraaf 6.3 met behulp van deze antwoorden de hoofdvraag beantwoord. In paragraaf 6.4 volgen tenslotte aanbevelingen ter verbetering van DigiD.

6.2 Beantwoording deelvragen

Naast de hoofdvraag kent mijn onderzoek acht deelvragen. In deze paragraaf worden deze deelvragen achtereenvolgens beantwoord. Bij het beantwoorden van deze deelvragen maak ik steeds gebruik van hetzelfde voorbeeld waarbij een burger op de website van de gemeente waar hij woont een uittreksel uit de gemeentelijke basisadministratie aanvraagt.

1. *Welke eisen stelt de Wet Bescherming Persoonsgegevens aan het verwerken van persoonsgegevens?*

De Wet Bescherming Persoonsgegevens stelt dat persoonsgegevens niet voor andere doelen mogen worden gebruikt dan de doelen waarvoor ze verkregen zijn. Bij het verzamelen van persoonsgegevens moet de betrokkene worden geïnformeerd over de identiteit van de voor de verwerking verantwoordelijke, de doeleinden van de gegevensverwerking, de ontvangers van persoonsgegevens en een eventuele overdracht naar derde landen. Mededeling is echter niet nodig indien de betrokkene op de hoogte is van het verkrijgen van de gegevens door de organisatie die de gegevens verwerkt. Iedereen heeft het recht om onjuiste of onvolledige registratie van de eigen gegevens te laten corrigeren of verwijderen. Verder stelt de Wet Bescherming Persoonsgegevens dat de verantwoordelijke voor de verwerking van de persoonsgegevens passende technische en organisatorische maatregelen moet nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Bij DigiD begint de verzameling van persoonsgegevens van een bepaald persoon bij het aanvragen van een DigiD. De aanvrager stelt zelf een aantal persoonsgegevens ter beschikking van DigiD en moet hierbij de gebruiksvoorwaarden van DigiD accepteren om de aanvraag te kunnen voltooien.

In deze gebruiksvoorwaarden staan de doeleinden van gegevensverwerking, de voor de verwerking verantwoordelijke en de ontvangers van de gegevens vermeld. De doeleinden van gegevensverwerking zijn het verifiëren van de identiteit van de gebruiker van een DigiD door de aanbieder van een overheidsdienst en het controleren op misbruik of oneigenlijk gebruik van DigiD. In het geval van het aanvragen van een uittreksel uit de gemeentelijke basisadministratie is het doel van de gegevensverwerking het verifiëren van de identiteit van de aanvrager van het uittreksel door de gemeente waar deze woonachtig is.
De voor de verwerking verantwoordelijke is in alle gevallen GBO.Overheid.

De ontvangers van de gegevens zijn de gebruiker zelf, GBO.Overheid en de aanbieder van de overheidsdienst die de identiteit van de gebruiker verifieert. In het voorbeeld is deze overheidsdienst de gemeente waar de aanvrager van het uittreksel uit de gemeentelijke basisadministratie woonachtig is. Wanneer elk van deze ontvangers toegang krijgt tot welke persoonsgegevens vormt een aparte deelvraag. Hierop kom ik later in dit hoofdstuk uitgebreid terug.
De eigenaar van een DigiD kan na inloggen zijn eigen gegevens aanpassen of verwijderen, dus ook aan dit vereiste is voldaan. De getroffen technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking vormen een aparte deelvraag. Ook hierop kom ik later in dit hoofdstuk terug.

2. *Tot welke persoonsgegevens reguleert DigiD toegang?*

Bij de beantwoording van de eerste deelvraag is aangegeven dat binnen DigiD persoonsgegevens worden verwerkt met twee doeleinden. Bij het eerste doeleinde, het verifiëren van de identiteit van de gebruiker, worden de persoonsgegevens verwerkt die de gebruiker zelf heeft opgegeven bij zijn aanvraag. Deze gegevens zijn het burgerservicenummer van de gebruiker, een zelfgekozen gebruikersnaam, een zelfgekozen wachtwoord en eventueel een e-mailadres en een mobiel telefoonnummer. Tevens horen bij deze categorie ook enkele persoonsgegevens die gebruikt worden voor het verifiëren van de aanvraag, namelijk de geboortedatum van de gebruiker, zijn postcode en huisnummer en eventueel een huisnummertoevoeging.

Bij het tweede doeleinde, het controleren op misbruik of oneigenlijk gebruik van een DigiD, wordt de toegang gereguleerd tot persoonsgegevens die niet door de gebruiker zelf zijn opgegeven. Hier gaat het om logs van transacties.

Alle aanvragen, activeringen en opzeggingen van DigiD, evenals alle wijzigingen in persoonlijke gegevens en alle authenticatiepogingen die worden ondernomen, worden opgeslagen. De gegevens die worden gelogd zijn het burgerservicenummer van de burger in kwestie, de actie die door hem is uitgevoerd en het tijdstip en de datum waarop deze actie plaatsvond. Tevens wordt het IP-adres waar het verzoek vandaan is gekomen opgeslagen, evenals de dienst waarbij de actie is uitgevoerd. In het geval van het aanvragen van een uittreksel uit de gemeentelijke basisadministratie is dit de gemeente waar de aanvrager woonachtig is.

3. *Waar worden deze persoonsgegevens opgeslagen, door wie gebeurt dit en hoelang blijven deze persoonsgegevens op deze plaats opgeslagen?*

Alle door de gebruiker bij aanvraag opgegeven persoonsgegevens worden door GBO.Overheid in een centrale database opgeslagen. GBO.Overheid is formeel en juridisch verantwoordelijk voor het beheer van deze database, maar heeft de uitvoering hiervan uitbesteed aan de belastingdienst. De bij aanvraag opgegeven geboortedatum en adresgegevens blijven 10 weken na aanvraag bewaard en worden hierna uit de database verwijderd. De overige door de gebruiker opgegeven persoonsgegevens, namelijk het burgerservicenummer, de gebruikersnaam, het wachtwoord en eventueel een e-mailadres en mobiel telefoonnummer, blijven bewaard gedurende het bestaan van de DigiD of tot de gebruiker ze wijzigt of verwijdert. In principe blijft een DigiD net zo lang bestaan tot de gebruiker deze verwijdert, maar indien een DigiD anderhalf jaar niet gebruikt is, vervalt deze en worden de bijbehorende persoonsgegevens verwijderd uit de database van DigiD. Ook kan GBO.Overheid in geval van misbruik besluiten een DigiD te verwijderen.

De logs van transacties blijven 3 maanden bewaard op de productieomgeving van DigiD om ondersteuning te kunnen bieden aan burgers. Om statistieken te kunnen uitvoeren over een bepaalde periode en om prognoses te kunnen maken voor de toekomst, worden deze logs versleuteld voor langere tijd op een apart Management Informatie systeem opgeslagen. Wat “langere tijd” is heb ik ondanks herhaald aandringen niet kunnen achterhalen. Voor het bepalen van statistieken is het voldoende om de logs geanonimiseerd op te slaan. Een aanbeveling is daarom om na afloop van de 3 maanden dat de logs bewaard blijven op de productieomgeving van DigiD, deze logs eerst te anonimiseren alvorens ze op te slaan op het voor statistieken gebruikte Management Informatie systeem. Voor eventuele audit trails, zoals bijvoorbeeld fraudeonderzoeken, worden de logs voor langere tijd versleuteld op tape bewaard bij GBO.Overheid.

4. *Wie behoren op welk moment toegang te hebben tot (een deel van) deze gegevens op grond van de Wet Bescherming Persoonsgegevens?*

Op het moment dat een burger een DigiD aanvraagt, of als hij op een later moment zijn e-mailadres of mobiel telefoonnummer wijzigt of toevoegt, geeft hij hiermee een aantal persoonsgegevens aan GBO.Overheid. Laatstgenoemde is op grond van de Wet Bescherming Persoonsgegevens uitsluitend bevoegd om deze persoonsgegevens te raadplegen, dan wel te verstrekken aan anderen, wanneer dit geschiedt voor het doel waarvoor de persoonsgegevens zijn verkregen. Uitzondering hierop is het opvragen door politie, inlichtingendiensten of bijzondere opsporingsdiensten, bijvoorbeeld in het kader van de Wet Bevoegdheden Vorderen Gegevens. Binnen DigiD zijn er twee doeleinden waarvoor persoonsgegevens verwerkt mogen worden, namelijk het verifiëren van de identiteit van de gebruiker van een DigiD door de aanbieder van een overheidsdienst en het controleren op misbruik of oneigenlijk gebruik van DigiD.

Het verifiëren van de identiteit van de gebruiker wordt geïnitieerd door iemand die de beschikking heeft over een DigiD en gebruik wil maken van een dienst waarvoor authenticatie vereist is, bijvoorbeeld het aanvragen van een uittreksel uit de gemeentelijke basisadministratie. Wanneer de gebruiker vervolgens zijn inlognaam en wachtwoord invoert, is GBO.Overheid op basis van de eigen gebruiksvoorwaarden bevoegd deze te vergelijken met de gegevens zoals die in de centrale database staan. Indien de burger zich wenst te authenticeren op zekerheidsniveau midden is GBO.Overheid bovendien bevoegd om het mobiele telefoonnummer te raadplegen teneinde een sms te kunnen verzenden. Indien de authenticatie succesvol is verlopen, is GBO.Overheid bevoegd het burgerservicenummer behorende bij de DigiD te verstrekken aan de overheidsdienst waarvoor verificatie van de identiteit van de gebruiker vereist was. Andere gegevens worden door GBO.Overheid niet verstrekt aan overheidsdiensten. In het geval van het aanvragen van een uittreksel uit de gemeentelijke basisadministratie, ontvangt de gemeente waarbij deze aanvraag plaatsvindt dus geen andere persoonsgegevens van de aanvrager dan zijn burgerservicenummer.

Om te kunnen controleren op misbruik worden alle transacties van DigiD gelogd. Ten behoeve van deze doelstelling is GBO.Overheid daarom bevoegd bij elke transactie het burgerservicenummer behorende bij het gebruikte DigiD te raadplegen en op te slaan, evenals het IP-adres waarvandaan de transactie werd uitgevoerd. Deze logs kunnen worden geraadpleegd op het moment dat bij de eigenaar van een DigiD of bij GBO.Overheid vermoedens bestaan over mogelijk misbruik van een DigiD.

Uitsluitend de functioneel beheerder van de Serviceorganisatie van GBO.Overheid heeft toegang tot deze logs en deze is uitsluitend bevoegd deze gegevens te verstrekken aan derden indien hier een wettelijke grondslag voor bestaat, zoals bijvoorbeeld gegeven door de Wet Bevoegdheden Vorderen Gegevens.

5. *Welke technische en organisatorische maatregelen zijn getroffen om te reguleren dat uitsluitend toegang wordt verschaft tot gegevens waartoe men volgens de Wet Bescherming Persoonsgegevens gerechtigd is en in welke mate bereiken deze maatregelen het gestelde doel?*

De technische maatregelen die zijn getroffen om te voorkomen dat onbevoegden toegang kunnen krijgen tot met behulp van DigiD verwerkte persoonsgegevens zijn algemene PET-maatregelen. Deze maatregelen zijn het versleuteld opslaan van het wachtwoord in de centrale database, het over SSL tunnelen van alle communicatie tussen de burger en de DigiD server en het tekenen van de communicatie tussen de DigiD server en de overheidsdienst waarvoor authenticatie vereist is op basis van een gedeelde sleutel. Andere, effectievere, hoofdvormen van PET-maatregelen, namelijk scheiden van gegevens, privacymanagementsystemen en anonimiseren zijn niet toegepast. Dit is opmerkelijk, aangezien zowel de Tweede Kamer als het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties zich sterk hebben uitgesproken over het gebruik van PET-maatregelen.

Een organisatorische maatregel die is getroffen om te voorkomen dat onbevoegden toegang kunnen krijgen tot met behulp van DigiD verwerkte persoonsgegevens is het gebruiken van verschillende zekerheidsniveaus. Processen die als gevoeliger beschouwd worden, kunnen authenticatie op een hoger zekerheidsniveau vereisen. Het doel hiervan is het bieden van meer zekerheid aan een overheidsdienst over de identiteit van de persoon die van deze dienst gebruik wil maken. Iedereen die over de gebruikersnaam en het wachtwoord van een DigiD beschikt, kan deze DigiD echter uitbreiden met sms-authenticatie op een mobiel nummer naar keuze, indien hij de activeringscode weet te onderscheppen die per post wordt verstuurd naar het adres waarop de rechtmatige eigenaar van de DigiD staat ingeschreven. De extra zekerheid die het niveau midden zou moeten bieden, wordt dus niet of nauwelijks geboden. Verder zijn organisatorische maatregelen getroffen om te voorkomen dat een DigiD in verkeerde handen valt. Deze maatregelen komen aan bod bij deelvraag 7 die specifiek ingaat op identiteitsroof.

6. *Op welke wijze is identiteitsroof mogelijk met DigiD?*

Er zijn grofweg twee manieren om identiteitsroof te plegen met behulp van DigiD. De eerste methode is het aanvragen van een DigiD op basis van de gegevens van een andere persoon. De tweede methode is het in gebruik nemen van een reeds bestaande DigiD behorende bij een andere persoon.

Om een DigiD aan te kunnen vragen op basis van de gegevens van een andere persoon moet men beschikken over een geldig burgerservicenummer, de geboortedatum van de persoon met dit burgerservicenummer en de postcode en het huisnummer waarop deze persoon staat ingeschreven in de gemeentelijke basisadministratie. Wanneer een onrechtmatige aanvrager vervolgens de activeringscode, die per post wordt verzonden naar het adres waarop de eigenaar van het burgerservicenummer staat ingeschreven in de gemeentelijke basisadministratie, weet te onderscheppen, kan hij hiermee de DigiD activeren.

Om een reeds bestaande DigiD behorende bij een andere persoon te kunnen gebruiken moet men in ieder geval beschikken over de gebruikersnaam en het wachtwoord behorende bij deze DigiD. Men kan deze proberen te raden of te verkrijgen door middel van phishing, social engineering of door het installeren van een keylogger of kwaadwillende software. Voorts is het niet ondenkbaar dat iemand zijn gebruikersnaam en wachtwoord opschrijft en dat dit briefje in verkeerde handen terechtkomt.

7. *Welke technische en organisatorische maatregelen zijn getroffen om identiteitsroof te voorkomen en in welke mate bereiken deze maatregelen het gestelde doel?*

Bij het antwoorden van deze vraag maak ik hetzelfde onderscheid in twee manieren om identiteitsroof te plegen als bij de vorige vraag.

Om te voorkomen dat iemand een DigiD kan aanvragen op basis van de gegevens van iemand anders is een tweetal maatregelen getroffen. Allereerst wordt gecontroleerd of het adres en de geboortedatum die zijn opgegeven overeenkomen met de gegevens die bij het betreffende burgerservicenummer bekend zijn in de landelijk raadpleegbare deelverzameling. Met name het burgerservicenummer wordt hierbij gezien als een persoonsgegeven dat niet bekend is bij derden.

De toenmalige ministers De Graaf voor Bestuurlijke Vernieuwing en Koninkrijksrelaties en Hoogervorst van Volksgezondheid, Welzijn en Sport, spreken in een brief van 14 mei 2004 waarin zij de kamer informeren over de implementatie van het burgerservicenummer van een nummer dat "op zich betekenisloos" is. Het huidige sofinummer wordt echter al in zulke hoge mate gebruikt door verschillende instanties, dan wel afgedrukt op correspondentie of documenten, dat het betrekkelijk eenvoudig is om een correcte combinatie van sofinummer, geboortedatum en woonadres te verkrijgen. Het geplande overheidsbrede gebruik van het burgerservicenummer zal dit nog versterken.

Een tweede maatregel is het per post versturen van een activeringscode naar het adres waarop de persoon op wiens sofinummer de DigiD is aangevraagd staat ingeschreven in de gemeentelijke basisadministratie. Wanneer deze activeringscode niet binnen 3 weken wordt ingetoetst, komt de aangevraagde DigiD te vervallen. Tevens kan geen nieuwe DigiD worden aangevraagd zolang de oude aanvraag nog niet geactiveerd is en deze 3 weken nog niet om zijn. Wanneer iemand die een DigiD op basis van de gegevens van iemand anders heeft aangevraagd de activeringscode weet te onderscheppen voor deze de geadresseerde bereikt, beschikt hij echter alsnog over een werkende DigiD.

Ook om te voorkomen dat een persoon gebruik kan maken van de DigiD van iemand anders zijn maatregelen getroffen. Allereerst zijn er eisen gesteld aan de te kiezen gebruikersnaam en wachtwoord. De gebruikersnaam is minimaal 4 tekens lang en mag bestaan uit hoofdletters, kleine letters, cijfers en de tekens '-' en '_'. Ook mag deze nog niet in gebruik zijn bij DigiD. Het wachtwoord is minimaal 8 en maximaal 32 tekens lang, mag zowel uit letters, cijfers als speciale tekens bestaan, en moet minimaal één cijfer en één letter bevatten. Deze eisen bemoeilijken het achterhalen van deze gegevens.
Bovendien wordt na 3 foute pogingen het DigiD 10 minuten geblokkeerd en loopt deze blokkade bij herhaling op tot 24 uur, waardoor ook brute force aanvallen worden tegengewerkt.

Tevens wordt in een begeleidende brief bij de activeringscode voorlichting gegeven over hoe men om moet gaan met de gebruikersnaam, wachtwoord, activeringscode en transactiecodes. Hierin wordt duidelijk gemaakt dat DigiD nooit om deze gegevens zal vragen en dat men deze dan ook niet moet verstrekken aan derden. Zo probeert men te voorkomen dat een kwaadwillende door phishing of social engineering deze gegevens in handen krijgt. Ook wordt de burger hierin opgedragen zijn wachtwoord regelmatig te veranderen en niet op te schrijven.

Het is gezien de strenge eisen aan de wachtwoorden, maar de vraag of elke burger hier gehoor aan zal geven, zeker als hij zijn DigiD slechts enkele keren per jaar gebruikt. Ook is het erg tegenstrijdig dat de burger juist wel wordt opgedragen de activeringscode goed te bewaren, omdat deze opnieuw gebruikt kan worden om sms-authenticatie te activeren of een eerder opgegeven mobiel telefoonnummer te wijzigen.

Een andere getroffen maatregel is dat indien men zijn gebruikersnaam en/of wachtwoord vergeten is, DigiD deze niet verstuurt. In plaats daarvan dient men in deze gevallen een nieuwe DigiD aan te vragen. Op het moment van aanvragen vervallen de oude gebruikersnaam en het oude wachtwoord. Deze maatregel vereist echter wel dat het niet mogelijk is een DigiD aan te vragen op basis van de persoonsgegevens van iemand anders. De huidige aanvraagprocedure voldoet hier niet aan, want het is betrekkelijk eenvoudig om een correcte combinatie van sofinummer, geboortedatum en woonadres te verkrijgen. Indien iemand anders op basis van deze gegevens een nieuwe DigiD aanvraagt, leidt dit tot een Denial of Service voor de oorspronkelijke eigenaar, wiens DigiD nu geblokkeerd wordt.

Een mobiel telefoonnummer mag maximaal aan één DigiD zijn gekoppeld. Hiermee wordt voorkomen dat één persoon met behulp van dezelfde mobiele telefoon meerdere DigiD's kan gebruiken op zekerheidsniveau midden. Wanneer twee personen dezelfde telefoon delen, wordt hier echter niet mee voorkomen dat beide personen de transactiecodes kunnen ontvangen die maar voor één van hen bedoeld zijn. Ook wordt niet gecontroleerd of het opgegeven nummer daadwerkelijk het mobiele telefoonnummer van de eigenaar van de DigiD is.

Een laatste maatregel is het loggen van alle authenticatiepogingen, veranderingen in de opgegeven persoonsgegevens en aanvragen, activeringen en opzeggingen van DigiD's. Hoewel deze maatregel niet helpt bij het voorkomen van identiteitsroof, maakt deze het wel mogelijk om te achterhalen wanneer authenticaties hebben plaatsgevonden met een geroofde DigiD en voor welke overheidsdienst de authenticatie bestemd was. Zodoende kan worden achterhaald welke acties met de geroofde DigiD zijn ondernomen, zodat deze mogelijk teruggedraaid kunnen worden. Ook kan GBO.Overheid met behulp van deze logs proberen te achterhalen wie de pleger van de identiteitsroof is, bijvoorbeeld op basis van het gebruikte IP-adres.

6.3 Beantwoording onderzoeksvraag en aanbevelingen

De hoofdvraag in mijn onderzoek luidde:
In welke mate voldoen de technische en organisatorische maatregelen, die zijn getroffen om confidentialiteit en integriteit van persoonsgegevens te garanderen bij het reguleren van de toegang tot persoonsgegevens door DigiD, aan de eisen die de Wet Bescherming Persoonsgegevens stelt en op welke wijze kunnen of moeten deze maatregelen verbeterd worden?

In de vorige paragraaf heb ik aangegeven welke technische en organisatorische maatregelen zijn getroffen om de confidentialiteit en integriteit van persoonsgegevens te garanderen bij het reguleren van de toegang tot persoonsgegevens door DigiD. Ook heb ik aangegeven in hoeverre zij hun doel bereikten. Ik heb echter nog niet aangegeven hoe deze maatregelen kunnen worden verbeterd, indien zij hun doel niet of onvoldoende bereiken. De Wet Bescherming Persoonsgegevens stelt dat de verantwoordelijke voor de verwerking van de persoonsgegevens passende technische en organisatorische maatregelen moet nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. De getroffen technische maatregelen zijn algemene PET-maatregelen. De Wet Bescherming Persoonsgegevens geeft helaas geen uitsluitsel of dit voldoende is om te kunnen spreken van passende technische maatregelen. Dit uitsluitsel wordt wel gegeven door een kamerbreed aangenomen motie, waarin de regering wordt verzocht "te bevorderen dat de ontwikkeling en gebruik van PET krachtig ter hand wordt genomen en te bevorderen dat de overheid als innovatieve aanbesteding het voortouw zal nemen bij de inzet van PET bij haar eigen verwerking van persoonsgegevens." Aan dit verzoek is onvoldoende krachtig gehoor gegeven bij de ontwikkeling van DigiD, door uitsluitend algemene PET-maatregelen te implementeren.

De tweede hoofdvorm van PET, scheiding van gegevens, is uitstekend toe te passen binnen het huidige systeem en verkleint bovendien de kans op identiteitsfraude, omdat het algemene identiteitsnummer niet langer wordt gebruikt voor externe communicatie. Om dit te realiseren moet binnen DigiD een persoon worden geïdentificeerd door een uniek nummer, dat uitsluitend bekend is bij DigiD en de burger die erdoor geïdentificeerd wordt. Dit is een nieuw, niet openbaar, nummer. De overheidsdiensten die voor authenticatie gebruik maken van DigiD worden ingedeeld in verschillende sectoren, waarbij elke sector een eigen sectoraal identiteitsnummer gebruikt om een burger te identificeren. Deze sectorale nummers komen uiteraard niet overeen met het door DigiD gebruikte identiteitsnummer.

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. Wanneer een burger gebruik wil maken van een overheidsdienst waarvoor hij zich moet authenticeren met behulp van DigiD, verandert er voor de burger niets. Hij geeft nog steeds zijn gebruikersnaam en wachtwoord op, eventueel vergezeld van zijn mobiele telefoonnummer, en kan na een succesvol verloop gebruik maken van de overheidsdienst. De overheidsdienst communiceert nu niet langer met DigiD, maar met de partij die als tolk optreedt. Indien de authenticatie succesvol verloopt, stuurt DigiD het algemene identiteitsnummer naar de tolk. Deze vertaalt dit naar het sectorale identiteitsnummer en stuurt dit vervolgens door naar de overheidsdienst. Deze beschikt dus niet over het globale identiteitsnummer en kan dan ook geen koppeling leggen met gegevensverzamelingen uit andere domeinen.

In de huidige invulling van DigiD is het relatief eenvoudig om een DigiD aan te vragen op basis van de gegevens van iemand anders. Ook als de aanvrager er niet in slaagt de activeringscode te bemachtigen, ondervindt de rechtmatige eigenaar hier schade van, want een eventuele bestaande DigiD wordt geblokkeerd op het moment van een nieuwe aanvraag. Gewenst is een situatie waarin uitsluitend de persoon op wiens burgerservicenummer de DigiD staat, beschikt over de persoonsgegevens die benodigd zijn om de DigiD aan te vragen. Het burgerservicenummer voldoet hier niet aan, omdat dit te breed gebruikt wordt om als onbekend verondersteld te worden. 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.

Een aangevraagde DigiD kan pas gebruikt worden, wanneer deze is geactiveerd. In de huidige situatie wordt hiertoe een activeringscode per post verzonden naar het adres waarop de eigenaar van een burgerservicenummer staat ingeschreven in de gemeentelijke basisadministratie. Deze activeringscode kan echter onderschept worden, waardoor zowel bij de aanvraag als bij de activering van de DigiD geen garantie kan worden geboden over de identiteit van de eigenaar van de DigiD. Bij een authenticatie met DigiD wordt de overheidsdienst waarvoor een burger zich authenticeert echter wel geacht erop te kunnen vertrouwen dat dit het geval is.

Indien een burger aan het loket van een overheidsinstantie gebruik wil maken van een dienst, moet hij zich legitimeren door het tonen van zijn paspoort of identiteitskaart. Hierbij wordt niet alleen gekeken naar de persoonsgegevens die in het legitimatiebewijs staan, maar wordt ook geverifieerd of de persoon voor het loket overeen komt met de pasfoto in het legitimatiebewijs. Bij het aanvragen van een DigiD wordt wel gevraagd om een aantal identificerende persoonsgegevens die op het legitimatiebewijs staan, maar ontbreekt de verificatie met de pasfoto. Zo zal zelfs het hoogste zekerheidsniveau het qua betrouwbaarheid altijd afleggen tegenover de traditionele manier van authenticatie. Een oplossing hiervoor is het versturen van een afhaalbericht voor de activeringscode in plaats van de code zelf. Door de activeringscode pas af te geven na legitimatie op het gemeentehuis heeft men bij afgifte dezelfde zekerheid over de eigenaar van de DigiD als men zou hebben bij de afname van een overheidsdienst aan het loket. Opvallend detail hierbij is dat op basis van de Wet Identificatie Dienstverlening verplicht is gesteld dat iedereen met een bank- of girorekening zich opnieuw identificeert bij de bank of op het postkantoor. De openbare veiligheid woog in dit geval zwaarder dan het gemak van de rekeninghouder. Voor de persoonlijke veiligheid bij het gebruik van DigiD wordt een dergelijke gang naar een instantie kennelijk niet nodig geacht. Zo'n gang naar het gemeentehuis zou juist als extra voordeel kunnen hebben dat het vertrouwen van de burger in DigiD groeit, omdat een DigiD op deze manier meer gewicht krijgt.

Tenslotte zijn er de verschillende zekerheidsniveaus, die in de huidige invulling geen verhoogde zekerheid kunnen garanderen, omdat het op basis van uitsluitend een gebruikersnaam en wachtwoord mogelijk is sms-authenticatie aan te vragen op een mobiel telefoonnummer naar keuze. De meest eenvoudige aanpassing is het versturen van een afhaalbericht voor een activeringscode bij het opgeven van een nieuw telefoonnummer of het wijzigen van een bestaand nummer. Hoewel dit meer zekerheid geeft over de identiteit van de persoon die het mobiele telefoonnummer heeft opgegeven, geeft dit geen extra garantie dat dit ook echt het nummer van de mobiele telefoon van deze persoon is. Een maatregel die deze zekerheid wel kan geven, is het door een bevoegde instantie laten verifiëren van het opgegeven telefoonnummer bij het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Het is wellicht interessant een steekproef onder een aantal DigiD's uit te voeren om te bepalen in hoeverre de momenteel opgegeven telefoonnummers overeenkomen met de gegevens van het CIOT.

7 Literatuurlijst

7.1 Boeken en artikelen

Berkvens, J.M.A. en Prins, J.E.J
De bescherming van persoonsgegevens
In: Franken, H., Kaspersen, H.W.K. en De Wild, A.H. (redactie)
Recht en Computer, pagina 339-384
Kluwer, Deventer, 2004

Blok, P.
Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht
Boom Juridische Uitgevers, Den Haag, 2002

De Boer, R.J.
Alternatieve authenticatietechnieken
In: Handboek Informatievoorziening
Deel IV B, maart 2004
Pagina 600-1 – 600-50

Gavison, R.
Privacy and the limits of law
In: Schoeman, F.D. (redactie)
Philosophical Dimensions of Privacy: An Anthology, pagina 346-402
Cambridge University Press, Cambridge, 1984

Grijpink, J.H.A.M.
Identiteitsfraude en overheid
In: Justitiële verkenningen, jaargang 32, nummer 7, november 2006,
Pagina 37-56

Grijpink, J.H.A.M.
Identiteitsfraude als uitdaging voor de rechtstaat
In: Privacy & Informatie, jaargang 6, nummer 4, 2003
Pagina 148-153

Jacobs, B.
De Menselijke Maat in ICT, versie 1.0
2007
Beschikbaar via www.cs.ru.nl/B.Jacobs/MM/

Koops, B.J. en Lenes, R.
'Code' and the slow Erosion of Privacy
In: Michigan Telecommunications and Technology Law Review,
Jaargang 12, Nummer 1, 2005
Pagina 115-188

Koops, B.J. en Lenes, R.
ID Theft, ID Fraud and/or ID-related Crime – Definitions matter
In: Datenschutz und Datensicherheit, jaargang 30, nummer 9, 2006

Koorn, R., Van Gils, H., Ter Hart, J., Overbeek, P. en Tellegen, R.
Privacy Enhancing Technologies - Witboek voor beslissers
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Den Haag, 2004

Mettau, P.
Mijnoverheid.nl – Publieke dienstverlening in de toekomst
Stichting Het Expertise Centrum, Den Haag, 2005

Overbeek, P. , Lindgreen, E. R. en Spruit, M.
Informatiebeveiliging onder controle –
Grondslagen, management, organisatie en techniek
Pearson Education Benelux, Amsterdam, 2005

Prins, J.E.J. en De Vries, M.
ID or not to be? Naar een doordacht stelsel voor digitale identificatie.
Werkdocument 91
Rathenau Instituut, Den Haag, 2003

Rachels, J.
Why privacy is important
In: Schoeman, F.D. (redactie)
Philosophical Dimensions of Privacy: An Anthology, pagina 290-299
Cambridge University Press, Cambridge, 1984

Schoeman, F.D.
Privacy – Philosophical dimensions of the literature
In: Schoeman, F.D. (redactie)
Philosophical Dimensions of Privacy: An Anthology, pagina 1-33
Cambridge University Press, Cambridge, 1984

7.2 Websites

http://www.andereoverheid.nl
http://www.bsnweb.nl
http://www.digid.nl
http://www.e-overheid.nl/
http://www.ftc.gov/idtheft
http://www.gbo.overheid.nl/