Auteursrechterlijke overeenkomst

Opdat de Universiteit Hasselt uw eindverhandeling wereldwijd kan reproduceren, vertalen en distribueren is uw akkoord voor deze overeenkomst noodzakelijk. Gelieve de tijd te nemen om deze overeenkomst door te nemen, de gevraagde informatie in te vullen (en de overeenkomst te ondertekenen en af te geven).

Ik/wij verlenen het wereldwijde auteursrecht voor de ingediende eindverhandeling met

Titel: De werking van de digitale handtekening en het gebruik ervan binnen e-government
Richting: 2de masterjaar handelsingenieur - operationeel management en logistiek Jaar: 2009

in alle mogelijke mediaformaten, - bestaande en in de toekomst te ontwikkelen - , aan de Universiteit Hasselt.

Niet tegenstaand deze toekenning van het auteursrecht aan de Universiteit Hasselt behoud ik als auteur het recht om de eindverhandeling, - in zijn geheel of gedeeltelijk -, vrij te reproduceren, (her)publiceren of distribueren zonder de toelating te moeten verkrijgen van de Universiteit Hasselt.

Ik bevestig dat de eindverhandeling mijn origineel werk is, en dat ik het recht heb om de rechten te verlenen die in deze overeenkomst worden beschreven. Ik verklaar tevens dat de eindverhandeling, naar mijn weten, het auteursrecht van anderen niet overtreedt.

Ik verklaar tevens dat ik voor het materiaal in de eindverhandeling dat beschermd wordt door het auteursrecht, de nodige toelatingen heb verkregen zodat ik deze ook aan de Universiteit Hasselt kan overdragen en dat dit duidelijk in de tekst en inhoud van de eindverhandeling werd genotificeerd.

Universiteit Hasselt zal mij als auteur(s) van de eindverhandeling identificeren en zal geen wijzigingen aanbrengen aan de eindverhandeling, uitgezonderd deze toegelaten door deze overeenkomst.

Ik ga akkoord,

POSTELMANS, Laura

Datum: 14.12.2009

De werking van de digitale handtekening en het gebruik ervan binnen e-government

Laura Postelmans

promotor :
Prof.dr.ir Frans LEMEIRE

Eindverhandeling voorgedragen tot het bekomen van de graad
master in de toegepaste economische wetenschappen:
handelsingenieur operationeel management en logistiek

universiteit hasselt

Woord vooraf

Deze masterproef, voorgedragen tot het behalen van mijn diploma Handelsingenieur – Operationeel Management en Logistiek, vormt het sluitstuk van mijn opleiding aan de Universiteit Hasselt.

De realisatie van deze masterproef was niet mogelijk geweest zonder de hulp en de steun van verschillende personen. Ik wil dan ook even de tijd nemen om deze te bedanken.

Allereerst wil ik een woord van dank richten aan Prof. dr. ir. Frans Lemeire, mijn promotor, voor zijn deskundige begeleiding. Zijn expertise was erg belangrijk bij het schrijven van deze masterproef. Daarnaast wil ik de gemeente Diepenbeek, en in het bijzonder Ronny Nelissen, bedanken voor hun medewerking aan mijn onderzoek. Ook Tristan Fransen van de XIOS hogeschool, Lode Blokken en de inwoners van Diepenbeek die hun medewerking hebben verleend bij de afname van mijn enquête verdienen een dankwoord.

Verder wil ik ook mijn vriend Pieter, mijn broer Yannick en al mijn vrienden bedanken voor hun steun doorheen mijn hele opleiding. Natuurlijk mag ik mijn ouders niet vergeten. Zij verdienen een speciaal woord van dank omdat ze mij de mogelijkheid geboden hebben deze studies te realiseren en voor hun onvoorwaardelijke steun gedurende mijn loopbaan aan de Universiteit Hasselt.

Laura Postelmans

Samenvatting

Het internet speelt een belangrijke rol in de hedendaagse maatschappij. Het vormt niet alleen een belangrijk communicatiemiddel, maar wordt ook steeds meer gebruikt om bijvoorbeeld handel te drijven. Een gevolg hiervan is dat papieren documenten worden vervangen door hun elektronische tegenhanger. Het aanpassen en verzenden van zulke elektronische documenten is eenvoudig en snel, wat heel wat voordelen met zich mee brengt. Deze soepelheid houdt echter ook in dat de kans op fraude toeneemt. De veiligheid is voor bepaalde toepassingen dan ook uitermate belangrijk.

De fraude kan op verschillende gebieden plaatsvinden. Men kan de integriteit van een document schaden. Hiermee wordt bedoeld dat het bericht gewijzigd wordt door een derde persoon, zonder dat zender of ontvanger hiervan op de hoogte zijn. Hiernaast kan er fraude voorkomen met betrekking tot de authenticiteit van de afzender. De persoon die het bericht verstuurd heeft, kan een ander persoon zijn dan de ontvanger denkt. Verder kan de verzender na het versturen van een bericht ontkennen dat hij dit verstuurd heeft. Dit heeft te maken met de onweerlegbaarheid. Ten laatste kan een vertrouwelijk bericht onderschept en gelezen worden door een derde persoon. Deze vertrouwelijkheid is natuurlijk niet belangrijk voor elk bericht.

Om de fraude op deze gebieden tegen te gaan, werden verscheidene wiskundige methoden ontwikkeld. Om de **integriteit** van een bericht te waarborgen, kan men een hashfunctie gebruiken. Elke wijziging in een bericht, hoe klein ook, levert een volledig verschillende hashwaarde op, waardoor de ontvanger weet dat er iets gewijzigd is aan de tekst.

De **authenticiteit** van de afzender kan gegarandeerd worden door gebruik te maken van de digitale handtekening. De digitale handtekening is geen echte 'handtekening', maar het is het omvormen van de hash waarde van het bericht met de private sleutel van de ondertekenaar. De ondertekenaar is in het bezit van een private sleutel die alleen hij kent en een publieke sleutel, die openbaar is. Enkel als de hashwaarde met de private sleutel van de verzender is versleuteld, zal het toepassen van de publieke sleutel op de omgevormde hashwaarde terug de oorspronkelijke hashwaarde geven. Als een verzender zijn bericht versleutelt met zijn private sleutel, is de ontvanger dus zeker dat het bericht van die persoon komt.

Door de digitale handtekening toe te passen, kan de afzender dus ook niet meer ontkennen dat hij het bericht verstuurd heeft. Op deze manier kan men dus de **onweerlegbaarheid** verzekeren.

De digitale handtekening op zich verzekert geen **confidentialiteit** van gegevens. Dit kan echter wel gerealiseerd worden door het gebruik van cryptografie. Zowel symmetrische cryptografie (DES), als asymmetrische cryptografie (RSA) kunnen hiervoor worden gebruikt.

De voornoemde methoden kunnen als zeer veilig beschouwd worden. Zelfs de kleinste wijziging aan een bericht zal niet onopgemerkt blijven; het nabootsen van een handtekening is onmogelijk; ... .

Als de digitale handtekening wil fungeren als geldig alternatief voor de handgeschreven handtekening is het noodzakelijk dat er een wettelijk kader voor bestaat. Dit wordt voorzien door de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen. Deze Europese richtlijn werd in 2000 omgezet in een Belgische wet, namelijk de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten. Deze wet stelt dat een geavanceerde elektronische handtekening, gerealiseerd op basis van een gekwalificeerd certificaat en op een veilige manier aangemaakt, gelijkgesteld wordt met de handgeschreven handtekening en dus rechtsgeldig is. De digitale handtekening voldoet aan de voorwaarden van een geavanceerde elektronische handtekening en is dus, als voorzien van een geldig certificaat, rechtsgeldig.

Er bestaan heel wat mogelijke toepassingen van de digitale handtekening, waaronder het gebruik bij e-commerce, elektronisch factureren, het bewaren van documenten, het versturen van vertrouwelijke informatie via e-mail, e-banking en e-government en het gebruik binnen de logistieke sector. Het gebruik van de digitale handtekening bij e-government wordt uitgebreid besproken binnen deze masterproef.

De twee belangrijkste peilers van e-government zijn de elektronische identiteitskaart en de federale portaalsite. De elektronische identiteitskaart, eID afgekort, heeft naast het bewijs van identiteit ook nog andere functies, namelijk de authenticatie van de eigenaar en het genereren van een gekwalificeerde elektronische handtekening. Voor beide functies bevat de eID twee verschillende certificaten. De eID kan dus bijvoorbeeld gebruikt worden om toegang te verkrijgen tot beveiligde internetsites (authenticatie) en om een elektronisch document te ondertekenen (elektronische handtekening), dit beide m.b.v. een digitale handtekening. E-government kent enkele belangrijke realisaties zoals de kruispuntbank van de sociale zekerheid, tax-on-web en het e-loket. Deze laatste toepassing maakt, samen met de eID, het onderwerp uit van een enquête, afgenomen binnen de gemeente Diepenbeek. Uit deze enquête blijkt dat zowel het e-loket als de eID zeer weinig gebruikt worden en dat er te weinig informatie voorhanden is over de functies en de werking ervan. De toepassingen van de eID worden nochtans als veilig en nuttig bestempeld door de meeste respondenten. Bovendien zegt de meerderheid dat ze zowel de eID als het e-loket meer zouden gebruiken als er meer informatie beschikbaar zou zijn. Hieruit blijkt dat overheid en gemeenten de eID meer moeten promoten. Op 20 april 2009 heeft de overheid de campagne 'In 1-2-3 met je eID' aangekondigd om de toepassingen van de eID meer bekend te maken bij het brede publiek. Voor deze campagne is een website opgericht die de burger informeert over de eID (www.welcome-to-e-belgium.be). Bovendien zal de 'eID-bus' tussen april en september het hele

land doorkruisen. Bij een bezoek aan de bus krijg je een infopakket en een gratis kaarlezer mee, hetgeen het gebruik al sterk kan doen toenemen.

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

Hoofdstuk 1 Probleemstelling

In hoofdstuk 1 wordt ingegaan op het praktijkprobleem, evenals op de onderzoeksvragen en de gebruikte onderzoeksstrategieën.

1.1 Praktijkprobleem

Het internet is niet meer weg te denken uit de hedendaagse maatschappij. Vrijwel iedereen is bekend met manieren om te communiceren via het internet. Meer nog, jongeren en zelfs volwassenen die geen gebruik maken van dit communicatiemiddel, worden soms met de vinger gewezen. Het internet als communicatiemiddel wordt zelfs bestempeld als het meest gebruikte ooit (wikipedia, 2008 a). Naast de communicatie hebben ook andere toepassingen hun weg gevonden naar het internet. Het wordt steeds eenvoudiger om bijvoorbeeld aankopen via internet te realiseren, zowel voor consumenten als voor bedrijven. Deze elektronische handel, of e-commerce, is al sterk geëvolueerd het afgelopen decennium. Deze evolutie brengt met zich mee dat papieren documenten voor een deel plaats moeten ruimen voor hun elektronische tegenhanger. Elektronische gegevens hebben als voordeel dat ze snel aangepast kunnen worden indien nodig en dat ze zeer snel geraadpleegd kunnen worden door verschillende personen. Het is bovendien eenvoudig, snel en goedkoop om informatie te verzenden en te ontvangen. De digitale handtekening kan een manier zijn om deze elektronische communicatie en elektronische handel veiliger te maken.

Deze voordelen impliceren immers eveneens grote nadelen. Aangezien een elektronisch document snel aangepast kan worden, is het erg vatbaar voor fraude. Hierdoor zal het bewaren van elektronische gegevens bijna altijd gepaard gaan met het bewaren van een papieren kopie. Spreken van een papierloze administratie is dan ook erg voorbarig (*digitale handtekening: een stand van zaken,* 2000). Een ander probleem dat zich stelt bij het communiceren via internet is identificatie. Communiceren via e-mail is snel en erg handig, maar zekerheid betreffende de werkelijke identiteit van de verzender is er niet. De ontvanger kan er immers niet zeker van zijn dat degene die de e-mail verstuurt, wel degelijk de persoon is waarvoor hij zich uitgeeft. Door de e-mail te vergezellen van een digitale handtekening is de ontvanger zeker van de identiteit van de verzender. Er kan bovendien ook geen wijziging aangebracht worden aan de inhoud van het bericht zonder dat de ontvanger hier achter komt. De ontvanger zal een gewijzigd bericht immers niet kunnen ontsleutelen (Vercammen, z.d.).

Naast het nut als beveiligingstechniek, kan de digitale handtekening ook dienst doen als equivalent van de geschreven handtekening. Immers, een document afhalen van het internet en invullen op computer vormt geen probleem, maar indien men het moet ondertekenen zal het alsnog geprint

moeten worden (*digitale handtekening: een stand van* zaken, 2000). De digitale handtekening kan hierbij een grotere beveiliging bieden dan de geschreven handtekening.

Het gebruik van het internet voor allerlei toepassingen is sterk gegroeid de afgelopen jaren, en het zal nog sterk blijven evolueren. Ondanks het gemak en de snelheid is toch gebleken dat er heel wat nadelen aan verbonden zijn die het vertrouwen van de gebruiker beïnvloeden. De vraag is of de digitale handtekening dit vertrouwen een boost kan geven. Dit kan natuurlijk niet zonder een juridische ondersteuning van deze vrijwel nieuwe techniek. Deze juridische omkadering kan zich niet beperken tot nationaal niveau, maar moet een internationaal karakter hebben. Internet kent immers ook geen landsgrenzen.

De digitale handtekening is geen handtekening in de strikte vorm van het woord, maar is gebaseerd op de cryptologie, een wetenschap gericht op onder andere het beveiligen van digitale gegevens. Het is meer bepaald de asymmetrische encryptie waarop de digitale handtekening meestal zal steunen. Encryptie duidt op het omzetten van leesbare tekst naar niet-leesbare tekst. Asymmetrische encryptie is encryptie die gebruik maakt van twee sleutels, een openbare en een private sleutel. Hiernaast bestaat ook symmetrische encryptie, die slechts van één sleutel gebruik maakt. Het toevoegen van een digitale handtekening aan een e-mail of aan een elektronisch document, kan de integriteit en de authenticiteit ervan verzekeren (Koops & Van der Hof, 2002). Het is hierdoor één van de belangrijkste beveiligingstechnieken op dit moment.

1.2 Centrale onderzoeksvraag en deelvragen

Door de opkomst van e-commerce en andere nieuwe internettoepassingen worden de begrippen vertrouwen en veiligheid steeds belangrijker. Het doel van deze masterproef is daarom het achterhalen van de rol die de digitale handtekening speelt of kan spelen binnen deze nieuwe trend. De digitale handtekening is immers één van de belangrijkste beveiligingstechnieken van dit moment, en kan dus een uitstekende manier zijn om het vertrouwen van de internetgebruiker te bevorderen.

Om dit doel te bereiken is het niet onbelangrijk de grondslagen van deze techniek te kennen. Deze masterproef zal dan ook uitgebreid ingaan op de wiskundige grondslagen en de principes van de cryptologie. De digitale handtekening zal echter enkel aan belang kunnen winnen indien er een juridische waarde aan gegeven wordt. Daarom komt ook het juridische kader aan bod. Hiernaast is het belangrijk om de al bestaande toepassingen van deze beveiligingstechniek nader te bekijken, met uitdieping van één bepaalde toepassing.

Het doel van dit onderzoek wordt samengevat in onderstaande centrale onderzoeksvraag:

Welke beveiligingsmogelijkheden bestaan er voor een veilig internetgebruik, welke rol speelt de digitale handtekening hierin en hoe wordt dit toegepast binnen e-government?

Het uitdiepen van de centrale onderzoeksvraag gebeurt aan de hand van een aantal deelvragen:

1. Wat is cryptologie?

Letterlijk betekent cryptologie 'leer van het geheimschrift'. Het is een wetenschap die zowel cryptografie en cryptoanalyse bestudeert (online encyclopedie, 2007). Tieleman en Vernooij (2002) definiëren in hun werkstuk cryptografie als volgt: "Cryptografie is de wetenschap die zich bezighoudt met het versleutelen en ontcijferen van al dan niet versleutelde informatie."(p.3) Er kunnen twee soorten cryptografie onderscheiden worden, namelijk symmetrische en asymmetrische cryptografie. De digitale handtekening is een toepassing van de asymmetrische cryptografie (Koops & Van der Hof, 2002). Cryptoanalyse daarentegen focust zich op het breken van de gecodeerde berichten (wikipedia,2008 b).

2. Wat zijn de wiskundige fundamenten van de digitale handtekening?

Om deze deelvraag te beantwoorden, gaat de masterproef dieper in op de algemene wiskundige basis waarvan de cryptografie gebruik maakt. Begrippen die aan bod zullen komen, zijn onder andere one-way functions (hash functions en trapdoor functions) en de code theorie. Een belangrijke vorm van de digitale handtekening, namelijk de RSA- digitale handtekening, steunt bovendien op het modulo-rekenen. Dit aspect komt dan ook uitgebreid aan bod.

3. Wat is de digitale handtekening en hoe werkt deze techniek?

De digitale handtekening is een vorm van elektronische handtekening en kan dienst doen als alternatief voor de gewone handtekening. Hiernaast kan een digitale handtekening aan een elektronisch document toegevoegd worden om de authenticiteit en de integriteit van het bericht te verzekeren. De digitale handtekening steunt op het principe van de asymmetrische cryptografie (Van der Hof, 1997).

4. Welke voordelen levert het gebruik van de digitale handtekening op?

Zoals reeds vermeld, is het bij het krijgen van bijvoorbeeld een e-mail heel moeilijk te achterhalen wie de werkelijke afzender is. Het is immers mogelijk dat de afzender niet degene is die hij beweerd te zijn. Een digitale handtekening kan bij zulke problemen als bewijs van

identiteit dienen. Hiernaast is het bij het versturen van elektronische documenten mogelijk dat een derde persoon de inhoud zou wijzigen tijdens de verzending. Wanneer de afzender zijn document versleutelt met een digitale handtekening zal de ontvanger het bericht enkel kunnen ontsleutelen indien er niets aan de inhoud gewijzigd is. Hier doet de handtekening dienst als bewijs van integriteit. Een derde belangrijk voordeel van het gebruik van een digitale handtekening is dat, door het toevoegen ervan aan een e-mail, de afzender niet kan ontkennen dat hij deze e- mail verstuurd heeft. Deze onweerlegbaarheid is ook erg belangrijk bij het elektronisch verzenden van orders. Kortom, de digitale handtekening zorgt voor veiligheid en vertrouwen bij het uitwisselen van gegevens via het internet.

5. Wat zijn de wettelijke bepalingen omtrent de digitale handtekening?

De digitale handtekening zal pas veelvuldig gebruikt kunnen worden als equivalent van de gewone handtekening indien er ook een wettelijk kader voor bestaat. De gewone handtekening wordt immers vaak geëist door de wet en een ondertekend geschrift kan gebruikt worden als bewijsmiddel. Dit mede doordat de handtekening enkele essentiële functies vervult, namelijk integriteit en identiteit. Pas als de digitale handtekening hetzelfde statuut krijgt als de gewone handtekening, zal deze kunnen gebruikt worden op belangrijke documenten. Begin 2000 werd een richtlijn gepubliceerd die dit mogelijk maakt, namelijk de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (*digitale handtekening: stand van* zaken, 2000). In België is er de wet van 20 oktober 2000, deze van 9 juli 2001 en het koninklijk besluit van 6 december 2002.

6. Welke toepassingen van de digitale handtekening bestaan er?

Enkele gekende toepassingen zijn het gebruik van de digitale handtekening bij de elektronische BTW-aangifte, de elektronische identiteitskaart, het ondertekenen van een e-mail voor vertrouwelijke communicatie, het gebruik bij elektronische handel, ... (VERCAMMEN, z.d.). De digitale handtekening kan ook gebruikt worden binnen de logistieke sector.

Deze deelvragen komen aan bod in de hoofdstukken twee tot en met zeven.

In het praktijkgedeelte komt het gebruik van de digitale handtekening bij e-government aan bod. In het kader van deze uitdieping komen volgende deelvragen naar voor:

7. Wat is e-government?

Niet alleen consumenten en bedrijven, maar ook de overheid past zich aan in deze digitale leefwereld. Velle (2002) definieert e-government als volgt: "het gebruik van (ICT-) technologie om de toegang tot en het verlenen van openbare diensten voor burgers, zakenpartners, leveranciers en ambtenaren te vergemakkelijken." E-government heeft dus zowel betrekking tot

de relatie tussen bestuursorganen onderling, als tot de relatie met ondernemingen en burgers. Het gebruik van bijvoorbeeld een e-loket levert allerlei voordelen op. Zo kunnen papieren online ingevuld worden, hetgeen niet meer gepaard gaat met een fysieke verplaatsing. Het digitale loket is ook altijd 'open' en overal bereikbaar (Federale Overheidsdienst Economie, z.d.).

8. Welke toepassingen zijn er mogelijk binnen e-government en wat is de rol van de digitale handtekening hierin?

De elektronische identiteitskaart, die kan gebruikt worden als digitale handtekening, is het meest gekende en waarschijnlijk ook belangrijkste resultaat van e-government. Ook het elektronisch opvragen en indienen van documenten is al mogelijk. Op de site van de federale overheid kan bijvoorbeeld online een schatting van het pensioen gemaakt worden. Een andere belangrijke toepassing is het online invullen van de belastingaangifte. Hiervoor zal de elektronische identiteitskaart dienst doen als digitale handtekening (Vanvelthoven, 2003).

9. Wat is de rol van de elektronische identiteitskaart?

De elektronische identiteitskaart of eID is de opvolger van de gewone identiteitskaart, maar heeft heel wat meer functies. Zoals reeds aangehaald kan de eID gebruikt worden om een digitale handtekening te genereren. Bij E-government zijn aspecten als veiligheid, integriteit en authenticiteit van groot belang. De digitale handtekening, en dus ook de eID kan hiervoor zorgen (Vanvelthoven, 2003). We vragen ons hierbij af of de verschillende functies van de eID werkelijk gebruikt worden door de burgers.

In hoofdstukken acht en negen wordt getracht een antwoord te formuleren op deze deelvragen.

1.3 Onderzoeksmethodologie

1.3.1 Literatuurstudie

De masterproef is, naast dit inleidende hoofdstuk, opgebouwd uit 8 hoofdstukken die grotendeels gebaseerd zijn op een uitgebreide literatuurstudie en een laatste hoofdstuk met betrekking tot de conclusie. Een aantal zoektermen zoals de digitale handtekening, e-commerce, e-government, cryptologie, beveiliging, ... hebben geleid tot voldoende wetenschappelijke bronnen, bestaande uit boeken en artikels. Zowel verschillende bibliotheken als het internet zijn een goede bron van informatie. Een gevonden bron levert dan weer nieuwe bronnen op, ook het 'sneeuwbaleffect' genoemd, waardoor een heel scala aan verschillende literatuur ontstaat.

Na dit eerste hoofdstuk over de probleemstelling, komen in hoofdstuk 2 de wiskundige grondslagen van de digitale handtekening aan bod. Hoofdstuk 3 behandelt het concept cryptologie en hoofdstuk

4 gaat dieper in op de cryptografie. Deze hoofdstukken zijn volledig gebaseerd op bestaande literatuur over cryptologie en moderne algebra en proberen een antwoord te formuleren op de deelvragen één en twee. Hoofdstuk 5 tracht te antwoorden op deelvragen drie en vier aan de hand van bestaande literatuur over de digitale handtekening. Deelvraag vijf wordt behandeld in hoofdstuk 6 en deelvraag zes in hoofdstuk 7. Voor beide deelvragen wordt ook gebruik gemaakt van literatuur over de digitale handtekening. Hoofdstuk 8 focust zich op één bepaalde toepassing van de digitale handtekening, namelijk het gebruik binnen e-government. E-government zal hierbinnen nader besproken worden aan de hand van bestaande literatuur om zo een antwoord te formuleren op deelvragen zeven en acht.

1.3.2 Praktijkgedeelte

Hoofdstuk 8 zal, naast de theoretische uiteenzetting van e-government, ook steunen op enkele interviews met bevoorrechte getuigen. Op basis hiervan wordt een aanvullend antwoord gegeven op deelvragen zeven tot negen. We maken gebruik van semigestructureerde interviews. Er vindt een interview plaats met de dienstverantwoordelijke secretariaat van de gemeente Diepenbeek, Ronny Nelissen, alsook met een boekhouder bij D&D Consulting, Lode Blokken. Hiernaast hebben we ook een gesprek gehad met Tristan Fransen, medewerker aan de XIOS hogeschool Limburg. Eveneens zal gepeild worden naar de mening van de gebruikers van de elektronische overheidsdiensten aan de hand van een enquête. De resultaten hiervan worden opgenomen in hoofdstuk 9.

Hoofdstuk 2 Wiskundige hulpmiddelen voor de RSA digitale handtekening

In dit hoofdstuk komen enkele wiskunde basisbegrippen aan bod die gebruikt worden in de cryptologie en bij de digitale handtekening. Allereerst wordt de oplosbaarheid van problemen met de computer besproken, alsook de concepten complexiteit en simpliciteit. Hierna gaat dit hoofdstuk in op de definities van algemene algebraïsche structuren zoals groepen en ringen, waarna het modulo rekenen aan bod komt. Vervolgens wordt de stelling van Euler behandeld, evenals het algoritme van Euclides voor het berekenen van de grootste gemene deler, met als toepassing het inverteren bij modulo rekenen. Ook komt het gebruik van drie belangrijke functies aan bod, namelijk de one-way functie, de trapdoor functie en de hash functie. Tenslotte zal de codetheorie kort besproken worden.

2.1 Numerieke oplosbaarheid met behulp van een computer

De rekenkracht van een computer is afhankelijk van het aantal bewerkingen dat deze kan doen per seconde (aantal flops, floating point operations per second). Volgende indeling kan worden gemaakt:

a. gewone computer: 10^6 flops
b. snelle computer: 10^9 flops
c. super snelle computer: 10^{12} flops
d. snelste computer momenteel: 10^{15} flops (Husquinet, 2009)
e. onmogelijk: 10^{50} flops

Volgens de Wet van Moore zouden de prestaties van de computer per 18 maanden verdubbelen. Indien we 1965, toen een computer met 10^6 flops uitzonderlijk was, vergelijken met 2010, kunnen we stellen dat deze wet gevolgd is. Immers op 45 jaar, zouden de mogelijke prestaties dan 2^{30} keer groter moeten zijn (want 45 jaar = 30 * 18 maanden).

➔ dus aantal flops in 1965 * 2^{30} ($\approx * 10^9$)
➔ $10^6 * 10^9 = 10^{15}$ flops in 2010

Indien deze wet ook nog de volgende 18 jaar (tot 2027) zou gelden, zouden de mogelijke prestaties 2^{12} keer groter zijn in 2027 (want 18 jaar = 12 * 18 maanden).

➔ dus aantal flops in 2010 * 2^{12} ($\approx * 10^4$)
➔ $10^{15} * 10^4 = 10^{19}$ flops in 2027

Indien we 10^9 flops bekijken, dan bestrijkt één flop een tijd van 1 nanoseconde (10^{-9} s). We kunnen dit vergelijken met de afstand die het licht (en dus ook informatie) aflegt op die tijd.

➔ $\frac{300\ 000\ 000\ m/s}{10^9\ s} = 30\ cm$

Bij het sequentieel rekenen (berekeningen gebeuren na elkaar) lijkt de gangbare limiet dus op 10^9 flops te zitten. Bij parallel rekenen (parallel geschakelde processoren) is echter meer mogelijk. Bij cryptologie is dikwijls parallel rekenen mogelijk.

2.2 Complexiteit en simpliciteit van problemen

In deze paragraaf komen de concepten logaritmische, polynomiale en niet-polynomiale problemen en de complexiteit en simpliciteit van problemen aan bod.

2.2.1 Logaritmisch (L), Polynomiaal (P) en Niet-polynomiaal (NP) aantal berekeningen

Logaritmisch aantal berekeningen	$\cong \alpha \ln n$	
Polynomiaal aantal berekeningen	$\cong \alpha+\beta n$	(lineair)
	$\cong \alpha+\beta n + \gamma n^2$	(kwadratisch)
	$\cong \alpha+\beta n + \gamma n^2 + \lambda n^3$	(kubisch)
Niet-polynomiaal aantal berekeningen, bv.	$\cong \alpha e^{\lambda n}$	(exponentieel)

Het aantal berekeningen wordt weergegeven in functie van de grootte van het probleem (n).

Tabel 2.1 geeft enkele voorbeelden van logaritmisch, polynomiaal en niet-polynomiaal aantal berekeningen.

Tabel 2.1 Logaritmisch, Polynomiaal en Niet-polynomiaal aantal berekeningen

	Aantal berekeningen (voorbeelden)				
	Logaritmisch	Polynomiaal (P)			Niet-polynomiaal (NP)
n	**ln n**	**n**	**n^2**	**n^3**	**$e^{0,01n}$**
10^2	≈ 4,6	10^2	10^4	10^6	$e^1 \approx 3$
10^3	≈ 6,9	10^3	10^6	10^9	$e^{10} \approx 10^3$
10^4	≈ 9,2	10^4	10^8	10^{12}	$e^{10^2} \approx 10^{30}$
10^5	≈ 11,5	10^5	10^{10}	10^{15}	$e^{10^3} \approx 10^{300}$
10^6	≈ 13,8	10^6	10^{12}	10^{18}	$e^{10\text{^}4} \approx 10^{3000}$

Bij een niet-polynomiaal aantal berekeningen, zal het aantal berekeningen voor een voldoende grote n veel sneller stijgen naarmate een probleem groter wordt dan bij een polynomiaal aantal berekeningen. Bij een logaritmisch aantal berekeningen, stijgt het aantal berekeningen slechts gering naarmate het probleem groter wordt. Als n in het eerste geval (NP) groot wordt, is het niet mogelijk om het probleem op te lossen (bv. $n=10^4$).

2.2.2 Complexiteit en simpliciteit van een probleem

a. De **complexiteit** van een probleem is het aantal nodige berekeningen voor sommige, eventueel zeldzame gevallen (met een kans van bijvoorbeeld 10^{-100} dat deze voorkomen). Heel wat problemen hebben een hoge complexiteit. Voor praktische toepassingen vergen ze evenwel dikwijls slechts weinig rekenwerk, maar kunstmatig geconstrueerde problemen kunnen praktisch onoplosbaar zijn. Een voorbeeld hiervan is het simplex algoritme.

b. Met de **simpliciteit** van een probleem wordt het aantal berekeningen bedoeld, nodig voor nagenoeg alle willekeurig gekozen gevallen. Het is dus de hoeveelheid rekenwerk voor de simpelste gevallen. Problemen met hoge simpliciteit zijn problemen die voor bijna alle willekeurige gevallen heel veel rekenwerk vergen.

Tabel 2.2 geeft een voorstelling van de complexiteit en simpliciteit van problemen.

Tabel 2.2 Complexiteit en simpliciteit van problemen

COMPLEXITEIT

SIMPLICITEIT

	Lage complexiteit (P)	**Hoge complexiteit (NP)**
Lage simpliciteit (P)	Altijd met weinig rekenwerk oplosbaar	Meestal met weinig rekenwerk oplosbaar, heel zelden veel rekenwerk. Vb. Simplex algoritme
Matig hoge simpliciteit (P)	Meestal veel bewerkingen nodig, maar geen 'eeuwigheid' Vb. Digitale handtekening	Idem als bij lage complexiteit
Zeer hoge simpliciteit (NP)	Onmogelijk	? (vermoedens dat deze niet bestaan)

2.2.3 Problemen met hoge en lage simpliciteit

a. Problemen met priemgetallen

- Het ontbinden van een getal in priemfactoren (zie sectie 2.4.4) heeft een hoge simpliciteit. Het vergt bijna altijd heel veel rekenwerk om deze problemen op te lossen (voor een grote n).

  Problemen die bijvoorbeeld van de grootte orde 2^{512} zijn, zijn niet ontbindbaar;

  Opmerking: Met "bijna altijd" wordt hier bedoeld dat de kans dat dit niet zo is, bijvoorbeeld 10^{-20} bedraagt.

- Het bepalen van priemgetallen heeft een lage simpliciteit. Dit is een probleem dat met relatief weinig rekenwerk opgelost kan worden, zelfs voor zeer grote getallen (bv. 10^{500}).

b. Problemen met modulo n rekenen

- Het berekenen van a^{-1} mod n als ggd(a,n)=1 en n gekend, heeft een lage simpliciteit (zie sectie 2.9);
- Het berekenen van a^{-1} mod n als n niet gekend is, heeft een hoge simpliciteit;

- Het berekenen van machten mod n heeft een lage simpliciteit (zie sectie 2.7);
- Het berekenen van logaritmen mod n heeft een hoge simpliciteit.

2.3 Groepen – ringen – lichamen – velden

In deze sectie worden enkele algemene algebraïsche structuren gedefinieerd die van belang zijn bij het modulo rekenen.

2.3.1 Groepen

Een groep kan als volgt gedefinieerd worden:

Stel G is een niet lege verzameling en * is een operatie op G. Dan is het paar (G,*) een groep indien:

1) de operatie overal bepaald is: $(\forall a,b \in G)(\exists c \in G)\ a * b = c$;

2) de operatie associatief is, dit wil zeggen: $(\forall a,b,c \in G)\ a*(b*c) = (a*b)*c$;

3) G een neutraal element e bevat, dit wil zeggen dat

$(\exists\, e \in G)\ (\forall a \in G)\ \ a*e = e*a = a$;

4) elk element een invers/tegengesteld element heeft:

$(\forall a \in G)\ (\exists\, b \in G)\ a*b = b*a = e$,

We noteren $b = a^I$

Als we (+) gebruiken voor de operatie

- noemen we dit additief, optelling;
- en noteren we $a^I = -a$ (het tegengesteld element).

Als we (.) gebruiken als operatie

- noemen we dit multiplicatief;
- en noteren we $a^I = a^{-1}$ (het invers element).

Voorbeeld

De verzameling van de gehele getallen $\mathbb{Z}$ vormt een groep samen met de operatie optelling. De operatie is associatief, aangezien (a+b)+c = a+(b+c), het neutraal element is nul en elk geheel getal a heeft een tegengestelde -a, waarbij a + (-a) = 0.

$\mathbb{Z}$ vormt daarentegen geen groep met de vermenigvuldiging. Het neutraal element is weliswaar één, maar aan de vierde voorwaarde is hier echter niet voldaan. Het invers element van a voor de vermenigvulding is immers a^{-1}, en dit is geen element van $\mathbb{Z}$ als $a \neq 1$.

De verzameling van de rationale getallen zonder nul ($\mathbb{Q}_0 = \mathbb{Q} \setminus \{0\}$) vormt wel een groep met de vermenigvuldiging. 1 is ook hier het neutrale element.

2.3.2 Commutatieve of abelse groepen

Beschouw de groep (G, *) als zijnde commutatief of abels, indien de operatie * commutatief is. Een commutatieve groep moet aan al de voorwaarden voldoen van een gewone groep, met als bijkomende voorwaarde:

5) De groep G uit 2.1.1 is abels of commutatief indien $(\forall a, b \in G)\ a * b = b * a$.

2.3.3 Deelgroepen en nevenklassen

Een niet-lege deelverzameling H van een groep G is een **deelgroep** of deler van G indien H zelf een groep is met betrekking tot de operatie van G.

Voorbeeld deelgroep

De gehele getallen vormen een groep met de optelling ($\mathbb{Z}$, +). De verzameling van de even getallen in $\mathbb{Z}$ vormt dan een deelgroep.

Een **nevenklasse** kan beschreven worden als een verzameling elementen van een groep die ontstaat door de elementen van een deelgroep samen te stellen met een vast element van de groep. Er bestaat een linker en rechter nevenklasse. Stel groep (G,*) met deelgroep H:

Een linker nevenklasse voor $g \in G$ kan worden voorgesteld door $H_g = \{g*h \mid h \in H\}$

Een rechter nevenklasse voor $g \in G$ wordt gegeven door $\tilde{H}_g = \{h*g \mid h \in H\}$

In een abelse groep zijn deze nevenklassen altijd aan elkaar gelijk. We beperken ons verder tot abelse groepen.

Onderstel de nevenklassen H_1,H_2, …, H_k

Met $H_i = \{g_i * h \mid h \in H\}$

De deelgroep en zijn nevenklassen vormen een partitie van de groep G:

$H_1 = e * H = H$ (met e het neutraal element)

$H_2 = g_2 * H$

…

$H_k = g_k * H$

Al de nevenklassen van H bevatten evenveel elementen als de deelgroep H zelf. Bij eindige groepen is het aantal elementen van een deelgroep dus een deler van het aantal elementen van de groep.

2.3.4 Quotiëntgroep

Met $G = \{g_1, g_2, g_3, \ldots\}$ een groep, vormt $G/H = \{H_1, H_2, H_3, \ldots)$ een quotiëntgroep.

Voor een quotiëntgroep geldt:

$g_h * g_i = g_j \Leftrightarrow H_k * H_l = H_p$

Als $g_h \in H_k$

$g_i \in H_l$

$g_j \in H_p$

2.3.5 Ringen

Een ring (R, +, *) bestaat uit een verzameling R met twee binaire operaties op R, hier de optelling + en de vermenigvuldiging *, en voldoet aan volgende voorwaarden:

- (R,+) is een commutatieve groep met neutraal element 0;
- de operatie * is associatief;
- de operatie * is distributief over + Dit wil zeggen dat
  $(\forall a,b,c \in R)\ a*(b+c) = (a*b)+(a*c)$;
- er is een multiplicatief neutraal element 1, met 1 ≠ 0, zodat
  $(\forall a \in R)\ a*1 = 1*a = a$.

Indien ook (R, *) commutatief is, wordt ook de ring commutatief genoemd.

Een ring kan nuldelers hebben. Dit wil zeggen dat het mogelijk is dat

$$a * b = 0 \ met \ a \neq 0 \ en \ b \neq 0$$

Voorbeeld

*Zowel ($\mathbb{Z}$, +, *) als ($\mathbb{Q}$, +, *) en ($\mathbb{R}$, +, *) zijn commutatieve ringen.*

2.3.6 Lichamen

Een lichaam is een ring waarin de vermenigvuldiging een neutraal element heeft en waarin er voor elk element ≠0 een multiplicatieve inverse bestaat.

2.3.7 Velden

Indien bij een lichaam de vermenigvuldiging bovendien commutatief is, spreken we van een veld.

M.a.w. (K, +, *) is een veld indien:

- (K, +) een commutatieve groep is;
- ($K_{(0)}$, *) een commutatieve groep is;
- de bewerking * distributief is ten opzichte van +.

Een veld heeft geen nuldelers.

Voorbeeld

$\mathbb{R}$ en $\mathbb{Q}$ vormen een veld met de optelling en de vermenigvuldiging. Voor $\mathbb{Z}$ is dit niet het geval aangezien alle gehele getallen, behalve 1, geen invers element voor de vermenigvuldiging hebben.

2.3.8 Quotiëntstructuur

Neem bijvoorbeeld de ring $\mathbb{Z}$. Voor de optelling (+) vormt $\mathbb{Z}$ een groep. Hiervoor kunnen we nevenklassen definiëren. Met deze nevenklassen kunnen we bewerkingen uitvoeren.

Deze nevenklassen vormen een ring R_n, die een quotiëntstructuur vormt.

➔ Ring Rn = $\mathbb{Z}$ / H

2.4 Priemgetallen (in ℕ)

Allereerst komt de definitie van priemgetallen aan bod, waarna enkele elementaire eigenschappen aan bod komen alsook het bepalen van, en het ontbinden in priemgetallen.

2.4.1 Definitie

Een priemgetal heeft volgende definitie:

"Een natuurlijk getal p>1 is een priemgetal als 1 en p zijn enige delers zijn."

1 wordt niet als priemgetal beschouwd omdat de formulering van stellingen over priemgetallen anders omslachtiger zou zijn. Een voorbeeld hiervan is de tweede elementaire eigenschap (zie sectie 2.4.2). Indien 1 als priemgetal zou worden beschouwd, zou het ontbinden van een natuurlijk getal aan de hand van priemgetallen niet enig zijn. Een getal zou dan immers op verschillende manieren geschreven kunnen worden. (bv. 6 = 2*3 = 1*2*3 = 1²*2*3)

Twee gehele getallen a en b zijn relatief priem als ze slechts één gemeenschappelijke deler hebben, namelijk 1, dus de ggd(a,b) = 1.

2.4.2 Elementaire eigenschappen

1. Er bestaan oneindig veel priemgetallen.
2. Een geheel getal groter dan 1 kan aan de hand van priemgetallen ontbonden worden en deze ontbinding is enig.

   Onderstel het natuurlijk getal a, dan kan a ontbonden worden in:

   $a = p_1^{a1} p_2^{a2} \ldots p_t^{at}$ met $p_1 > p_2 > \ldots > p_t$ priemgetallen

3. De dichtheid van priemgetallen neemt geleidelijk af naarmate n groter wordt. De kans (probability Pr) dat een getal n een priemgetal is, wordt weergegeven door volgende functie:

   Pr (n priem) $\cong \frac{1}{\ln n}$. Dit impliceert dat de gemiddelde afstand tussen twee priemgetallen voor grote n, ongeveer gelijk is aan ln n, en dus steeds groter wordt naarmate n groter is. (Stinson, 2006)

Voorbeeld ontbinden in factoren

11011 = 7 x 11² x 13

Voorbeeld dichtheid priemgetallen

N=100 → Pr ≅ 1/ln 100 = 0,2171 → Ongeveer één getal op 5 is priem

N=1000 → Pr ≅ 0,1447 → Ongeveer één getal op 7 is een priemgetal

$N=2^{512}$ → Pr ≅ 1/ln (2^{512}) ≅ 0,0028 → ongeveer één getal op 355 is een priemgetal

Uitwerking: $\log_a b = \ln b / \ln a$

- ➔ $\log_{10} (2^{512}) = \ln (2^{512}) / \ln 10$
- ➔ $\ln (2^{512}) = \ln 10 * \log_{10} (2^{512}) = \ln 10 * (512 * \log_{10} 2)$
- ➔ $\ln (2^{512}) = 512 * \ln 10 * \log_{10} 2 \approx 355$

2.4.3 Bepalen van (grote) priemgetallen

Onder grote priemgetallen worden bijvoorbeeld priemgetallen van de orde $N = 2^{128}$ verstaan. Men kan als volgt te werk gaan:

1) Men kiest een willekeurig getal van de orde $2^n = N$, met N oneven en n 128 bits.
2) Test dan of N, N+2, N+4, … priem is aan de hand van de omgekeerde stelling van Euler (zie sectie 2.6).

p priem → $\Phi(p) = p-1$
→ $(\forall a<p)\ a^{p-1} = 1 \bmod p$ (stelling van Euler)

- ➔ $a^{p-1} = 1 \bmod p$ is een aanwijzing dat p priem kan zijn. Dit is een noodzakelijke maar niet voldoende voorwaarde.
- ➔ Als dit echter geldt voor verscheidene a's, dan zijn we er zo goed als zeker van dat p priem is. Men dient wel rekening te houden met Carmicheal getallen. Dit zijn getallen die wel voldoen aan de stelling van Euler, maar niet priem zijn. Deze getallen zijn echter zeer zeldzaam.

Het genereren van priemgetallen heeft zo een lage simpliciteit.

2.4.4 Ontbinden in priemfactoren.

Er bestaan twee wijzen om voor een oneven getal n de priemfactoren te vinden.

1. Kleine priemfactoren proberen van klein naar groot (tot $\sqrt{n}$);
2. Grote priemfactoren zoeken: onderzoek of $n = a^2 - b^2 = (a+b)*(a-b)$, met a dicht bij (en kleiner dan) $\sqrt{n}$, en b dus klein.

Hierbij is het noodzakelijk te weten dat alle niet-priemgetallen, die oneven zijn, van volgende vorm zijn:

$$n = pq = \frac{(p+q)^2 - (p-q)^2}{4} = (\frac{p+q}{2})^2 - (\frac{p-q}{2})^2$$

met p en q oneven, dus zijn $(\frac{p+q}{2})$ en $(\frac{p-q}{2})$ geheel.

Beide methoden hebben een hoge simpliciteit. Het ontbinden kan ook gedaan worden door een combinatie van de twee vorige wijze, maar ook via deze methode is de simpliciteit nog steeds hoog. Voor een probleem van grootte n=512 bits, zal er nog eeuwen computertijd nodig zijn.

2.5 Modulair rekenen

Modulair rekenen wordt veelvuldig toegepast binnen de cryptologie en komt in deze sectie uitgebreid aan bod.

2.5.1 Definitie

Stel a is een willekeurig geheel getal en n is een positief geheel getal. Indien we a delen door n, bekomen we het quotiënt q en een rest r.

Deze rest kan gedefinieerd worden als r = a (mod n).

Twee gehele getallen a en b zijn congruent modulo n als a-b = qn. Men schrijft dit als a ≡ b mod n

---

Voorbeeld 1

Stel a=13 en n=5 → q=2 en r=3 aangezien 13 = 2x5 + 3

Dus 13 (mod 5)=3

Voorbeeld 2

73≡4 (mod 23)

*Aangezien 73 – 4 = 3 * 23*

Volgende eigenschappen zijn eigen aan de operator modulo:

- a ≡ b mod n indien n|(a-b) dus indien n een deler is van (a-b);
- uit (a mod n) = (b mod n) volgt dat a ≡ b mod n;

- a ≡ b mod n houdt in dat b ≡ a mod n;
- als a ≡ b mod n en b ≡ c mod n , dan is a ≡ c mod n

2.5.2 Restklassen modulo n

Willekeurige getallen uit $\mathbb{Z}$ kunnen opgedeeld worden in verschillende groepen naar gelang de rest die ze opleveren bij deling door n.

Definieer partities van $\mathbb{Z}$: {0; n; 2n; 3n; …} of {-n; -2n; …}

D = {k*n | n ∈ $\mathbb{N}$; k ∈ $\mathbb{Z}$ } en is een deelring van $\mathbb{Z}$.

Nevenklassen van D zijn:

0 + D = $\bar{0}$;

1 + D = $\bar{1}$;

2 + D = $\bar{2}$;

…

(n-1) + D = $\overline{n\text{-}1}$

Er bestaan dus n nevenklassen, die een ring vormen voor de optelling en vermenigvuldiging. Deze klassen worden restklassen modulo n genoemd en zijn partities van $\mathbb{Z}$. Er zijn n restklassen modulo n, gaande van 0 tot n-1.

Dit steunt op volgende stelling:

$$(\forall x \in \bar{a})\ (\forall y \in \bar{b})$$

$$\begin{cases} \text{x+y bevinden zich in dezelfde restklasse} \\ \text{x*y bevinden zich in dezelfde restklasse} \end{cases}$$

Met de restklassen modulo n kunnen we dus rekenen:

$$\bar{a} + \bar{b} = \bar{c} \Leftrightarrow a + b = c \pmod{n}$$
$$\bar{a} * \bar{b} = \bar{c} \Leftrightarrow a * b = c \pmod{n}$$

Dit rekenen met de restklassen modulo n wordt geïllustreerd door onderstaand voorbeeld.

Voorbeeld

Tabel 2.3 Restklassen Modulo 6 in $\mathbb{Z}$

Restklassen Modulo 6 in $\mathbb{Z}$

Er zijn hier zes restklassen modulo 6, zoals zichtbaar in tabel 2.3.

Restklasse 0, aangeduid als $\overline{0}$,
bevat deze getallen die,
wanneer ze gedeeld worden door zes,
geen rest met zich meebrengen.

$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
-6	-5	-4	-3	-2	-1
0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
…	…	…	…	…	…

Tabel 2.4 De optelling met de restgroepen modulo 6

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Tabel 2.4 geeft de optelling weer met de restklassen modulo 6.

Tabel 2.5 De vermenigvuldiging met de restgroepen modulo 6

*	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Tabel 2.5 geeft de vermenigvuldiging weer met de restklassen modulo 6. We kunnen hierbij nuldelers terugvinden, bijvoorbeeld: $\overline{2} * \overline{3} = \overline{0}$

2.5.3 De ring R_n

De restklassen modulo n, met de bewerkingen optelling en vermenigvuldiging, vormen een ring Rn. Ze vormen echter geen veld aangezien er nuldelers bestaan. Indien n een priemgetal zou zijn, vormen de restklassen modulo n wel een veld. De ring R_n vormt een quotiëntstructuur ($R_n = \mathbb{Z} / D_n$).

Voorbeeld

Stel n=6. De restklassen modulo 6 zijn $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ *en* $\bar{5}$*.*

$\bar{2} * \bar{3} = \bar{0}$*, dus* $\bar{2}$ *en* $\bar{3}$ *zijn nuldelers.*

Opmerking: indien geen verwarring mogelijk, noteren we $\bar{a}$ als a.

2.5.4 Multiplicatieve groep van de relatief prieme restklassen modulo n ($\mathcal{M}_n$)

Met de restklassen, beschreven in de vorige sectie, kan men rekenen. Voor de optelling vormen de restklassen modulo n een groep. Het additief invers van a is –a zodat a +(-a) = 0. Voor de vermenigvuldiging vormen de restklassen modulo n in het algemeen echter geen groep aangezien niet elk element een inverse (a^{-1}) heeft.

Indien we in R_n ons echter beperken tot de relatief prieme restklassen modulo n, heeft elk element wel een inverse. De relatief prieme restklassen zijn deze restklassen die enkel de deler 1 gemeenschappelijk hebben met n, dus ggd(a,n) =1. Deze restklassen vormen wel een groep voor de vermenigvuldiging. Dit noemen we de multiplicatieve groep van de relatief prieme restklassen modulo n ($\mathcal{M}_n$).

Voorbeeld n=8 → modulo 8

Voor n=8 kunnen we 8 restklassen onderscheiden:

$\bar{0}$ = *[…,-8,0,8,16,…]* $\bar{4}$ = *[…,-4,4,12,20,…]*

$\bar{1}$ = *[…,-7,1,9,17,…]* $\bar{5}$ = *[…,-3,5,13,21,…]*

$\bar{2}$ = *[…,-6,2,10,18,…]* $\bar{6}$ = *[…,-2,6,14,22,…]*

$\bar{3}$ = *[…,-5,3,11,19,…]* $\bar{7}$ = *[…,-1,7,15,23,…]*

De relatief prieme restklassen modulo 8

$\overline{1}$, $\overline{3}$, $\overline{5}$ *en* $\overline{7}$ *zijn de relatieve prieme restklassen modulo 8. We kijken immers naar de restklassen die relatief priem zijn ten opzichte van 8.*

Tabel 2.6 De vermenigvuldiging van de relatief prieme restklassen modulo 8

x	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

De relatief prieme restklassen modulo 8, weergegeven in tabel 2.6 vormen een groep met de vermenigvuldiging, met neutraal element $\overline{1}$ *. Elk element heeft een inverse, namelijk zichzelf.*

2.6 De stelling van Euler

In deze sectie komt eerst Euler's totiëntfunctie aan bod, alvorens de stelling van Euler te bespreken.

2.6.1 Euler's totiëntfunctie Φ(n)

Φ(n) is Euler's totiëntfunctie en wordt gedefinieerd als het aantal positieve gehele getallen kleiner dan n en relatief priem met n (ggd(a,n)=1). ϕ(n) is dus ook gelijk aan het aantal elementen in de multiplicatieve groep van relatief prieme restklassen modulo n, $\mathcal{M}_n$.

Voorbeeld 1 Euler's totiëntfunctie

Stel n=14, dan zijn 1,3,5,9,11 en 13 de positieve getallen kleiner dan 14, die relatief priem zijn met 14, en dus slechts één gemeenschappelijke deler hebben, namelijk 1. Φ(14) = 6, want er zijn zes getallen die aan de voorwaarde voldoen.

Voorbeeld 2

Stel n=8, dan zijn de relatief prieme restklassen modulo 8: $\overline{1}, \overline{3}, \overline{5}$ *en* $\overline{7}$ → *Φ(8)=4*

2.6.2 Waarden van $\phi(n)$

- Voor een priemgetal p geldt dat $\phi(p) = p-1$.

- Onderstel 2 verschillende priemgetallen p en q, waarbij n = pq.
  ➔ $\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$.

- Meer algemeen kan vorige eigenschap als volgt geschreven worden:

  Onderstel pj verschillende priemgetallen, waarbij $n = p_1^{k1} p_2^{k2} \ldots p_m^{km}$, dan

  $$\Phi(n) = n\ (1-\frac{1}{p_1})\ (1-\frac{1}{p_2})\ \ldots\ (1-\frac{1}{p_m})$$

Voorbeelden eigenschap 2

n = 42 = 2 x 3 x 7 → $\phi(42) = \phi(2) \times \phi(3) \times \phi(7) = 1 \times 2 \times 6 = 12$

$$= 42 \times (1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{7}) = 12$$

n = 8 = 2^3 → $\phi(8) = \phi(2^3) = 8\ (1-\frac{1}{2}) = 4$

In tabel 2.7 staan een aantal waarden van $\phi(n)$ .De priemgetallen zijn omcirkeld. De waarde $\phi(1)$ heeft geen betekenis, maar krijgt per definitie de waarde 1.

Tabel 2.7 Enkele waarden van Euler's totiëntfunctie $\phi(n)$

n	$\phi(n)$	n	$\phi(n)$
1	1	11	10
2	1	12	4
3	2	13	12
4	2	14	6
5	4	15	8
6	2	16	8
7	6	17	16
8	4	18	6
9	6	19	18
10	4	20	8

2.6.3 Stelling van Euler

De stelling van Euler luidt als volgt:

$(\forall\ a,n \in \mathbb{N})$

ggd (a,n) = 1 $\Rightarrow$ **$a^{\phi(n)} = 1 \bmod n$** = 1+k*n

De stelling kan bijvoorbeeld worden toegepast ter vereenvoudiging van hoge machten in $\mathcal{M}_n$ (zie sectie 2.7). Hierbuiten bestaan er echter 2 essentiële toepassingen van deze stelling:

1) controle of p een priemgetal is (zie sectie 2.4.3).
2) gebruik bij het RSA algoritme (zie sectie 4.2.1).

Voorbeeld stelling van Euler

Stel n=10, dus $\mathcal{M}_{10}$ bevat $\bar{1}, \bar{3}, \bar{7}$ en $\bar{9}$

→ $\phi(10) = 4 = \phi(2) \times \phi(5) = 1 \times 4 = 4$

Stel a=$\bar{3}$ (is relatief priem met n=10)

$a^{\phi(n)} = 1 \bmod n \rightarrow 3^{\phi(10)} = 1 \bmod 10$

aangezien $\phi(10) = = 4 \rightarrow 3^4 = 81 = 1 \bmod 10$,

want (-8 x10) + 81 = 1

Een gevolg van deze stelling is:

$$\boldsymbol{a^m \bmod n = a^{m \bmod \Phi(n)} \bmod n}$$

Deze formule wordt gebruikt bij het berekenen machten modulo n (sectie 2.7)

De stelling kan gebruikt worden om de geldigheid van het RSA algoritme aan te tonen (zie sectie 4.2.1)

(Stallings, 2000)

2.7 Berekenen machten modulo n

Als a en n relatief priem zijn, bestaat er minstens één geheel getal dat aan de vergelijking $a^m = 1 \bmod n$ voldoet, namelijk $m = \phi(n)$. Dit klopt volgens de stelling van Euler.

Stel we willen $a^m \bmod n$ berekenen, met a en m zeer groot. Er kunnen zich dan twee scenario's voordoen.

<u>Scenario 1:</u> $\phi(n)$ bekend

Als $\phi(n)$ gekend is, kan de stelling van Euler gebruikt worden om eenvoudig hoge machten uit te rekenen. We gebruiken hiervoor meer bepaald volgende formule:

$$\boldsymbol{a^m = a^{m \bmod \phi(n)} \bmod n}$$

Voorbeeld

We willen $7^{315} \bmod 8$ berekenen:

$a=7$, $m=315$ en $n=8 \rightarrow \phi(n) = 4$

➔ *$7^{315} \bmod 8 = 7^{315 \bmod 4} \bmod 8$*

➔ *$= 7^3 \bmod 8$*

*Want 315 (mod 4) = 3 aangezien 315 = 4*78 + 3*

➔ *= 343 mod 8*

➔ *= 7 aangezien 8*42 + 7 = 343*

<u>Scenario 2:</u> ϕ(n) onbekend

Als ϕ(n) niet gekend is, kan a^m mod n berekend worden door m te herschrijven in een tweetallig stelsel: $m= x_0 + 2x_1 + 4x_2 + 8x_3 + \ldots = 2^0x_0 + 2^1x_1 + 2^2x_2 + 2^3x_3 + \ldots$ De uitleg hiervan gebeurd aan de hand van volgend voorbeeld.

Voorbeeld

We willen 7^{100} modulo 15 berekenen (a=7, m=100 en n=15), waarbij m als volgt kan worden herschreven: $100 = 64 + 32 + 4 = 2^6 + 2^5 + 2^2$

$7^0 = 1 \pmod{15} = 1$

$7^1 = 7 \pmod{15} = 7$

$7^2 = (7^1)^2 = 7^2 \pmod{15} = 49 \pmod{15} = 4$

$7^4 = (7^2)^2 = 4^2 \pmod{15} = 16 \pmod{15} = 1$

$7^8 = (7^4)^2 = 1^2 \pmod{15} = 1 \pmod{15} = 1$

$7^{16} = (7^8)^2 = 1^2 \pmod{15} = 1 \pmod{15} = 1$

$7^{32} = (7^{16})^2 = 1^2 \pmod{15} = 1 \pmod{15} = 1$

$7^{64} = (7^{32})^2 = 1^2 \pmod{15} = 1 \pmod{15} = 1$

$7^{100} \pmod{15} = 7^{(64+32+4)} \pmod{15} = 1 \times 1 \times 1 = 1 \bmod 15$

Ook op deze manier vergt het relatief weinig rekenwerk om een hoge macht modulo n uit te rekenen. Via beide scenario's is het berekenen van hoge machten modulo n een probleem met lage simpliciteit.

2.8 Algoritme van Euclides voor het berekenen van de grootste gemene deler (ggd)

Het algoritme van Euclides wordt gebruikt om de grootste gemene deler van twee positief gehele getallen te berekenen. Het algoritme steunt op volgend principe:

Stel d+e=f

Als g een deler is van d en e, dan is g ook een deler van f.

Het algoritme wordt weergegeven in tabel 2.8 (met $r_1 > r_2$).

Tabel 2.8 Het algoritme van Euclides

$d = r_1$	$e = r_2$	$\frac{r_1}{r_2} = q_1 + \frac{r_3}{r_2}$ ➔ $r_1=q_1*r_2+r_3$ ➔ $r_3 = r_1 \pmod{r_2}$	$r_3 < r_2$ en als $r_3 > 0$ ⟹
r_2	r_3	$\frac{r_2}{r_3} = q_2 + \frac{r_4}{r_3}$	$r_4 < r_3$ en als $r_4 > 0$ ⟹
…	…	…	…
r_{n-1}	r_n	$\frac{r_{n-1}}{r_n} = q_{n-1} + \frac{r_{n+1}}{r_n}$	$r_{n+1} < r_n$ en als $r_{n+1} = 0$

In de eerste stap is $r_1=q_1*r_2+r_3$, dus $r_1 - q_1*r_2 = r_3$

- ➔ Elke deler van r_1 en r_2, is een deler van r_3
- ➔ Elke deler van r_2 en r_3 is een deler van r_1

Dan: $ggd(d,e) = ggd(r_1,r_2) = ggd(r_2,r_3) = \ldots = ggd(r_{n-1},r_n)$;

dus **$ggd(d,e)= r_n$**

Zelfs voor een zeer grote d en e kan de grootste gemene deler in beperkte rekentijd gevonden worden. Het is dus een probleem met lage simpliciteit. Het aantal stappen zal maximaal van de orde ln n zijn.

Voorbeeld: ggd(6518,3458)

ggd(6518,3548)

In tabel 2.9 staat het uitgewerkt algoritme voor het vinden van deze ggd.

d=6518 en e =3548

Tabel 2.9 ggd(6518,3548)

d = 6518	e = 3548	$\frac{6518}{3548} = 1 + \frac{2970}{3548}$	2970 < 3548 en 2970 > 0, dus $\Longrightarrow$
3548	2970	$\frac{3548}{2970} = 1 + \frac{578}{2970}$	578 < 2970 en 578 > 0, dus $\Longrightarrow$
2970	578	$\frac{2970}{578} = 5 + \frac{80}{578}$	80 < 578 en 80 > 0, dus $\Longrightarrow$
578	80	$\frac{578}{80} = 7 + \frac{18}{80}$	18 < 80 en 18 > 0, dus $\Longrightarrow$
80	18	$\frac{80}{18} = 4 + \frac{8}{18}$	8 < 18 en 8 > 0, dus $\Longrightarrow$
18	8	$\frac{18}{8} = 2 + \frac{2}{8}$	2 < 8 en 2 > 0, dus $\Longrightarrow$
8	2	$\frac{8}{2} = 4 + \frac{0}{2}$	r_{n+1}=0, dus STOP

➔ ggd(6518,3548) = r_n = 2

➔ ln (6518) = 8,8 ≅ max. 8 stappen

2.9 Berekening van de inverse in $\mathcal{M}_n$ of R_n met het algoritme van Euclides

Met het algoritme van Euclides kan de grootste gemende deler berekend worden van twee positieve gehele getallen. Indien deze ggd 1 blijkt te zijn, zijn beide getallen relatief priem ten opzichte van elkaar.

In $\mathcal{M}_n$ (de multiplicatieve groep van prieme restklassen modulo n) bestaat de inverse altijd. In R_n bestaat de inverse enkel als ggd(a,n)=1. De inverse a^{-1} kan worden berekend door het algoritme van Euclides van achter naar voor toe te passen.

$$\boxed{\begin{aligned} a * a^{-1} &= 1 \mod n \\ a * a^{-1} &= 1 + kn \end{aligned}}$$ (met k een willekeurig getal)

Stel in het schema in tabel 2.7 d=n en e=a:

$r_1 = q_1 * r_2 + r_3 \rightarrow r_3 = r_1 - q_1 * r_2$

$r_2 = q_2 * r_3 + r_4 \rightarrow r_4 = r_2 - q_2 * r_3$

…

$r_{n-4} = q_{n-4} * r_{n-3} + r_{n-2} \rightarrow r_{n-2} = r_{n-4} - q_{n-4} * r_{n-3}$

$r_{n-3} = q_{n-3} * r_{n-2} + r_{n-1} \rightarrow r_{n-1} = r_{n-3} - q_{n-3} * r_{n-2}$

$r_{n-2} = q_{n-2} * r_{n-1} + r_n \rightarrow r_n = r_{n-2} - q_{n-2} * r_{n-1}$

Via substitutie verkrijgen we:

$r_n = (r_{n-4} - q_{n-4} * r_{n-3}) - q_{n-2} * (r_{n-3} - q_{n-3} * r_{n-2})$

$= \ldots$

$= \alpha r_1 + \beta r_2$

Aangezien de inverse van a (namelijk a^{-1}) bestaat als ggd(a,n) = 1, is $r_n = 1$

$\rightarrow \alpha r_1 + \beta r_2 = \alpha n + \beta a = 1$

$\rightarrow \beta a = 1 - \alpha n = 1 + kn$

→ Dus: $\boxed{\beta = a^{-1} \mod n}$

We kunnen dit verduidelijken aan de hand van volgend voorbeeld:

Voorbeeld 87^{-1} in $\mathcal{M}_{124}$

Allereerst dienen we de ggd(124,87) te berekenen, om te weten of de inverse kan worden berekend. Dit wordt weergegeven in tabel 2.10.

Tabel 2.10 ggd (124,87)

d = 124	e = 87	$\frac{124}{87} = 1 + \frac{37}{87}$	37 < 87 en 37 > 0, dus ⟹
87	37	$\frac{87}{37} = 2 + \frac{13}{37}$	13 < 37 en 13 > 0, dus ⟹
13	37	$\frac{37}{13} = 2 + \frac{11}{13}$	11 < 13 en 11 > 0, dus ⟹
13	11	$\frac{13}{11} = 1 + \frac{2}{11}$	2 < 11 en 2 > 0, dus ⟹
11	2	$\frac{11}{2} = 5 + \frac{1}{2}$	1 < 2 en 1 > 0, dus ⟹
2	1	$\frac{2}{1} = 2 + \frac{0}{1}$	r_{n+1}=0, dus STOP

➔ *dus ggd(124,87) = 1*

De ggd(124.87)=1, dus de inverse van de relatief prieme restklasse modulo 124 (relatief priem aangezien de grootste gemende deler 1 is) bestaat. We kunnen nu de inverse berekenen door het algoritme van Euclides van achter naar voor toe te passen.

$\overline{87}^{-1}$ in $\mathcal{M}_{124}$:

1 = 11 – (5 x 2)

= 11 – 5 x (13 – 11) = (6 x 11) – (5 x 13)

= 6 x (37 – (2 x 13)) – 5 x (87 – (2 x 37))

= (16 x 37) – (12 x 13) – (5 x 87)

= 16 x (124 – 87) – 12 x (87 – (2 x 37)) – (5 x 87)

= (16 x 124) – (1 x 87) + (24 x 37)

= (16 x 124) – (1 x 87) + 24 x (124 - 87)

= (40 x 124) – (25 x 87)

➔ $\overline{87}^{-1} = \overline{25} \pmod{124}$

2.10 One-way functies

De one-way functies of eenrichtingsfuncties vormen een belangrijke basis voor de public-key cryptografie (asymmetrische cryptografie). Een mogelijke definitie voor een one-way functie luidt als volgt: Een functie f (x)=y is een 'one-way' functie als het gemakkelijk is om $(\forall x \in X)$ f(x)=y te berekenen, maar voor $(\forall y \in Y)$ is het rekenkundig bijna onhaalbaar om een x ϵ X te vinden zodat f(x) = y (o.a. Menezes, Van Oorschot en Vanstone, 1997). Dit betekent dat het relatief eenvoudig is om f(x) uit x te berekenen, maar het bijna onhaalbaar is om x uit f(x), dus f^{-1} f(x) te berekenen. Dit principe kan vergeleken worden met het breken van het glas. Dit is ook erg gemakkelijk, maar het lijmen van de scherven is heel wat moeilijker (Wilschut, 2000).

Menezes et al. (1997) halen volgend voorbeeld aan om deze functie te verduidelijken:

Stel X= (1,2,3,...,16) en f(x)= 3^x (mod 17). In tabel 2.5 worden enkele waarden weergegeven.

Tabel 2.11 Waarden van de functie f(x) = 3^x (mod 17)

x	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*
f(x)	*3*	*9*	*10*	*13*	*5*	*15*	*11*	*16*	*14*	*8*	*7*	*4*	*12*	*2*

Bron: Menezes et al., 1997 (p.8)

Het is relatief eenvoudig om vanuit een x waarde de f(x) te berekenen, maar om vanuit de f(x) de x-waarde te vinden is bijna onmogelijk. (p.8)

2.11 Trapdoor functie

Een trapdoor one-way functie of valfunctie is een speciale vorm van one-way functie. Net zoals bij een gewone one-way functie is het relatief gemakkelijk om $(\forall x \in X)$ f(x)=y te berekenen. De trapdoor functie bevat echter de mogelijkheid om aan de hand van bepaalde informatie, de

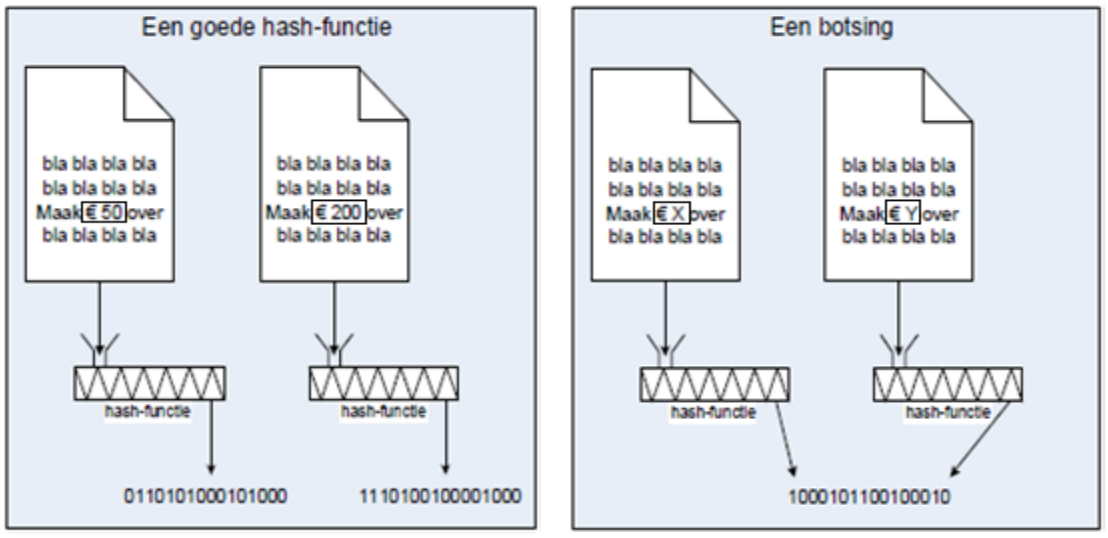
trapdoor informatie, $(\forall y \in Y)$ x ϵ X te berekenen zodat f(x)=y (Menezes, van Oorschot & Vanstone, 1997). Deze functies vormen de basis voor de public-key cryptografie. Hierbij geeft de private sleutel informatie over de 'trapdoor'. Degene die deze private sleutel bezit, kan dus de functie berekenen (RSA Laboratories ,2008 a).

2.12 Hash functie

Een manier om naar een hash functie te kijken is als een functie die uit een rij bits een soort vingerafdruk maakt, ook wel hashwaarde genoemd (De Weger, 2005). Vanuit een bepaalde input m berekent de hash functie H een output h van vaste lengte (RSA Laboratories, z.d. b).

Hash functie: h = H(m)

Hash functies zijn voor de digitale handtekening van groot belang. Maar dit gebruik vergt aandacht voor bepaalde eigenschappen. Een goede hash functie maakt voor elke zinnige rij bits een andere hashwaarde. Wanneer dit niet gebeurt, is er sprake van een botsing. Zulke botsingen kunnen niet uitgesloten worden aangezien er slecht een eindig aantal hash functies bestaan en het mogelijk aantal klare teksten veel groter is. Maar in praktijk zal het bij een goede hash functie onmogelijk veel tijd en rekenwerk vergen om botsingen te verkrijgen. In figuur 2.1 is het verschil zichtbaar tussen een goede hash functie en een botsing. Bij een goede hash functie leiden twee andere berichten tot twee verschillende hashwaarden. Bij een botsing wordt dezelfde hashwaarde verkregen.

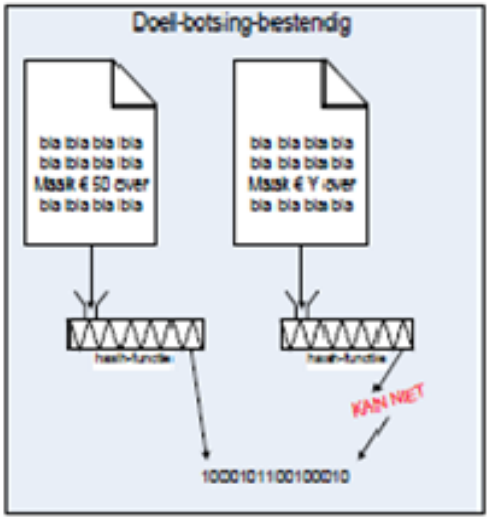


Figuur 2.1 Een goede hash functie versus een botsing bij een hash functie

Bron: De weger (2005)

Samengevat omschrijft RSA Laboratories (2008 b) volgende eigenschappen voor een goede hash functie:

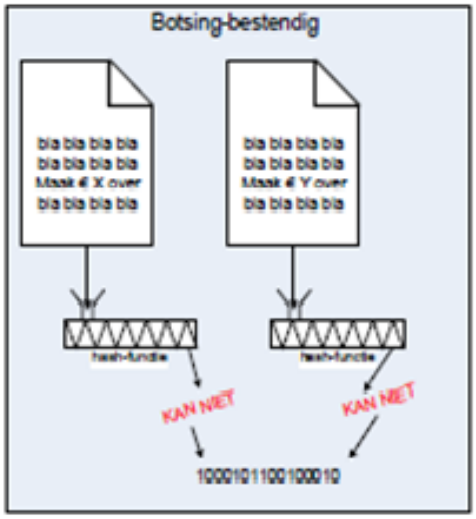
- de input x heeft een willekeurige lengte;
- de output h heeft een vaste lengte. Synoniemen voor deze output zijn de hash waarde of message digest;
- het is relatief eenvoudig om vanuit een bepaalde x de H(x) te berekenen
- één-richting (one-way) : om vanuit de hash-waarde h , de rij van bits (x) terug te vinden zodat H(x) = h, is rekenkundig onmogelijk. De functie werkt maar in één richting. (Het is een meerduidige eenrichtingsfunctie);
- doel-botsing-bestendig (weakly collision-free): het is niet mogelijk om vanuit één rij bits een andere rij af te leiden die dezelfde hash waarde oplevert. M.a.w., als een zinvol bericht x gegeven is, met h(x)=z, heeft het vinden van een zinvolle y (y≠x) zodat h(y)=z een hoge simpliciteit (Figuur 2.2);



Figuur 2.2 Doel-botsing-bestendigheid bij hash functies

Bron: De weger (2005)

- botsing-bestendig (strongly collision-free) : het is niet mogelijk twee rijen van bits x en y te vinden (die beide betekenisvol zijn), waarbij x ≠ y, die dezelfde hashwaarde hebben, dus zodat h(x) = h(y) (Figuur 2.3);



Figuur 2.3 Botsing-bestendigheid bij hash functies

Bron: De weger (2005)

Er zijn twee belangrijke hash functies hedendaags, namelijk Message Digest 5, MD5 en Secure Hash Algoritm 1, SHA1 (Silva, 2003).

– MD5 is de vijfde herziening van Message Digest, ontwikkeld door Rivest in 1991. Hun gebruik is vooral terug te vinden bij het digitaal ondertekenen van lange berichten. Het lange bericht zal dan eerst verkort worden alvorens te "ondertekenen". De input mag van willekeurige lengte zijn terwijl de output altijd uit 128 bits zal bestaan (RSA Laboratories, 2008 c).

– SHA1 is een algoritme ontwikkeld door het 'National Security Agency' in 1995. De input mag willekeurig zijn, maar niet langer dan 2^64 bits. De output is dan een bericht met een lengte van 160 bits.

Beide hash functies werden geacht veilig en botsingvrij te zijn. In 2004 werd echter bekend gemaakt dat de MD5 hash functie gekraakt was. Het is mogelijk botsingen te vinden voor dit algoritme binnen een uur. Ook de veiligheid van de hash functie SHA1 werd in vraag gesteld. Een gereduceerde versie van dit algoritme is al gekraakt en de geschatte nodige werktijd om SHA 1 volledig te kraken is reeds verminderd.

De meest gebruikte toepassingen van een hash functie in de cryptografie zijn het gebruik bij de digitale handtekening en het gebruik om de data integriteit te waarborgen (Menezes, et.al., 1997).

- Om de integriteit van data te waarborgen, kan de hashwaarde berekend worden. Nadien kan men dan, om na te gaan of de inhoud niet veranderd is, opnieuw de hash waarde berekenen. Deze dient dan dezelfde te zijn als eerst berekend, omwille van de eigenschap 'doel-botsing-bestendig'.

- Vaak zijn de berichten die we digitaal willen ondertekenen erg groot en vraagt het veel rekenwerk om hiervoor een digitale handtekening te berekenen. Een mogelijke oplossing is het bericht te verdelen in stukken van elk slechts een lengte van bijvoorbeeld 160 bits, en deze stukken elk digitaal te ondertekenen, maar dit vergt ook veel werk. Door het gebruik van een hash functie kan het lange bericht omgezet worden naar een bericht van vaste lengte (bijvoorbeeld 160 bits). Deze hash waarde (of message digest) wordt dan digitaal ondertekend. Merk op dat dit "ondertekenen" niet impliceert dat er iets wordt bijgevoegd, maar wel dat men het versleutelt met zijn private sleutel.

Voorbeeld hash functie

Context: Een gevangene werd door de tsaar van Rusland uitgewezen naar Siberië. De gevangene vroeg echter gratie aan de tsaar om niet naar Siberië te moeten gaan. De tsaar antwoordde hierop "In geen geval, naar Siberië". De tsarina had echter medelijden met de gevangene en verwijderde de komma. De gevangene kreeg dus volgend bericht aan: "In geen geval naar Siberië", waardoor hij foutief dacht dat hij gratie gekregen had. Dit illustreert dat de kleinste wijziging een heel andere boodschap kan opleveren. Beide boodschappen zullen ook een andere hashwaarde hebben.

Hash functie: *1) Neem de som van de twee uiterste letters, daarna de som van de 2^e en de voorlaatste letter, enz. De komma wordt als 27^{ste} teken voorgesteld. (reken modulo 26)*

2) draai per twee letters de tekst om

Boodschap: In geen geval, naar Siberië

Hashwaarde

1^e toepassing hash functie:

1) 14 23 25 10 7 23 26 23 23 2 26 1
n w y j g w z w w b z a

2) w n j y w g w z b w a z
23 14 10 25 23 7 23 26 2 23 1 26

2e toepassing hash functie:

1) *23 15 7 1 23 4*
   w o g a w d

2) *o w a g d w*
   15 23 1 7 4 23

3e toepassing hash functie

1) *12 1 8*
   l a h

2) *a l h*
   1 12 3

Boodschap: In geen geval naar Siberië

Hashwaarde

1e toepassing hash functie:

1) *14 23 25 10 7 23 26 23 23 2 26*
   n w y j g w z w w b z

2) *w n j y w g w z b w z*
   23 14 10 25 23 7 23 26 2 23 26

2e toepassing hash functie:

1) *23 11 12 25 20 7*
   w k l y t g

2) *k w y l g t*
   11 23 25 12 7 20

3e toepassing hash functie

1) *5 4 11*
   e d k

2) *d e k*
   4 5 11

2.13 Code theorie

De online encyclopedie (2008) omschrijft coderingstheorie als "een onderdeel van de informatietheorie dat zich richt op het toevoegen van redundantie aan gecodeerde informatie, waardoor het beter beschermd is tegen mogelijke fouten die kunnen optreden tijdens transport over een onbetrouwbaar kanaal". Code theorie mag niet verward worden met cryptografie.

Coderen kan opgesplitst worden in drie stappen (Buyst, 1967). De bron bestaat uit een verzameling symbolen. Elk symbool kan gekoppeld worden aan een getal, uitgedrukt in cijfers. Meestal wordt gebruik gemaakt van binaire cijfers (0 en 1). Deze omzetting maakt deel uit van de eerste stap. De verkregen cijfers moeten omgezet worden in elektrische impulsen om ze te versturen over een kanaal. Zo kan bijvoorbeeld het cijfer één voorgesteld worden door een elektrische puls en het cijfer nul door de afwezigheid ervan.

Voorbeeld: BCD code *(Buyst, 1967, p.11)*

De BCD code is een code voor het seinen van decimaal geschreven getallen. Elk cijfer van een getal wordt voorgesteld in binaire vorm:

0: 0000	*3: 0011*	*6: 0110*	*9: 1001*
1: 0001	*4: 0100*	*7: 0111*	
2: 0010	*5: 0101*	*8: 1000*	

Aangezien voor de cijfers 8 en 9 vier bits nodig zijn, worden er overal 4 bits gebruikt. Met vier bits kunnen 16 (=2^4) combinaties gevormd worden. Er worden echter maar 10 combinaties gebruikt, waardoor er sprake is van redundantie. Hierdoor kunnen fouten opgespoord worden. Immers als de code 1101 voor komt, weet men dat er ergens een fout gebeurd is. Het is echter niet mogelijk de fout aan te passen, aangezien het oorspronkelijke zowel 1001 (=9) als 0101 (=5) kan zijn. Het is dus geen code waarbij fouten kunnen worden verbeterd.

2.13.1 Foutendetectie en foutenverbetering

Een code kan foutendetecterend zijn. Indien er - zoals in het vorige voorbeeld - sprake is van redundantie, kunnen sommige fouten opgespoord worden. Het opnemen van een aantal testwoorden is een manier van foutendetectie. Indien er een testwoord doorgeseind wordt, is men zeker van een fout. Men kan echter nooit 100% zeker zijn dat al de fouten opgespoord worden. Immers bij het doorkrijgen van een goed codewoord, onderstelt men geen fout. Dit is echter niet altijd correct. Voor foutenverbetering is er erg veel redundantie nodig in een code. Bij ontvangst van een foutief woord, gaat men na welk codewoord dit met de meeste waarschijnlijkheid benadert. Bij een goede code is de kans op een juiste verbetering echter veel groter dan de kans op een foute verbetering (Buyst, 1967).

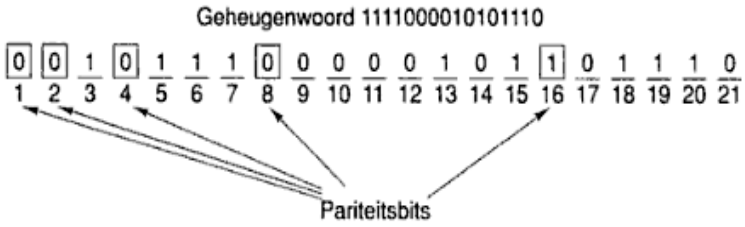
De meest eenvoudige vorm van foutendetecterende code is waarschijnlijk de pariteitsbit. De pariteitsbit (1 of 0) wordt toegevoegd aan een rij van bits en zorgt ervoor dat het aantal enen in het codewoord even of juist oneven is. De toegevoegde bit bevat op zich geen informatie maar dient uitsluitend ten opsporing van fouten. Elke fout van slechts één bit levert een codewoord met een foute pariteit (Buyst, 1967).

2.13.2 De Hamming-code

Waarschijnlijk de meest bekende foutencorrigerende code is de Hamming code. Voor een woord dat kan worden weergegeven door m bits, worden r pariteitsbits gebruikt. Het woord wordt dus weergegeven door m+r bits. Elke bit krijgt een nummering, te beginnen met de meest linkse bit die het nummer 1 toebedeeld krijgt. In totaal zijn er dus r+m bits. Elke bit waarbij de nummering een macht van twee is, is een pariteitsbit. In een codewoord van 16 bits, zijn de bits 1($=2^0$), 2 ($=2^1$), 4 ($=2^2$), 8 ($=2^3$) en 16 (2^4) de pariteitsbits. De overige bits zijn informatiedragers. Elke bit wordt gecontroleerd door bepaalde pariteitsbits. De algemene regel is dat pariteitsbits met bitnummers b_1,b_2,… de bit b controleren waarvoor $b=b_1 + b_2 + \dots$. Bit 5 wordt bijvoorbeeld gecontroleerd door de pariteitsbits 1 en 4. Een pariteitsbit krijgt de waarde 1 of 0 toegekend zodat het totaal aantal enen op de betrokken nummers even is (Tanenbaum en Geurts, 2005).

V***oorbeeld van de Hamming-code***.

Het codewoord bevat 16 bits, aangevuld met 5 pariteitsbits.



Figuur 2.4 Voorbeeld Hamming-code

Bron: Tanenbaum en Geurts, 2005 (p.77)

Bit 2 (=pariteitsbit) heeft betrekking op de bits 2, 3, 6, 7, 10, 11, 14, 15, 18 en 19. Bit 16(=pariteitsbit) heeft hier betrekking op de bits op nummer 16, 17, 18, 19, 20 en 21. Dit is correct aangezien enkel deze bits de som kunnen zijn van bit 16 met een andere bit. Het totaal aantal enen van al deze bits moet dus even zijn om de code te doen kloppen. Dit klopt hier.

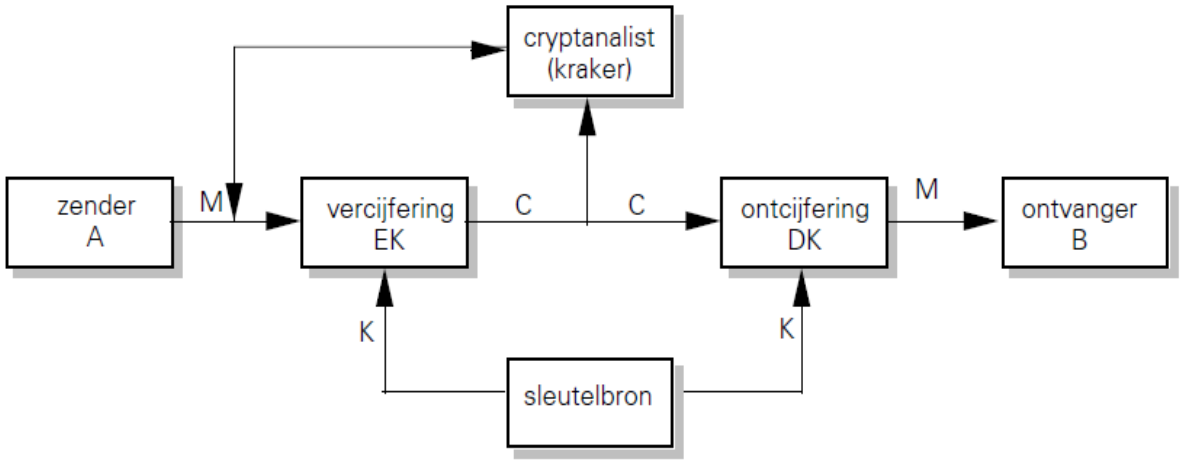
Om een code te corrigeren, dienen eerst al de pariteitsbits berekend te worden. Zijn deze allemaal correct, is de code correct. Bij een fout gaat men als volgt te werk: tel de bitnummers van de foute pariteitsbits op. De uitkomst van deze som geeft de positie weer van de foute bit (Tanenbaum en Geurts, 2005).

Hoofdstuk 3 Cryptologie

In dit hoofdstuk komt het begrip cryptologie aan bod. Het woord cryptologie is afkomstig uit het Grieks en komt voort uit twee woorden, namelijk kryptós, hetgeen verborgen betekent, en lógos of woord (Encyclopedie Britannica, 2008). Van Tilborg (1993) omschrijft cryptologie als de wetenschap die cryptosystemen bestudeert. Enerzijds bestudeert deze wetenschap de realisatie van cryptosystemen, anderzijds is er het 'kraken' van deze systemen. De eerste variant wordt cryptografie genoemd, terwijl zijn tegenhanger de naam cryptoanalyse meekrijgt.

3.1 Begrippen

Figuur 3.1 geeft een overzicht van een mogelijk cryptosysteem.



Figuur 3.1 Een cryptosysteem

Bron: Van der Lubbe, 1997

Eerst komt een verklaring van enkele begrippen aan bod, alvorens we figuur 3.1 uitgeleggen:

- Plaintext of klare tekst: het niet-vercijferde bericht M dat afzender A wil versturen naar ontvanger B;
- Ciphertext of cijfertekst: de vercijferde tekst C;
- Key of sleutel: de klare tekst wordt omgezet naar de cijfertekst aan de hand van een sleutel K;
- Encryptie of vercijfering: het omzetten van de klare tekst naar de cijfertekst;
- Decryptie of ontcijfering: het omzetten van de cijfertekst naar de klare tekst;

– Cryptoanalist: de persoon die probeert de cijfertekst te ontsleutelen of te kraken zonder dat de boodschap voor hem bedoeld is.

Aan de hand van deze definities kan figuur 3.1 besproken worden. De afzender A wil een bericht M versturen naar ontvanger B zonder dat een derde partij dit bericht kan lezen. De klare tekst wordt omgezet naar een vercijferde tekst C aan de hand van sleutel K. De ontvanger kan ook gebruik maken van de sleutel K om de ciphertekst te ontsleutelen. EK staat voor encryptie met sleutel K. DK staat voor decryptie met sleutel K. De cryptoanalyst zal proberen de ciphertekst te ontsleutelen (Van der Lubbe, 1997). In dit schema wordt slechts één sleutel gebruikt. Er is dus sprake van symmetrische cryptografie (zie sectie 3.2).

Aan figuur 3.1 kan bovendien ook gebruik van de codetheorie toegevoegd worden. Op ciphertext c zou dan bijvoorbeeld de Hamming-code toegepast kunnen worden alvorens het te verzenden. We verkrijgen dan bericht K dat A naar B verstuurt. B ontvangt dan bericht K + ε (met ε een transmissiefout). Na decodering verkrijgt B terug ciphertext C waarop hij dan sleutel K kan toepassen voor de decryptie.

3.2 Cryptografie

Cryptografie kan gedefinieerd worden als de wetenschap die zich bezighoudt met het versleutelen van informatie en ontcijferen van versleutelde informatie (o.a. Tieleman & Vernooij, 2002). Net zoals bij cryptologie, is het woord cryptografie gebaseerd op twee Griekse woorden, kryptós en gráphein (schrijven). Kortom kan cryptografie dus omschreven worden als verborgen, of geheim schrijven (Encyclopedie Britannica, z.d.). Door het vercijferen van gegevens (encryptie) wordt een boodschap onleesbaar gemaakt. De ontvanger van de boodschap kan het bericht enkel ontcijferen (decryptie) als hij de gebruikte encryptiemethode en de bijhorende sleutel kent. Deze vormen samen het cryptosysteem.

Er bestaan twee soorten cryptografie, afhankelijk van de gebruikte sleutel:

- **Symmetrische cryptografie**: Indien er voor encryptie en decryptie dezelfde geheime sleutel wordt gehanteerd, spreekt men over symmetrische cryptografie. Het gebruik van eenzelfde sleutel is het belangrijkste verschil met de asymmetrische cryptografie. Het DES algoritme is waarschijnlijk de meest gebruikte vorm van dit soort cryptografie (Van der Lubbe, 1998).

- **Asymmetrische cryptografie**: Asymmetrische cryptografie daarentegen maakt gebruik van twee verschillende sleutels, één private en één publieke. De publieke sleutel wordt gebruikt voor het versleutelen van de informatie en de private voor het ontsleutelen. Deze

vorm wordt ook public-key system genoemd. Hierbij is het RSA-cryptosysteem het meeste bekende algoritme (Stallings, 2000).

De oorsprong van cryptografie, of het coderen van boodschappen, is terug te brengen naar het begin van onze beschaving. Al zodra de mensen met elkaar konden communiceren, ontstond de behoefte om sommige boodschappen geheim te houden, en er dus een bepaalde code voor te hanteren. Een van de meest bekende oude toepassingen van cryptografie is wellicht de 'Caesar's code'. Het Romeinse leger maakte gebruik van deze code om informatie geheim te houden van hun tegenstanders. De code bestond eruit elke letter van een woord te vervanger door de letter die zich 3 plaatsen naar achter in het alfabet bevond. Een 'a' werd dus een 'd' en een 'l' werd een 'o'. Maar reeds voor Caesar's code is er in de 5^{e} eeuw voor Christus een toepassing van cryptografie terug te vinden bij de Grieken. De verzender van de boodschap gebruikte een stok, scytale genaamd, waarrond een papier gebonden werd. Het bericht werd in de lengte op het papier geschreven waardoor het niet leesbaar was zonder een stok van de juiste dikte. Hedendaags zijn de cryptografische toepassingen veeleer op wiskunde gebaseerd (Loidreau, 2002).

In hoofdstuk 4 gaan we uitgebreid in op cryptografie.

3.3 Cryptoanalyse

Cryptoanalyse is het tweede onderdeel van cryptologie, en de opponent van cryptografie. Terwijl cryptografie een bericht versleutelt om het uit handen van derden te houden, wordt cryptoanalyse kort omschreven als het breken van geheimschrift (Van der Meer, 2007). Een vaak aangenomen assumptie is dat de 'opponent' of cryptoanalist weet heeft van het gebruikte cryptosysteem. Deze assumptie wordt het principe van Kerckhoff genoemd. De ontwikkeling van een cryptosysteem om informatie te versleutelen gaat vaak uit van dit principe.

De cryptoanalist kan op drie manieren een 'aanval' plegen op het cryptosysteem:

- De eerste vorm is een aanval op de gecodeerde tekst alleen, de **'ciphertext-only-attack**'. Hierbij beschikt de cryptoanalist enkel over de vercijferde tekst, en moet hij zo op zoek gaan naar de sleutel. Dit is de moeilijkste uitgangspositie.

- Bij een tweede vorm, de **'known-plaintext-attack'**, beschikt de kraker over informatie van zowel cijfertekst als klare tekst. Op basis hiervan kan hij trachtten de sleutel te vinden om zo het resterende deel van de cijfertekst te ontsleutelen.

- Het beste scenario voor de cryptoanalist doet zich voor indien hij willekeurige tekst kan vinden en de daarbij horende vercijferde tekst kan achterhalen, om zo de sleutel te vinden. Hierbij spreekt men van de **'chosen-plaintext-attack'** (Van der Lubbe, 1997).

Er zijn twee uiteenlopende meningen terug te vinden over cryptoanalyse. Een eerste stroming vindt dat het 'proberen' te kraken op zich niet strafbaar is. De systemen moeten gemaakt zijn zodat ze niet gekraakt kunnen worden. Een andere stroming vindt dat elke poging tot kraken ook strafbaar moet zijn.

3.4 De digitale handtekening

Een digitale handtekening kan steunen op asymmetrische cryptografie. De private sleutel dient hierbij ter aanmaak van de handtekening terwijl de publieke sleutel dienst doet als verificatiemethode. De digitale handtekening maakt tevens ook gebruik van een ander belangrijk principe, namelijk 'hashing'. De hash-functie is reeds aan bod gekomen in sectie 2.12. Om de digitale handtekening nog veiliger te maken, kan men werken met certificaten. Aan de hand hiervan kan bijvoorbeeld ook de werkelijke identiteit achter een e-mailadres gegarandeerd worden. Certificaten worden uitgereikt door een speciale instelling, de certificatieautoriteit. Zowel de digitale handtekening als de certificatieautoriteit komen verder aan bod in hoofdstuk 5.

Hoofdstuk 4 Cryptografie

Zoals reeds in hoofdstuk 3 aangehaald, betekent cryptografie het geheim schrijven. Er bestaan twee soorten, namelijk symmetrische en asymmetrische cryptografie. Beide komen hier uitgebreid aan bod.

4.1 Symmetrische cryptografie

Deze vorm van cryptografie wordt ook wel de conventionele vorm genoemd omdat dit de eerst gebruikte soort cryptografie is. Het is hedendaags ook nog de meest gebruikte.

De klare tekst of plaintext wordt omgezet in een versleutelde tekst of ciphertekst. Deze omzetting of encryptie bestaat uit een algoritme en een sleutel. De versleutelde tekst is afhankelijk van de gebruikte sleutel. Een andere sleutel levert een ander resultaat. Na verzending zal de versleutelde tekst terug omgezet worden naar de oorspronkelijke plaintext aan de hand van dezelfde sleutel en een decryptie algoritme. Het gebruik van dezelfde sleutel voor encryptie en decryptie is de belangrijkste eigenschap van symmetrische cryptografie in vergelijking met de asymmetrische variant (Stallings, 2000).

Vervolgens komen een aantal conventionele systemen van cryptografie aan bod. We maken een opdeling in de klassieke technieken en de modernere technieken van symmetrische crytografie. Een andere mogelijke opdeling zou deze van stroom- en blokvercijferingen kunnen zijn. Bij stroomvercijfering wordt elke bit apart vercijferd, terwijl bij een blokvercijfering een blok uit de klare tekst in één keer vercijferd wordt tot een blok van dezelfde lengte (o.a. Stallings, 2000).

4.1.1 Klassieke technieken

Bij deze technieken worden de letters van een woord vervangen door een andere letter, een cijfer of symbool. De meeste van deze technieken zijn stroomvercijferingen, behalve de Hill-vercijfering. Deze behoort tot de blokvercijferingen.

- **Caesar-vercijfering**

  De meest bekende toepassing van deze techniek is de Caesar- vercijfering, reeds besproken in sectie 2.1. Een letter in een woord wordt hierbij vervangen door de letter die drie posities later komt in het alfabet. Indien we de letters gelijkstellen aan nummers (a=1, b=2,…), kunnen we de letter in ciphertext als volgt voorstellen:

  $C = E(p) = (p+3) \bmod(26)$

De C staat hier voor de letter in de ciphertext, de p voor de letter in de plaintext.

Bij deze vercijfering is het relatief eenvoudig om vanuit een ciphertext de oorspronkelijke tekst te achterhalen. Er wordt gezegd de toepassing van een brute- kracht cryptoanalyse mogelijk is. Er zijn immers slechts 25 sleutels mogelijk, de taal van de oorspronkelijke tekst is bekend en ook de encryptie- en decryptie- algoritmen zijn gekend.

- **Monoalfabetische vercijferingen**

Deze soort vercijfering is een variant op de Caesar vercijfering, maar is moeilijker te kraken omdat er een willekeurige substitutie wordt toegestaan. Er zijn hier dan 26! of meer dan $4x10^{26}$ mogelijke sleutels. Ze zijn echter nog vrij eenvoudig te kraken omdat er een patroon terug te vinden is.

- **Playfair- vercijfering**

Dit algoritme maakt gebruik van een matrix. De letters i en j worden gezien als één letter, waardoor de resterende 25 letters in een matrix geplaatst kunnen worden aan de hand van een sleutelwoord. Het sleutelwoord wordt eerst in de matrix geplaatst, van links naar rechts en van boven naar onder. Een letter die meerdere keren in een woord voorkomt, wordt maar één keer geschreven. Na het woord, worden de resterende letters van het alfabet achter elkaar in de matrix geschreven. Hierdoor zijn de 25 plaatsen opgevuld. Indien het sleutelwoord 'Monarchy' zou zijn, levert dit de matrix op, weergegeven door tabel 4.1.

Tabel 4.1 Playfair – vercijfering met sleutelwoord 'monarchy'

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Bron: Stallings, 2000

De klare tekst wordt dan aan de hand van volgende regels versleuteld. Er worden telkens twee letters te samen versleuteld.

- Indien een paar van letters uit dezelfde letters zouden bestaan, worden deze gescheiden door een opvulletter.

- Letters die zich in de zelfde rij van de matrix bevinden, worden vervangen door de letter die er naast staat, aan de rechter kant, of door de eerste letter van de rij die rondgaand na het laatste element komt. Ar wordt zo dus RM.
- De letters die zich in dezelfde kolom bevinden, worden vervangen door de letter er onder, of door de bovenste letter die rondgaand na het eerste element komt. Mu wordt zo versleuteld tot CM.
- De overige letters worden elk vervangen door de letter die in dezelfde rij ligt als zichzelf en die in de kolom ligt die door de andere letter wordt bezet. Hs wordt zo BP en ea wordt IM of JM.

- **Hill- vercijfering**

De encryptie gebeurt doordat m opeenvolgende letters van de klare tekst vervangen worden door m opeenvolgende letters van de versleutelde tekst. Een aantal (m) lineaire vergelijkingen bepalen de subsitutie, waarbij elk teken een numerieke waarde toegekend krijgt, van 0 (=a) tot 25 (=z). Voor m= 3 kunnen we volgende vergelijkingen onderscheiden:

$$\left.\begin{aligned} C_1 &= (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26 \\ C_2 &= (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26 \\ C_3 &= (k_{31}p_1 + k_{32}p_3 + k_{33}p_3) \bmod 26 \end{aligned}\right\} \quad \text{in termen van vectoren: } C = KP$$

C (ciphertext) en P (plaintext) zijn kolomvectoren van lengte 3 en K is een 3x3 matrix die de encryptiesleutel voorstelt. Al de bewerkingen worden uitgevoerd modulo 26.

Voorbeeld

We willen de plaintext 'paymoremoney' versleutelen. Onderstel $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

De eerste drie letten 'pay' worden weergegeven door $P = \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$

➔ $C = KP = \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = LMS$

Op deze manier kan de gehele plaintext gecodeerd worden.

Om de ciphertext nadien te ontsleutelen, is er nood aan de inverse van K, met eenheidsmatrix

$I=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Over hoe we de inverse K^{-1} juist bepalen, wordt hier niet verder op in gegaan.

We kunnen stellen dat voor de decryptie geldt dat $P= K^{-1}C$.

- **Vigenère cryptosysteem**

Deze techniek is ook een variant op de Caesar vercijfering, maar is heel wat moeilijker te kraken. Het aantal op te schuiven letters in het alfabet zal hier variëren met een bepaald sleutelwoord. In principe tel je de zin die je wil coderen op met het sleutelwoord, of hier een herhaling van (Tieleman & Vernooij, 2002). Het Vigenère vierkant, weergegeven in tabel 4.2, is een hulpmiddel bij het coderen. Je moet op de horizontale as kijken naar de letter die je wil versleutelen en op de verticale as naar de overeenkomstige letter van het sleutelwoord. Op die manier vind je de cipher letter (o.a. Stallings, 2000).

Voorbeeld

Klare tekst: jan en mien liepen door het bos

Sleutelwoord: crypt

De letter 'j' versleuteld, geeft de 'l'.

➔ *Op die manier kan de gehele zin versleuteld worden.*

Klare tekst	*J A N E N M I E N L I E P E N D O O R H E T B O S*
Sleutel	*C R Y P T C R Y P T C R Y P T C R Y P T C R Y P T*
Versleutelde tekst	*L R L T G O Z C E E K V N T G F F M G A G K Z D L*

Tabel 4.2 Het Vigenère vierkant

	a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Bron: Stallings, 2000

4.1.2 Data Encryption Standard (DES)

DES is waarschijnlijk de meest bekende en meest gebruikte vorm van symmetrische cryptografie, en behoort tot de blokalgoritmes. DES is gebaseerd op het door IBM ontwikkelde Lucifer-algoritme. Dit algoritme versleutelt blokken van 128 bits. DES daarentegen werkt met blokken van 64 bits. Ook de gebruikte sleutel is 64 bits, maar er wordt slechts gebruik gemaakt van 56 bits omdat elke 8^{ste} bit gebruikt wordt ter controle. Het aantal mogelijke sleutels loopt dus op tot 2^{56} (Van der Lubbe, 1998).

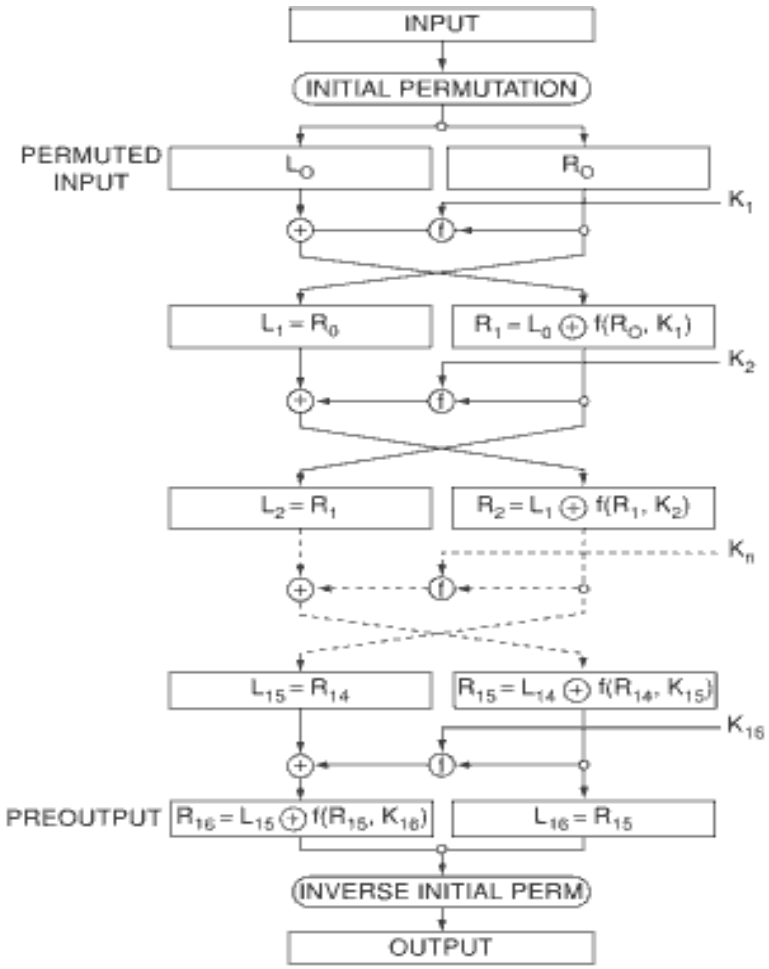
Feistel-vercijfering

DES maakt gebruikt van het Feistelnetwerk. De Feistel-vercijfering maakt geen gebruik van simpele optellingen of substituties, maar van productvercijfering. Hiermee wordt bedoeld dat twee (of meer) basisvercijferingen achtereenvolgens uitgevoerd worden, om de klare tekst beter te coderen en beveiligen. Bij het feistelnetwerk is er meer specifiek sprake van een afwisseling van permutaties en substituties. De klare tekst wordt opgedeeld in twee deelblokken die elk een aantal ronden doorlopen, met elk een bijhorende deelsleutel (Stallings, 2000). De exacte werking wordt uitgelegd aan de hand van de Data Encryption Standard. Hiervoor is het echter noodzakelijk om het concept van productvercijfering, of XOR, kort te bespreken. De XOR functie, aangeduid met $\oplus$, kan een combinatie van de waarden 1 en 0 aannemen. De XOR van twee waarden is 1 indien precies één van deze twee waarden 1 is. In de andere gevallen is de XOR waarde 0 (Tieleman en Vernooij, 2002).

De plaintext bestaat onder DES uit 64 bits en wordt aan de hand van 16 ronden omgezet in een ciphertext van 64 bits op basis van een 56 bits sleutel. Deze sleutel vormt samen met de plaintext de input van de encryptiefunctie. Alle stappen van het proces zijn weergegeven in figuur 4.1. Allereerst vindt er een beginpermutatie plaats (IP) waar de bits gerangschikt worden tot de gepermuteerde input, $X_0=IP(X)=(L_0,R_0)$. Hierna volgen de 16 ronden, waar de 64 bits lange plaintext gesplitst wordt in twee blokken van 32 bits, aangeduid als L en R (links en rechts). R wordt in elke ronde gebruikt door de functie f, waarna opgeteld bij L. De gebruikte functie bestaat uit 4 delen (Van Tilborg, 2005):

- Expansie: de input van 32 bits wordt omgevormd tot één van 48 bits, door de helft van de bits te kopiëren en opnieuw te rangschikken.
- Mixen van de sleutel: er wordt gebruik gemaakt van een sleutel van 48bits (geselecteerd uit de 56-bits sleutel). Elke ronde wordt een andere sleutel geselecteerd. Op basis van deze sleutel wordt op de input een XOR toegepast. $F(L,R) = (L \oplus F(R,SK), R)$ waarbij SK de deelsleutel is.
- Substitutie: Het resultaat van 48 bits gaat door een substitutiefunctie om uiteindelijk een uitvoer van terug 32 bits te verkrijgen. Dit gebeurt als volgt: men splitst de blok van 48 bits in 8 S-boxen van zes bits die als uitvoer elk 4 bits hebben.

- Permutatie: de 32 bits worden dan opnieuw geordend.



Figuur 4.1 Des-encryptie

Bron: Van Tilborg, 2005 (p. 129)

Volgende formules geven een samenvatting van elke ronde i:

- $L_i = R_{i-1}$ →in elke ronde wordt de rechterhelft naar links gebracht
- $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$ → op de rechterkant wordt dan de functie van het feistel-netwerk toegepast aan de hand van deelsleutel K_i.

Na de 16 ronden, wordt een eindpermutatie (IP^{-1}) toegepast om zo de ciphertekst van 64 bits te verkrijgen (Stallings, 2000).

Het DES-decryptiealgoritme verloopt exact hetzelfde als dit van de encryptie. Alleen de deelsleutels worden in omgekeerde volgorde gebruikt. Het veranderen van één bit in de plaintext resulteert bij

DES in een grote verandering van de ciphertext. Dit effect wordt het lawine-effect genoemd en is aanzienlijk groot bij het gebruik van DES (Stallings, 2000).

Symmetrische of conventionele cryptografie wordt voornamelijk gebruik voor het onleesbaar maken van informatie voor derden omwille van vertrouwelijkheid. Het kan echter ook aangewend worden om de oorsprong en integriteit van een bericht te verzekeren. Hiervoor is het natuurlijk belangrijk dat er groots wederzijds vertrouwen bestaat tussen verzender en ontvanger, aangezien ze beide op de hoogte moeten zijn van de geheime sleutel (Van Eecke, 2004). Om dit probleem te omzeilen, kan de uitwisseling van sleutels veilig gebeuren door gebruik te maken van asymmetrische cryptografie.

4.2 Asymmetrische cryptografie

Het belangrijkste kenmerk van asymmetrische cryptografie is het gebruik van twee verschillende sleutels, één voor encryptie en één voor decryptie. Eén van deze sleutels is openbaar, de andere privé (Van Tilborg, 2005). De openbare sleutel wordt gebruikt voor de encryptie, terwijl de private sleutel dient om de boodschap terug te ontsleutelen. Deze techniek wordt ook public-key cryptografie genoemd. Het principe is dat wanneer persoon A een geheim bericht naar persoon B wil versturen, A de plaintext versleutelt met de publieke sleutel van B, waarna B de ciphertext kan ontsleutelen met zijn geheime sleutel. Iedereen kan dus een geheime boodschap verzenden naar persoon B. Naast dit gebruik voor encryptie en decryptie, wordt een public-key cryptosysteem ook gebruikt voor de digitale handtekening. Hierbij zal persoon A het bericht "ondertekenen" met zijn/haar geheime sleutel. Een ander belangrijk verschil met de symmetrische variant is dat deze methode gebruik maakt van wiskundige functies in plaats van simpele bewerkingen zoals substitutie en permutatie. Het bekendste public-key cryptosysteem is het RSA algoritme (Stallings, 2000).

4.2.1 Het algemeen principe van asymmetrische cryptografie

- De trapdoor functie:

y = f(x) is een trapdoor functie als

1) y = f(x) relatief eenvoudig kan worden berekend (lage simpliciteit).
   → Publieke sleutel;
2) $x = f^{-1}(x)$ niet kan worden berekend als men enkel de informatie heeft om f(x) te berekenen (hoge simpliciteit);

3) $x = f^{-1}(x)$ wel eenvoudig kan worden berekend als men bijkomende informatie ter beschikking heeft (lage simpliciteit).
   → Private sleutel

- Personen in het communicatienet zijn A, B, C, …. Zij hebben elk respectievelijk een publieke sleutel (f_A, f_B, f_C, …) en een private sleutel (f_A^{-1}, f_B^{-1}, f_C^{-1}, …).

Dan:

- Als A een geheim bericht x naar B wil zenden, versleutelt hij het bericht eerst met de publieke sleutel van B. → A zendt dus naar B: $y = f_B(x)$.
  Iedereen kan y ontvangen, maar enkel B kan het ontsleutelen met zijn geheime sleutel:
  → B berekent $x = f_B^{-1}(y)$

- Als A een bericht wil ondertekenen alvorens het naar B te verzenden, moet hij het versleutelen met zijn eigen private sleutel. → A zendt $z = f_A^{-1}(y)$.
  B berekent $f_A(z) = y$ (Iedereen kan dit doen).
  Niemand kan een z vinden zodat $f_A(z) = y$ (met y zinvol), behalve A. Dit impliceert dat enkel A het zinvolle bericht kan verstuurd hebben.

- Als A een geheim en ondertekend bericht naar B wil verzenden, moet hij het bericht eerst versleutelen met de publieke sleutel van B, en daarna met zijn private sleutel. → A zendt $f_A^{-1}(f_B(x)) = z$
  Iedereen (dus ook B) kan dit ontvangen en $f_A(z) = y$ berekenen,
  maar enkel B kan het oospronkelijke bericht $x = f_B^{-1}(y)$ vinden.
  Als x zinvol is, kan enkel A dit verzonden hebben.

  A kan ook $f_B(f_A^{-1}(x)) = z$ berekenen en verzenden. Enkel B kan dan $y = f_B^{-1}(z)$ berekenen en dus ook $f_A(y) = x$ berekenen. Ook nu kan enkel B het oorspronkelijke bericht achterhalen en kan enkel A dit bericht verzonden hebben.

4.2.2 Het RSA-cryptosysteem

Dit cryptosysteem is vernoemd naar zijn drie grondleggers Rivest, Shamir en Adleman. Het in 1977 uitgevonden algoritme was het eerste public-key cryptosysteem en kan zowel gebruikt worden voor gewone encryptie/decryptie, als voor de digitale handtekening.

Het RSA-algoritme

De RSA vercijfering bestaat uit verschillende stappen die vervolgens uitgebreid besproken worden. Elke persoon van het communicatienetwerk moet een sleutelpaar genereren, zoals in stap 1 besproken is voor persoon A.

Stap 1: Sleutelgeneratie

De eerste stap is het genereren van een private en een publieke sleutel door persoon A. Dit gebeurt als volgt:

1. Genereer eerst twee grote, willekeurige priemgetallen p_A en q_A (bv. 512 bits) (zie sectie 2.4.3). Deze dienen van ongeveer dezelfde grootte te zijn.
   - ➔ p_A en q_A zijn geheim
   - ➔ probleem met lage simpliciteit

2. Bereken $n_A = p_A * q_A$
   - ➔ lage simpliciteit

3. Bereken Euler's totiëntfunctie $\Phi(n_A) = (p_A-1)*(q_A-1)$
   - ➔ n_A is publiek
   - ➔ $\Phi(n_A)$ is geheim

4. Selecteer een willekeurig getal e_A (met $1<e_A<\Phi(n_A)$)
   zodat $ggd(e_A, \Phi(n_A)) = 1$
   - ➔ e_A is dus relatief priem met $\Phi(n_A)$
   - ➔ e_A is publiek

5. Aangezien de $ggd(e_A, \Phi(n_A)) = 1$, kan de inverse van e_A (modulo $\Phi(n_A)$) worden berekend met het algoritme van Euclides (zie sectie2.9).

   ➔ **$d_A = e_A^{-1} \bmod \Phi(n_A)$** $\quad (0<d_A<\Phi_A(n))$

   Dan voldoet d_A aan volgende vergelijkingen:

   $$d_A * e_A = 1 \bmod \Phi(n_A)$$

$d_A * e_A = 1 + k * \Phi(n_A) \rightarrow d_A * e_A + k * \Phi(n_A) = 1$ (met k willekeurig)

6. Het sleutelpaar (voor A) is nu gevonden:

Publieke sleutel : n_A en e_A Private sleutel: d_A en $\Phi(n_A)$

Zo kan elke persoon een sleutelpaar genereren.

Stap 2: Trapdoor functie

Stel B wil een bericht x verzenden naar A:

Bericht x (plaintext) moet worden versleuteld tot ciphertext y.

- Encryptieproces door B met de publieke sleutel van A:

$$f_A = x^{e_A} \bmod n_A = y$$

- Decryptieproces door A met de eigen private sleutel

$$f_A^{-1} = y^{d_A} \bmod n_A = x$$

Want:

$$\begin{aligned} f_A^{-1} &= y^{d_A} \bmod n_A = (x^{e_A})^{d_A} \bmod n_A \\ &= x^{e_A d_A} \bmod n_A \\ &= x^{e_A d_A \bmod \Phi(n_A)} \bmod n_A \\ &= x^1 \bmod n_A \\ &= x \bmod n_A \end{aligned}$$

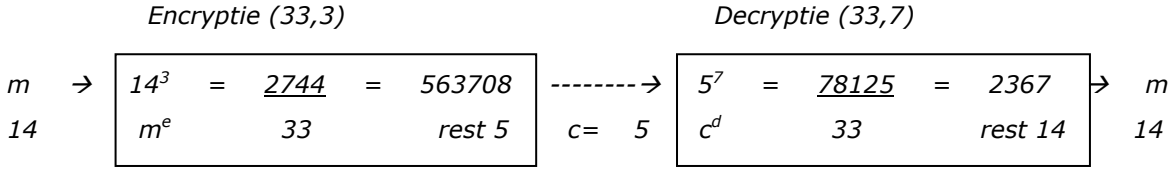
(Stelling van Euler, sectie 2.6)

➔ Lage simpliciteit als d_A gekend is (anders hoge simpliciteit).

➔ Opmerking: als n=p*q, met p en q zeer grote priemgetallen, dan is voor een willekeurige x bijna zeker dat x en n relatief priem zijn, dus de stelling van Euler kan worden toegepast.

Voorbeeld RSA-algoritme

- *kies twee priemgetallen: p=3 en q=11;*
- *bereken n=pq: n =3*11 =33;*
- *bereken $\phi(n) = (p-1)(q-1) = 2*10 = 20$;*
- *kies e, relatief priem is met $\phi(n)$ en kleiner dan $\phi(n)$. Hier is e = 3;*
- *bereken d (<20), waarvoor d*e = 1 mod 20.*
  *d =7, aangezien 7*3=21=1*20+1;*
- *de publieke sleutel is (33,3) en de private sleutel is (33,7);*
- *in onderstaande figuur wordt het encryptie en decryptie proces weergegeven:*



In bovenstaand voorbeeld zijn q en p heel klein. In werkelijkheid moeten zij echter zeer groot zijn (bijvoorbeeld 2^{256}) om de veiligheid van het algoritme te verzekeren. (Stallings, 2000).

De veiligheid van het RSA algoritme

De publieke sleutel is (n, e). Louter op basis van die publieke sleutel kan men de private sleutel d niet berekenen. Als men echter p en q kan achterhalen, kan Φ (n) en dus ook d wel berekend worden. De veiligheid van het RSA algoritme hangt dus af van de moeilijkheid om n te factoriseren. Hoe groter n is, hoe moeilijk het is om p en q te achterhalen (RSA Laboratories, 2008 d). Het probleem van factoriseren is besproken in sectie 2.4.4. Tabel 4.3 toont enkele resultaten van de factorisering van RSA, tot en met 2005.

Tabel 4.3 Evolutie in factorisering van RSA

RSA-algoritme	**Aantal decimale cijfers**	**Datum**	**MIPS-of CPU- jaren**
RSA-155	155	augustus 1999	8000 MIPS-jaren
RSA-160	160	maart 2003	2.7 Pentium 1GHz CPU-jaren
RSA-576	174	december 2003	13.2 Pentium 1GHz CPU-jaren
RSA-200	200	mei 2005	121 Pentium 1GHz CPU-jaren

Met bijvoorbeeld RSA-155 wordt een publieke sleutel n bedoeld van 155 decimale cijfers (512 bits). De uitdaging was deze te factoriseren. Dit is gelukt in 1999. Beide factoren waren getallen van elk 78 cijfers. De uitdaging is om telkens een groter getal te factoriseren.

Tot 1999 spreekt men van MIPS-jaren. Dit is het aantal jaren dat één computer, die een miljoen instructies per seconde verwerkt, nodig heeft voor het factoriseren. Nadien wordt gesproken over Pentium 1GHz CPU-jaren. Dit is het aantal jaren dat een Pentium van 1GHz nodig heeft voor het factoriseren (Factorworld, 2009).

4.2.3 Certificatieautoriteit

Om het asymmetrisch encryptie-algoritme nog veiliger te maken, kan men gebruik maken van een certificatieautoriteit. De publieke sleutel mag in principe beschikbaar zijn voor iedereen, maar er moet nog een veilige manier zijn om ze publiek te maken. Stel, iemand stuurt zijn publieke sleutel naar een ander persoon, hoe kan deze persoon dan weten wie de werkelijke persoon achter die sleutel is. Om zulke misbruiken uit te sluiten, kan men beroep doen op een derde partij, een trusted third party. Zulke partij is bijvoorbeeld een certificatieautoriteit. Deze instelling voorziet openbare sleutels van een certificaat dat bewijst dat een sleutel bij een bepaalde persoon hoort. Al de publieke sleutels worden tevens verzameld in een soort digitaal telefoonboek. Controle van de echtheid van het certificaat zelf is ook mogelijk aan de hand van de openbare sleutel van de certificatie -autoriteit.

Hoofdstuk 5 De digitale handtekening

In dit hoofdstuk gaan we verder in op het gebruik en de werking van de digitale handtekening. Allereerst wordt besproken wat de digitale handtekening juist is, waarna de eigenschappen aan bod komen. Vervolgens wordt de werking besproken en tot slotte gaan we in op de certificatieautoriteit.

5.1 Wat is een digitale handtekening

Een digitale handtekening heeft net zoals een gewone handtekening tot doel het mogelijk te maken voor een persoon om zijn identiteit te verbinden met een document of iets dergelijk. De digitale handtekening is een getal dat afhankelijk is van het bericht en van een private sleutel van de auteur van het bericht. Het is erg belangrijk dat een handtekening verifieerbaar is. Het moet dus achterhaalbaar zijn of de handtekening niet nagemaakt is. Dit kan aan de hand van een derde partij, a trusted third party (Menezes, 1997). Naast deze authenticiteit, kent de digitale handtekening nog drie belangrijke eigenschappen, namelijk het bewaken van de integriteit, de onweerlegbaarheid, en de confidentialiteit. Deze eigenschappen komen aan bod in sectie 5.2.

De digitale handtekening kan geschetst worden binnen het ruimer concept van de elektronische handtekeningen. In Richtlijn 1999/93/EG betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PB.L.13/12, 19/01/2000) wordt volgende definitie gegeven aan een elektronische handtekening: "Elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie"(art.2). Voorbeelden van elektronische handtekeningen zijn de volgende (Van der Hof, 1997):

- digitale handtekening;
- gescande handtekening;
- pincode;
- handtekening met elektronische pen;
- biometrische handtekening, bijvoorbeeld een vingerafdruk.

In de voornoemde richtlijn komt het begrip geavanceerde elektronische handtekening ook aan bod. Hieronder wordt het volgende verstaan:

"Een elektronische handtekening die voldoet aan volgende eisen:

- zij is op unieke wijze aan de ondertekenaar verbonden;
- zij maakt het mogelijk de ondertekenaar te identificeren;

- zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en
- zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord; "

Op basis van deze eigenschappen kan de digitale handtekening gelijk gesteld worden aan de geavanceerde elektronische handtekening.

5.2 Eigenschappen van de digitale handtekening

De digitale handtekening kent vier belangrijke eigenschappen die het tot een waardevol concept maken.

5.2.1 Authenticiteit

Onder authenticatie wordt het verifiëren van een gebruiker, van de afkomst van een bericht verstaan. De digitale handtekening kan zekerheid bieden omtrent de authenticiteit van een bericht, dus vanwaar het bericht afkomstig is.

De authenticatie gebeurt doordat de afzender zijn bericht of de hashwaarde van het bericht versleutelt met zijn geheime sleutel. Wanneer de ontvanger het bericht dan ontsleutelt met de bijhorende publieke sleutel, kan hij er zeker van zijn dat het bericht van die persoon afkomstig is. De identiteit achter deze persoon wordt daarentegen niet verzekerd. Dit is wel het geval indien gebruik gemaakt wordt van een certificatiedienstverlener. Hierop wordt later dieper ingegaan (Kaspersen & Stuurman, 2001).

5.2.2 Integriteit

Met integriteit wordt bedoeld dat een bericht ongewijzigd blijft. Dit kan men verzekeren door het gebruik van een hash functie op het oorspronkelijke bericht. De kleinste wijziging in het bericht levert immers een andere hashwaarde op. Indien de ontvanger dus de hashwaarde herberekent en deze is niet gelijk aan de oorspronkelijke hashwaarde, weet hij dat er iets aan het bericht gewijzigd is (Kaspersen & Stuurman, 2001). Er kan dus niet voorkomen worden dat iemand iets aan het bericht wijzigt, maar de ontvanger zal dit wel weten.

5.2.3 Onweerlegbaarheid

Met onweerlegbaarheid wordt bedoeld dat de afzender van een bericht niet kan ontkennen dat hij het bericht verstuurd heeft. Deze persoon kan dus geen afstand doen van de informatie (Certipost, 2008 a). Dit principe is vergelijkbaar met dit van een aangetekende zending per post.

5.2.4 Confidentialiteit

In principe garandeert de digitale handtekening op zich geen geheimhouding. Omdat dit echter vaak gevraagd is, kan dit voorzien worden via encryptie. Confidentialiteit kan men bereiken door ,bij public-key cryptografie, het bericht te coderen met de publieke sleutel van de ontvanger. De ontvanger op zijn beurt decodeert het bericht dan met zijn eigen private sleutel. Aangezien hij de enige is die deze bijhorende private sleutel kent, kan alleen hij het bericht ontsleutelen (Panko, 2005 a). Het gebruik van public-key cryptografie is echter vaak omslachtig. Het gebruik van DES in combinatie met RSA is hiervoor een alternatief. Dit wordt besproken in sectie 5.3.3.

5.3 Werking van de digitale handtekening

Het algemene principe van de digitale handtekening gaat als volgt:

Stap 1

Om aan een bericht x een digitale handtekening toe te voegen (het bericht te 'ondertekenen'), dient men eerst de hashwaarde van dit bericht te berekenen via een hash functie h. Deze hashfunctie is openbaar. Een ander oorspronkelijk bericht levert een andere hashwaarde op.

→ $h(x) = z$

Stap 2

Vervolgens dient een sleutelpaar gegenereerd te worden, met een private en publieke sleutel, zoals besproken bij het RSA algoritme (sectie 4.2.2.).

De publieke sleutel wordt weergegeven door f_A, f_B, … en de bijhorende private sleutels door f_A^{-1}, f_B^{-1}, ….

Stap 3: encryptie

De hashwaarde wordt dan versleuteld met de private sleutel van persoon A (de afzender). Dit vormt de digitale handtekening (u) en deze wordt dan samen met het al dan niet versleutelde bericht verzonden naar persoon B (de ontvanger). → $f_A^{-1}(z) = u$

Stap 4: decryptie

B kan dan met de publieke sleutel van A nagaan of het bericht werkelijk van A komt en of het onderweg niet gewijzigd is (Van der Hof, 1997). B berekent daarvoor eerst $f_A(u) = z$ en $h(x) = z$.

Als beide aan elkaar gelijk zijn, impliceert dit dat het bericht ongewijzigd is en dat het van A afkomstig is.

Om bovendien transmissiefouten te kunnen opsporen en verbeteren, kan gebruik gemaakt worden van codetheorie. Bijvoorbeeld de Hamming code (H) kan worden toegepast alvorens het bericht verzonden wordt. De manier van creatie van de digitale handtekening is afhankelijk van de gewenste beveiliging. Verschillende soorten beveiliging met de bijhorende werking zullen vervolgens besproken worden.

5.3.1 Bericht moet enkel confidentieel zijn

Om een bericht geheim te houden voor derden komt cryptografie aan bod. Stel A wil een bericht naar B versturen, zonder dat een persoon C dit zou kunnen lezen.

Indien het bericht gewoon confidentieel moet zijn, maar niet 'ultra'-confidentieel, kan men gebruik maken van DES encryptie. Het gevaar van het DES algoritme zit echter in het uitwisselen van de sleutel tussen beide partijen. Om dit op een veilige manier te laten verlopen, kan hiervoor asymmetrische cryptografie gebruikt worden.

Stap 1: A versleutelt het bericht x met het DES algoritme

➔ $DES(x) = y$

en A versleutelt de sleutel om DES^{-1} te berekenen (aangeduid als DES^{-1}) met de publieke sleutel van B, zodat enkel B de sleutel kan achterhalen met zijn private sleutel.

➔ $f_B(DES^{-1}) = D\tilde{E}S$

Stap 3: A zendt [y; DẼS]. Iedereen (dus ook B) kan dit ontvangen.

Stap 4: B ontcijfert DẼS met zijn private sleutel, om zo de DES sleutel te achterhalen.

➔ $f_B^{-1}(D\tilde{E}S) = DES^{-1}$. Enkel B kan dit.

en B kan dan aan de hand van deze sleutel het oorspronkelijke bericht x vinden.

➔ $DES^{-1}(y) = x$

5.3.2 Bericht moet enkel ultraconfidentieel zijn

Als het bericht enkel confidentieel moet zijn, maar deze confidentialiteit is zeer belangrijk, dan kan men gebruik maken van public-key cryptografie. A kan dan met behulp van de publieke sleutel van B, het bericht x coderen.

a) *Algemeen principe* (zie sectie 4.2.1)

De publieke sleutel van A en B zijn respectievelijk f_A en f_B. De bijhorende private sleutels zijn f_A^{-1}en f_B^{-1}.

➔ A berekent f_B (x) = y en verzendt dit.
➔ Enkel B kan berekenen: f_B^{-1} (y) = x en dus het oorspronkelijke bericht achterhalen.

b) *Via het RSA-algoritme* (zie sectie 4.2.2)

Stap 1: A zoekt de publieke sleutel van B op en versleuteld het bericht.

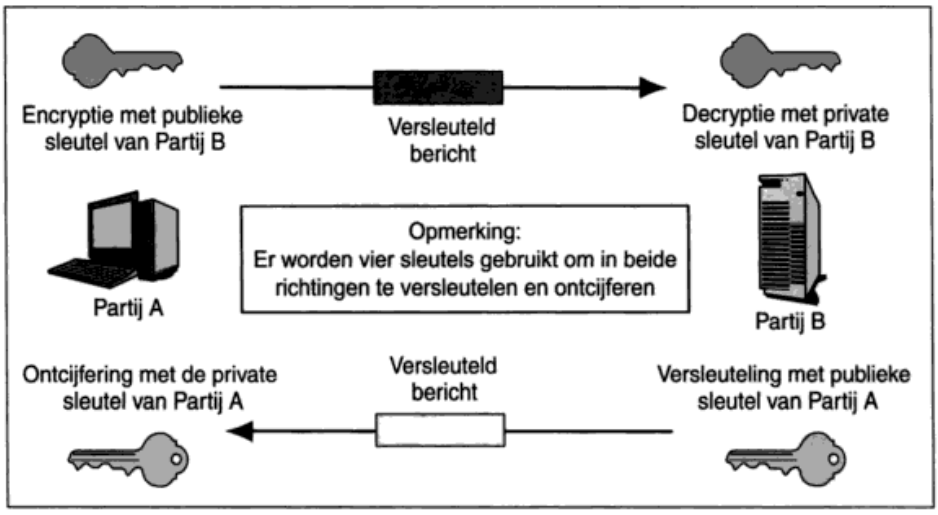
➔ $f_B(x) = x^{e_B} \bmod n_B = y$

Stap 2: A verzendt het gecodeerde bericht y.

Stap 3: B kan aan de hand van zijn private sleutel d_B het originele bericht terug kan achterhalen.

➔ $f_B^{-1}(y) = y^{d_B} \bmod n_B = x$

Enkel B kent de geheime sleutel d_B en kan dus als enige het originele bericht achterhalen. Panko (2005 b) bevestigd dit principe. Figuur 5.1 brengt dit in beeld.



Figuur 5.1 Het gebruik van public-key cryptografie voor het bereiken van confidentialiteit

Bron: Panko, 2005 b (p. 383)

5.3.3 Bericht moet onweerlegbaar zijn

Bij een onweerlegbaar bericht kan de afzender niet ontkennen dat hij het bericht verstuurd heeft. Dit vraagt dezelfde procedure als bij het garanderen van de integriteit. Hiertoe wordt een digitale handtekening aangemaakt. We gaan er van uit dat het bericht niet confidentieel moet zijn.

Stap 1: Om onweerlegbaarheid te kunnen bereiken dient A eerst de hashwaarde van het bericht te berekenen via de hash functie. De hash functie dient botsingsvrij te zijn en is publiek.

➔ $h(x) = z$

(Z heeft een standaard lengte)

Het doel van een botsingsvrije hash functie is dat niemand een y ≠ x kan vinden, waarvoor $h(y) = z$.

Stap 2: Persoon A versleutelt vervolgens de hashwaarde met zijn private sleutel d_A om de digitale handtekening te verkrijgen.

➔ $f_A^{-1}(z) = z^{d_A} \bmod n_A = u$

Deze versleutelde hashwaarde is de digitale handtekening. Enkel A kan deze digitale handtekening berekenen, aangezien enkel hij/zij over de private sleutel beschikt.

Stap 3: Om transmissiefouten te kunnen opsporen, past A nog de hammingcode (H) toe op het oorspronkelijke bericht x en de digitale handtekening u alvorens dit te verzenden.

➔ H [x; u] = [y; v] (langer dan [x; u])

Stap 4: A verzendt [y; v] naar persoon B.

Stap 5: B ontvangt [y; v] + ε (met ε = transmissiefout)

en berekent:

➔ H^{-1} ([y; v] + ε) = [x; u]

➔ $f_A(u) = u^{e_A} \bmod n_A = z$

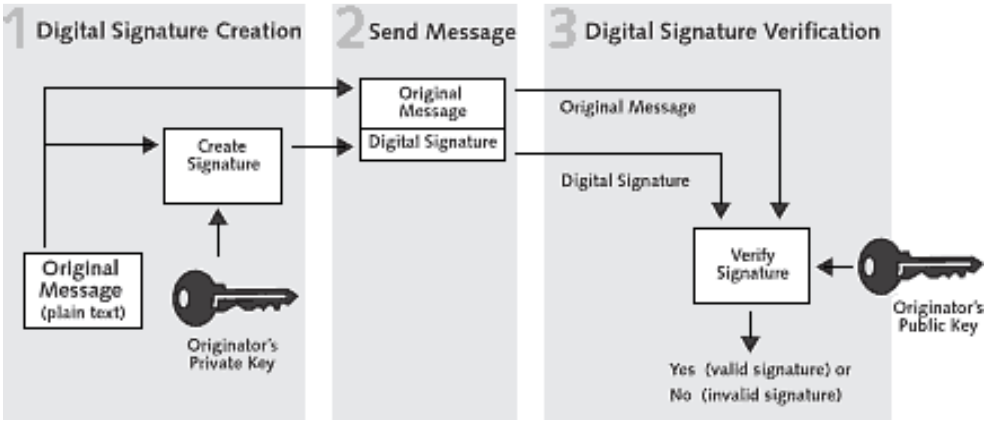
➔ $h(x) = \tilde{z}$

Als $\tilde{z} = z$, dan is het bericht niet gewijzigd en kan het enkel van A komen. De integriteit, authenticiteit en dus ook de onweerlegbaarheid zijn aldus verzekerd.

In principe kan iedereen H^{-1} berekenen en de digitale handtekening ontsleutelen aangezien de publieke sleutel van A bekend is, maar dit is geen probleem aangezien vertrouwelijkheid niet

belangrijk is. Om deze reden moet het bericht zelf niet versleuteld worden. Slechts één persoon kan daarentegen het bericht versleuteld hebben.

Figuur 5.2 geeft de werking van een digitale handtekening weer.



Figuur 5.2 De werking van de digitale handtekening voor het verzekeren van de integriteit en de onweerlegbaarheid van een bericht

Bron: Entrust, 2008

5.3.4 Bericht moet confidentieel en onweerlegbaar zijn

Indien het bericht zowel geheim als onweerlegbaar moet zijn, maar niet ultrageheim, kan het symmetrische encryptie-algoritme DES gebruikt worden. Dit algoritme werd besproken in sectie 4.1.2. Deze sectie is een combinatie van de secties 5.3.1 en 5.3.3. Indien A een bericht naar B wil verzenden, moeten volgende stappen doorlopen worden:

Stap 1: Gebruik de Data Encryption Standard om het bericht te versleutelen en versleutel de DES sleutel met de publieke sleutel van B (asymmetrische cryptografie). Deze stap dient om de betrouwbaarheid te verzekeren.

- ➔ $\mathrm{DES}(x) = \tilde{x}$
- ➔ $f_B\,(\mathrm{DES}^{-1}) = \mathrm{D\tilde{E}S}$

Stap 2: A berekent de hash waarde van het bericht x en versleuteld deze hashwaarde met zijn private sleutel. Deze stap zorgt voor de onweerlegbaarheid en de integriteit.

- ➔ h(x) = z
- ➔ $f_A^{-1}(z) = z^{d_A} \bmod n_A = u$

Dit kan enkel A, aangezien hij/zij als enige over de private sleutel beschikt.

Stap 3: Pas de hammingcode toe op het versleutelde bericht, de versleutelde DES sleutel en de digitale handtekening alvorens te verzenden naar B.

➔ H [$\tilde{X}$; D$\tilde{E}$S; u] = [y; w; v]

Stap 4: B ontvangt [y; w; v] + ε en berekent H^{-1}.

➔ H^{-1} ([y; w; v] + ε) = [$\tilde{X}$; D$\tilde{E}$S; u]

Iedereen kan dat bericht ontvangen en H^{-1} berekenen.

Stap 5: Enkel B kan:

- de DES sleutel achterhalen met zijn private sleutel

➔ f_B^{-1} (D$\tilde{E}$S) = DES^{-1}

- via de DES sleutel het oorspronkelijk bericht achterhalen

➔ DES^{-1} ($\tilde{X}$) = x

Iedereen, en dus ook B kan:

- met de publieke sleutel van A de hashwaarde achterhalen

➔ $f_A(u) = u^{e_A} \bmod n_A = z$

- de hashwaarde van het oorspronkelijke bericht via de hash functie berekenen.

➔ $h(x) = \tilde{z}$

Als $\tilde{z} = z$, dan kan het bericht enkel van persoon A komen en is het ongewijzigd en enkel B kan het oorspronkelijke bericht lezen, hetgeen de vertrouwelijkheid verzekerd.

5.3.5 Bericht moet ultraconfidentieel en onweerlegbaar zijn

In vorige sectie was het voldoende als het bericht behoorlijk confidentieel was. Indien dit niet het geval is, moet asymmetrische cryptografie gebruikt worden in plaats van de symmetrische variant. A wil het bericht $x=[x_1,x_2,\ldots,x_k]$ versturen naar B. (x_i van standaardlengtes, bijvoorbeeld 512 bits).

Persoon A ondergaat volgende stappen:

Stap 1: A versleutelt x (blok per blok) aan de hand van zijn private sleutel

➔ f_A^{-1} (x) = y

➔ $f_A^{-1}(x) = [x_1^{d_A} \bmod n_A \ldots x_k^{d_A} \bmod n_A]$
$= [y_1 \ldots y_K] = y$

Stap 2: Versleutel y (blok per blok) en met de publieke sleutel van B om de vertrouwelijkheid te verzekeren.

➔ $f_B[y] = [y]^{e_B} \bmod n_B = [y_1^{e_B} \bmod n_B \ \ldots \ y_k^{e_B} \bmod n_B \mid u^{e_B} \bmod n_B]$
$= [z_1 \ldots z_k] = z$

Stap 3: Pas de Hamming code toe alvorens z te verzenden.

➔ H [z] = u

Stap 4: Iedereen kan u + ε ontvangen en H^{-1} berekenen.

➔ H^{-1} (u + ε) = z

Stap 5: Enkel B kan:

- z ontcijferen aan de hand van de eigen private sleutel om y te achterhalen;

➔ $f_B^{-1}(z) = [z^{d_B} \bmod n_B] = y$

- met de publieke sleutel van A het oorspronkelijke bericht vinden;

➔ $f_A(y) = y^{e_A} \bmod n_A = x$

Doordat het bericht versleuteld is met de private sleutel van persoon A, is persoon B er zeker van dat het bericht van A afkomstig is. De geheimhouding van het bericht is verzekerd door het versleutelen van y met de publieke sleutel van B. Enkel B kan dit ontsleutelen. Zo zijn de belangrijkste principes gegarandeerd.

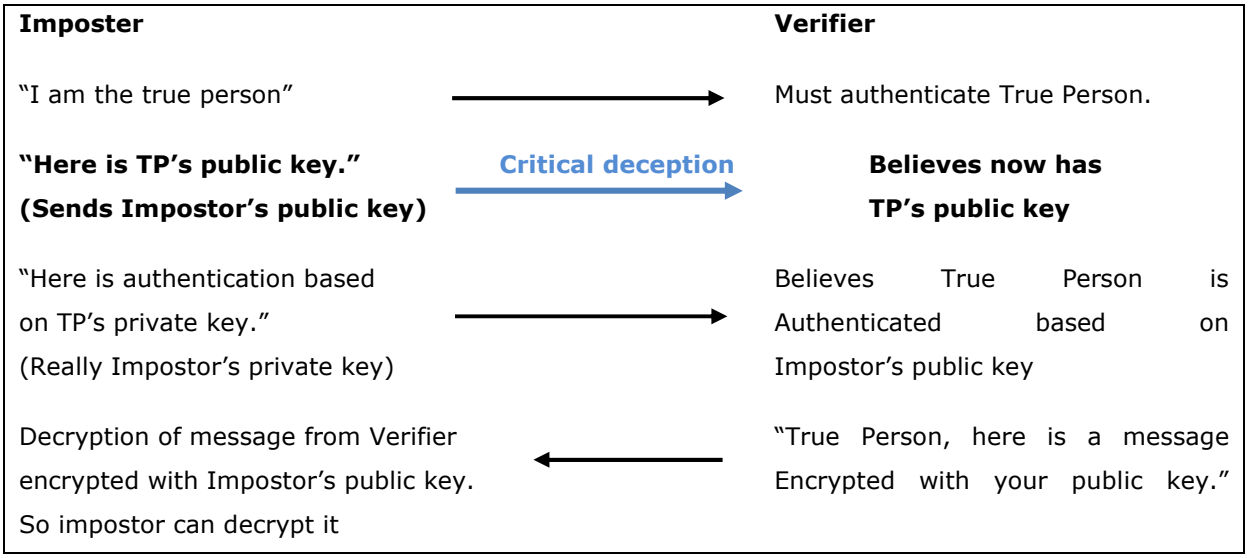
5.3.6 Samenvatting

A wil een bericht verzenden naar B.

Enkel confidentieel	• Bericht versleutelen met DES algoritme • DES sleutel versleutelen met f_B
Enkel ultraconfidentieel	• Bericht versleutelen met f_B
Enkel onweerlegbaar	• Hashwaarde versleutelen met f_A^{-1} → digitale handtekening
Gewoon confidentieel en onweerlegbaar	• Bericht versleutelen met DES algoritme • DES sleutel versleutelen met f_B • Hashwaarde versleutelen met f_A^{-1} → digitale handtekening
Ultraconfidentieel en onweerlegbaar	• Bericht indelen in blokken van standaardlengte • Elke blok versleutelen met achtereenvolgens f_A^{-1} en f_B

5.4 Certificatieautoriteit

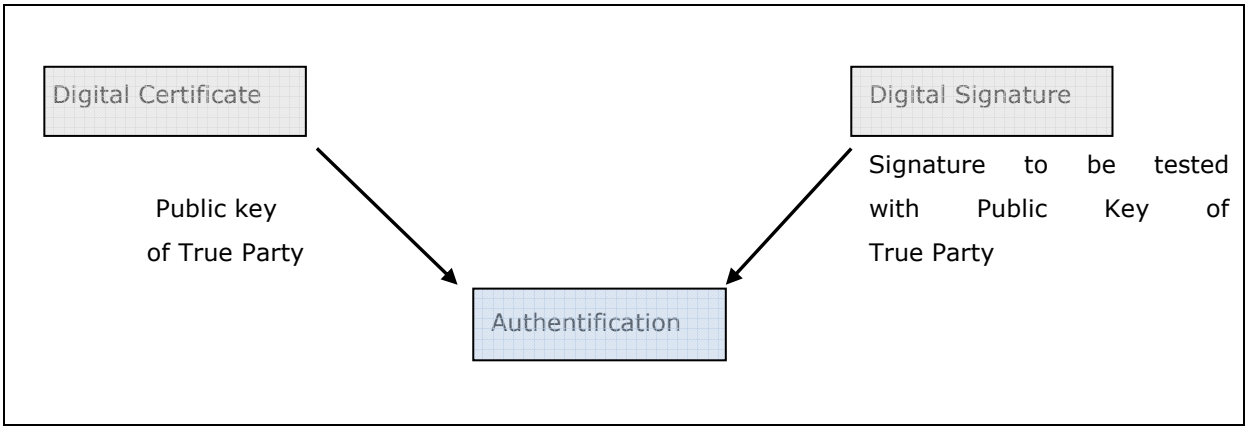
De certificatieautoriteit kwam reeds kort aan bod onder hoofdstuk 4, maar wordt nu uitgebreider besproken. Door gebruik te maken van bovenstaand principe ter verzekering van de authenticiteit, is de ontvanger zeker dat het bericht afkomstig is van de persoon wiens publieke sleutel hij heeft. Wie de werkelijke persoon achter deze publieke sleutel is, kan hij echter niet met zekerheid weten. Daarom wordt gebruik gemaakt van een derde partij. Figuur 5.3 geeft het voornoemde probleem weer.



Figuur 5.3 Probleem van authenticiteit

Bron: Panko, 2005 a(p.542)

De ontvanger moet de publieke sleutel opvragen bij de certificatieautoriteit. Zoals reeds eerder aangehaald, voorziet deze instelling openbare sleutels van een certificaat dat bewijst dat een sleutel bij een bepaalde persoon behoort. Zulk certificaat bevat de publieke sleutel en de naam van diens eigenaar. Aan de hand van de publieke sleutel kan dan de ontvangen digitale handtekening gecontroleerd worden, zoals zichtbaar op figuur 5.4 (Panko, 2005 a).



Figuur 5.4 De rol van digitale certificaten en de digitale handtekening bij de authenticatie van een bericht

Bron: Panko, 2005 a (p. 544)

Er zijn drie soorten certificaten mogelijk:

- Klasse 1 certificaat: Als iemand een certificaat aanvraagt, wordt diens identiteit niet gecontroleerd.
- Klasse 2 certificaat: Hierbij wordt de identiteit wel gecontroleerd, maar van op afstand.
- Klasse 3 certificaat: Hierbij dient de identiteit van de aanvrager vastgesteld te worden door een speciale autoriteit,de registratieautoriteit, om deze 100% te garanderen. Deze certificaten zijn bedoeld voor professionele doeleinden.

Isabel N.V. is een voorbeeld van een certificatieautoriteit. Zij verstrekken enkel niveau 3 certificaten, en is met een 80 000 tal certificaten de grootse verstrekker hiervan in België. Op de certificaten van Isabel is volgende informatie terug te vinden (Isabel, 2008):

- de identiteit van de ondertekenaar en diens publieke sleutel;
- de periode dat het certificaat geldig is;
- het serienummer;
- de identiteit van de certificatieautoriteit en diens de elektronische handtekening.

Een andere certificatieautoriteit is Certipost. Zij leveren zowel certificaten van het hoogste beveiligingsniveau, als van lagere beveiligingsniveaus en dit voor verschillende toepassingen, gaande van het gebruik voor e-mail circulatie tot gebruik voor BTW aangifte. Certipost biedt aan om simpelweg via hun site een certificaat aan te kopen, dat u via e-mail zal toegestuurd worden (Certipost, 2008 b). Het is dus relatief eenvoudig om hiervan gebruik te maken, en maakt het elektronisch verkeer veiliger.

Hoofdstuk 6 Het juridische kader van de digitale handtekening

De digitale handtekening kan slechts gebruikt worden als equivalent van de gewone handtekening indien deze dezelfde wettelijke status heeft. De gewone handtekening wordt immers vaak geëist door de wet en een ondertekend geschrift kan gebruikt worden als bewijsmiddel. Dit mede doordat de handtekening enkele essentiële functies vervult, namelijk bewijs van integriteit en identiteit. Pas als de digitale handtekening hetzelfde statuut krijgt als de gewone handtekening, zal deze kunnen gebruikt worden op belangrijke documenten. Begin 2000 werd dan ook een richtlijn gepubliceerd die dit mogelijk maakt, namelijk de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (*Digitale handtekening: stand van zaken*, 2000). In België is er de wet van 20 oktober 2000, alsook deze van 9 juli 2001 en het koninklijk besluit van 6 december 2002. De geldende wetgevingen spitsen zich meer toe op de elektronische handtekening in het algemeen, maar zoals reeds vermeld is de digitale handtekening hier een onderdeel van. Vervolgens zullen de wetgevingen één voor één aan bod komen.

6.1 Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PB.L.13/12, 19/01/2000)

Deze richtlijn, gepubliceerd in januari 2000, beoogt een eenvoudiger gebruik van de elektronische handtekening en een wettelijk kader hiervoor. In de richtlijn wordt een onderscheid gemaakt tussen de elektronische handtekening en de geavanceerde elektronische handtekening (art.2).

Artikel 2.1

*"**Elektronische handtekening**": elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie.*

Artikel 2.2

*"**Geavanceerde elektronische handtekening**": een elektronische handtekening die voldoet aan de volgende eisen:*

a) Zij is op unieke wijze aan de ondertekenaar verbonden;

b) Zij maakt het mogelijk de ondertekenaar te identificeren;

c) Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en

d) Zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

De digitale handtekening (gebaseerd op asymmetrische cryptografie) is een geavanceerde elektronische handtekening. De eerste eis wordt gerealiseerd door het gebruikt van de private sleutel van de ondertekenaar om de digitale handtekening te maken. Door gebruik te maken van certificaten is de identiteit van de ondertekenaar bekend. De private sleutel van de ondertekenaar is enkel door hemzelf gekend. Op deze manier komt men tegemoet aan de derde eis. Ten slotte zorgt het gebruik van een hash functie voor het bereiken van de laatste eis, namelijk het behoud van de integriteit.

In bijlage van deze richtlijn worden tevens eisen weergegeven voor gekwalificeerde certificaten en de certificatiehouders die zulke certificaten uitgeven.

6.2 De Belgische wetgeving

De Europese richtlijn diende omgezet te worden in een Belgische wetgeving.

- **Wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure (Wet-Bourgeois) (B.S. 22/12/2000)**

  Deze wet beslaat de nodige aanpassingen in het burgerlijk en het gerechtelijk wetboek die betrekking hebben op het gebruik van telecommunicatiemiddelen en de elektronische handtekening. In verband met de elektronische handtekening wijzigt enkel artikel 1322 van het burgerlijk wetboek. Dit artikel behandelt de vereisten voor een handtekening.

- **Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten (B.S. 29/09/2001)**

Deze wet zet de bepalingen uit de Europese richtlijn om in een Belgische wetgeving en is terug te vinden in Bijlage 1. Artikel 4 *§4* geeft de voorwaarden voor een elektronische handtekening waardoor deze op gelijke voet komt met de handgeschreven handtekening. Indien niet voldaan wordt aan al deze voorwaarden, mag dit echter geen reden zijn om de elektronische handtekening als bewijsmiddel te weigeren.

Artikel 4 §4
Onverminderd de artikelen 1323 en volgende van het burgerlijk wetboek wordt een geavanceerde elektronische handtekening, gerealiseerd op basis van een gekwalificeerd certificaat en aangemaakt door een veilig middel voor het aanmaken van een handtekening, geassimileerd met een handgeschreven handtekening, ongeacht of deze handtekening gerealiseerd wordt door een natuurlijke dan wel door een rechtspersoon.

Artikel 4 *§5*
Een elektronische handtekening kan geen rechtsgeldigheid worden ontzegd en niet als bewijsmiddel in gerechtelijke procedures worden geweigerd louter op grond van het feit dat:
- *de handtekening in elektronische vorm is opgesteld, of*
- *niet is gebaseerd op een gekwalificeerd certificaat, of*
- *niet is gebaseerd op een door een geaccrediteerd certificatiedienstverlener afgegeven certificaat, of*
- *zij niet met een veilig middel is aangemaakt.*

Een geavanceerde elektronische handtekening wordt bij wet gelijk gesteld aan de handgeschreven handtekening. Een document dat hiermee ondertekend wordt, heeft aldus dezelfde waarde als een onderhandse akte (Storme, z.d.). Elke vorm van elektronische handtekening daarentegen moet juridisch erkend worden en mag dus niet geweigerd worden, louter om het feit dat het om een elektronisch ondertekend document gaat.

De voorwaarden voor een certificaat om gekwalificeerd te zijn en deze voor een middel tot aanmaken om veilig te zijn, worden uiteengezet in de bijlagen van deze wet.

- **Koninklijk besluit van 6 december 2002 houdende organisatie van de controle en de accreditatie van de certificatiedienstverleners die gekwalificeerde certificaten afleveren (17/01/03)**

  Dit koninklijk besluit heeft betrekking op de accreditatie van de certificatieverleners, BE.SIGN genoemd, en de bijhorende procedures. De wet van 9 juli 2001 schrijft voor dat een certificatiedienstverlener die gekwalificeerde certificaten uitgeeft die aangemaakt zijn aan de hand van veilige middelen, een accreditatie, of schriftelijk bewijs, kunnen aanvragen. De voornoemde voorwaarden moeten wel voldoen aan de gestelde eisen in de bijlagen van de wet van 9 juli 2001. De details hieromtrent vallen echter niet binnen het bereik van deze masterproef.

Hoofdstuk 7 Toepassingen van de digitale handtekening

In dit hoofdstuk komen enkele belangrijke domeinen aan bod waarin de digitale handtekening kan worden gebruikt, namelijk e-commerce, het veilig bewaren van documenten, e-government, elektronisch dataverkeer, e-banking en het gebruik binnen de logistieke sector.

7.1 E-commerce

Electronic commerce, of E-commerce, is een breed begrip dat elke mogelijke vorm van elektronische handel omvat, zowel business-to-business (B2B), business-to-consumer (B2C) als consumer-to-consumer (C2C) (Goddyn, 2001). E-commerce heeft heel wat gevolgen, zowel voor koper als verkoper. Zo wordt de marktplaats vergroot. De koper heeft een grote waaier aan koopmogelijkheden, die plaatsonafhankelijk zijn, terwijl de verkoper zijn afzetgebied kan uitbreiden. E-commerce kan gaan van een eenvoudige elektronische aankoop op e-bay tot het elektronisch afsluiten van belangrijke contracten tussen ondernemingen. Communicatie tussen de partijen kan vaak sneller verlopen via elektronische weg, hetgeen ook een JIT- systeem toelaat voor de verkoper. Het is natuurlijk voor de klant uitermate belangrijk dat de financiële en persoonlijke gegevens veilig behandeld worden. (wikipedia, 2008 c) Hier kan het gebruik van de digitale handtekening het vertrouwen vergroten.

7.2 Elektronisch factureren

Elektronisch factureren is een nieuwe trend die onder andere binnen de e-commerce terug te vinden is. Het vervangen van facturen op papier door elektronische facturen kan de personeelskosten doen dalen en fouten verminderen. Bovendien blijven bedrijven gespaard van kleine administratieve kosten zoals deze van postzegels, enveloppen,… . Natuurlijk dient deze nieuwe trend te worden beschermd tegen frauduleuze praktijken. Dit gebeurt aan de hand van de digitale handtekening, waardoor de integriteit en echtheid verzekerd is.

Sinds 2004 wordt elektronisch factureren in Nederland erkend door de wet op omzetbelasting. Maar dit enkel indien de factuur voorzien is van een geavanceerde elektronische handtekening. De verzender dient geen verzendingskosten meer te betalen en de ontvanger heeft recht op een BTW voordeel. Bovendien kan zo ook de papieren administratie verminderd worden (Jungslager, 2004).

7.3 Archivering van documenten

De opkomst van het internet en daarbij gepaard gaande het gebruik van elektronische documenten zou moeten leiden tot een papierloze administratie. Toch worden de meeste elektronische documenten nog uitgeprint om te ondertekenen of simpelweg om te bewaren. Dit duidt op een nog steeds beperkt vertrouwen betreffende de veiligheid. De integriteit en authenticiteit van de bewaarde gegevens moet immers verzekerd worden. De digitale handtekening kan hier een oplossing bieden.

De archivering van elektronische documenten verloopt dan als volgt: Eerst dient het elektronische document overgedragen te worden aan het archief, waarna het gehashed wordt. De hashwaarde wordt versleuteld met de private sleutel van het archief, waardoor de digitale handtekening wordt bekomen. Zowel het oorspronkelijke document, als de digitale handtekening worden dan elektronisch bewaard in het archief. Wanneer het document terug opgevraagd wordt, wordt de hash waarde opnieuw berekend en de opgeslagen hash waarde wordt gedecodeerd aan de hand van de publieke sleutel van het archief. Indien beide hash waarden aan elkaar gelijk zijn, bewijst dit dat de gegevens nog intact zijn. De digitale handtekening kan echter niet vermijden dat er eventueel iets aan de gegevens veranderd wordt, maar wijst er enkel op indien dit gebeurt. Het is eveneens niet mogelijk om vanuit de digitale handtekening terug de oorspronkelijke tekst af te leiden aangezien de hash functie een meerduidige one-way functie is (Van den Eynde en Dumortier, z.d.).

Tegenargument bij het gebruik van digitale handtekening bij de archivering van elektronische documenten is dat de digitale handtekening een tijdsgebonden concept is. Het is immers gebaseerd is op technologie, hetgeen sterk voor veroudering vatbaar is. Computers worden bovendien steeds krachtiger en kunnen steeds meer algoritmes kraken (Boudrez,2005).

7.4 Het versturen van vertrouwelijke informatie via e-mail

In dit digitale tijdperk wordt briefwisseling grotendeels vervangen door e-mail verkeer, zowel voor persoonlijke als zakelijke correspondentie. Aan het versturen van informatie via e-mail zijn echter risico's verbonden. Zo bestaat er het gevaar dat een derde persoon, een hacker, het bericht onderschept en de inhoud ervan leest of zelfs wijzigt. Bovendien kan men niet zeker zijn dat het bericht werkelijk afkomstig is van de persoon die men verwacht. Dit vormt natuurlijk niet zo een groot probleem bij persoonlijk e-mail verkeer, maar bij het verzenden vertrouwelijke informatie kan dit voor grote problemen en wantrouwen zorgen (Microsoft Corporation, 2009). Afhankelijk van het beveiligingsniveau, kan een andere beveiligingsmethode toegepast worden, zoals omschreven

in hoofdstuk 5. Een e-mail kan elektronische ondertekend worden aan de hand van de elektronische identiteitskaart, die aan bod komt in hoofdstuk 8.

7.5 E-banking

Het elektronisch bankieren kent de laatste jaren een grote opkomst. Zowel particulieren als bedrijven maken er veelvuldig gebruik van. Het is immers erg gemakkelijk in gebruik en toegankelijk voor iedereen die over een pc en een internetverbinding beschikt. Veiligheid is hierbij natuurlijk uitermate belangrijk. De desbetreffende bank dient een veilig systeem te hanteren, maar ook de gebruiker moet omzichtig omspringen met zijn informatie.

Er zijn twee dingen die dienen om de authenticiteit te waarborgen, namelijk de digipass zelf enerzijds, die alleen de gebruiker bezit, en een code anderzijds, die alleen de gebruiker kent. Het is natuurlijk uitermate belangrijk dat de gebruiker zijn persoonlijke code zorgvuldig bewaart, want deze wordt gebruikt om de digitale handtekening te berekenen. De bank op zijn beurt maakt gebruik van een beveiligde server, voorzien van een certificaat. Op dat certificaat staat de naam van de site, het serienummer, de vervaldatum van het certificaat, een kopie van de publieke sleutel van de site en de digitale handtekening van de certificatieautoriteit. De digipass zorgt voor het aanmaken van een persoonlijke en unieke digitale handtekening, die zorgt voor de identificatie van de gebruiker. De handtekening kan gecreëerd worden ter identificatie bij het openen van een e-banking sessie. Daarnaast dient er ook een handtekening aangemaakt te worden ter bevestiging van een transactie (Fortis, 2009).

7.6 Het gebruik van de digitale handtekening in de logistieke sector

Ook binnen de logistieke sector zou de digitale handtekening gebruikt kunnen worden. Elektronische handtekeningen, zoals het plaatsen van een handtekening op een PDA scherm, worden al veelvuldig gebruikt, maar over het gebruik van de digitale handtekening is nog geen informatie voor handen. Er bestaan echter wel enkele mogelijkheden voor het gebruik hiervan. Indien de overheid dit zou aanbieden, zou een logistiek bedrijf bijvoorbeeld de nodige vervoersvergunningen elektronisch kunnen aanvragen en hiervoor gebruik maken van de digitale handtekening. Ook de communicatie met klanten kan beveiligd worden door het gebruik van de digitale handtekening, evenals de communicatie met vrachtvervoerders. Dit kan men doen om eventuele spionage door concurrenten te verhinderen. Hiervoor dient deze communicatie weliswaar elektronisch te verlopen. De digitale handtekening zou ook kunnen worden gebruikt om de

vrachtbrief te ondertekenen. Dit impliceert wel dat de vrachtbrief elektronisch moet zijn, en de vrachtwagens dus over een boordcomputer moeten beschikken.

7.7 E-government

Het digitale tijdperk zet niet enkel consumenten en bedrijven aan tot aanpassingen, maar ook de overheid speelt in op deze trend. Zowel de communicatie tussen overheden onderling als deze met de burgers verloopt steeds meer via elektronische weg. De elektronische identiteitskaart, die kan gebruikt worden om een digitale handtekening te creëren, speelt hier een erg belangrijke rol in. Enkele mogelijke toepassingen van e-government zijn het e-loket van de gemeenten en de elektronische BTW-aangifte. In hoofdstuk 8 wordt e-government meer in detail besproken.

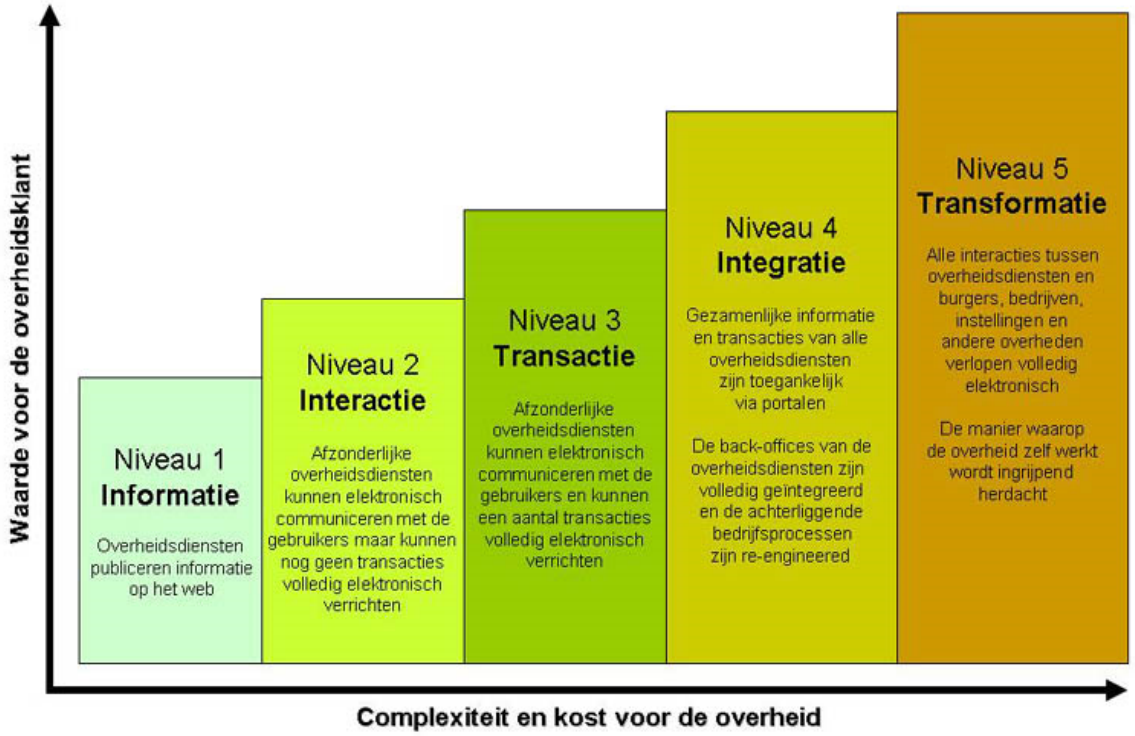
Hoofdstuk 8 E-government

Niet alleen consumenten en bedrijven, maar ook de overheid past zich aan in de digitale leefwereld. E-government of de elektronische overheid kan als volgt gedefinieerd worden: "Het gebruik van (ICT-) technologie om de toegang tot en het verlenen van openbare diensten voor burgers, zakenpartners, leveranciers en ambtenaren te vergemakkelijken."(Velle, 2002) Het heeft dus zowel betrekking op de relatie tussen bestuursorganen onderling, als op de relatie met ondernemingen en burgers.

Er zijn vijf stadia die doorlopen moeten worden om het optimale niveau van e-government te bereiken:

- Dienstverlening via websites;
- Automatische verwijsfuncties: via een centrale poort dient de burger doorverwezen te worden naar de juiste website, zodat hij zelf niet meer op zoek moet gaan;
- Non-stop dienstverlening;
- Administratieve vereenvoudiging: het samenbrengen van de dienstverlening, zowel binnen één overheid als tussen de verschillende overheden.
- Volledige integratie van diensten en proactiviteit: een proactieve administratie waarbij de burger verwittigd wordt indien bijvoorbeeld een termijn verstreken is.

Figuur 8.1 geeft een overzicht van deze 5 gradaties van e-government.



Figuur 8.1 Gradaties van e-government

Bron: CORVE, 2008

Om e-government te realiseren en in te burgeren, moet er natuurlijk zekerheid bestaan omtrent enkele aspecten, waaronder veiligheid, authenticiteit (zowel van de overheidsdienst als van de burger), vertrouwelijkheid en integriteit. De digitale handtekening kan voor deze zekerheid zorgen en is dus onontbeerlijk voor een goed e-government systeem (Van Sebroeck, 2001). De elektronische identiteitskaart, vanaf nu aangeduid als eID, kan gebruikt worden om een digitale handtekening te creëren. De eID is dan ook één van de twee fundamenten van e-government, samen met de federale portaalsite (Vanvelthoven,2003).

8.1 De elektronische identiteitskaart (eID)

De elektronische identiteitskaart of de eID is de opvolger van de gewone identiteitskaart, maar heeft heel wat meer functies. Tegen eind 2009 zou de gehele bevolking voorzien moeten zijn van een eID. België is, samen met Finland en Estland, de koplopers op gebied van de eID ("eID without boundaries", 2008).

De eID kan volgende functies vervullen:

- Bewijs van identiteit, zowel visueel als elektronisch;
- Authenticatie van de eigenaar m.b.v. de digitale handtekening;
- Het genereren van een gekwalificeerde elektronische handtekening m.b.v. de digitale handtekening;
- Het bewijzen van karakteristieken van de eigenaar m.b.v. de digitale handtekening.

Uit de verschillende functies blijkt dat de digitale handtekening een grote en belangrijke rol vervult bij het gebruik van de eID (Robben,z.d.).

Bepaalde gegevens van de kaarteigenaar worden op de kaart gedrukt en zijn dus visueel zichtbaar:

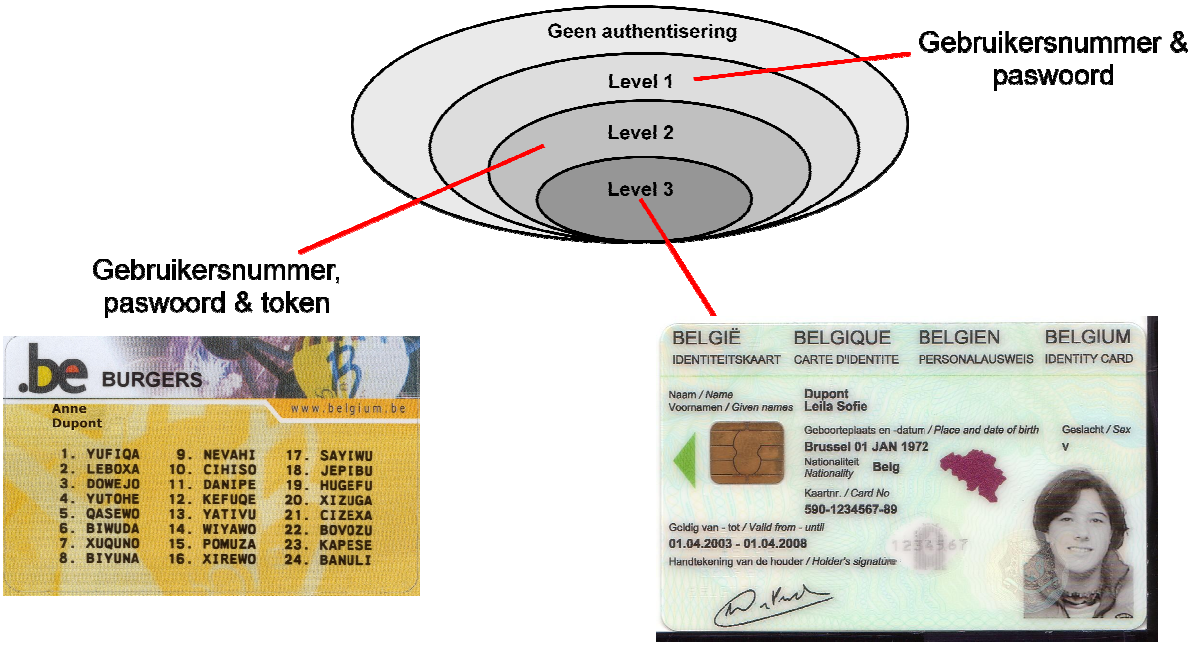
- rijksregisternummer, dat dienst doet als unieke identificatiesleutel;
- kaartnummer;
- identificatiegegevens (naam, geslacht, geboortedatum en –plaats);
- een foto;
- de geldigheidsperiode van de eID.

Dezelfde gegevens zijn ook opgeslagen op de chip van de eID, samen met nog andere gegevens, namelijk:

- het adres van de eigenaar;
- een private sleutel met identiteitscertificaat voor elektronische authenticatie;
- een private sleutel met identiteitscertificaat voor het plaatsten van een elektronische handtekening.

Het is niet mogelijk andere dan voornoemde gegevens op de eID op te slaan. De eID bevat dus twee certificaten, één voor authenticatie en één voor het plaatsen van een handtekening. Het authenticatie certificaat dient gebruikt te worden indien enkel een identiteitsbewijs belangrijk is. Een handtekening op basis van dit certificaat heeft dan ook geen juridische waarde. Dit certificaat wordt voornamelijk gebruikt om aan de hand van de eID toegang te verkrijgen op beveiligde websites.

De private sleutels en bijhorend identiteitscertificaat worden beveiligd met een pincode. Telkens een handtekening dient worden geplaatst, moet de eigenaar zijn pincode ingeven. De gemeenten zorgen voor de toekenning van de identiteitscertificaten (Robben,z.d.). Aangezien de eID, als middel om transacties veilig te laten verlopen, nog niet volledig ingeburgerd is, kan een token aangevraagd worden door degene die gebruik willen maken van bepaalde online diensten. De token is een code die de burger identificeert en toegang geeft tot beveiligde diensten. Figuur 8.2 geeft een overzicht van de mogelijke identificatiecodes die gebruikt kunnen worden bij het elektronisch verkeer.



Figuur 8.2 Een vergelijking van beveiligingsmiddelen

Bron: Robben, 2006

8.1.1 Toepassingen van de eID

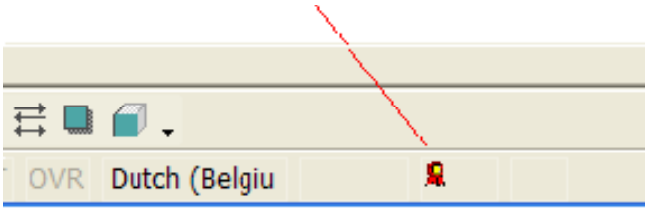
In het ingenieursblad (mei 2008) staat te lezen dat er ruim 300 toepassingen bestaan van de eID, gaande van het online invullen van de belastingsaangifte, tot het zich identificeren op internet. Toch kennen vele toepassingen geen groot succes. Uit een enquête blijkt dat meer dan de helft van de ondervraagden niet weet hoe de eID werkt. Een grootscheepse campagne, georganiseerd door de overheid lijkt dan ook aangewezen. Actie kan best ondernomen worden op korte termijn want er zijn ook andere spelers op de markt van identificatie-instrumenten, waarvan er heel wat zijn die eenvoudiger te gebruiken zijn dan de eID. De overheid heeft op 20 april 2009 een campagne aangekondigd om de eID en bijhorende toepassingen te promoten. Sectie 8.1.2 gaat verder in op dit initiatief. Er zijn twee belangrijke hinderpalen bij het gebruik van de eID. Vertrouwen is een

essentieel begrip aangezien handelingen binnen e-government vaak betrekking hebben op persoonlijke gegevens. Een andere hinderpaal is het feit dat de eID en de bijhorende toepassingen nieuw zijn, waardoor ze ook onbekend zijn en men niet weet hoe er mee te werken ("the use of eID cards in Belgium",2008).

In principe zijn er drie basisgebruiken van de eID, namelijk opslag van data, authenticatie en elektronische handtekening. De opslag van data doet dienst om de gegevens van de persoon op te vragen. Dit gebruik is goed voor 40-50% van al de toepassingen van de eID. Authenticatie, of het bewijzen van de identiteit op bijvoorbeeld een internetsite, staat in voor 40-45%. Dus in slecht 5-10% van de gevallen wordt de eID gebruikt voor de digitale handtekening ("the use of eID cards in Belgium",2008). Verder worden enkele toepassingen van de eID besproken.

Ondertekenen van elektronische documenten

Men kan dus ook documenten ondertekenen aan de hand van de eID, om zo de authenticiteit en integriteit van het bericht te garanderen ("Adobe kiest voor eID", 2005). Hoe men een document kan ondertekenen aan de hand van de eID wordt vervolgens besproken. De procedure is gelijklopend voor Microsoft Word en Excel. Ga naar 'Opties' in het menu 'Extra'. Ga dan naar het tablat 'Beveiliging' en klik op 'Digitale Handtekeningen'. Klik op 'Toevoegen' om een handtekening te plaatsen. Er komt dan een lijst tevoorschijn met beschikbare certificaten, die afkomstig zijn van de eID. De eID bevat zoals reeds aangehaald, twee certificaten. Het 'handtekeningcertificaat' kan gebruikt worden om het document geldig te ondertekenen. De details van het certificaat kunnen bekeken worden door op ''Certificaat weergeven' te klikken. Als u het handtekeningcertificaat gekozen hebt, zal gevraagd worden naar de PIN-code. Deze pin-code is de persoonlijke code die bij uw eID behoort. Indien de correcte pin-code ingegeven wordt, kan de eID de handtekening berekenen. Deze wordt dan aan het document toegevoegd. De handtekening zal niet leesbaar of expliciet zichtbaar zijn, maar maakt deel uit van het document. Wanneer het document verstuurd wordt via bijvoorbeeld e-mail, zal de handtekening aldus automatisch mee verzonden worden. Indien iets gewijzigd wordt aan het document, zal Word om een bevestiging vragen en meedelen dat hierdoor de digitale handtekening verwijderd wordt. De ontvanger dient niet over een eID te beschikken om de handtekening te verifiëren. Indien een document een handtekening bevat, verschijnt er onderaan in Word een pictogram, zoals zichtbaar op figuur 8.3. Om de handtekening te verifiëren, dient men ook naar 'Beveiliging' te gaan (Extra-Opties) en op 'Digitale handtekeningen' te klikken. Er opent dan een venster waarin al de handtekeningen zichtbaar zijn die het document bevat. Om het certificaat te bekijken, moet men klikken op 'Certificaat weergeven'. Men kan dan de persoonlijke gegevens van de ondertekende nakijken, evenals de geldigheid van het certificaat (POD MI, 2008 a).



Figuur 8.3 Icoon dat een digitale handtekening aanduidt in Word

Bron: POD MI, 2008

Scholenwedstrijd eID

Eind 2006 organiseerde de Federale overheidsdienst Binnenlandse zaken een scholenwedstrijd met betrekking tot de eID. Het doel van deze wedstrijd was om studenten te doen nadenken over mogelijke toepassingen van de eID. Er werden uiteindelijk meer dan 200 projecten ingezonden, waaruit 11 laureaten gekozen werden (FOD Binnenlandse Zaken, 2007). Een van de uitkozen projecten is dit van de XIOS Hogeschool Limburg onder leiding van Tristan Fransen, die tijdens een interview het project kort heeft toegelicht. Het project gaat in op mogelijke manieren om de eID te integreren in het leven van de student. Er zijn drie cases uitgewerkt binnen het project, aldus T. Fransen. Een eerste case behandelt de mogelijkheid om, aan de hand van de eID, authenticatie toe te passen bij computersystemen. De tweede case heeft betrekking op het verkrijgen van toegang tot bepaalde ruimten. De laatste case onderzoekt de mogelijkheid om met de eID aanwezigheden op te nemen tijdens examens. Binnen elke case werd onderzocht hoe de toepassing werkt of kan werken. Om na te gaan of één of meerdere van deze toepassingen effectief realiseerbaar zijn, werd contact opgenomen met een beveiligingsbedrijf. Daaruit bleek echter dat het gebruik van de eID niet zo handig is voor dagelijkse toepassingen. De eID moet immers fysisch verbonden worden met de kaartlezer om deze te gebruiken. Door veelvuldig gebruik kan de chip hierdoor beschadigd worden en zal de eID regelmatig vervangen moeten worden, hetgeen kosten met zich mee brengt. Om toegang te verkrijgen tot bepaalde ruimten is bijvoorbeeld de RFID technologie meer geschikt. Geen van de cases zijn dus in praktijk omgezet. De eID wordt binnen de XIOS enkel gebruikt voor de registratie van nieuwe studenten. T. Fransen geeft tevens aan dat er heel wat moeilijkheden opduiken bij het gebruik van de eID, bijvoorbeeld bij e-services zoals Tax-on-web en Intervat. Het is immers niet eenvoudig in gebruik, aangezien er een bijkomend programma moet geïnstalleerd worden dat soms geblokkeerd kan worden door een virusscanner. Bovendien weten heel veel mensen niet hoe met deze toepassingen te werken. Het is vaak veel eenvoudiger om gebruik te maken van certificaten van bijvoorbeeld Isabel of Certipost.

Diverse toepassingen voor burgers

- Inloggen op eBay: Sinds februari 2007 kunnen Belgen die gebruik willen maken van de internetsite eBay, gebruik maken van hun eID om in te loggen. Via deze mogelijkheid kan

het vertrouwen van kopers en verkopers versterkt worden. De Belgische tak van eBay is de eerste die zulke identificatie mogelijk maakt (FOD Binnenlandse Zaken, 2008);
- Cm online: het online dossier van je ziekenkas bekijken;
- Bevolkingsdossier opvragen via de website www.eid.belgium.be;
- My certipost: persoonlijke online brievenbus: ontvangen van loonbrieven, facturen, …;
- My minfin: je persoonlijk fiscaal dossier beheren;
- VEV kinderbijslag: toegang tot kinderbijslag gegevens;
- Saferchat: beveiligd chatten;
- Selor: profiel aanmaken bij het selectiekantoor voor jobs bij de overheid;
- Aanvraag van studiefinanciering bij het departement onderwijs & vorming bij het ministerie van de Vlaamse gemeenschap;
- Aanvraag van een abonnement van De Lijn;
- Vanaf juni 2009: reizen met de nmbs zonder vervoersbewijs. Je kan online een ticket kopen op de website en dit verzenden naar je eID. Bij controle kan de conducteur je eID lezen en hij zal het vervoersbewijs dan op zijn scherm zien verschijnen;
- Toegang tot het containerpark van je gemeente;
- …

Diverse toepassingen voor ondernemingen

- Fysieke toegangscontrole
- Medattest: online bestellen van medische attesten
- DentAdmin en Titanium by flexsoft: tandartspakketten voor volledige eID integratie zodat het aanmaken en up-to-date houden van patiëntenfiches zeer eenvoudig is.
- Leeftijdscontrole, bijvoorbeeld te gebruiken bij sigarettenautomaten
- Webbased contract management: op legale wijze contracten afsluiten over het internet
- Identificatie van hotelgasten
- …

Andere mogelijkheden voor de toekomst

- eID als bibliotheekkaart;
- digitaal prikbord in de keuken waarop staat welke producten nog voorradig zijn in je koelkast en je zo je bestellingen kan doorgeven aan een winkel;
- toegangscontrole op school, in bijvoorbeeld labo's;
- eID vervangt badges op werk;
- stemmen vanachter je computer;
- Als het treinticket op de eID succesvol blijkt, kan op termijn ook het treinabonnement op de eID gezet worden; (msn, 2009)

- In de loop van 2010 zouden de eerste elektronische maaltijdcheques verdeeld moeten worden. Deze maken de huidige papieren variant overbodig. Eén mogelijkheid is dat dit gebeurd via de eID (*Groen licht voor elektronische maaltijdcheques,* 2009).

(eID startpagina, 2009)

8.1.2 "In 1-2-3 met de eID"

De eID kent heel wat nuttige toepassingen, maar wordt tot nu weinig gebruikt. Om hierin verandering te brengen, heeft de overheid een actie op poten gezet, "In 1-2-3 met de eID". De website www.welcome-to-e-belgium.be dient als eerste informatiepunt voor de burgers. Hierop kan men wat meer informatie vinden over de functies van de eID. Er is ook een wedstrijd georganiseerd, waarbij iedereen een mogelijke toepassing kan inzenden. Naast de website, kunnen de burgers ook terecht in de eID bus, die het land doorkruist tussen april en september. De bezoekers leren hier meer over huidige en toekomstige toepassingen van de eID. Bovendien krijgt iedereen een infopakket en een gratis kaartlezer. Een derde manier waarop men de burgers tracht te bereiken, is via Living Tomorrow. Hier kan je een dag vol eID toepassingen beleven in 'Welcome to e-Belgium' (In 1-2-3 met je eID, 2009).

8.2 De federale portaalsite

In 2002 werd in het kader van e-government de federale portaalsite www.belgium.be opgericht. Deze site vormt een poort naar de verschillende overheidsdiensten en bevat veel informatie op uiteenlopende gebieden voor de burgers. In eerste instantie was de site slechts een statisch gegeven, waarop enkel informatie terug te vinden was. Nu heeft deze website eerder een dynamisch karakter. De portaalsite geldt ook als e-loket. In 2008 werd de portaalsite volledig vernieuwd en is nu erg toegankelijk en gebruiksvriendelijk. De startpagina bevat de verschillende overheidsdomeinen, zoals mobiliteit, economie en belastingen. Hierdoor is het erg eenvoudig snel te navigeren naar de nodige informatie.

8.3 Realisaties binnen E-government

Eén van de belangrijkste realisaties binnen e-government is deze op vlak van sociale zekerheid. Hiernaast is ook de online belastingsaangifte en BTW aangifte bijzonder populair. Ook de communicatie tussen overheidsdiensten onderling wordt besproken. Tenslotte komt het e-loket aan bod, dat zijn opmars kent binnen de steden en gemeenten.

8.3.1 Kruispuntbank van de sociale Zekerheid

De kruispuntbank vormt de kern van de e-government activiteiten binnen de sociale zekerheid. In 2008 werd één van de initiatieven van de kruispuntbank zelfs bekroond met een e-government award. De kruispuntbank zorgt voor een coördinatie tussen de verschillende diensten van de sociale sector om snel en veilig gegevens uit te wisselen.

Er is ook een geïntegreerd portaal opgericht waar de gebruiker toegang heeft tot al de diensten van de sociale zekerheid, namelijk www.socialsecurity.be. Dit portaal is bedoeld voor zowel de gewone burgers, als sociale secretariaten, werknemers, ondernemingen,…. De aangeboden diensten worden opgesplitst in deze voor werkgevers, voor sociaal verzekerden en voor professionals (bijvoorbeeld OCMW's) en zijn beschikbaar via de portaalsite. Er zijn verschillende veiligheidsniveaus voorzien:

- niveau 0: iedereen heeft toegang. Bijvoorbeeld simulatie van het pensioen voor verzekerden;
- niveau 1: gebruikersnaam + paswoord nodig. Bijvoorbeeld aangifte RSZ voor werkgevers;
- niveau 2: gebruikersnaam, paswoord, private sleutel en gekwalificeerd certificaat nodig. Bijvoorbeeld wijziging van de aangifte van RSZ;
- niveau 3: enkel met eID toegankelijk. Bijvoorbeeld raadpleging door de veiligheidsconsulenten van de security logs.

Sommige diensten op niveau 1 en 2 zijn natuurlijk ook toegankelijk met de eID, maar dit is niet noodzakelijk.

Om de uitwisseling van gegevens tussen burgers en diensten van de sociale zekerheid vlot te laten verlopen, beschikt elke persoon over een uniek identificatienummer voor de sociale zekerheid, zijnde het rijksregisternummer. Dat rijksregisternummer is zowel op de eID als op de SIS-kaart terug te vinden. Ook ondernemingen beschikken over een uniek nummer, namelijk het ondernemingsnummer dat toegekend wordt door de kruispuntbank voor ondernemingen. Zodra alle burgers beschikken over een eID, en alle sociale instanties zijn aangesloten bij de kruispuntbank, kan de SIS-kaart afgeschaft worden aangezien de eID dezelfde identificatiefunctie vervult als de SIS-kaart (Kruispuntbank van de sociale zekerheid, 2008 b).

8.3.2 Tax-on-web

Tax-on-web is de online dienst voor de aangifte van de personenbelasting en bestaat reeds sedert 2003. In de beginfase was de dienst enkel beschikbaar voor degene die alleen deel 1 van de aangifte moesten invullen, voornamelijk werknemers en gepensioneerden. Nu is de dienst echter beschikbaar voor bijna iedereen. Het voordeel van deze dienst is dat het erg eenvoudig en veilig is en je krijgt bovendien onmiddellijk een eerste schatting van de te betalen belastingen. De eenvoudigste manier om hier gebruik van te maken, is indien de burger in het bezit is van een eID.

Hiernaast dient hij ook te beschikken over een kaartlezer. Heel wat nieuwe laptops beschikken reeds over een ingebouwde kaartlezer. Via de pincode, bijhorend bij de eID, kan hij dan toegang krijgen tot de aangifte. Indien de burger nog geen eID in zijn bezit heeft, of geen kaartlezer om deze te lezen, kan hij een token aanvragen. Een token is een lijst met persoonlijke codes. U logt in met een gekozen gebruikersnaam en paswoord waarna er gevraagd zal worden één van de codes op uw token in te geven. Het is ook mogelijk voor een belastingplichtige om volmacht te verlenen aan bijvoorbeeld een boekhouder, die dan de aangifte online kan verrichten in naam van de burger (Tax-on-web, 2008). Lode Blokken, boekhouder bij D&D consulting, bevestigt dit. Hij geeft aan dat ook heel wat particulieren beroep doen op hem om de belastingsaangifte te doen. Hiernaast benadrukt hij dat de overschakeling naar het elektronisch invullen van belastingsaangiften heel wat tijd- en kostenbesparingen oplevert in vergelijking met het handmatig invullen, aangezien er heel wat minder administratief werk bij te pas komt.

In figuur 8.4 worden de stappen weergegeven die men moet doorlopen om zijn/haar belastingsaangifte te doen.

Figuur 8.4 Stappen bij de aangifte van de personenbelasting

Bron: Tax-on-web.be, z.d.

Stap drie zal weliswaar enkel doorlopen moeten worden indien deze toepasbaar is op de burger.

In 2008 hebben meer dan 1.5 miljoen mensen hun belastingsaangifte gedaan via Tax-on-web, waarvan 95% zegt dat hij het volgend jaar opnieuw zou doen. Dat betekent een stijging 26% ten opzichte van 2007. Dit illustreert de stijgende populariteit van deze online dienst, die voornamelijk te danken is aan het eenvoudig gebruik (De Tijd, 2008). Mr. Blokken geeft aan dat al heel wat gegevens reeds automatisch ingevuld staan bij het elektronisch invullen van de belastingsaangifte, dit omwille van de informatieplicht die de burger heeft ten opzichte van de overheid. Zo is het merendeel dat betrekking heeft op inkomsten, uitkeringspremies, pensioensparen,… al ingevuld.

8.3.3 Intervat

Intervat is de online dienst van de federale overheid waar een onderneming zijn periodieke BTW-aangifte kan doen. De identificatie gebeurt aan de hand van een digitale handtekening gekoppeld aan de eID of een digitaal certificaat niveau 3, verkregen bij Globalsign, Isabel of Certipost. Ondertussen is Intervat ook uitgebreid tot het indienen van klantenlistings en trimesteriële intracommunautaire opgaven (FOD financiën, 2009 a). Volgens Mr. Blokken is het vanaf 1 april 2009 verplicht om de BTW aangifte elektronisch in te vullen.

8.3.4 Vensoc

Vensoc is een online dienst van de overheid om de vennootschapbelasting in te vullen. Deze dienst is beschikbaar sinds 2005. Ook hier is registratie vereist aan de hand de eID of een klasse 3 digitaal certificaat. Daarnaast moet de persoon die de belastingaangifte invult in het bezit zijn van een machtiging wegens de onderneming. Er dienen twee stappen doorlopen worden om de aangifte succesvol af te ronden (FOD financiën, 2009 b):

- Het downloaden van de elektronische aangifte en bijlagen. Dit bestand kan opgeslagen worden op de computer om het nadien in te vullen;
- Wanneer het bestand volledig ingevuld is, kan het via Vensoc naar de belastingsadministratie verstuurd worden. Het is eerst noodzakelijk om je te identificeren alvorens je de aangifte kan versturen, waarna een ontvangstbewijs bekomen wordt.

8.3.5 E-loket

De portaalsite van de overheid vormt voor de burgers een eenvoudige weg naar verschillende diensten. Maar e-government moet zich zelfs tot op de laagste administratieve niveaus ontplooien. Hiermee wordt e-government binnen gemeenten en steden bedoeld. Indien elektronisch een geboorteaangifte gedaan wordt bij de gemeente, moet dit automatisch doorgegeven worden aan de dienst van kinderbijslag. Een gemeente kan elektronische diensten aanbieden via het zogenaamde e-loket. Hier kan de burger zowel terecht om formulieren op te vragen als om ze weer in te dienen. Vandaag de dag is het e-loket echter nog niet overal even goed ontwikkeld. De stad Leuven is één van de koplopers op gebied van e-government. Enkele mogelijke online diensten zijn (Leuven, 2008):

- Aanvraag geboorteakte;
- Aanvraag huwelijksakte;
- Aanvraag getuigschrift van woonst;
- Aangifte vertrek buitenland.

Het is voor de hand liggend dat het gebruik van het e-loket talrijke voordelen biedt voor de burger. Zo zijn lange wachttijden in gemeentehuis overbodig. Het e-loket is tevens 24u op 24 beschikbaar, 7dagen op 7.

De gemeente Diepenbeek was één van de eerste gemeenten die het e-loket toegankelijk maakte voor de burgers volgens Ronny Nelissen, dienstverantwoordelijke secretariaat van de gemeente Diepenbeek. In Juli 2004 werd het elektronisch loket, I-loket genaamd, online beschikbaar en vanaf maart 2005 kunnen bewoners hierop inloggen via hun eID. Het I-loket van de gemeente Diepenbeek staat bekend om zijn gebruiksvriendelijkheid en werd bekroond door Microsoft met een e-Gov Award voor 'het e-ID project van het jaar' (FOD Binnenlandse Zaken, 2006). Desondanks wordt er slechts zelden gebruik gemaakt van het e-loket om documenten aan te vragen of dergelijk, aldus R. Nelissen. Er is echter ook geen grote campagne gevoerd om het gebruik te promoten. Het gebruik is zowel voor de burger enerzijds als voor de ambtenaar anderzijds heel eenvoudig en kan erg tijdsbesparend zijn. Een nadeel is dat, bij het elektronisch aanvragen van een document, het document ook elektronisch verstuurd wordt en dus elektronisch ondertekend. Bij het afprinten van dat document zal het dus geen handtekening bevatten, hetgeen soms nog noodzakelijk is.

Wanneer een aanvraag via het e-loket wordt gedaan, vergt dit heel wat minder tijd voor de gemeenteadministratie om deze aanvraag te verwerken. Een aanvraag van het document 'attest samenstelling gezin' die via het e-loket gebeurt, vergt ongeveer 2 à 3 minuten verwerkingstijd, terwijl dit bij een aanvraag via de balie ongeveer 5 minuten in beslag neemt. Wetende dat er naar schatting ongeveer 300 dergelijke aanvragen (via eender welke weg) gebeuren, kan dit een besparing van 600 tot 900 minuten per maand opleveren. Uitgaand van een werkdag van 8 uur (480 minuten) en een gemiddelde besparing van 750 minuten, levert dit ongeveer 1,5 dag minder werk op per maand, enkel met betrekking tot de aanvragen van attesten en formulieren. De kost van een administratieve werknemers bedraagt 18.28 euro per uur, hetgeen dus een kostenbesparing van 228.5 euro oplevert. Hierbij wordt weliswaar uitgegaan van het feit dat er minder uren betaald dienen te worden, wat in realiteit niet zal kloppen, tenzij een personeelslid half time kan gaan werken door de besparing.

Vanaf 20 april 2009 reikt de gemeente Diepenbeek ook de elektronische identiteitskaarten voor kinderen jonger dan 12 jaar uit, de kids-ID-kaart genoemd. Deze identiteitskaart is niet verplicht en wordt enkel aangemaakt op aanvraag personen die het ouderlijk gezag uitoefenen over het kind. De kaart heeft dezelfde kenmerken als de gewone eID, maar bevat geen handtekeningcertificaat aangezien kinderen niet rechtgeldig kunnen tekenen (Diepenbeek, 2009).

Niet alleen de gemeenten en steden maken gebruik van een e-loket. Ook sociale instanties kunnen met dit principe hun klanten bereiken. Zo heeft de christelijke mutualiteit op zijn website een 'self-

service'. Hier kan men documenten opvragen, uitgaven berekenen, maar ook zijn persoonlijk dossier beheren. Voor dit laatste dient men zich aan te melden met de elektronische identiteitskaart of met een token. Dit is hetzelfde principe als bij het e-loket (cm, 2009).

Ook de politie beschikt sinds januari 2007 over een e-loket, Police-on-web genoemd. Mogelijke aangiften zijn deze van winkeldiefstal, fietsdiefstal en vandalisme. Wanneer er gewonden zijn, geweld gebruikt werd of bedreigingen geuit werden, is het gebruik van het e-loket weliswaar niet geschikt. Er zijn drie mogelijke manieren om zich te identificeren op Police-on-web, via de eID, aan de hand van een token of door het aanmaken van een account op het federaal portaal. Police-on-web is bereikbaar via de website www.lokalepolitie.be (FOD Binnenlandse Zaken, 2007).

8.3.6 Communicatie tussen overheidsdiensten onderling

Zoals reeds gezegd bestrijkt e-government niet enkel de elektronische communicatie tussen overheden en burgers, maar ook tussen overheidsdiensten onderling. Zo kondigde de POD MI (Programmatorische Federale Overheidsdienst Maatschappelijke Integratie, Armoedebestrijding, Sociale Economie en Grootstedenbeleid) begin 2008 aan dat vanaf 1 juni 2008 alle communicatie met de OCMW's elektronisch zou verlopen. Vanaf 1 januari 2009 is het zelfs niet meer mogelijk om de POD MI via de klassieke post te bereiken om de administratieve vereenvoudiging te bevorderen. De voordelen hiervan zijn een verhoging van de uitwisselingssnelheid evenals een verlaging van de werkdruk en de financiële kosten met betrekking tot verzending. Om de integriteit en authenticiteit te waarborgen, zal de communicatie gebeuren met de digitale handtekening, aan de hand van de eID. De handtekening zal weliswaar enkel gebruikt worden voor officiële documenten die anders ook een handgeschreven handtekening vereisten. Gewoon e-mail verkeer zal niet gepaard gaan met een handtekening (POD MI, 2008 b).

Hoofdstuk 9 Enquête over de elektronische identiteitskaart en het e-loket

Aangezien de toepassing e-government heel wat aandacht krijgt in deze masterproef, zal dit het onderwerp uitmaken van een enquête.

9.1 Doel van de enquête

De enquête handelt niet over e-government in het algemeen maar over een bepaalde toepassing, namelijk het elektronisch loket van de gemeenten. De afname zal gebeuren binnen één bepaalde gemeente, daar niet alle gemeenten een even geavanceerd e-loket hebben. De keuze is uitgegaan naar de gemeente Diepenbeek aangezien zij de eerste gemeente in België was die over een e-loket beschikte. De enquête heeft tot doel een algemeen beeld te scheppen van de kennis over en het gebruik van het e-loket. Hiernaast peilt de enquête ook naar het gebruik van de elektronische identiteitskaart, aangezien deze gebruikt kan worden om toegang te verkrijgen tot het e-loket. Het onderzoek is om die reden op beperkte schaal gevoerd, dit omwille van praktische beperkingen. Het is de bedoeling dat de resultaten een aanzet kunnen zijn tot verder en ruimer onderzoek en niet om statistisch representatieve resultaten te bekomen.

Binnen de enquête worden volgende ideeën getoetst:

- Zijn de burgers voldoende ingelicht over de werking en het gebruik van de eID, en maken ze bovendien daadwerkelijk gebruik van de extra functies.
- Weten de burgers welke verrichtingen ze met het e-loket kunnen doen en maken ze hier gebruik van?
- Is er voldoende informatie voorhanden omtrent de eID en het e-loket?

De enquête wordt via drie wegen verspreid:

- Via een e-mail, waarin een link staat naar de online vragenlijst;
- Via een brief, waarin een link staat naar de online vragenlijst.
- Via mondelinge ondervraging.

De online enquête werd aangemaakt met behulp van de internetsite www.studentenenquete.nl en is terug te vinden in bijlage 2.

Omdat we slechts een klein aantal personen mondeling ondervragen en de grote meerderheid via brief of e-mail bereikt wordt, is de kans op een hoge non-respons reëel. Om hierop in te spelen zijn er in totaal ongeveer 40 enquêtes verspreid via e-mail, 90 enquêtes via een brief en 25 mondeling

afgenomen om zo toch een minimum van 40 valide enquêtes te verkrijgen. Uiteindelijk zijn er 49 valide enquêtes verkregen.

9.2 Het opstellen van de vragenlijst

De opstelling van de enquête gebeurde aan de hand van de te toetsen ideeën die in vorige sectie aan bod kwamen. Bij ieder idee werden enkele meerkeuzevragen geformuleerd. Bovendien werden enkele inleidende, persoonlijke vragen gesteld om de burgers onder te verdelen in verschillende doelgroepen. De criteria zijn hier leeftijd, geslacht en opleidingsniveau.

9.3 Verwerking van de gegevens

De gegevens worden verwerkt met zowel SPSS als Excel. Bijlage 3 bevat de dataset. De vragen zullen één voor één geanalyseerd worden, om zo de nodige conclusies te kunnen trekken. Er is slechts beperkt gebruik gemaakt van de persoonlijke informatie van de respondenten om de gegevens te groeperen, aangezien de kleine steekproef statistisch representatieve resultaten niet toelaat.

Om een idee te hebben van de statistische waarde van het onderzoek, kunnen we kijken naar de standaardafwijking die kan weergegeven worden door volgende formule:

$$\sigma_p = \sqrt{\frac{p(1-p)}{n}}$$ (Keller & Warrack, 2003)

Met p de proportie: $p \in [0,1]$ en n de steekproefgrootte.

- ➔ p(1-p) bedraagt maximaal ¼.
- ➔ Dus $\sigma_p < \frac{1}{2}\sqrt{\frac{1}{n}}$

Als n = 49 → $\sigma_p < 1/14 \cong 7\%$

Het betrouwbaarheidsinterval bedraagt dan $\pm$ 2 σ_p, dus $\pm$ 14%. Dit is mogelijk voor een verkennend onderzoek.

Indien echter n=7 (zoals dit bij enkele vragen in de enquête is), dan $\sigma_p < 19\%$

Het betrouwbaarheidsinterval is hier ± 38%. De steekproef is hier dus te klein om enige conclusies te kunnen trekken.

Om bijvoorbeeld een standaardafwijking van 1% te bekomen, zou de steekproef 2500 respondenten moeten omvatten.

9.4 Resultaten

In deze sectie zullen de resultaten besproken worden. Eerst zal de ondervraagde populatie geschetst worden. Een volgend punt handelt over de bevindingen met betrekking tot de eID. Hierna komen de bevindingen over het e-loket aan bod.

9.4.1 Persoonlijke gegevens van de respondenten

De respondenten dienden allereerst hun geslacht aan te duiden. De verspreide enquêtes zijn gelijkmatig verdeeld tussen mannen en vrouwen. De verkregen respons is echter ongelijkmatig verdeeld. Uit tabel 9.1 blijkt dat het grootste deel van de respondenten vrouwelijk is, namelijk 65%. In dezelfde tabel is bovendien de verdeling van de respondenten naar leeftijd en opleiding af te lezen.

We hebben gekozen voor 5 leeftijdscategorieën, met de nadruk op de personen jonger 45 jaar, aangezien deze leeftijdsgroep met de grootste waarschijnlijkheid over internet beschikt. De grootste groep respondenten bevindt zich in de leeftijdscategorie 40-45 jaar (27%) , gevolgd door de personen jonger dan 25 jaar (22%). De groep van personen ouder dan 45 jaar is het minst vertegenwoordigd, met 6% van de respondenten.

Uit de tabel blijkt dat bijna de helft van de respondenten secundair onderwijs als hoogst behaald diploma heeft (49%). De categorie ‘lager onderwijs’ is niet terug te vinden op deze grafiek, aangezien dit door geen enkele respondent geantwoord is. Binnen het hoger onderwijs zijn de menswetenschappen het best vertegenwoordigd (24%).

Tabel 9.1 Persoonlijke gegevens respondenten

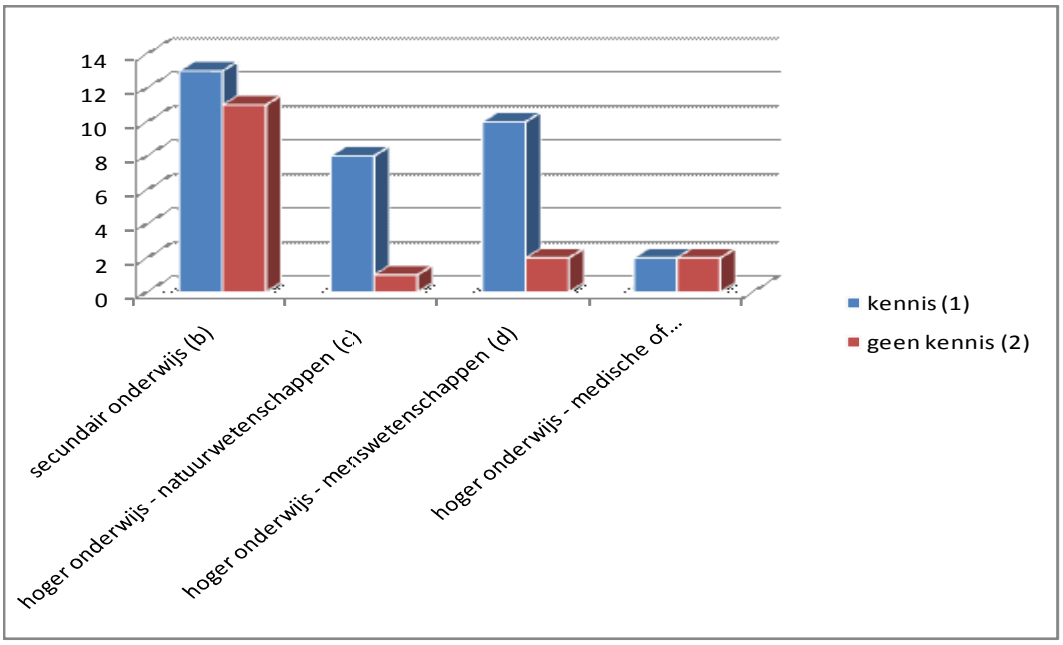
Geslacht		Leeftijd		Opleiding	
	%		%		%
mannelijk	65%	< 25 jaar	22%	secundair onderwijs	49%
vrouwelijk	35%	25-29 jaar	12%	hoger onderwijs -natuurwetenschappen	18%
		30-34 jaar	18%	hoger onderwijs - menswetenschappen	25%
		35-39 jaar	14%	hoger onderwijs - medische of	8%
		40-45 jaar	27%	paramedische wetenschappen	
		> 45 jaar	6%		

9.4.2 De elektronische identiteitskaart (eID)

Volgens R. Nelissen van de gemeente Diepenbeek beschikt reeds 90% van de bevolking over een elektronische identiteitskaart. Binnen de enquête beschikte 94% van de respondenten over een eID. Dit percentage sluit ongeveer aan bij het percentage, meegedeeld door R. Nelissen. De kleine afwijking is te verklaren door de beperkte schaal waarop de enquête gevoerd is.

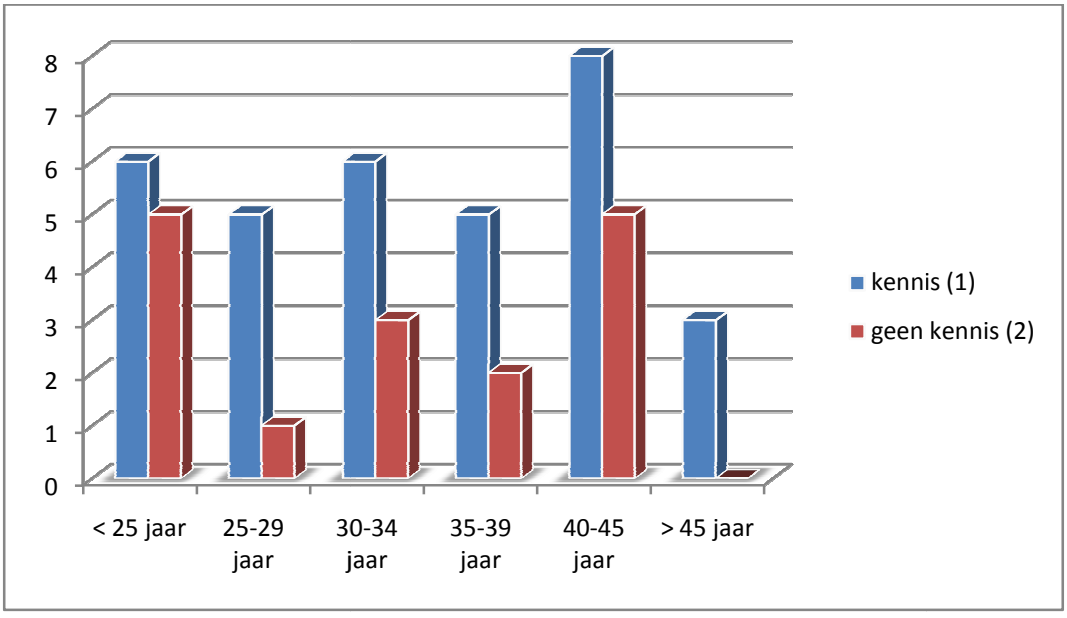
De vijfde en zesde vraag van de enquête peilen naar de kennis die de respondenten hebben over mogelijke functies van de eID. 67% van de respondenten heeft weet van het feit dat de eID nog andere functies heeft buiten het bewijs van identiteit.

Wanneer hierbinnen een onderscheid gemaakt wordt naar geslacht, zien we geen opmerkelijk verschil tussen mannen en vrouwen. Bij het maken van een onderscheid naar opleiding zien we wel een klein verschil, zoals zichtbaar op figuur 9.1. Opvallend is dat bij respondenten met het secundair diploma als hoogste opleiding, ongeveer de helft weet dat de eID nog andere functies heeft, de andere helft weet dit niet. Bij de hogere geschoolde respondenten is het aandeel van de respondenten die weet hebben van de functies van de eID opmerkelijk groter. De laatste categorie, hoger onderwijs – medische en paramedische wetenschappen, is hier een uitzondering op. Deze categorie bevat echter slechts 4 respondenten, waardoor het moeilijk is conclusies te trekken.



Figuur 9.1 Kennis functies eID ingedeeld volgens opleiding (n=49)

Met betrekking tot de leeftijd kan vastgesteld worden dat enkel bij de jongste respondenten (<25 jaar), het aandeel respondenten dat kennis heeft over de functies van de eID ongeveer even groot is dan het aandeel respondenten dat er geen kennis van heeft, zoals zichtbaar op figuur 9.2. In de andere categorieën heeft een duidelijke meerderheid kennis van de functies.



Figuur 9.2 Kennis functies eID ingedeeld volgens leeftijd (n=49)

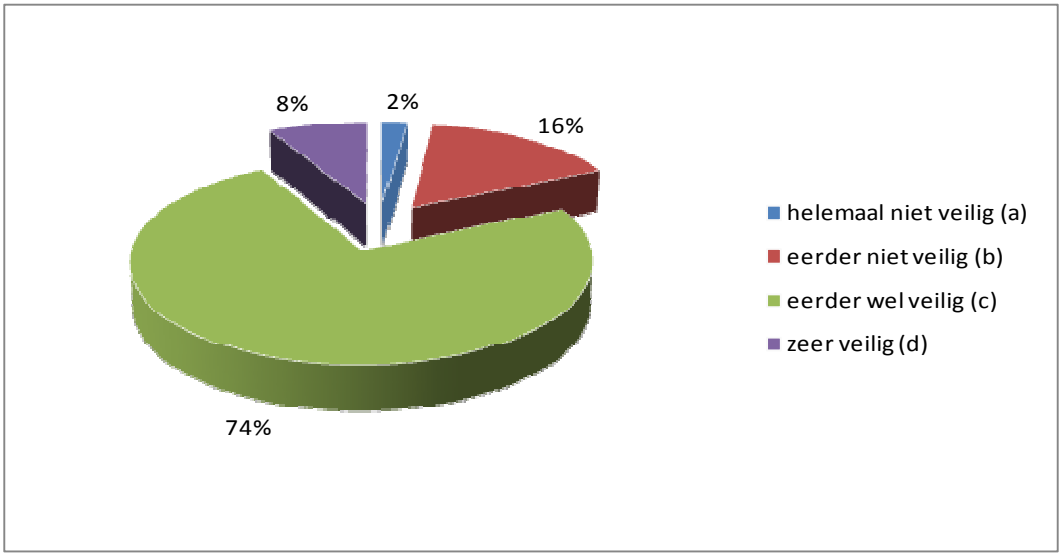
Het gebruik van de functies van de eID is relatief laag, hetgeen blijkt uit tabel 9.2. De meerderheid van de ondervraagden kent de toepassingen wel, maar heeft ze nog nooit gebruikt. Bij het elektronisch ondertekenen van een document met behulp van de eID zegt 57% van de respondenten dat ze deze toepassing kennen, maar nog nooit gebruikt hebben. 33% van de respondenten kent dit niet, en slechts 10% heeft ooit al één of meerdere keren gebruik gemaakt van de toepassingen. Voor de toepassing 'belastingsaangifte online invullen en indienen' is de verdeling gelijkaardig. Hier zegt 16% de toepassing niet te kennen, 67% kent de functie, maar heeft deze nog nooit gebruikt en 16% heeft de toepassing al ooit, of meerdere keren gebruikt.

Voor de laatste ondervraagde toepassing zegt 29% de toepassing niet te kennen, 59% kent ze, maar heeft ze nog nooit gebruikt en 12% heeft de eID reeds gebruikt om toegang te verkrijgen tot het e-loket.

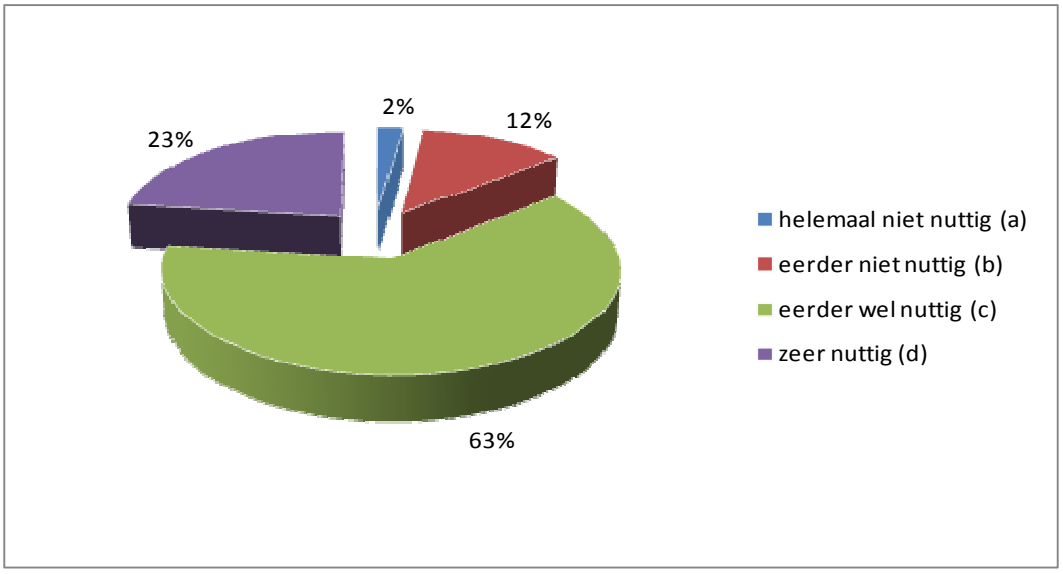
Tabel 9.2 Gebruik functies eID (n=49)

	Elektronisch document ondertekenen	Belastingsaangifte online indienen	Toegang verkrijgen tot het e-loket van uw gemeente
Niet bekend	33%	16%	29%
Bekend, maar nog niet gebruikt	57%	67%	59%
Al eens gebruikt	6%	8%	8%
Al meerdere keren gebruikt	4%	8%	4%

De verdelingen van de 3 toepassingen zijn gelijkaardig. Meer dan de helft van de respondenten kent de toepassing, maar maakt er nooit gebruik van. Slechts een klein percentage maakt daadwerkelijk gebruik van de toepassing. Nochtans vindt 82% van de respondenten de toepassingen van de eID eerder wel, tot zeer veilig, zoals zichtbaar op figuur 9.3. Bovendien vindt ook 86% deze toepassingen eerder wel, tot zeer nuttig. Deze bevindingen, zichtbaar op figuur 9.4, staan in contrast met het lage percentage dat gebruik maakt van de toepassingen. Een mogelijke reden hiervoor kan zijn dat er weinig informatie over beschikbaar is en dat veel personen niet weten hoe de toepassingen werken. Indien we een onderscheid trachten te maken naar geslacht, levert dit geen significante verschillen, zowel niet voor de veiligheid als het nut van de eID. Ook naar gelang de leeftijd en het opleidingsniveau zijn er geen opmerkelijke verschillen terug te vinden.

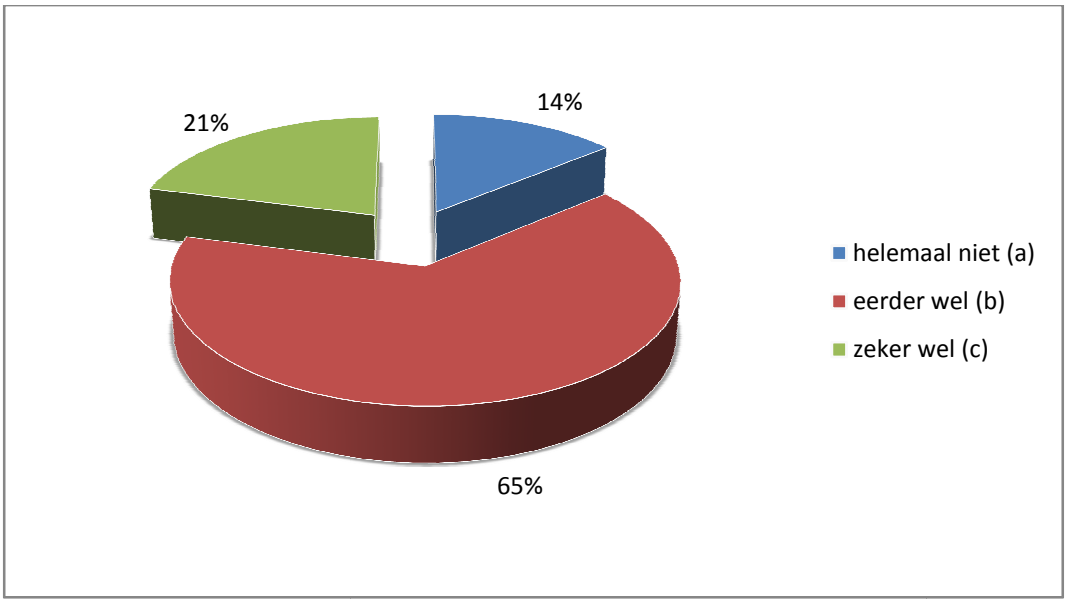


Figuur 9.3 Veiligheid van de eID toepassingen (n=49)



Figuur 9.4 Nut van de eID toepassingen (n=49)

Vervolgens werd ondervraagd of men meer van de eID gebruik zou maken indien er meer informatie beschikbaar zou zijn. Het antwoord op deze vraag is voor het grootste deel van de respondenten positief, zoals figuur 9.5 weergeeft. Immers, 86% van de respondenten zegt dat hij/zij meer gebruik zou maken van de eID voor de verschillende toepassingen als er meer informatie beschikbaar zou zijn.



Figuur 9.5 Toename gebruik eID als er meer informatie beschikbaar is (n=49)

Er is enige samenhang terug te vinden tussen de toename in gebruik van de eID bij meer informatie en het feit of de mensen de toepassingen van de eID nuttig vinden. Tabel 9.3 illustreert dit. De persoon die de toepassingen van de eID helemaal niet nuttig vindt (a), zegt dat hij/zij de eID niet meer zal gebruiken als er meer informatie voorhanden zou zijn (a). Dit resultaat is weliswaar niet veralgemeenbaar. De meerderheid van de personen die de functies van de eID eerder wel tot zeer nuttig (c en d) vinden, zullen eerder wel meer gebruik maken hiervan bij een toename van de informatie (b).

Tabel 9.3 Samenhand tussen de variabelen 'eIDnuttig' en 'eIDinfo' (n=49)

			eIDnuttig				Total
			a	b	c	d	
eIDinfo	a	Count	1	2	4	0	7
		% within eIDnuttig	100,0%	33,3%	12,9%	,0%	14,3%
	b	Count	0	4	18	10	32
		% within eIDnuttig	,0%	66,7%	58,1%	90,9%	65,3%
	c	Count	0	0	9	1	10
		% within eIDnuttig	,0%	,0%	29,0%	9,1%	20,4%
Total		Count	1	6	31	11	49
		% within eIDnuttig	100,0%	100,0%	100,0%	100,0%	100,0%

Ook de variabelen ‘eID veilig’ en ‘eID info’ vertonen een bepaalde samenhang (tabel 9.4), hetzij minder evident. De persoon die de toepassingen van de eID helemaal niet veilig vindt (a) zegt toch

de eID eerder wel meer te gebruiken indien er meer informatie voorhanden is (b). Dit geldt ook voor de personen die de toepassingen zowel eerder niet als eerder wel nuttig vinden (b en c). Indien men de toepassingen zeer veilig vindt (d), zal het gebruik zeker toenemen indien er meer informatie beschikbaar is (c).

Tabel 9.4 Samenhang tussen de variabelen 'eIDveilig' en 'eIDinfo' (n=49)

			eIDveilig				Total
			a	b	c	d	
eIDinfo	a	Count	0	1	5	1	7
		% within eIDveilig	,0%	12,5%	13,9%	25,0%	14,3%
	b	Count	1	7	23	1	32
		% within eIDveilig	100,0%	87,5%	63,9%	25,0%	65,3%
	c	Count	0	0	8	2	10
		% within eIDveilig	,0%	,0%	22,2%	50,0%	20,4%
Total		Count	1	8	36	4	49
		% within eIDveilig	100,0%	100,0%	100,0%	100,0%	100,0%

In de toekomst zal de SIS kaart geïntegreerd worden in de eID. 90% van de respondenten zegt dit nuttig te vinden. Bovendien hadden de respondenten de mogelijkheid om zelf suggesties te doen omtrent mogelijke toepassingen. Toepassingen die naar voor kwamen zijn:

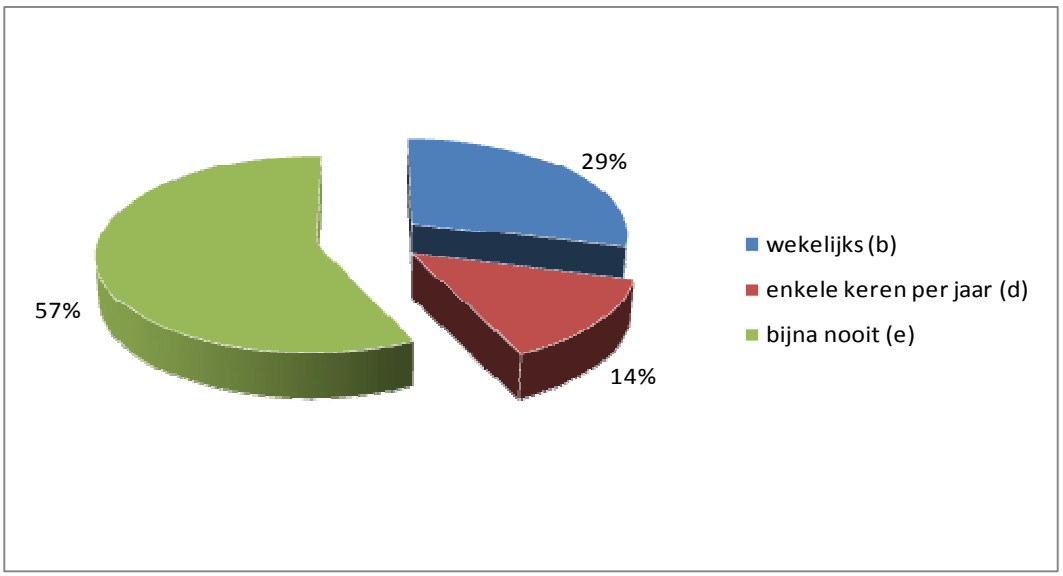
- Rijbewijs integreren in de eID
- Bloedgroepkaart integreren
- Verzekeringen opnemen in de eID
- Bankkaarten integreren

Opvallend bij deze peiling is dat men voornamelijk denkt aan mogelijke dingen die geïntegreerd kunnen worden in de eID, en niet zozeer aan nieuwe toepassingen van de huidige eID.

9.4.3 Het elektronische loket

In verband met het elektronisch loket werd eerst gepeild naar de kennis over het bestaan ervan. Toch 74% van de respondenten is hiervan op de hoogte. Om het e-loket te raadplegen, moet men naar de website van de gemeente surfen. 86% van de respondenten zegt dit al ooit gedaan te hebben. Slechts ongeveer 14% (7 personen) daarentegen heeft ook het e-loket van de gemeente bezocht. Het zijn relatief meer mannen dan vrouwen die het e-loket al bezocht hebben. Bij dit kleine deel van de respondenten werd dan gepeild naar het gebruik van het e-loket. Het aantal respondenten is hier echter te klein om echte conclusies te kunnen trekken uit deze vragen. Een eerste vraag had betrekking op de frequentie. De resultaten hiervan zijn weergegeven in figuur 9.6. Van de respondenten die het e-loket al eens bezocht hebben, zegt de meerderheid dit slechts

zelden te doen. Dit is echter logisch aangezien je enkel het e-loket zal bezoeken indien je een attest of iets dergelijk nodig hebt, en dit normaal niet zo vaak nodig is.

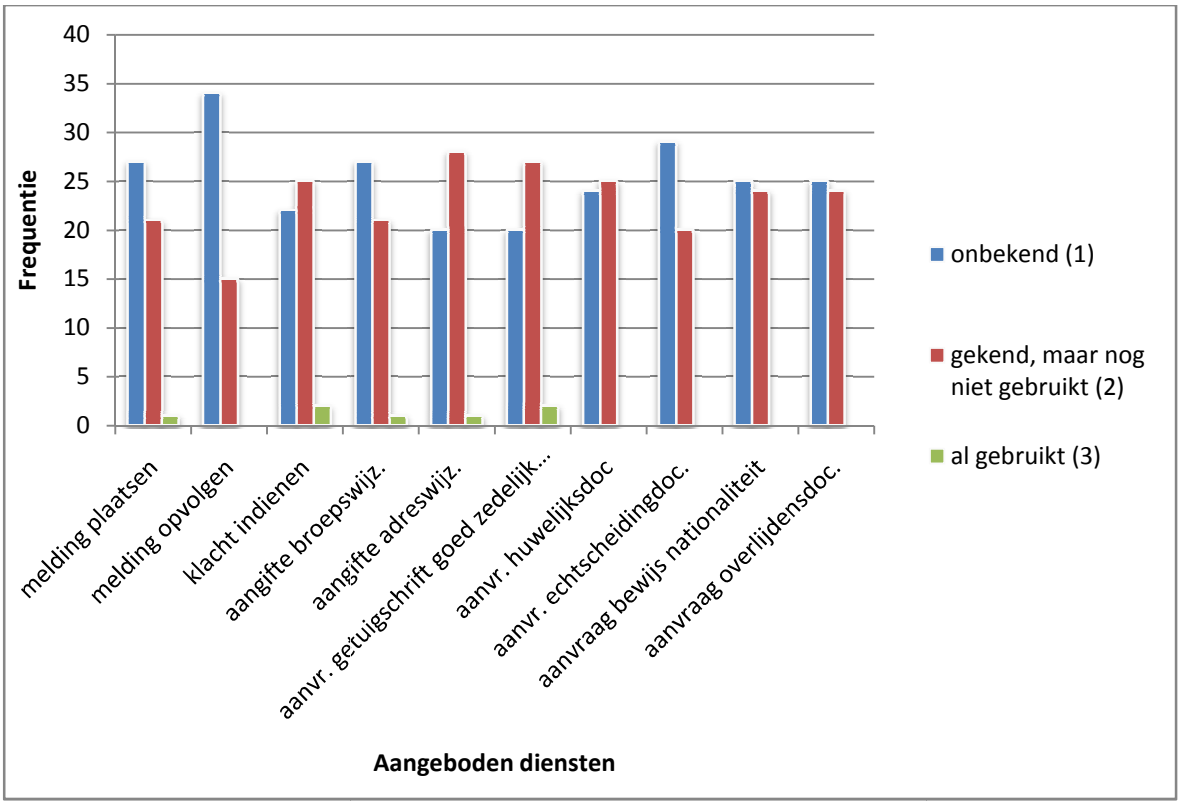


Figuur 9.6 Frequentie gebruik e-loket (n=7)

Ook de tevredenheid over het e-loket werd ondervraagd. Al de respondenten die al eens van het e-loket gebruik hebben gemaakt (n=7) , zijn tevreden tot erg tevreden over het e-loket, zowel met betrekking tot de aangeboden diensten als tot de gebruiksvriendelijkheid. 57% van de respondenten die het e-loket al eens gebruikt hebben, zouden dit ook aanraden aan anderen. Niemand zou het gebruik van het e-loket afraden. Anderen zouden het noch aanraden noch afraden. Op basis van vorige bevindingen kan toch geconcludeerd worden dat de personen die het e-loket reeds gebruikt hebben, hier tevreden over zijn. 5 van de 7 personen die het e-loket al gebruikt hebben, maakten hiervoor gebruik van hun eID. De andere 2 personen deden dit aan de hand van een token.

Vervolgens kregen de deelnemers een lijst met de diensten die via het e-loket van de gemeenten Diepenbeek aangeboden werden. Voor elke dienst dienden ze aan te duiden welke mogelijkheid voor hen van toepassing was: niet gekend / gekend maar nog niet gebruikt / al gebruikt. De resultaten zijn weergegeven in figuur 9.7.

Uit deze figuur blijkt dat de diensten slechts een enkele keer gebruikt worden. De meest populaire diensten zijn het indienen van een klacht en de aanvraag van een getuigschrift van goed zedelijk gedrag. Het aandeel respondenten dat een dienst niet kent, of kent maar niet gebruikt is overal ongeveer gelijk verdeeld. De dienst ‘melding opvolgen’ is echter door het grootste deel respondenten niet gekend. Er zijn bovendien 14 respondenten, hetgeen overeenkomt met ongeveer 29%, die zeggen geen enkele dienst te kennen.

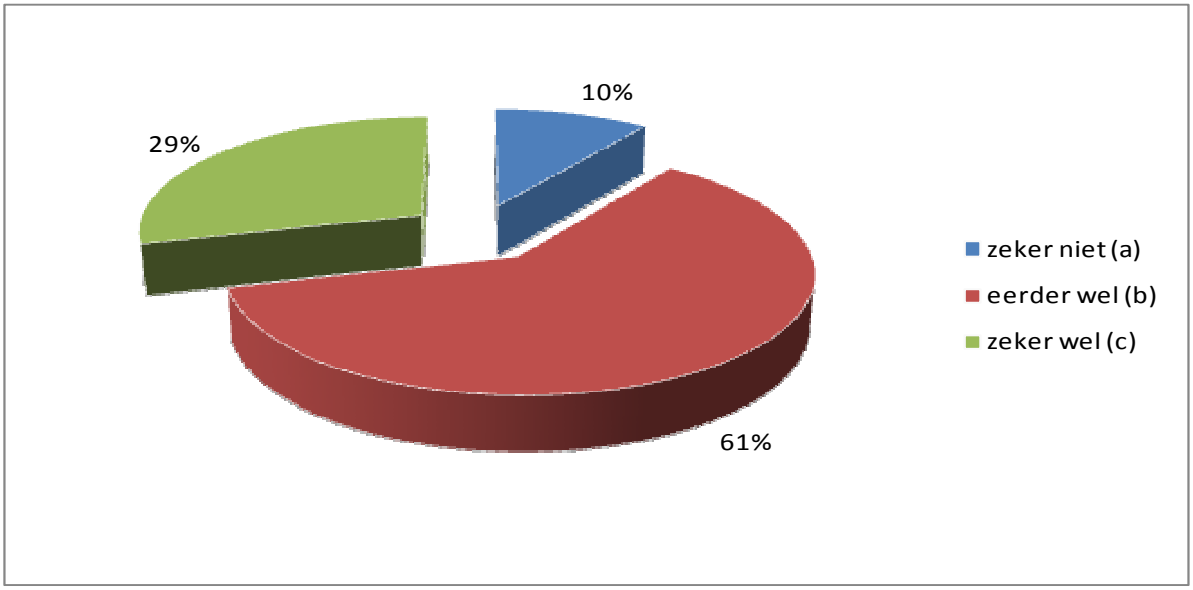


Figuur 9.7 Gebruik diensten e-loket (n=49)

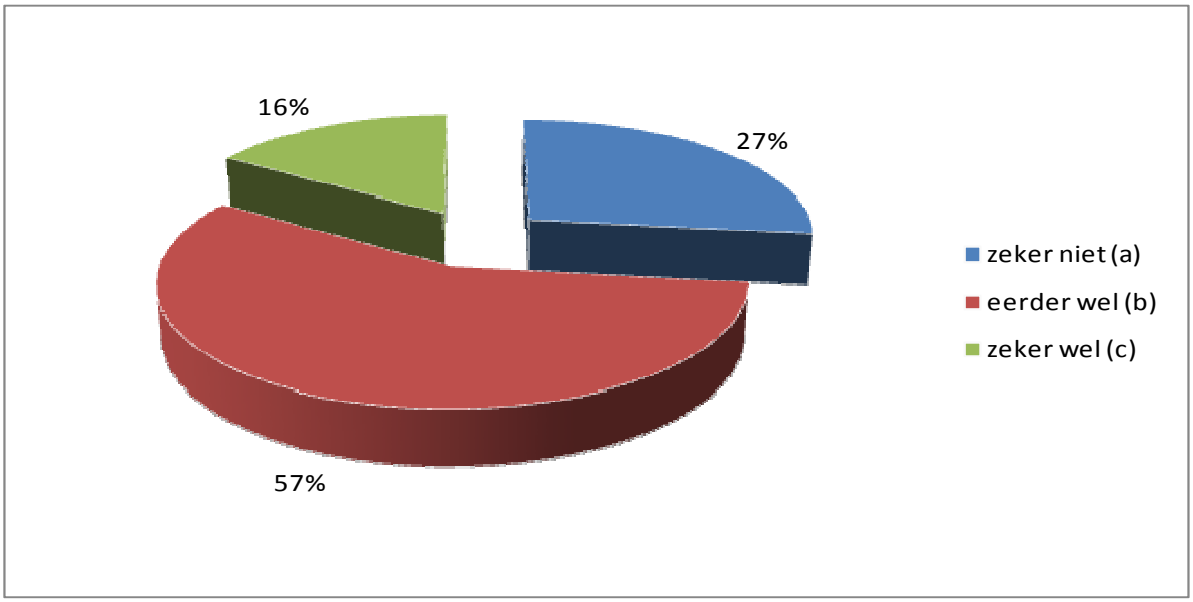
Ook hier was er de mogelijkheid voor respondenten om suggesties te doen omtrent de aangeboden diensten via het e-loket. Er werd één suggestie genoteerd, namelijk de mogelijkheid om aan te geven, dat ingeval van overlijden, hij/zij een donor wil schenken.

Vervolgens werd gepeild naar de informatiewens van de respondenten. De eerste vraag hieromtrent was of er genoeg informatie beschikbaar is over het e-loket. Ongeveer 3/4de van de respondenten (76%) vindt dat er niet voldoende informatie beschikbaar is.

Hierna onderzochten we de intenties om het e-loket meer te gebruiken indien er meer informatie voorhanden zou zijn. We splitsten dit op in informatie via brochures (figuur 9.8) en informatie via een infosessie (figuur 9.9). Via beide informatiewegen zei de meerderheid van de respondenten dat ze meer geneigd zouden zijn om het e-loket te gebruiken.



Figuur 9.8 Extra gebruik e-loket bij meer informatie via brochures (n=49)

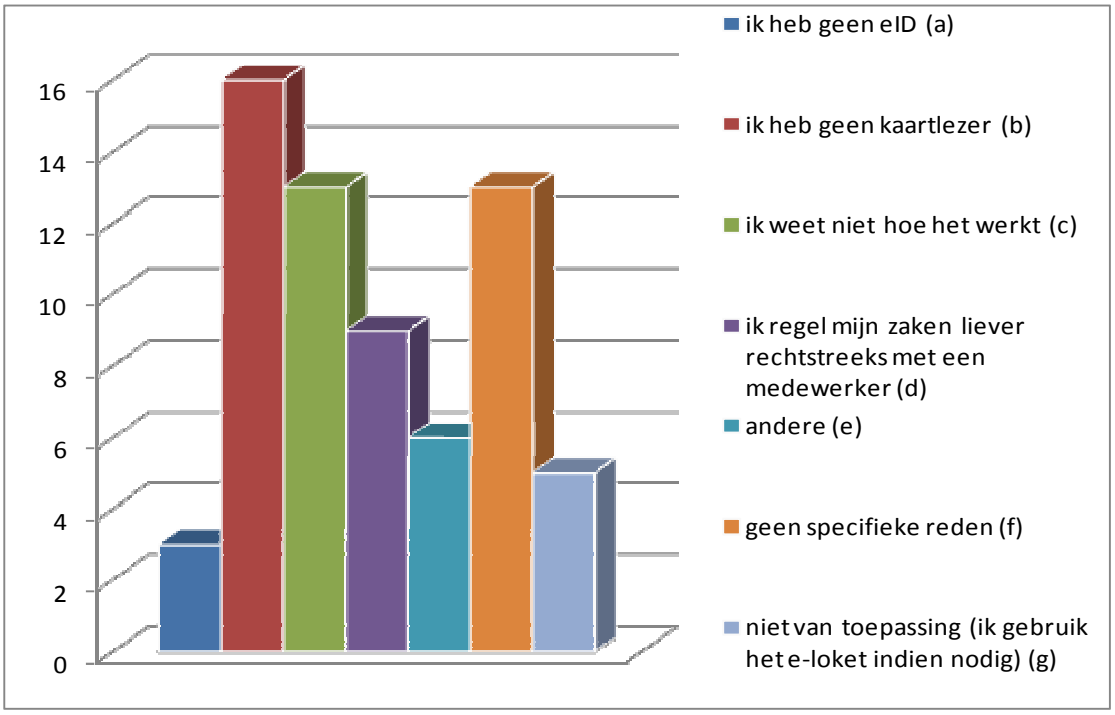


Figuur 9.9 Extra gebruik e-loket bij meer informatie via een infosessie (n=49)

De brochures zijn wel populairder dan de infosessie. Dit wordt duidelijk als we het aantal respondenten dat 'zeker wel' meer gebruik zou maken van het e-loket vergelijken. Bij informatie via brochures is dit 29%, bij een infosessie 16%. In totaal kunnen we dus zeggen dat bij extra informatie via brochures 90% van de respondenten geneigd is meer gebruik te maken van het e-loket, in vergelijking met 73% bij extra informatie via een infosessie. Hieruit blijkt dus dat de

gemeente meer informatie zou moeten verspreiden om het gebruik van het e-loket te doen stijgen. Dit blijkt eveneens uit volgende vraag waarin gevraagd wordt of de gemeente het e-loket meer zou moeten promoten; De resultaten zijn hier vergelijkbaar, namelijk 91% van de respondenten antwoord positief op deze vraag. De campagne van de overheid speelt in op deze informatiewens.

Tenslotte wordt nagegaan welke redenen aan de basis liggen van het lage gebruik van het e-loket. De resultaten hiervan worden weergegeven in figuur 9.10. De meest populaire redenen zijn dat men niet over een kaartlezer beschikt en dan men niet weet hoe het werkt. Als andere redenen werd aangehaald dat de kaartlezer niet werkt, dat men het nog niet nodig gehad heeft en dat er te weinig informatie voorhanden is.



Figuur 9.10 Oorzaken van het lage gebruik van het e-loket (n=49)

9.5 Conclusie

Op basis van voorgaande grafieken, kunnen we als conclusie een antwoord formuleren op de vragen gesteld in sectie 9.1.

Zijn de burgers voldoende ingelicht over de werking en het gebruik van de eID, en maken ze bovendien daadwerkelijk gebruik van de extra functies?

Uit de enquête blijkt dat de meerderheid wel kennis heeft van de mogelijkheden die de eID biedt, maar ze er zelden of nooit gebruik van maken. Bovendien vindt meer dan de helft van de respondenten deze toepassingen redelijk veilig en nuttig. De meeste ondervraagden geven ook mee dat ze de toepassingen meer zouden gebruiken indien er meer informatie voorhanden zou zijn.

Weten de burgers welke verrichtingen ze met het e-loket kunnen doen en maken ze hier gebruik van?

De grote meerderheid is ervan op de hoogte dat de gemeente over een e-loket beschikt, terwijl slechts een klein percentage ooit het e-loket heeft bezocht. De aangeboden diensten worden slechts zelden gebruikt alhoewel ze gemiddeld door ongeveer de helft van de respondenten gekend zijn. Er is hoe dan ook een grote meerderheid die vindt dat er te weinig informatie voorhanden is en beweert meer gebruik te maken van het e-loket als er meer informatie beschikbaar zou zijn. Hierbij is een infobrochure het populairste middel tot het verstrekken van informatie. De belangrijkste redenen voor het niet gebruiken van het e-loket zijn dat men niet over een kaartlezer beschikt en dat men niet weet hoe het werkt.

Is er voldoende informatie voorhanden omtrent de eID en het e-loket?

Uit de resultaten blijkt dat er te weinig informatie beschikbaar is, zowel over het e-loket als over de eID en dat een informatiecampagne het gebruik van beide tools kan doen stijgen. Bovendien kan het nuttig zijn om via de gemeente kaartlezers te verspreiden, of goedkoop te verkopen.

Hoofdstuk 10 Conclusies en mogelijkheden tot verder onderzoek

Het laatste hoofdstuk omvat de belangrijkste conclusies en enkele mogelijkheden tot verder onderzoek.

10.1 Conclusies

De wereld is geïnformatiseerd. Er wordt steeds minder gebruik gemaakt van gewone briefwisseling. Zowel communicatie als transacties gebeuren via het internet en papieren documenten worden steeds zeldzamer. Een leven zonder computer en zonder internet is voor velen onder ons niet meer denkbaar. Er zijn immers heel wat voordelen aan verbonden, zoals eenvoud en snelheid. Maar deze soepelheid impliceert ook nadelen, zoals de vergrote vatbaarheid voor fraude. Deze masterproef gaat in op een mogelijke manier om de gebruikers voor deze gevaren te beschermen.

Het gebruik van cryptologie, of de studie van het geheim schrijven, is hierbij belangrijk. Cryptologie bestaat uit cryptografie, of het geheim schrijven, en cryptoanalyse, of het breken van het geheimschrift. De digitale handtekening steunt op de principes van asymmetrische cryptografie. Deze vorm maakt gebruik van twee verschillende sleutels, een private en een publieke sleutel. De digitale handtekening is echter geen echte handtekening, die onder aan een document gezet wordt. Het is het versleutelen van een hashwaarde van een bericht met de private sleutel van de afzender.

De hashwaarde wordt bekomen door het toepassen van een hash functie op het bericht. Een goede hash functie is een wiskundige functie die voor elke zinnige tekst een andere ‘vingerafdruk’ berekent, de hashwaarde genoemd. Voor verzending kan de afzender de hashwaarde van zijn bericht berekenen. De ontvanger dient dan, na ontvangst van het bericht, de hashwaarde opnieuw te berekenen. Indien deze ongewijzigd is, betekent dit dat ook het bericht ongewijzigd is. Op deze manier wordt de **integriteit** van een bericht verzekerd. Het gebruik van een hash functie kan dus niet verhinderen dat er iets aan het bericht wordt gewijzigd, maar zal dit wel signaleren aan de ontvanger.

De ondertekenaar beschikt over een private sleutel, die enkel hij kent, en een publieke sleutel die openbaar is. De verzender zal de hashwaarde van het bericht versleutelen met zijn private sleutel en deze omgevormde hashwaarde naar de ontvanger sturen, samen met het bericht. De ontvanger zal de oorspronkelijke hash waarde enkel kunnen terug vinden als hij de publieke sleutel, horend bij de private sleutel van de verzender, toepast op de omgevormde hashwaarde. Doordat de zender de hashwaarde versleutelt met zijn private sleutel, is de ontvanger er dus zeker van dat hij

of zij deze boodschap verstuurd heeft, hetgeen de authenticiteit van een bericht bevorderd. Er bestaat echter nog geen zekerheid over wie de persoon is achter dat sleutelpaar. Hiervoor is het noodzakelijk om gebruik te maken van een certificatieautoriteit. Zulke autoriteit voorziet publieke sleutels van een certificaat dat de identiteit van de eigenaar en de geldigheid van het certificaat bevat. Isabel en Certipost zijn voorbeelden van certificatieautoriteiten. Op deze manier is dus een tweede belangrijk concept verzekerd, namelijk de **authenticiteit**.

Door gebruik te maken van de digitale handtekening kan de afzender ook niet ontkennen dat hij het bericht verzonden heeft, aangezien het versleuteld is met zijn private sleutel. Dit verzekert de **onweerlegbaarheid**. Dus zowel de integriteit van een bericht, als de authenticiteit en de onweerlegbaarheid kan men dus verzekeren door gebruik te maken van een digitale handtekening.

De digitale handtekening kan niet voor **vertrouwelijkheid** zorgen, maar het gebruik van cryptografie kan dit wel. Men kan zowel van symmetrische (DES) als van asymmetrische cryptografie (RSA) gebruik maken. Bij asymmetrische cryptografie kan de afzender zijn bericht versleutelen met de publieke sleutel van de ontvanger, zodat enkel de ontvanger dit kan ontsleutelen met zijn private sleutel. In praktijk wordt echter voornamelijk de symmetrische variant gebruikt, omdat het asymmetrische RSA algoritme heel veel rekenwerk vergt.

Door van voornoemde principes gebruik te maken, kan elektronisch verkeer zeer veilig verlopen. Om documenten 'ondertekend' met een digitale handtekening ook rechtsgeldig te maken, is er in 1999 een Europese richtlijn opgesteld met betrekking tot de elektronische handtekening. Deze richtlijn is omgezet naar de Belgische wetgeving in 2000. Deze wet stelt dat een geavanceerde elektronische handtekening die aan bepaalde voorwaarden voldoet, wettelijk gelijkgesteld wordt met een handgeschreven handtekening. Een digitale handtekening, gebaseerd op een geldig certificaat, voldoet aan die voorwaarden en kan dus als juridisch geldig worden beschouwd.

De digitale handtekening kan worden toegepast in heel wat gebieden, gaande van veilig e-mail verkeer, over het veilig bewaren van documenten tot het gebruik bij e-government. Binnen deze laatste toepassing speelt de elektronische identiteitskaart een zeer belangrijke rol. Deze identiteitskaart kan, naast identificatie, nog voor andere doeleinden gebruikt worden. Het is een middel tot authenticatie, bijvoorbeeld op beveiligde internetsites en men kan er bovendien documenten elektronisch mee ondertekenen, beide aan de hand van een digitale handtekening. E-government kent talrijke toepassingen, zoals het elektronisch indienen van de belastingsaangifte via Tax-on-web. Voor bedrijven bestaan gelijkaardige tools, Vensoc voor de aangifte van de vennootschapsbelasting en Intervat voor de BTW aangifte. Verscheidene gemeenten beschikken reeds over een elektronisch loket waar burgers bepaalde formulieren kunnen aanvragen of bijvoorbeeld een adreswijzing kunnen aangeven. Ook de politie beschikt over een elektronisch loket, 'Police-on-web', waar men bijvoorbeeld een diefstal kan aangeven. Burgers kunnen toegang krijgen tot deze diensten aan de hand van een eID, die hier als middel tot authenticatie dient.

Er wordt echter nog zeer weinig gebruik gemaakt van deze diensten. Dit blijkt ook uit de enquête over het e-loket en de eID, die in het kader van dit onderzoek gevoerd werd binnen de gemeente Diepenbeek. Zowel de eID als het e-loket worden slechts zelden gebruikt, terwijl de meeste respondenten dit toch nuttig vinden. Er wordt voornamelijk gezegd dat er te weinig informatie voorhanden is over deze concepten en hun werking. Hieruit blijkt dat de overheid de eID en zijn toepassingen meer moet promoten. Om dit te doen heeft Minister van Binnenlandse zaken, Guido de Padt en Minister van Administratieve Vereenvoudiging, Vincent Van Quickenborne op 20 april 2009 een campagne aangekondigd onder de naam 'In 1-2-3 met je eID'. Het doel is de mensen meer bewust te maken van de gebruiken en de toepassingen van de eID. Dit gebeurt via een website, waarop de burger informatie kan vinden over de eID en door middel van de 'eID-bus' die het land zal doorkruisen. Bij een bezoek aan de bus wordt je ingelicht over de werking van de eID en bestaande en toekomstige toepassingen. Bovendien krijgt elke bezoeker een informatiepakket en een eID-lezer mee. Dit is alvast een goed initiatief om het gebruik van de eID te doen toenemen. We dienen echter op te merken dat de eID misschien niet geschikt is voor alledaags gebruik. Er moet immers fysiek contact zijn tussen de eID en de kaartlezer om de eID te kunnen gebruiken. Dit impliceert dat de kaart onderhevig kan zijn voor slijtage.

10.2 Mogelijkheden tot verder onderzoek

Deze eindverhandeling bespreekt slechts een deel van de bestaande topics rondom de digitale handtekening. We kunnen hier dan ook nog enkel suggesties formuleren voor verder onderzoek.

Allereerst is het belangrijk om continu onderzoek te verrichten naar betere hash functies. Hedendaagse hash functies zijn immers niet perfect en zeker voor verbetering vatbaar. Hiernaast kan het interessant zijn om ook een blik te werpen op andere bestaande toepassingen van de digitale handtekening, zoals het gebruik bij medische toepassingen.

Binnen e-government zijn er ook nog heel wat mogelijkheden tot onderzoek. Zo kan men de impact van de huidige overheidscampagne op het gebruikt van de eID nagaan. Ook het berekenen van de kosten en baten die gepaard gaan bij het gebruik van de eID, zowel voor de burger als voor de overheid, kan nuttig zijn. Hiernaast moeten de verdere ontwikkelingen in verband met nieuwe toepassingen opgevolgd worden. Hierbij is het belangrijk om aandacht te besteden aan mogelijke beperkingen van de eID, zoals de kwetsbaarheid bij veelvuldig gebruik.

Tenslotte zou ook een vergelijkende studie kunnen worden uitgevoerd, die het gebruik van de digitale handtekening en de eID binnen België kadert in een internationale context.

Lijst van geraadpleegde werken

Boeken

Buyst, L. (1967). *Codetheorie*. Antwerpen: N.V. Scriptoria.

Kaspersen, H.W.K., Stuurman, K. (2001). *Juridische aspecten van e-mail* [Elektronische versie]. Kluwer.

Keller, G., & Warrack, B. (2003). *Statistics for management and economics.* Pacific Grove: Thomson.

Menezes, A.J., Van Oorschot, P.C., & Vanstone, S.A. (1997). *Handbook of applied cryptography.* Florida: CRC Press LLC.

Panko, R. R. (2005 a). *Business Data Networks and telecommunications*. Upper Saddle River, N.J. : Pearson.

Panko, R. R. (2005 b) *Datanetwerken en telecommunicatie* [Elektronische versie] (M. Kerkhof, Vertaling) Pearson Education. (Oorspronkelijk verschenen in het Engels)

Stallings, W. (2000). *Netwerkbeveiliging en cryptografie*. Schoonhoven: Academic Service.

Stinson, D.R. (1995). *Cryptography: theory and practice.* Florida: Chapman & Hall/CRC.

Stinson, D.R. (2006). *Cryptography: theory and practice* [Elektronische versie]. Florida: Chapman & Hall/CRC.

Tanenbaum, A.S., & Geurts, L. (2005). *Gestructureerde computerarchitectuur* [Elektronische versie]*.* Pearson Education.

Van der Lubbe, J.C.A. (1997). *Basismethoden cryptografie* [Elektronische versie]. Delftse Universitaire Pers.

Van der Lubbe, J.C.A. (1998). *Basic Methods of cryptography* [Elektronische versie]. (S. Gee, Vertaling). Cambridge University Press. (Oorspronkelijk verschenen in het Nederlands in 1994).

Van Eecke, P. (2004). *De handtekening in het recht: Van pennentrek tot elektronische handtekening* [Elektronische versie]. Larcier

Van Tilborg, H.C.A. (1993). *An introduction to cryptology.* Boston: Kluwer.

Van Tilborg, H.C.A. (2005). *Encyclopedia of cryptography and security* [Elektronische versie]. Springer.

Kranten en tijdschriften

Adobe kiest voor elektronische identiteitskaart [Elektronische versie]. (2005, 8 april). *De standaard.*

EID without boundaries. (2008, februari). *Information security industry report,* 12.

Elektronische identiteitskaart mag geen flop worden. (2008, mei). H*et ingenieursblad*, 8.

FOD Binnenlandse Zaken. (2006). *EID-Newsletter, 2* [Elektronische versie].

FOD Binnenlandse Zaken. (2007). *EID-Newsletter, 4* [Elektronische versie].

FOD Binnenlandse Zaken. (2008). *EID-Newsletter, 8* [Elektronische versie].

Groen licht voor elektronische maaltijdcheques [Elektronische versie]. (2009, 21 juli). *Het nieuwsblad.*

Kwart meer belastingaangiftes via Tax-on-web [Elektronische versie]. (2008, 1 november). *De tijd*.

The use of eID cards in Belgium. (2008, februari). *Information security industry report*, 11.

Van der Hof, S. (1997). De juridische status van de digitale handtekening [Elektronische versie]. *Nationaal programma informatietechnologie en recht*, 7.

Internetbronnen

Boudrez, F. (2005). *Digitale handtekeningen en archiefdocumenten*. Opgevraagd op 8 september 2008, van de volgende website: http://www.expertisecentrumdavid.be/docs/digitalehandtekeningen_archiefdocumenten.pdf.

Certipost. (2008 a) *Wat betekent onweerlegbaarheid.* Opgevraagd op 5 november 2008, van de volgende website: http://www.certipost.be/dpsolutions/nl/eid-faq.html

Certipost. (2008 b) *E-certificates.* Opgevraagd op 5 november 2008, van de volgende website: http://www.certipost.be/dpsolutions/nl/e-certificates-overzicht.html

CM. (2009). *CM-selfservice*. Opgevraagd op 5 februari 2009, van de volgende website: http://www.cm.be/nl/100/selfservice/index.jsp

Codetheorie. (2008). In *Online encyclopedie*. Opgevraagd op 16 november 2008, van de volgende website: http://www.encyclo.nl/zoek.php

CORVE. (2008). *Wat is e-government?* Opgevraagd op 15 december 2008, van de volgende website: http://www.corve.be/overegov/wat/index.php

Cryptology. (2008). In *Encyclopædia Britannica*. Opgevraagd op 29 september 2008, van de volgende website: http://www.britannica.com/EBchecked/topic/145058/cryptology.

De Weger, B. (2005). *Hash-functies onder vuur: De situatie van MD5 en SHA-1*. Opgevraagd op 3 oktober 2008, van de volgende website: http://www.win.tue.nl/~bdeweger/Hashbotsingen.pdf.

Diepenbeek. (2009). *Diepenbeek start met kids-ID.* Opgevraagd op 2 april 2009, van de volgende website: http://www.diepenbeek.be/fb111pfme141tyf1tyf237.aspx

Eid startpagina. (2009). Opgevraagd op 5 augustus 2009, van de volgende website: http://eid.startpagina.be.

Entrust. (2008). *Digital Signatures*. Opgevraagd op 26 november 2008, van de volgende website: http://www.entrust.com/digitalsig/howtheywork.htm

Factorworld (2009). *General Purpose Factoring Records*. Opgevraagd op 13 augustus 2009, van de volgende website: http://www.crypto-world.com/FactorRecords.html.

Fod Economie. (2008). *E-government.* Opgevraagd op 3 oktober 2008, van de volgende website: http://mineco.fgov.be/information_society/administrations/e-government_BE/e_government_definition_nl_001.htm

FOD financiën. (2009 a). *Wat houdt Intervat in?* Opgevraagd op 9 februari 2009, van de volgende website: http://minfin.fgov.be/portail2/nl/e-services/intervat/faq/01.htm#A

FOD financiën. (2009 b). *Wat is Vensoc?* Opgevraagd op 9 februari 2009, van de volgende website: http://www.minfin.fgov.be/portail1/nl/vensoc/FAQ_NL.htm#_Toc95538734

Fortis. (2009). *Veilig surfen op het internet*. Opgevraagd op 13 februari 2009, van de volgende website: https://www.fortisbanking.be/private/Start.asp

Goddyn, B. (2001). *Elektronische handel en consumentenbescherming. Een vergelijking tussen de E.U. en de V.S. (UCITA).* Opgevraagd op 8 september 2008, van de volgende website: http://users.skynet.be/bgoddyn/publpdf/e-commerce.pdf

Husquinet, M. (2009). *Belgische supercomputers kunnen niet meer mee.* Opgevraagd op 18 augustus 2008, van de volgende website: http://www.datanews.be/nl/news/90-6-24676/belgische-supercomputers-kunnen-niet-meer-mee.html

In 1-2-3 met je eID. (2009). Opgevraagd op 5 mei 2009, van de volgende website: http://www.welcome-to-e-belgium.be/nl/.

Isabel. (2008). *Welk type van certificaten wordt uitgereikt door Isabel NV.* Opgevraagd op 24 november 2008, van de volgende website: http://www.isabel.be/gps/nl/index.php-

Jungslager, F. (2004). *Elektronische authenticatie en de elektronische handtekening*. Opgevraagd op 5 november 2008, van de volgende website: http://www.ivory.nl/bestanden/Artikel%20de%20waarde%20van%20digitaal%20tekenen.pdf

Koops; B.J., Van der Hof, S. (2002). Informatiebeveiliging, e-handel en recht [Elektronische versie]. Verschenen in: Van Esch, R.E.,& Prins, J.E.J. (red.) *Recht en elektronische handel*. Deventer: Kluwer 2002, p. 387-409.

Kruispuntbank sociale zekerheid. (2008 a). *Missie.* Opgevraagd op 19 december 2008, van de volgende website: http://www.ksz-bcss.fgov.be/Nl/mission/mission_home.htm

Kruispuntbank sociale zekerheid. (2008 b). *Veiligheid.* Opgevraagd op 19 december 2008, van de volgende website: http://www.ksz-bcss.fgov.be/Nl/securite/securite_home.htm

K.U. Leuven. (2000). *De digitale handtekening: een stand van zaken*. Opgevraagd op 23 augustus 2008, van de volgende website: http://www.law.kuleuven.be/icri/publications/111bijdrage%20digitale%20overheden.pdf.

Leuven. (2008). *E-loket*. Opgevraagd op 18 december 2008, van de volgende website: http://www.leuven.be/showpage.asp?iPageID=840

Loidreau, P. (2002). *Introductie in cryptografie*. Opgevraagd op 22 september 2008, van de volgende website: http://www.linuxfocus.org/Nederlands/May2002/article243.meta.shtml.

Microsoft Corporation. (2009). *Digitale handtekening maakt uw e-mail veilig.* Opgevraagd op 12 februari 2009, van de volgende website: http://www.microsoft.com/netherlands/ondernemers/ondernemen_communicatie/e-mail/digitalehandtekening.aspx

Msn. (2009). *Kan eID het treinabonnement vervangen?* Opgevraagd op 5 augustus 2009, van de volgende website: http://tech.be.msn.com/eid/article.aspx?cp-documentid=148303026

POD MI. (2008 a). *Digitale handtekening.* Opgevraagd op 18 december 2008, van de volgende website: http://www.mi-is.be/themes/egov/Digitale%20Handtekening/index_nl.htm

POD MI. (2008 b). *Gebruik van de elektronische identiteitskaart om de digitale documenten te ondertekenen*. Opgevraagd op 19 december 2008, van de volgende website: http://www.mi-is.be/themes/egov/Digitale%20Handtekening/index_nl.htm

Robben, F. (z.d.). *E-government.* Opgevraagd op 15 december, van de volgende website: http://www.law.kuleuven.ac.be/icri/frobben/publications/2004%20-%20E-government.pdf

Robben, F. (2006). *E-government*. Opgevraagd op 15 december, van de volgende website*:* www.law.kuleuven.be/icri/frobben/presentations/20060327b.ppt

RSA Laboratories. (2008 a). *What is a one-way function*. Opgevraagd op 1 oktober 2008, van de volgende website: http://www.rsa.com/rsalabs/node.asp?id=2188.

RSA Laboratories. (2008 b). *What is a hash function*. Opgevraagd op 1 oktober 2008, van de volgende website: http://www.rsa.com/rsalabs/node.asp?id=2176.

RSA Laboratories. (2008 c). *What are MD2, MD4, and MD5*. Opgevraagd op 3 oktober 2008, van de volgende website: http://www.rsa.com/rsalabs/node.asp?id=2253.

RSA Laboratories. (2008 d). *What would it take to break the RSA cryptosystem?* Opgevraagd op 1 oktober 2008, van de volgende website: http://www.rsa.com/rsalabs/node.asp?id=2216

Silva, J.E. (2003). *An overview of cryptografic hash functions and their uses*. Opgevraagd op 30 september, van de volgende website: http://www.sans.org/reading_room/whitepapers/vpns/879.php.

Tax-on-web. (2009). Opgevraagd op 9 februari 2009, van de volgende website: http://www.taxonweb.be/taxonweb/app/citizen/public/taxbox/home.do

Tieleman, O., & Vernooij, J. (2002). *Cryptografie.* Opgevraagd op 18 september, van de volgende website: http://jelmer.vernstok.nl/publications/cryptografie.pdf

Van den Eynde, S., & Dumortier, J. (z.d.). *De rol van de digitale handtekening bij de archivering van elektronische documenten*. Opgevraagd op 15 september, van de volgende website: http://www.law.kuleuven.be/icri/publications/80artikel%20DH%20nederlands%202.pdf?where=

Van der Meer, H. (2007). *Syllabus Cryptografie.* Opgevraagd op 23 september 2008, van de volgende website: http://staff.science.uva.nl/~hansm/pubs/syllabus-s.pdf.

Van Sebroeck, H. (2001). *E-GOV naar een elektronische overheid in België.* Opgevraagd op 15 september, van de volgende website: http://www.plan.be/admin/uploaded/200605091448082.WP0104nl.pdf

Vanvelthoven, P. (2003). *Beleidsnota van de Staatssecretaris voor Informatisering van de Staat*. Opgevraagd op 8 september 2008, van de volgende website: http://economie.fgov.be/information_society/administrations/e-government_BE/note_strateg_inform_Etat_nl.pdf

Velle (2002). *E-government en de archivaris.* Opgevraagd op 9 september 2008, van de volgende website: http://www.vvbad.be/files/200206_Velle.pdf

Vercammen, E. (z.d.). *De digitale handtekening.* Opgevraagd op 20 augustus 2008, van de volgende website: http://www.babantwerp.be/DIGIT.pdf.

Wikipedia. (2008 a). *Internet.* Opgevraagd op 20 september 2008, van de volgende website: http://nl.wikipedia.org

Wikipedia. (2008 b). *Cryptoanalyse.* Opgevraagd op 18 september 2008, van de volgende website: http://nl.wikipedia.org

Wikipedia. (2008 c). *E-commerce.* Opgevraagd op 18 februari 2009, van de volgende website: http://nl.wikipedia.org/wiki/Electronic_commerce

Wilschut, D.E. (2000). *Digitale handtekeningen: een experimentele vergelijking*. Opgevraagd op 20 augustus 2008, van de volgende website: http://ftp.cwi.nl/CWIreports/MAS/MAS-N0001.pdf

Wetteksten

Koninklijk besluit van 6 december 2002 houdende organisatie van de controle en de accreditatie van de certificatiedienstverleners die gekwalificeerde certificaten afleveren. Opgevraagd op 16 augustus 2008, van de volgende website: http://mineco.fgov.be/information_society/e-signatures/law_e_signature_004.pdf

Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen. Opgevraagd op 16 augustus 2008, van de volgende website: http://mineco.fgov.be/information_society/e-signatures/directive_1999_93_nl.pdf.

Wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure. Opgevraagd 16 augustus 2008, van de volgende website: http://mineco.fgov.be/information_society/e-signatures/law_e_signature_001.pdf.

Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten. Opgevraagd op 16 augustus 2008, van de volgende website:

http://mineco.fgov.be/information_society/e-signatures/law_e_signature_002.pdf.

Geraadpleegde eindverhandelingen

Deckers, M. (2005). *De digitale handtekening als stimulans voor e-commerce en economische vooruitgang.* Limburgs Universitair Centrum, Diepenbeek.

Hermans, I. (2002). *De digitale handtekening en de elektronische bedrijfsvoering.* Limburgs Universitair Centrum, Diepenbeek.

Lambrichts, B. (2007). *De invloed van de digitale handtekening op de elektronische aangifte van de vennootschapsbelasting.* Universiteit Hasselt, Diepenbeek.

Schraepen, P. (2006). *De rol van de cryptologie en de digitale handtekening inzake de veiligheid van elektronische informatie-uitwisseling.* Universiteit Hasselt, Diepenbeek.

Thijs, H. (2005). *Analyse van de digitale handtekening en de mogelijkheden in de logistieke sector.* Limburgs Universitair Centrum, Diepenbeek.

Lijst van bijlagen

Bijlage 1 Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten

(Belgisch Staatsblad van 29 september 2001)

HOOFDSTUK I. ALGEMENE BEPALING

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

HOOFDSTUK II. DEFINITIES EN TOEPASSINGSGEBIED VAN DE WET

AFDELING 1. DEFINITIES

Art. 2. Deze wet zet de bepalingen om van de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen.

Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder:

1° « elektronische handtekening » : gegevens in elektronische vorm, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie;

2° « geavanceerde elektronische handtekening » : elektronische gegevens vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie en aan de volgende eisen voldoet :

a) zij is op unieke wijze aan de ondertekenaar verbonden :

b) zij maakt het mogelijk de ondertekenaar te identificeren;

c) zij wordt aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;

d) zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke latere wijziging van de gegevens kan worden opgespoord;

3° « certificaat » : een elektronische bevestiging die de gegevens voor het verifiëren van de handtekening koppelt aan een natuurlijke persoon of een rechtspersoon en de identiteit van die persoon bevestigt;

4° « gekwalificeerd certificaat » : een certificaat dat voldoet aan de eisen van bijlage I van deze wet en dat wordt afgegeven door een certificatiedienstverlener die voldoet aan de eisen van bijlage II van deze wet;

5° « certificaathouder » : een natuurlijke persoon of rechtspersoon aan wie een certificatiedienstverlener een certificaat heeft afgegeven;

6° « gegevens voor het aanmaken van een handtekening » : unieke gegevens, zoals codes of cryptografische privé-sleutels, die door de ondertekenaar worden gebruikt om een geavanceerde elektronische handtekening aan te maken;

7° « veilig middel voor het aanmaken van een handtekening » : geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het aanmaken van een handtekening te implementeren en die voldoet aan de eisen van bijlage III van deze wet;

8° « gegevens voor het verifiëren van een handtekening » : gegevens, zoals codes of cryptografische openbare sleutels, die worden gebruikt voor het verifiëren van een geavanceerde elektronische handtekening;

9° « middel voor het verifiëren van een handtekening » : geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het verifiëren van een handtekening te implementeren;

10° « certificatiedienstverlener » : elke natuurlijke persoon of rechtspersoon die certificaten afgeeft en beheert of andere diensten in verband met elektronische handtekeningen verleent;

11° « product voor elektronische handtekeningen » : software of hardware, of relevante componenten daarvan, die door certificatiedienstverleners kunnen worden gebruikt om diensten op het gebied van elektronische handtekeningen te verlenen of die voor het aanmaken of verifiëren van elektronische handtekeningen kunnen worden gebruikt;

12° « Bestuur » : het bestuur van het ministerie van Economische Zaken dat belast is met de taken betreffende de accreditatie en de controle van de certificatiedienstverleners die gekwalificeerde certificaten afgeven en in België gevestigd zijn;

13° « entiteit » : instelling die haar bevoegdheid aantoont op grond van een certificaat afgegeven door het Belgisch accreditatiessysteem conform de wet van 20 juli 1990 betreffende de accreditatie van certificatie- en keuringsinstellingen alsmede van beproevingslaboratoria of door een gelijkwaardige instelling opgericht binnen de Europese Economsiche Ruimte.

AFDELING 2. TOEPASSINGSGEBIED

Art. 3. Deze wet legt bepaalde regels vast in verband met het juridisch kader voor elektronische handtekeningen en bepaalt het juridisch stelsel van toepassing op de activiteiten van de

certificatiedienstverleners evenals de door deze laatste en de certificaathouders na te leven regels, zonder afbreuk te doen aan de wettelijke bepalingen met betrekking tot de bevoegdheid tot het stellen van rechtshandelingen voor rekening van rechtspersonen.

Deze wet voert eveneens een vrijwillig accreditatiestelsel in.

HOOFDSTUK III. ALGEMENE PRINCIPES

Art. 4. § 1. Behoudens andersluidende wettelijke bepalingen kan niemand verplicht worden rechtshandelingen te stellen via elektronische weg.

§ 2. Een certificatiedienstverlener kan niet verplicht worden een voorafgaande machtiging aan te vragen voor de uitoefening van zijn activiteiten.

De in belgië gevestigde certificatiedienstverleners die gekwalificieerde certificaten afgeven dienen niettemin, ofwel in de loop van de maand die volgt op de bekendmaking van deze wet, ofwel voor de aanvang van hun activiteiten, de volgende inlichtingen mee te delen aan het Bestuur :

- hun naam;
- het geografisch adres waar ze gevestigd zijn;
- hun coördinaten, waardoor ze gemakkelijk te bereiken zijn, met inbegrip van hun adres voor elektronische post;
- in voorkomend geval, hun beroep, referenties en identificatienummers (handelsregister, BTW);
- het bewijs dat er een verzekering onderschreven werd ter dekking van hun verplichtingen bedoeld in artikel 14.

Het Bestuur overhandigt hen een ontvangstbewijs binnen vijf werkdagen volgend op de ontvangst van hun mededeling.

§ 3. De Koning kan, bij een besluit vastgesteld na overleg in Ministerraad, voor het gebruik van elektronische handtekeningen in de openbare sector eventuele aanvullende eisen stellen. Deze eisen moeten objectief, transparant, evenredig en niet discriminerend zijn en mogen slechts op de specifieke kenmerken van de betrokken toepassing betrekking hebben. Zij mogen geen belemmering vormen voor grensoverschrijdende diensten voor de burgers.

§ 4. Onverminderd de artikelen 1323 en volgende van het Burgerlijk Wetboek wordt een geavanceerde elektronische handtekening, gerealiseerd op basis van een gekwalificieerd certificaat en aangemaakt door een veilig middel voor het aanmaken van een handtekening, geassimileerd met een handgeschreven handtekening ongeacht of deze handtekening gerealiseerd wordt door een natuurlijke dan wel door een rechtspersoon.

§ 5. Een elektronische handtekening kan geen rechtsgeldigheid worden ontzegd en niet als bewijsmiddel in gerechtelijke procedures worden geweigerd louter op grond van het feit dat :

- de handtekening in elektronische vorm is gesteld, of
- niet is gebaseerd op een gekwalificeerd certificaat, of
- niet is gebaseerd op een door een geaccrediteerd certificatiedienstverlener afgegeven certificaat, of
- zij niet met een veilig middel is aangemaakt.

Art. 5. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten aanzien van de verwerking van persoonsgegevens, mag een certificatiedienstverlener die voor het publiek bestemde certificaten afgeeft enkel rechtstreeks bij de betrokken persoon of met diens uitdrukkelijke toestemming persoonlijke gegevens inwinnen en enkel indien dit noodzakelijk is voor de afgifte en de bewaring van het certificaat. De gegevens mogen niet voor andere doeleinden worden verzameld of verwerkt zonder de uitdrukkelijke toestemming van de betrokken persoon.

§ 2. Wanneer de houder van het certificaat een pseudoniem gebruikt en wanneer het onderzoek dit vereist, is de certificatiedienstverlener die het certificaat heeft afgegeven ertoe gehouden alle gegevens betreffende de identiteit van de titularis mee te delen in de omstandigheden en volgens de voorwaarden waarin de artikelen 90ter tot 90decies van het Wetboek van Strafvordering voorzien.

HOOFDSTUK IV. PRODUCTEN VOOR ELEKTRONISCHE HANDTEKENINGEN

Art. 6. Wanneer een product voor elektronische handtekeningen overeenstemt met de normen waarvan de referentienummers worden gepubliceerd in het Publicatieblad van de Europese Gemeenschappen, overeenkomstig de procedure bedoeld in de richtlijn 99/93/EG van het Parlement en van de Raad van 13 december 1999 betreffende een communautair kader voor de elektronische handtekeningen, wordt dit product verondersteld te voldoen aan de eisen van bijlage II, punt f), en bijlage III van deze wet.

Art. 7. § 1. De eisen in verband met de veilige middelen voor het aanmaken van een elektronische handtekening zijn vermeld in bijlage III van deze wet.

§ 2. De overeenstemming van de veilige middelen voor het aanmaken van een elektronische handtekening met de eisen van bijlage III van deze wet, wordt bevestigd door de bevoegde instellingen, aangewezen door het Bestuur en waarvan de lijst wordt meegedeeld aan de Europese Commissie.

§ 3. De Koning bepaalt de voorwaarden waaraan de instellingen bedoeld in de vorige paragraaf moeten voldoen.

§ 4. De overeenstemming vastgesteld door een instelling aangewezen door een andere lidstaat van de Europese Economische Ruimte, wordt in België erkend.

HOOFDSTUK V. CERTIFICATIEDIENSTVERLENERS DIE GEKWALIFICEERDE CERTIFICATEN AFGEVEN

AFDELING 1. GEKWALIFICEERDE CERTIFICATEN

ONDERAFDELING 1. OPDRACHTEN

Art. 8. § 1. Vooraleer een certificaat af te geven, onderzoekt de certificatiedienst-verlener de complementariteit van de gegevens voor het aanmaken en het verifiëren van de handtekening.

§ 2. Na de identiteit en, in voorkomend geval, de specifieke hoedanigheden geverifieerd te hebben, geeft de certificatiedienstverlener één of meer certificaten af aan elke persoon die daarom verzoekt.

§ 3. Voor de rechtspersonen houdt de certificatiedienstverlener een register bij met de identiteit en de hoedanigheid van de natuurlijke persoon die de rechtspersoon vertegenwoordigt en die gebruik maakt van de handtekening verbonden aan het certificaat, op zo een wijze dat bij elk gebruik van deze handtekening de identiteit van de natuurlijke persoon kan achterhaald worden.

Art. 9. De certificatiedienstverlener verschaft een exemplaar van het certificaat aan de kandidaat-houder.

Art. 10. De certificatiedienstverlener houdt een elektronisch register bij met de certificaten die hij afgeeft en het tijdstip waarop ze vervallen.

ONDERAFDELING 2 - VEREISTEN BETREFFENDE DE GEKWALIFICEERDE CERTIFICATEN

Art. 11. § 1. De gekwalificeerde certificaten moeten voldoen aan de eisen van bijlage I van deze wet.

§ 2. De certificatiedienstverleners die gekwalificeerde certificaten afgeven, moeten voldoen aan de eisen van bijlage II van deze wet.

ONDERAFDELING 3 - HERROEPING VAN DE GEKWALIFICEERDE CERTIFICATEN

Art. 12. § 1. Op aanvraag van de vooraf geïdentificeerde certificaathouder herroept de certificatiedienstverlener onmiddellijk het certificaat.

§ 2. De certificatiedienstverlener herroept eveneens een certificaat indien :

1° er ernstige redenen bestaan om aan te nemen dat het certificaat werd afgegeven op basis van foutieve of vervalste gegevens, dat de in het certificaat opgenomen informatie niet meer met de werkelijkheid overeenstemt of dat de vertrouwelijkheid van de gegevens voor het aanmaken van een handtekening werd geschonden;

2° de rechtbanken de maatregelen hebben bevolen waarin artikel 20, § 4, b), voorziet;

3° de certificatiedienstverlener zijn activiteiten stopzet zonder dat deze worden overgenomen door een andere certificatiedienstverlener die een gelijkwaardig kwaliteits- en veiligheidsniveau waarborgt;

4° de certificatiedienstverlener op de hoogte gebracht wordt van het overlijden van de natuurlijke persoon of van de ontbinding van de rechtspersoon die certificaathouder is.

De certificatiedienstverlener brengt de certificaathouder, behalve in geval van overlijden, op de hoogte van de herroeping en motiveert zijn beslissing. Een maand voor het vervallen van een certificaat brengt de certificatiedienstverlener de certificaathouder hiervan op de hoogte.

§ 3. De herroeping van een certificaat is definitief.

Art. 13. § 1. De certificatiedienstverlener treft de nodige maatregelen om op elk ogenblik en onverwijld gevolg te kunnen geven aan een aanvraag tot herroeping.

§ 2. Onmiddellijk na de beslissing tot herroeping van een certificaat schrijft de certificatiedienstverlener de vermelding van de herroeping in in het elektronisch register zoals bedoeld in artikel 10.

Vanaf deze inschrijving is de herroeping tegenstelbaar ten aanzien van derden.

ONDERAFDELING 4. AANSPRAKELIJKHEID VAN DE CERTIFICATIEDIENSTVERLENERS DIE GEKWALIFICEERDE CERTIFICATEN AFGEVEN

Art. 14. § 1. Een certificatiedienstverlener die een gekwalificeerd certificaat aan het publiek afgeeft of een dergelijk certificaat publiekelijk waarborgt, is aansprakelijk voor de schade die hij toebrengt aan elke instelling of natuurlijke persoon of rechtspersoon die, als een goede huisvader, redelijkerwijze vertrouwen stelt in dit certificaat, voor wat betreft :

a) de juistheid van alle gegevens die in het gekwalificeerd certificaat opgenomen zijn op de datum dat het werd afgegeven en de vermelding, in dit certificaat, van alle voorgeschreven gegevens voor een gekwalificeerd certificaat;

b) de garantie dat de in het gekwalificeerde certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het certificaat, de gegevens bevat voor het aanmaken van de handtekening overeenstemmend met de in het certificaat vermelde of geïdentificeerde gegevens voor het verifiëren van de handtekening;

c) de garantie dat de gegevens voor het aanmaken en die voor het verifiëren van een handtekening complementair kunnen worden gebruikt, in geval de certificatiedienstverlener beide

soorten gegevens genereert;tenzij de certificatiedienstverlener bewijst dat er van geen enkele nalatigheid sprake is.

§ 2. Een certificatiedienstverlener die aan het publiek een certificaat heeft afgegeven dat als gekwalificeerd bestempeld wordt, is aansprakelijk voor de schade die hij toebrengt aan een instelling of natuurlijke persoon of rechtspersoon die zich op redelijke wijze beroept op het certificaat, wanneer werd nagelaten de herroeping van het certificaat te laten registreren, tenzij de certificatiedienstverlener bewijst dat er van geen enkele nalatigheid sprake is.

§ 3. Een certificatiedienstverlener kan in een gekwalificeerd certificaat de beperkingen voor het gebruik ervan bepalen, op voorwaarde dat die beperkingen voor derden herkenbaar zijn. De certificatiedienstverlener is niet aansprakelijk voor de schade die voortvloeit uit het gebruik van een gekwalificeerd certificaat waarbij de aangegeven beperkingen voor het gebruik worden overschreden.

§ 4. Een certificatiedienstverlener kan in een gekwalificeerd certificaat de maximumwaarde bepalen van de transacties waarvoor het certificaat kan worden gebruikt, op voorwaarde dat die waarde voor derden herkenbaar is. De certificatiedienstverlener is niet aansprakelijk voor de schade die voortvloeit uit het overschrijden van die maximumwaarde.

ONDERAFDELING 5. STOPZETTING VAN DE ACTIVITEITEN VAN DE CERTIFICATIEDIENSTVERLENERS DIE GEKWALIFICEERDE CERTIFICATEN AFGEVEN

Art. 15. § 1. De certificatiedienstverlener die gekwalificeerde certificaten afgeeft, brengt binnen een redelijke termijn het Bestuur op de hoogte van zijn bedoeling om zijn activiteiten van gekwalificeerde certificatiedienstverlener stop te zetten alsook van elke maatregel die de stopzetting van zijn activiteiten tot gevolg kan hebben. In dit geval dient hij zich te vergewissen van de overname ervan door een andere certificatiedienstverlener die eenzelfde kwaliteits- en veiligheidsniveau waarborgt. Wanneer dit niet mogelijk is, herroept hij de certificaten twee maanden na de houders ervan te hebben ingelicht. In dit geval treft de certificatiedienstverlener de nodige maatregelen om te voldoen aan de verplichting waarin Bijlage II, i), voorziet.

§ 2. De certificatiedienstverlener die zijn activiteiten stopzet om redenen buiten zijn wil of in geval van faillissement, brengt het Bestuur daarvan onmiddellijk op de hoogte. Hij zorgt in voorkomend geval voor de herroeping van de certificaten en treft de nodige maatregelen om te voldoen aan de in Bijlage II, i), bepaalde verplichting.

ONDERAFDELING 6. CERTIFICATEN AFGEGEVEN ALS GEKWALIFICEERDE CERTIFICATEN DOOR BUITENLANDSE CERTIFICATIEDIENSTVERLENERS

Art. 16. § 1. Een voor het publiek bestemd gekwalificeerd certificaat afgegeven door een certificatiedienstverlener gevestigd in een lidstaat van de Europese Economische Ruimte, wordt

gelijkgesteld met de gekwalificeerde certificaten afgeven door een in België gevestigde certificatiedienstverlener.

§ 2. De voor het publiek bestemde certificaten, die als gekwalificeerde certificaten worden afgegeven door een certificatiedienstverlener gevestigd in een derde land, worden op juridisch vlak gelijkgesteld met de certificaten afgegeven door een certificatiedienstverlener die in België gevestigd is :

a) indien de certificatiedienstverlener voldoet aan de voorwaarden van de nationale reglementering waarin de richtlijn 99/93/EG van het Parlement en van de Raad van 13 december 1999 betreffende een communautair kader voor de elektronische handtekeningen werd omgezet en indien hij geaccrediteerd werd op basis van een vrijwillig accreditatiesysteem ingevoerd in een lidstaat van de Europese Economische Ruimte;
of
b) indien een in de Europese Gemeenschap gevestigde certificatiedienstverlener, die voldoet aan de eisen van de nationale reglementering waarin de richtlijn 99/93/EG van het Parlement en van de Raad van 13 december 1999 betreffende een communautair kader voor de elektronische handtekeningen werd omgezet, het certificaat waarborgt;
of
c) indien het certificaat of de certificatiedienstverlener erkend wordt in het kader van de toepassing van een bilaterale of multilaterale overeenkomst tussen de Europese Gemeenschap en derde landen of internationale organisaties.

AFDELING 2. GEACCREDITEERDE CERTIFICATIEDIENSTVERLENERS

Art. 17. § 1. Een certificatiedienstverlener die voldoet aan de eisen van bijlage II, gekwalificeerde certificaten afgeeft die overeenkomen met de eisen van bijlage I en aanmaakmiddelen gebruikt die overeenkomen met de eisen van bijlage III, kan het Bestuur om een accreditatie vragen.

De accreditatie waarin deze wet voorziet, steunt op het resultaat van een evaluatie, door een entiteit bedoeld in artikel 2, 13°, van de overeenstemming met de eisen van de bijlagen I, II en III en in voorkomend geval, met die verbonden aan andere diensten en producten afgegeven door de certificatiedienstverleners.

§ 2. De Koning preciseert de voorwaarden bedoeld in § 1 en bepaalt :

1° de procedure voor de toekenning, schorsing en intrekking van de accreditatie;

2° de aan het « Fonds voor accreditatie » verschuldigde bedragen voor het afleveren, beheren en controleren van de accreditatie;

3° de onderzoekstermijnen voor de aanvraag;

4° de regels voor de controle van de geaccrediteerde certificatiedienstverleners.

§ 3. De keuze om zich te wenden tot een geaccrediteerde certificatiedienstverlener is vrij.

Art. 18. Het Bestuur :

1° kent accreditaties toe en trekt ze in. Deze opdracht is onderworpen aan procedures en wordt uitgevoegd door personen en diensten die verschillend zijn van deze bedoeld in artikel 20, § 2;

2° coördineert de coherente en transparante toepassing van de accreditatieprincipes en -procedures met toepassing van deze wet;

3° superviseert de auditprocedures van de entiteiten bedoeld in artikel 2, 13°), evenals de activiteiten van deze entiteiten in het kader van de accreditatieprocedures;

4° deelt aan de Commissie en aan de landen van de Europese Economische Ruimte het volgende mee :

a) de informatie over het vrijwillig accreditatiestelsel ingevoerd met toepassing van deze wet;

b) de naam en het adres van alle in dit kader geaccrediteerde certificatiedienstverleners;

5° voert het geheel van notificaties uit bedoeld in artikel 11 van de richtlijn 1999/93/EG van het Europees Parlement en van de Raad van 13 december 1999 betreffende een communautair kader voor de elektronische handtekeningen.

HOOFDSTUK VI. CERTIFICAATHOUDERS

Art. 19. § 1. Zodra de gegevens voor het aanmaken van een handtekening samengesteld zijn, is de certificaathouder alleen verantwoordelijk voor de vertrouwelijkheid van deze gegevens.

§ 2. Wanneer er twijfel bestaat over het behoud van de vertrouwelijkheid van de gegevens voor het aanmaken van een handtekening of wanneer de in het certificaat opgenomen gegevens niet meer met de werkelijkheid overeenstemmen, dient de houder het certificaat te laten herroepen.

§ 3. Wanneer een certificaat vervalt of herroepen wordt, mag de houder na de vervaldatum van het certificaat of na herroeping geen gebruik meer maken van de overeenkomstige gegevens voor het aanmaken van een handtekening om deze gegevens te ondertekenen of te laten certificeren door een andere certificatiedienstverlener.

HOOFDSTUL VII. CONTROLE EN SANCTIES

Art. 20. § 1. De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, de regels betreffende de controle van de certificatiedienstverleners evenals de rechtsmiddelen die het Bestuur kan aanwenden.

§ 2. Het Bestuur is belast met de controle van de certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek. Onder bepaalde voorwaarden, bepaald door de Koning, is het Bestuur bevoegd om de certificatiedienstverleners alle informatie te vragen die noodzakelijk is om te controleren of zij deze wet eerbiedigen.

§ 3. Wanneer het Bestuur vaststelt dat een in België gevestigd certificatiedienstverlener, die gekwalificeerde certificaten afgeeft, zich niet houdt aan de voorschriften van deze wet, wijst het hem op die tekortkoming en stelt het een redelijke termijn vast tijdens welke de certificatiedienstverlener alle nodige maatregelen dient te hebben getroffen om opnieuw te handelen in overeenstemming met de wet.

§ 4. Indien na afloop van die termijn de nodige maatregelen niet werden getroffen, maakt het Bestuur de zaak aanhangig bij de rechtbank teneinde :

a) de certificatiedienstverlener te verbieden verder gekwalificeerde certificaten af te geven

en
b) de certificatiedienstverlener te gelasten onmiddellijk de houders van gekwalificeerde certificaten, die door hem werden afgegeven, op de hoogte te brengen van het feit dat ze niet langer voldoen aan de voorschriften van deze wet.

§ 5. Wanneer, na afloop van de voormelde termijn, de certificatiedienstverlener geaccrediteerd krachtens artikel 17 de toestand niet heeft geregulariseerd, trekt het Bestuur ambtshalve zijn accreditatie in.

De certificatiedienstverlener is verplicht de intrekking van de accreditatie in zijn elektronisch register te vermelden en de certificaathouders daarvan onverwijld op de hoogte te brengen.

Art. 21. § 1. Wie zich de hoedanigheid aanmatigt van geaccrediteerd certificatiedienstverlener wordt gestraft met gevangenisstraf van acht dagen tot drie maanden en met een geldboete van duizend tot tienduizend frank, of met een van die straffen alleen.

§ 2. Bij veroordeling op grond van de in paragraaf 1 bedoelde overtreding kan de bevoegde rechtbank de volledige of gedeeltelijke opneming van het vonnis in een of meerdere dagbladen bevelen, onder de door haar bepaalde voorwaarden en op kosten van de veroordeelde.

Kondigen deze wet af, bevelen dat zij met 's Lands zegel zal worden bekleed en door het Belgisch Staatsblad zal worden bekendgemaakt.

Gegeven te Brussel

Bijlage 2 Enquête elektronische identiteitskaart en het elektronisch loket

universiteit hasselt

Enquête elektronische identiteitskaart

en het elektronisch loket (e-loket)

Beste,

Ik ben een studente Handelsingenieur aan de Universiteit Hasselt. In het kader van mijn masterproef over de digitale handtekening doe ik een onderzoek naar de kennis over en het gebruik van de elektronische identiteitskaart en het elektronisch loket

Het elektronisch loket is een realisatie van E-government en is bereikbaar via de website van uw gemeente. Via dit loket kan u formulieren aanvragen en invullen, gegevens wijzigen, enz… op een uiterst veilige manier. Een manier om het elektronisch loket te gebruiken, is door in te loggen met behulp van uw elektronische identiteitskaart (eID). U dient dan te beschikken over een eID-kaartlezer en over een PC en internetverbinding. Het voordeel van het e-loket is, dat het vrij snel en eenvoudig is om formulieren in te vullen en dat u zich hiervoor niet moet verplaatsen.

In de enquête zal gepeild worden naar uw kennis over en gebruik van de elektronische identiteitskaart en het E-loket en naar eventuele wensen en voorstellen tot verbetering.

Er zijn weliswaar geen goede of slechte antwoorden. De enquête wordt gebruikt om een beeld te krijgen van de populariteit van dit concept. Uw gegevens worden dan ook vertrouwelijk behandeld.

De enquête zal slechts 10 minuten van uw tijd vergen. Gelieve telkens het antwoord dat voor u van toepassing is, aan te klikken.

Onder de deelnemers zal ik twee filmtickets verloten. Indien u hiervoor kans wil maken, kan u op het einde van de vragenlijst uw gegevens doorgeven.

Ik dank u bij voorbaat voor uw tijd.

Vriendelijke groeten,

Laura Postelmans

Allereerst volgen er enkele vragen over uw persoonlijke situatie.

1. Leeftijdscategorie (lft)[1]
   - < 25 jaar
   - 25-29 jaar
   - 30-34 jaar
   - 35-39 jaar
   - 40-45 jaar
   - >45 jaar

2. Geslacht
   - Man
   - Vrouw

3. Opleidingsniveau (hoogst behaald diploma) (opleid)
   - Lager onderwijs
   - Secundair onderwijs
   - Hoger onderwijs - natuurwetenschappen
   - Hoger onderwijs – menswetenschappen
   - Hoger onderwijs – medische of paramedische wetenschappen

Volgende reeks vragen hebben betrekking op de elektronische identiteitskaart;

4. Beschikt u reeds over een elektronische identiteitskaart? (eID)
   - Ja
   - Neen

5. De eID vervangt uw oude identiteitskaart als bewijs van uw identiteit. Hiernaast kan u met uw eID echter nog andere handelingen doen (zoals het inloggen op beveiligde internetsites). Wist u dit? (eID2)
   - Ja
   - Neen

[1] Na elke vraag staan de afkortingen die gebruikt worden in de dataset (bijlage 3)

6. Onderstaand staan enkele mogelijke toepassingen van de eID en enkele toepassingen die in de toekomst mogelijk zouden zijn. Gelieve aan te duiden of u deze toepassing kent en of u er reeds gebruik van hebt gemaakt. (eIDtoep)

	Bekend	Niet bekend	Al eens gebruikt	Al meerdere keren gebruikt
Een elektronisch document ondertekenen (1)				
Belastingsaangifte elektronisch invullen en versturen (2)				
Toegang verkrijgen tot het elektronisch loket van uw gemeente (3)				

7. In welke mate vindt u deze toepassingen veilig? (eIDveilig)
   - Helemaal niet veilig
   - Eerder niet veilig
   - Eerder wel veilig
   - Zeer veilig

8. In welke mate vindt u deze toepassingen nuttig? (eIDnuttig)
   - Helemaal niet nuttig
   - Eerder niet nuttig
   - Eerder wel nuttig
   - Zeer nuttig

9. Indien er meer informatie beschikbaar zou zijn over het gebruik van de eID voor deze toepassingen, in welke mate zou u dan meer gebruik te maken van deze toepassingen? (eIDinfo)
   - Helemaal niet
   - Eerder wel
   - Zeker wel

10. In de toekomst zal de SIS-kaart geïntegreerd worden in de eID. Vindt u dit nuttig? (eIDSIS)
    - Ja
    - Neen

11. Heeft u nog andere suggesties over mogelijke toepassingen van de eID? (eIDsuggestie)
    - Ja , namelijk:
    - Neen

Volgende vragen hebben betrekking op het e-loket van uw gemeente (diepenbeek);

12. Wist u dat uw gemeente een elektronisch loket had? (eloket)
    - Ja
    - Neen

13. Hebt u al ooit de website van uw gemeente bezocht? (website)
    - Ja
    - Neen → ga naar vraag 20

14. Hebt u ooit al het e-loket van uw gemeente bezocht, te bereiken via de website van de gemeente? (eloket2)
    - Ja
    - Neen → ga naar vraag 20

15. Hoe vaak bezoekt u het e-loket van uw gemeente? (freqbezoek)
    - Dagelijks
    - Wekelijks
    - Maandelijks
    - Enkele keren per jaar
    - Bijna nooit

16. In welke mate bent u tevreden over het e-loket, met betrekking tot het aantal aangeboden diensten? (tevrdienst)
    - Erg tevreden
    - Tevreden
    - Niet echt tevreden
    - Erg ontevreden

17. In welke mate bent u tevreden over het e-loket, met betrekking tot de gebruiksvriendelijkheid? (tevrgebruik)
    - Erg tevreden
    - Tevreden
    - Niet echt tevreden
    - Erg ontevreden

18. Maakt u gebruik van uw eID om in te loggen bij het e-loket? (inlog)
    - Ja
    - Neen, ik maak gebruik van een token

19. In welke mate zou u het gebruik van het e-loket aanraden aan anderen? (aanraden)
    - Zeker aanraden
    - Niet aanraden of niet afraden
    - Afraden

20. Volgende diensten worden aangeboden via het e-loket. Kan u aanduiden of u deze diensten kent en of u er reeds gebruik van gemaakt hebt. (dienst)

	Ken ik niet	Ken ik, maar nog niet gebruikt	Al eens gebruikt	Al meerdere keren gebruikt
Melding plaatsen (bv. Straatlantaarn stuk) (1)				
Status melding opvolgen (bv. in behandeling) (2)				
Klacht indienen (3)				
Aangifte beroepswijziging (4)				
Aangifte adreswijziging (5)				
Aanvraag getuigschrift goede zedelijk gedrag (6)				
Aanvraag documenten ivm huwelijk (7)				
Aanvraag documenten ivm nationaliteit (8)				
Aanvraag documenten ivm echtscheiding (9)				
Aanvraag documenten ivm overlijden (10)				

21. Hebt u suggesties omtrent andere diensten die aangeboden kunnen worden via het elektronisch loket? (dienstsug)
    - Ja, namelijk:
    - Neen

22. Vindt u dat er voldoende informatie voor handen is over het gebruik en de werking van het e-loket? (eloketinfo)
    - Ja
    - Neen

23. Indien er meer informatie voorhanden zou zijn over het gebruik en de werking van het e-loket **via brochures**, zou u dan eerder/meer gebruik maken van het e-loket? (infobroch)
    - Helemaal niet
    - Eerder wel
    - Zeker wel

24. Indien er meer informatie voorhanden zou zijn over het gebruik en de werking van het e-loket **via een infosessie**, zou u dan eerder/meer gebruik maken van het e-loket? (infosessie)
    - Helemaal niet

- Eerder wel
- Zeker wel

25. Vindt u dat de gemeente het e-loket meer moet promoten? (eloketpromo)
    - Ja
    - Neen

26. Omwille van welke reden(-en) maakte u nog geen/weinig gebruik van het e-loket (u kan meerdere antwoorden aankruisen) (reden)

    - Ik heb geen eID (1)
    - Ik heb geen kaartlezer (2)
    - Ik weet niet hoe het werkt (3)
    - Ik regel mijn zaken liever rechtstreeks met een medewerker (4)
    - Andere: (5)
    - Geen specifieke reden (6)
    - Niet van toepassing (7)

Bedankt voor uw medewerking!

Laura Postelmans

Wenst u de resultaten van dit onderzoek per e-mail te verkrijgen?

- JA, e-mailadres:
- NEEN, dat is niet nodig

Indien u kans wil maken op één van de twee filmtickets, gelieve dan uw naam en adres onderstaand in te vullen. (Deze informatie is strikt geheim, en zal enkel voor dit doel gebruikt worden).

……

Bijlage 3 Gegevens enquête

id	InwD	Lft	geslacht	opleid	eID	eID2	eIDtoep1	eIDtoep2	eIDtoep3	eIDveilig	eIDnuttig	eIDinfo	eIDSIS	eIDsuggestie	eIDsugg	eloket
2	1	d	1	b	1	1	02	02	02	c	c	c	a	a	rijbewijs linken aan eID	1
3	1	e	2	c	1	1	02	02	02	c	c	b	a	b	0	2
4	1	b	1	d	1	1	02	02	02	c	c	c	a	b	0	2
5	1	a	1	b	2	2	01	01	01	c	c	b	a	b	0	2
6	1	a	2	b	1	2	01	04	02	c	c	c	a	b	0	1
9	1	a	2	b	1	1	02	02	02	a	d	b	a	b	0	1
10	1	b	2	c	1	1	02	02	02	c	c	c	a	b	0	1
11	1	a	1	d	1	1	02	02	02	c	d	b	a	b	0	2
12	1	e	1	e	1	2	01	02	01	b	d	b	a	b	0	2
13	1	b	2	c	1	1	02	02	02	c	d	b	a	b	0	1
14	1	c	1	d	1	1	02	02	02	c	c	a	b	b	0	1
15	1	e	1	d	1	2	02	02	02	c	c	b	b	b	0	2
16	1	e	1	b	1	1	02	02	02	c	c	b	a	b	0	1
17	1	c	1	b	1	2	02	02	02	c	c	b	a	b	0	1
18	1	e	1	b	1	2	01	01	01	b	c	b	a	b	0	2
19	1	c	2	d	1	1	02	02	02	c	c	a	b	b	0	1
20	1	b	1	b	1	1	02	02	01	c	c	b	a	b	0	2
21	1	d	2	b	1	1	02	02	01	c	c	b	a	b	0	1
22	1	a	1	b	1	2	02	02	02	c	c	b	a	b	0	1
23	1	e	1	b	1	2	02	02	01	c	d	b	a	b	0	2
24	1	d	1	b	1	1	03	01	02	c	b	a	b	b	0	1
25	1	c	1	d	1	1	01	03	02	b	c	b	a	b	0	1
26	1	b	1	c	1	1	01	02	02	c	d	b	a	b	0	1
27	1	e	1	c	1	1	02	02	02	c	c	c	a	b	0	1
28	1	a	1	d	1	1	02	02	01	c	c	b	a	b	0	2
29	1	f	1	d	1	1	02	02	02	c	c	b	a	a	rijbewijsbloedgroep	1
30	1	d	1	b	2	2	01	02	01	d	d	c	a	b	0	2
31	1	d	1	e	1	1	02	03	02	c	c	c	a	b	0	2
32	1	d	1	d	1	1	04	04	04	c	d	b	a	a	happy days,...	1
33	1	e	1	b	1	1	03	02	03	c	c	b	a	b	0	1
34	1	c	2	e	1	1	04	04	04	b	d	b	a	a	vb donor	1
35	1	e	2	d	1	1	03	03	02	d	c	c	a	b	0	1
36	1	d	1	b	1	2	02	02	02	b	b	b	a	b	0	2
37	1	b	2	b	1	2	01	02	01	c	c	b	a	a	rijbewijs, verzekering	2
38	1	a	1	b	1	2	01	01	03	c	b	b	a	b	0	1
39	1	e	1	b	1	1	02	02	02	c	c	b	a	b	0	1
40	1	a	1	b	1	1	01	02	01	c	c	a	a	b	0	2
41	1	a	2	b	1	2	01	03	03	c	d	b	a	a	bankhandelingen	1
42	1	a	1	d	1	1	01	01	01	d	b	a	b	b	0	1
43	1	a	1	b	1	1	01	02	02	b	b	b	a	b	0	1
44	1	f	2	b	2	1	02	02	01	c	c	a	a	a	bankkaart	1
45	1	c	1	e	1	2	01	01	02	c	c	b	a	b	0	2
46	1	f	1	b	1	1	02	02	02	d	c	b	a	b	0	1
47	1	e	2	c	1	1	02	02	02	c	c	c	a	b	0	1
48	1	c	2	b	1	1	02	04	03	c	d	b	a	b	0	1
49	1	e	2	c	1	2	01	01	01	b	a	a	a	b	0	2
50	1	e	1	c	1	1	02	02	02	c	c	b	a	b	0	1
51	1	c	2	d	1	2	01	01	01	b	b	b	a	b	0	2
52	1	c	2	c	1	1	02	02	02	c	c	c	a	b	0	1

id	website	eloket2	freqbezoek	tevrdienst	tevrgebruik	inlog	aanraden	dienst1	dienst2	dienst3	dienst4	dienst5	dienst6	dienst7	dienst8	dienst9	dienst10	dienstsug	suggestie
2	1	2	0	0	0	0	0	2	1	2	2	2	2	2	1	1	2	b	0
3	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
4	1	2	0	0	0	0	0	1	1	1	2	2	1	1	1	1	1	b	0
5	1	1	e	b	b	b	a	1	1	1	1	1	1	1	1	1	1	b	0
6	1	2	0	0	0	0	0	2	1	1	2	2	2	2	1	1	1	b	0
9	1	1	e	b	b	a	b	2	2	2	1	2	2	1	1	1	1	b	0
10	1	2	0	0	0	0	0	1	1	1	1	1	3	2	1	1	1	b	0
11	1	2	0	0	0	0	0	2	1	1	1	1	2	1	1	1	1	b	0
12	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
13	1	2	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	b	0
14	1	2	0	0	0	0	0	2	1	2	2	2	2	2	2	2	2	b	0
15	1	2	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	b	0
16	1	2	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	b	0
17	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
18	1	2	0	0	0	0	0	1	1	1	1	1	1	2	2	2	2	b	0
19	1	2	0	0	0	0	0	1	1	2	1	2	2	1	1	2	1	b	0
20	1	2	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	b	0
21	1	2	0	0	0	0	0	1	1	1	2	2	2	1	1	2	1	b	0
22	2	0	0	0	0	0	0	2	2	1	1	1	1	1	1	1	1	b	0
23	1	2	0	0	0	0	0	1	1	2	1	1	1	1	1	1	1	b	0
24	1	2	0	0	0	0	0	1	1	2	1	1	1	1	1	1	1	b	0
25	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
26	1	2	0	0	0	0	0	1	1	1	1	2	2	1	1	2	2	b	0
27	1	2	0	0	0	0	0	2	1	2	1	2	2	1	1	1	1	b	0
28	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
29	1	2	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	b	0
30	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
31	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
32	1	1	b	b	a	a	a	2	2	3	2	2	2	2	2	2	2	b	0
33	2	0	0	0	0	0	0	2	2	2	2	2	2	2	2	1	2	b	0
34	1	1	b	a	b	b	a	2	2	3	2	2	2	2	2	2	2	a	donor
35	1	2	0	0	0	0	0	1	1	2	1	2	1	2	1	2	2	b	0
36	2	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	b	0
37	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
38	2	0	0	0	0	0	0	1	1	2	2	2	2	2	2	2	2	b	0
39	1	1	d	b	b	a	b	1	1	2	2	2	3	2	2	2	2	b	0
40	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
41	1	1	e	b	b	a	b	2	2	2	3	3	2	2	2	2	2	b	0
42	1	2	0	0	0	0	0	2	1	2	1	2	2	2	2	2	2	b	0
43	1	2	0	0	0	0	0	2	1	2	1	2	2	2	2	2	2	b	0
44	2	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
45	2	0	0	0	0	0	0	1	1	2	2	2	2	2	2	2	2	b	0
46	1	2	0	0	0	0	0	1	1	2	2	2	2	2	2	2	2	b	0
47	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
48	1	1	e	b	b	a	a	3	2	2	2	2	2	2	2	2	2	b	0
49	2	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
50	1	2	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	b	0
51	1	2	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	b	0
52	1	2	0	0	0	0	0	2	2	2	2	2	2	2	1	2	2	b	0

id	eloketinfo	infobroch	infosessie	eloketpromo	reden1	reden2	reden3	reden4	reden5	reden6	reden7	redenander
2	2	b	b	1	0	Y	0	0	0	Y	0	0
3	2	c	b	1	0	0	0	0	0	Y	0	0
4	2	c	c	1	0	Y	Y	0	0	0	0	0
5	2	b	b	1	Y	Y	Y	0	0	0	0	0
6	2	c	c	1	0	0	Y	0	0	0	0	0
9	1	b	b	1	0	0	0	Y	0	0	0	0
10	2	b	b	1	0	Y	0	0	0	0	0	0
11	2	b	a	1	0	Y	Y	0	0	0	0	0
12	2	b	b	1	0	Y	0	0	0	0	0	0
13	1	b	a	1	0	Y	0	0	Y	0	0	software + kaartlezer
14	2	b	b	1	0	0	0	0	Y	0	0	nog niet nodig gehad
15	2	b	b	1	0	0	Y	0	0	0	0	0
16	2	b	b	1	0	0	0	0	0	Y	0	0
17	2	c	b	1	0	0	0	0	0	Y	0	0
18	2	b	b	1	0	0	Y	0	0	0	0	0
19	2	a	a	2	0	Y	0	0	0	0	0	0
20	1	b	b	1	0	0	0	Y	0	0	0	0
21	2	b	b	2	0	0	0	Y	0	Y	0	0
22	2	b	b	1	0	0	0	0	0	Y	0	0
23	2	c	c	1	0	0	0	0	0	Y	0	0
24	2	c	c	1	0	0	0	0	0	Y	0	0
25	2	b	a	1	0	Y	0	0	0	0	0	0
26	1	b	a	1	0	0	0	0	0	Y	0	0
27	2	c	b	1	0	0	0	0	Y	0	0	kaartlezer werkt niet
28	2	b	a	1	0	Y	Y	0	0	0	0	0
29	2	b	b	1	0	Y	0	Y	0	0	0	0
30	2	c	c	1	Y	0	0	0	0	0	0	0
31	1	c	a	1	0	0	0	0	Y	0	0	niet nodig gehad
32	1	c	c	1	Y	0	0	0	0	Y	0	0
33	2	b	b	1	0	Y	0	0	0	0	0	0
34	1	c	c	1	0	0	0	0	0	0	Y	0
35	2	b	b	1	0	Y	0	0	0	0	0	0
36	2	b	b	1	0	0	0	Y	0	0	0	0
37	2	b	b	1	0	0	0	0	Y	0	0	omdat er weinig informatie is
38	2	b	b	1	0	0	Y	0	0	0	0	0
39	1	a	a	1	0	0	0	Y	0	0	0	0
40	2	a	a	1	0	0	Y	0	0	Y	0	0
41	2	b	b	1	0	0	0	0	0	0	Y	0
42	2	b	a	1	0	0	Y	0	0	0	0	0
43	2	b	a	1	0	Y	0	0	0	0	0	0
44	1	a	a	2	0	0	0	0	Y	0	0	niet nodig
45	2	b	b	1	0	0	Y	0	0	0	0	0
46	1	b	b	1	0	0	0	Y	0	0	0	0
47	2	c	b	1	0	0	0	Y	0	0	0	0
48	1	b	b	1	0	0	0	0	0	0	Y	0
49	2	a	a	2	0	0	Y	0	0	0	Y	0
50	1	b	b	1	0	0	0	0	0	Y	Y	0
51	2	c	c	1	0	Y	Y	Y	0	Y	0	0
52	2	c	b	1	0	Y	0	0	0	0	0	0