



## **Elektronische handtekening**

### **Vooronderzoek**

**Plaats** Den Haag  
**Datum** Oktober 2002  
**Auteur** Drs. Kristel Lammers  
**Functie** Adviseur Zenc  
**Status** 1.0

### **Stichting Itafit**

Staringstraat 11  
Postbus 525  
6500 AM Nijmegen

T +31[0]24 365 16 60  
F +31[0]24 365 16 70  
I [www.itafit.nl](http://www.itafit.nl)

## Inhoudsopgave

<b>1</b>	<b>Inleiding.....</b>	<b>4</b>
1.1	Itafit.....	4
1.2	Inleiding.....	4
1.3	Opdrachtformulering.....	5
<b>2</b>	<b>De elektronische handtekening .....</b>	<b>7</b>
2.1	Inleiding .....	7
2.2	Algemene beschrijving elektronische handtekening.....	7
	Tabel 1 – Generieke typen elektronische handtekeningen.....	9
	Voorbeeld1 .....	9
2.3	Nederland.....	10
2.4	Onderzoekskader .....	12
2.5	Overzicht landen .....	13
2.5.1	Australië .....	13
2.5.2	Canada.....	14
2.5.3	Duitsland .....	16
2.5.4	Finland .....	18
2.5.5	Frankrijk .....	20
2.5.6	Japan .....	21
2.5.7	Singapore.....	21
2.5.8	Verenigd Koninkrijk .....	23
2.5.9	Verenigde Staten .....	24
2.5.10	Zweden .....	26
2.5.11	Conclusies.....	27
<b>3</b>	<b>Landenoverzicht .....</b>	<b>29</b>
3.1	Inleiding .....	29
3.2	Australië.....	29
3.2.1	Gatekeeper .....	29
3.2.2	ABN-DSC en Angus.....	31
3.2.3	Australian Tax Office.....	33
3.2.4	HIC Online.....	34
3.3	Duitsland.....	35
3.3.1	Elster .....	35
3.3.2	SPINX: Digtale Dienstausweis.....	37
3.3.3	Digitaler Dienstausweis.....	38
3.4	Verenigd Koninkrijk .....	39
3.4.1	Government Gateway .....	39
<b>4</b>	<b>Trends en ontwikkelingen .....</b>	<b>42</b>
4.1	Eén of meerdere handtekeningen.....	42
4.2	Top down of bottom up?.....	43
	<b>Bijlage 1 – Theoretische achtergrond netwerkeffecten .....</b>	<b>45</b>



## 1 Inleiding

### 1.1 Itafit

Itafit is een onderzoeksnetwerk dat zich richt op bestuurlijke vernieuwing en ICT. In het netwerk participeren vertegenwoordigers van de overheid, de IT-branche, organisatie-adviesbureaus, uitgeverijen en universiteiten. Doelstelling van Itafit is om de verspreiding van kennis over bestuurlijke vernieuwing en ICT te bevorderen. Dit gebeurt onder meer door het verrichten van casestudies.

Doel van de casestudies is om vanuit meerdere perspectieven een initiatief te belichten. Door het materiaal in meerdere vormen beschikbaar te stellen, kunnen ook anderen over de merites van initiatieven voor bestuurlijke vernieuwing en ICT discussiëren.

### 1.2 Inleiding

Op het gebied van overheidsinformatiestromen zijn diverse ontwikkelingen gaande. Er is in toenemende mate behoefte aan informatie-uitwisseling tussen overheidsorganisaties onderling, tussen overheid en bedrijfsleven en tussen overheid en burger. Een belangrijke randvoorwaarde voor elektronische communicatie en het elektronisch verlenen van diensten is de zekerheid dat beide partijen akkoord zijn met de gestelde voorwaarden. In het dagelijks leven zetten partijen hiervoor een 'geschreven' handtekening. In de elektronische wereld wordt hiervoor een digitale tegenhanger gebruikt. Eind 1999 is voor de Europese Unie richtlijn nr. 99/93/EG van het Europese Parlement en de Raad tot stand gekomen. Deze richtlijn beoogt het scheppen van een gemeenschappelijk kader voor elektronische handtekeningen binnen de EU. De rol van de nationale overheid als wetgever is beperkt tot het omzetten van de Europese richtlijn in nationale wetgeving (en wel voor 19 juli 2001)<sup>1</sup>. Dit laat onverlet dat nationale overheden in hun rol als uitvoerder en initiator de nodige speelruimte overhouden (ze kunnen bijvoorbeeld zelf handtekeningen gaan uitgeven). Een centrale vraag in dit onderzoek is daarom in hoeverre de beperkte wetgevende autonomie van de lidstaten doorwerkt in hun rol als uitvoerders. Laten deze landen in vergelijking tot landen buiten de EU bijvoorbeeld eerder het initiatief aan marktpartijen<sup>2</sup> of heeft de tussenlaag van de EU geen merkbare invloed op het uitvoeringsbeleid?

---

<sup>1</sup> Nederland heeft de elektronische handtekening nog niet officieel omgezet in nationale wetgeving. De wet op de elektronische handtekening is nog niet door de 1<sup>o</sup> Kamer aangenomen maar de verwachting is dat dit in het voorjaar van 2003 gaat gebeuren.

<sup>2</sup> Een passieve rol van de nationale overheid in de uitgifte van de handtekening laat onverlet dat diezelfde overheid als 'ontvanger' van de handtekening van derden wel een belangrijke rol speelt. Met andere woorden, in het hypothetische geval dat een bedrijf uit een andere lidstaat geaccrediteerd wordt door Brussel zal een Nederlandse overheid die

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

Deze rapportage gaat in op de ontwikkelingen in verschillende landen met betrekking tot de elektronische handtekening. Het onderzoek is een vooronderzoek en heeft een verkennend karakter. Het onderzoek heeft niet tot doel om een uitputtend overzicht te geven van de stand van zaken in de verschillende landen.

### 1.3 Opdrachtformulering

De doelstellingen van het onderzoek luidt als volgt:

- het verkrijgen van een beeld op het terrein van de elektronische handtekening in de volgende landen:
  - Australië
  - Canada
  - Duitsland
  - Frankrijk
  - Finland
  - Japan
  - Nederland
  - Singapore
  - Verenigd Koninkrijk
  - Verenigde Staten
  - Zweden.
- het vinden van patronen van succesvolle benadering voor het inrichten van een elektronische handtekening;
- het verkrijgen van een beeld van de ervaringen met een elektronische handtekening.

#### Vragen

1. Kennen de verschillende landen een elektronische handtekening en wat is de stand van zaken ten aanzien hiervan?
2. Hoe zijn deze voorbeelden georganiseerd op de volgende terreinen:
  - **Organisatorische dimensie:** Hoe wordt de elektronische handtekening (binnen een bepaald project) organisatorisch ondersteund?
  - **Technische dimensie:** Hoe wordt de elektronische handtekening technisch ondersteund (internationaal geaccepteerde standaards)? Van welke beveiligingstechnieken wordt gebruik gemaakt?
  - **Juridische dimensie:** hoe is de elektronische handtekening juridisch verankerd?
3. Welke trends en ontwikkelingen blijken uit de onderzoeksresultaten?

---

elektronische dienstverlening op haar site aanbiedt, deze handtekening zondermeer moeten erkennen en kunnen verwerken.

4. Welke aanpak kan als succesvol worden beschouwd en wat kunnen we hiervan leren?
5. Welke case(s) zou(den) nader onderzocht moeten worden?

#### **Randvoorwaarden en beperkingen**

Gezien de doorlooptijd van het onderzoek (circa 13 weken) en de te investeren tijd, is het onmogelijk om alle initiatieven uitgebreid te beschrijven. De gegevensverzameling van dit onderzoek heeft plaatsgevonden door middel van deskresearch (literatuurstudie) en Internetresearch, aangevuld met gericht vervolgonderzoek per telefoon en email. We richten ons op wat we kunnen vinden aan voorhanden zijnde materiaal. Het onderzoek is afhankelijk van wat we in termen van tijd en capaciteit boven tafel kunnen halen.

#### **Link met ICT en bestuurlijke vernieuwing**

Het project heeft een directe relatie met ICT en bestuurlijke vernieuwing. Het ontwikkelen en implementeren van een elektronische handtekening in de relaties overheid-overheid, overheid-bedrijfsleven en overheid-burger heeft indirecte consequenties voor de manier waarop overheidsorganisaties met hun klanten, partners en leveranciers in contactmomenten omgaan. De elektronische handtekening is een belangrijk instrument om elektronische communicatie tussen bedrijven, overheden en burgers te vergemakkelijken. Het onderzoek is interessant voor iedereen die zich bezighoudt met de ontwikkelingen binnen e-government en de informatiehuishouding van de overheid.

#### **Onderzoeker**

Drs. Kristel Lammers, adviseur Zenc

## 2 De elektronische handtekening

### 2.1 Inleiding

Een onlangs uitgevoerde enquête door ECP.NL<sup>3</sup> toont aan dat er – in potentie – voldoende belangstelling is voor de elektronische handtekening. Driekwart van de ondervraagde personen denkt dat het gebruik op korte termijn zeer sterk zal toenemen. De helft van de ondervraagden denkt zelfs dat over 10 jaar informatie-uitwisseling per e-mail alleen nog maar mogelijk in combinatie met een (vorm van) elektronische handtekening. Uit diezelfde enquête kwam echter ook naar voren dat tweederde van de respondenten momenteel nog geen gebruik maakt van een elektronische handtekening.

De voornaamste reden blijkt te zijn dat hun zakenrelaties hier nog geen gebruik van maken. De achterliggende reden is dat bij het gebruik van elektronische handtekeningen netwerk-effecten optreden<sup>4</sup>. Deze werken in de eerste fases van een diffusietraject averechts en in de latere fases juist versterkend. Op dit moment bevindt het gebruik van elektronische handtekeningen zich klaarblijkelijk nog in de prille fases. Omdat zakenrelaties geen gebruik maken van de elektronische handtekening wordt het niet zinvol geacht om zelf wel een elektronische handtekening te gebruiken.

De patstelling kan doorbreken worden door initiatieven van buiten te ontwikkelen waardoor er genoeg kritische massa wordt gegenereerd om het doorslagpunt te bereiken. In de telecom-sector spelen soortgelijke problemen. Hier proberen de aanbieders van technische infrastructures het gebruik van deze infrastructures van de grond te krijgen door eerst zelf diensten over deze infrastructures aan te bieden, in de hoop dat hierdoor een sneeuwbaaleffect zal optreden en er voldoende momentum op de markt wordt bereikt. Voor het publieke domein zou de overheid met grootschalige PKI-programma's voor een doorbraak kunnen zorgen.

### 2.2 Algemene beschrijving elektronische handtekening

Eind 1999 is de Europese richtlijn nr. 99/93/EG tot stand gekomen betreffende de elektronische handtekening (PbEG L 13). Deze richtlijn heeft tot doel het gebruik van elektronische handtekeningen te vergemakkelijken en tot de

---

<sup>3</sup> ECP heet een enquête gehouden onder haar deelnemers. Voor meer informatie over deze enquête verwijzen wij u naar:

[www.ecp.nl/nieuws/actueel/20020808elek.htm](http://www.ecp.nl/nieuws/actueel/20020808elek.htm)

<sup>4</sup> In bijlage 1 wordt een korte toelichting gegeven bij het theoretische concept van netwerk-effecten.

wettelijke erkenning ervan bij te dragen. De richtlijn zorgt voor harmonisatie in wet- en regelgeving tussen de verschillende landen binnen de Europese Unie<sup>5</sup>.

De richtlijn maakt onderscheid tussen de 'gewone' elektronische handtekening en de 'geavanceerde' elektronische handtekening. Onder de 'gewone' handtekening wordt de uitwisseling van elektronische gegevens verstaan die zijn vastgehecht aan of logisch geassocieerd zijn met ander elektronische gegevens en die worden gebruikt als middel van authenticatie. Hierbij kan bijvoorbeeld worden gedacht aan een ingescande handtekening van een papieren drager. Een 'geavanceerde' elektronische handtekening is een handtekening die:

- op unieke wijze is verbonden aan de ondertekenaar,
- het mogelijk maakt de ondertekenaar te identificeren,
- tot stand is gekomen met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden,
- op zodanige wijze aan de gegevens waarop zij betrekking heeft is verbonden, dat elke wijziging achteraf van gegevens kan worden opgespoord.

De geavanceerde elektronische handtekening is techniekonafhankelijk: ze kan met elke willekeurige techniek worden aangemaakt. Een veel gebruikte techniek is om twee codes te gebruiken die onlosmakelijk met elkaar zijn verbonden: een private en een publieke sleutel. Deze sleutels zijn uniek en horen daardoor bij één persoon. Welke sleutel bij welke persoon hoort wordt door een certificaatdienstverlener (CA), een onafhankelijke derde, vastgelegd in een digitaal certificaat<sup>6</sup>. De betreffende persoon kan elk elektronisch bestand ondertekenen met zijn private sleutel. De ontvanger kan vervolgens dit bestand lezen met de bijbehorende publieke sleutel. De geheimhouding van de private

---

<sup>5</sup> De consequenties van de Richtlijn beperken zich niet tot de EU. In de kleine lettertjes is bepaald dat gekwalificeerde certificaten die zijn afgegeven door CA's buiten de EG/EER *dezelfde* geldigheid hebben als een gekwalificeerd certificaat dat binnen de EG/EER is afgegeven. De CA in kwestie moet dan wel voldoen a) aan de eisen die in de Richtlijn zijn gesteld én beschikken over een door een (kandidaat-)lidstaat afgegeven bewijs van toetsing of b) een CA binnen de EG/EER bereid moet hebben gevonden om voor het certificaat in te staan of c) het certificaat in kwestie moet hebben laten erkennen in het kader van een bilaterale of multilaterale overeenkomst tussen de EU/EER en derde landen of internationale organisaties.

<sup>6</sup> De Europese richtlijn onderscheidt twee soorten certificaten: gekwalificeerde en niet-gekwalificeerde. In het eerste geval worden zowel aanvullende voorwaarden aan het certificaat zelf (Bijlage I Richtlijn) als aan de certificaatverlener (Bijlage II Richtlijn) gesteld. Gekwalificeerde CA's vallen onder een aansprakelijkheidsregeling die verder gaat dan de algemene aansprakelijkheidsregeling (in Nederland geregeld in het ABW). Kort gezet komt de regeling er op neer dat deze CA's aansprakelijk zijn voor de schade die verband houdt met het gebruik van het certificaat *tenzij* ze kunnen bewijzen dat ze niet onzorgvuldig hebben gehandeld.

sleutel is geborgd door kennis (van een code) of bezit (van een smart card of van een specifiek lichaamskenmerk – vingerafdruk of irisscan)<sup>7</sup>.

De gradaties in het certificaat gebruik voor de elektronische handtekeningen worden vaak in drie niveaus weergegeven<sup>8</sup>. In dit onderzoek hanteren we de volgende indeling.

**Tabel 1 – Generieke typen elektronische handtekeningen**

Niveau	Eisen	Voorbeeld1
0	Controle handschrift	Ingescande handtekening
1	Controle emailadres	User ID en password
2	Controle creditcard	Controle credit card
3	Niet-gekwalificeerde CA	<ul style="list-style-type: none"> <li>- Aanmelden bij centrale autoriteit (RA)</li> <li>- Digitale handtekening</li> </ul>
4	Gekwalificeerde CA	<ul style="list-style-type: none"> <li>- Aanmelden bij officieel erkende RA (</li> </ul>
5	Verificatie d.m.v. strikt persoonsgebonden kenmerken	<ul style="list-style-type: none"> <li>- biometrie (US)<sup>9</sup></li> </ul>

Niveau 1 vereist een controle van uw e-mailadres. Niveau 2 voegt daar een controle van de kredietkaart aan toe. Niveau 3 vereist dat de gebruiker zich aanmeldt bij een Registratie-autoriteit ("Registration Authority", RA) voordat hij een elektronisch certificaat kan krijgen. Na controle van de identiteit van de persoon bestelt de Registratie-autoriteit een elektronisch certificaat bij de

<sup>7</sup> Tweede Kamer, vergaderjaar 2000-2001, 27 743, nr.3 pag. 2.

<sup>8</sup> <http://www.cibg.irisnet.be/ci/NL/Departementen/Telemat/Knowhow>

<sup>9</sup> Vanaf volgend najaar zullen de Nederlandse paspoorten worden uitgerust met een chip. Op de chip staan biometrische gegevens. Voor het bezoeken van de Verenigde Staten is een dergelijk paspoort vanaf oktober 2004 verplicht. Bezoekers van de VS moeten een reisdocument kunnen overleggen met daarop de kenmerken van een gelaatsscan, een vingerafdruk of een irisscan. De Nederlandse overheid is al sinds 1998 bezig met de wetgeving die een paspoort met biometrische gegevens mogelijk maakt. Eind vorig jaar werd een onderzoek naar de mogelijkheid van een irisscan-beveiliging in paspoorten afgerond. Onder druk van de nieuwe Amerikaanse wetgeving maakt minister Johan Remkes (Binnenlandse Zaken) nu haast met de invoering van een dergelijk paspoort. Als Nederland volgend jaar nog geen nieuw paspoort heeft, kunnen bezoekers aan de Verenigde Staten gedwongen worden om een 'biometrisch visum' te kopen bij het Amerikaanse consulaat. Of dat daadwerkelijk zal gebeuren is de vraag. De Amerikaanse wet biedt de mogelijkheid om landen die hun nieuwe biometrische paspoort bijna af hebben, uitstel te verlenen (<http://www.webwereld.nl/nieuws/13941.phtml>).

Certificatie-autoriteit ("Certification Authority", CA) en levert deze aan de gebruiker af in de vorm van een chipkaart.

De Europese richtlijnen achten een beveiliging zonder biometrische gegevens (niveau 1-5) voldoende. Er mogen door lidstaten alleen extra veiligheidseisen – zoals het gebruik van biometrische gegevens – worden gesteld als soortgelijke eisen (dwz. identificatie m.b.v. lichaamseigen kenmerken) reeds voor de invoering van de elektronische handtekening werden gesteld.

De Europese richtlijn lijkt te worden ingehaald door de praktijk van de internationale politiek. Na de terroristische aanslagen van 11 september 2001 zijn de normen wat betreft veiligheid in de Verenigde Staten aanzienlijk opgeschroefd. Een van de concrete maatregelen is de verplichting voor bezoekers aan de VS om een paspoort met biometrische gegevens bij zich te dragen. De verplichting geldt vanaf oktober 2004<sup>10</sup>. Bezoekers van de VS moeten een reisdocument kunnen overleggen met daarop de kenmerken van een gelaatsscan, een vingerafdruk of een irisscan. Levert het land van herkomst dat paspoort niet, dan kunnen potentiële bezoekers worden gedwongen om een 'biometrisch visum' te kopen bij het Amerikaanse consulaat.

## 2.3 Nederland

### Organisatorische dimensie

In Nederland heeft de **Taskforce PKIoverheid** een stelstel van gezamenlijke afspraken op bestuurlijk, organisatorisch, juridisch en technisch vlak opgesteld waarmee de betrouwbaarheid van (de handelingen in) elektronische communicatie kan worden gegarandeerd tussen overheid en bedrijven, tussen overheid en burgers en tussen overheid en overheid.

Het Nederlandse PKI-overheid model is hiërarchisch van opbouw. In dit model is er één centraal punt van vertrouwen: het stamcertificaat. Alle elektronische certificaten vallen onder dit certificaat. Vertrouwt men het stamcertificaat, dan kan men alle afgeleide certificaten ook vertrouwen omdat deze op hun beurt zijn afgeleid van het stamcertificaat. In de Wet op de Elektronische Handtekening worden de eisen uit de Richtlijn overgenomen en aangevuld met de volgende 2 punten:

- De elektronische handtekening is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel dd Telecommunicatiewet; en
- De elektronische handtekening is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld is artikel 1.1, onderdeel gg Telecommunicatiewet.

<sup>10</sup> <http://www.webwereld.nl/nieuws/13941.phtml>. Overigens biedt de Amerikaanse wet de mogelijkheid om landen die hun nieuwe biometrische paspoort bijna af hebben (zoals Nederland), uitstel te verlenen.

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

Uitgangspunt van dit stelsel is dat PKI geschikt moet zijn voor het grootste deel van de overheidscommunicatie. Op 17 december 2002 is het stamcertificaat van de Public Key Infrastructure (PKI) voor de overheid officieel gecreëerd. Het gebruik van een elektronische handtekening binnen de Nederlandse overheid is nu mogelijk. De Taskforce PKI heeft in een zwaar beveiligde omgeving van PinkRocade Megaplex het stamcertificaat uitgegeven.

De Taskforce heeft daarmee een gestandaardiseerde en betrouwbare communicatie-infrastructuur opgezet die de volgende betrouwbaarheidsfuncties ondersteunt:

- vaststellen authenticiteit/identificatie;
- vertrouwelijkheid;
- elektronische handtekening<sup>11</sup>.

Deze infrastructuur zal de landelijke uitrol van de elektronische handtekening ondersteunen. De elektronische handtekening voor de communicatie tussen overheid en burger zal achter niet vanuit de overheid worden uitgerold. Dit vanwege de complexiteit van de uitrol en de verwachting dat burgers in haar communicatie met de overheid te weinig gebruik gaan maken van de elektronische handtekening. Voor het genereren van voldoende kritische massa in de eerste fasen van de diffusie van de elektronische handtekening wordt in dit domein gewacht op een initiatief vanuit de private sector, dat wil zeggen door grote leveranciers van hardware (bv. HP/Compaq) en/of software (bv. Microsoft). De uitrol van de elektronische handtekening naar overheidsorganisaties en bedrijven voor de communicatie overheid en overheid en overheid en bedrijfsleven gaat wel onverminderd door.

Hoe deze laatste ontwikkeling, het niet uitrollen van de elektronische handtekening naar burgers, zich verhoudt tot de ontwikkelingen ten aanzien van de e-NIK (de elektronische Nederlandse identiteitskaart) is ons onbekend. De verwachting was dat burgers in 2006 zouden kunnen beschikken over een elektronische identiteitskaart. Op deze kaart zou een certificaat worden opgeslagen. Het PKI-stelsel in combinatie met de e-NIK zou de basis vormen voor een goede elektronische identiteitsinfrastructuur. In het oorspronkelijke plan zou de chipkaart ook worden voorzien van biometrische gegevens. In de vigerende Europese regelgeving zijn dergelijke extra beveiligingsseisen niet toegestaan. De nieuwe Amerikaanse wetgeving (zie hiervoor) lijkt de ontwikkeling van een identiteitskaart annex paspoort met biometrische gegevens (in casu: irisscan) nu opnieuw een duw in de rug te geven<sup>12</sup>.

Op dit moment maken nog tal van overheidsorganisaties gebruik van 'work arounds'. Deze organisaties hebben een 'eigen' elektronische handtekening. Deze elektronische handtekeningen kunnen niet worden beschouwd als een 'geavanceerde' elektronische handtekening omdat ze niet voldoen aan de eisen als gesteld in de Europese Richtlijn. Voorbeelden van organisaties die hier

<sup>11</sup> Het betreft hier het derde niveau.

<sup>12</sup> <http://www.webwereld.nl/nieuws/13941.phtml>.

gebruik van maken zijn: de Belastingdienst die gebruik maakt van een pincode in combinatie met een inlognaam, de IB-Groep die een pilot heeft met pincode en inlognaam via SMS en gemeenten die werken met een combinatie van softnummer en het unieke nummer op het legitimatiebewijs (bijvoorbeeld Amersfoort en Apeldoorn). Voor deze organisaties biedt de 'inferieure' elektronische handtekening voorlopig blijkbaar voldoende waarborgen.

#### **Technische dimensie**

De geavanceerde elektronische handtekening zal zijn gebaseerd op PKI technologie waarbij gebruik wordt gemaakt van twee sleutelparen, een publieke sleutel en een private sleutel.

#### **Juridische dimensie**

Het wetsvoorstel 'Wet elektronische handtekeningen' ligt op dit moment ter goedkeuring bij de Eerste Kamer. De verwachting is dat deze dit voorjaar (2003) zal worden goedgekeurd.

## **2.4 Onderzoekskader**

In dit onderzoek wordt het volgende onderzoekskader gehanteerd. De volgende landen maken deel uit van dit onderzoek: Australië, Canada, Finland, Frankrijk, Duitsland, Japan, Singapore, Zweden, Verenigd Koninkrijk, Verenigde Staten.

De cases zullen in een quick-scan worden beoordeeld op de volgende drie criteria:

**Organisatorisch dimensie:** Hoe is de uitrol van de elektronische handtekening organisatorisch geregeld, welke projecten lopen er of is de elektronische handtekening al volop in gebruik?

**Technische dimensie:** Hoe wordt de elektronische handtekening in technische zin ondersteund?

**Juridische dimensie:** Is er bijvoorbeeld een wet op de elektronische handtekening?

Gekeken wordt in hoeverre deze landen gebruik maken van een (geavanceerde) elektronische handtekening, of er gebruik wordt gemaakt van één handtekening of dat er meerdere initiatieven naast elkaar bestaan.

## 2.5 Overzicht landen

### 2.5.1 Australië

#### Organisatorische dimensie

De ontwikkelingen op het terrein van de elektronische handtekening en breder de identiteitsinfrastructuur worden in Australië met name top-down vormgegeven binnen het Gatekeeper-project, maar Australië kent ook meer bottom-up activiteiten zoals het Argus-project.

In 1997 is de Australische overheid het **Gatekeeper-project**<sup>13</sup> (Commonwealth Governments Gateway PKI Framework) gestart. Dit project richt zich op het ontwikkelen van één nationale authenticatie-infrastructuur waarbinnen overheid en bedrijfsleven hun transacties online kunnen afhandelen. De kern van het Gatekeeper-project is de ontwikkeling van een authenticatieraamwerk, gebaseerd op een CA-model. De elektronische handtekening maakt deel van het PKI-framework. Een zevental overheidsorganisaties heeft een volledige Gatekeeper accreditation gekregen (zie hierna, paragraaf 3.2.1).

Een ander project op het terrein van elektronische handtekeningen dat wordt uitgevoerd onder regie van 'the Commonwealth Government' en dat hieraan direct verwant is, is het **Australian Business Number Digital Signature Certificate (ABN-DSC) project**<sup>14</sup>. Een ABN-DSC is een digitaal certificaat dat is gebaseerd op het Australische bedrijfsnummer. Dit certificaat wordt ontwikkeld door de rijksoverheid, in samenwerking met de provincies<sup>15</sup> en de private sector. Het hoofddoel van het project is om de verdere ontwikkeling van e-commerce te stimuleren. Daarnaast is het gericht op het totstandbrengen van substantiële kostenreducties in de communicatie van (met name kleine) bedrijven met de overheid. Het elektronisch aanbieden van diensten speelt hier een cruciale rol. Overheidsorganisaties maken daarbij gebruik van het ABN-DSC om bedrijven te authenticeren. Dit ABN-DSC mag alleen worden uitgegeven door één van de zeven daartoe gemachtigde organisaties. De 'Office for Government Online' is verantwoordelijk voor de uitvoering van dit project.

Naast dit landelijke initiatief hebben individuele organisaties ook 'home-made oplossingen' voor authenticatie van klanten:

Het **Angus project**<sup>16</sup> behelst de wederzijdse erkenning van digitale certificaten die zijn uitgereikt door de vier grootste banken van Australië (Australia and New Zealand Banking Group Limited, Commonwealth Bank of Australia, National Australia Bank Limited and Westpac Banking Corporation) door de ABN-DSC.

<sup>13</sup> <http://www.ogo.gov.au/projects/publickey/Gatekeeper.htm>

<sup>14</sup> <http://www.noie.gov.au/projects/govt/ABNDSC.htm>

<sup>15</sup> De *States* en *Territories* in Australië kennen een verregaande mate van autonomie.

<sup>16</sup> <http://www.ogo.gov.au/projects/publickey/abn%2Ddsc%2Dangus.htm>

De digitale handtekening die voor banken gebruikt wordt kan nu ook gebruikt worden in communicatie met de overheid. Hierdoor hoeven bedrijven niet langer over meerdere digitale certificaten te beschikken. Het project is wederom gericht op het vergroten van de kritische massa om het doorslagpunt op de diffusiecurve te bereiken<sup>17</sup>.

Naast deze projecten wordt een elektronische handtekening ook gebruikt door het Health Insure via **HIC Online**. HIC Online maakt het mogelijk om online informatie over patiënten te raadplegen ('*Medicare Claiming*'). Medicare is een soort ziekenfondsverzekering en ondersteunt voor universele medische hulp voor iedereen in Australië. HeSA (*Health e-Signature Authority*).

### Technische dimensie

In Australië is de technologie omtrent de elektronische handtekening gebaseerd op PKI-technologie.

### Juridische dimensie

Australië heeft in 1999 de '*Electronic Transactions Act*' aangenomen. Deze wet is gebaseerd op *UNICITRAL model Law on Electronic Commerce*. Binnen het Gatekeeper-project is een PKI-regime ontwikkeld, waaronder een accrediteringsschema voor certificatie autoriteiten (*PKI-scheme*).

## 2.5.2 Canada

### Organisatorische dimensie

Canada is in 1993 gestart met het ontwikkelen van een veilige infrastructuur voor elektronische communicatie voor de publieke sector. Deze inspanning heeft uiteindelijk geresulteerd in de '*Government of Canada (GOV) Public Key Infrastructure* (PKI), die het mogelijk maakt om elektronisch met de overheid te communiceren, zowel voor burgers als voor bedrijven. Daarnaast wordt PKI ook gebruikt in de communicatie tussen ambtenaren onderling, in de interne bedrijfsapplicaties. De elektronische handtekening wordt hier onder andere toegepast om gebruik door onbevoegden tegen te gaan.

Voorbeelden van PKI-toepassingen in Canada tussen overheid-bedrijven kunnen over drie categorieën worden verdeeld:

- **Electronic Customs processing: Customs and Revenue Agency (CCRA)**<sup>18</sup>: '*customs brokers*' spelen een belangrijke rol voor Canadese importeurs. Door dit project kunnen 'brokers' bij het importeren van

<sup>17</sup> Door twee deelpopulaties samen te voegen kan er een versnelling van de diffusie plaatsvinden (ofwel een omslag van het 'pinguin' naar het 'bandwagon' effect – zie Bijlage 1) die anders apart nooit zou zijn bereikt. Het geheel is in dit geval dus veel meer dan de som der delen.

<sup>18</sup> [http://www.cio-dpi.gc.ca/pki-icp/index\\_e.asp](http://www.cio-dpi.gc.ca/pki-icp/index_e.asp)

goederen op eenvoudige wijze online belastingen en provisie betalen aan de CCRA. Voorheen vonden deze activiteiten op papier plaats, waarbij documenten heen en weer gingen tussen 'brokers' en CCRA. Door gebruik te maken van online transacties wordt het proces versneld. Het online transactieproces verloopt via PKI, waarbij gebruik wordt gemaakt van digitale handtekening en encryptie. Deze toepassing is operationeel sinds juli 2000.

- Investing in Canada:
  - **Investment Canada**<sup>19</sup>: *Investment Canada* verleent diensten aan niet-Canadezen die een bedrijf willen starten in Canada. Sinds 1998 is het mogelijk als onderdeel van het online service programma om op een veilige en betrouwbare manier online formulieren in te vullen (*Investment Canada Act applications*). De online service blijkt met name aan te slaan bij advocatenkantoren die regelmatig te maken hebben met investeringsherziening processen in opdracht van buitenlandse investeerders. Om gebruik te maken van de online procedure moet een bedrijf een eerste verzoek voor een 'sleutel' en de benodigde software indienen door middel van een aanvraagformulier bij de *Investment Review Division of Investment Canada*. Nadat het verzoek tot aanvraag is ingediend, controleert de Divisie de informatie en authenticiteit en reikt een CD en gepaste software uit. De klant hoeft dan alleen nog maar zijn sleutel te activeren.
- Spectrum auction:
  - **Radio-veiling**<sup>20</sup>: Bij de veiling van breedbandfrequenties in Canada is PKI ingezet. Hierdoor waren bieders op de frequenties in staat om online betalingen te verrichten, maar ook om op veilige en betrouwbare wijze verklaringen af te leggen en technische gegevens uit te wisselen. Alle veilingen van het spectrum verlopen nu online m.b.v. PKI.

Canada kent de volgende initiatieven binnen de relatie overheid-burger:

- **Passport Online: Department of Foreign Affairs and International Trade**<sup>21</sup>: Op dit moment moet iedere Canadees voor het verkrijgen van een paspoort een aanvraagformulier invullen, een foto toevoegen, (fysiek) worden geïdentificeerd en een handtekening krijgen van een 'guarantor' voor de wettelijke validatie van de foto en van de identiteit van de aanvrager. Hierna kan het aanvraagformulier worden verstuurd of persoonlijk worden overhandigd aan de desbetreffende instantie. Binnen het project Paspoort Online wordt gekeken naar de mogelijkheden om een infrastructuur te ontwikkelen om reisdocumenten online aan te

<sup>19</sup> [http://www.cio-dpi.gc.ca/pki-icp/index\\_e.asp](http://www.cio-dpi.gc.ca/pki-icp/index_e.asp)

<sup>20</sup> [http://www.cio-dpi.gc.ca/pki-icp/index\\_e.asp](http://www.cio-dpi.gc.ca/pki-icp/index_e.asp)

<sup>21</sup> [http://www.cio-dpi.gc.ca/pki-icp/index\\_e.asp](http://www.cio-dpi.gc.ca/pki-icp/index_e.asp)

vragen. Dit is een grootschalig project aangezien het formulier online moet komen te staan, digitale foto's geaccepteerd moeten worden en er een online mogelijkheid moet komen om persoonsgegevens van burgers en ingezetenen te verifiëren en om het paspoort online te kunnen betalen. De elektronische handtekening is hierbij essentieel omdat zowel 'guarantors' als aanvragers zich digitaal moeten kunnen authenticeren.

- **Employment Insurance Appliweb: Human Resources Development Canada<sup>22</sup>**: Canadezen dienen jaarlijks tussen de 2,5 en 3 miljoen declaraties in voor 'Employment Insurance (EI)'. Om deze grote aantallen beter te stroomlijnen is het HRDC op zoek naar een aanpak die de dienstverlening verbetert en de kosten beheersbaar maakt. Appliweb maakt onderdeel uit van deze moderniseringsoperatie. Het EI-formulier wordt daarbij online gezet zodat mensen dit in kunnen vullen wanneer het hen uitkomt. Het formulier kan online worden ingevuld, maar moet vooralsnog worden uitgeprint en opgestuurd. HRDC werkt aan een oplossing die de Canadezen in staat stelt om de documenten elektronisch te ondertekenen. Omdat het hier om een vitale uitkering gaat vraagt dit om een hoog niveau van beveiliging.

#### **Technische dimensie**

Op technisch niveau worden de verschillende initiatieven ten aanzien van elektronische handtekening(en) in Canada ondersteund door PKI.

#### **Juridische dimensie**

Op 30 september 1999 heeft de *Uniform Law Conference of Canada* (ULCC) samen met het *Justice Department* de *Uniform Electronic Commerce Act* (UECA) aangenomen. In deze wet wordt het gebruik van de elektronische handtekening in de communicatie met de overheid ondersteund. Een groot aantal provincies en de federale overheid heeft e-commerce wetgeving geïmplementeerd op basis van de *Uniform E-Commerce Act of the Uniform Law Conference*. De overige provincies zullen op de korte termijn volgen. Hierdoor wordt elektronische communicatie, inclusief de elektronische handtekening, overheidsbreed juridische ondersteund.

### **2.5.3 Duitsland**

#### **Organisatorische dimensie**

Duitsland heeft al enkele jaren ervaring op kunnen doen met elektronisch identificatie. De ontwikkelingen ten aanzien van de elektronisch handtekeningen worden in Duitsland vaak van onderop, door de afzonderlijke overheidsorganisaties geïnitieerd. Duitsland kent geen landelijk aanpak ten

<sup>22</sup> [http://www.cio-dpi.gc.ca/pki-icp/index\\_e.asp](http://www.cio-dpi.gc.ca/pki-icp/index_e.asp)

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

aanzien van PKI/elektronische handtekening. Debet daaraan is het feit dat het koppelen van persoonsgegevens – om historische redenen – bij de grondwet (sic!) verboden is. Omdat er geen nationaal persoonsnummer is, is een PKI systeem waarbij de burger bij alle overheden terecht kan via internet en zich kan identificeren niet aan de orde. Wel kunnen de overheidsdiensten onderling zich online identificeren. Zowel de nationale ministeries, als de Länder, gemeenten en andere overheidsdiensten kunnen allemaal hun eigen certificatie-organisaties hebben. Deze organisaties worden vervolgens weer gecertificeerd door de centrale Policy Certification Authority (PCA-1-Verwaltung)<sup>23</sup>.

In Duitsland lopen er een aantal interessante projecten op het terrein van de elektronische handtekening:

- **Elster-systeem voor aangifte van inkomstenbelasting (elektronische steuererklärung)**<sup>24</sup>: De Duitse belastingwetgeving valt in principe onder de federale wetgeving, al vindt de uitvoering ervan decentraal plaats binnen de 16 Duitse staten. De formulieren en de wettelijke bepalingen zijn echter overal hetzelfde. De eerste experimenten met elektronische belastingaangifte zijn in 1993 van start gegaan in de deelstaat Beieren. Het belastingaangifte programma dat daar is ontworpen, 'ElsterFormular', wordt verstrekt door de overheidsorganisatie. In tegenstelling tot voorheen maken alle Duitse deelstaten gebruik van de Elster software kernel zoals in Beieren ontwikkeld. De aangifte wordt verzonden over een open netwerk, namelijk het Internet. Goede beveiliging is hier bij uitstek van belang. De Belastingdienst maakt gebruik van een elektronische handtekening waarbij een scala aan kaarten met handtekening wordt ondersteund. Hiervoor is een protocol ontwikkeld dat de kaart en handtekening-componenten aan de kant van de gebruiker automatisch herkent (chipkaart, chipkaartlezer, certificaat, driver et cetera. Iedere handtekening-component van elke type kaart en van elk 'trust centre' kan in de toekomst worden ondersteund. Vanaf het midden van 2002 is het mogelijk om de bankpas van een aantal grote banken in Duitsland te gebruiken voor Elster (zie hierna, paragraaf 3.3.1).
- **Digitale Dienstausweis**<sup>25</sup>: Binnen de Duitse overheid loopt een pilot waarbij door 200.000 federale ambtenaren gebruik wordt gemaakt van een elektronische handtekening (*digitale Dienstausweis*) om op een veilige manier onderling met elkaar te communiceren. De e-handtekening is uitgerold naar de hele federale overheid na een succesvolle pilot met een 70 medewerkers van het 'Bündesambtes für Sicherheit in der Informationstechnik (BSI) en 30 medewerkers van het Bundesministerium des Innern (BMI).

<sup>23</sup> Deze centrale Bridge-CA is aanvankelijk opgericht als clearing house tussen Deutsche Telekom AG en de Deutsche Bank, en later is ondersteuning voor zowel publieke als private partijen bewerkstelligd (Bundesministerium für Wirtschaft und Technologie, 2001)

<sup>24</sup> <https://www.elster.de/index.htm>

<sup>25</sup> [http://www.bundesdruckerei.de/de/behoerderservice/3\\_3.html](http://www.bundesdruckerei.de/de/behoerderservice/3_3.html)

- **SPINX:** een ander project van de Duitse overheid is gericht op het garanderen van betrouwbare communicatie via e-mail met behulp van een elektronische handtekening. De elektronische handtekening moet zekerheid bieden dat de oorspronkelijke tekst van de e-mail van de afzender onveranderd is gebleven. Binnen SPHINX wordt geëxperimenteerd met het garanderen van zekerheid van begin tot einde. Arbeidsplaatsen worden daartoe met een chipkaartlezer uitgerust.
- **Signaturcard Niedersachsen<sup>26</sup>:** Het Informatiecentrum Niedersachsen in Hannover heeft in opdracht van het departement van Financiën een systeem ontwikkeld waarmee de medewerkers van de overheid online kunnen communiceren met burgers en bedrijven via een smartcard in combinatie met een elektronische handtekening. De smartcard kan worden gebruikt voor het aanvragen van vergunningen, belastingen, bouwaanvraag, paspoort et cetera.

#### **Technische dimensie**

De basis voor de elektronische handtekening(en) is PKI.

#### **Juridische dimensie**

Duitsland heeft als eerste land de EU richtlijn voor de elektronische handtekening omgezet in een wet die op 1 augustus 1997 in werking is getreden. Deze wet is in mei 2001 vervangen door een nieuwe wet op de elektronische handtekening waarin de infrastructuur voor elektronische handtekening en de rechtsgeldigheid wordt geregeld. Sinds september 1998 is de *national root CA*, de Telecommunicatie & Post CA in Mainz operationeel. Deze nationale root CA is tegelijkertijd een *Bridge CA* wat zoveel inhoudt als dat de certificaat infrastructuur op elkaar worden aangesloten, waardoor een (inter)nationaal netwerk van certificaten kan ontstaan, gebaseerd op internationale standaards. CA diensten zijn verplicht voor het gebruik van de digitale handtekening onder de Duitse wet.

#### **2.5.4 Finland**

#### **Organisatorische dimensie**

Finland heeft al enige jaren ervaring met ontwikkelingen op het terrein van de elektronische handtekening. De eerste experimenten met elektronische identificatie dateren uit 1992. Toen vonden de eerste experimenten plaats in de

---

<sup>26</sup> <http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=20&tsid=222&tid=731&page=0>

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

private sector.<sup>27</sup> In het najaar van 1998 werden de eerste proeven met elektronische identiteitskaarten gestart. De kaarten die in de proeven werden gebruikt zijn uitgerust met drie sleutelparen: één voor het vaststellen van de authenticiteit (via een pincode), één voor de digitale handtekening(en) en één voor versleuteling (encryptie). De sleutels kunnen worden gebruikt om officiële documenten elektronisch te ondertekenen, zoals belastingformulieren en aanvraagformulieren voor sociale zekerheid. In 1999 werd het eerste prototype elektronisch identiteitsbewijs, de FINEID, in gebruik genomen. Finland was hiermee het eerste land ter wereld. De kaart kost momenteel € 29 en is drie jaar geldig en kan worden gebruikt als identificatiemiddel binnen de EU<sup>28</sup>.

Ruim 3 jaar later blijkt dat de kaart nog nauwelijks wordt gebruikt door de Finnen omdat er maar weinig bedrijven zijn die de dienst ondersteunen. Bedrijven nemen op hun beurt een afwachtende houding in omdat het aantal gebruikers gering is<sup>29</sup> (netwerk-effect: zie bijlage 1). Een andere remmende factor zijn de kosten van de benodigde randapparatuur (kaartlezer)<sup>30</sup> en de gecompliceerde installatieprocedure van de software.

Om de adoptie van de FINEID card te stimuleren is er in 2000 een grootschalig project opgezet op een identiteitskaart voor alle studenten in het hoger onderwijs in te voeren. Medio 2002 werd dit FEIDHE-pilot project afgerond. Voornaamste conclusies waren dat het gebruik van kaartlezers en dergelijke nog steeds gecompliceerd is en dat het gebruik van identiteitskaarten op gedeelde terminals (zoals meestal het geval is in een academische omgeving) goede beveiliging van de computers in kwestie vereist. Daarnaast vraagt het gebruik van de pas om een koppeling van alle afzonderlijke accounts van de gebruiker – alvorens de kaart op grote schaal kan worden ingevoerd, moet de gebruikersadministratie eerst gecentraliseerd worden<sup>31</sup>.

### **Technische dimensie**

De Finse elektronische handtekening is gebaseerd op PKI-technologie.

### **Juridische dimensie**

Op 1 december 1993 is de *Act on Electronic Commerce* in werking getreden. Op grond van deze wet is geen handtekening vereist op het moment dat contact

<sup>27</sup> Bijlage 1 Rapportage ICT-toets Pijler E: stand van zaken elektronische overheid-landenstudies, Dialogic/Zenc/Argitek, p.87

<sup>28</sup> <http://www.sahkoinenhenkilokortti.fi/default.asp?todo=setlang&lang=uk>

<sup>29</sup> Linden, Mikael, Kanner, Janne, Kivilompolo, Mika (2001), *FEIDHE (a project): Electronic Identification in Finnish Higher Education*, Tampere: Tampere University of Technology ([https://hstya.funet.fi/docs/FEIDHE\\_project.pdf](https://hstya.funet.fi/docs/FEIDHE_project.pdf))

<sup>30</sup> Ibid.

<sup>31</sup> Linden, Mikael, Linna, Pekka, Kivilompolo, Mika, Kanner, Janne (2002), 'Lessons Learned in PKI Implementation in Higher Education', in: L. Ribeiro et al. (ed.), *Proceedings of the 8<sup>th</sup> International Conference of European University Information Systems (EUNIS)*, Porto: University of Porto/Faculty of Engineering, pp. 246-251.

informatie voorhanden is. Op 1 december 1999 trad de wet op the *Identity Cards* in werking inclusief een amendement waardoor de *Population Registration Center* is aangewezen als CA voor elektronische dienstverlening met de overheid. Op 1 januari 2000 trad de wet *Electronic Service in Administration* in werking, waarin de juridische status van de elektronische handtekening wordt erkend.

### **2.5.5 Frankrijk**

#### **Organisatorische dimensie**

Frankrijk is een laatbloeiër op het gebied van elektronische identificatie. Sinds 2002 is het zowel voor particulieren als bedrijven mogelijk om belastingaangiften en het betalen van belastingen online in te dienen via **Tele-TVA**<sup>32</sup>. De Franse Belastingdienst, *les administrations fiscales Minifi*, heeft daartoe een methode ontwikkeld waarbij gebruik wordt gemaakt van een elektronische handtekening.

Het programma **OPPIDUM** heeft tot doel producten te ontwikkelen op het terrein van veilige internettransacties. Binnen het OPPIDUM programma zijn twee projecten gericht op het ontwikkelen van een digitale handtekening:

- E-GATE
- AUTHENTIS

Hoe deze projecten er voor staan is niet bekend.

#### **Technische dimensie**

De Franse projecten zijn gebaseerd op PKI.

#### **Juridische dimensie**

Sinds 1996 is het gebruik van cryptografie in Frankrijk gelegaliseerd. Hier viel ook het gebruik van de elektronische handtekening onder. Sinds april 2001 is de wet elektronische handtekening echter in werking getreden waarin de rechtsgeldigheid van de elektronische handtekening is geregeld. Door middel van deze wet is de EU richtlijn in Franse wetgeving geïmplementeerd. De rechtsgevolgen van de elektronische handtekening zijn daarmee gelijk gesteld aan die van de schriftelijke handtekening.

---

<sup>32</sup> [http://www.fisc.gouv.fr/espace\\_e\\_services.htm](http://www.fisc.gouv.fr/espace_e_services.htm)

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

## 2.5.6 Japan

### Organisatorische dimensie

In Japan bestaan verschillende initiatieven op het terrein van PKI. Japan heeft sinds 1 april 2001 een wet op de elektronische handtekening en certificatie diensten aangenomen. Het ministerie van Justitie werkt aan het opzetten van een framework voor elektronische handtekeningen. De Japanse overheid, zowel federaal als lokaal moet voor 2003 een systeem hebben om op elektronische wijze transacties met burgers en bedrijven af te kunnen handelen. Om de veiligheid te kunnen garanderen moeten 'secure administration IC' (identiteitskaarten) worden uitgegeven aan burgers. Deze kaarten moeten worden voorzien van een elektronische handtekening.<sup>33</sup> Japan werkt aan een overheidsbrede infrastructuur, inclusief authenticatie en elektronische handtekening, om op veilige wijze elektronisch met burgers/bedrijven te kunnen communiceren. Dit project wordt de ministeries MPHTP, EPO en JPO gezamenlijk opgepakt.

### Technische dimensie

De elektronische handtekening is gebaseerd op PKI.

### Juridische dimensie

Op 1 april 2001 is de *Law Concerning Electronic Signatures and Certification Services Act* in werking getreden. Daarnaast heeft de Japanse overheid een wet aangenomen die betrekking heeft op het gebruik van elektronische documenten binnen commerciële transacties. Er wordt inmiddels ook gewerkt aan een elektronische identiteitsinfrastructuur.

## 2.5.7 Singapore

### Organisatorische dimensie

Singapore is een sterk centralistische staat, waarin ontwikkelingen binnen de overheid traditioneel top-down worden ingegeven<sup>34</sup>. De elektronische handtekening wordt toegepast door enkele (commerciële) banken en daarnaast door beurshandelaren en overheidsorganisaties zoals *Integrated Land Information System by the Ministry of Law*, *CPF PAL Internet Online system*, *the Ministry of Defence*..

Op dit moment maken overheidsorganisaties, zoals het **Central Provident Fund** (CPF) gebruik van een combinatie van een uniek nummer met een 8-cijferige pincode (vergelijk de systemen in Apeldoorn en Amersfoort). Het CPF is

<sup>33</sup> [http://www.kantei.go.jp/foreign/it/network/0122full\\_e.html](http://www.kantei.go.jp/foreign/it/network/0122full_e.html)

<sup>34</sup> De schaal van het land leent zich uiteraard ook voor centrale sturing.

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

verantwoordelijk voor sociale zekerheid (pensioenen, werkloosheidsuitkeringen) en voor ziektekosten en onderwijsuitkeringen. In de loop van de tijd is het CPF uitgegroeid tot het Singaporese sociale zekerheidsvangnet. Via het **PAL-PIN nummer** (Personal Auto-Link Personal Identification Number) kunnen de Singaporezen online transacties verrichten. Naast de CPF PAL-PIN (een 8-cijferig nummer) is een CPF account nummer vereist. Dit CPF account nummer is gelijk aan het NRIC nummer (*National Registration Identity Card nummer*).

Het **Singapore Computer Emergency Response Team (SingCERT)** is verantwoordelijk voor veilige en betrouwbare elektronische transacties binnen de één-loket gedachte, waarmee wordt bedoeld dat diensten zo veel mogelijk geïntegreerd via één loket worden afgehandeld over een betrouwbare en veilige infrastructuur. SingCERT is een van de keyprogramma's van de *Information Development Authority (IDA)*.

#### **Technische dimensie**

De meest gehanteerde vorm van de elektronische handtekening, de PAL-PIN is gebaseerd op een pincode in relatie tot een uniek nummer. Deze technologie wordt op grond van de Europese richtlijn niet erkend als de 'geavanceerde' elektronische handtekening maar blijkt in de praktijk goed te werken.

#### **Juridische dimensie**

Singapore is een van de meest vooruitstrevende landen op het gebied van e-government. In 1998 is de '*Electronic Transactions Act*' aangenomen. Deze wet maakt online dienstverlening mogelijk en ondersteunt de elektronische handtekening. De formulering in de wet is technologie-onafhankelijk. In 1999 is wetgeving ten aanzien van de elektronische handtekening vastgelegd in '*Electronic Transactions (Certification Authority) Regulations*'. Overheidsorganisaties zijn verplicht om elektronische formulieren te accepteren. Burgers kunnen via de CA registreren voor een elektronische handtekening.<sup>35</sup> CA kunnen zich vrijwillig laten registreren als officieel erkende CA.

Op grond van de volgende eisen wordt de elektronische handtekening wettelijk erkend als een betrouwbare elektronische handtekening indien<sup>36</sup>:

- ze op unieke wijze is verbonden aan een persoon;
- ze het mogelijk maakt die persoon te identificeren;
- het gebruik slechts plaatsvindt met middelen die de ondertekenaar onder zijn exclusieve controle kan houden; en
- ze is op zodanige wijze is verbonden aan het elektronisch document waarop het betrekking heeft dat elke wijziging van een gegeven leidt tot ongeldigheid van de elektronische handtekening.

---

<sup>35</sup>

<http://www.ida.gov.sg/website/IDAContent.nsf/14899db7846d2bcc482568360017c696/9ee41fd04e0d105fc825683900020047?OpenDocument>

<sup>36</sup> *Electronic Transactions Act*.

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

Deze eisen lijken sterk op de eisen die worden gesteld aan de geavanceerde elektronische handtekening in de Europese richtlijn.

### 2.5.8 Verenigd Koninkrijk

#### Organisatorische dimensie

Ontwikkelingen ten aanzien van de elektronische handtekening worden in de UK met name top-down ingegeven. De overheid heeft een grootschalig project opgezet (*Government Gateway*) om PKI – waaronder het gebruik van de elektronische handtekening – uit te rollen.

Via de **Government Gateway** kunnen burgers, bedrijven en tussenpersonen zich registreren voor online overheidsdiensten. De *Government Gateway* ondersteunt eenzijdige<sup>37</sup> authenticatie van burgers, bedrijven en tussenpersonen met overheid<sup>38</sup>. Voorbeelden van toepassingen van de *Government Gateway* zijn:

- **PAYE year end filing for businesses and agents** (*Inland Revenue*); werknemers, tussenpersonen en loonadministratie kunnen via het Internet in combinatie met een digital certificaat of us- id met password na aanmelding bij *Government Gateway*.
- **Online VAT returns** (*HMC&E*); bij het *department of HM Customs and Exercise* kan een aantal diensten online worden afgehandeld waaronder de BTW-aangifte. Hiervoor is een digitaal certificaat vereist.
- **IACS<sup>39</sup> Area Aid Applications** (*Department of Environment, Food & Rural Affairs*);
- **DVLA**: electronic vehicle licence registration.

#### Technische dimensie

Op dit moment wordt gebruik gemaakt van twee methoden:

- de combinatie tussen een digitaal certificaat in combinatie met een password. Deze combinatie vormt samen een elektronische handtekening en staat gelijk aan de handgeschreven handtekening. Het digitale certificaat is te verkrijgen bij Equifax en Chambersign. Met dit

<sup>37</sup> Met eenzijdige authenticatie wordt bedoeld dat de overheid wel burgers, bedrijven en tussenpersonen controleert op identiteit en authenticiteit, maar dat burgers, bedrijven en tussenpersonen deze mogelijkheid niet hebben jegens de overheid.

<sup>38</sup> Men kan ook inloggen op *Gateway* door gebruik te maken van de diensten van een van de drie commerciële PKI aanbieders, die samenwerken met de *Government Gateway*. Dit zijn *ChamberSign*, *Equifax* en *BT Trust Services*, of een van de overheidsdepartementen die digitale handtekeningen uitdelen. De *Government Gateway* laat beveiligde, geautoriseerde transacties toe tussen burger en overheid via het web (*E-envoy*, 2002).

<sup>39</sup> *Integrated Administration and Control System*

digitaal certificaat kan de burger zich aanmelden voor elektronische diensten bij de *Government Gateway*.

- De combinatie van user ID met password (vergelijk Singapore). Dit is een lager niveau van beveiliging, maar voldoende voor de meeste overheidsdiensten. Hiervoor dient een burger, bedrijf of tussenpersoon zich via *de Government Gateway* aan te melden. Online verschijnt het user ID in beeld. Binnen 7 dagen wordt een bevestiging per post verstuurd. Voor elke afzonderlijke dienst moet worden geregistreerd. Hiervoor ontvang je een pincode via de post binnen 7 dagen.

De combinatie van digitaal certificaat of user ID met password wordt gezien als een elektronische handtekening en is rechtsgeldig<sup>40</sup>.

### **Juridische dimensie**

De Electronic Communications Bill is op 25 mei 2000 in werking getreden, ruim voor de Europese Richtlijn. Door deze wet is een groot deel van de eisen van de richtlijn al geïmplementeerd. Deze wet maakt elektronische communicatie met de overheid mogelijk, doordat de wet de elektronische handtekening erkend. Onlangs is een root CA (HMG Root Authority) ingesteld. Alles zal via deze root authority worden gecertificeerd. Nederland heeft met de UK afspraken gemaakt over het onderlinge gebruik van PKI-toepassingen.

### **2.5.9 Verenigde Staten**

#### **Organisatorische dimensie**

Ontwikkelingen in de US worden vaak bottom-up, door de commerciële sector ingegeven. Zo ook de ontwikkelingen ten aanzien van de elektronische handtekening. Tal van initiatieven bestaan er op dit terrein, bij banken, overheidsorganisaties e.d. De federale overheid probeert daar nu uniformiteit in te creëren.

Er loopt een federaal project **ACES**<sup>41</sup> (*access certificates for electronic services*) dat ervoor moet zorgen dat de bestaande PKI-oplossingen dichter bij elkaar worden gebracht, waardoor een 'web of trust' kan ontstaan. Dit federale project wordt getrokken door de *Federal PKI Policy Authority* (FPKIPA) in samenwerking met de *Federal Bridge Certification Authority* (FBCA)<sup>42</sup>. De FBCA is sinds 7 juni 2001 operationeel. De FBCA zorgt voor interoperabiliteit tussen de verschillende public key infrastructures van de aangesloten overheidsorganisaties. Hierdoor kunnen certificaten onderling worden uitgewisseld.

---

<sup>40</sup> Vergelijk de situatie in Singapore.

<sup>41</sup> [www.gsa.gov/aces](http://www.gsa.gov/aces)

<sup>42</sup> <http://csrc.nist.gov/pki/fbca/welcome.html>

PKI, waaronder de elektronische handtekening voor authenticatie wordt o.a. door de volgende overheidsorganisaties gebruikt<sup>43</sup>:

- Department of Agriculture/National Financial Center: online aanvragen voor RDA en FSA;
- Department of Labor/Bureau of Labor Statistics: Centralized Internet Data Collection facility;
- Department of Commerce/NITS: elektronisch invullen van circa 200 formulieren door medewerkers van de NITS;
- Department of Commerce/USPTO: vanuit binnen- en buitenland kan gebruik worden gemaakt van het registeren van patenten;
- Department of Defense;
- Department of Energy;
- Environmental Protection Agency;
- NASA;
- Department of Health and Human Services: HHS;
- NRC;
- Social Security Administration;
- Department of FFA;
- Department of Treasury;
- USITC;
- Department of VA.
- 

#### **Technische dimensie**

De elektronische handtekening is gebaseerd op PKI-technologie.

#### **Juridische dimensie**

In het kader van de *Government Paperwork Elimination Act*, moeten steeds meer transacties online plaats vinden waaronder tussen overheid en burgers/bedrijven.

De elektronische handtekening is door tal van staten binnen de Verenigde Staten in meer of mindere mate erkend. Staten hebben hierin enige vrijheid. 46 van de 50<sup>44</sup> staten hebben één of meerdere wetten ten aanzien van een elektronische handtekening aangenomen<sup>45</sup>.

---

<sup>43</sup> <http://www.cio.gov/fpkipa/documents/pki-brochure.pdf>

<sup>44</sup> Geen wetgeving hebben: Michigan, New Jersey and South Dakota

<sup>45</sup> Er is geen uniforme wet die voor alle staten binnen de Verenigde Staten geldt. Op zichzelf hoeft dit geen probleem te zijn. In de praktijk is het mogelijk dat elke staat een eigen standaard kiest.

### 2.5.10 Zweden

#### Organisatorische dimensie

Ontwikkelingen ten aanzien van de elektronische handtekening vinden bottom up plaats. Er zijn nog niet veel voorbeelden te vinden van het gebruik van de elektronische handtekening. De volgende private organisaties maken gebruik van een elektronische handtekening:

- Government e-Link;
- F-secure;
- Telia elektroniska ID-kort standard.<sup>46</sup>

De Zweeds en Engelse overheid willen samen met het bedrijfsleven werken aan de Europese IT Strategie zoals opgesteld door de Europese Unie, waar de elektronische handtekening deel van uit maakt. Dit om de interoperabiliteit van de elektronische handtekening tussen de verschillende EU-landen te vergroten. Een bedrijf met een geldige elektronische handtekening in Zweden kan bijvoorbeeld deze handtekening niet gebruiken in haar communicatie met landen buiten Zweden doordat er andere standaards worden gebruikt of doordat de CA en dus ook de handtekening niet wordt erkend.

#### Technische dimensie

De elektronische handtekening is gebaseerd op PKI.

#### Juridische dimensie

De Zweedse overheid heeft op 18 mei 2000 een voorstel ingediend voor de erkenning van de elektronische handtekening (2000:832) die de Europese Richtlijn implementeert. Deze wet is op 1 januari 2001 in werking getreden. Daarvoor werd de elektronische handtekening echter al vaak de facto erkend. De de jure erkenning van de elektronische handtekening kan wellicht bijdragen aan het vertrouwen van burgers in e-commerce. Het Zweedse ministerie van Industrie, Werkgelegenheid & Communicatie '*Näringsdepartementet*' is belast met de elektronische handtekening.<sup>47</sup> Het *National Department of Post en Telecommunications* treedt op als root CA. De distributie van PKI vindt decentraal plaats via de *Swedish National Tax Board, Social Insurance Office, Patent and Registration Board and Statskontoret*. Er wordt een onderscheid gemaakt in 3 typen certificaten: hoog, midden, laag waarvan het certificaat hoog overeenkomt met de eisen zoals gesteld in de EU richtlijn, midden overeenkomt met het '*sign on*' principe waarbij gebruik wordt gemaakt van private key software en laag overeenkomst met een User ID en paswoord.

---

<sup>46</sup> Telia maakt gebruik van een elektronische handtekening in combinatie met een chipcard bij het betalen van facturen via het internet.

<sup>47</sup> <http://www.naring.regeringen.se/fragor/it/esign.htm>

### 2.5.11 Conclusies

Uit de bovenstaande quick scan kunnen voorlopig de volgende conclusies worden getrokken:

- Er wordt nog weinig gewerkt met **de** geavanceerde elektronische handtekening. Er moet eerst een noodzaak zijn of een praktisch nut wil de burger, het bedrijf of de medewerker van een overheidsorganisatie de elektronische handtekening ook daadwerkelijk gaan gebruiken. Daarnaast heeft men wellicht angst voor het nieuwe. Ook is het minimale gebruik van de geavanceerde elektronische handtekening te wijten aan het feit dat de meest standaard (e-mail) software het gebruik van elektronische handtekeningen en elektronische certificaten (nog) niet ondersteund.
- In alle landen worden meerdere elektronische handtekeningen naast elkaar gebruikt: 'geavanceerde' en 'gewone' elektronische handtekeningen. Er is niet zoiets als één (inter)nationale elektronische handtekening. Wel zien we dat er wordt gewerkt aan de interoperabiliteit van de verschillende handtekeningen.
- Bottom up ontwikkelingen, vanuit de verschillende overheidsorganisaties, lijken meer vruchten af te werpen, dan de zware topdown PKI-overheidsprogramma's.
- De 'gewone' elektronische handtekening blijkt in tegenstelling tot de 'geavanceerde' elektronische handtekening eenvoudiger te zijn in gebruik en lijkt daardoor eerder succesvol te zijn: zie bijvoorbeeld de pincode-combinatie van de Singaporese overheid, de pincode oplossing binnen de Britse Gateway, de pincode van de Nederlandse Belastingdienst et cetera.

**Tabel 2 – Internationaal overzicht elektronische handtekening (eind 2002)**

	Nederland	Australië	Canada	Duitsland	Finland	Frankrijk	Japan	Singapore	Verenigd Koninkrijk	Verenigde Staten	Zweden
<i>Organisatie</i>											
Top-down/centraal	X	X	X		X	X	X	X	X		
Bottom-up/decentraal		X		X	X		X			X	X
<i>Veiligheidsniveau</i>											
1											
2	A	C	E	F					J	K	L
3	B		D		G			H	I		
<i>Subdomein</i>											
G2C		X	X	X	X			X	X	X	X
G2B	X	X	X	X				X	X	X	X
G2G	X	X		X				X	X		
<i>Diffusie</i>	--	0	-	0	--	--	--	0	0	-	-

Legenda:

A belastingdienst, gemeente Apeldoorn, gemeente Amersfoort

B PKI Overheid, gereed december 2002

C Gatekeeper, ABN-DSC, Angus, HIC Online: overgang naar niveau 3 in gang gezet

D CCRA (in toekomst ook passport online en HRDC)

E Investment Canada, Radio-veiling

F Elster, Sphinx, Signaturcard Niedersachsen (bezig met overgang naar fase 3)

G Fineid

H Central Provident Fund

I Government Gateway, Online VAT

J Government Gateway Paye, IACS, DVLA

K ACES en andere projecten: niveau 2 met overgang naar niveau 3 voor ACES

L Government e-Link, F-secure, Telia elektroniska ID-kort standard: Government e-link overgang naar 3 beoogt.

Uit de korte beschrijvingen lijken de volgende drie landen voor dit onderzoek het meest interessant:

- *Australië*: vanwege de enkele jaren ervaring, de interessante projecten en het omzetten van een bottom-up aanpak in één centrale e-identiteitsinfrastructuur;
- *Duitsland*: vanwege de landelijke uitrol van het SPHINX-project;
- *Verenigd Koninkrijk*: vanwege het grootschalige Gateway-programma.

## 3 Landenoverzicht

### 3.1 Inleiding

In dit hoofdstuk zullen 3 landen, Australië, Duitsland en het Verenigd Koninkrijk uitvoeriger worden beschreven. Een elektronische handtekening kan worden gebruikt binnen e-mail, Internet transacties, Internetpagina's, EDI transacties et cetera. Binnen deze landen zal uitvoering aandacht worden besteed aan de volgende aspecten:

- Organisatie
- Techniek
- Juridisch

### 3.2 Australië

Australië kent een Commonwealth brede strategie ten aanzien van PKI ontwikkelingen waaronder de elektronische handtekening. Ontwikkelingen worden vanuit deze strategie vaak top down ingegeven. Australië kent echter ook een aantal interessante initiatieven die vanuit overheidsorganisaties zelf vorm hebben gekregen zoals het hieronder beschreven project van ATO en Angus. Een van de belangrijkste uitdagingen in Australië is het zorgdragen voor interoperabiliteit tussen de verschillende afzonderlijke overheidsactiviteiten.

#### 3.2.1 Gatekeeper

##### Organisatorische dimensie

Gatekeeper<sup>48</sup> is de Commonwealth strategie op het gebied van PKI. De basis voor de Gatekeeper strategie is terug te vinden in de verklaring *'Investment for Growth'* die de minister-president in 1997 uitsprak. In de verklaring wordt de noodzaak aangegeven voor een nationale public key technology (PKT) framework om het vaststellen van de authenticiteit van gebruikers van online diensten te kunnen waarborgen. Als reactie hierop werd in 1998 de *'Gatekeeper-strategy for public key technology use in the Government'* van kracht. Op basis van deze strategie moet een infrastructuur worden geïmplementeerd die overheidsorganisaties integriteit, authenticiteit en veiligheid biedt bij informatie-uitwisseling en transacties met bedrijven. Gatekeeper certificaten en elektronische handtekeningen worden in toenemende mate gebruikt door Commonwealth organisaties in het elektronisch verkeer om de integriteit, authenticiteit, vertrouwelijkheid en non-repudiatie te kunnen garanderen.

---

<sup>48</sup> <http://www.govonline.gov.au/projects/publickey/Gatekeeper.htm>

Het Gatekeeper project moet bijdragen aan een gunstig klimaat voor e-commerce, voor het uitwisselen van overheidsinformatie en voor inkopen van diensten door de overheid. Het Gatekeeper project was oorspronkelijk opgezet om alleen de accreditatie van service providers met betrekking tot elektronische handtekening applicaties voor overheidsorganisaties te ondersteunen. Gatekeeper is gebaseerd op nationale en internationale standaards. Met de overheidsbrede erkenning van de digitale handtekening<sup>49</sup> uit het Angus/Identrus-project (financiële sector) is het Commonwealth accreditatieschema ook opengesteld voor de private sector. Het Gatekeeper project garandeert daarmee 'trust' in de relatie overheid-bedrijf en zelfs bedrijf-bedrijf. Dit is van groot belang voor het succes van de elektronische handtekening. Met name in de volgende sectoren lijkt behoefte te zijn aan een hoogwaardige authenticatie-standaard:

- Overheid;
- Financiële sector;
- Gezondheidssector.

In alle drie de sectoren wordt persoonsgevoelige informatie gebruikt.

Binnen de overheid maken de Australian Tax Office (ATO) en de the Health Insurance Commission (HIC) gebruik van een elektronische handtekening. Daarnaast zit nog een aantal andere overheidsorganisaties in een pilotfase. De ATO accepteert de electronic logment of Business Activity Statements en de HIC maakt gebruik van de elektronische handtekening via de Health E-Signature Authority (HeSA). Andere overheidsorganisaties zoals de Australian Customs Service (ACS) en the Department of Defence werken op dit moment aan een uitrol van een elektronische handtekening. Op statenniveau maakt de Victoria's Transport Accident Commission (TAC) gebruik van de ABN-DSC. Hierdoor kan zij online een goed alternatief bieden voor de 2000 brieven en de 700 faxen die zij dagelijks ontvangt.

In haar communicatie met bedrijven maakt de overheid gebruik van het digitale ABN certificaat (zie ook paragraaf 3.2.2.) waarbij gebruik wordt gemaakt van een unieke ABN digitale handtekening in combinatie met een '*universal business identifier*'. Het ABN-DSC concept zorgt ervoor dat bedrijven slechts over één certificaat hoeven te beschikken in hun communicatie met de overheid.

Zeven organisaties hebben een volledige Gatekeeper accreditatie, wat wil zeggen dat zij bevoegd zijn tot het uitgeven van '*digital signature certificates*'. Deze organisaties zijn:

- PricewaterhouseCoopers (beTRUSTed): ABN-DSCs;
- Australia Post: Registered Authority;
- Telestra Corporations Limited: ABN-DSCs;
- eSign Australia Limited: ABN-DSCs;

---

<sup>49</sup> Een digitale handtekening is een elektronische handtekening gebaseerd op een Private Key Signature. Voor de Private Key Signature wordt vaak van PKI gebruik gemaakt.

- Health eSignature Authority Pty LTD: Registerd Authority extended services;
- Baltimore Certificates Australia Pty LTD (CAPL): Certification Authority;
- Australian Taxation Office: Certification Authority, Registration Authority.

Daarnaast hebben negen organisaties onlangs een aanvraag ingediend voor een officiële Gatekeeper accreditatie. Hierover is nog geen besluit genomen. De Australische aanpak kent geen root authority.

Andere sectoren lijken niet of nauwelijks behoefte te hebben aan een dergelijke geavanceerde oplossing – zij kunnen uit met een lager beveiligingsniveau. Zowel vanuit het perspectief van de overheid als vanuit het perspectief van de burger en het bedrijfsleven lijkt de toepassing van meerdere niveaus dan ook wenselijk.

#### **Technische dimensie**

De Australische PKI standaards zijn gebaseerd op internationale standaarden op het terrein van Public Key Infrastructure. Het *Standards Australia Committee IT/12/4/1* is verantwoordelijk voor de ontwikkeling van Public Key Authentication Framework (PKAF) gerelateerde standaards. De *Australian Standard 4539* heeft betrekking op de PKAF en bestaat uit de volgende delen:

- AS4539.1.1 (working draft) General-PKAF architecture
- AS4539.1.3 (published) General-X.509 supported algorithms profile
- AS4539 1.2 (at public comment) General-X.509 certificate and CRL profile
- AS4539.2.1 (working draft) A framework for assurance of Certification Authorities
- AS4539.XX (new work item) Registration-Identification and authentication
- AS4539.XX (new work item) Registration-Selected Identification Items

#### **Juridische dimensie**

Er is geen specifieke juridische basis voor het Gatekeeper-project. Gatekeeper is in principe een louter administratieve aangelegenheid. De '*Electronic Transactions Act 1999*' is van toepassing op alle elektronische transacties.

### **3.2.2 ABN-DSC en Angus**

#### **Organisatorische dimensie**

Het **Australian Business Number-Digital Signature Certificate (ABN-DSC)**<sup>50</sup> concept is ontwikkeld om tegemoet te komen aan de wens van de Australische overheid om op grote schaal digitale certificaten te gaan gebruiken die gebaseerd zijn op het ABN. Dit om online transacties tussen overheid-bedrijf en

<sup>50</sup> <http://www.govonline.gov.au/projects/publickey/abn-dsc.htm>

tussen bedrijf-bedrijf te vergemakkelijken. Dit project kwam naar voren uit het 'tax reform program' en de ontwikkeling van een ABN. HET ABN-DSC is een digitaal certificaat dat is gekoppeld aan een entiteit, in dit geval het ABN. Het ABN-DSC kan worden verkregen bij elke door de Gatekeeper geaccrediteerde CA. 'Commonwealth agencies' kunnen het certificaat gebruiken voor het identificeren van bedrijven bij online transacties. Het ABN-DSC is in beginsel ontwikkeld voor de communicatie tussen overheid-bedrijf. De overheid wil echter niet dat bedrijven verschillende certificaten moeten hebben om met de overheid en met andere bedrijven te kunnen communiceren en biedt daarom inmiddels 'one online identity' aan bedrijven aan. Deze ontwikkeling staat niet op zichzelf maar kent een eigen geschiedenis.

In december 1999 heeft de Australische overheid besloten om het ABN-DSC te gebruiken voor de Commonwealth overheid in den brede. Een volgende stap was de interoperabiliteit van het ABN tussen de Commonwealth overheid en de States en Territories. In november 2000 is de ministeriële bijeenkomst van de Online Council, States and Territories akkoord gegaan met de Gatekeeper strategie en daarmee met het feit dat ABN-DSC certificaten uitgegeven door de State/Territory agency worden geaccepteerd door de Commonwealth agencies en vice versa. Tot slot is deze 'one online identity' voor de overheid ook nog uitgebreid naar de private sector. Sinds eind 2001 worden digital signature certificates die uitgegeven zijn door de Australische banken ook geaccepteerd door alle Commonwealth overheidsorganisaties. Deze certificaten zullen worden beschouwd als ABN-DSC digital certificates. Dit is in maart 2001 besloten door de overheid. De basis hiervan ligt in het Angus-project.

Het **Angus-project** is van oorsprong een werkgroep bestaande uit de vier grote banken van Australië (zie hieronder), die zichzelf tot doel had gesteld het ontwikkelen van een framework voor e-commerce, gebaseerd op vertrouwen en authenticatie. Dit framework zou worden gebaseerd op het internationale Identrus TM schema. De Identrus infrastructuur is primair ontwikkeld om de groei van Business-Business e-commerce te faciliteren. Deze infrastructuur is toegankelijk voor alle financiële instituties, hun klanten en 'security vendors' overal ter wereld. Het 'Gatekeeper scheme' wordt hiervoor gekoppeld aan Identrus. Vier Australische banken hebben een volwaardige Gatekeeper accreditatie als Registration Authority (RA). Dit zijn de volgende vier banken:

- Australia and New Zealand Banking Group Limited;
- Commonwealth Bank of Australia;
- National Australia Bank Limited;
- Westpac Banking Corporation.

Angus organisaties kunnen pas officieel Gatekeeper certificaten verstrekken nadat ze geaccrediteerd zijn op grond van het Identrus schema. De Australische overheid en het bedrijfsleven hoopt dat door het aanbieden van de mogelijkheid van een 'single online identity' welke meervoudig kan worden gebruikt, de technologie sneller zal worden geïmplementeerd in de bestaande bedrijfsvoeringsprocessen. Hier speelt wederom het motief van het genereren van een kritische massa.

### **Technische dimensie**

Het digital signature scheme van Angus (Identrus) is gebaseerd op nationale en internationale standaards. Dit geldt zowel voor Gatekeeper als voor Angus. De banken maken gebruik van faciliteiten die Gatekeeper compliant zijn, wat betekent dat de certificaten alleen worden uitgegeven door een Gatekeeper geaccrediteerde organisatie gebaseerd op een geaccrediteerd en geëvalueerd digitaal certificaten schema dat wederzijds is erkend (cross recognition) door Gatekeeper.

### **Juridische dimensie**

De juridische basis voor het ABN-DSC is net als voor Gatekeeper de '*Electronic Transactions Act 1999*'.

### **3.2.3 Australian Tax Office**

#### **Organisatorische dimensie**

De ATO was de eerste overheidsorganisatie in Australië die met PKI via de Electronic Commerce Interface (ECI) online transacties ondersteunde. Deze ontwikkeling vloeide direct voort uit het Australische belastingherzieningsbeleid<sup>51</sup>. Het belastingherzieningsbeleid heeft geresulteerd in een '*new tax system*' waarbij bedrijven en non-profit organisaties o.a. online met behulp van een elektronische handtekening belastingtransacties kunnen verrichten. De elektronische handtekening voor bedrijven is momenteel gebaseerd op het ABN-nummer en gebaseerd op de Gatekeeper strategie. Dit was oorspronkelijk nog niet zo, doordat het Gatekeeper initiatief van een latere datum was dan de ECI. De ATO Organisation Certification Authority (OCA) was de eerste officiële Gatekeeper CA. De ATO heeft op dit moment meer dan 70.000 certificaten uitgereikt. Dit certificaat kan worden gebruikt bij het elektronisch indienen van een verzoek tot belastingteruggave.

#### **Technische dimensie**

Voor het online zakendoen met de ATO moet de Electronic Commerce Interface software zijn geïnstalleerd op de PC. Deze software kan worden gedownload van de ATO site of van de ECI cd die ieder bedrijf heeft ontvangen. Om de software te kunnen installeren moet een bedrijf in het bezit zijn van digitale certificaten en sleutels die gekoppeld zijn aan de 'ondertekenaar' van de entiteit 'bedrijf'. De digitale sleutels (voor authenticatie en encryptie) en certificaten fungeren vervolgens als een 'digitale handtekening' en garanderen daarmee veiligheid in de communicatie met de ATO.<sup>52</sup> Het ATO-stelsel is gebaseerd op Gatekeeper PKI. De private sleutel is beveiligd door middel van een password. Op deze manier kan een geautoriseerd individu binnen een bedrijf online transacties

<sup>51</sup> <http://www.taxreform.ato.gov.au/>

<sup>52</sup> [http://www.ato.gov.au/esd/about\\_eci/31about\\_eci.htm](http://www.ato.gov.au/esd/about_eci/31about_eci.htm)  
[http://www.ato.gov.au/esd/about\\_eci/321about\\_pki.htm](http://www.ato.gov.au/esd/about_eci/321about_pki.htm)

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

verrichten met ATO. De geldigheid van de digitale certificaten en sleutels bedraagt 2 jaar. De digitale certificaten en sleutels moeten na die 2 jaar worden vernieuwd.

### **3.2.4 HIC Online**

#### **Organisatorische dimensie**

HIC is de overheidsorganisatie die verantwoordelijk is voor algemene gezondheidsinformatie en betalingen. Het is een van de grootste organisaties in de Australische gezondheidszorg. HIC probeert haar dienstverlening in samenwerking met de Health eSignature Authority te verbeteren door middel van het inzetten van ICT in innovatieve projecten.

Een belangrijk component van elektronische dienstverlening in de gezondheidszorg is vertrouwelijke communicatie. Om dit mogelijk te maken is een PKI uitgerold binnen de gezondheidszorg, die voldoet aan het Gatekeeper scheme. De kosten voor PKI-registratie (o.a. digitale certificaten) bij de Health eSignature Authority PTY Ltd (HeSA) van abonnees zoals artsen, specialisten, apothekers en andere professionals worden gedragen door HIC. Met behulp van het HCL certificate zijn abonnees in staat om berichten elektronisch te ondertekenen en uit te wisselen met andere abonnees in de Australische gezondheidssector. Meerdere personen op een locatie kunnen gebruik maken van hetzelfde certificaat. De HCL Certificaat identificeert slechts de locatie waarvan het bericht afkomstig is. Berichten zijn niet tot een persoon herleidbaar. Daarom garandeert het HCL Certificaat niet het non-repudiation principe<sup>53</sup>.

De HIC maakt gebruik van de PKI-toepassingen voor al haar EDI- en e-business oplossingen.

#### **Technische dimensie**

De HeSA infrastructuur is gebaseerd op PKI standaarden, digitale certificaten in combinatie met tokens zoals i-keys, smartcards/smartcardreaders). Op deze manier kan gevoelige medische informatie eenvoudig via het internet worden uitgewisseld met inachtneming van de privacywetgeving en de individuele rechten van de burger.

#### **Juridische dimensie**

HeSA is tot stand gekomen onder de Corporations Law . Haar taak is het faciliteren van een PKI in de gezondheidszorg. HeSA registreert zowel individuen als locaties. HeSA is in feite de RA en Baltimore Certificates Australia Pty.Ltd. (BCAPL) treedt op als CA. Beiden, zowel HeSA als BCAPL, hebben het volledige Gatekeeper-proces doorlopen en zijn beiden volwaardig geaccrediteerd.

---

<sup>53</sup> Voor patiënten wil je anonimiteit garanderen. Echter, voor medewerkers wil je weten wie de handeling heeft uitgevoerd, de arts of de medisch secretaresse.

### 3.3 Duitsland

De Duitse aanpak ten aanzien van de elektronische handtekening is decentraal van aard. Overheidsorganisaties maken zelf een keuze of ze al dan niet online transacties met burgers willen aangaan. Er is dan ook niet zo iets als één nationaal initiatief. Verschillende overheidsorganisaties ontplooiën initiatieven of maken gebruik van een elektronische handtekening<sup>54</sup>. Hieronder volgt een aantal van deze projecten.

#### 3.3.1 Elster

##### Organisatorische dimensie

De naam Elster staat voor 'Elektronische Steuererklärung' oftewel elektronische belastingaangifte. Via het Elster-project wordt elektronische belastingaangifte via het Internet mogelijk. Elster is als pilot project in januari 1999 van start gegaan. Het percentage dat online aangifte doet is anno 2002 nog steeds laag doordat het vanuit het perspectief van de burger nog nauwelijks voordeel oplevert<sup>55</sup>. De burger moet namelijk nog altijd een korte getekende verklaring omtrent de aangifte per post versturen. Dit om aan de wetgeving te voldoen, die namelijk een schriftelijke handtekening vereist. Voor de Duitse belastingdienst is zelfs deze vorm van elektronische aangifte al zeer nuttig, omdat het een besparing oplevert in administratiekosten, de interne werkprocessen sneller kunnen verlopen, maar ook de kwaliteit van gegevens sterk is toegenomen doordat handmatige invoer aan de kant van de belastingdienst is komen te vervallen. Naast de loonbelasting zijn er bijna 10 miljoen omzetbelastingaangiften via het Internet ingediend sinds januari 2000.

De aanleiding voor dit overheidsbrede project, was de succesvolle implementatie van Elster in 1993 in een van de deelstaten, Beieren. Wat bijzonder is aan dit project voor een land als Duitsland is dat een systeem ontwikkeld door één van de deelstaten wordt overgenomen door de anderen. Dit is revolutionair omdat tot voor kort alle Duitse deelstaten eigen informatiesystemen ontwikkelden.

Binnen Elster wordt momenteel een tweede fase ingezet, waarbij gebruik wordt gemaakt van een digitale handtekening bij de belastingaangifte. Voor een periode van vijf jaar is het toegestaan om binnen het Elster-project in plaats van een 'gekwalificeerde' handtekening gebruik te maken van een elektronische handtekening die voldoet aan de eisen als gesteld in paragraaf 87 AO<sup>56</sup>: een 'gevorderde' elektronische handtekening. Het belangrijkste verschil tussen de

<sup>54</sup> In een andere Itafit-studie, *Transactiewebsites* (zie [www.itafit.nl](http://www.itafit.nl)) is een interessante case beschreven (Bremen-Online) die niet in deze studie is opgenomen.

<sup>55</sup> In 2002 dienden 540.000 Duitse belastingbetalers (minder dan 2% van het totaal) hun inkomstenbelasting via Elster in. Ter vergelijking: medio 2002 deden in Nederland 3,7 miljoen belastingbetalers (70% van het totaal) hun aangifte elektronisch.

<sup>56</sup> Projekt Elster, Pberfinanzdirektion München IT-Bereich, Stand Juli 2002.

'gekwalficeerde' elektronische handtekening en de 'gevorderde' elektronische handtekening is dat voor de 'gevorderde' elektronische handtekening geen nieuwe registratie van de eigenaar van de kaart plaats hoeft te vinden ten overstaande van de verstrekker van de kaart. Dit creëert een mogelijkheid om gebruik te maken van bestaande al werkende oplossingen ('eenmalige gegevensverstrekking').

Sinds 1 juli 2002 is de Elster software aangepast en ondersteunt Elster digitale handtekeningen. De Elster software is compatibel met meerdere kaarten en kaartlezers. In de zomer van 2002 is een pilot met de digitale handtekening van start gegaan voor de inkomensaangifte. Pilots met de nieuwe software vinden plaats in Beieren, Niedersachsen, Nordrhein-Westfalen en Saarland. In de pilotfase wordt gebruik gemaakt van bankpassen van de pilot-partners Deutsche Bank 24, HypoVereinsbank en Sparkassen Finanzgruppe. Binnen Elster is het in de pilotstaten mogelijk om met behulp van de bankpas elektronisch belastingaangifte te doen. Via deze bankpas, een smartcard, en een kaartlezer á € 50, kan men belastingaangifteformulieren digitaal ondertekenen. Een nadeel hiervan is dat de kosten die gemoeid zijn met het digitaal tekenen van documenten (certificaat en kaartlezer) vrij hoog zijn. Een grove schatting is dat ongeveer 50.000 burgers in bezit zijn van een kaart met digitale handtekening. Het merendeel van deze kaartbezitters heeft zo'n kaart omdat ze meewerken aan een pilot, bijvoorbeeld de pilot van een van de Duitse banken. Om dit voor burgers rendabel te maken moeten veel meer diensten online worden aangeboden. Naast de inkomensbelastingaangifte kan de digitale handtekening ook worden gebruikt voor voor een online verklaring omtrent het pensioenaccount van werknemers ([www.bfa.de](http://www.bfa.de)) en enkele regionale diensten waaronder diensten van de stad Bremen ([www.bremen.de/haupt.html](http://www.bremen.de/haupt.html)).

In de andere staten moet vooralsnog een deel van de aangifte via papier gebeuren. Na gebleken succes zal de nieuwe ElsterFormular 2001/SIG landelijk worden uitgerold. De verwachting is dat dit in 2003 plaats zal vinden. Dan kunnen naast de bankpassen van de bovenstaande banken ook bankpassen worden gebruikt van Deutschen Telecom (TeleSec) en de Deutsche Post (SignTrust). Deze zijn momenteel ook al compatibel.

Op termijn wordt het mogelijk om alle belastingaangiften online in te dienen.

### **Technische dimensie**

Elster is een software kernel die gebruik kan worden voor het elektronisch uitwisselen van data via het Internet tussen de belastingdienst en de eigen PC. De kernel wordt gratis verstrekt aan z'n 250 belastingprogramma ontwikkelaars die zich bevinden op de Duitse markt. De gebruikers van deze software kunnen vervolgens eenvoudig aangifte doen via het Internet.

De Elster software (Elster-2) maakt gebruik van encryptie-technologie, een server certificaat in combinatie met een SSL-verbinding die garandeert dat de software ook daadwerkelijk van de officiële site is gedownload. Daarnaast checkt een verificatieprogramma de handtekening in de software. Er wordt gebruik

gemaakt van X.509 certificaten, een internationale standaard. Zowel Windows, Linux als Mac wordt ondersteund.

Er is speciale software ontwikkeld voor het ondersteunen van de digitale handtekening binnen Elster, ElsterFormular 2001/SIG genaamd. Naast de mogelijkheid van versleutelen en verzenden via de nieuwe Elster-clientsoftware, ElsterOnlineManager EOM, kan het aangifteformulier ook worden ondertekend<sup>57</sup>.

### **Juridische dimensie**

De wet op de digitale handtekening is op 1 november 1997 in werking getreden. Deze wet heeft tot doel het creëren van een wettelijk kader voor het veilig kunnen gebruiken van de elektronische handtekening en het beschermen tegen misbruik van de handtekening door derden. De wet uit 1997 is in mei 2001 vervangen door de 'Signaturgesetz 2, Fassung'. Deze wetgeving vormt slechts het wettelijke kader. Alle sectorale wetgeving, zoals de belastingwetgeving, moet aan deze wet worden aangepast. Anders dan in bijvoorbeeld de VS valt de Duitse belastingwetgeving onder de federale wetgeving en is daardoor voor alle staten hetzelfde. De wet is aangepast waardoor het mogelijk is om belastingaangiften elektronisch te ondertekenen met behulp van een bankpas, tenminste tot 2006. De eisen als gesteld in de wet op de digitale handtekening zijn echter volgens de Belastingdienst te hoog. Op grond van de wet op de digitale handtekening is het elektronisch ondertekenen met behulp van een bankpas met elektronische handtekening niet afdoende, omdat niet aan alle eisen voor 100% wordt voldaan.

Elk van de 16 staten is echter zelf verantwoordelijk voor de administratieve verwerking van de belastingen.

### **3.3.2 SPINX: Digitale Dienstausweis**

#### **Organisatorische dimensie**

Het overheidsinitiatief BundOnline 2005 is gericht op het elektronisch leveren van overheidsdiensten in 2005. Belangrijk aspecten bij het elektronisch leveren van diensten is de zekerheid tussen ontvanger en afzender bij het uitwisselen van informatie. Een zekerheidsinfrastructuur gebaseerd op open standaarden die overal in kan worden geïntegreerd is hierbij een noodzakelijke voorwaarde. Onderdeel van z'n zekerheidsinfrastructuur is het garanderen van betrouwbare e-mail-uitwisseling via PKI en een elektronische handtekening<sup>58</sup>.

Het SPHINX-project<sup>59</sup> is een project van 'das Bundesamt für Sicherheit in der Informationstechnik' en moet vertrouwelijke communicatie garanderen tussen

<sup>57</sup> Het ondertekeningsformat is gebaseerd op Java en XML en ondersteunt het gebruik van de bankpas.

<sup>58</sup> <http://www.bund.de/BundOnline2005-.6164.htm>

<sup>59</sup> <http://www.bsi.bund.de/aufgaben/projekte/sphinx/index.htm>

zender en ontvanger en interoperabiliteit creëren tussen de afzonderlijke communicatieproducten. SPHINX is gebaseerd op PKI en wordt momenteel op alle bestuursniveaus uitgerold binnen de Duitse overheid. Hierdoor kunnen burgers, bedrijven en andere instellingen over een veilige infrastructuur elektronisch communiceren met de overheid.

De SPHINX-pilot waaraan z'n 180 medewerkers binnen de rijksoverheid, enkele ambtenaren uit de deelstaten, 2 deelnemers in het buitenland en z'n 20 medewerkers uit het bedrijfsleven deelnamen, is met succes afgesloten. De pilot zal een vervolg krijgen in de vorm van een overheidsbrede uitrol van de SPHINX standaard.

#### **Technische dimensie**

De door de Duitse overheid ontwikkelde SPHINX standaard is op PKI gebaseerd via een mechanisme van centrale openstelling van certificaten. Voor een gecontroleerd gebruik moet een centraal register worden opgesteld. Binnen SPHINX zullen de te ontwikkelen producten worden getest op interoperabiliteit. De producten zijn in ieder geval te gebruiken onder Microsoft Outlook, Lotus Notes en Novell Groupwise. Daarnaast zal in het aanverwante 'Ägypten project, software worden ontwikkeld die ook andere besturingssystemen zoals Linux zal ondersteunen. Dit ondersteunt de Open Source gedachte van de Duitse overheid. Voor de elektronische handtekening wordt gebruik gemaakt van de grondslagen en specificaties MailTrust versie 2 standaard van TeleTrust e.V.. Deze standaard is gebaseerd op internationale standaards als S/MIME, X.509v3 en PKIX standaards. De ontwikkelde software zal gratis op internet beschikbaar worden gesteld.

#### **Juridische dimensie**

SPHINX valt onder de bestaande wet- en regelgeving omtrent elektronische communicatie.

### **3.3.3 Digitaler Dienstausweis**

#### **Organisatorische dimensie**

Het project '*Digitaler Dienstausweis*' is sterk verbonden met het SPHINX-project. In november 2001 is een pilot gestart met een digitale medewerkerspas (dienstausweis) onder 70 medewerkers van 'das *Bünderamt für Sicherheit in der Informationstechnik* (BSI) en 30 medewerkers van *das Bundesministerium des Innern* (BMI). Deze pilot is in mei 2002 succesvol beëindigd. De pilot heeft laten zien dat er behoefte is aan betrouwbare communicatie.

De '*digitale dienstausweis*' is een multifunctionele chipkaart die ook zekerheidsdiensten zoals de elektronische handtekening ondersteunt. De kaart in combinatie met de kaartlezer en software om te ondertekenen en verifiëren biedt een hoogwaardig niveau van beveiliging. De ondertekeningssoftware

ondersteunt de gekwalificeerde handtekening zoals vermeld in de wet op de digitale handtekening. Naast bovenstaande functionaliteit biedt de contactloze chip op de kaart ook de mogelijkheid om aan te sluiten bij het bestaande tijdregistratiesysteem. Besloten is om de multifunctionele chipkaart onder 200.000 federale ambtenaren uit te rollen.

De benodigde infrastructuur wordt in een aantal pilots verder uitgebouwd en getest. Binnen de departementen en overheidsinstanties moeten medewerkers zich legitimeren door middel van een medewerkerspas. De bestaande pas zal worden vervangen door een digitale pas.

### **Technische dimensie**

Het digitale dienstausweis-project is in technisch opzicht gebaseerd op in de in SPHINX ontwikkelde standaarden ten aanzien van certificaten, handtekeningformaat e.d. De software voor de elektronische handtekening wordt als Plugin in MS-Office geïntegreerd. Deze Software is net als bij SPHINX gebaseerd op MailTrusT.

In technisch opzicht bestaat de chipkaart uit een aantal componenten:

- Een contactloze chip met magneetstip
- Een contactchip met certificaten: 'signatur, endnutzertzertificat zur signatur gemäss MailTrusT-Spezifikation, endnutzertzertificat zur Verschlüsselung gemäss MailTrusT-Spezifikation, endnutzertzertificat zur Authentifizierung.

De certificaten worden uitgegeven door D-Trust, een geaccrediteerde CA.

Met betrekking tot de elektronische handtekening wordt gebruik gemaakt van Single Sign On (via pincode en kaartlezer).

### **Juridische dimensie**

In juridisch opzicht is het digitale dienstausweis in overeenstemming met de eisen als gesteld in de wet Elektronische handtekening 2001, *Signaturgesetz* (SigG) 2001.

## **3.4 Verenigd Koninkrijk**

### **3.4.1 Government Gateway**

### **Organisatorische dimensie**

Binnen het UK Online programma, het nationale actieprogramma om burgers, bedrijven en overheidsorganisaties binnen de UK online te krijgen, wordt gekeken naar de mogelijkheden om een zo groot mogelijk deel van overheidstransacties online en zo veel mogelijk geïntegreerd ('joined up') te laten verlopen. De Britse overheid heeft haarzelf tot doel gesteld al haar transacties voor het eind 2005 online plaats te laten vinden.

De Government Gateway, de centrale online ingang naar de verschillende back-office organisaties, vormt de spil in dit ambitieuze programma. Government Gateway is een centrale registratiedienst voor alle e-overheidsdiensten binnen de UK.

De volgende diensten worden momenteel online aangeboden<sup>60</sup>:

- Internet Service for Self Assessment: Self Assessment tax return;
- Electronic VAT Return: VAT-registered business;
- DEFRA IACS Area Aid Application: farmers and agents who complete DEFRA forms on behalf of farmers;
- PAYE Internet Services: employees and their agents;
- Corporation TAX: organisations and their agents;
- Duty Deferment Electronic Statements: traders with deferment approval;
- DTI Export Licence Application: exporters of items controlled for strategic reasons or because of sanctions;
- Tax Credits: individuals to apply for Child Tax Credit and Working Tax Credit.

Burgers, bedrijven en tussenpersonen die online transacties met de overheid willen verrichten moeten zich eerst registreren bij de Government Gateway. Er zijn twee manieren om te registreren: door middel van een certificaat of door middel van een User ID en password combinatie. Daarnaast moet de aanvrager zich aanmelden voor een online dienst die hij/zij wenst af te nemen. Na registratie ontvangt de aanvrager in het geval dat gekozen is voor de User ID binnen zeven dagen een User ID thuis. De gebruiker kan zelf een password kiezen en deze op het registratieformulier doorgeven. Sommige diensten vereisen echter het gebruik van certificaten vanwege het hogere beveiligingsniveau. De online diensten van de Britse Belastingdienst (de 'Inland Revenue') 'PAYE Internet Services' en de 'Internet Service for Self Assessment' vereisen een laag niveau van beveiliging. De combinatie User ID en password is hiervoor voldoende. Dit wordt gezien als beveiligingsniveau 1. De HM Customs and Exise's Electronic VAT Returns en de DEFRA's IACS Area Aid Application vereisen een digitaal certificaat (niveau 2 en 3). Hierbij wordt gebruik gemaakt van een elektronische ondertekening via PKI technologie.

De Government Gateway autenticeert burgers, (personen binnen) bedrijven en tussenpersonen en na authenticatie kan men zich via een User ID in combinatie met een password of een digitaal certificaat inschrijven bij de afzonderlijke

---

<sup>60</sup> [www.gateway.gov.uk/](http://www.gateway.gov.uk/)

overheidsorganisaties voor het afnemen van online diensten (zoals het invullen van formulieren zoals loonbelasting- en BTW-teruggave).

#### **Technische dimensie**

De Government Gateway fungeert als middleware: autonome software ('self-contained' software) in combinatie met een infrastructuur die zich bevindt tussen de back-office systemen van de departementen en de front-office applicaties zoals overheidswebsites, portals en commerciële applicaties (zoals software pakketjes). De Government Gateway heeft als primaire taak het waarborgen van betrouwbare en veilige communicatie.

De Government Gateway biedt twee methoden voor authenticatie, de User ID in combinatie met een password of het digitaal certificaat (van Equifax). De User ID, maar ook de activeringscodes bestaan uit 12 'at random' gegenereerde karakters bestaande uit cijfers en letters (bijvoorbeeld 8ck3sa27u4g8). De activeringscodes worden verzonden naar het huisadres door het overheidsdepartement waarbij de eerste aanvraag voor online diensten heeft plaatsgevonden. De certificaten zijn gebaseerd op PKI technologie. Deze methode is technisch gezien zeker niet waterdicht.

#### **Juridische dimensie**

Het Gateway project valt onder de *Electronic Communications Bill*.

## 4 Trends en ontwikkelingen

In dit hoofdstuk zullen de trends en ontwikkelingen uit de voorafgaande twee hoofdstukken worden teruggekoppeld. Enkele interessante projecten hebben in de voorgaande hoofdstukken de revue gepasseerd. Aan het einde van het tweede hoofdstuk is op grond van de verworven inzichten een aantal voorlopige conclusies getrokken. Deze conclusies zullen in dit hoofdstuk worden aangevuld met de inzichten uit hoofdstuk 3.

### 4.1 Eén of meerdere handtekeningen

In de onderzochte landen zijn met betrekking tot het gebruik van de elektronische handtekening de volgende situaties aangetroffen:

- Landen met één of meerdere geavanceerde handtekening(en);
- Landen met één of meerdere gewone handtekening(en);
- Landen met zowel geavanceerde als gewone handtekening(en).

Over het algemeen wordt er nog weinig gewerkt met elektronische handtekeningen. In alle landen zijn verschillende typen handtekeningen in omloop. De meest gangbare is nog steeds de 'simpele' handtekening met behulp van conventionele beveiligingstechnieken zoals pincodes, user ID's, credit cards of combinaties daarvan. In 5 van de 11 landen worden daarnaast geavanceerde typen gebruikt – dat wel zeggen handtekeningen die voldoen aan de Europese richtlijn.

De simpele typen lijken over het algemeen afdoende oplossingen te bieden voor de problemen van individuele organisaties. De geavanceerde typen zijn moeilijk in gebruik (vgl. FINEID/ FEIDHE in Finland), de invoering is complex en kost veel tijd. Organisaties gebruiken dan conventionele (ad hoc) oplossingen als *work arounds* (pincode Nederlandse Belastingdienst etc.). Het voordeel van deze aanpak is dat je op korte termijn snel resultaten kunt boeken. Op de lange termijn moet er daarentegen veel werk worden verzet om de verschillende oplossingen naar één standaard terug te brengen. Een tussenweg is dat andere partijen de oplossing van een individuele organisatie overnemen – bij voldoende kritische massa ontstaat er zo een de facto standaard (zie bijlage 1).

Hoewel de overheden in de meeste landen in theorie zoveel mogelijk proberen aan te sluiten bij internationale (technologie)standaarden kiezen dienstverlenende organisaties in de praktijk voor eigen oplossingen. Hierdoor ontstaat de situatie dat zelfs op nationaal niveau een persoon of bedrijf reeds ver meerdere elektronische handtekeningen moet beschikken om met verschillende organisaties te kunnen communiceren. Er zijn wel ontwikkelingen gaande op het terrein van interoperabiliteit van elektronische handtekeningen. Groot-Brittannië heeft hierover bijvoorbeeld met Nederland en Zweden afspraken gemaakt.

## 4.2 Top down of bottom up?

In de meeste landen worden ontwikkelingen van uit een top-down perspectief vormgegeven. Op hoofdlijnen kunnen de volgende trends worden onderscheiden:

1. Een nationale aanpak ten aanzien van PKI en elektronische handtekening;
2. Geen nationale aanpak ten aanzien van PKI en elektronische handtekening, maar ontwikkelingen worden door afzonderlijke overheidsorganisaties van onderop aangepakt;
3. Een aantal organisaties start met de elektronische handtekening en vervolgens wordt een nationale aanpak ontwikkeld, zo veel mogelijk afgestemd op de voorlopers.

Voorbeelden van de eerste trend zijn Nederland, Verenigd Koninkrijk, Canada, Singapore en in mindere mate Japan. Kenmerkend voor deze aanpak is dat ze grootschalig en complex van opzet zijn waardoor trajecten vaak enige tijd duren voor de eerste vruchten kunnen worden geplukt.

Duitsland en Zweden zijn typische voorbeelden van de tweede trend. Het initiatief wordt in deze landen vaak genomen door afzonderlijke overheidsorganisaties. De juridische kaders zijn geregeld en het is aan de overheidsorganisaties zelf om gebruik te maken van de elektronische handtekening.

Ontwikkelingen op het gebied van de elektronische handtekening binnen Australië, maar ook binnen de Verenigde Staten werden aanvankelijk bottom-up vormgegeven. In Australië was de ATO de eerste organisatie die gebruik maakte van de elektronische handtekening. In de Verenigde Staten werd de elektronische handtekening als eerste in de private sector gebruikt. Na enkele jaren pionieren hebben beide landen besloten dat het tijd wordt voor een aanpak op nationaal niveau. Australië heeft hiertoe het Gatekeeper project opgericht met als doel het realiseren van één nationale authenticatie-infrastructuur. Binnen de Verenigde Staten wil men via het ACES-project, een federaal project, werken aan een 'web of trust', waarbij de bestaande PKI oplossingen dichterbij elkaar moeten worden gebracht.

Onze oosterburen laten treffend zien dat een grootschalige nationale aanpak niet per definitie leidt tot het beste resultaat. Een pragmatische aanpak, zie bijvoorbeeld de Belastingdienst in Beieren en bewezen nut (zie bijlage 1) lijken er voor te zorgen dat de elektronische handtekening binnen de Duitse overheid althans op korte termijn breed wordt uitgerold.

De keuze voor een van de drie aanpakken loopt dwars door de tweedeling in EU lidstaten en overige landen. Op grond van de – beperkte – gegevens kunnen we daarom concluderen dat de beperkte autonomie van lidstaten geen merkbaar effect heeft op het feitelijke gebruik van overheden in die landen van elektronische handtekeningen. De mate van gebruik van elektronische

handtekeningen lijkt met name te worden bepaald door de ontwikkelingen op sectoraal, niet op nationaal niveau. De bredere adoptie van een praktisch werkbare lokale oplossing – de bottom-up route – lijkt een belangrijker succesfactor dan de aanwezigheid van een alomvattend nationaal plan – de top-down route. De rol van de centrale overheid is dan met name gelegen in het genereren van netwerk-effecten, dat wil zeggen in het doen optreden van sneeuwbaaleffecten van succesvolle lokale oplossingen.

## Bijlage 1 – Theoretische achtergrond netwerkeffecten<sup>61</sup>

Netwerk-effecten (*network externalities*) ontstaan als het nut van een product (of dienst) wordt beïnvloed door het aantal gebruikers van dat product (Rohlf's, 1974; Farrell & Saloner, 1985, 1986; Katz & Shapiro, 1985, 1986; Katz, 1987). Met andere woorden, het nut van het individuele product komt pas naar voren op een hoger aggregatieniveau (de groep van gebruikers). Een vrije markt – die in principe is gebaseerd op een ieder-voor-zich mechanisme – voorziet niet in het aanbod van dergelijke 'merit goods'. Hier ligt dan ook van oudsher een rol voor de overheid die boven de partijen staat en vanuit het langere termijn perspectief kan handelen. In het domein van de elektronische overheid gaat het bijvoorbeeld om het instellen van standaarden (XML), basiscomponenten (elektronische handtekening, unieke nummers) en het uitrollen van infrastructures (PKI, breedbandnetwerken).

Netwerk effecten kunnen direct of indirect zijn (Bental en Spiegel, 1995). Het klassieke voorbeeld van producten met directe netwerk-effecten zijn de telefoon en de fax. Het totale nut van het systeem als geheel neemt (meer dan evenredig) toe met het aantal gebruikers. In tegenstelling tot producten zonder netwerk-effecten hebben deze producten geen enkele nut per se – hun nut bestaat puur en alleen in de aanwezigheid van andere gebruikers (Größler, Thun en Milling, 2001).

Een voorbeeld van een product met indirecte netwerk-effecten is een besturingssysteem voor computers. Hoewel het nut van het product niet direct is gerelateerd aan het aantal gebruikers treden er wel netwerk-effecten op: hoe meer mensen hetzelfde besturingssysteem gebruiken hoe meer software ervoor wordt geschreven, hoe eerder bugs worden ontdekt en nieuwe releases worden uitgebracht, hoe meer handleidingen er worden gepubliceerd, hoe meer ondersteunende diensten worden aangeboden enzovoort (Xie en Sirbu, 1995). Voor de elektronische handtekening gelden dezelfde zaken – het is een product met indirecte netwerk-effecten.

Bij de diffusie van producten met netwerk-externaliteiten treden twee effecten op die de verspreiding respectievelijk versnellen en vertragen. Het eerste effect is het zwaan kleef aan-('bandwagon') effect: hoe meer mensen afkomen op een bepaald product, hoe meer mensen erdoor aangetrokken worden. Dit effect ('mond-op-mond-reclame') treedt ook op bij conventionele producten maar is veel sterker in het geval van netwerk-externaliteiten (Serman, 2000). Het 'pinguïn'-effect is het omgekeerde van de zwaan kleef aan-effect: hoe meer mensen koudwatervrees hebben bij het gebruik van een nieuw product, hoe meer mensen ook soortgelijke twijfels krijgen<sup>62</sup>. Het 'pinguïn'-effect speelt met

<sup>61</sup> Auteur: Robbin te Velde. Bijlage 1 is grotendeels gebaseerd op Größler, Thun en Milling (2001).

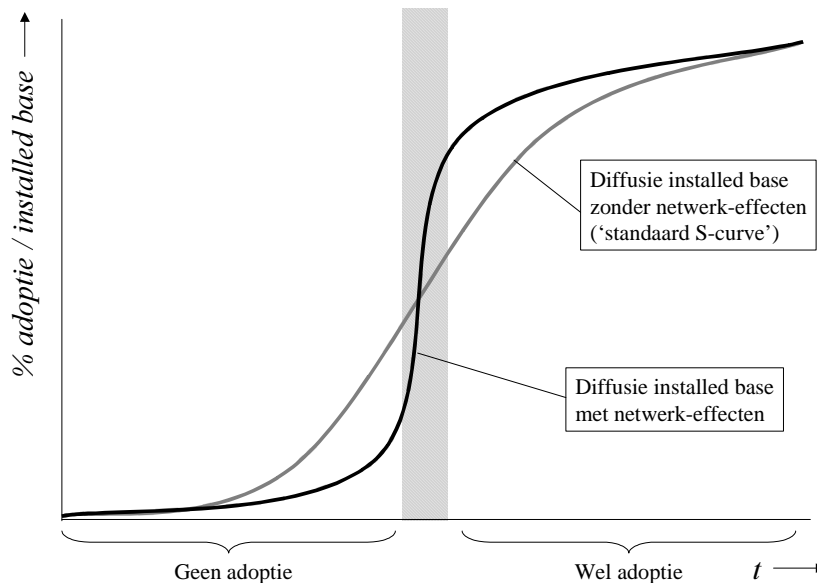
<sup>62</sup> Ontleend aan Farrell en Saloner: "Penguins who must enter the water to find food often delay doing so because they fear the presence of predators. Each

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

name in de eerste fasen van de diffusie (wanneer nog maar weinig mensen het product gebruiken), het zwaan kleef aan-effect met name in de latere fasen. De (voortdurend veranderende) verhouding tussen het aantal adopters en non-adopters beïnvloedt echter gedurende de gehele levensspan van een product de verloop van de diffusie van het product. Een plotselinge afwijzing door een relatief klein aantal (ex-)gebruikers bijvoorbeeld kan ook in latere fasen een lawine-effect veroorzaken waardoor de vraag naar het product instort.

De aanwezigheid van netwerk-effecten zorgt voor een steiler verloop van de diffusie S-curve (zie ). Het omslagpunt waarop er voldoende kritische massa is bereikt voor een verdere autonome verspreiding van het product is daardoor veel radicaler dan in het geval van conventionele producten.

**Figuur 1 - Invloed netwerkeffecten op diffusie van een product**



In het simulatiemodel voor de diffusie van producten met netwerk externaliteiten dat Größler, Thun en Milling (2001) hebben ontwikkeld spelen een viertal variabelen een cruciale rol:

1. patience of users with the installed based (PATIENCE)
2. willingness of potential users to take risk (RISK)
3. desired utility of users (DESIRED UTILITY)
4. interest of users in theoretically possible communication relations (RELEVANT ADOPTER FRACTION).

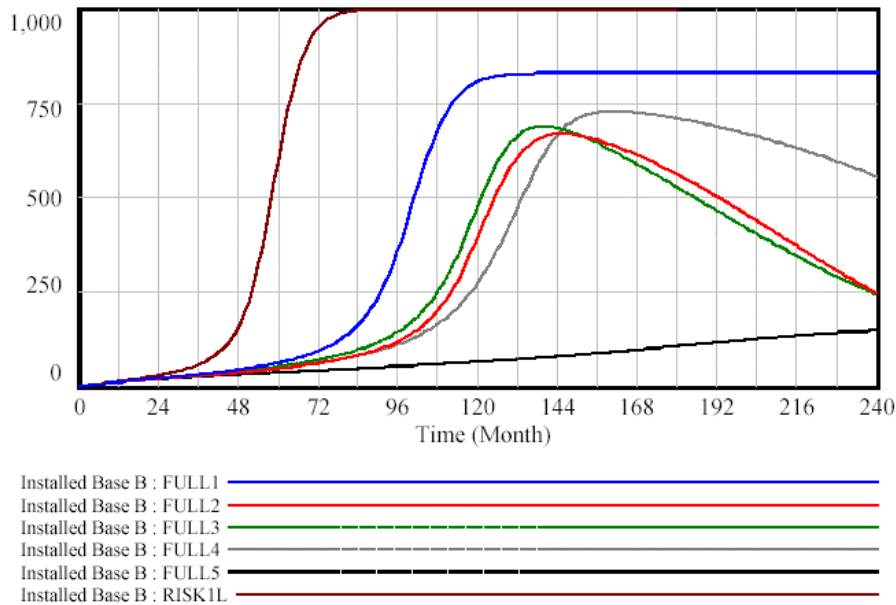
In de onderstaande runs (figuur 2) zijn alleen de eerste drie variabelen beschouwd. RISK1L is de referentiecurve: dit is het nul-scenario waarin

would prefer some other penguin to test the water first." (1986:943).  
Koudwatervrees moet hier dus letterlijk worden opgevat...

Lammers (2002), Elektronische Handtekening, Den Haag: Itafit.

PATIENCE, RISK en DESIRED UTILITY nog niet zijn meegenomen. FULL1 is dezelfde referentiecurve maar nu met PATIENCE – de andere twee variabelen zijn positief ingesteld. In de scenario's FULL2, FULL3 en FULL4 is telkenmale een van de drie variabelen negatief gezet. Hieruit kan worden afgeleid dat er alleen een stabiel patroon ontstaat (RISK1L en FULL1) als alle variabelen positief worden gezet. De belangrijkste conclusie is dat gebruikers niet (althans niet op langere termijn) kunnen worden verlost cq. overreed om een product te gebruiken dat voor hun klaarblijkelijk weinig nut heeft. Met andere woorden, er zijn maar weinig situaties waarin 'lock-in' optreedt. Notoire criticasters uit de neo-klassieke school van economen – volgens welk discours historie per definitie geen rol kan spelen – betwijfelen dan ook de empirische relevantie van de theorie van netwerk-externaliteiten (Liebowitz en Margolis, 1994; 1999).

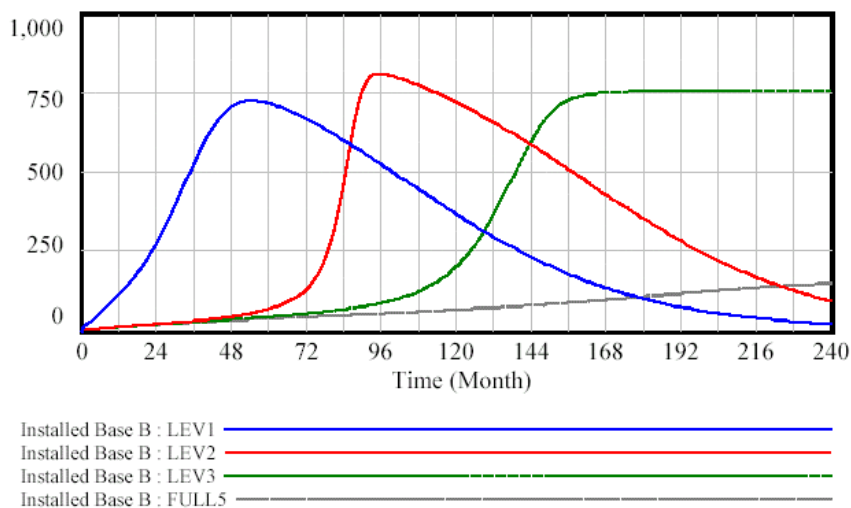
**Figuur 2 – Diffusie met netwerk-effecten volgens verschillende scenario's**



Op theoretische gronden kan desalniettemin worden gesteld dat de diffusie van producten met netwerk-externaliteiten is gebaat bij een zo snel mogelijke toename van het totale aantal gebruikers. Dit kan worden gedaan door zoveel mogelijk mensen van het nut van het product te overtuigen (bijvoorbeeld door middel van reclame) of door de 'contact rate' tussen de adopters en non-adopters te intensiveren. Geen van beide strategieën leidt echter tot duurzame resultaten.

De enige variabele waarop wel een strategie kan worden gebaseerd die leidt tot structurele verspreiding is de vierde variabele, RELEVANT ADOPTER FRACTION. De overige variabelen gaan uit van een theoretisch maximale installed base van 100%. In sommige gevallen (bijvoorbeeld ICQ) is een gebruiker niet geïnteresseerd in de gehele theoretische populatie gebruikers maar slechts in een deelverzameling van die populatie (vrienden en bekenden). De verhouding tussen het theoretische en gewenste aantal gebruikers neemt daardoor toe. Dit versterkt het zwaan kleef aan- en verzwakt het pinguïneffect. Wanneer de RELEVANT ADOPTER FRACTION boven de 50% uitkomt wordt er een plotseling omslagpunt bereikt (zie figuur 3) waardoor er een situatie van structurele verspreiding ontstaat (LEV3). Blijft deze verhouding onder de 50% (LEV1; LEV2) valt de verspreiding op termijn weer terug tot vlak bij het nulpunt.

**Figuur 3 – Diffusie met netwerkeffecten en kleinere theoretische maximale populaties**



De RELEVANT ADOPTER FRACTION kan worden verhoogd door het aantal interessante communicatiepartners voor de bestaande gebruikers in de installed base te vergroten. Größler, Thun en Milling suggereren daarvoor een drietal (beleids)maatregelen:

1. Gebruikers met voorheen onbekende mensen in contact brengen (bijvoorbeeld door het oprichten van (virtuele) 'communities').
2. Nieuwe functionaliteiten toevoegen aan bestaande producten waardoor nieuwe gebruikers kunnen worden bereikt (bijvoorbeeld SMS als toevoeging aan GSM; SMS maakt het ook mogelijk om berichten naar meerdere ontvangers tegelijkertijd te versturen [multicast]; geldt ook voor email).

3. De installed base uitbreiden door haar compatible te maken met de installed base van andere producten – zie ook voetnoot 10.

Al deze maatregelen zijn ceteris paribus ook relevant voor de invoering van de elektronische handtekening, dat wil zeggen voor het genereren van voldoende kritische massa om het omslagpunt in de diffusiecurve te bereiken.

#### Literatuur

- Bental, B. en M. Spiegel (1995). Network Competition, Product Quality, and Market Coverage in the Presence of Network Externalities. *Journal of Industrial Economics* 43(2): 197-208.
- Farrell, J. en G. Saloner (1985). 'Standardization, Compatibility, en Innovation'. *Rand Journal of Economics* 16:70-83.
- Farrell, J. en G. Saloner (1986). 'Installed Base and Compatibility: Innovation, Product Announcements, and Predation'. *American Economic Review* 76:940-955.
- Größler, A., J-H. Thun en P.M. Milling (2001). *The Diffusion of Goods Considering Network Effects: A System Dynamics-Based Approach*. Working paper at Industry Seminar Mannheim University.
- Katz, M. (1987). 'The Welfare Effects of Third Degree Price Discrimination in Intermediate Goods Markets', *American Economic Review* 77:154-167.
- Katz, M. en C. Shapiro (1985). 'Network Externalities, Competition, and Compatibility'. *American Economic Review* 75:424-440.
- Katz, M. en C. Shapiro (1986). 'Technology Adoption in the Presence of Network Externalities'. *Journal of Political Economy* 94:822-841.
- Liebowitz, S.J. en S.E. Margolis (1994). 'Network Externality; An Uncommon Tragedy'. *Journal of Economical Perspectives* 8(2).
- Liebowitz, S.J. en S.E. Margolis (1999). *Winners, Losers, en Microsoft: How Technology Markets Choose Products*. The Independent Institute.
- Rohlf, J. (1974). 'A Theory of Interdependent Demand for a Communication Service'. *Bell Journal of Economics* 5:16-37.
- Xie, J. en M. Sirbu. (1995). Price Competition and Compatibility in the Presence of Positive Demand Externalities. *Management Science* 41(5): 909:926.
- Sterman, J.D. (1987). Expectation Formation in Behavioral Simulation Models. *Behavioral Science* 32, 190-211.